RÉSUMÉ THÉORIQUE – FILIÈRE INFRASTRUCTURE DIGITALE

Option Cybersécurité

M212 – Assurer le durcissement des systèmes et des réseaux informatiques

40 heures

SOMMAIRE

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

PARTIE 1

Présenter les normes et standards de durcissement

Dans ce module, vous allez :

- Connaître la définition et les objectifs du durcissement
- Analyser les normes et les standards du durcissement
- S’initier aux bonnes pratiques de l’administration sécurisée

6 heures

CHAPITRE 1

Identifier les normes et référentiels de durcissement

Ce que vous allez apprendre dans ce chapitre :

- Le cadre des normes ANSSI
- Le cadre et les bases du référentiel CIS

2 heures

CHAPITRE 1

Identifier les normes et référentiels de durcissement

1. **Normes ANSSI**
2. Référentiel CIS

Durcissement : Définitions

- Le **Durcissement** des systèmes d'information fait partie des principes les plus importants de la sécurité des SI. À mesure que les SI évoluent, le durcissement doit être ajusté pour suivre l'évolution de la technologie du système d'exploitation.
- Le durcissement consiste à réduire la surface d'attaque disponible pour l'attaque.
- Cela rentre dans les principes du :
  - ✓ Zero trust
  - ✓ Sécurité en profondeur
  - ✓ Moindres privilèges
- Le principe des 3D est compris dans cette partie :
  - ✓ Deter (Dissuader)
  - ✓ Deny (Bloquer)
  - ✓ Delay (Retarder)

- Nous détaillerons ces principes généraux avant de passer aux normes et référentiels qui se basent principalement sur ces principes.

01 – Identifier les normes et référentiels de durcissement

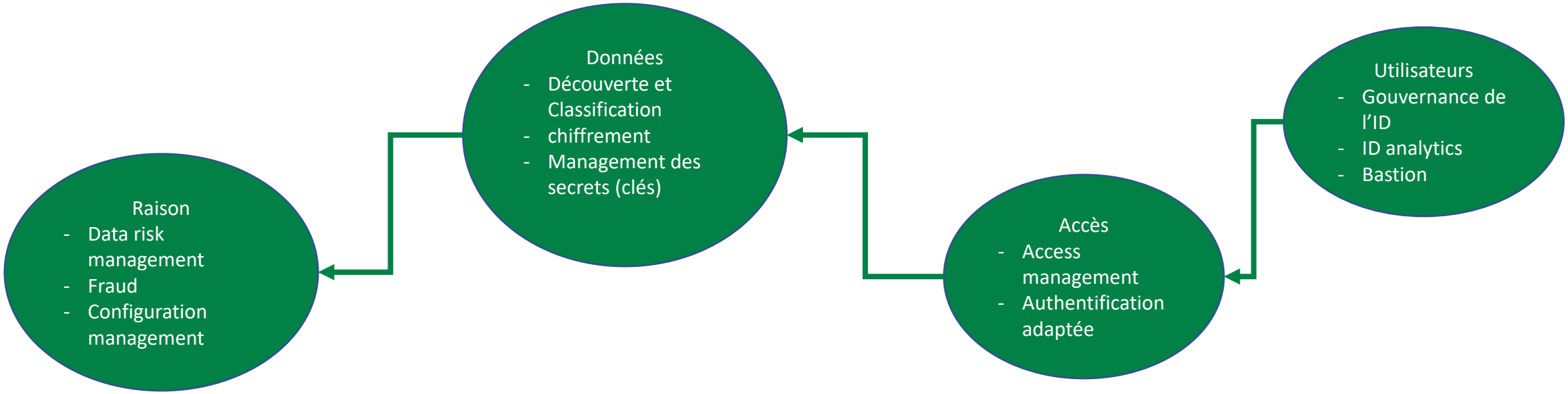
Normes ANSSI

Principe : zero trust

- Le principe de zéro trust peut être résumé de la manière suivante :

"Seulement les utilisateurs légitimes qui ont seulement les bons accès seulement aux justes données pour seulement la bonne raison"

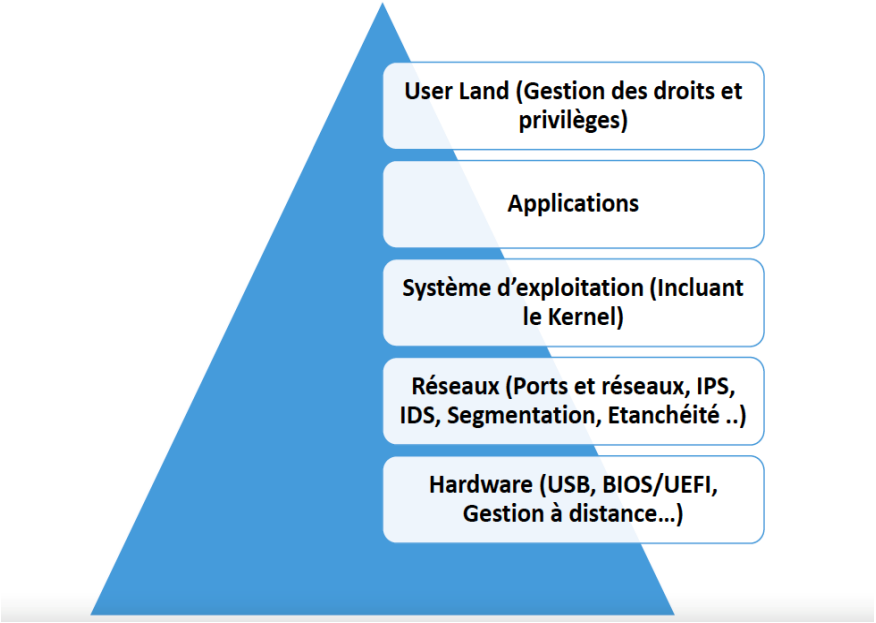
"Only right users have only the right access to only the right data for only the right reason"



PARTIE 1

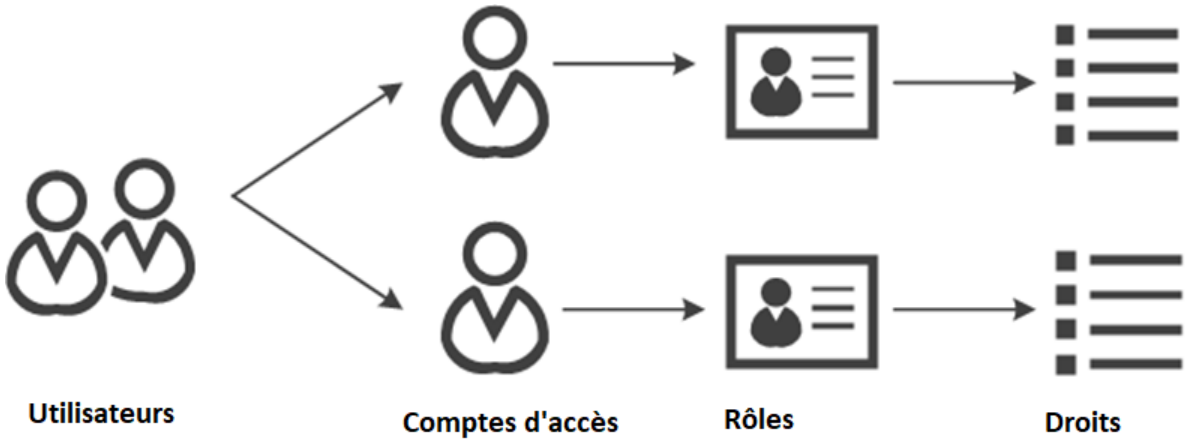
Principe : sécurité en profondeur

- Le principe de sécurité en profondeur impose la conception de plusieurs couches de sécurité indépendantes et complémentaires en vue de retarder un attaquant dont l'objectif est la compromission du système.
- Chaque couche de sécurité est donc un point de résistance que l'attaquant doit franchir. La mise en défaut d'une couche s'accompagne de signaux, d'alarme ou de messages de journalisation permettant de détecter une activité suspecte et de pouvoir y réagir. L'étape de remédiation se trouve aussi facilitée grâce aux informations supplémentaires agrégées sur le contexte de la compromission.
- Ce principe a donc un réel avantage : détection, facilité de remédiation et amélioration de la sécurité.



Principe : moindres privilèges

- Le principe de moindres privilèges ou principe de minimisation indique que les systèmes conçus et installés doivent éviter autant que possible toute complexité inutile en vue de :
  - ✓ Réduire la surface d'attaque au strict minimum
  - ✓ Permettre une mise à jour et un suivi du système efficace
  - ✓ Rendre l'activité de surveillance des systèmes plus accessible, dans la mesure où le nombre de composants à surveiller est réduit



01 – Identifier les normes et référentiels de durcissement

Normes ANSSI

ANSSI

- ANSSI (Agence nationale de la sécurité des systèmes d'information) est l'autorité nationale française en matière de sécurité et de défense des systèmes d'information, l'ANSSI constitue un réservoir de compétences qui assiste les administrations et les opérateurs d'importance vitale.
- Elle est chargée de la promotion des technologies, des systèmes et des savoir-faire nationaux. Elle contribue au développement de la confiance dans le numérique.
- Pour sensibiliser aux bonnes pratiques de sécurité numérique et accompagner les entreprises et administrations dans la mise en œuvre de ces mesures de sécurité, l'ANSSI produit de nombreux documents destinés à des publics variés.
- Des guides techniques aux recueils de bonnes pratiques élémentaires en passant par les infographies, l'agence autorise et encourage le téléchargement, le partage et la réutilisation de ces informations dans le respect des conditions de réutilisation de l'information publique ou de la Licence ETALAB, qui prévoient la mention explicite de l'auteur, de la source et de la version de l'information.

ANSSI Agence nationale de la sécurité des systèmes d'information

PARTIE 1

Normes ANSSI

- ANSSI se base sur les grands principes des slides précédentes pour produire des guides de recommandations pour durcir plusieurs systèmes. Nous pouvons citer parmi ces guides les plus connus et les plus utilisés :

✓ **RECOMMANDATIONS DE CONFIGURATION D'UN SYSTÈME GNU/LINUX :** se concentre principalement sur des directives de configuration système génériques et des principes de bon sens qu'il convient d'appliquer lors du déploiement de services sur un système GNU/Linux.

✓ **RECOMMANDATIONS RELATIVES À L'ADMINISTRATION SÉCURISÉE DES SYSTÈMES D'INFORMATION :** décrit les objectifs de sécurité et les principes d'élaboration d'une architecture technique sécurisée d'administration. Il propose des éléments utiles d'aide à la conception. Il présente quelques cas d'usages concrets mais n'a pas vocation à être exhaustif.

✓ **SÉCURISER UN SITE WEB :** concerne la sécurité des contenus présentés par un navigateur web aux utilisateurs. Les sujets abordés se concentrent autour des standards du Web, dont les implémentations côté navigateur requièrent des paramètres à spécifier lors du développement et de l'intégration d'un site ou d'une application web, de façon à en garantir la sécurité.

✓ **RECOMMANDATIONS DE SÉCURITÉ RELATIVES À ACTIVE DIRECTORY :** fournit des recommandations et des procédures permettant la sécurisation d'un annuaire AD.

CHAPITRE 1

Identifier les normes et référentiels de durcissement

1. Normes ANSSI
2. **Référentiel CIS**

01 – Identifier les normes et référentiels de durcissement

Référentiel CIS

CIS

- Le Center for Internet Security (CIS) est une organisation à but non lucratif créée en octobre 2000. Sa mission est de faire du monde connecté un endroit plus sûr en développant, validant et promouvant des solutions opportunes de meilleures pratiques qui aident les personnes, les entreprises et les gouvernements à se protéger contre les cybermenaces omniprésentes.
- CIS utilise un modèle de crowdsourcing fermé pour identifier et affiner les mesures de sécurité efficaces, les individus développant des recommandations qui sont partagées avec la communauté pour évaluation par le biais d'un processus de prise de décision par consensus. Au niveau national et international, le CIS joue un rôle important dans l'élaboration des politiques et des décisions de sécurité en maintenant les contrôles et les repères du CIS, et en hébergeant le Centre de partage et d'analyse d'informations multi-États (MS-ISAC) et l'infrastructure électorale Centre de partage et d'analyse de l'information (EI-ISAC)

CIS® Center for Internet Security®

PARTIE 1

CIS Benchmark

- Les benchmarks du Center of Internet Security (CIS) sont un ensemble de bonnes pratiques reconnues mondialement et faisant l'objet d'un consensus pour aider les praticiens de la sécurité à mettre en œuvre et à gérer leurs défenses de cybersécurité. Élaborées avec une communauté mondiale d'experts en sécurité, les directives aident les organisations à se protéger de manière proactive contre les risques émergents. Les entreprises mettent en œuvre les directives du Benchmark CIS afin de limiter les vulnérabilités de sécurité liées à la configuration de leurs actifs numériques.

- Nous pouvons citer parmi ces guides les plus connus et les plus utilisés :
  - ✓ L'authentification multifactorielle
  - ✓ CIS AWS Foundations Benchmark
  - ✓ Windows Server 2016 Benchmark
  - ✓ CIS F5 Benchmarks

CIS Benchmark : les avantages

- En adoptant les benchmarks CIS, l'organisation peut bénéficier de plusieurs avantages en matière de cybersécurité, tels que :

✓ **Directives expertes en matière de cybersécurité :** un cadre de configurations de sécurité qui sont contrôlées par des experts et qui ont fait leurs preuves. Les entreprises peuvent éviter les scénarios par tâtonnement, qui mettent la sécurité en danger, et bénéficier de l'expertise d'une communauté informatique et de cybersécurité diversifiée.

✓ **Normes de sécurité reconnues mondialement :** grâce à la communauté mondiale et diversifiée qui travaille sur un modèle décisionnel basé sur le consensus, les benchmarks CIS ont une applicabilité et une acceptabilité bien plus larges que les lois et les normes de sécurité régionales.

✓ **Prévention rentable des menaces :** l'objectif est d'atteindre une gouvernance informatique et éviter les dommages financiers et de réputation causés par des cybermenaces évitables.

✓ **Conformité règlementaire :** les benchmarks CIS s'alignent sur les principaux cadres de sécurité et de confidentialité des données, tels que (PCI DSS, RGPD, etc.).

CIS Benchmark : les catégories

- Les technologies couvertes par les benchmarks CIS peuvent être regroupées dans les sept catégories suivantes :

✓ **Systèmes d'exploitation :** les benchmarks CIS pour les systèmes d'exploitation fournissent des configurations de sécurité standards pour les systèmes d'exploitation populaires.

✓ **Infrastructure cloud et services :** les benchmarks CIS pour l'infrastructure cloud fournissent des normes de sécurité que les entreprises peuvent utiliser pour configurer en toute sécurité les environnements cloud.

✓ **Logiciel de serveur :** les benchmarks CIS pour les logiciels de serveur fournissent des bases de configuration et des recommandations pour les paramètres du serveur, les contrôles d'administration du serveur, les paramètres de stockage et les logiciels de serveur des fournisseurs les plus populaires.

✓ **Logiciels de bureau :** les benchmarks CIS couvrent la plupart des logiciels de bureau que les organisations utilisent généralement.

✓ **Appareils mobiles :** les benchmarks CIS pour les appareils mobiles couvrent les configurations de sécurité pour les systèmes d'exploitation qui fonctionnent sur les téléphones mobiles, les tablettes et autres appareils portatifs.

✓ **Périphériques réseau :** les benchmarks CIS fournissent également des configurations de sécurité pour les périphériques réseau tels que les pare-feu, les routeurs, les commutateurs et les réseaux privés virtuels (VPN).

✓ **Périphériques d'impression multifonctions :** les benchmarks CIS pour les périphériques réseau tels que les imprimantes multifonctions, les scanners et les photocopieurs couvrent les bonnes pratiques de configuration sécurisée telles que les paramètres de partage de fichiers, les restrictions d'accès et les mises à jour de micrologiciels.

CIS Benchmark : les niveaux

- Les organisations peuvent choisir un profil en fonction de leurs besoins en matière de sécurité et de conformité.

✓ **Profil niveau 1 :** les recommandations de configuration pour le profil de niveau 1 sont des recommandations de sécurité de base pour la configuration des systèmes informatiques. Elles sont faciles à suivre et n'ont pas d'impact sur les fonctionnalités ou le temps d'activité de l'entreprise. Ces recommandations réduisent le nombre de points d'entrée dans vos systèmes informatiques, diminuant ainsi vos risques en matière de cybersécurité.

✓ **Profil niveau 2 :** les recommandations de configuration du profil de niveau 2 fonctionnent mieux pour les données hautement sensibles où la sécurité est une priorité. La mise en œuvre de ces recommandations nécessite une expertise professionnelle et une planification minutieuse pour obtenir une sécurité complète avec un minimum de perturbations. La mise en œuvre des recommandations de profil de niveau 2 aide également à atteindre une conformité réglementaire.

✓ **Profil STIG :** le Security Technical Implementation Guide (STIG) est un ensemble de lignes de base de configuration de la Defense Information Systems Agency (DISA). Le ministère américain de la Défense publie et maintient ces normes de sécurité. Les STIG sont spécifiquement rédigées pour répondre aux exigences du gouvernement américain.

CHAPITRE 2

Connaître les bonnes pratiques de l'administration sécurisée

Ce que vous allez apprendre dans ce chapitre :

- Les bonnes pratiques pour administration sécurisée
- Les outils d'administration
- Les outils utilisés dans le durcissement

2 heures

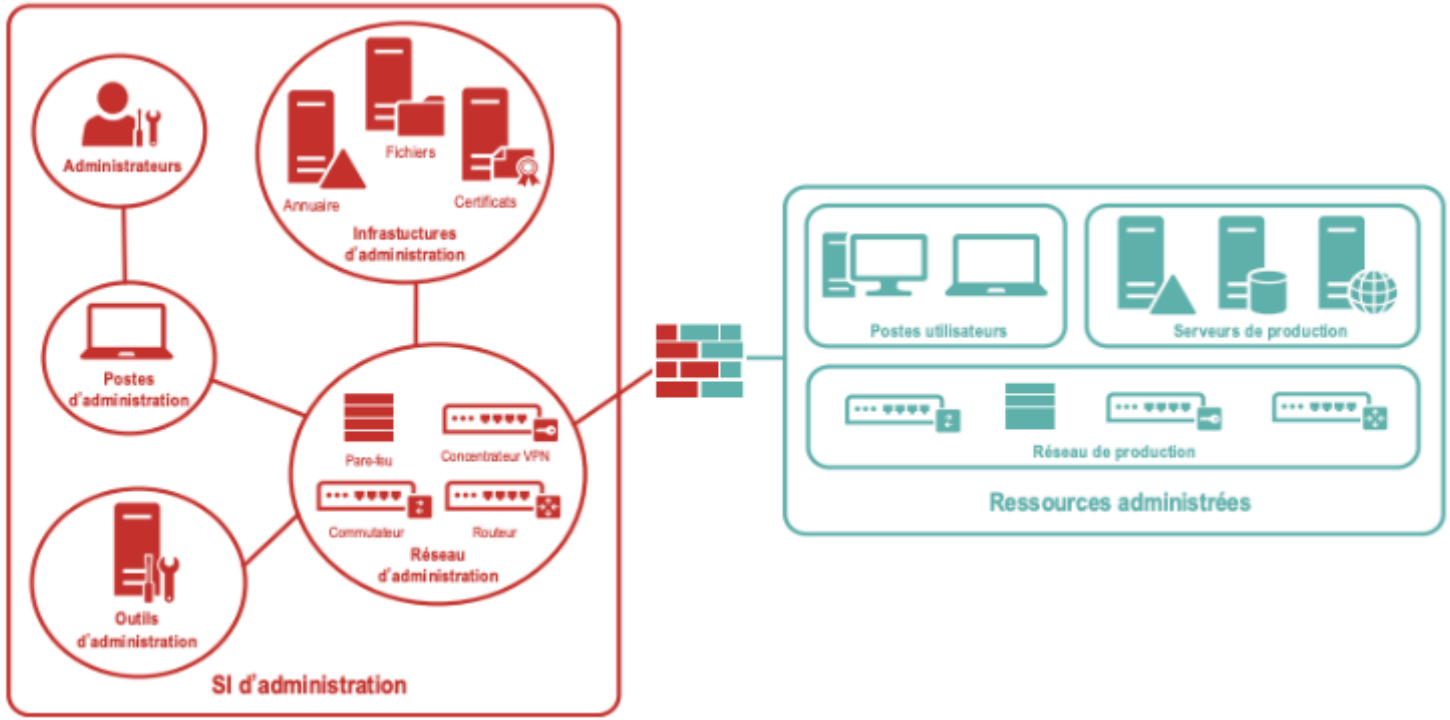
CHAPITRE 2

Connaître les bonnes pratiques de l'administration sécurisée

1. **SI d'administration (bastion)**
2. Outils d'administration (local/centralisé)
3. Automatisation des règles de durcissement (Lynis, PingCastle, CIS-CAT)

SI d'administration

- Dans le système d'information global d'une organisation, le système d'information d'administration est le système d'information utilisé pour administrer des ressources qui sont présentes dans un autre SI dit SI administré, distinct du SI d'administration.

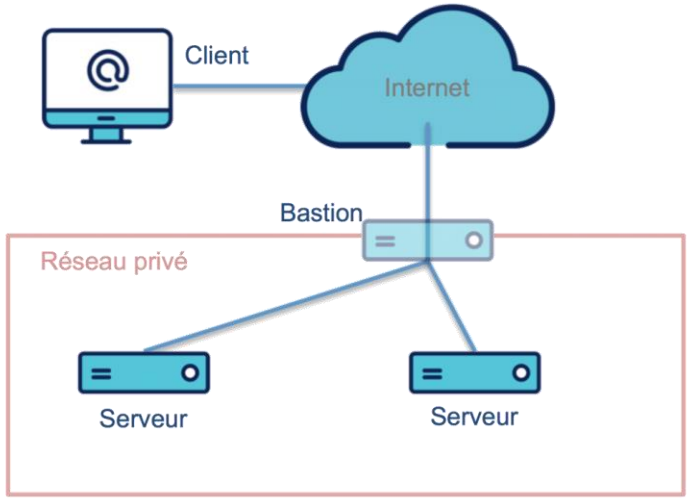


Source :https://www.ssi.gouv.fr/uploads/2018/10/guide_anssi_secure_admin_is_pa_022_en_v2.pdf

PARTIE 1

SI d'administration : bastion

- Dans le SI d'information, nous avons plusieurs ressources d'administration, qui sont l'ensemble des dispositifs physiques ou virtuels du SI d'administration : poste d'administration, serveurs d'infrastructures d'administration, serveurs outils d'administration, équipements de réseau d'administration, etc. ; et en fonction du juste besoin opérationnel.
- Le bastion est une ressource essentielle dans un SI d'administration. Le bastion d'administration renforce la protection de vos comptes administrateurs. Cette solution vous permet d'avoir un point d'accès unique à votre réseau via une passerelle HTTPS. Elle fait office de proxy et SSH entre vos ressources et les utilisateurs qui ont besoin d'y accéder. Elle offre une protection plus fine de l'ensemble des accès à privilège, occupant ainsi une place maitresse dans votre arsenal de protection.
- Il existe sur le marché des produits nommés bastions d'administration ou plus simplement bastions. Il s'agit d'une déclinaison du rebond. Ces équipements concentrent généralement plusieurs fonctions de sécurité, comme par exemple la gestion centralisée de l'authentification, la traçabilité, le renouvellement automatique des secrets.



Source: https://blog.octo.com/wp-content/uploads/2018/01/a-principes-de-base-1-1024x771.png

PARTIE 1

SI d'administration : bastion

- Le déploiement d'un bastion pour les actions d'administration ne se substitue évidemment pas à l'ensemble des outils de sécurité, notamment le cloisonnement du SI d'administration et la sécurisation du poste d'administration. En effet, le bastion constitue une ressource d'administration critique dans la mesure où il concentre potentiellement à un instant des secrets d'authentification des comptes d'administration ou des journaux liés aux actions d'administration. Il ne doit donc pas être exposé sur un SI de faible niveau de confiance, un SI bureautique par exemple.
- Un Bastion permet de compartimenter les utilisateurs, les règles d'accès et les serveurs cibles pour s'assurer que seulement le bon utilisateur pourra accéder à la bonne ressource, avec les bons droits. Ainsi, aucune personne tierce ne pourra accéder à vos ressources et corrompre votre travail.
- Parmi les technologies Bastion les plus utilisées sur le marché, nous pouvons citer :

ONE IDENTITY by Quest

WALLIX CYBERSECURITY SIMPLIFIED

CYBERARK®

SI d'administration : bastion

- Les avantages à espérer d'une solution de Bastion sont les suivants : (cela dépendra de la technologie utilisée)

- ✓ **Authentification multifacteur :** la solution Bastion doit prendre en charge l'authentification multifacteur à l'aide d'OTP mobile, de mots de passe de messagerie, de clés physiques, etc., en fonction du rôle de l'utilisateur. Une autre bonne idée consiste à déployer MFA à chaque point de demande et pas seulement au moment de la connexion. Bastion doit également s'intégrer à un MFA tiers pour une protection supplémentaire.
- ✓ **Pistes d'audit pour la conformité :** l'une des raisons les plus courantes pour lesquelles les entreprises mettent en œuvre des solutions de gestion des accès privilégiés est d'assurer une piste d'audit des activités d'accès. La solution doit conserver des enregistrements détaillés des tentatives de connexion et des approbations d'accès, de préférence sous forme de documentation et de formats vidéo. Ceux-ci doivent être enfermés dans un coffre-fort sécurisé.

PARTIE 1

SI d’administration : bastion

- ✓ **Coffres-forts de mots de passe :** les coffres-forts d'une solution Bastion stockent des données confidentielles telles que les identifiants d'accès, les mots de passe, les enregistrements de conformité, les enregistrements d'écran, les données de frappe, etc. Le coffre-fort doit être entièrement chiffré et accessible de manière centralisée pour une seule source de visibilité sur l'activité d'accès dans toute l'organisation.

- ✓ **Prise en charge des systèmes distants :** l'accès à distance sécurisé est désormais un incontournable de l'organisation avec l'essor du télétravail. Outre les utilisateurs internes distants, vous devez également surveiller et enregistrer les accès privilégiés des comptes invités, tels que les fournisseurs de confiance, les auditeurs externes, les employés contractuels, etc. Bastion placera votre entreprise distribuée sous votre parapluie de sécurité sans aucun risque d'exposition.

- ✓ **Prise en charge des environnements d'hébergement hybrides :** votre solution Bastion doit être en mesure de gérer et de suivre l'accès aux entrepôts de données traditionnels, aux applications de cloud public/privé et aux applications SaaS basées sur le Web. Parallèlement à cela, il devrait y avoir une protection d'application à application, afin que les privilèges d'un environnement ne «s'infiltrent» pas dans des activités ailleurs.

- ✓ **Intégrations SIEM :** en s'intégrant à votre logiciel de gestion des informations et des événements de sécurité (SIEM), Bastion peut directement envoyer des alertes de sécurité, générer des tickets et déclencher une correction automatisée. Les intégrations Bastion-SIEM peuvent vous faire économiser une quantité considérable d'efforts informatiques, car il existe des workflows d'approbation connectés sans fragmenter la piste d'audit.

- ✓ **Gouvernance des flux de travail d'accès :** la fonction de gestionnaire de flux de travail de Bastion vous permet de définir et d'appliquer des règles de sécurité pour différentes conditions d'accès. Il détermine comment l'utilisateur obtient l'accès et les scénarios dans lesquels l'accès peut être réinitialisé ou révoqué.

CHAPITRE 2

Connaître les bonnes pratiques de l’administration sécurisée

1. SI d’administration (bastion)
2. **Outils d’administration (local/centralisé)**
3. Automatisation des règles de durcissement (Lynis, PingCastle, CIS-CAT)

Outils d’administration

- Bien que le Bastion soit l’élément le plus important des ressources d’administration, il existe aussi d’autres outils d’administration qui permettent la réalisation d’actions d’administration, qui sont mis à disposition des administrateurs, soit localement sur leur poste d’administration soit de façon déportée et centralisée sur des serveurs.
- Un outil d'administration à distance ou centralisé est un outil qui donne à l’administrateur le contrôle total ou partiel à des fonctionnalités et des ressources technologiques à distance. Nous pouvons en citer quelques uns connus sur le marché :
    - Dameware Remote Support
    - Atera
    - ISL Online

- Un outil d’administration local est ou un outil installé ou connecté directement sur des ressources technologiques et qui donne à l’administrateur le contrôle total ou partiel à des fonctionnalités des ressources administrées. Nous pouvons citer quelques uns connus sur le marché :
    - ADManager Plus
    - AD Pro toolkit
    - phpMyAdmin

ManageEngine ADManager Plus

phpMyAdmin

Outils d'administration : sécurisation

- Ces outils d'administration donnent en général des accès privilégiés aux administrateurs. C'est pour cette raison qu'ils sont parmi les cibles intéressantes des cyberattaques.
- Dans le cas d'outils d'administration locaux au poste d'administration, le cloisonnement par zone d'administration est difficilement applicable. Il est rappelé que ces outils doivent être déployés en fonction du strict besoin opérationnel conformément aux principes suivants :
  - ✓ Dresser et maintenir la liste des outils d'administration utiles
  - ✓ Mettre en œuvre un processus de validation et de distribution des outils d'administration suivant des critères techniques et organisationnels

- Dans le cas d'outils d'administration centralisés, la mise en œuvre de serveurs dédiés par zone d'administration permet la mise en œuvre du cloisonnement recherché et facilite la mise à jour des outils.
  - ✓ Déployer les outils d'administration sur des serveurs dédiés par zone d'administration
  - ✓ Appliquer un filtrage entre les postes d'administration et les serveurs outils d'administration

CHAPITRE 2

Connaître les bonnes pratiques de l'administration sécurisée

1. SI d'administration (bastion)
2. Outils d'administration (local/centralisé)
3. **Automatisation des règles de durcissement (Lynis, PingCastle, CIS-CAT)**

Automatisation des règles de durcissement

- Pour des objectifs de conformité, les standards CIS et ANSSI ou d'autres sont de plus en plus utilisés. Cependant, le nombre de règles de vérification est souvent très élevé et la remédiation des écarts peut s'avérer encore plus longue et répétitive quand il s'agit de passer sur des milliers de serveurs.
- Dans cette situation là, l'automatisation des vérifications des règles de durcissement devient indispensable. L'automatisation de l'application des corrections est aussi intéressante, mais doit être mieux préparée et contrôlé surtout dans un environnement de production.
- Beaucoup d'outils payants ou open source sont utilisés et donnent satisfaction sur plusieurs plans. Dans ce guide nous allons présenter 3 outils qui vont nous permettre de couvrir l'automatisation du durcissement sur plusieurs types d'OS et de technologies :

  - **Lynis** est un outil de sécurité pour les systèmes exécutant un système d'exploitation Linux, macOS ou Unix. Il effectue une analyse approfondie de l'état de vos systèmes pour prendre en charge le durcissement du système et les tests de conformité. Le projet est un logiciel open source avec la licence GPL et disponible depuis 2007.

  - **PingCastle** fournit des indicateurs de sécurité Active Directory. L'outil lance une batterie de requêtes AD (LDAP ou AD webservice) pour vérifier un ensemble de bonnes pratiques et de configurations.

  - **CIS-CAT** proposé par CIS en version pro payante et en version Lite gratuite, c'est un outil d'évaluation de la configuration qui compare la configuration des systèmes cibles aux paramètres de configuration sécurisés recommandés dans les benchmarks CIS dans un contenu lisible par ordinateur.

Automatisation des règles de durcissement : Lynis

- **Lynis** n'effectuera aucun durcissement du système automatiquement, mais il vous proposera des suggestions qui vous montreront comment vous pouvez renforcer vous-même le système. En tant que tel, il sera utile si vous avez une connaissance fondamentale de la sécurité du système Linux. Vous devez également être familiarisé avec les services exécutés sur la machine que vous prévoyez d'auditer, tels que les serveurs Web, les bases de données et les autres services que Lynis peut analyser par défaut. Cela vous aidera à identifier les résultats que vous pouvez ignorer en toute sécurité.
- Sur une distribution basée sur Debian, l'installation s'effectue simplement avec **: apt-get install lynis**

```
root@debian:/home/hamza# apt-get install lynis
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  apt-listbugs debsecan debsums tripwire samhain fail2ban
The following NEW packages will be installed:
  lynis
0 upgraded, 1 newly installed, 0 to remove and 150 not upgraded.
Need to get 0 B/261 kB of archives.
After this operation, 1,626 kB of additional disk space will be used.
Selecting previously unselected package lynis.
(Reading database ... 146584 files and directories currently installed.)
Preparing to unpack .../archives/lynis_3.0.2-1_all.deb ...
Unpacking lynis (3.0.2-1) ...
Setting up lynis (3.0.2-1) ...
lynis.service is a disabled or a static unit not running, not starting it.
Processing triggers for gnome-menus (3.36.0-1) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for mailcap (3.69) ...
Processing triggers for desktop-file-utils (0.26-1) ...
root@debian:/home/hamza#
```

Automatisation des règles de durcissement : Lynis

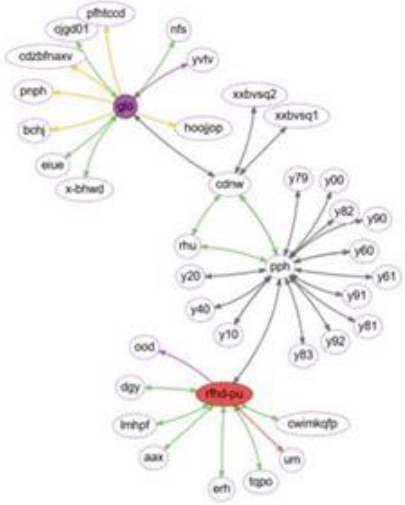
- Nous pouvons ensuite voir les options de lancement juste avec lynis ou lynis -h

```
root@debian:/home/hamza# /usr/sbin/lynis -h

[ Lynis 3.0.2 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2020, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------


  Usage: lynis command [options]


  Command:

    audit
        audit system                : Perform local security scan
        audit system remote <host>  : Remote security scan
        audit dockerfile <file>     : Analyze Dockerfile
```

PARTIE 1

Automatisation des règles de durcissement : PingCastle

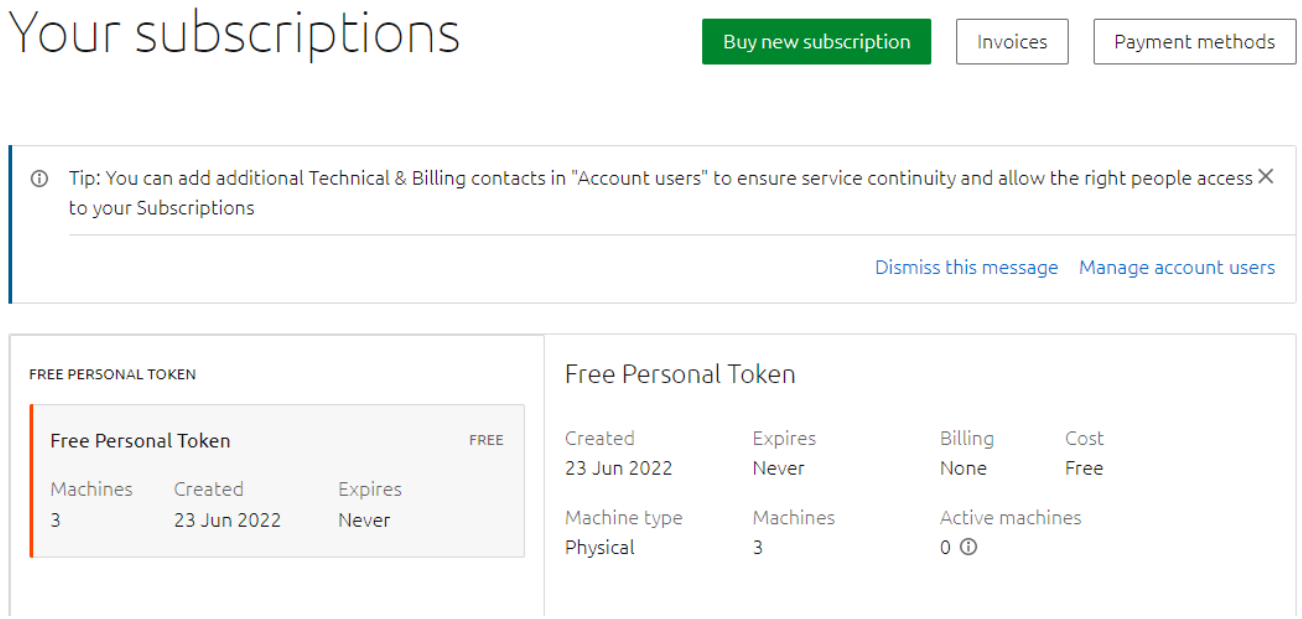
- **PingCastle** est un programme autonome (pas besoin de l'installer), qui scanne la configuration de votre AD et contrôle si toutes les règles préconisées par l'ANSSI sont appliquées. En cas de mauvais réglage, vous avez des points "malus" répartis en 4 catégories (Stale Object, Privileged Accounts, Trusts et Anomalies). Le nombre de points varie en fonction de la gravité. Cela peut aller de plusieurs dizaines de points pour les cas les plus critiques à 0 pour les règles d'information.



PARTIE 1

Automatisation des règles de durcissement : CIS-CAT

- Le **Center for Internet Security-Configuration Assessment Tool (CIS-CAT)** est un outil d'évaluation de la configuration qui compare la configuration des systèmes cibles aux paramètres de configuration sécurisés recommandés dans un contenu lisible par ordinateur. L'outil est conçu pour évaluer principalement par rapport aux recommandations de configuration de référence du CIS. L'outil fournit un rapport de conformité allant de 0 à 100 avec des étapes de correction pour les paramètres non conformes. Utilisez cet outil pour vous assurer que vos systèmes informatiques restent sécurisés et conformes.
- Ubuntu offre la possibilité d'utiliser une version CIS-CAT pro sur 3 machine en créant un compte sur https://ubuntu.com/advantage



PARTIE 1

Automatisation des règles de durcissement : CIS-CAT

- Nous pouvons attacher notre machine au compte ubuntu advantage avec : ua attach token (le token est à récupérer dans votre compte ubuntu advantage)

```
root@hnakabi-VirtualBox:/home/hnakabi# ua enable cis
One moment, checking your subscription first
CIS Audit is already enabled.
See: sudo ua status
root@hnakabi-VirtualBox:/home/hnakabi#
```

```
root@hnakabi-VirtualBox:/home/hnakabi# ua status
SERVICE       ENTITLED  STATUS    DESCRIPTION
cis           yes       enabled   Center for Internet Security Audit Tools
esm-infra     yes       enabled   UA Infra: Extended Security Maintenance (ESM)
fips          yes       disabled  NIST-certified core packages
fips-updates  yes       disabled  NIST-certified core packages with priority se
curity updates
livepatch     yes       enabled   Canonical Livepatch service

Enable services with: ua enable <service>

     Account: hamza.nakabi@gmail.com
Subscription: hamza.nakabi@gmail.com
root@hnakabi-VirtualBox:/home/hnakabi#
```

```
root@hnakabi-VirtualBox:/home/hnakabi# cis-audit -h
Profile '-h' is not valid!
Usage: /usr/sbin/cis-audit [ level1_workstation | level1_server | level2_workst
ation | level2_server ]
Note: default is level1_server
root@hnakabi-VirtualBox:/home/hnakabi#
```

PARTIE 1

PARTIE 2

Maitriser le durcissement du réseau

Dans ce module, vous allez :

- Identifier les composants basiques d’un réseau informatique
- Appliquer les configurations de sécurité sur les composants d’un réseau informatique

12 heures

CHAPITRE 1

Identifier les composants basiques d’un réseau informatique

Ce que vous allez apprendre dans ce chapitre :

- Connaître les composants indispensables d’un réseau informatique
- Maitriser les points à contrôler des composants d’un réseau informatique

5 heures

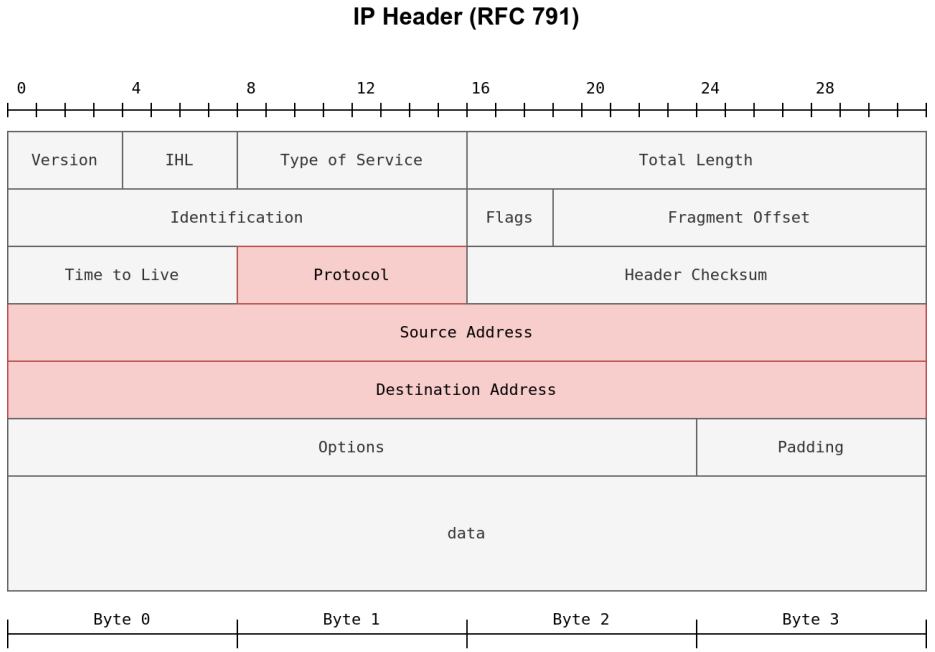
CHAPITRE 1

Identifier les composants basiques d’un réseau informatique

1. **Pare-feux (UTM inclus)**
2. VPN (OpenVPN, Wireguard et IPSEC)

Pare-feux (Firewalls) : principe de fonctionnement

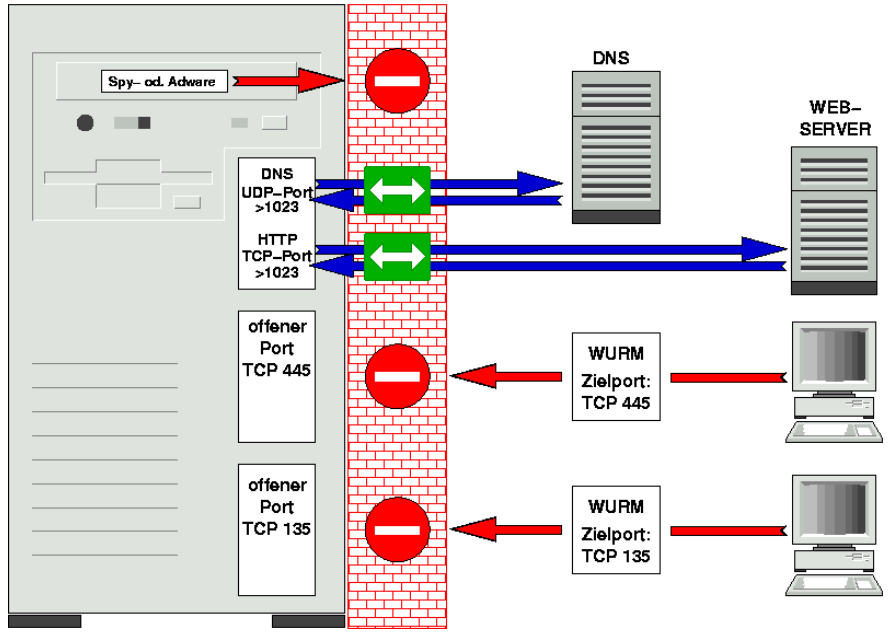
- Un pare-feu est un logiciel ou un matériel qui surveille le trafic réseau et le compare à un ensemble de règles avant de le transmettre ou de le bloquer. Une analogie simple est un garde à l'entrée d'un événement. Ce portier peut vérifier l'identité des individus par rapport à un ensemble de règles avant de les laisser entrer (ou sortir).
- Avant d'entrer dans plus en détails sur les pare-feu, il est utile de rappeler le contenu d'un paquet IP et d'un segment TCP. La figure suivante montre les champs que nous nous attendons à trouver dans une en-tête IP. Différents types de pare-feux sont capables d'inspecter divers champs de paquets; cependant, le pare-feu le plus basique devrait être capable d'inspecter au moins les champs suivants :
  - ✓ Protocole
  - ✓ Adresse source
  - ✓ Adresse de destination



PARTIE 2

Pare-feux (Firewalls) : principe de fonctionnement

- Selon le champ de protocole, les données du datagramme IP peuvent être l'une des nombreuses options. Trois protocoles courants sont :
  - ✓ TCP
  - ✓ UDP
  - ✓ ICMP
- Dans le cas de TCP ou UDP, le pare-feu doit au moins être en mesure de vérifier les en-têtes TCP et UDP pour :
  - ✓ Numéro de port source
  - ✓ Numéro de port de destination



Source: https://commons.wikimedia.org/wiki/File:Personal_firewall.png?uselang=fr

PARTIE 2

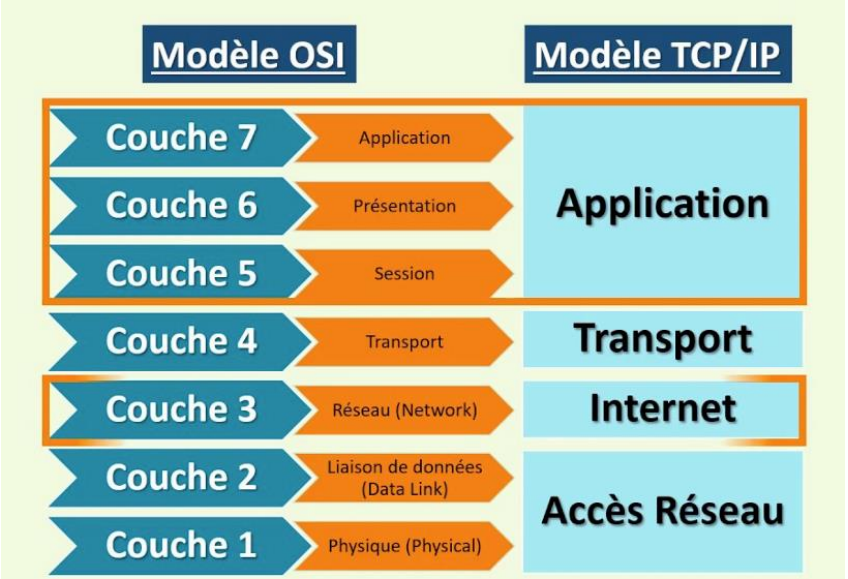
Pare-feux (Firewalls) : les types

- Il existe plusieurs types de pare-feux :
  - ✓ **Pare-feu matériel (pare-feu d'appliance) :** comme son nom l'indique, un pare-feu d'appliance est un élément matériel distinct par lequel le trafic réseau doit passer. Les exemples incluent Cisco ASA (appliance de sécurité adaptative), WatchGuard Firebox et l'appliance Netgate pfSense Plus.
  - ✓ **Pare-feu logiciel :** il s'agit d'un logiciel fourni avec le système d'exploitation, ou vous pouvez l'installer en tant que service supplémentaire. MS Windows dispose d'un pare-feu intégré, le pare-feu Windows Defender, qui fonctionne avec les autres services du système d'exploitation et les applications utilisateur. Un autre exemple est Linux iptables et firewalld.

Pare-feu matériel	Pare-feu logiciel
Protège l’ensemble du réseau	Protège un seul hôte
Équipement physique autonome	Doit être installé sur chaque hôte
Doit être surveillé	Auto surveillance système
Nécessite un expert pour l’installation et le management	Peut être installé par un non expert

Pare-feux (Firewalls) : les types

- Nous pouvons également classer les pare-feux en :
  - ✓ **Pare-feu personnel :** un pare-feu personnel est conçu pour protéger un seul système ou un petit réseau, par exemple, un petit nombre d'appareils et de systèmes sur un réseau domestique. Par exemple, de nombreux points d'accès sans fil conçus pour les maisons ont un pare-feu intégré. Un exemple est Bitdefender BOX. Un autre exemple est le pare-feu qui fait partie de nombreux points d'accès sans fil et routeurs domestiques de Linksys et Dlink.
  - ✓ **Pare-feu commercial :** un pare-feu commercial protège les réseaux moyens à grands. Par conséquent, vous vous attendez à une fiabilité et une puissance de traitement plus élevées, en plus de prendre en charge une bande passante réseau plus élevée. Très probablement, vous traversez un tel pare-feu lorsque vous accédez à Internet depuis votre université ou votre entreprise.
- Avant de classer les pare-feux en fonction de leurs capacités, il convient de rappeler que les pare-feux se concentrent sur les couches 3 et 4 et, dans une moindre mesure, sur la couche 2. Les pare-feux de nouvelle génération sont également conçus pour couvrir les couches 5, 6 et 7. Plus un pare-feu peut inspecter de couches, plus il devient sophistiqué et plus il a besoin de puissance de traitement.



PARTIE 2

Pare-feux (Firewalls) : les types

- En fonction des capacités du pare-feu, nous pouvons aussi classer les de pare-feux dans les types suivants :
  - ✓ **Pare-feu à filtrage de paquets :** le filtrage de paquets est le type de pare-feu le plus élémentaire. Ce type de pare-feu inspecte le protocole, les adresses IP source et destination, ainsi que les ports source et destination dans le cas des datagrammes TCP et UDP. Il s'agit d'un pare-feu d'inspection sans état.
  - ✓ **Passerelle au niveau du circuit :** en plus des fonctionnalités offertes par les pare-feux de filtrage de paquets, les passerelles au niveau du circuit peuvent fournir des fonctionnalités supplémentaires, telles que la vérification de la prise de contact TCP à trois par rapport aux règles du pare-feu.
  - ✓ **Pare-feu d'inspection avec état :** par rapport aux types précédents, ce type de pare-feu offre une couche de protection supplémentaire car il garde une trace des sessions TCP établies. Par conséquent, il peut détecter et bloquer tout paquet TCP en dehors d'une session TCP établie.
  - ✓ **Pare-feu proxy :** un pare-feu proxy est également appelé pare-feu d'application (AF) et pare-feu d'application Web (WAF). Il est conçu pour se faire passer pour le client d'origine et demande en son nom. Ce processus permet au pare-feu proxy d'inspecter le contenu de la charge utile du paquet au lieu de se limiter aux en-têtes de paquet. En règle générale, cela est utilisé pour les applications Web et ne fonctionne pas pour tous les protocoles.
  - ✓ **Pare-feu de nouvelle génération (NGFW) :** NGFW offre la protection de pare-feu la plus élevée. Il peut pratiquement surveiller toutes les couches du réseau, de la couche OSI 2 à la couche OSI 7. Il dispose d'une reconnaissance et d'un contrôle des applications. Les exemples incluent la série Juniper SRX et Cisco Firepower.
  - ✓ **Cloud Firewall ou Firewall as a Service (FWaaS) :** FWaaS remplace un pare-feu matériel dans un environnement cloud. Ses fonctionnalités peuvent être comparables à NGFW, selon le fournisseur de services ; cependant, il bénéficie de l'évolutivité de l'architecture cloud. Un exemple est Cloudflare Magic Firewall, qui est un pare-feu au niveau du réseau. Un autre exemple est Juniper vSRX ; il a les mêmes fonctionnalités qu'un NGFW mais est déployé dans le cloud. Il convient également de mentionner AWS WAF pour la protection des applications Web et AWS Shield pour la protection DDoS.

Pare-feux (Firewalls) : nouvelle génération

- Les pare-feux traditionnels, tels que les pare-feux à filtrage de paquets, attendent d'un numéro de port qu'il dicte le protocole utilisé et identifie l'application. Par conséquent, si vous souhaitez bloquer une application, vous devez bloquer un port. Malheureusement, cela n'est plus valable car de nombreuses applications se camouflent en utilisant des ports affectés à d'autres applications. En d'autres termes, un numéro de port n'est plus suffisant ni fiable pour identifier l'application utilisée. Ajoutez à cela l'utilisation généralisée du cryptage, par exemple via SSL/TLS.

- Le pare-feu de nouvelle génération (NGFW) est conçu pour relever les nouveaux défis auxquels sont confrontées les entreprises modernes. Par exemple, certaines des fonctionnalités NGFW incluent :
    - Intégrez un pare-feu et un système de prévention des intrusions (IPS) en temps réel. Il peut arrêter toute menace détectée en temps réel.
    - Identifiez les utilisateurs et leur trafic. Il peut appliquer la politique de sécurité par utilisateur ou par groupe.
    - Identifiez les applications et les protocoles quel que soit le numéro de port utilisé.
    - Identifiez le contenu transmis. Il peut appliquer la politique de sécurité en cas de détection de contenu en infraction.
    - Capacité à déchiffrer le trafic SSL/TLS et SSH. Par exemple, il limite les techniques évasives construites autour du cryptage pour transférer des fichiers malveillants.
    - Un NGFW correctement configuré et déployé rend de nombreuses attaques inutiles.

Pare-feux (Firewalls) : NGFW et UTM

- Les pare-feux traditionnels, tels que les pare-feux à filtrage de paquets, attendent d'un numéro de port qu'il dicte le protocole utilisé et identifie l'application. Par conséquent, si vous souhaitez bloquer une application, vous devez bloquer un port. Malheureusement, cela n'est plus valable car de nombreuses applications se camouflent en utilisant des ports affectés à d'autres applications. En d'autres termes, un numéro de port n'est plus suffisant ni fiable pour identifier l'application utilisée. Ajoutez à cela l'utilisation généralisée du cryptage, par exemple via SSL/TLS.

- Le pare-feu de nouvelle génération (NGFW) et le pare-feu de management unifié des menaces (UTM) sont tous deux conçus pour consolider plusieurs fonctions de sécurité en une seule solution.
- NGFW est conçu pour relever les nouveaux défis auxquels sont confrontées les entreprises modernes. Par exemple, certaines des fonctionnalités NGFW incluent :
  - ✓ Intégrez un pare-feu et un système de prévention des intrusions (IPS) en temps réel. Il peut arrêter toute menace détectée en temps réel.
  - ✓ Identifiez les utilisateurs et leur trafic. Il peut appliquer la politique de sécurité par utilisateur ou par groupe.
  - ✓ Identifiez les applications et les protocoles quel que soit le numéro de port utilisé.
  - ✓ Identifiez le contenu transmis. Il peut appliquer la politique de sécurité en cas de détection de contenu en infraction.
  - ✓ Capacité à déchiffrer le trafic SSL/TLS et SSH. Par exemple, il limite les techniques évasives construites autour du cryptage pour transférer des fichiers malveillants.
  - ✓ Un NGFW correctement configuré et déployé rend de nombreuses attaques inutiles.

Pare-feux (Firewalls) : NGFW et UTM

- UTM est conçu pour une gestion unifiée des menaces et améliorer l'efficience et l'efficacité des équipes de sécurité en réduisant le nombre de solutions de sécurité autonomes qu'elles doivent déployer, configurer, surveiller et entretenir. Par exemple, certaines des fonctionnalités UTM incluent :
  - ✓ **Consolidation de la sécurité :** les solutions de gestion unifiée des menaces intègrent plusieurs fonctions de sécurité dans une seule solution. Cela permet aux équipes de sécurité de détecter plus rapidement les menaces potentielles sur la base de données plus riches et plus contextuelles et prend en charge une réponse rapide dans l'ensemble de l'environnement de l'entreprise.
  - ✓ **Complexité réduite :** avec l'UTM, une organisation passe de plusieurs produits de sécurité autonomes à une solution unique. Cet outil unique est plus facile à configurer, à mettre à jour et à gérer qu'un éventail de solutions indépendantes.
  - ✓ **Économies de coûts :** les solutions UTM remplacent plusieurs produits de sécurité. Cette consolidation permet à une organisation de profiter d'importantes économies de coûts.
  - ✓ **Flexibilité de la sécurité :** la gestion unifiée des menaces est conçue pour adapter et intégrer de nouvelles fonctions de sécurité dès qu'elles sont disponibles. Cela offre un niveau de flexibilité plus élevé qu'une approche qui nécessite le déploiement d'un nouvel appareil pour prendre en charge de nouvelles fonctions.
  - ✓ **Gestion centralisée :** UTM centralise la surveillance et la gestion dans une console unique. En éliminant le changement de contexte entre les tableaux de bord, cela améliore l'efficience et l'efficacité du personnel de sécurité.
  - ✓ **Conformité simplifiée :** les solutions UTM avec des politiques de sécurité basées sur l'identité simplifient le processus de mise en œuvre des contrôles d'accès basés sur le moindre privilège. Cela facilite le respect des exigences de contrôle d'accès des réglementations telles que PCI DSS, HIPAA et GDPR.

CHAPITRE 1

Identifier les composants basiques d’un réseau informatique

1. Pare feux (UTM inclus)
2. **VPN (OpenVPN, Wireguard et IPSEC)**

VPN : principe de fonctionnement

- Un réseau privé virtuel (VPN) est une technologie qui permet aux appareils situés sur des réseaux distincts de communiquer en toute sécurité en créant un chemin dédié entre eux sur Internet (appelé tunnel). Les appareils connectés dans ce tunnel forment leur propre réseau privé.
- Par exemple, seuls les appareils d'un même réseau (par exemple, au sein d'une entreprise) peuvent communiquer directement.
- Couvrons quelques-uns des autres avantages offerts par un VPN dans le tableau ci-dessous :

L'avantage	La description
Permet aux réseaux de différents emplacements géographiques d'être connectés.	Par exemple, une entreprise avec plusieurs bureaux trouvera les VPN avantageux, car cela signifie que des ressources telles que les serveurs/l'infrastructure sont accessibles depuis un autre bureau.
La confidentialité	La technologie VPN utilise le chiffrement pour protéger les données. Cela signifie qu'elles ne peuvent être comprises qu'entre les appareils à partir desquels elles ont été envoyées et auxquelles elles sont destinées, ce qui signifie que les données ne sont pas vulnérables au reniflage. Ce cryptage est utile dans les endroits avec WiFi public, où aucun chiffrement n'est fourni par le réseau.
L'anonymat.	Le niveau d'anonymat fourni par un VPN dépend uniquement de la manière dont les autres appareils du réseau respectent la confidentialité. Par exemple, un VPN qui enregistre toutes vos données/historiques revient essentiellement à ne pas utiliser de VPN à cet égard.

VPN : les technologies

- La technologie VPN s'est améliorée au fil des années. Explorons quelques technologies VPN existantes ci-dessous :

La technologie	La description
PPP	Cette technologie est utilisée par PPTP (expliqué ci-dessous) pour permettre l'authentification et assurer le chiffrement des données. Les VPN fonctionnent en utilisant une clé privée et un certificat public (similaire à SSH). Une clé privée et un certificat doivent correspondre pour que vous puissiez vous connecter.
PPTP	Le protocole PPTP (Point-to-Point Tunneling Protocol) est la technologie qui permet aux données de PPP de voyager et de quitter un réseau. PPTP est très facile à configurer et est pris en charge par la plupart des appareils. Il est cependant faiblement chiffré par rapport aux alternatives.
IPSEC	La sécurité du protocole Internet (IPsec) chiffre les données à l'aide de la structure IP (Internet Protocol) existante. IPSec est difficile à mettre en place par rapport aux alternatives ; cependant, en cas de succès, il bénéficie d’un chiffrement fort et est également pris en charge sur de nombreux appareils.

VPN : les solutions

- **OpenVPN** est un logiciel libre permettant de créer un réseau privé virtuel VPN. Il peut être utilisé pour simplement accéder à un serveur VPN existant ou pour mettre en place un serveur et y accéder. Que ce soit en configuration client ou serveur, il est possible de tout configurer en CLI ou par interface graphique.
- Principe de fonctionnement : pour accepter une connexion, OpenVPN passe par 5 étapes :
    1. Le serveur doit recevoir la clé partagée.
    2. Il envoie son certificat électronique, qui est vérifié par le client.
    3. Le client envoie son compte/mot de passe ou son certificat.
    4. Le serveur vérifie le compte/mot de passe auprès du serveur Radius, ou il vérifie le certificat de manière autonome.
    5. Si la connexion est établie, une adresse IP est fournie au client et elle est routée par le tunnel.

VPN : les solutions

- **Openvpn** peut être installé facilement sur les distributions basées dur Debian : apt-get install openvpn

```
root@debian:/home/hamza# apt-get install openvpn
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  easy-rsa libccid libpkcs11-helper1 opensc opensc-pkcs11 pcscd
Suggested packages:
  pcmciautils resolvconf openvpn-systemd-resolved
The following NEW packages will be installed:
  easy-rsa libccid libpkcs11-helper1 opensc opensc-pkcs11 openvpn pcscd
0 upgraded, 7 newly installed, 0 to remove and 150 not upgraded.
Need to get 2,374 kB of archives.
After this operation, 7,227 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://deb.debian.org/debian bullseye/main amd64 libccid amd64 1.4.34-1 [337 kB]
Get:2 http://deb.debian.org/debian bullseye/main amd64 pcscd amd64 1.9.1-1 [98.1 kB]
Get:3 http://deb.debian.org/debian bullseye/main amd64 easy-rsa all 3.0.8-1 [45.2 kB]
Get:4 http://deb.debian.org/debian bullseye/main amd64 libpkcs11-helper1 amd64 1.27-1
[47.5 kB]
```

VPN : les solutions

- Nous pouvons ensuite nous connecter à n'importe quel serveur Openvpn en utilisant son fichier de configuration .ovpn :

```
root@debian:/home/hamza# /usr/sbin/openvpn /home/hamza/Downloads/hamza.ovpn
2022-09-10 13:45:55 WARNING: Compression for receiving enabled. Compression has been u
sed in the past to break encryption. Sent packets are not compressed unless "allow-com
pression yes" is also set.
2022-09-10 13:45:55 --cipher is not set. Previous OpenVPN version defaulted to BF-CBC
as fallback when cipher negotiation failed in this case. If you need this fallback ple
ase add '--data-ciphers-fallback BF-CBC' to your configuration and/or add BF-CBC to --
data-ciphers.
2022-09-10 13:45:55 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPO
LL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
2022-09-10 13:45:55 library versions: OpenSSL 1.1.1n  15 Mar 2022, LZO 2.10
2022-09-10 13:45:55 WARNING: Your certificate is not yet valid!
2022-09-10 13:45:55 Outgoing Control Channel Authentication: Using 512 bit message has
h 'SHA512' for HMAC authentication
2022-09-10 13:45:55 Incoming Control Channel Authentication: Using 512 bit message has
h 'SHA512' for HMAC authentication
2022-09-10 13:45:55 TCP/UDP: Preserving recently used remote address: [AF_INET]18.202.
129.195:1194
2022-09-10 13:45:55 Socket Buffers: R=[212992->212992] S=[212992->212992]
2022-09-10 13:45:55 UDP link local: (not bound)
2022-09-10 13:45:55 UDP link remote: [AF_INET]18.202.129.195:1194
2022-09-10 13:45:55 TLS: Initial packet from [AF_INET]18.202.129.195:1194, sid=d943e87
```

VPN : les solutions

- **WireGuard** est un protocole VPN de nouvelle génération sous licence GPLv2 (ou MIT, BSD, Apache 2.0 ou GPL suivant le contexte) créé par Jason A. Donenfeld. WireGuard est intégré à partir de la version 5.6 du noyau Linux. Toutes distributions ayant une version égale ou supérieur sont donc compatibles pour l'utilisation de WireGuard.
- WireGuard fonctionne uniquement avec le protocole UDP (ce qui est recommandé pour un VPN afin d'éviter les problèmes que provoque l'encapsulation TCP dans du TCP). Aucun port standard n'a été affecté à WireGuard par l'IANA, mais les documentations utilisent généralement le port 51820.
- Le nouveau concept central autour du protocole WireGuard est celui du routage cryptographique :
  - ✓ Le routage cryptographique associe des adresses IP ou des sous-réseaux à des clefs publiques.
  - ✓ Les clefs cryptographiques fonctionnent à peu près comme celles que l'on retrouve avec le protocole SSH : une paire de clef, l'une dite privé et l'autre publique, sont utilisées afin d'utiliser des mécanismes de chiffrement asymétrique.

CHAPITRE 2

Appliquer les configurations de sécurité sur les composants d'un réseau informatique

Ce que vous allez apprendre dans ce chapitre :

- Les contrôles et les vérifications des protocoles réseau
- Les règles de durcissement basiques des protocoles réseau
- Le durcissement d'un firewall

12 heures

CHAPITRE 2

Appliquer les configurations de sécurité sur les composants d'un réseau informatique

1. **Durcissement des protocoles réseaux (NBT-NS, LLMNR, WPAD, TLS)**
2. Durcissement d'un Firewall

NBT-NS / LLMNR : vulnérabilité

- Link-Local Multicast Name Resolution (LLMNR) et Netbios Name Service (NBT-NS) sont deux composants présents en environnement Microsoft. LLMNR a été introduit dans Windows Vista et est le successeur de NBT-NS. Ces composants permettent d'aider à identifier des hôtes sur le même sous-réseau lorsque les services DNS centraux échouent. Ainsi, si une machine tente de résoudre un hôte particulier, mais que la résolution DNS échoue, la machine tentera alors de demander à toutes les autres machines du réseau local la bonne adresse via NBT-NS ou LLMNR :
  - ✓ NBT-NS est basée sur l'identification par le nom NetBIOS – Utilise le port TCP 137
  - ✓ LLMNR est basé sur le format DNS (Domain Name System) – Utilise le port UDP 5355

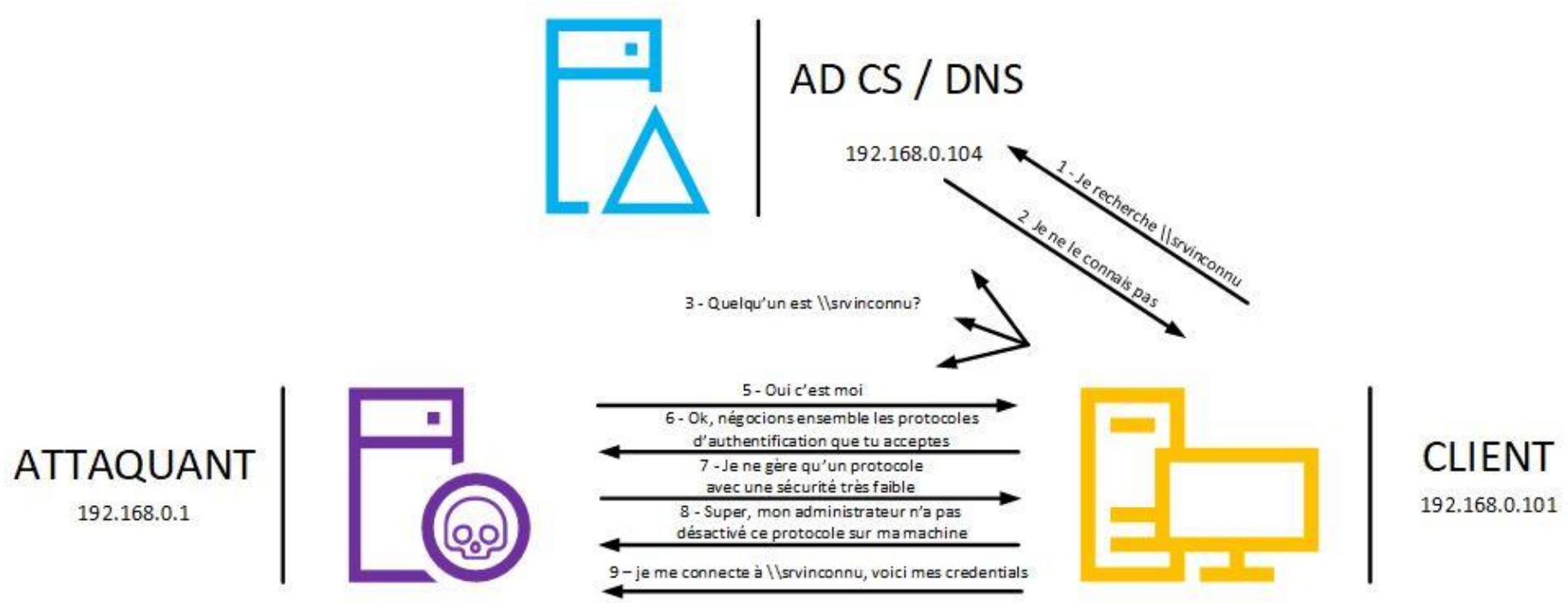
- Alors que LLMNR ou NBT-NS sont obsolètes, ils sont très utilisés dans Windows. Ces protocoles semblent inoffensifs, Ils ne sont là que pour faciliter la vie les utilisateurs et leur permettre d'accéder aux ressources sans configuration complexe.

- Malheureusement, cela ouvre une vulnérabilité majeure que des attaquants peuvent utiliser pour obtenir des informations d'identification complètes d'utilisateurs.

- Un attaquant pourrait librement écouter sur un réseau les diffusions LLMNR (UDP / 5355) ou NBT-NS (UDP / 137) et y répondre, en prétendant que l'attaquant connaît l'emplacement de l'hôte demandé (Poisoning). Cette réponse contiendrait l'adresse IP d'un serveur malveillant qui disposerait d'une fonction de collecte de valeur d'identification (comme les hashs NTLMv1/v2 par exemple).

NBT-NS / LLMNR : attaque

- L'attaque consiste pour l'attaquant à écouter sur le réseau les diffusions LLMNR ou NBT-NS, et répondre quand un client essaye de se connecter à un serveur qui n'est pas connu du DNS. Cela signifie pour le client qu'il faut qu'il essaye de se connecter à un serveur inexistant ou pour lequel il se trompe d'orthographe. Par exemple \\SVR01 au lieu de \\SRV01 ou dans notre cas \\SRVINCONNU :



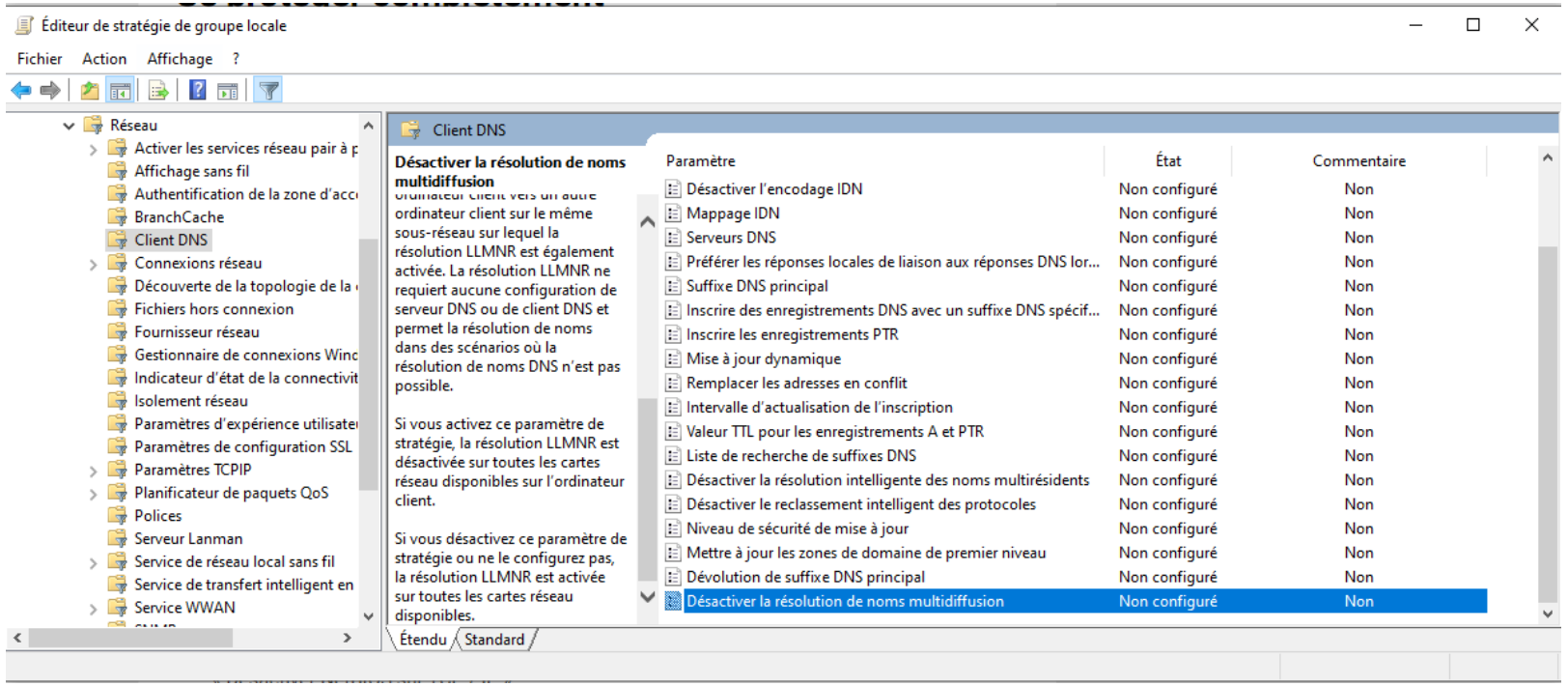
Source: http://remivernier.com/wp-content/uploads/2018/08/protocoles-nbt-ns-llmnr-et-exploitation-des-failles-sch1.jpg

PARTIE 2

NBT-NS / LLMNR : durcissement

- La meilleure défense contre l'empoisonnement LLMNR est de désactiver LLMNR et NBT-NS :

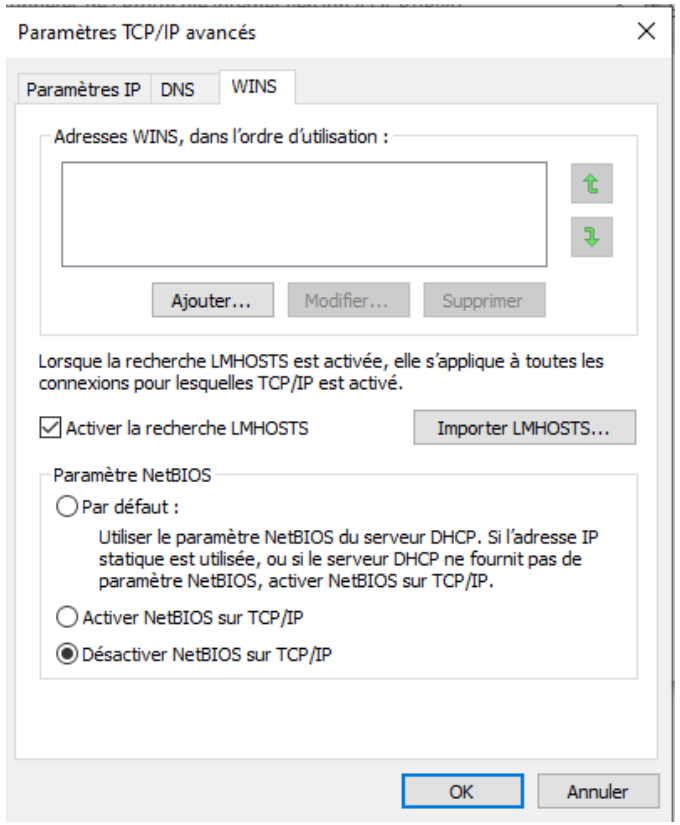
✓ Pour désactiver LLMNR, sélectionnez "Désactiver la résolution de noms multicat" sous Stratégie de l'ordinateur local > Configuration ordinateur > Modèles d'administration > Réseau > Client DNS > Désactiver la résolution du nom de multidiffusion



PARTIE 2

NBT-NS / LLMNR : durcissement

- ✓ Pour désactiver NBT-NS, accédez à Connexions réseau > Propriétés de l'adaptateur réseau > Propriétés TCP/IPv4 > onglet Avancé > onglet WINS et sélectionnez « Désactiver NetBIOS sur TCP/IP ».



PARTIE 2

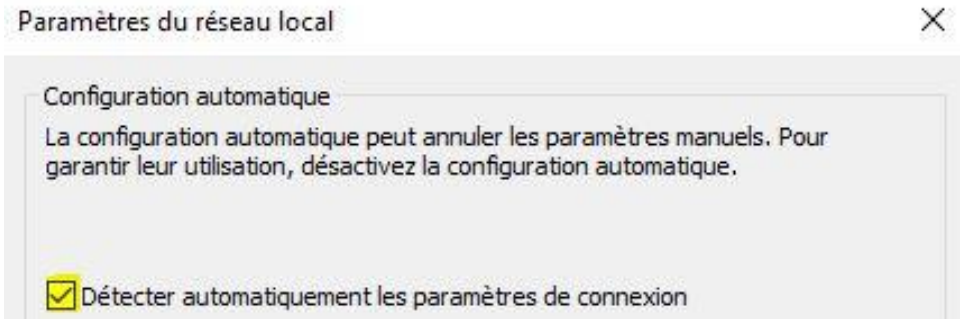
NBT-NS / LLMNR : durcissement

- Si une entreprise doit utiliser ou ne peut pas désactiver LLMNR / NBT-NS, la meilleure ligne de conduite est de :

  - Exiger la mise en place du NAC (Network Access Control).
  - Exiger des mots de passe utilisateur forts (par exemple > 14 caractères de long et limitez l'utilisation des mots courants). Plus le mot de passe est complexe et long, plus il est difficile pour un attaquant de déchiffrer le hash.

WRAD : vulnérabilité

- Le protocole WPAD (Web Proxy Auto-Discovery Protocol) est une méthode utilisée par les navigateurs pour localiser l'URL d'un fichier de configuration. Une fois la détection et le téléchargement du fichier de configuration terminés, il peut être exécuté pour déterminer le proxy pour une URL spécifiée. Encore une fois ce mécanisme est implémenté pour faciliter la configuration des navigateurs web et c'est cette simplification qui va se retourner contre ce protocole.
- Par défaut les navigateur web activent cette recherche WPAD.



Source : http://remivernier.com/wp-content/uploads/2018/08/protocoles-nbt-ns-llmnr-et-exploitation-des-failles-img6.jpg

- Le principe est simple, si le navigateur est configuré pour détecter automatiquement la configuration du proxy, il essayera de télécharger le fichier : wpad.<domaine_local>/wpad.dat ou le fichier proxy.pac. Sur un réseau d'entreprise, une entrée DNS (Type A) «wpad» doit donc être créée. Comme pour un partage SMB, si cette requête DNS échoue, le client utilise les protocoles maintenant bien connus LLMNR ou NBT-NS pour résoudre «wpad».

WRAD : durcissement

- La première option pour se défendre contre des attaques WRAD est de désactiver LLMNR et NBT-NS comme expliqué dans les slides précédentes.
- La deuxième option est tout simplement de décocher la case « Détecter automatiquement les paramètres de connexion ». Pourtant, plusieurs services et sous composants Windows n'utilisent pas les paramètres proxy WinINET définis dans IE et prennent aussi en charge la découverte automatique d'une configuration de proxy via son implémentation du protocole WPAD. Les services sont les suivants :
  - ✓ WinHttp-Autoproxy-Service
  - ✓ MSDW
  - ✓ Microsoft WNS
  - ✓ MpCommunication
  - ✓ NCSI
  - ✓ Windows-Update-Agent
  - ✓ Microsoft CryptoAPI
- Cependant, il n'est pas recommandé de désactiver ces services. La méthode universelle mais néanmoins radicale est de créer une entrée wpad dans host local (C:\Windows\System32\drivers\etc\hosts) du client pointant sur la boucle locale 127.0.0.1.

TLS : fonctionnement

- TLS (Transport Layer Security) est un protocole cryptographique utilisé pour sécuriser les communications réseau.

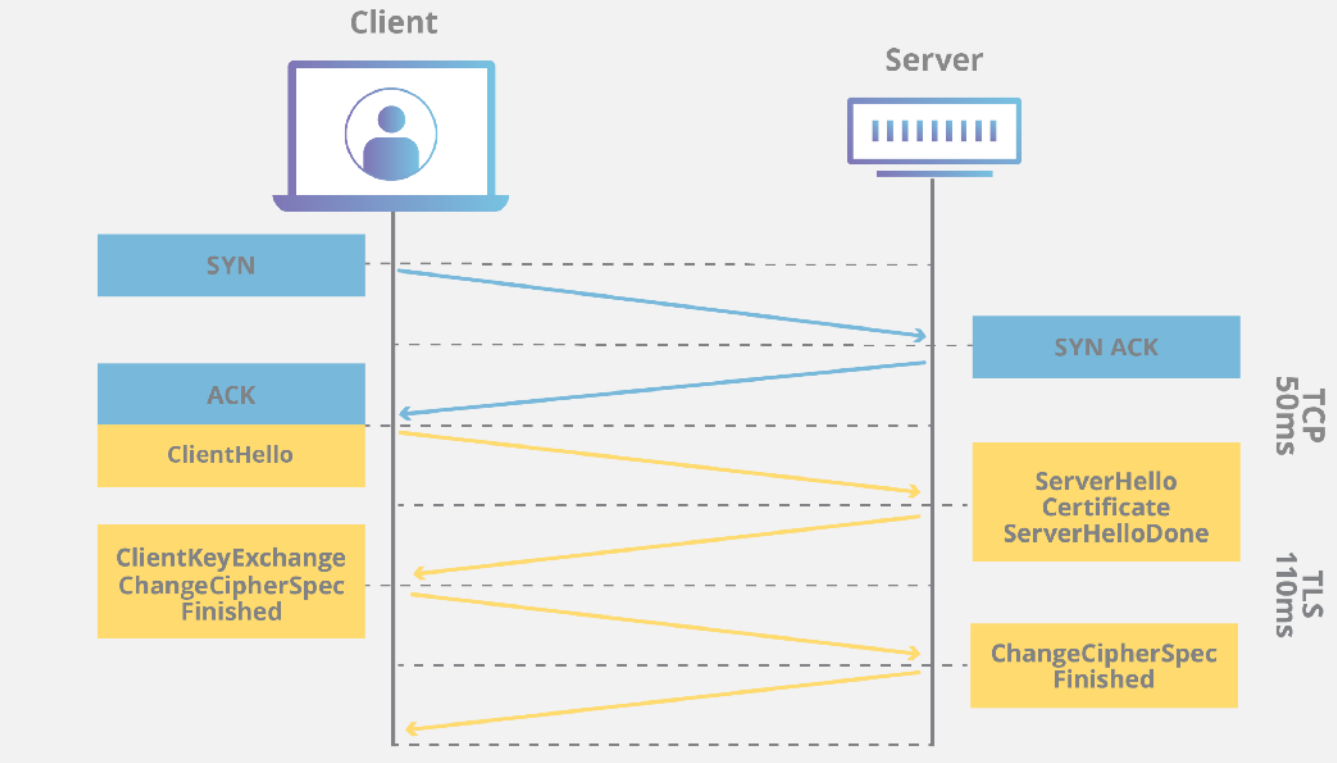
- TLS permet de chiffrer tout le trafic qui est envoyé sur TCP en utilisant une méthode de chiffrement symétrique. Le problème de base est que le serveur doit indiquer la clé au client et cela avant que la communication avec le TLS soit sécurisée. Toute personne qui envoie des pièces jointes chiffrées connaît bien ce problème : vous chiffrez un fichier et devez alors communiquer au destinataire le mot de passe secret, par exemple par téléphone.

- Le protocole TLS utilise la procédure suivante pour résoudre ce problème :

1. Lorsque le client, par exemple un navigateur Internet, contacte le serveur Web, celui-ci envoie d'abord son certificat au client. Ce certificat SSL prouve que le serveur est authentique et qu'il ne dissimule pas une fausse identité.
2. Le client vérifie la validité du certificat et envoie un numéro aléatoire au serveur, chiffré avec la clé publique (Public Key) du serveur.
3. Le serveur utilise ce numéro aléatoire pour générer la clé de session (Session Key), qui est utilisée pour chiffrer la communication. Comme le numéro aléatoire provient du client, celui-ci peut être sûr que la clé de session émane effectivement du serveur adressé.
4. Le serveur envoie la clé de session au client sous forme chiffrée. Ce chiffrement est effectué au moyen de l'échange de clés Diffie-Hellmann.
5. Les deux parties peuvent maintenant envoyer leurs données de manière sécurisée avec la clé de session.

TLS : fonctionnement

- Les étapes de négociation entre le client et le serveur peuvent être illustrées avec le schéma suivant :



TLS : vulnérabilités

- TLS n'est pas à l'abri des attaques et n'est pas exempt de certaines vulnérabilités. Les points les plus connus sont les suivants :

  - ✓ **Erreurs de programmation :** le « Heartbleed Bug », un bug important dans les versions précédentes d'OpenSSL, est devenu célèbre. Il a été réparé en 2014.
  - ✓ **Faiblesse du chiffrement** : en raison des restrictions à l'exportation de la cryptographie américaine, des versions « exportables » plus faciles à pirater que les versions originales ont été développées.
  - ✓ **Attaque via la compression** : si la compression HTTP est utilisée au lieu de la compression TLS, il est possible pour les pirates de découvrir le contenu chiffré TLS par certaines méthodes.
  - ✓ L'**attaque BEAST** a affecté la version TLS 1.0 et a été décrite dès 2014. Les versions actuelles de TLS sont à l'abri de ce danger.
  - ✓ **L'attaque Padding-Oracle** a été découverte en 2002 et était en fait possible jusqu'à la version SSL 3.0. La version 1.3 actuelle de TLS n'est pas concernée.

- Des efforts ont également été déployés pour empêcher un chiffrement TLS entièrement sécurisé afin que les autorités puissent avoir un aperçu des communications chiffrées, par exemple en relation avec des transactions financières et des activités criminelles. L'ETSI (Institut européen des normes de télécommunications) est l'une des organisations qui a cherché à atteindre un tel « point de rupture » du TLS.

TLS : durcissement

- Lors du durcissement des paramètres de sécurité du système en configurant les protocoles d'échange de clés, les méthodes d'authentification et les algorithmes de chiffrement, il est nécessaire de garder à l'esprit que plus la gamme de clients pris en charge est large, plus la sécurité résultante est faible. À l'inverse, des paramètres de sécurité stricts entraînent une compatibilité limitée avec les clients, ce qui peut entraîner le verrouillage de certains utilisateurs du système.

- Parmi les points importants à configurer pour avoir une implémentation sécurisée de TLS :

  ✓ **Choix des algorithmes à activer :**

  - **Versions de protocole :** la dernière version de TLS fournit le meilleur mécanisme de sécurité. À moins que vous n'ayez une raison impérieuse d'inclure la prise en charge des anciennes versions de TLS (ou même de SSL), autorisez vos systèmes à négocier des connexions en utilisant uniquement la dernière version de TLS. N'autorisez pas la négociation à l'aide de SSL version 2 ou 3. Ces deux versions présentent de graves failles de sécurité. Autoriser uniquement la négociation à l'aide de TLS version 1.0 ou supérieure. La version actuelle de TLS, 1.3, doit toujours être préférée.

  - **Suites de chiffrement :** les suites de chiffrement modernes et plus sécurisées doivent être préférées aux anciennes et non sécurisées. Désactivez toujours l'utilisation des suites de chiffrement eNULL et aNULL, qui n'offrent aucun cryptage ni aucune authentification. Dans la mesure du possible, les suites de chiffrement basées sur RC4 ou HMAC-MD5, qui présentent de graves lacunes, doivent également être désactivées. Il en va de même pour les soi-disant suites de chiffrement d'exportation, qui ont été intentionnellement affaiblies et sont donc faciles à casser.
  - **Longueur de la clé publique :** lorsque vous utilisez des clés RSA, préférez toujours des longueurs de clé d'au moins 3072 bits signées par au moins SHA-256, ce qui est suffisamment grand pour une véritable sécurité de 128 bits.

TLS : durcissement

✓ **Utilisation des implémentations recommandées de TLS**

- **Utilisation des suites de chiffrement dans OpenSSL :** OpenSSL est une boîte à outils Open Source robuste, de qualité commerciale et complète pour le protocole TLS (Transport Layer Security), anciennement connu sous le nom de protocole SSL (Secure Sockets Layer). L'implémentation du protocole est basée sur une bibliothèque cryptographique complète à usage général, qui peut également être utilisée de manière autonome.

- **Travailler avec les suites de chiffrement dans GnuTLS :** GnuTLS est une bibliothèque de communication sécurisée implémentant les protocoles et technologies SSL, TLS et DTLS qui les entourent. Il fournit une interface de programmation d'application (API) en langage C simple pour accéder aux protocoles de communication sécurisés ainsi que des API pour analyser et écrire X.509, PKCS #12 et d'autres structures requises.

CHAPITRE 2

Appliquer les configurations de sécurité sur les composants d'un réseau informatique

1. Durcissement des protocoles réseaux (NBT-NS, LLMNR, WPAD, TLS)
2. **Durcissement d'un Firewall**

Le durcissement d'un Firewall

- Le durcissement comme nous l'avons présenté, n'est pas une action ou tâche limitée dans le temps, mais un processus continu et un travail d'amélioration et d'adaptation aux différents changements et menaces qui évoluent, dans l'exemple d'un durcissement d'un firewall (logiciel ou appliance). Il est important qu'une configuration sécurisée du firewall soit réalisée, cependant elle n'est pas suffisante et unique dans tous les environnements et dans toutes les situations.
- Voici quelques étapes pour un durcissement et une sécurisation continue d'un firewall dans un environnement de production d'une entreprise :

  - ✓ Durcir et configurer correctement le pare-feu
  - ✓ Planifier le déploiement de votre pare-feu
  - ✓ Sécuriser le pare-feu
  - ✓ Comptes utilisateurs sécurisés
  - ✓ Verrouiller l'accès de la zone au trafic approuvé
  - ✓ S'assurer que la politique et l'utilisation du pare-feu soient conformes aux normes
  - ✓ Tester pour vérifier la politique et identifier les risques
  - ✓ Logiciel d'audit ou micrologiciel et journaux

Le durcissement d'un Firewall

Durcir et configurer correctement le pare-feu :

La plupart des systèmes d'exploitation de solutions de pare-feu tout-en-un sont renforcés par le fournisseur. Si vous déployez une solution de pare-feu logiciel, assurez-vous que le système d'exploitation est d'abord corrigé et renforcé.

En plus de commencer avec un système d'exploitation renforcé, les administrateurs de la sécurité voudront s'assurer que le pare-feu est configuré en toute sécurité. Des guides sont disponibles auprès de fournisseurs et de tiers comme le Center for Internet Security (CIS), qui publie les CIS Benchmarks Network Devices.

Planifier le déploiement de votre pare-feu :

Les pare-feux sont un outil essentiel pour appliquer les principes de sécurité Zero Trust. Ils surveillent et contrôlent l'accès entrant et sortant à travers les limites du réseau dans un réseau macro-segmenté. Cela s'applique à la fois aux déploiements de pare-feu routés de couche 3 (où le pare-feu agit comme une passerelle connectant plusieurs réseaux) et aux déploiements de pare-feu de pont de couche 2 (où le pare-feu connecte et isole les périphériques au sein d'un seul réseau).

Verrouiller l'accès de la zone au trafic approuvé :

La fonction principale d'un pare-feu est d'appliquer et de surveiller l'accès pour la segmentation du réseau. Les pare-feu peuvent inspecter et contrôler le trafic nord/sud à travers une limite de réseau. Dans ce cas d'utilisation de macro-segmentation, les zones sont de grands groupes comme le Wi-Fi externe, interne, DMZ et invité. Il peut également s'agir de groupes d'entreprises sur des réseaux internes distincts tels que le centre de données, les ressources humaines et la finance ou un étage de production dans une usine de fabrication qui utilise des systèmes de contrôle industriels (ICS).

Le durcissement d'un Firewall

Sécuriser le pare-feu :

Un pare-feu est un élément essentiel de l'infrastructure de sécurité d'une organisation et doit être protégé contre toute exploitation. Pour sécuriser votre pare-feu, procédez comme suit :

- ✓ Désactivez les protocoles non sécurisés comme telnet et SNMP ou utilisez une configuration SNMP sécurisée.
- ✓ Planifiez des sauvegardes périodiques de la configuration et de la base de données.
- ✓ Activez l'audit des modifications du système et envoyez les journaux via syslog sécurisé ou une autre méthode à un serveur SIEM externe, sécurisé et central ou à une solution de gestion de pare-feu pour l'investigation et la création de rapports.
- ✓ Ajoutez une règle furtive dans la stratégie de pare-feu pour masquer le pare-feu des analyses du réseau.
- ✓ Limitez l'accès de gestion à des hôtes spécifiques.
- ✓ Les pare-feux ne sont pas à l'abri des vulnérabilités. Vérifiez auprès du fournisseur pour voir s'il existe des vulnérabilités connues et des correctifs de sécurité qui corrigent la vulnérabilité.

Le durcissement d'un Firewall

Comptes utilisateurs sécurisés :

La prise de contrôle de compte est une technique courante utilisée par les cybercriminels. Pour sécuriser les comptes utilisateur sur votre pare-feu, procédez comme suit :

- Renommer ou modifier les comptes et mots de passe par défaut.
- Exiger MFA et/ou définir une politique de mot de passe fort (mots de passe complexes avec des lettres majuscules et minuscules, des caractères spéciaux et des chiffres, 12 caractères ou plus, empêcher la réutilisation du mot de passe).
- Utilisez le contrôle d'accès basé sur les rôles (RBAC) pour les administrateurs de pare-feu. Déléguer et limiter l'accès en fonction des besoins d'accès de l'utilisateur (c'est-à-dire autoriser uniquement l'accès en lecture seule pour les auditeurs et créer des rôles et des comptes d'accès dédiés pour les équipes DevSecOps).

Le durcissement d'un Firewall

S'assurer que la politique et l'utilisation du pare-feu sont conformes aux normes :

Les réglementations ont des exigences spécifiques pour les pare-feux. Toute bonne pratique de sécurité doit se conformer à ces exigences et peut nécessiter l'ajout de contrôles de sécurité supplémentaires à tout pare-feu déployé. Des exemples d'exigences incluent l'utilisation de réseaux privés virtuels (VPN) pour chiffrer les données en transit, un antivirus pour empêcher les logiciels malveillants connus et des systèmes de détection et de prévention des intrusions (IDS/IPS) pour détecter toute tentative d'intrusion sur le réseau.

Tester pour vérifier la politique et identifier les risques :

Avec une politique de sécurité plus importante, il peut être difficile de visualiser comment elle traiterait une nouvelle connexion. Des outils existent pour effectuer une analyse de chemin et peuvent exister dans le système de gestion de la sécurité pour rechercher et trouver des règles.

En outre, certains systèmes de gestion de la sécurité avertissent lorsqu'un objet en double est créé ou n'installent pas une stratégie dont une règle en cache une autre. Testez régulièrement votre stratégie pour vérifier qu'elle fonctionne comme prévu pour trouver les objets inutilisés et en double.

Les stratégies de pare-feu sont généralement appliquées dans l'ordre descendant et peuvent être optimisées en déplaçant les règles les plus touchées plus haut dans l'ordre d'inspection. Inspectez régulièrement la politique pour optimiser les performances de votre pare-feu.

Enfin, effectuez régulièrement des tests d'intrusion pour identifier les risques de mesures de sécurité supplémentaires qui peuvent être nécessaires en plus du pare-feu pour sécuriser votre organisation.

Le durcissement d'un Firewall

Audit logiciel ou/et firmware et journaux :

Des audits réguliers sont essentiels pour garantir que les logiciels et micrologiciels sont corrects et à jour et que les journaux sont correctement configurés et opérationnels. Voici quelques bonnes pratiques pour ces audits :

- ✓ Établissez un plan formel de contrôle des changements pour modifier la politique de sécurité afin de garantir que la sécurité n'est pas compromise.
- ✓ Les règles avec Tout défini dans la source, la destination ou le port peuvent être des trous dans la politique de sécurité. Lorsque cela est possible, modifiez-les pour ajouter la source, la destination ou le service spécifique qui est l'objet de la règle.
- ✓ Créez des sections ou des couches pour ajouter une hiérarchie à la politique de sécurité, ce qui en facilite la révision.
- ✓ Ajoutez des règles de nettoyage à la fin de la section ou du calque qui correspondent à l'intention du calque (c'est-à-dire tout autoriser ou tout refuser).
- ✓ Ajoutez des commentaires et des noms aux règles pour aider à identifier l'objectif initial de chaque règle.
- ✓ Activez la journalisation pour mieux suivre les flux réseau et ajouter de la visibilité pour les enquêtes et les rapports d'investigation.
- ✓ Consultez régulièrement les journaux d'audit et les rapports pour savoir qui a modifié la stratégie de pare-feu.

PARTIE 3

Maitriser le durcissement du système

Dans ce module, vous allez :

- Identifier les différents OS du marché
- Connaître la différence entre les OS
- Appliquer les règles de durcissement du système

15 heures

CHAPITRE 1

Identifier les systèmes d'exploitation

Ce que vous allez apprendre dans ce chapitre :

- Les différents OS présents sur le marché
- Les faiblesses et les avantages de chaque OS

8 heures

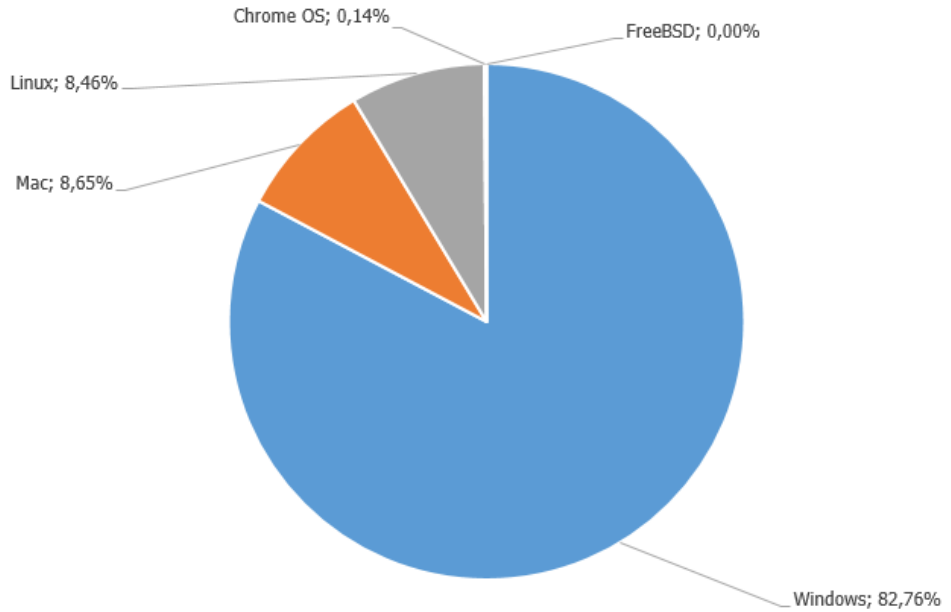
CHAPITRE 1

Identifier les systèmes d’exploitation

1. **Système Windows (serveurs et poste de travail)**
2. Systèmes Linux

Windows

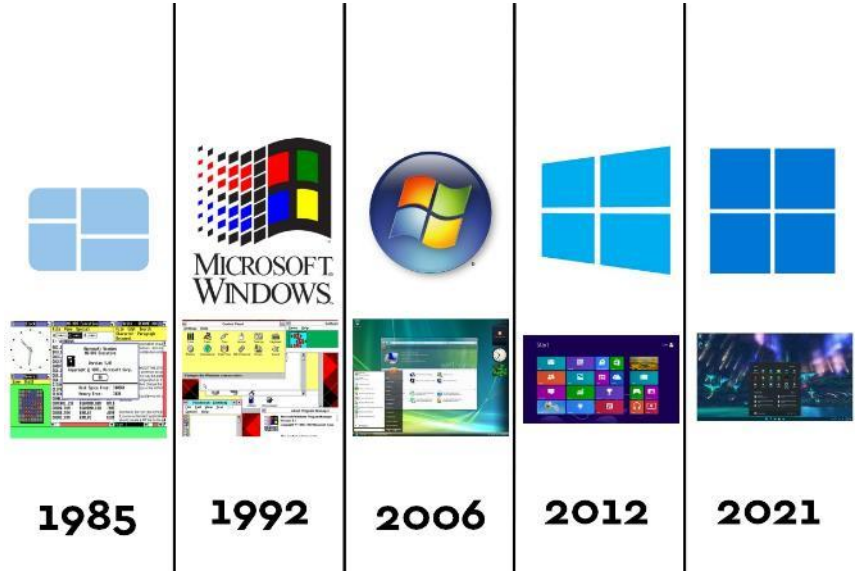
- Le système d'exploitation Windows a une longue histoire remontant à 1985, et actuellement, c'est le système d'exploitation dominant à la fois pour l'utilisation domestique et les réseaux d'entreprise. Pour cette raison, Windows a toujours été ciblé par les pirates et les auteurs de logiciels malveillants.



PARTIE 3

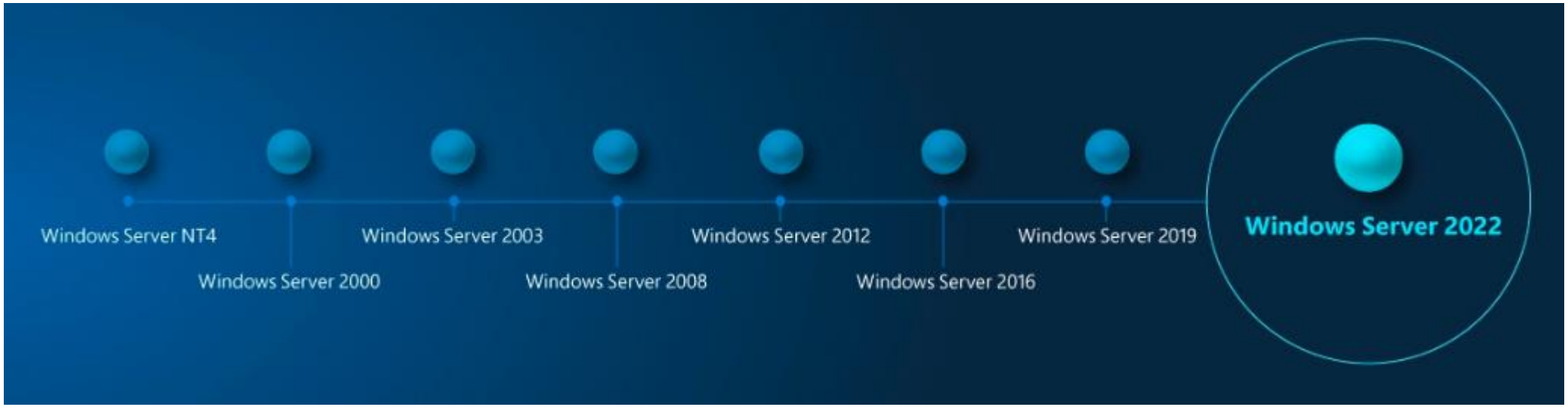
Les versions de Windows poste de travail

- Windows XP était une version populaire de Windows et avait une longue durée de vie. Microsoft a annoncé ensuite Windows Vista, qui était une refonte complète du système d'exploitation Windows. Il y avait de nombreux problèmes avec Windows Vista. Il n'a pas été bien accueilli par les utilisateurs de Windows et a été rapidement supprimé.
- Windows 7 a été publié peu de temps après et a été marqué par une date de fin de support. Windows 8.x est venu et a été de courte durée, comme Vista.
- Puis est arrivé Windows 10, qui est la version actuelle du système d'exploitation Windows la plus utilisée pour les ordinateurs de bureau. Windows 10 est disponible en 2 versions, Home et Pro.
- Depuis le 5 octobre 2021 - Windows 11 est désormais le système d'exploitation Windows actuel pour les utilisateurs finaux.



Les versions de Windows serveur

- Durant les années 90, la nécessité de concurrencer les systèmes serveur de l'époque pousse Microsoft à concevoir un système orienté services et non pas bureautique. Cela a donné naissance au **Windows Server** avec les versions NT.
- La popularité de cette nouvelle version de Windows (Windows NT) dans le domaine de l'entreprise pousse Microsoft à continuer d'investir dans ce domaine. En 2003 arrive enfin la première version de Windows Server (Windows Server 2003). Cette version marque un tournant dans la conquête de l'entreprise par Microsoft. Ce sera une version **massivement** adoptée en entreprise. Se suivent alors, régulièrement, de nouvelles versions de ce système : 2008, 2012, 2016, 2019 et actuellement 2022.



CHAPITRE 1

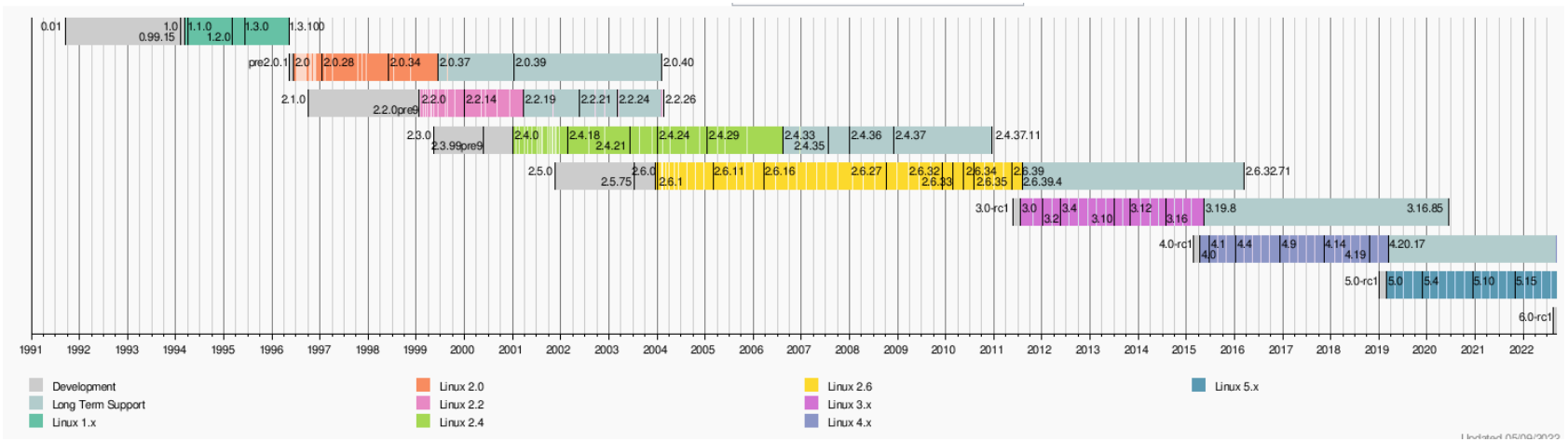
Identifier les systèmes d’exploitation

1. Système Windows (serveurs et poste de travail)
2. **Systèmes Linux**

PARTIE 3

Linux

- Linux est un système d'exploitation ou un noyau distribué sous une licence open-source. Sa liste de fonctionnalités ressemble beaucoup à UNIX. Le noyau est un programme au cœur du système d'exploitation Linux qui s'occupe de choses fondamentales, comme faire communiquer le matériel avec le logiciel.
- Alors Linus (Linus Torvalds le créateur de Linux) a conçu un noyau nommé Linux en 1991. Bien qu'il ait besoin de programmes comme le gestionnaire de fichiers, les éditeurs de documents, les programmes audio-vidéo pour s'exécuter dessus.
- Au fil du temps, il a collaboré avec d'autres programmeurs dans des endroits comme le MIT et des applications pour Linux ont commencé à apparaître. Ainsi, vers 1991, un système d'exploitation Linux fonctionnel avec certaines applications a été officiellement lancé, et ce fut le début de l'une des options de système d'exploitation open source les plus appréciées disponibles aujourd'hui.
- Les versions antérieures du système d'exploitation Linux n'étaient pas aussi conviviales et elles étaient utilisées par les programmeurs informatiques et Linus Torvalds n'a jamais eu l'idée de commercialiser son produit. Cela a définitivement freiné la popularité de Linux alors que d'autres systèmes d'exploitation Windows à vocation commerciale sont devenus célèbres. Néanmoins, l'aspect open source du système d'exploitation Linux l'a rendu plus robuste.



Les avantages de Linux

- Le système d'exploitation Linux jouit désormais d'une popularité à son apogée, et il est célèbre parmi les programmeurs ainsi que les utilisateurs réguliers d'ordinateurs du monde entier. Ses principaux avantages sont :
  - ✓ Il offre un système d'exploitation gratuit.
  - ✓ Étant open-source, toute personne ayant des connaissances en programmation peut le modifier.
  - ✓ Il est facile d'apprendre Linux pour les débutants.
  - ✓ Les systèmes d'exploitation Linux offrent désormais des millions de programmes/applications et logiciels Linux parmi lesquels choisir, la plupart d'entre eux sont gratuits !
  - ✓ Il existe une communauté mondiale de développement qui cherche constamment des moyens d'améliorer sa sécurité. À chaque mise à niveau, le système d'exploitation devient plus sécurisé et robuste.
  - ✓ Le logiciel gratuit Linux est le système d'exploitation de choix pour les environnements de serveur en raison de sa stabilité et de sa fiabilité (des entreprises comme Amazon, Facebook et Google utilisent Linux pour leurs serveurs). Un serveur basé sur Linux pourrait fonctionner sans arrêt sans redémarrage pendant des années.

CHAPITRE 2

Appliquer les configurations de sécurité sur les OS

Ce que vous allez apprendre dans ce chapitre :

- Appliquer les règles du durcissement
- Utiliser les outils d’automatisation des contrôles des règles

7 heures

CHAPITRE 2

Appliquer les configurations de sécurité sur les OS

1. **Durcissement Windows**
2. Durcissement Linux

Durcissement par objectif

- Avant de commencer à parler des techniques et règles de durcissement à appliquer, il est toujours important de clarifier l'objectif du projet ou processus du durcissement. Plusieurs objectifs peuvent être visés. Par exemple :

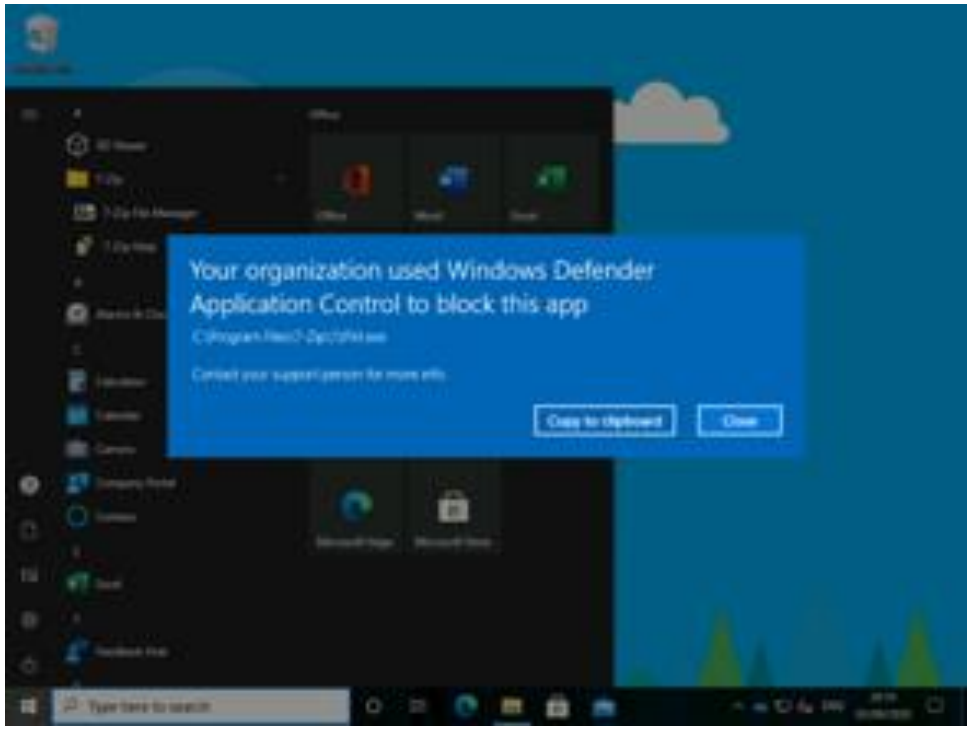
  - ✓ Prévention des scénarios d'attaque connus : en coordination avec l'équipe de veille technologique, nous devons être au courant des dernières menaces, vulnérabilités et attaques pour voir si nos actifs peuvent être impactés.
  - ✓ Réduction de la surface d'attaque : dans le cadre du principe de minimisation, l'idée est aussi de réduire la surface d'attaque pour plus de contrôle et de visibilité.
  - ✓ Améliorer la protection des données : si nos systèmes traitent ces données sensibles ou des données personnelles, nous devons nous engager à mettre en place les mécanismes nécessaires pour les protéger.
  - ✓ Minimiser les décisions clés en matière de sécurité et de confidentialité ainsi et les choix de l'utilisateur : dans le cadre de l'automatisation du processus du durcissement, il faut un processus clair avec moins de changements et d'actions manuelles.
  - ✓ Application de paramétrage par défaut raisonnable pour empêcher les modifications par l'utilisateur : avoir une configuration homogène sur tout le parc informatique facilite la gestion et la maintenance et aussi la réponse en cas d'incident.

Durcissement Windows

- Les dernières versions Windows sont livrées avec un éventail de fonctionnalités, d'applications et de logiciels qui doivent être correctement configurés pour garantir que le système soit aussi renforcé que possible. Parmi les outils intéressant à utiliser :

Windows Defender Application Control :

- ✓ Contrôle d'intégrité
- ✓ WDAC a été introduit avec Windows 10 et permet aux organisations de contrôler quels pilotes et applications sont autorisés à s'exécuter sur leurs clients Windows 10.
- ✓ Il a été conçu comme une fonctionnalité de sécurité selon les critères de maintenance définis par le Microsoft Security Response Center (MSRC).



Durcissement Windows

Pour une utilisation de Windows Defender Application Control sécurisée :

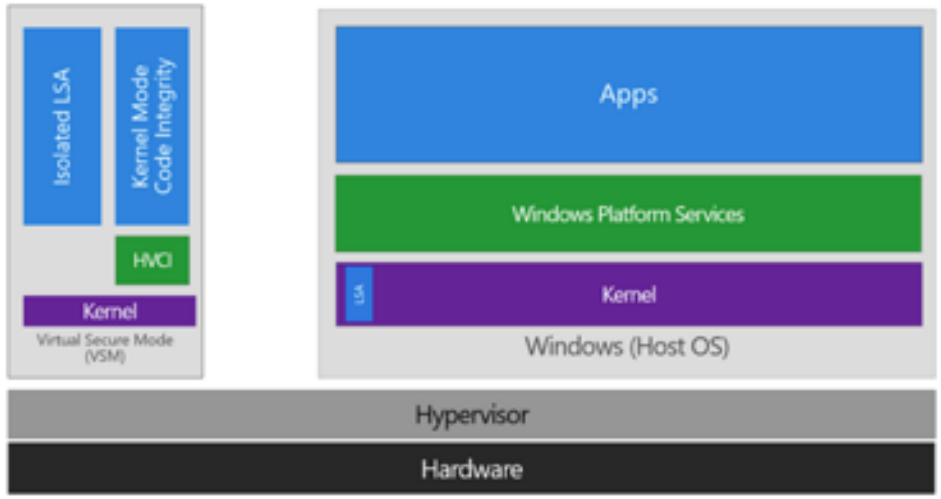
- ✓ **Activer Unified Extensible Firmware Interface (UEFI) :** le firmware UEFI fournit un stockage sécurisé pour les paramètres et fichiers de configuration WDAC pertinents, par exemple, pour la protection de l'intégrité d'un fichier de stratégie WDAC. Le stockage des paramètres et des fichiers de configuration WDAC sensibles dans le micrologiciel permet une protection contre la manipulation par un utilisateur Windows non autorisé.

- ✓ **Signature des politiques WDAC :** s'assurer que chaque stratégie WDAC est signée numériquement pour empêcher les modifications non autorisées des stratégies. Dans les organisations, cela nécessite un certificat de signature correctement géré, idéalement fourni par une infrastructure à clé publique (PKI). La politique WDAC elle-même doit être signée sur un système dédié pour assurer la protection du certificat de signature et du processus de signature. De plus, la politique WDAC signée ne doit être transférée que via un canal sécurisé vers les systèmes cibles correspondants.

Durcissement Windows

Virtualization Based Security (VBS) :

- ✓ La sécurité basée sur la virtualisation (VBS) est une fonctionnalité basée sur l'hyperviseur Microsoft qui sépare l'architecture Windows traditionnelle en deux environnements.
- ✓ La séparation de l'architecture Windows permet de créer et isoler une région sécurisée de mémoire du système d'exploitation normal, et donc isoler les fonctionnalités critiques de sécurité du mode normal, ce qui conduit à une protection accrue contre les accès non autorisés.
- ✓ Une base pour d'autres mesures de protection.
- ✓ Possibilité d'utiliser une approche de signature, ex : l'intégrité du code en mode noyau vérifie tous les pilotes et fichiers binaires en mode noyau avant leur démarrage, et empêche le chargement de pilotes ou de fichiers système non signés dans la mémoire système.



Durcissement Windows

Pour une utilisation de Virtualization Based Security (VBS) sécurisée :

Les paramètres de composant de base VBS suivants augmentent la sécurité de l'initialisation du système Windows 10 et protègent contre les attaques de plateforme (par exemple, les attaques qui abusent des fonctions au niveau du matériel).

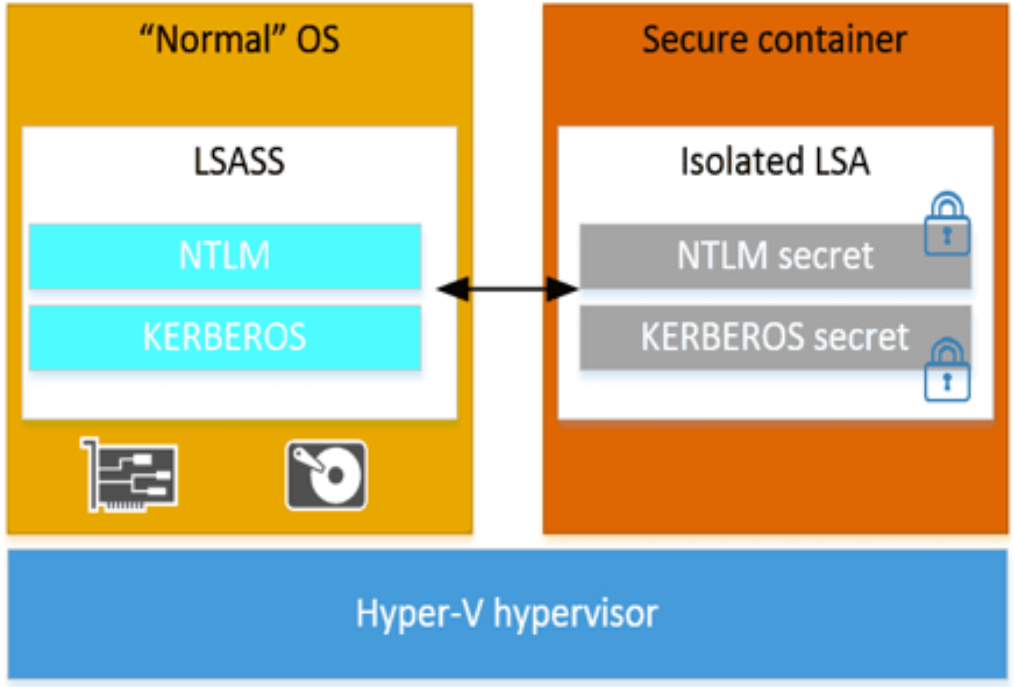
- ✓ **Démarrage sécurisé et protection DMA :** Secure Boot est une norme de démarrage sécurisé des ordinateurs, de sorte que l'ordinateur ne charge que les logiciels que le fabricant de l'ordinateur et/ou le fournisseur du système d'exploitation juge dignes de confiance. Le démarrage sécurisé et la protection DMA doivent être activés sur toutes les plateformes prenant en charge l'accès direct à la mémoire (DMA). Il s'agit de plateformes avec des périphériques dotés d'unités de gestion de mémoire d'entrée-sortie (IOMMU). Cette option de stratégie permet aux mécanismes de se défendre contre les attaques DMA et nécessite une prise en charge matérielle.
- ✓ **Configuration du lancement sécurisé :** cette configuration garantit qu'une plateforme n'est lancée qu'avec un code fiable. Il active la fonctionnalité dynamique de racine de confiance (DRTM) qui protège la plateforme contre les attaques basées sur le firmware.

Dans les slides suivantes, nous présenterons les configurations au niveau des applications VBS…

Durcissement Windows

Credential Guard :

- ✓ Credential Guard utilise VBS pour stocker et gérer en toute sécurité les informations d'identification Windows.
- ✓ Microsoft Defender Credential Guard utilise la sécurité basée sur la virtualisation pour isoler et protéger les secrets (par exemple, les hachages de mot de passe NTLM et les tickets d'octroi de tickets Kerberos) pour bloquer les attaques de hachage de passe ou de passage (Pass the Hash).
- ✓ La configuration de "Enabled with UEFI lock" active Credential Guard et demande à Windows de stocker les paramètres de configuration Credential Guard pertinents dans le stockage sécurisé d'UEFI.



Source: https://4sysops.com/wp-content/uploads/2016/06/Microsoft-Windows-Credential-Guard-schematic-diagram-600x363.png

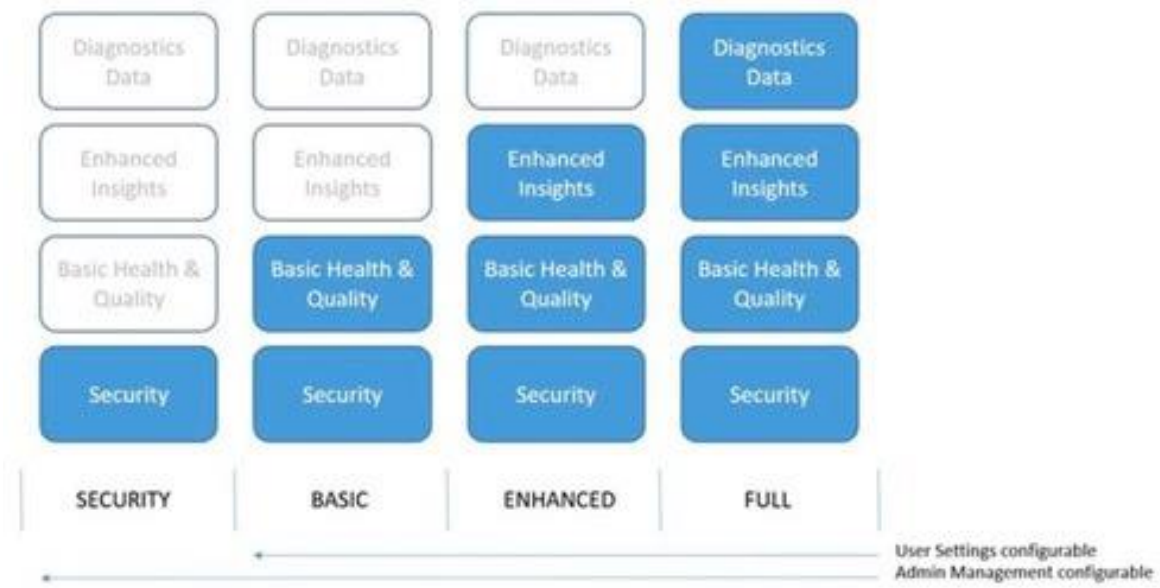
PARTIE 3

Durcissement Windows : les fonctionnalités à désactiver

- Certaines fonctionnalités de Windows qui ont comme objectif l'amélioration de l'expérience utilisateur ou qui sont destinées à un public spécifique, doivent être désactivées dans l'objectif de réduire la surface d'attaque de l'actif. Parmi ces fonctionnalités, nous pouvons citer :

  ✓ **Windows Telemtry**

Windows Telemtry est un composant windows 10 chargé de collecter et de transférer automatiquement des données vers une infrastructure backend exploitée par Microsoft.



Durcissement Windows : les fonctionnalités à désactiver

✓ PowerShell

Windows PowerShell fournit un environnement administratif puissant. Diverses ressources du système d'exploitation sont accessibles via Windows PowerShell. Cette énorme variété de fonctions fournit non seulement à l'administrateur de nombreux outils, mais est également de plus en plus utilisée par des attaquants pour mener des attaques complexes.

- Première étape : Désactiver Powershell 2.0 (vulnérable)
- Ensuite, restreindre les exécutions de script powershell (Restricted) :

Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2Root

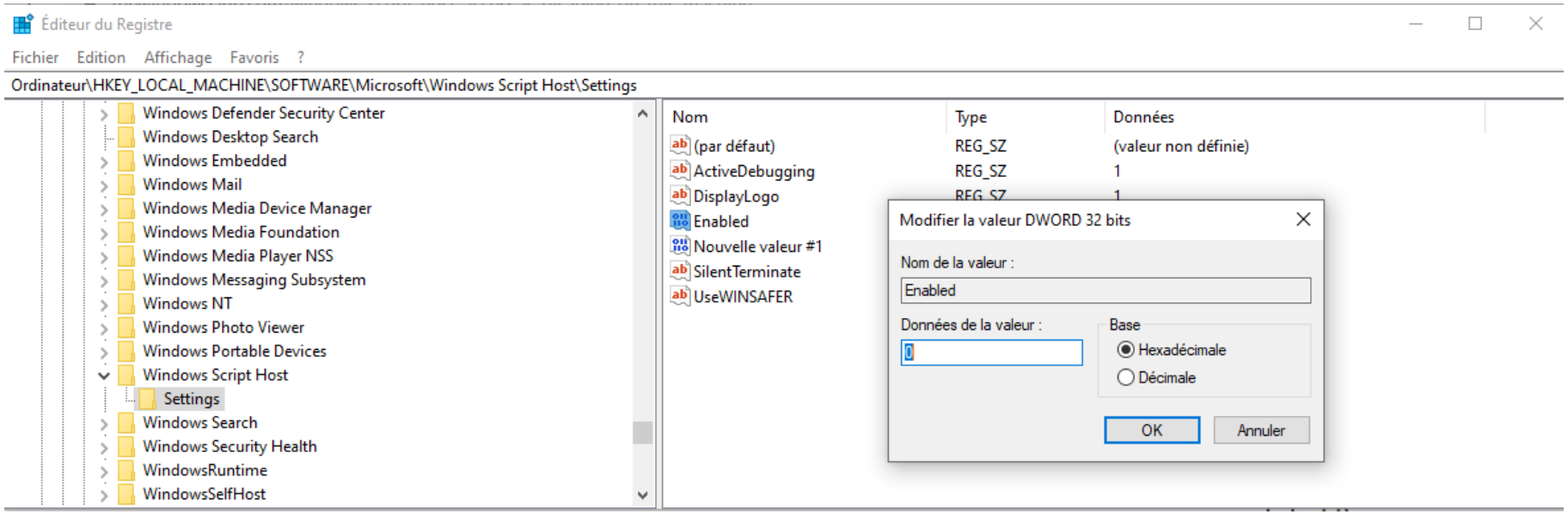
```
Testez le nouveau système multiplateforme PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2Root


Path          :
Online        : True
RestartNeeded : False



PS C:\WINDOWS\system32>
```

Durcissement Windows : les fonctionnalités à désactiver

✓ Windows Script Host

L'hôte de script Windows (WSH) fournit un environnement d'exécution pour un certain nombre de langages de script. Il peut être utilisé par les utilisateurs et les administrateurs pour automatiser des tâches. Plusieurs ransomwares, backdoors sont envoyés dans des fichiers .zip qui contiennent un code en JavaScript et qui sera exécuté via WSH.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings



PARTIE 3

Durcissement Windows : AD

- Il n'est pas possible de parler du durcissement de Windows sans parler du durcissement de l'AD qui Active Directory joue un rôle essentiel dans l'infrastructure informatique Windows et garantit l'harmonie et la sécurité des différentes ressources réseau dans un environnement global interconnecté.
- Pour continuer de présenter le durcissement dans le cadre des principes énoncés dans la partie 1. Nous allons nous concentrer sur les contrôles techniques à implémenter pour réduire la surface d'attaque de l'installation d'Active Directory :

L'implémentation de moindres privilèges comme modèle d'administration :

- Pour rappel, ce principe se concentre sur l'identification du risque que présente l'utilisation de comptes à privilèges élevés pour l'administration quotidienne, en plus de fournir des recommandations pour la mise en œuvre afin de réduire le risque que présentent les comptes privilégiés.
- Les privilèges excessifs n'est pas seulement un problème dans l'Active Directory , mais toute l'infrastructure qui l'entoure et qui peut l'impacter. Pour résumer les composants où le principe de moindres privilèges est à implémenter :

  - ✓ Active directory
  - ✓ les serveurs membres
  - ✓ les stations de travail
  - ✓ les applications

Durcissement Windows : AD

L'implémentation d'hôtes d'administration sécurisés :

- Cette recommandation présentée dans la partie 2 suit les principes de déploiement de systèmes d'administration dédiés et sécurisés. Nous rappelons ici quelques principes, pour plus de détails consulter la page officielle de Microsoft https://docs.microsoft.com/fr-fr/windows-server/identity/ad-ds/plan/security-best-practices/implementing-secure-administrative-hosts

✓ **Configuration de compte :** par exemple, les hôtes d'administration doivent être configurés pour exiger l'ouverture de session par carte à puce.

✓ **Sécurité physique :** la sécurité physique comprend le contrôle de l'accès physique aux hôtes d'administration.

✓ **AppLocker :** les hôtes d'administration doivent être configurés avec des scripts, des outils et des applications par le biais d'AppLocker ou d'un logiciel de restriction d'application tiers.

✓ **Restrictions RDP :** inclure des restrictions sur les comptes et les ordinateurs qui peuvent être utilisés pour établir des connexions protocole RDP (Remote Desktop Protocol) (RDP) aux systèmes gérés.

✓ **Gestion des correctifs et des configurations :** les organisations plus petites peuvent s'appuyer sur des offres telles que Windows Update ou Windows Server Update Services (WSUS) pour gérer le déploiement des mises à jour sur les systèmes de Windows, tandis que les grandes entreprises peuvent implémenter des logiciels de gestion des configurations et des correctifs d'entreprise tels que Microsoft Endpoint Configuration Manager.

✓ **Blocage de l'accès à Internet :** les hôtes d'administration ne doivent pas être autorisés à accéder à Internet, et ils ne doivent pas être en mesure de parcourir l'intranet d'une organisation.

Durcissement Windows : AD

Les bonnes pratiques pour sécurisation des contrôleurs de domaine contre les attaques :

- Cette partie traite des stratégies et des paramètres qui contiennent des recommandations spécifiques au contrôleur de domaine.

✓ **Gérer les groupes de sécurité Active Directory :** les membres affectés à des groupes de sécurité Active Directory tels que les administrateurs de domaine, d'entreprise et de schéma bénéficient du niveau de privilège maximal dans un environnement Active Directory. Ainsi, un attaquant ou un initié malveillant, affecté à l'un de ces groupes, aura libre cours sur votre environnement AD ainsi que sur vos données critiques. Vous devez limiter l'accès à ces groupes aux seuls utilisateurs qui en ont besoin.

✓ **Nettoyer les comptes d'utilisateurs inactifs dans AD :** les comptes d'utilisateurs inactifs présentent un risque sérieux pour la sécurité de votre environnement Active Directory car ils sont souvent utilisés par des administrateurs malveillants et des pirates pour accéder à des données critiques sans éveiller les soupçons.

✓ **Surveiller les administrateurs locaux :** il est très important pour les organisations de savoir ce que font les administrateurs locaux et comment leur accès a été accordé. Lors de l'octroi de l'accès aux administrateurs locaux, il est important de suivre la règle du « principe du moindre privilège ».

✓ **Auditer les connexions au contrôleur de domaine (DC) :** il est très important que les administrateurs système aient la possibilité de vérifier qui se connecte à un contrôleur de domaine afin de protéger les utilisateurs privilégiés et tous les actifs auxquels ils ont accès.

Durcissement Windows : AD

- ✓ **Assurer la protection LSASS :** à l'aide d'outils de piratage comme Mimikatz, les attaquants peuvent exploiter le service de sous-système de l'autorité de sécurité locale (LSASS) pour extraire les informations d'identification de l'utilisateur, qui peuvent ensuite être utilisées pour accéder aux actifs associés à ces informations d'identification.

- ✓ **Une politique de mot de passe stricte :** avoir une politique de mot de passe efficace est crucial pour la sécurité de votre organisation. Il est important que les utilisateurs changent périodiquement leurs mots de passe. Les mots de passe qui sont rarement, voire jamais modifiés, sont moins sécurisés car ils créent une plus grande possibilité de vol.

- ✓ **Backup et restaure de l'Active Directory :** il est recommandé de sauvegarder régulièrement votre Active Directory, avec des intervalles ne dépassant pas 60 jours. En effet, la durée de vie des objets de désactivation AD est, par défaut, de 60 jours. Vous devez viser à inclure votre sauvegarde AD dans votre plan de reprise après sinistre pour vous aider à vous préparer à tout événement catastrophique. En règle générale, au moins un contrôleur de domaine doit être sauvegardé.

- ✓ **Activer la surveillance de la sécurité d'Active Directory pour les signes de compromis :** être en mesure d'auditer et de surveiller de manière proactive et continue votre Active Directory vous permettra de repérer les signes d'une violation ou d'un compromis. Dans la plupart des cas, de graves failles de sécurité peuvent être évitées grâce à l'utilisation de solutions de surveillance.

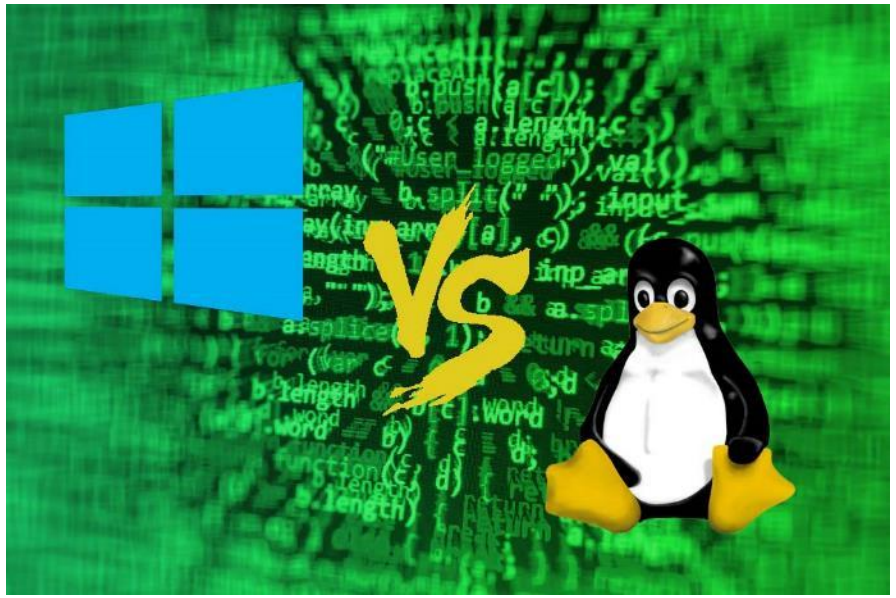
CHAPITRE 2

Appliquer les configurations de sécurité sur les OS

1. Durcissement Windows
2. **Durcissement Linux**

La sécurité dans Linux

- Contrairement à Windows, Linux a été conçu dès le départ comme un OS multi-user. Ainsi, la sécurité des utilisateurs a tendance à être un peu meilleure sur un Linux. Linux offre une meilleure séparation entre les utilisateurs administrateurs et utilisateurs sans privilèges. Cela rend la tâche plus difficile pour un utilisateur sans privilèges pour infecter une machine avec un code malicieux.
- Linux est beaucoup plus résistant aux virus et aux infections par des logiciels malveillants que Windows. Certaines distributions Linux sont livrées avec des mécanismes intégrés, tels que SELinux dans Red Hat et Centos, et AppArmor dans Ubuntu, qui empêchent les attaquants de prendre le contrôle d'un système.
- Linux est un logiciel libre et open source. Cela permet à toute personne ayant les compétences d'auditer le code Linux pour rechercher des bugs ou des backdoors.
- Cependant, Linux n'est pas parfait.



La sécurité dans Linux

- Le système d'exploitation Linux et les applications de support deviennent une cible de choix pour les adversaires. Linux est utilisé comme système d'exploitation principal pour de nombreux composants qui automatisent les facettes de l'infrastructure critique, les technologies sur site et basées sur le cloud et les appareils Internet des objets (IoT).
- Comme pour les architectures basées sur Windows, les protections de sécurité doivent être alignées pour les machines Linux afin de renforcer les informations d'identification, les méthodes d'accès, de protéger le noyau et de renforcer l'audit et la visibilité des activités.
- La sécurité Linux comporte de nombreux aspects, notamment le renforcement, l'audit et la conformité du système Linux.

Aspect	Core	Ressources	Services	Environnement
Durcissement système	process de démarrage conteneurs frameworks kernel service Manager virtualisation	accès authentification cryptographie traçabilité réseau applications stockage	bases de données mail surveillance impression shell web	analyse numérique réponse aux incidents logiciels malveillants risques surveillance de la sécurité intégrité systèmes
Audit sécurité				
Conformité				

Durcissement Linux

Gardez le noyau Linux et les logiciels à jour :

- L'application de correctifs de sécurité est une partie importante de la maintenance du serveur Linux. Linux fournit tous les outils nécessaires pour maintenir votre système à jour et permet également des mises à niveau faciles entre les versions. Toutes les mises à jour de sécurité doivent être examinées et appliquées dès que possible. La mise à jour est possible en utilisant le gestionnaire de packages RPM tel que **yum** et/ou **apt-get** et/ou **dpkg** pour appliquer toutes les mises à jour de sécurité.

Minimiser les logiciels pour minimiser la vulnérabilité sous Linux :

- Souvent, en principe nous n'avons pas vraiment besoin de toutes sortes de services installés. Il faut éviter d'installer des logiciels inutiles pour éviter les vulnérabilités des logiciels. Utilisez le gestionnaire de packages RPM tel que yum ou apt-get et/ou dpkg pour examiner tous les ensembles de packages logiciels installés sur un système. Supprimez tous les packages indésirables.

Durcissement Linux

Sécurisation des comptes utilisateurs :

- La gestion des utilisateurs de n'importe quel système n'est pas une mince tâche. Le principe du moindre privilège stipule que chaque utilisateur ne doit avoir qu'un accès suffisant pour effectuer ses tâches quotidiennes. Cela signifie qu'un administrateur RH ne doit pas avoir accès aux fichiers journaux du système. Cependant, cela peut signifier qu'un administrateur informatique a accès au lecteur RH, mais pas nécessairement aux informations sur les employés.
- En plus, sur Linux l'utilisateur root est l'utilisateur le plus élevé d'un système Linux. Il peut tout faire, y compris modifier les fichiers système et de démarrage. Sachant cela, nous pouvons comprendre pourquoi la connexion en tant que root n'est probablement pas idéale dans la plupart des situations.

Renforcer le contrôle d'accès noyau (SELinux) :

- SELinux est un mécanisme de sécurité du contrôle d'accès dans le noyau. Si le serveur est accessible depuis le net, il fortement conseillé de l'activer. 3 modes sont possible pour SELinux :
  - ✓ **Enforcing :** mode par défaut qui active et applique la stratégie de sécurité SELinux sur la machine.
  - ✓ **Permissive :** SELinux n'appliquera pas la politique de sécurité, mais avertira seulement et enregistrera les actions.
  - ✓ **Désactivé**.

Durcissement Linux

Configuration d'AppArmor :

- AppArmor peut être utilisé par l'administrateur pour associer chaque programme à un profil de sécurité qui restreint les capacités de celui-ci. Il est très pratique pour protéger la confidentialité des données.

Partitions de disque séparées pour le système Linux :

- La séparation des fichiers du système d'exploitation des fichiers utilisateur peut donner lieu à un système meilleur et sécurisé. Assurez-vous que les systèmes de fichiers suivants sont montés sur des partitions distinctes :
  - ✓ /usr
  - ✓ /home
  - ✓ /var et /var/tmp
  - ✓ /tmp

Durcissement Linux en utilisant Lynis

Lynis :

Afin d'automatiser cette tâche de durcissement, nous pouvons utiliser l'outil Lynis présenté dans la partie 2. Dans cet exemple, nous lançons Lynis en local avec :

Lynis audit system

```
root@debian:/home/hamza# /usr/sbin/lynis audit system

[ Lynis 3.0.2 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2020, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
```

Durcissement Linux en utilisant Lynis

Lynis :

Les résultats sont organisés par classe, dans l'exemple suivant lynis rapporte qu'il n'y pas de framework de contrôle comme AppArmor ou SELinux qui sont installés.

```
------------------------------------

[+] Security frameworks
------------------------------------
  - Checking presence AppArmor                                [ NOT FOUND ]
  - Checking presence SELinux                                 [ NOT FOUND ]
  - Checking presence TOMOYO Linux                            [ NOT FOUND ]
  - Checking presence grsecurity                              [ NOT FOUND ]
  - Checking for implemented MAC framework                    [ NONE ]

[+] Software: file integrity
------------------------------------
  - Checking file integrity tools
    - AIDE                                                    [ FOUND ]
      - AIDE config file                                      [ FOUND ]
      - AIDE database                                         [ NOT FOUND ]
      - AIDE config (Checksum)                                [ OK ]
  - Checking presence integrity tool                          [ FOUND ]
```

PARTIE 4

Déployer des solutions DLP et de traçabilité

Dans ce module, vous allez :

- Définir la fonction et le rôle d'une solution DLP
- Analyser les options de déploiement d'une solution DLP
- Comprendre les rôles et les types des solutions de traçabilité

7 heures

CHAPITRE 1

Configurer une solution DLP

Ce que vous allez apprendre dans ce chapitre :

- Définition et rôle des solutions DLP
- Les options de déploiement d’une solution DLP

1 heures

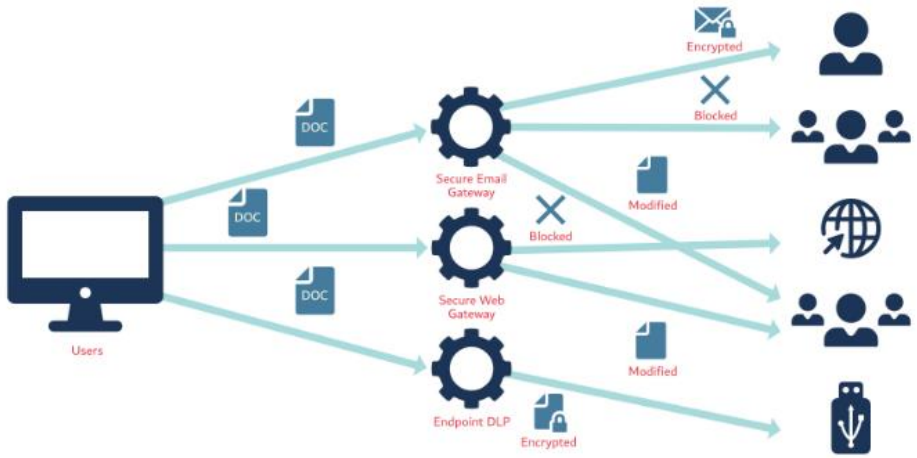
CHAPITRE 1

Configurer une solution DLP

1. **Définition de la notion DLP**
2. Configuration des politiques de détection

DLP

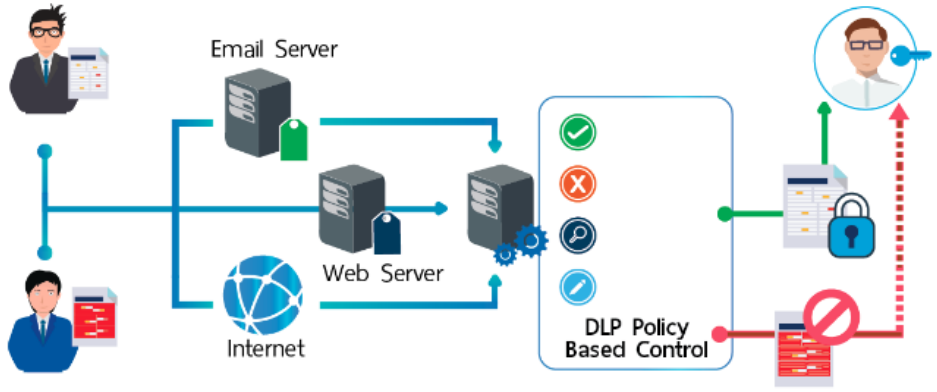
- DLP (Data Leak Prevention/ Data Loss Prevention / Data Leak Protection / Data Loss Protection) - est une stratégie visant à atténuer les menaces pesant sur les données critiques. Le DLP est généralement mis en œuvre dans le cadre du plan d'une organisation pour la sécurité globale des données.
- En utilisant une variété d'outils logiciels et de pratiques de confidentialité des données, DLP vise à empêcher l'accès non autorisé aux informations sensibles. Pour ce faire, il classe les différents types de contenu au sein d'un objet de données et applique des politiques de protection automatisées.
- Une stratégie DLP multicouche garantit que les informations sensibles restent derrière un pare-feu réseau. La création d'un plan DLP permet également à une organisation d'examiner et de mettre à jour ses politiques de stockage et de conservation des données afin de maintenir la conformité réglementaire.
- Par exemple La tendance du télétravail, associée à des cyberattaques plus sophistiquées, a accentué l'intérêt croissant pour le DLP. Le cabinet d'études Gartner a estimé que 90 % des organisations ont mis en œuvre au moins une forme de DLP intégré en 2021, contre 50 % en 2017.



Source : https://bbes-group.com/wp-content/uploads/2021/06/how-works-DLP.png

Fonctionnement du DLP

- Le logiciel DLP surveille, détecte et empêche les données sensibles de quitter une organisation. Cela signifie surveiller à la fois les données entrant dans les réseaux d'entreprise, ainsi que les données tentant de sortir du réseau.
- La plupart des produits logiciels DLP se concentrent sur les actions de blocage. Par exemple, si un employé tentait de transférer un e-mail professionnel contre la politique de l'entreprise en dehors du domaine de l'entreprise ou de télécharger un fichier d'entreprise sur un service de stockage cloud grand public tel que Dropbox, l'autorisation serait refusée.
- En outre, le logiciel DLP peut empêcher les ordinateurs des employés de lire et d'écrire sur des clés USB pour empêcher toute copie non autorisée.
- La détection se concentre principalement sur la surveillance des e-mails entrants, la recherche de pièces jointes et d'hyperliens suspects pour les attaques de phishing. La plupart des logiciels DLP offrent aux organisations la possibilité de signaler le contenu incohérent pour que le personnel l'examine manuellement ou le bloque complètement.
- Au début du DLP, les équipes de sécurité établissaient les règles de détection et de blocage, mais celles-ci étaient simplistes et souvent contournées. Les nouveaux logiciels utilisent l'intelligence artificielle basée sur l'apprentissage automatique, qui peut apprendre et améliorer l'approche de détection et de blocage au fil du temps.



Les technologies DLP

- Il existe deux types de produits DLP : dédiés et intégrés.
  - ✓ Les produits dédiés sont des produits autonomes approfondis et complexes.
  - ✓ Les produits intégrés sont plus basiques, fonctionnent avec d'autres outils de sécurité concernant l'application des politiques et sont moins chers que les outils DLP dédiés.
- Il est peu probable qu'un seul outil réponde à tous les besoins de prévention des pertes de données d'une organisation. De nombreux fournisseurs DLP se concentrent sur un domaine, tandis que d'autres proposent des suites d'outils qui s'intègrent. Les entreprises peuvent assembler un ensemble d'outils de pointe ou utiliser une suite tout-en-un.
- Certains des principaux fournisseurs incluent les éléments suivants :
  - ✓ **Symantec Data Loss Prevention de Broadcom :** Ce logiciel DLP de niveau entreprise couvre les terminaux, les centres de données et le cloud computing.
  - ✓ **Checkpoint Data Loss :** Cet outil se concentre sur les violations et l'exfiltration de données.
  - ✓ **CoSoSys Endpoint Protector :** Il s'agit d'un protecteur tout-en-un dédié pour Windows, Apple et Linux.
  - ✓ **ManageEngine Device Control Plus :** Il s'agit d'un protecteur de point de terminaison dédié axé sur la sécurité USB.
  - ✓ **McAfee Total Protection for DLP :** Il s'agit d'une suite de six produits DLP pour la découverte, la surveillance et la prévention.
  - ✓ **SolarWinds Data Loss Prevention with Access Rights Manager :** Malgré la faille de sécurité massive, SolarWinds est largement considéré comme l'un des meilleurs fournisseurs de DLP.
  - ✓ **VikingCloud Endpoint Protection :** Ce produit se concentre sur les risques internes, tels que le vol de données et l'utilisation non autorisée d'Internet.

La mise en place d'un programme DLP

- Indépendamment des technologies utilisées, les organisations peuvent suivre plusieurs étapes pour mettre en œuvre un programme DLP, notamment :

✓ **Réaliser un inventaire et une évaluation :** les entreprises ne peuvent pas protéger ce qu'elles ignorent avoir. Un inventaire complet est indispensable. Certains produits DLP - de fournisseurs tels que Barracuda Networks, Cisco et McAfee - effectueront une analyse complète du réseau.

✓ **Classer les données :** les organisations ont besoin d'un cadre de classification des données pour les données structurées et non structurées. Ces catégories comprennent les informations personnellement identifiables (PII), les données financières, les données réglementaires et la propriété intellectuelle.

✓ **Établir des politiques de traitement et de correction des données :** l'étape suivante après la classification des données consiste à créer des politiques pour les gérer. Cela est particulièrement vrai pour les données réglementées ou dans les zones soumises à des règles strictes, telles que l'Europe avec le RGPD et la Californie avec le CCPA.

✓ **Mettre en œuvre un programme DLP unique et centralisé :** de nombreuses organisations mettent en œuvre plusieurs plans DLP dans différents départements et unités commerciales. Cela conduit à une incohérence de la protection et à l'absence d'une image complète du réseau. Il devrait y avoir un programme global.

✓ **Éduquer les employés :** les actions involontaires sont beaucoup plus courantes que les intentions malveillantes. La sensibilisation et l'acceptation des politiques et procédures de sécurité par les employés sont essentielles pour DLP.

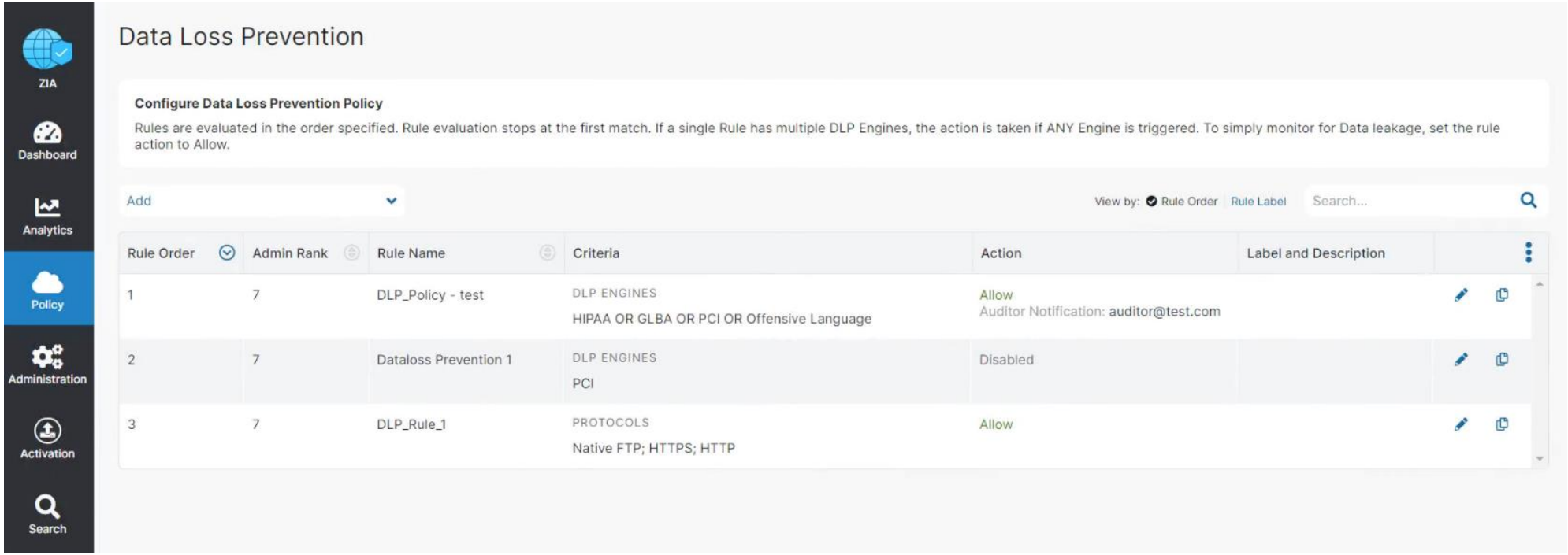
CHAPITRE 1

Configurer une solution DLP

1. Définition de la notion DLP
2. **Configuration des politiques de détection**

Configuration de DLP Zscaler

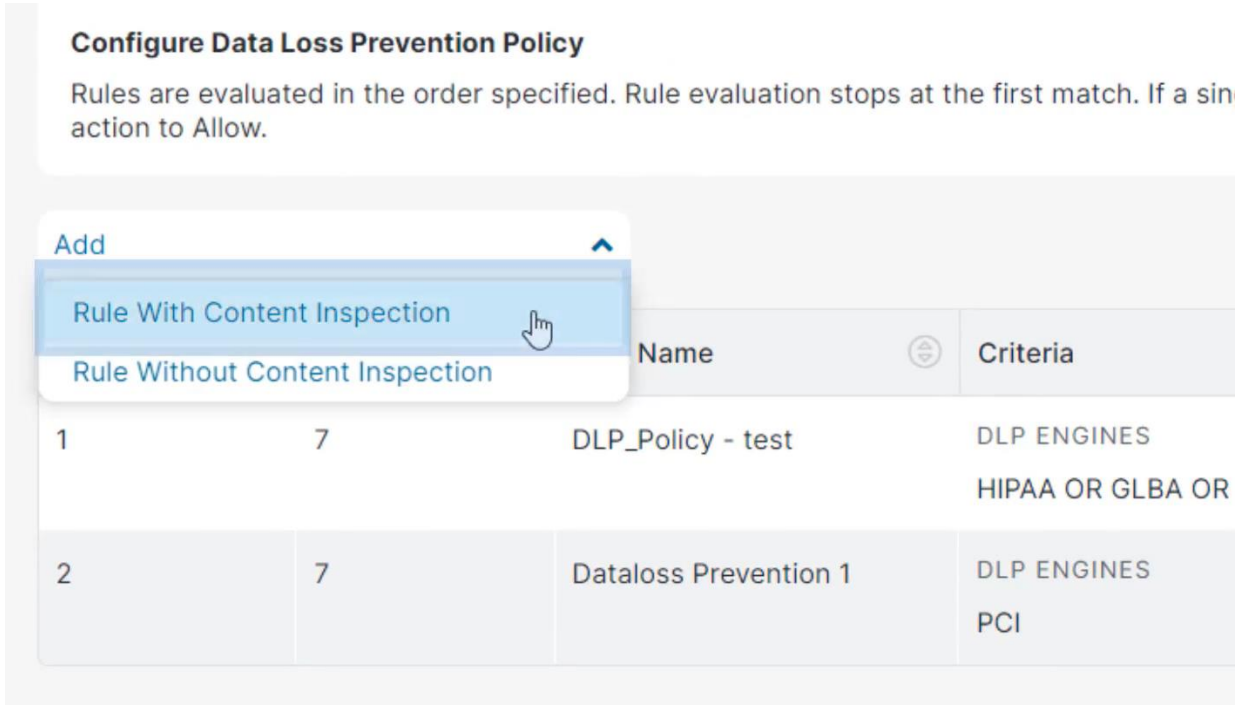
- Dans cet exemple, nous allons présenter la page de configuration des politiques de détection du DLP Zscaler.
- D'abord, en arrivant à la page d'accueil nous pouvons cliquer sur Data Loss Prevention, ce qui donnera la liste des politiques configurées actuellement :



Configuration de DLP Zscaler

- Nous pouvons ajouter 2 types de règles en cliquant sur Add :

  - ✓ Règle avec l'inspection de contenu : le DLP va réaliser la détection et l'inspection du contenu du trafic.
  - ✓ Règle sans l'inspection de contenu : le DLP se charge seulement de la détection et envoie le trafic suspect à un autre outil pour la partie inspection.



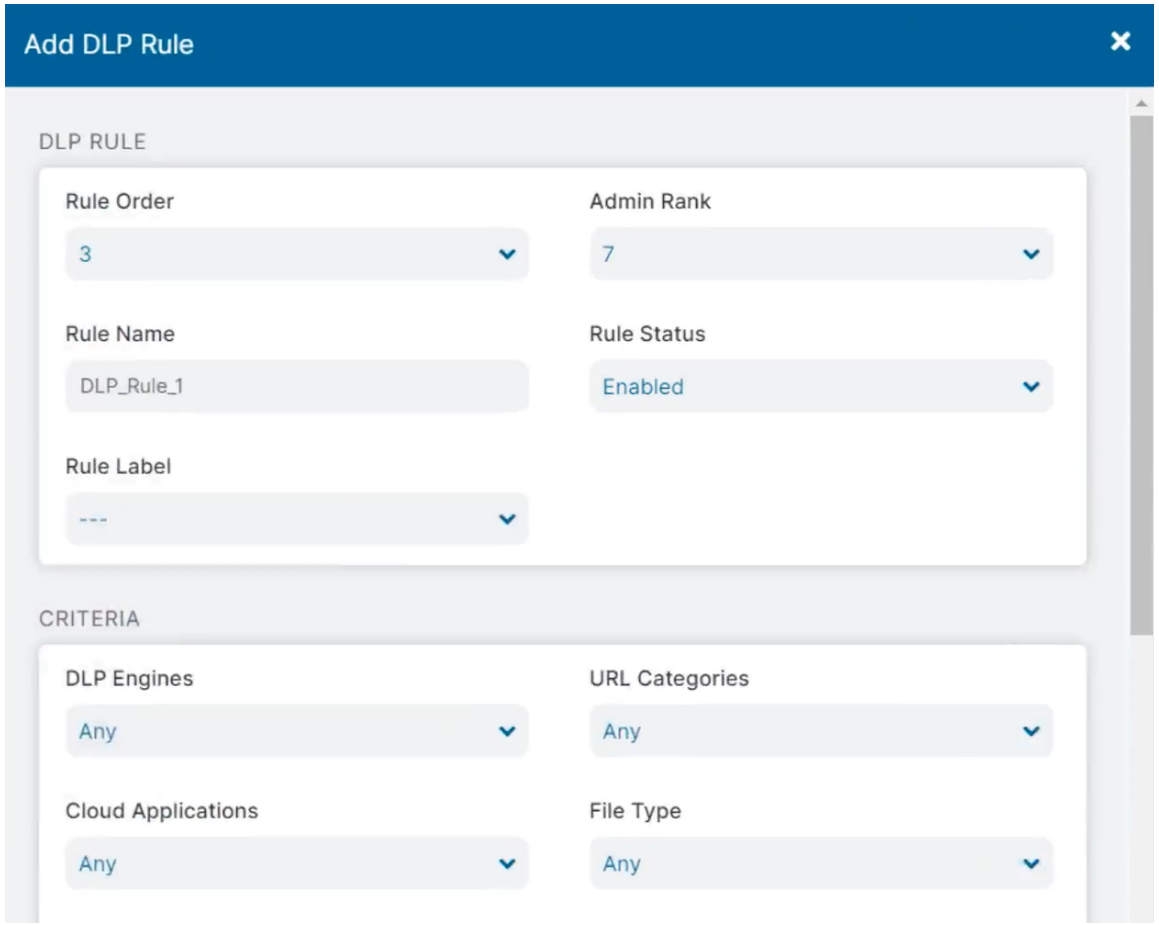
PARTIE 4

Configuration de DLP Zscaler

- Ensuite il faut préciser :

  - ✓ **L'ordre de la règle :** les règles sont évaluées dans l'ordre numérique croissant (règle 1 avant la règle 2, etc.), et l'ordre des règles reflète la place de cette règle dans l'ordre. Vous pouvez modifier la valeur, mais si vous avez activé le classement administrateur, le classement administrateur attribué détermine les valeurs d'ordre des règles que vous pouvez sélectionner.
  - ✓ **Le nom de la règle**
  - ✓ **Le statut de la règle : activé ou désactivé**
  - ✓ **Le rang admin de la règle :** le rang administrateur de la règle détermine la valeur que vous pouvez sélectionner dans l'ordre des règles, de sorte qu'une règle avec un rang administrateur plus élevé précède toujours une règle avec un rang admin inférieur.

- Pour les critères, nous pouvons garder any par défaut pour détecter et inspecter tout type de trafic

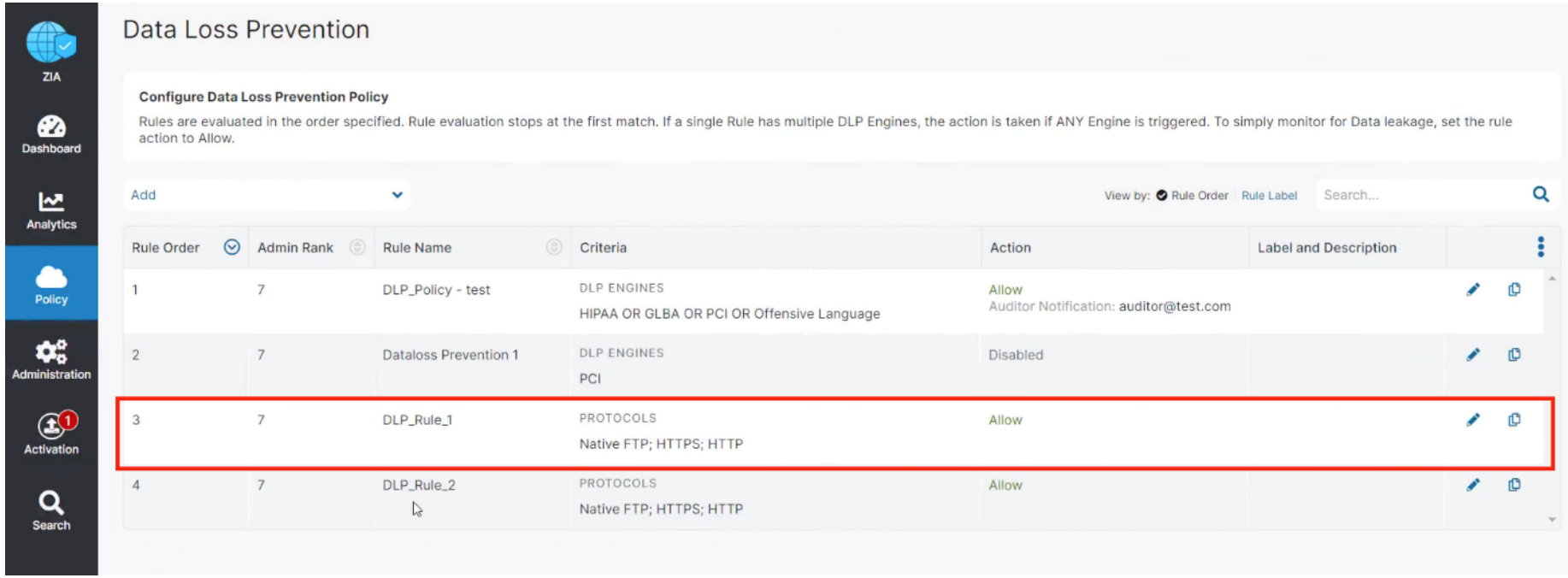


PARTIE 4

PARTIE 4

Configuration de DLP Zscaler

- Dès que la règle est enregistrée, elle est ajoutée et classée selon sa configuration. Dans notre cas, elle sera la 3ème règle à vérifier pour tout type de trafic.



CHAPITRE 2

Configurer une solution de gestion de la traçabilité

Ce que vous allez apprendre dans ce chapitre :

- Définition et rôle des solutions de traçabilité
- Les options de déploiement d’une solution de traçabilité

1 heures

CHAPITRE 2

Configurer une solution de gestion de la traçabilité

1. **Définition de la traçabilité**
2. Configuration des politiques de traçabilité

La traçabilité

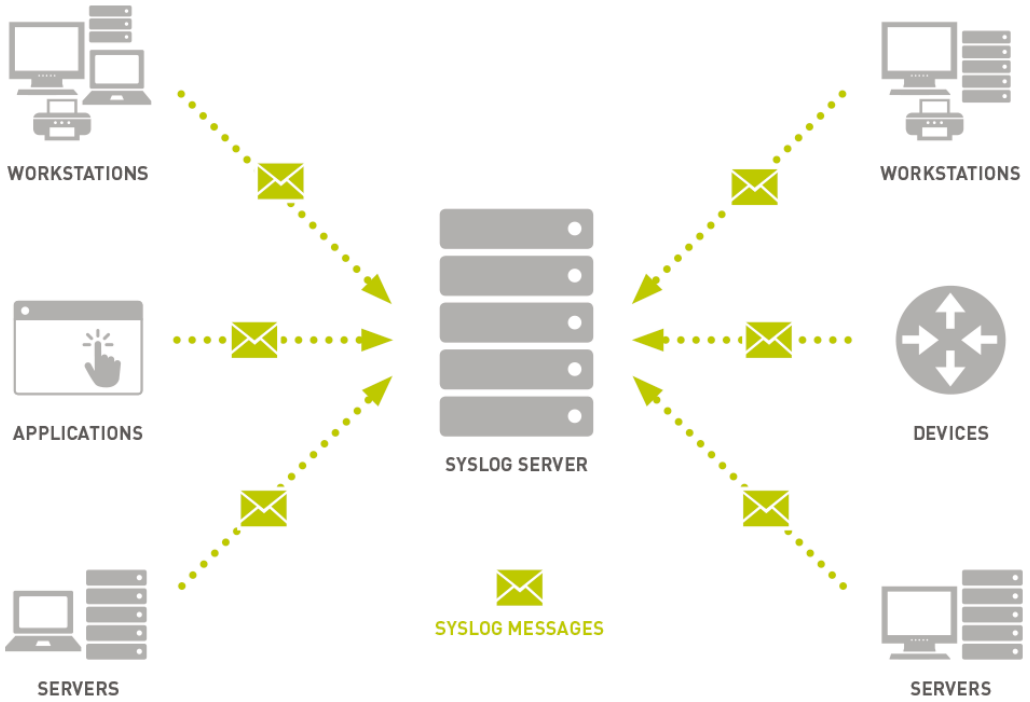
- La traçabilité est la possibilité d'identifier l'origine et de reconstituer le parcours d'un élément (donnée, attaque, action, changement, accès, etc.) aux différents stades de sa production et de sa transformation.
- Toutes les actions sur le SI doivent être tracées, c'est-à-dire qu'il faut être capable de savoir qui réalise quoi, et quand. Nous parlons également parler de non-répudiation.
- Certaines solutions et protocoles ont été mis au point dans le but d'aider à maintenir ces liens de traçabilité : syslog, SNMPv3, Windows Event, etc.

- Dans le cadre de la définition de la traçabilité nous pouvons trouver des process qui se chevauchent mais sont différents dans leurs objectifs :

  ✓ **Journalisation (logging) :** l'objectif de la journalisation est de suivre les rapports d'erreurs et les données associées de manière centralisée. La journalisation doit être utilisée dans les grandes applications et peut être utilisée dans les applications plus petites, surtout si elles fournissent une fonction cruciale. Le terme journalisation peut faire référence à la fois à la pratique de la journalisation des événements ou aux fichiers journaux réels qui en résultent.

  ✓ **Surveillance (monitoring) :** bien que la surveillance puisse être un terme informel qui peut être appliqué à la traçabilité ou à la journalisation ou à un certain nombre d'autres activités, dans ce contexte, la surveillance est beaucoup plus spécifique : instrumenter une application, puis collecter, agréger et analyser des métriques pour améliorer votre compréhension de la façon dont le système se comporte.

La traçabilité : la journalisation et la surveillance des événements



- La journalisation et la surveillance des événements de sécurité sont deux parties d'un processus singulier qui fait partie intégrante de la traçabilité dans une infrastructure sécurisée. Chaque activité sur votre environnement, des e-mails aux connexions en passant par les mises à jour du pare-feu, est considérée comme un événement de sécurité. Tous ces événements sont (ou devraient être) enregistrés afin de garder un œil sur tout ce qui se passe dans votre paysage technologique.
- Lorsqu'il s'agit de surveiller ces journaux, les organisations examineront les fichiers journaux d'audit électroniques contenant des informations confidentielles à la recherche de signes d'activités non autorisées.
- Si des activités non autorisées (ou des tentatives de celles-ci) sont découvertes, les données seront transférées vers une base de données centrale pour des enquêtes supplémentaires et les actions nécessaires.
- À une époque où les menaces numériques sont répandues et en constante évolution, les données extraites de ces fichiers journaux sont essentielles pour maintenir l'agilité et la réactivité de l'infrastructure.

La traçabilité : la journalisation et la surveillance des événements

- Un processus efficace de collecte et d'analyse des données de journaux doit intégrer des outils permettant d'examiner rapidement et facilement les journaux d'audit à la recherche de preuves d'événements critiques tels que :

  - ✓ **Reconnaissance contre votre environnement :** où les adversaires effectuent des recherches sur votre environnement… qui pourraient faire de vous leur prochaine cible.
  - ✓ **Armement** *:* une intrusion dans votre environnement où des adversaires ont décidé de prendre des mesures contre votre réseau et vos systèmes informatiques.
  - ✓ **Livraison :** la manifestation d'un exploit contre une vulnérabilité au sein de votre réseau ou de vos systèmes informatiques.
  - ✓ **Installation de logiciels malveillants :** observée lorsqu'un adversaire a modifié la fonctionnalité native de votre environnement pour maintenir la persistance.
  - ✓ **Commande et contrôle :** lorsque des pirates informatiques accèdent à votre serveur et à vos systèmes et prennent efficacement le contrôle de votre environnement.
  - ✓ **L'action commence :** déterminer les actions de l'adversaire et maintenir une visibilité sur lui à tout moment sont essentiels, vous voulez comprendre son objectif souhaité et empêcher l'intrusion réussie.

CHAPITRE 2

Configurer une solution de gestion de la traçabilité

1. Définition de la traçabilité
2. **Configuration des politiques de traçabilité**

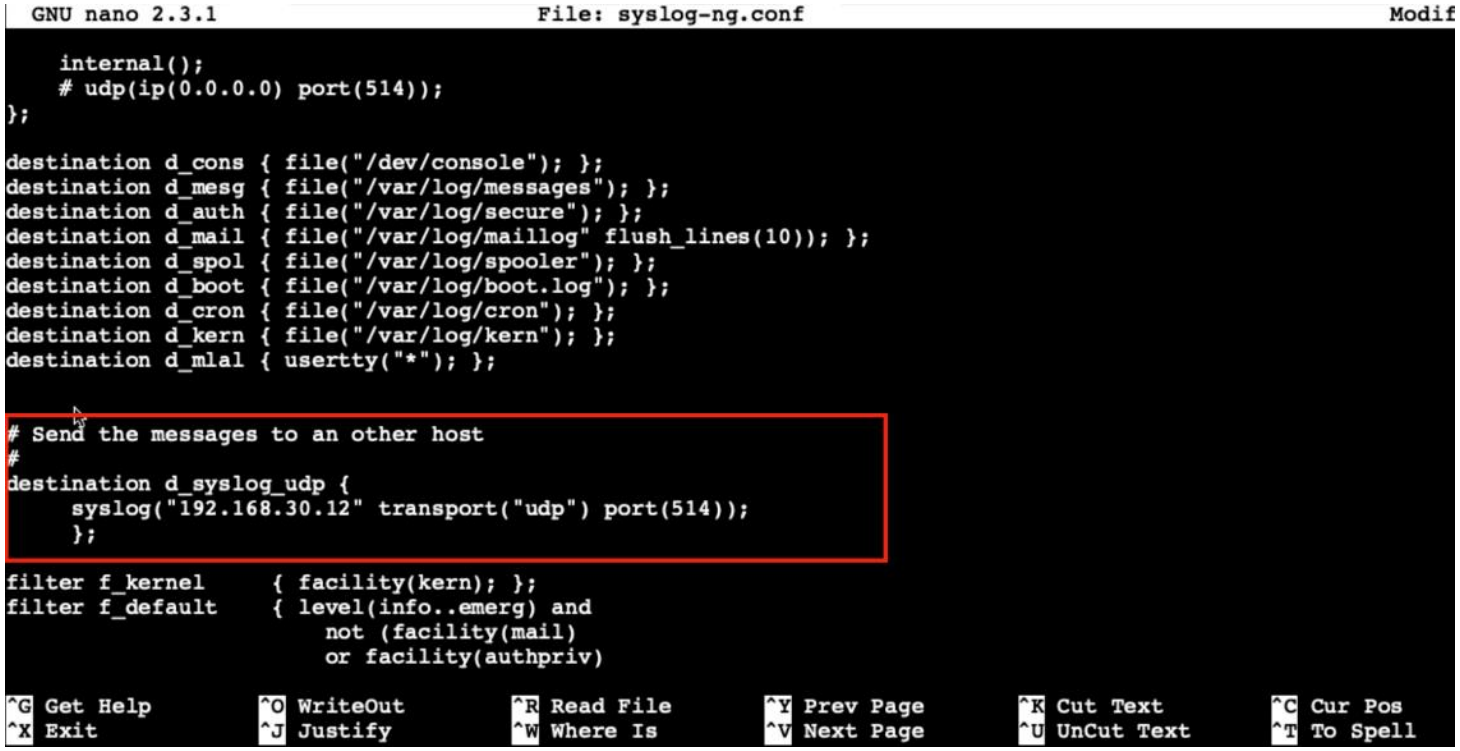
Configuration syslog-ng

- Dans cet exemple, nous allons configurer syslog-ng, la nouvelle version de syslog.
- D'abord, nous commençons par l'installation de syslog-ng, dans notre cas, nous l'installons sur une distribution centos avec : yum install syslog-ng

```
[root@localhost /]# yum install syslog-ng
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirrors.codec-cluster.org
 * epel: d2lzkl7pfhq30w.cloudfront.net
 * extras: mirror.sjc02.svwh.net
 * updates: centos.sonn.com
Resolving Dependencies
--> Running transaction check
---> Package syslog-ng.x86_64 0:3.24.1-1.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package         Arch         Version              Repository                 Size
================================================================================
Installing:
 syslog-ng       x86_64       3.24.1-1.el7         copr:copr.fedorainfracloud.org:czanik:syslog-ng324       810 k

Transaction Summary
================================================================================
Install  1 Package

Total download size: 810 k
Installed size: 3.0 M
Is this ok [y/d/N]:
```

Configuration syslog-ng

- Dans le fichier de configuration que nous pouvons trouver dans /etc/syslog-ng/syslog-ng.conf, nous pouvons configurer un envoi des messages syslog vers un autre serveur (SIEM par exemple) pour traitement, visualisation ou simplement pour un besoin de stockage :



PARTIE 4

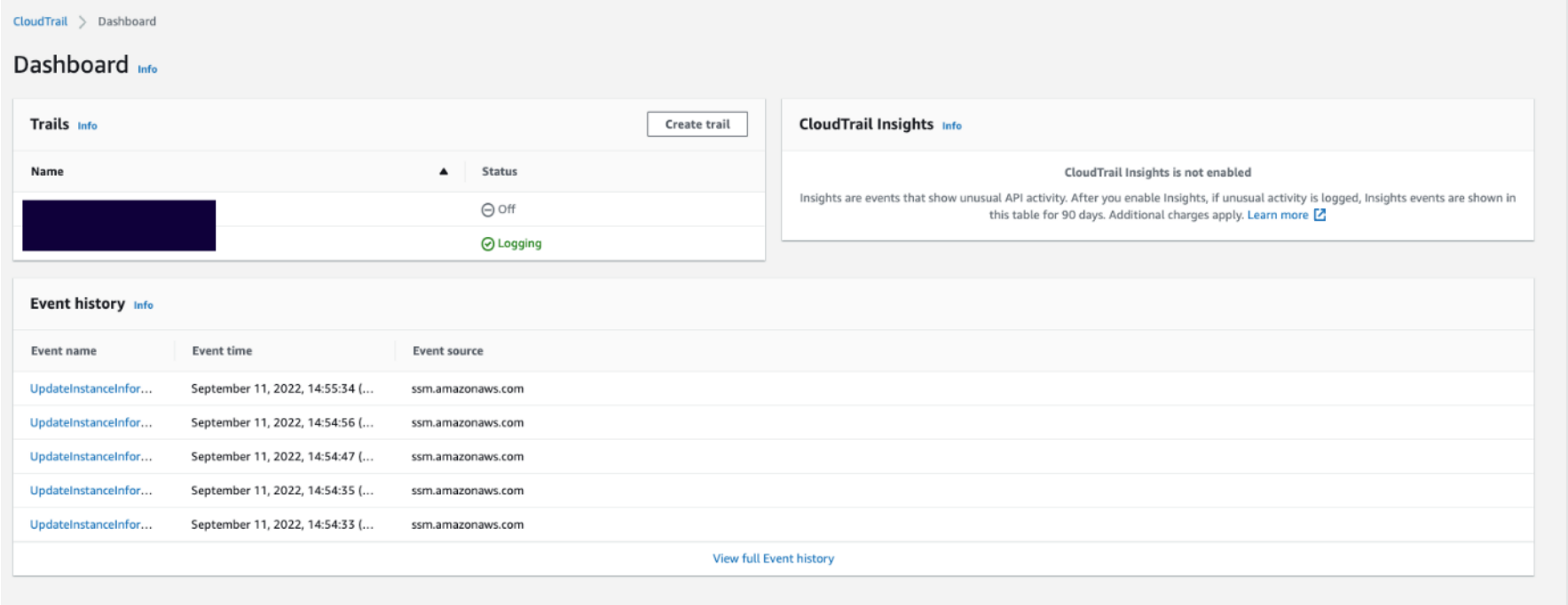
Configuration syslog-ng

- Nous pouvons ensuite démarrer le service syslog-ng et vérifier le statut : systemctl start syslog-ng et systemctl status syslog-ng

```
[root@localhost syslog-ng]# systemctl start syslog-ng
[root@localhost syslog-ng]# systemctl status syslog-ng
● syslog-ng.service - System Logger Daemon
   Loaded: loaded (/usr/lib/systemd/system/syslog-ng.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2020-01-14 17:24:28 PST; 8s ago
     Docs: man:syslog-ng(8)
 Main PID: 23784 (syslog-ng)
   CGroup: /system.slice/syslog-ng.service
           └─23784 /usr/sbin/syslog-ng -F -p /var/run/syslogd.pid

Jan 14 17:24:28 localhost.localdomain systemd[1]: Starting System Logger Daemon...
Jan 14 17:24:28 localhost.localdomain syslog-ng[23784]: [2020-01-14T17:24:28.629711] WARNING: Configuration fil...
Jan 14 17:24:28 localhost.localdomain syslog-ng[23784]: [2020-01-14T17:24:28.665206] Plugin module not found...tp'
Jan 14 17:24:28 localhost.localdomain syslog-ng[23784]: [2020-01-14T17:24:28.671879] Plugin module not found...tp'
Jan 14 17:24:28 localhost.localdomain syslog-ng[23784]: [2020-01-14T17:24:28.673025] Plugin module not found...tp'
Jan 14 17:24:28 localhost.localdomain syslog-ng[23784]: [2020-01-14T17:24:28.681323] WARNING: With use-dns(n...o!;
Jan 14 17:24:28 localhost.localdomain systemd[1]: Started System Logger Daemon.
Hint: Some lines were ellipsized, use -l to show in full.
[root@localhost syslog-ng]#
```

Configuration CloudTrail

- Nous allons aussi donner un exemple de configuration des politiques de traçabilité pour une infrastructure cloud AWS.
- Le service qui nous permet de le faire sur AWS est CloudTrail



PARTIE 4

PARTIE 4

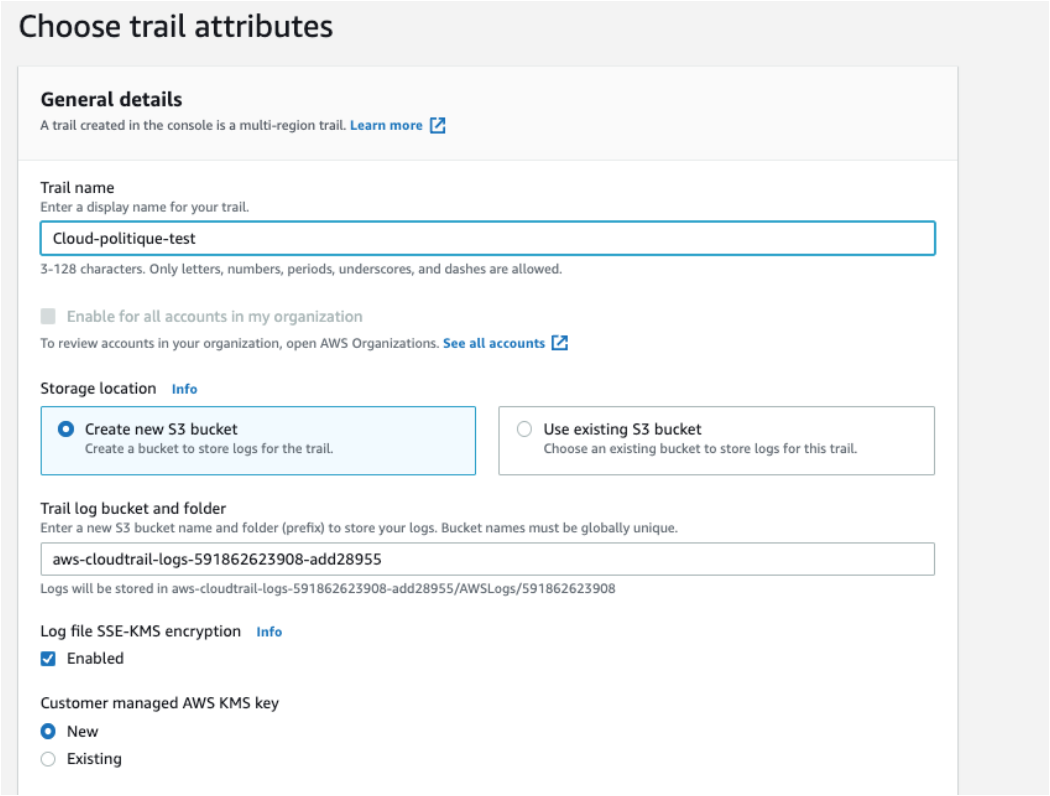
Configuration CloudTrail

- Nous pouvons ajouter une politique CloudTrail en cliquant sur create Trail et ensuite choisir les détails de la politique :

✓ Le nom.

✓ Le lieu du stockage des logs, chez AWS, on stocke les logs dans les buckets S3.

✓ Le chiffrement des logs.



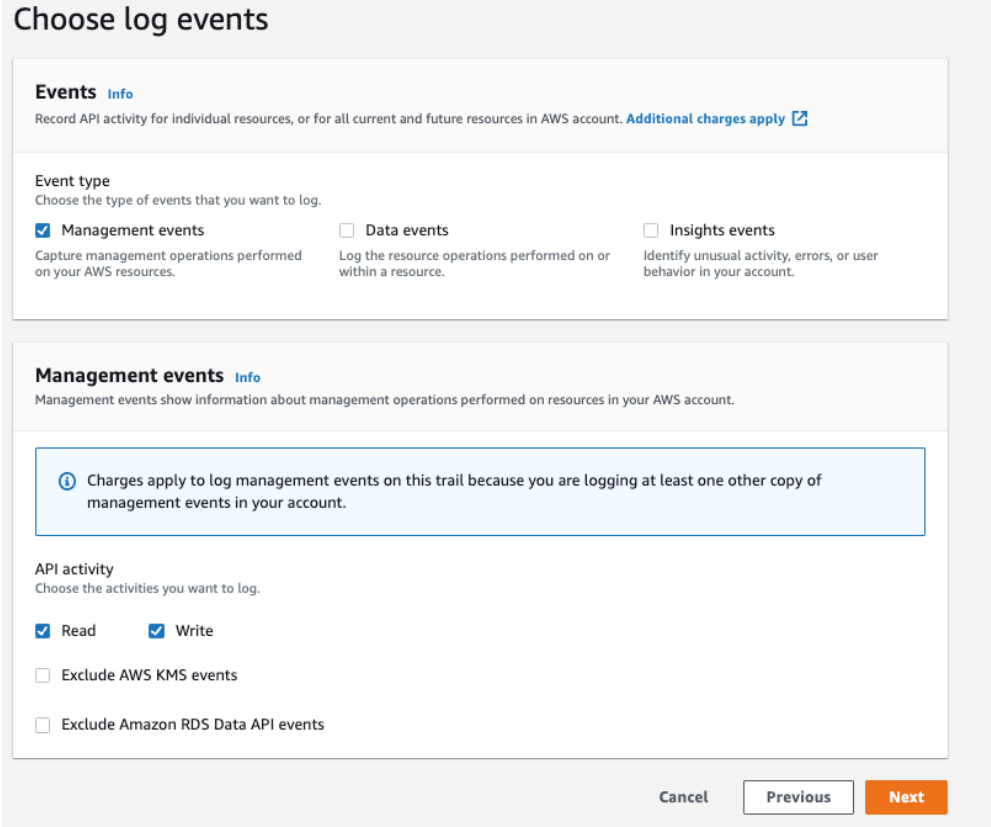
Configuration CloudTrail

- Dans la page suivante, nous devons choisir les types d'événements que nous souhaitons tracer :

✓ **Événement de Management :** logger les opérations de gestion effectuées sur vos ressources AWS
Nous pouvons préciser aussi quels types d'opérations (lecture, écriture, chiffrement, etc.)

✓ **Les événements sur les données :** logger les opérations de ressource effectuées sur ou dans une ressource.

✓ **De la reconnaissance sur les événements :** identifier les activités inhabituelles, les erreurs ou le comportement des utilisateurs dans votre compte.



PARTIE 4

Configuration CloudTrail

- Après une page de revue de la configuration, nous pouvons confirmer la création de la nouvelle politique :