Nmap + Nessus

Made By: Haroun Mohamed Akli

Objectifs du scan du réseau

- Découvrir les hôtes (les machines actives sur le réseau)
- Découvrir les ports (ouverts, fermés et filtrés) sur chaque hôte
- Reconnaitre le type de chaque hôte (ordinateur, routeur, ...etc)
- Reconnaitre le système d'exploitation s'exécutant sur chaque hôte
- Reconnaitre les applications et services s'exécutant sur chaque hôte ainsi que leurs versions

✔️Ces informations peuvent être utilisées plus tard pour la recherche de vulnérabilités dans les os, les services et les applications installés dans ces hôtes

SCAN du réseau

Découverte des hôtes

Identifier les machines actives en cherchant une réaction de leurs part

Plusieurs techniques sont utilisées

✔️**ICMP ECHO REQUEST (ping)** : un paquet de ICMP de type 8 (ping) est envoyé par le scanner. Si la cible est active, elle répond par un ICPM de type 0 (echo replay)

✔️**ICMP Time Stamp**: un paquet de ICMP de type 13 est envoyé par le scanner. Si la cible est active, elle répond par un ICPM de type 14 (l'heure actuelle)

✔️**ICMP Address Mask Request**: un paquet de ICMP de type 17 est envoyé par le scanner. Si la cible est active, elle répond par un ICPM de type 18 (Le masque de sous réseau)

✔️**TCP Ping**: Le scanner envoie un TCP Sync ou un TCP Ack . Si la cible est active, elle répond par un TCP Sync, ACK ou un TCP RST

✔️**UDP Ping**: Le scanner envoie un paquet UDP à un port de la cible. Si cette dernière est active et que le port est fermée, elle renvoie un paquet ICMP Port Unreacheable

SCAN du réseau

Détection de services et ports

- La connaissance des ports ouverts et services peut aider l'intrus à connaitre les vulnérabilités du système.
- Les services et ports peuvent être les points d'entrée dans le système
- Un port est dit ouvert si un service est actif et à l'écoute de ce port. Il est dit fermé si non. Il est dit filtré si un pare-feu bloque ce dernier
- L'intrus utilise le scan de port pour découvrir les ports ouverts

On peut classer les scans de port en trois catégories :

✔️**Connect scan** : tentative d'établir une connexion complète vers un port en envoyant un Syn, et en attendant la réponse qui peut être un Syn,Ack puis en terminant par ack.

✔️**Half scan** : A la réception d'un syn, ack, le scanneur ferme immédiatement la connexion avec le message RST

✔️**Scan furtif** : utilise d'autres bits du paquet TCP pour susciter une réponse quelconque de la cible

Détection du système d'exploitation (OS detection)

Déterminer le système d'exploitation utilisé par la cible

- **Détection active**

✔️Le scanner envoie des paquets de plusieurs types à la cible

✔️Les réponses sont analysées et comparées aux comportements connus des systèmes d'exploitation

- **Détection passive**

✔️N’engendre pas de trafic depuis le scanner

✔️Se contente d’analyser le trafic réseau

✔️Même principe que détection active

Nmap

NMAP (Network Mapper) NMAP est un outil de scan réseau gratuit distribué en licence libre

Il supporte plusieurs types de scan

Disponible en ligne de commande et en interface graphique

NMAP - Lancement

Ligne de commande

La syntaxe de base pour exécuter une commande Nmap est la suivante :

```
nmap [Scan Type] [Options] <target hosts>
```

- Les paramètres entre crochets `[ ]` sont **optionnels**.
- Si aucun paramètre n'est spécifié, Nmap utilise ses **paramètres par défaut**.

Paramètres par défaut de Nmap :

1. **Recherche des ports ouverts usuels** (1000 ports les plus connus).
2. **Utilisation du message TCP SYN** pour tenter de se connecter aux ports ouverts (SYN scan).

Exemple simple :

Commande :

```
nmap 192.168.0.25
```

- Cela scanne la machine cible `192.168.0.25` avec les **options par défaut**.

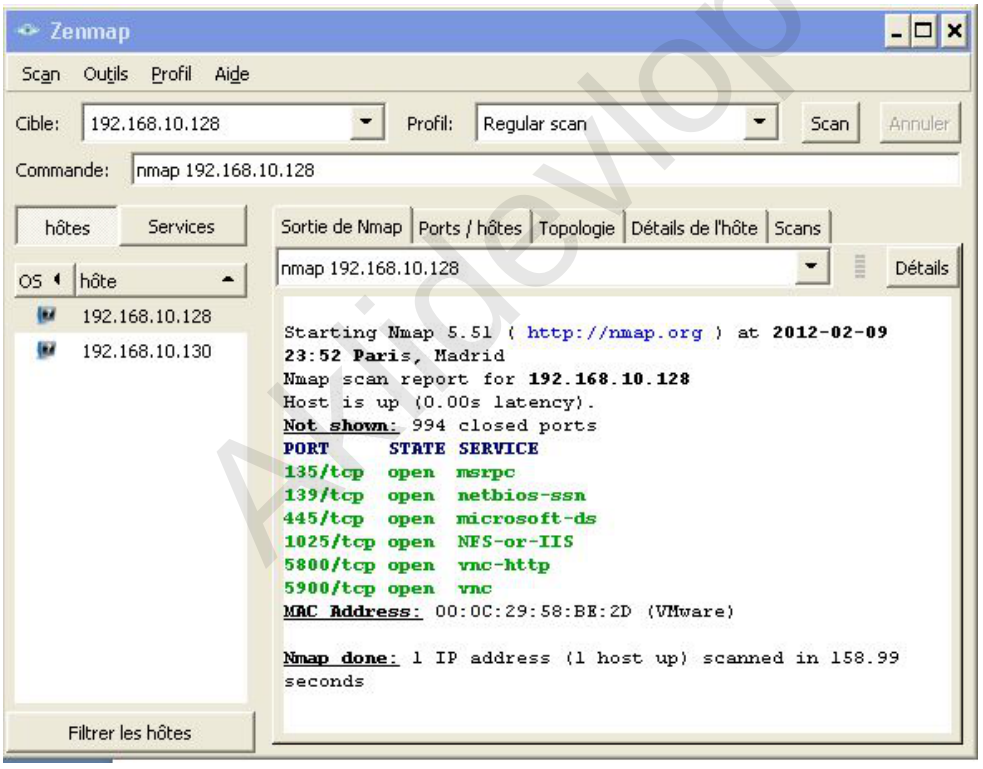
Sortie de Nmap :

1. **Ports ouverts** :
   - Si un port est **ouvert**, la machine cible renvoie un paquet **SYN, ACK**.
2. **Ports fermés** :
   - Si un port est **fermé**, la machine cible renvoie un paquet **RST**.
3. **Ports filtrés (bloqués)** :
   - Si un port est **filtré** (bloqué par un pare-feu), aucune réponse n'est renvoyée.

```
Starting Nmap 7.93 ( https://nmap.org ) at 2024-12-11 12:34 UTC
Nmap scan report for 192.168.0.10
Host is up (0.0030s latency).
Not shown: 996 closed ports
PORT     STATE    SERVICE
22/tcp   open     ssh
80/tcp   open     http
443/tcp  open     https
3306/tcp open     mysql
Nmap done: 1 IP address (1 host up) scanned in 1.20 seconds
```

•Si le port est bloqué par le pare-feu (filtré), aucune réponse

Interface graphique (ex: ZenMAP ous Windows)



NMAP-Découverte des hôtes

NMAP utilise une variétés de techniques pour déterminer si un hôte est actif.

1. Ping Scan (`sP`)

Commande :

```
nmap -sP 192.168.0.0/24
```

Options utilisées :

- `sP` : Effectue un scan de type **Ping Scan**, qui consiste uniquement à envoyer des paquets pour déterminer si les hôtes sont actifs sur un réseau.
- `192.168.0.0/24` : Spécifie la plage d'adresses IP à scanner (ici, le réseau complet avec un masque de sous-réseau de 24 bits).

Fonctionnement :

1. Envoie des paquets ICMP (ping) à chaque adresse de la plage spécifiée.
2. Affiche les hôtes actifs avec leurs adresses **IP** et parfois leurs adresses **MAC**.

Limitations :

- Certains pare-feux bloquent les paquets ICMP, empêchant Nmap de détecter les hôtes actifs.

---

2. TCP SYN Ping (`PS`)

Commande :

```
nmap -PS 192.168.0.0/24
```

Options utilisées :

- `PS` : Effectue un **TCP SYN Ping**. Envoie des paquets TCP avec le drapeau **SYN** à des ports spécifiques pour déterminer si les hôtes répondent.
- `192.168.0.0/24` : Plage d'adresses IP à scanner.

Fonctionnement :

1. Envoie des paquets SYN à des **ports usuels** (par défaut, les ports 80, 443, etc.).
2. Si un hôte répond avec un **SYN/ACK**, il est considéré comme actif.
3. Si un port est fermé, l'hôte répond avec un paquet **RST**, ce qui prouve également qu'il est actif.

Scan des Ports TCP

Commande :

```
nmap -sS 192.168.10.131
```

Options utilisées :

- `sS` : Effectue un **TCP SYN Scan**. Cette méthode est rapide et furtive, souvent appelée **stealth scan**.

Fonctionnement :

1. Envoie un paquet **TCP SYN** aux **ports usuels** de la machine cible (par défaut, les 1000 ports les plus courants).

2. Interprète la réponse de la cible pour déterminer l'état du port :
    - Si la cible renvoie un **SYN/ACK**, cela indique que le port est **ouvert**. Nmap termine la connexion en envoyant un **RST**, ce qui évite de la maintenir ouverte.
    - Si la cible renvoie un **RST**, le port est **fermé**.
    - Si aucune réponse n'est reçue, le port est **filtré** (bloqué par un pare-feu).

Avantages :

- Rapide et efficace.
- Furtif : il ne complète pas la connexion TCP, ce qui réduit les chances d'être enregistré dans les journaux du serveur cible.

Scan des Ports UDP

Commande :

```
nmap -sU 192.168.10.123
```

Options utilisées :

- `sU` : Effectue un **UDP Scan**. Cette méthode explore les ports UDP pour identifier les services actifs.

Fonctionnement :

1. Envoie un paquet **UDP** à l'application cible sur chaque port.
2. Analyse la réponse pour déterminer l'état du port :
    - Si le port est **fermé**, la cible peut renvoyer un message ICMP **Port unreachable**.
    - Si aucune réponse n'est reçue, cela peut signifier :
        - Le port est **filtré** (bloqué par un pare-feu).
        - Le port est **ouvert**, mais l'application cible ne répond pas aux paquets envoyés.

Caractéristiques :

- Plus lent que le scan TCP en raison de la nature du protocole UDP (sans connexion).
- Moins fiable : l'absence de réponse peut prêter à confusion entre un port filtré ou un port ouvert sans réponse.

comparaison des quatre scans :

Type de Scan	Commande	Protocole	Fonctionnement	Avantages	Inconvénients
Ping Scan	`nmap -sP`	ICMP	Envoie des paquets ICMP (Ping) pour	Rapide, simple, non intrusif.	Échec si les pare-feux

			détecter les hôtes actifs sur un réseau.		bloquent les ICMP.
TCP SYN Ping	`nmap -PS`	TCP	Envoie des paquets TCP SYN à des ports spécifiques pour identifier les hôtes actifs.	Contourne les restrictions ICMP ; efficace si au moins un port répond.	Détectable par les IDS ; peut être bloqué par des pare-feux.
TCP SYN Scan	`nmap -sS`	TCP	Envoie des paquets TCP SYN pour scanner les ports ouverts, fermés ou filtrés sans établir une connexion complète.	Rapide, furtif (stealth scan), ne génère pas de traces dans les logs serveur.	Peut être bloqué par des pare-feux avancés.
UDP Scan	`nmap -sU`	UDP	Envoie des paquets UDP aux ports pour identifier les services actifs ; analyse les réponses ou leur absence.	Indispensable pour identifier les services UDP.	Lent ; absence de réponse peut être ambiguë entre un port filtré ou ouvert.

Méthodes avancées de scan avec Nmap

Nmap offre des techniques avancées pour :

- Accélérer la détection de ports.
- Contourner les pare-feux ou les systèmes de détection d'intrusion (IDS).Ces méthodes manipulent les drapeaux TCP (flags) autres que **SYN** et **ACK** comme **FIN**, **PUSH**, et **URG**.

⚠ **Limitation** : Ces méthodes supposent que la cible respecte les normes TCP définies par la RFC. Si ce n'est pas le cas, les résultats peuvent être incorrects.

Méthodes par manipulation de flags TCP

Méthode	Commande	Description	Drapeaux positionnés
TCP SYN/ACK Scan	`nmap -sM 192.168.10.131`	Positionne les drapeaux **SYN** et **ACK** pour tester les ports.	SYN, ACK
TCP Xmas Scan	`nmap -sX 192.168.10.131`	Positionne les drapeaux **FIN**, **PUSH**, et **URG**, rendant le paquet "lumineux" comme un sapin de Noël.	FIN, PUSH, URG
TCP ACK Scan	`nmap -sA 192.168.10.131`	Utilise uniquement le drapeau **ACK** pour déterminer les règles du pare-feu ou l'état	ACK

		des ports.	
TCP FIN Scan	`nmap -sF 192.168.10.131`	Envoie un paquet avec uniquement le drapeau **FIN** positionné.	FIN
TCP Null Scan	`nmap -sN 192.168.10.131`	N'envoie aucun drapeau. Permet d'identifier des ports ouverts si la cible répond avec un **RST**.	Aucun flag

Idle Scan (Scan par hôte zombie)

Commande :

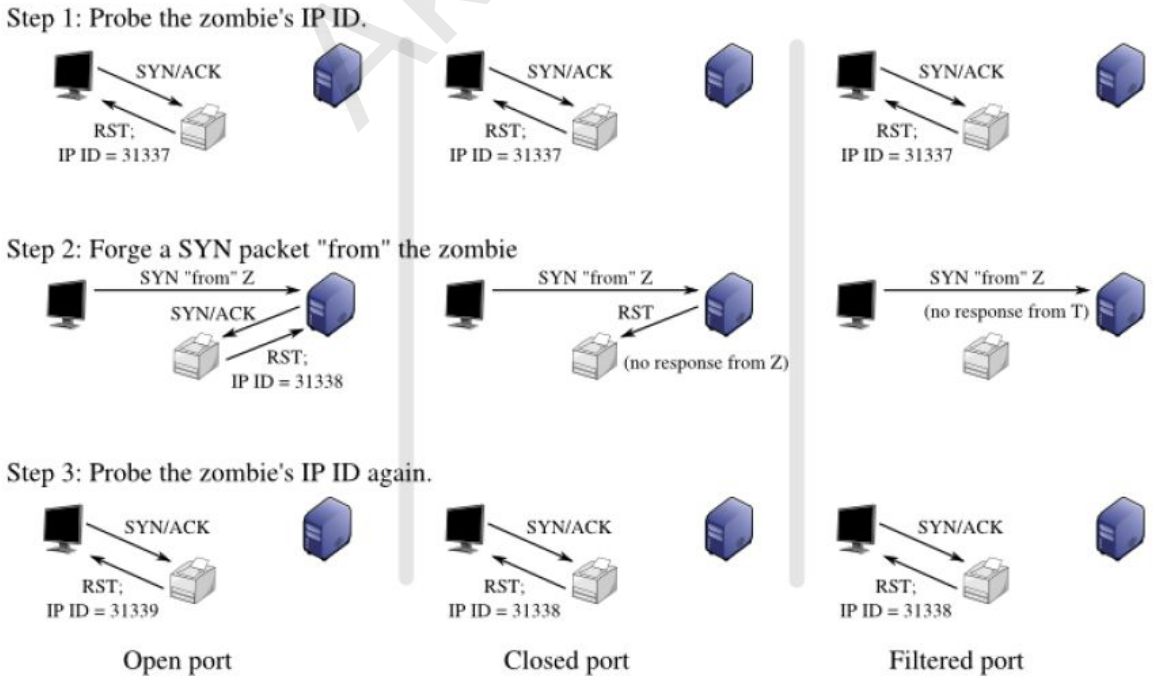
```
nmap -sI [Zombie_IP] [Target_IP]
```

Exemple :

```
nmap -sI 192.168.10.128 192.168.10.131
```

Fonctionnement :

- **Objectif :** Cacher l'origine du scan en utilisant une machine intermédiaire (zombie).
- Le zombie envoie des paquets à la victime, et la réponse est interprétée par le scanner.
- Nmap calcule la différence dans les identifiants de paquets IP (IPID) pour déduire l'état du port cible :
  - **IPID + 2** : Le port est **ouvert**.
  - **IPID + 1** : Le port est **fermé** ou **filtré**.



Avantages :

- Très furtif : l'origine du scan est masquée.
- Utile pour contourner les systèmes de détection d'intrusion.

Inconvénients :

- Nécessite un zombie avec un comportement prévisible sur l’incrémentation de l’IPID.
- Lent, car il dépend des réponses du zombie.

Comparaison des méthodes

Méthode	Furtivité	Vitesse	Utilisation principale
TCP SYN/ACK Scan	Moyenne	Rapide	Détection générale des ports ouverts.
TCP Xmas Scan	Moyenne	Moyenne	Contournement des pare-feux ; identification furtive.
TCP ACK Scan	Moyenne	Moyenne	Identifier les règles de pare-feux sans tester les ports.
TCP FIN Scan	Moyenne	Moyenne	Détection furtive des ports ouverts.
TCP Null Scan	Moyenne	Moyenne	Test des ports ouverts sans signal évident.
Idle Scan	Très élevée	Lente	Masquer l’origine du scan pour des cibles sensibles.

Détection du système d’exploitation

Commande :

```
nmap -O [Adresse_IP_Cible]
```

Exemple :

```
nmap -O 192.168.10.128
```

Fonctionnement

- Nmap utilise une méthode d'analyse des réponses aux paquets envoyés à la machine cible.
- Les réponses obtenues sont comparées à une base de données d’implémentations TCP/IP connues.
- Grâce à ces comparaisons, Nmap identifie :
  - Le système d’exploitation probable.
  - La version approximative.

Informations récupérées

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-12-11 14:05 UTC
Nmap scan report for 192.168.10.128
Host is up (0.0025s latency).
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
443/tcp   open     https
3306/tcp  open     mysql
8080/tcp  filtered http-proxy

Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.4 - 5.11
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.22 seconds
```

✔️ **Système d'exploitation** : Par exemple, Windows, Linux, macOS, etc.

✔️ **Nom du vendeur** : Microsoft, Sun Microsystems, Apple, etc.

✔️ **Version** : Version approximative du système d'exploitation.

✔️ **Type de machine** : Indique si la cible est un ordinateur, un routeur, une imprimante, ou autre.

⚠️ **Limite** :

- Nmap ne détecte pas toujours la version exacte du système d'exploitation.
- Dans ces cas, il fournit des **probabilités** sur les systèmes possibles.

Avantages

- **Rapide** : Permet de récolter des informations sur une machine cible en quelques secondes.
- **Précision élevée** pour des systèmes d'exploitation courants.
- Utile pour évaluer l'environnement réseau.

Inconvénients

- Moins efficace sur les machines configurées pour limiter les réponses aux scans.
- Peut être bloqué ou détecté par des systèmes de sécurité comme les IDS/IPS.

Détection des versions des applications et services

Commande :

```
nmap -sV [Adresse_IP_Cible]
```

Exemple :

```
nmap -sV 192.168.10.10
```

Fonctionnement

- Cette option interroge les ports ouverts de la machine cible pour confirmer les services qu'ils hébergent.
- Elle recueille des informations sur les applications ou services associés aux ports détectés comme ouverts.

Informations récupérées

✔️ **Nom du service/application** associé au port (si disponible).

✔️ **Numéro de version** du service/application (si disponible).

✔️ **Nom de la machine** (*hostname*).

✔️ **Type de la machine** : ordinateur, routeur, imprimante, etc.

✔️ **Famille du système d'exploitation** : Windows, Linux, macOS, etc.

✔️ **Informations diverses** : version du noyau, numéro de série matériel, etc.

Avantages

- **Précision accrue** : Permet de valider la nature réelle des services derrière les ports ouverts.
- **Diagnostic des vulnérabilités** : La détection des versions aide à repérer d'éventuelles failles de sécurité connues dans les logiciels ou services utilisés.

Limites

- Peut être **bloqué ou limité** par des pare-feux ou systèmes de sécurité.
- Peut générer des **alertes dans les systèmes IDS/IPS**.

Exemple de sortie :

Voici une sortie standard après exécution de la commande :

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-12-11 14:20 UTC
Nmap scan report for 192.168.10.10
Host is up (0.0031s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; p
```

```
rotocol 2.0)
80/tcp   open  http     Apache httpd 2.4.41 ((Ubuntu))
443/tcp  open  https    nginx 1.18.0
3306/tcp open  mysql    MySQL 8.0.26-0ubuntu0.20.04.3
Service Info: Host: example-host.local; OS: Linux; CPE: cpe:/o:linux:lin
ux_kernel

Nmap done: 1 IP address (1 host up) scanned in 3.57 seconds
```

Interprétation des résultats :

1. **Détails des services :**
   - **22/tcp** : OpenSSH 8.2 (protocole 2.0, basé sur Ubuntu Linux).
   - **80/tcp** : Apache HTTP Server, version 2.4.41.
   - **443/tcp** : nginx version 1.18.0.
   - **3306/tcp** : MySQL version 8.0.26.
2. **Informations générales :**
   - **Nom de l'hôte** : `example-host.local`.
   - **Système d'exploitation** : Linux.

Détection des vulnérabilités connues

Commande :

```
nmap --script vuln [Adresse_IP_Cible]
```

Exemple :

```
nmap --script vuln 192.168.10.10
```

Fonctionnement

- Cette option utilise les scripts préconçus de Nmap pour rechercher des vulnérabilités sur la machine cible.
- Ces scripts effectuent des tests automatisés basés sur des signatures connues pour identifier les failles de sécurité sur les services ou applications.

Informations récupérées

✔️ **Code de la vulnérabilité** détectée.

✔️ **Risque** associé à la vulnérabilité (faible, moyen, élevé).

✔️ **Liens web** pour des informations supplémentaires, souvent des rapports ou des documents de vulnérabilité disponibles sur des sites comme Exploit-DB ou le site de l'éditeur.

Exemple de sortie :

Voici une sortie standard après exécution de la commande :

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-12-11 14:45 UTC
Nmap scan report for 192.168.10.10
Host is up (0.0031s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; p
rotocol 2.0)
80/tcp   open  http     Apache httpd 2.4.41 ((Ubuntu))
443/tcp  open  https    nginx 1.18.0
3306/tcp open  mysql    MySQL 8.0.26-0ubuntu0.20.04.3
|_ssl-date: 2024-12-11T14:45:00+00:00; +0s from scanner time.
|_ssh-hostkey:
|   2048 24:b6:1e:cc:ce:1d:4f:b3:8f:91:b4:cc:17:5a:16:90 (RSA)
|   256 a0:57:db:07:1d:9b:3b:2c:72:a0:89:44:ba:57:18:bf (ECDSA)
|_  256 a0:57:db:07:1d:9b:3b:2c:72:a0:89:44:ba:57:18:bf (ED25519)
| http-auth-bypass:
|   VULNERABLE:
|   Description: A path traversal vulnerability in Apache HTTPD versions
prior to 2.4.48 can lead to unauthorized access to files.
|   Solution: Upgrade to version 2.4.48 or later.
|   Port: 80/tcp
|   ID: CVE-2020-13949
|_ssl-heartbleed:
|   VULNERABLE:
|   Description: The OpenSSL heartbeat extension is enabled. This can be
exploited to leak memory from the server.
|   Solution: Upgrade OpenSSL to version 1.0.1f or later.
|   Port: 443/tcp
|   ID: CVE-2014-0160
|_mysql-empty-password:
|   VULNERABLE:
|   Description: The MySQL server allows logins without a password.
|   Solution: Set a strong password for the MySQL root user.
|   Port: 3306/tcp
|   ID: CVE-2017-3307
Nmap done: 1 IP address (1 host up) scanned in 3.57 seconds
```


Interprétation des résultats :

1. **http-auth-bypass (CVE-2020-13949)** :

- **Risque** : Élevé
- **Description** : Vulnérabilité de dépassement de chemin dans Apache HTTPD.
- **Solution** : Mettre à jour vers Apache HTTPD version 2.4.48 ou ultérieure.
- **Port** : 80/tcp

2. **ssl-heartbleed (CVE-2014-0160)** :
   - **Risque** : Élevé
   - **Description** : Le heartbeat extension dans OpenSSL est activé, permettant une fuite de mémoire.
   - **Solution** : Mettre à jour OpenSSL à la version 1.0.1f ou plus récente.
   - **Port** : 443/tcp
3. **mysql-empty-password (CVE-2017-3307)** :
   - **Risque** : Moyen
   - **Description** : Le serveur MySQL permet les connexions sans mot de passe.
   - **Solution** : Définir un mot de passe sécurisé pour l'utilisateur root MySQL.
   - **Port** : 3306/tcp

Points importants :

- **CVE (Common Vulnerabilities and Exposures)** : Les identifiants CVE permettent d'identifier de manière unique chaque vulnérabilité.
- **Solutions** : Pour chaque vulnérabilité, une solution est fournie afin de corriger ou d'atténuer le risque associé.
- **Interprétation des risques** : Les CVE indiquent un niveau de gravité pour chaque vulnérabilité, ce qui aide à prioriser les actions de remédiation.

L'audit de sécurité du réseau

L'audit de sécurité du réseau est une étape cruciale pour protéger efficacement un environnement informatique. Il permet d'identifier, de classer et de remédier aux vulnérabilités existantes, assurant ainsi la sécurité et la continuité des opérations. Voici un processus pour effectuer un audit de sécurité du réseau :

Étapes d'un audit de sécurité du réseau :

1. **Identification des vulnérabilités** :
   - **Services vulnérables ou inutiles actifs** : Identifier les services non utilisés sur les systèmes (par exemple, le partage de fichiers inutilisé, les services de gestion à distance, etc.).
   - **Erreurs de configuration** : Détecter les configurations incorrectes qui pourraient exposer des ressources critiques (par exemple, des ports ouverts incorrectement configurés).

- **Patchs de sécurité non installés** : Rechercher les correctifs de sécurité manquants pour les systèmes d'exploitation et les applications.
- **Mots de passe par défaut non changés** : Repérer les équipements (routeurs, switches, systèmes) avec des mots de passe d'usine non modifiés.
- **Utilisation de mots de passe faibles** : Analyser les pratiques de création de mots de passe pour identifier les mots de passe trop simples ou facilement devinables.

2. **Classement des vulnérabilités en niveaux de gravité** :
   - **Évaluation des risques** : Chaque vulnérabilité doit être classée selon son niveau de gravité, basé sur des critères comme l'impact potentiel, la probabilité d'exploitation, et les conséquences possibles sur la sécurité.
   - **Priorisation des remédiations** : Prioriser les vulnérabilités par ordre d'importance. Par exemple, une vulnérabilité critique comme un service web non sécurisé serait priorisée par rapport à une erreur mineure de configuration.
3. **Proposition de solutions pour renforcer la sécurité** :
   - **Installation des correctifs** : Mettre à jour les systèmes avec les correctifs disponibles pour les vulnérabilités identifiées.
   - **Renforcement des configurations** : Réaliser des ajustements de configuration, tels que la désactivation des services inutiles, le resserrage des paramètres de pare-feu et la réduction des droits d'accès.
   - **Changement de mots de passe** : Modifier les mots de passe par défaut et instaurer des mots de passe forts pour tous les comptes.
   - **Sécurisation des accès** : Implémenter des politiques de sécurité telles que l'authentification multifactorielle, la gestion des mots de passe, et la surveillance continue pour détecter les comportements anormaux.
   - **Formation et sensibilisation** : Former les utilisateurs sur les meilleures pratiques de sécurité pour minimiser les erreurs humaines, comme l'ouverture de pièces jointes non sécurisées ou l'accès à des sites Web douteux.

Exemple d'audit avec Nmap :

Utiliser Nmap pour auditer la sécurité réseau permet d'identifier rapidement les points faibles. Par exemple :

- **Scanner les ports** pour détecter les services ouverts.
- **Analyser les vulnérabilités** pour identifier les failles exploitables sur les systèmes.
- **Détecter les versions d'applications** pour identifier les versions obsolètes susceptibles d'être vulnérables.
- **Tester les politiques de filtrage** pour vérifier la sécurité des flux de données.

Conclusion :

Un audit de sécurité bien réalisé permet d'éclairer sur les risques potentiels et de guider les actions nécessaires pour renforcer la sécurité du réseau. Il est essentiel d'effectuer

régulièrement ces audits pour maintenir une posture de sécurité robuste et proactive contre les menaces.

Audit de sécurité du réseau Nessus

Nessus est un outil puissant d'audit de sécurité utilisé pour évaluer et analyser les réseaux informatiques en identifiant les vulnérabilités. Il offre une gamme de fonctionnalités qui permettent une évaluation complète de la sécurité d'un réseau, mais il ne fournit pas de solutions directes pour corriger ces vulnérabilités. Voici un aperçu détaillé de ce que Nessus peut faire et ne peut pas faire :

Ce que Nessus fait :

1. **Identification des vulnérabilités connues** :
   - **Nessus scanne les hôtes** du réseau pour rechercher des vulnérabilités déjà connues comme des failles dans les logiciels, des services ouverts mal sécurisés, des erreurs de configuration, et des signatures de logiciels malveillants.
   - **Détection de vulnérabilités potentielles** non connues par rapport aux bases de données de vulnérabilités actuelles.
2. **Analyse des erreurs de configuration** :
   - **Scanner les machines du réseau** pour détecter les configurations inadéquates qui pourraient rendre un système vulnérable.
   - **Identifier les patchs non installés** qui sont critiques pour la sécurité, ce qui peut prévenir des exploits malveillants.
3. **Réalisation de tests de pénétration** :
   - **Simuler les actions d'un attaquant** en testant les vulnérabilités des systèmes. Cela permet de vérifier si des attaques telles que des attaques par déni de service, des vulnérabilités des serveurs web, ou des attaques de réseaux sans fil sont possibles.
4. **Rapport bien documenté** :
   - **Fournir un rapport exhaustif** à la fin de l'analyse, avec une liste détaillée des vulnérabilités détectées, des conseils sur la manière de les corriger et des recommandations sur les meilleures pratiques pour renforcer la sécurité.

Ce que Nessus ne fait pas :

- **Il n'est pas un pare-feu** : Nessus ne bloque pas les tentatives d'intrusion ni ne surveille en temps réel les activités malveillantes. Il se contente d'identifier les vulnérabilités existantes.
- **Il ne peut pas supprimer le code malicieux** : Une fois qu'un code malveillant est détecté, Nessus ne fournit pas de méthode pour le supprimer ou nettoyer le système.
- **Il ne bloque pas les intrusions** : Nessus ne dispose pas de mécanismes pour bloquer ou interdire l'accès aux attaquants potentiels une fois les vulnérabilités identifiées.

- **Il ne peut pas appliquer ou télécharger les correctifs** : Nessus détecte les correctifs nécessaires, mais ne les installe pas. Les administrateurs doivent appliquer manuellement les correctifs sur les systèmes.

Présentation de Nessus

Lancement de Nessus sur le serveur (machine où Nessus est installé) :

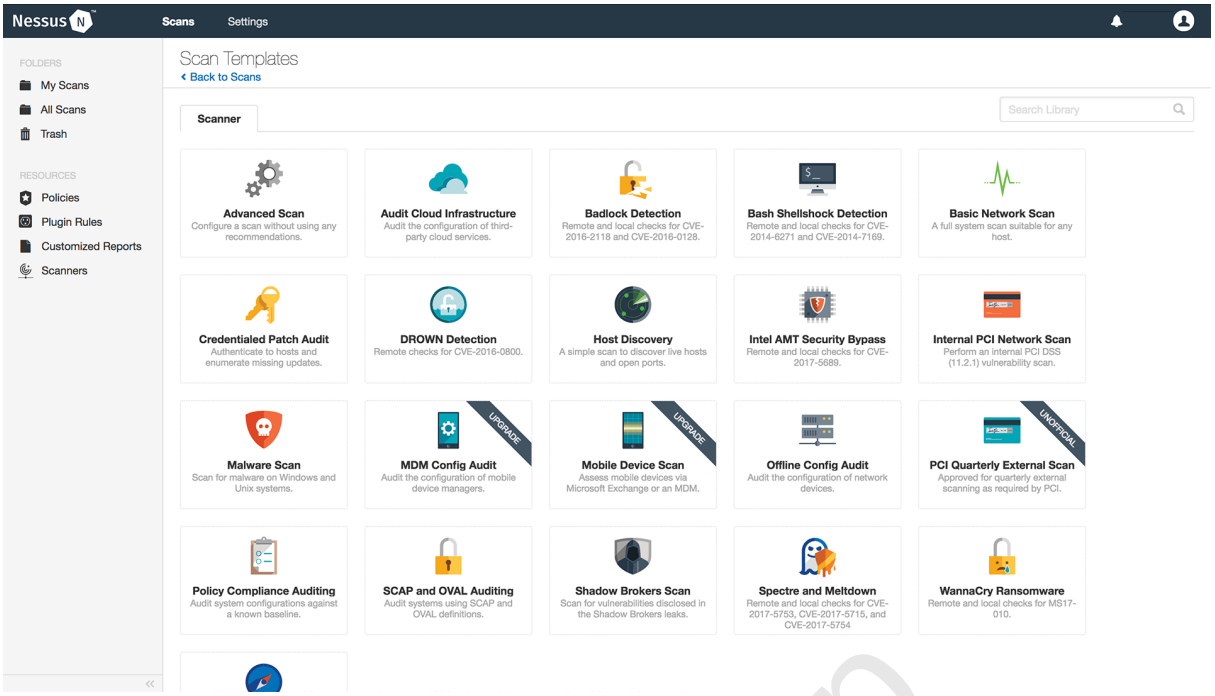
1. **Sur une machine serveur sous Linux** :
   - Ouvrez un terminal.
   - Pour lancer le service Nessus, utilisez l'une des commandes suivantes :
     - `/etc/init.d/nessusd start`
     - ou
     - `systemctl start nessusd.service`
   - Cela démarre le service Nessus sur le serveur.

Accès à Nessus depuis la machine cliente :

1. **Sur la machine cliente** :
   - Ouvrez un navigateur web.
   - Entrez l'adresse suivante dans la barre d'URL pour accéder à l'interface web de Nessus :
     - `https://ip_serveur_nessus:8834`
   - Remplacez `ip_serveur_nessus` par l'adresse IP du serveur où Nessus est installé.
   - Une fois sur la page de connexion, saisissez les informations de votre compte Nessus (nom d'utilisateur et mot de passe) pour vous connecter.
   - Après la connexion, vous accédez à l'interface graphique de Nessus.

Utilisation de l'interface graphique de Nessus :

- **Configurer une politique d'analyse** : Vous pouvez définir une politique d'analyse qui inclut des règles de scan spécifiques, des plages d'adresses à analyser, et des options avancées comme les scans TCP, UDP, ou les scans d'applications spécifiques.



- **Lancer une analyse** : Sélectionnez une machine locale ou distante et lancez l'analyse. Nessus exécutera le scan en fonction de la politique définie.
- **Consulter le rapport d'analyse** : Après l'analyse, vous pouvez consulter le rapport d'analyse détaillé. Le rapport inclut les vulnérabilités détectées, les conseils pour les corriger, et d'autres informations pertinentes pour renforcer la sécurité du réseau ou des machines ciblées.