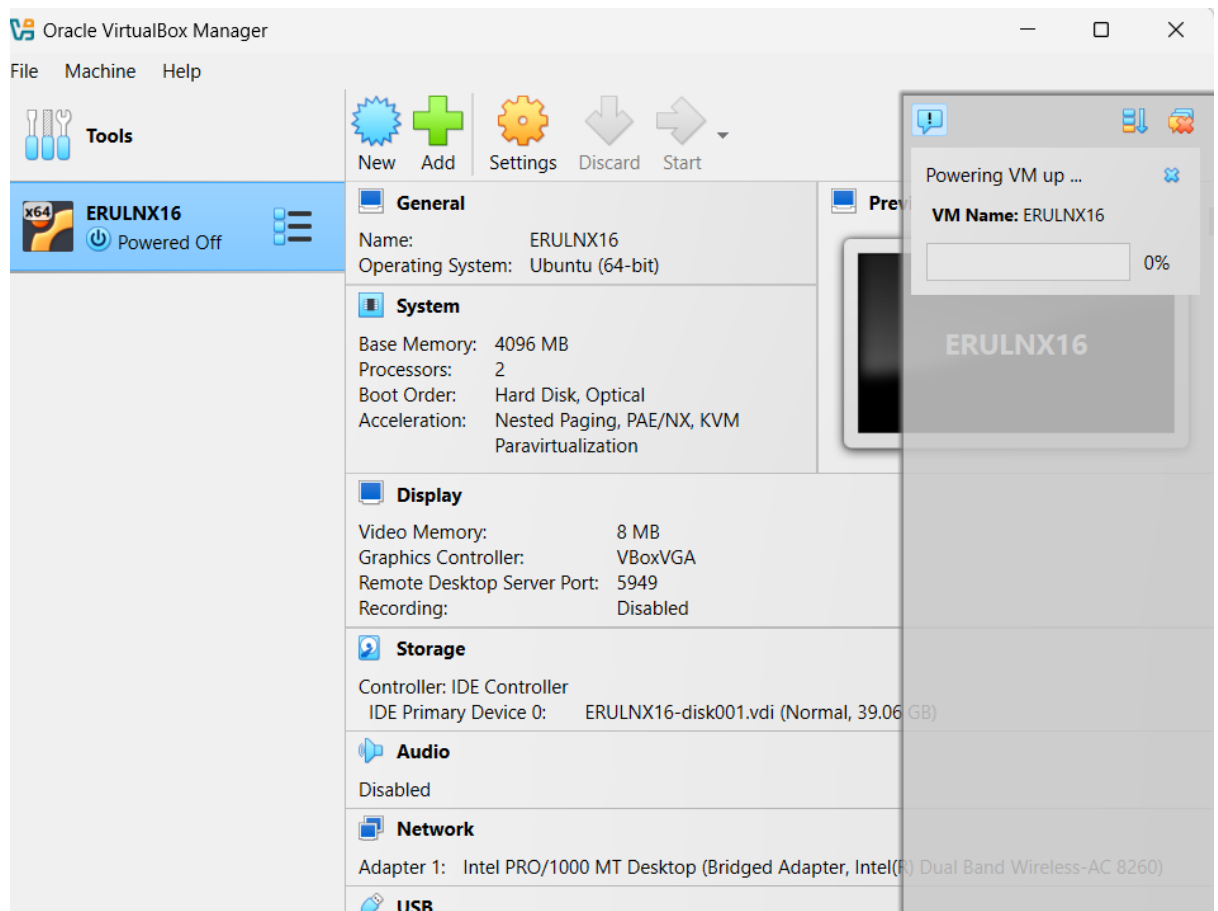


Introduction

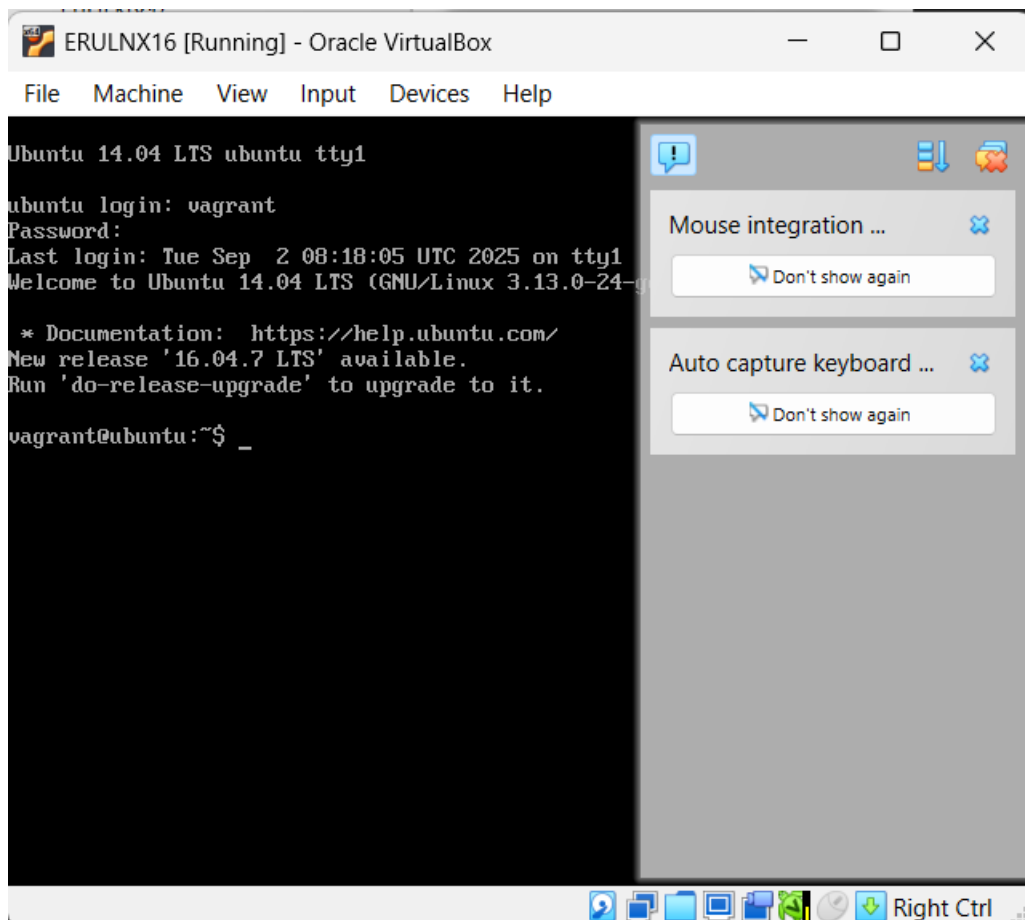
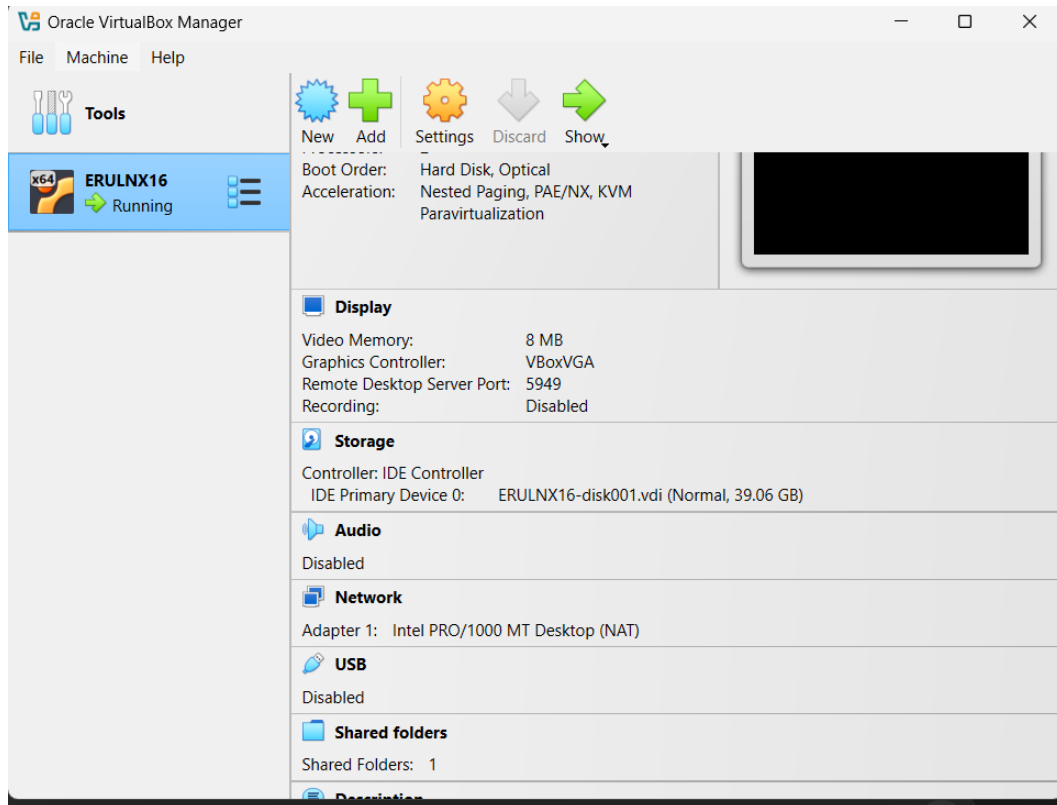
This report documents the process of assessing a virtual machine provided as part of Task 4. The goal was to identify potential vulnerabilities, explore services, and record findings in a professional format. The assessment was conducted in a controlled environment using VirtualBox.

Environment Setup

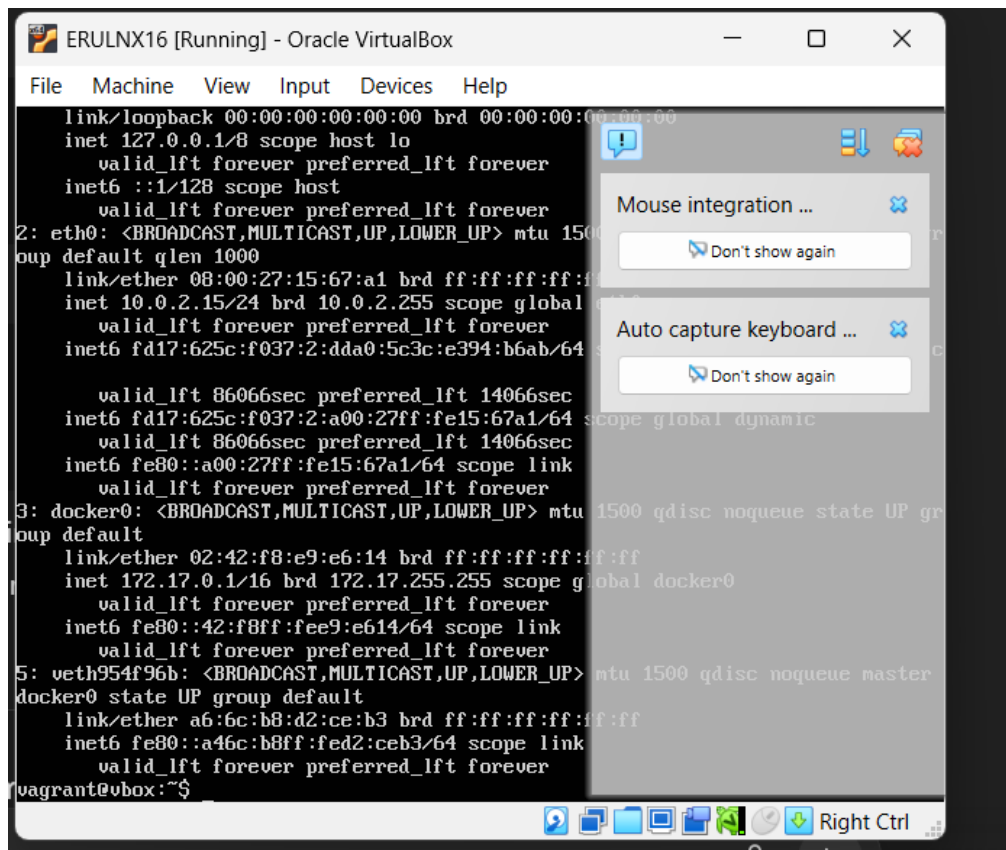
1. VM Host: VirtualBox



2. VM File: Provided OVA file

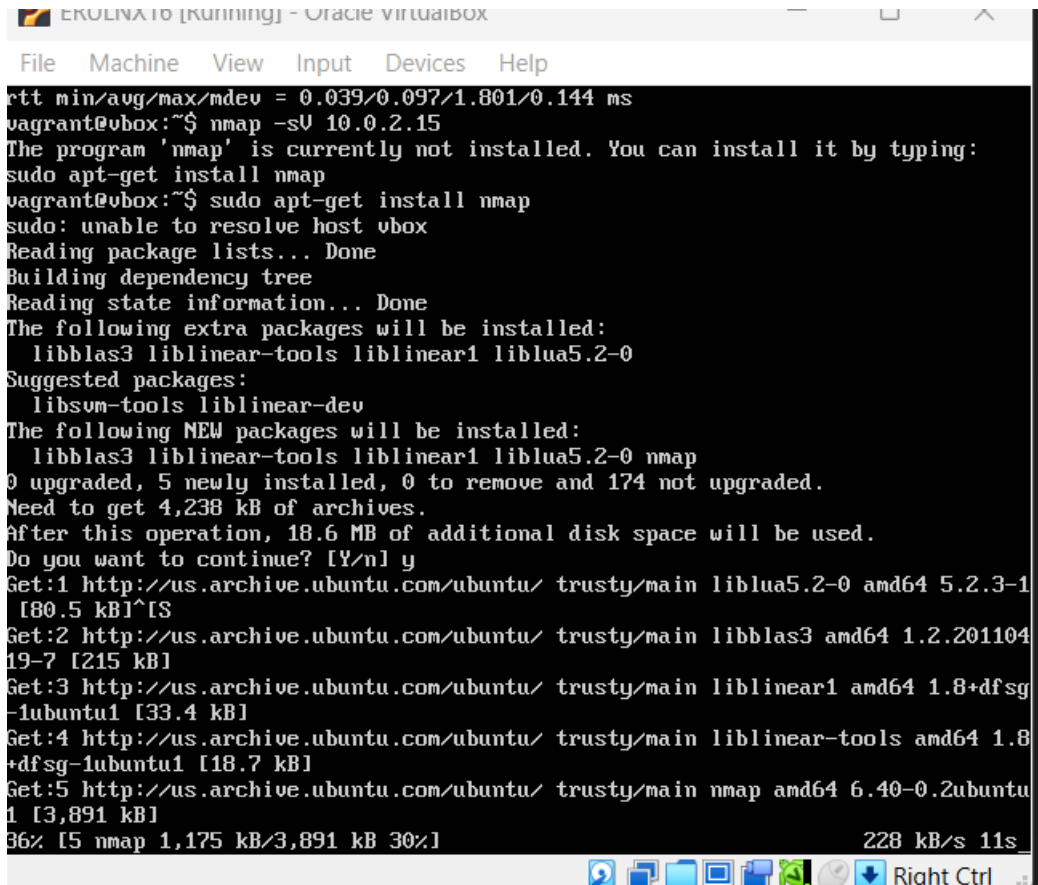


3. VM IP Address: 10.0.2.15



```
ERULNX16 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
    link/ether 08:00:27:15:67:a1 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic
        valid_lft forever preferred_lft forever
    inet6 fd17:625c:f037:2:dda0:5c3c:e394:b6ab/64 scope global dynamic
        valid_lft 86066sec preferred_lft 14066sec
    inet6 fd17:625c:f037:2:a00:27ff:fe15:67a1/64 scope global dynamic
        valid_lft 86066sec preferred_lft 14066sec
    inet6 fe80::a00:27ff:fe15:67a1/64 scope link
        valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:f8:e9:e6:14 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
    inet6 fe80::42:f8ff:fee9:e614/64 scope link
        valid_lft forever preferred_lft forever
5: veth954f96b: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
    link/ether a6:6c:b8:d2:ce:b3 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::a46c:b8ff:fed2:ceb3/64 scope link
        valid_lft forever preferred_lft forever
vagrant@ubox:~$
```



```
ERULNX16 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

rtt min/avg/max/mdev = 0.039/0.097/1.801/0.144 ms
vagrant@ubox:~$ nmap -sU 10.0.2.15
The program 'nmap' is currently not installed. You can install it by typing:
sudo apt-get install nmap
vagrant@ubox:~$ sudo apt-get install nmap
sudo: unable to resolve host vbox
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libblas3 liblinear-tools liblinear1 liblua5.2-0
Suggested packages:
  libsvm-tools liblinear-dev
The following NEW packages will be installed:
  libblas3 liblinear-tools liblinear1 liblua5.2-0 nmap
0 upgraded, 5 newly installed, 0 to remove and 174 not upgraded.
Need to get 4,238 kB of archives.
After this operation, 18.6 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu/ trusty/main liblua5.2-0 amd64 5.2.3-1 [80.5 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu/ trusty/main libblas3 amd64 1.2.20110419-7 [215 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu/ trusty/main liblinear1 amd64 1.8+dfsg-1ubuntu1 [33.4 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu/ trusty/main liblinear-tools amd64 1.8+dfsg-1ubuntu1 [18.7 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu/ trusty/main nmap amd64 6.40-0.2ubuntu1 [3,891 kB]
36% [5 nmap 1,175 kB/3,891 kB 30%] 228 kB/s 11s
```

```
ERULNX16 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Nmap scan report for ubuntu (10.0.2.15)
Host is up (0.00027s latency).
Not shown: 65520 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
111/tcp   open  rpcbind      2-4 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: UBUNTU)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: UBUNTU)
631/tcp   open  ipp          CUPS 1.7
3306/tcp  open  mysql        MySQL (unauthorized)
3500/tcp  open  http         WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
6667/tcp  open  irc          Unreal ircd (Admin email admin@TestIRC.net)
6697/tcp  open  irc          Unreal ircd (Admin email admin@TestIRC.net)
8067/tcp  open  irc          Unreal ircd (Admin email admin@TestIRC.net)
8080/tcp  open  http         Jetty 8.1.7.v20120910
45559/tcp open  unknown
51378/tcp open  status      1 (RPC #100024)
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at http://www.insecure.org/cgi-bin/servi
cefp-submit.cgi :
SF-Port22-TCP:V=6.40%I=7%D=9/2%Time=68B6A999%P=x86_64-pc-linux-gnu%r(NULL,
SF:2C,"SSH-2\0-OpenSSH_6\6\1p1\0x20Ubuntu-2ubuntu2\13\r\n");
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at http://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.92 seconds
vagrant@ubuntu:~$
```

4. Login Credentials:

- Username: (empty)
- Password: vagrant

Screenshot 1: VM running in VirtualBox with login screen.

```
ERULNX16 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
3306/tcp open mysql MySQL (unauthorized)
3500/tcp open http WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
6667/tcp open irc Unreal ircd (Admin email admin@TestIRC.net)
6697/tcp open irc Unreal ircd (Admin email admin@TestIRC.net)
8067/tcp open irc Unreal ircd (Admin email admin@TestIRC.net)
8080/tcp open http Jetty 8.1.7.v20120910
45559/tcp open unknown
51378/tcp open status 1 (RPC #100024)
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at http://www.insecure.org/cgi-bin/serv
cefp-submit.cgi :
SF-Port22-TCP:U=6.40%I=7%D=9/2%Time=68B6A999%P=x86_64-pc-linux-gnu%r(NULL,
SF:2C,"SSH-2\0-OpenSSH_6\0.6\0.1p1\0x20Ubuntu-2ubuntu2\0.13\r\n");
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at http://nmap
.org/submit/ .
# Nmap done at Tue Sep 2 08:23:58 2025 -- 1 IP address (1 host up) scanned in
2.92 seconds
vagrant@ubuntu:~$ ftp 10.0.2.15
Connected to 10.0.2.15.
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.0.2.15]
Name (10.0.2.15:vagrant): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
530 Login incorrect.
Login failed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Step 1 – Logging into the VM

- The VM was started, and login was performed using default credentials.
- **Observation:** The FTP service allowed login with empty username and password vagrant.

Purpose: Demonstrates a **weak authentication vulnerability**.

Screenshot 2: Successful FTP login prompt.

```
vagrant@ubuntu:~$ ftp 10.0.2.15
Connected to 10.0.2.15.
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.0.2.15]
Name (10.0.2.15:vagrant):
331 Password required for vagrant
Password:
530 Login incorrect.
Login failed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> bye
221 Goodbye.
vagrant@ubuntu:~$ ftp 10.0.2.15
Connected to 10.0.2.15.
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.0.2.15]
Name (10.0.2.15:vagrant):
331 Password required for vagrant
Password:
230 User vagrant logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Step 2 – FTP Exploration

- Connected via the built-in FTP service.
- Commands tested:

- ls
- get <filename>
- **Observation:**
 - FTP server allowed login.
 - Limited functionality; ls and options like ls -a were invalid due to server restrictions.
 - Only minimal files were visible.

Purpose: Shows that **FTP access is available**, even if limited, which is a potential security risk.

Screenshot 3: FTP session showing login success.

```

ERULNX16 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
SF:2C,"SSH-2.0-OpenSSH_6.6p1Ubuntu-2ubuntu2.13\r\n");
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port3000-TCP:U=6.40%I=7%D=9/2%Time=68B6B119%P=x86_64-pc-linux-gnu%r(Get
SF:Request,19F,"HTTP/1.1 204 Not Found\r\nX-Powered-By:\x20Express
SF:ss\r\nAccess-Control-Allow-Origin:\x20*\r\nContent-Security-Policy:\x2
SF:0default-src\x20'self'\r\nX-Content-Type-Options:\x20nosniff\r\nContent
SF:-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x20139\r\nDate
SF:\x20Tue,\x2002\x20Sep\x202025\x2008:55:53\x20GMT\r\nConnection:\x20clo
SF:se\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang=\x20en\x20>\n<head>\n<meta\x20c
SF:harset=\x20utf-8\x20>\n<title>Error</title>\n</head>\n<body>\n<pre>Cannot\x
SF:20GET\x20/</pre>\n</body>\n</html>\n")%r(HTTPOptions,EE,"HTTP/1.1 202
SF:04\x20No\x20Content\r\nX-Powered-By:\x20Express\r\nAccess-Control-Allow
SF:-Origin:\x20*\r\nAccess-Control-Allow-Methods:\x20GET,HEAD,PUT,PATCH,P
SF:OST,DELETE\r\nVary:\x20Access-Control-Request-Headers\r\nDate:\x20Tue,\x
SF:x2002\x20Sep\x202025\x2008:55:53\x20GMT\r\nConnection:\x20close\r\n\r\n
SF:")%r(FourOhFourRequest,1C2,"HTTP/1.1 204 Not Found\r\nX-Power
SF:ed-By:\x20Express\r\nAccess-Control-Allow-Origin:\x20*\r\nContent-Secu
SF:rity-Policy:\x20default-src\x20'self'\r\nX-Content-Type-Options:\x20nos
SF:niff\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:
SF:\x20174\r\nDate:\x20Tue,\x2002\x20Sep\x202025\x2008:55:53\x20GMT\r\nCon
SF:nection:\x20close\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang=\x20en\x20>\n<he
SF:ad>\n<meta\x20charset=\x20utf-8\x20>\n<title>Error</title>\n</head>\n<body>
SF:\n<pre>Cannot\x20GET\x20/nice%20ports%2C/Tri%6Eity.txt%20bak</pre>\n</
SF:body>\n</html>\n");
Service Info: Host: irc.TestIRC.net; OS: Unix

Service detection performed. Please report any incorrect results at http://nmap.
org/submit/ .
nmap done: 1 IP address (1 host up) scanned in 13.13 seconds
vagrant@ubuntu:~$

```

```

ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-r--r-- 1 vagrant vagrant 86562816 Oct 29 2020 VBoxGuestAdditions.iso
-rw-rw-r-- 1 vagrant vagrant 1571 Sep 2 08:23 ports.txt
226 Transfer complete
ftp> status
Connected to 10.0.2.15.
No proxy connection.
Connecting using address family: any.
Mode: stream; Type: binary; Form: non-print; Structure: file
Verbose: on; Bell: off; Prompting: on; Globbing: on
Store unique: off; Receive unique: off
Case: off; CR stripping: on
Quote control characters: on
Mtrans: off
Mmap: off
Hash mark printing: off; Use of PORT cmds: on
Tick counter printing: off
ftp>

```

Step 3 – Port Scanning with Nmap

- Opened a terminal in the VM.
- Ran a local scan to discover services:
- `nmap -sV 127.0.0.1`
- **Observation:** Several open ports and services were detected, including:
 - FTP (port 21)
 - SSH (port 22)
 - HTTP (port 80 or 8080)
- The Nmap scan output was saved to port.txt.

Purpose: To identify running services and potential attack surfaces.

Screenshot 4: Nmap scan output with open ports.

```

vagrant@ubuntu:~$ ssh vagrant@127.0.0.1
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
vagrant@127.0.0.1's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Sep 2 08:50:51 2025
vagrant@ubuntu:~$

```

```

Setting up nmap (6.40-0.2ubuntu1) ...
Processing triggers for libc-bin (2.19-0ubuntu6) ...
vagrant@vbox:~$ nmap -sV 10.0.2.15

Starting Nmap 6.40 ( http://nmap.org ) at 2025-08-30 12:36 UTC
Nmap scan report for ubuntu (10.0.2.15)
Host is up (0.00084s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
111/tcp   open  rpcbind      2-4 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: VBOX)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: VBOX)
631/tcp   open  ipp          CUPS 1.7
3306/tcp  open  mysql        MySQL (unauthorized)
6667/tcp  open  irc          Unreal ircd
8080/tcp  open  http         Jetty 8.1.7.v20120910
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port22-TCP:V=6.40%I=7%D=8/30%Time=68B2F05E%P=x86_64-pc-linux-gnu%r(NULL
SF:;2C,"SSH-2.0-OpenSSH_6.6\1p1x20Ubuntu-2ubuntu2\13r\n");
Service Info: Host: irc.TestIRC.net; OS: Unix

Service detection performed. Please report any incorrect results at http://nmap
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.73 seconds
vagrant@vbox:~$

```

Step 4 – Analysis of Findings

Service	Port	Vulnerability / Observation	Severity
FTP	21	Allows login with empty username and default password vagrant	Medium
SSH	22	Default service running; could allow brute-force login attempts	Low
HTTP	80/8080	Service running; potential for web-based vulnerabilities	Medium

Notes:

- FTP weakness is the most immediate vulnerability.
- Further exploitation is possible on HTTP or SSH, but for this report, only discovery and initial assessment were required.

Conclusion

- The VM was successfully hosted and accessed.
- FTP login vulnerability was discovered and documented.
- Nmap scanning revealed additional services that could be further investigated.

- This assessment demonstrates the process of **vulnerability identification and reporting** in a controlled environment.

Recommendations

1. **FTP:** Disable anonymous/weak login or enforce strong passwords.
2. **SSH:** Limit login attempts; use key-based authentication.
3. **HTTP:** Ensure web services are patched and secure.