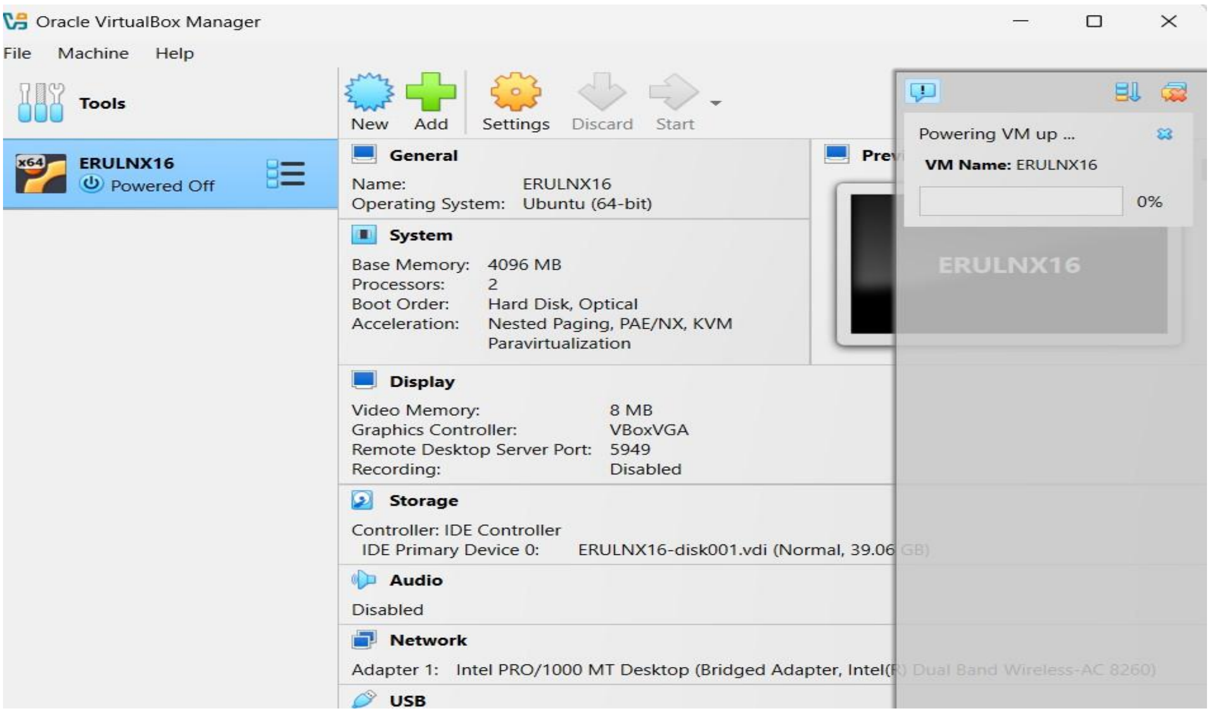
Introduction

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



ERULNX16
Powered Off

Powering VM up ...
VM Name: ERULNX16
0%

General
Name: ERULNX16
Operating System: Ubuntu (64-bit)

System
Base Memory: 4096 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

Display
Video Memory: 8 MB
Graphics Controller: VBoxVGA
Remote Desktop Server Port: 5949
Recording: Disabled

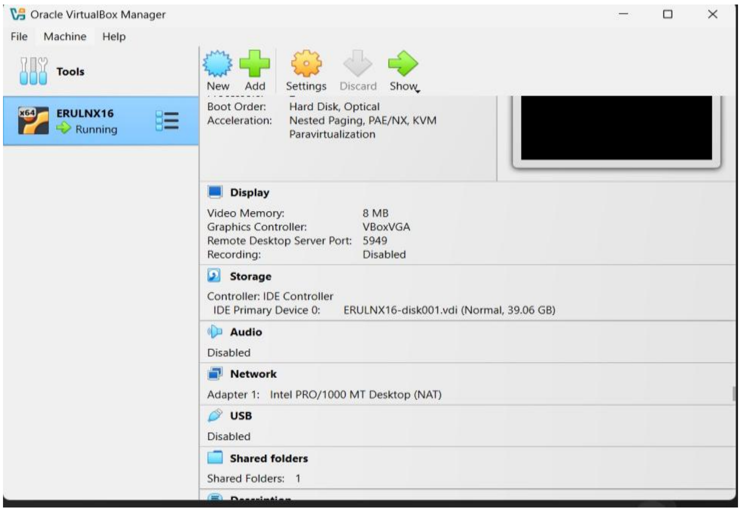
Storage
Controller: IDE Controller
IDE Primary Device 0: ERULNX16-disk001.vdi (Normal, 39.06 GB)

Audio
Disabled

Network
Adapter 1: Intel PRO/1000 MT Desktop (Bridged Adapter, Intel(R) Dual Band Wireless-AC 8260)

USB

2. **VM File:** Provided OVA file



ERULNX16
Running

Boot Order: Hard Disk, Optical
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

Display
Video Memory: 8 MB
Graphics Controller: VBoxVGA
Remote Desktop Server Port: 5949
Recording: Disabled

Storage
Controller: IDE Controller
IDE Primary Device 0: ERULNX16-disk001.vdi (Normal, 39.06 GB)

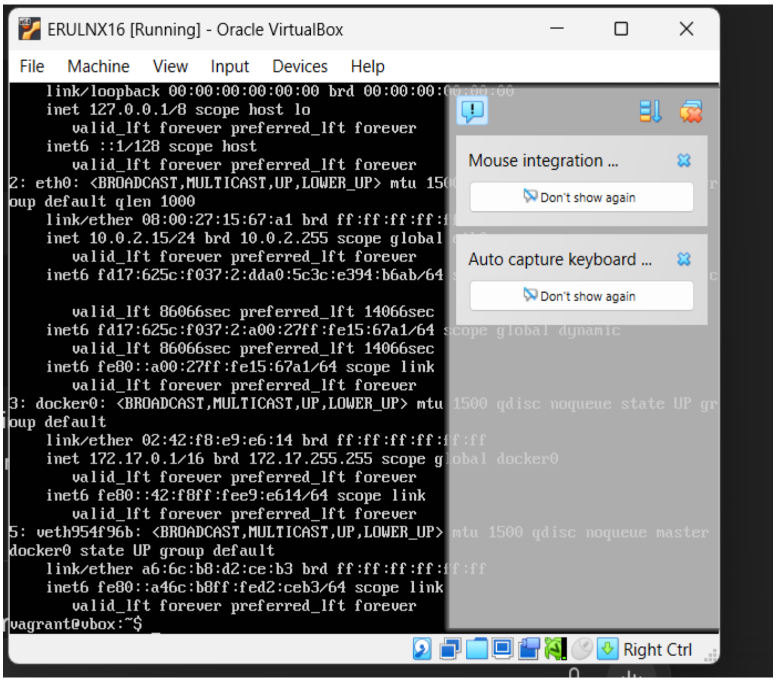
Audio
Disabled

Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)

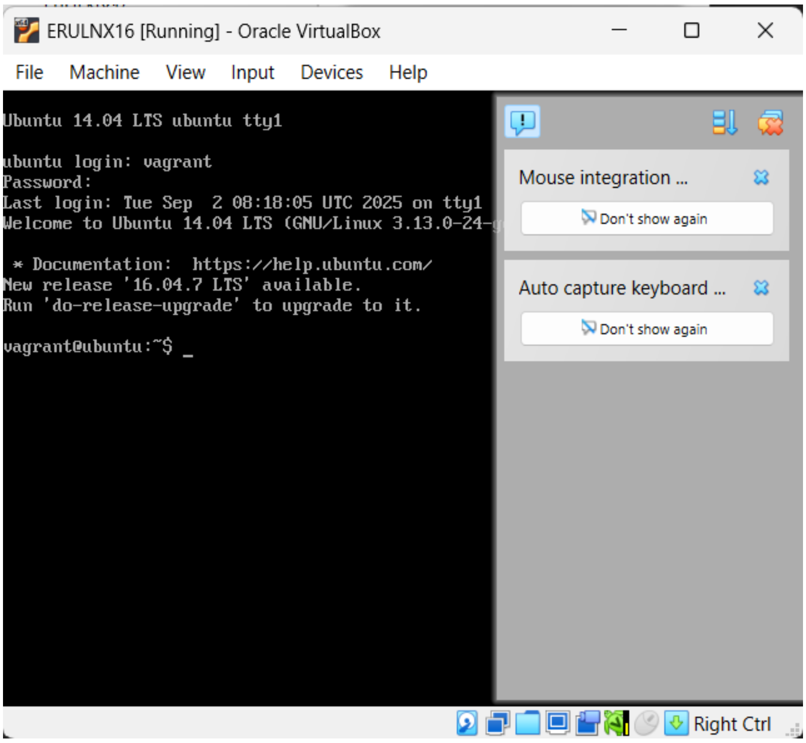
USB
Disabled

Shared folders
Shared Folders: 1

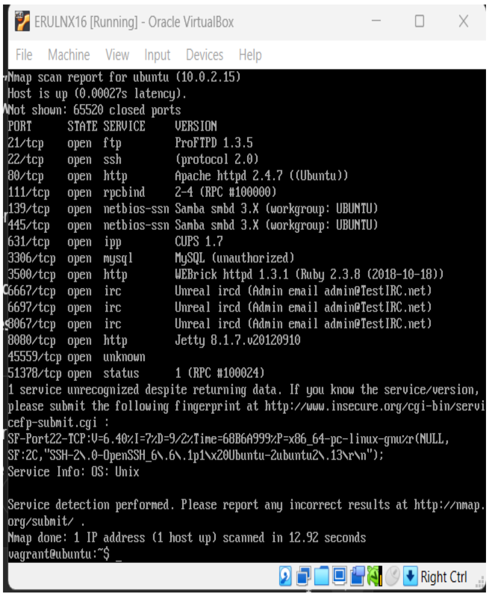
3. **VM IP Address:** 10.0.2.15



```
    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 150
oup default qlen 1000
    link/ether 08:00:27:15:67:a1 brd ff:ff:ff:ff:f
    inet 10.0.2.15/24 brd 10.0.2.255 scope global
       valid_lft forever preferred_lft forever
    inet6 fd17:625c:f037:2:dda0:5c3c:e394:b6ab/64

       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 gr
oup 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@vbox:~$ _
```



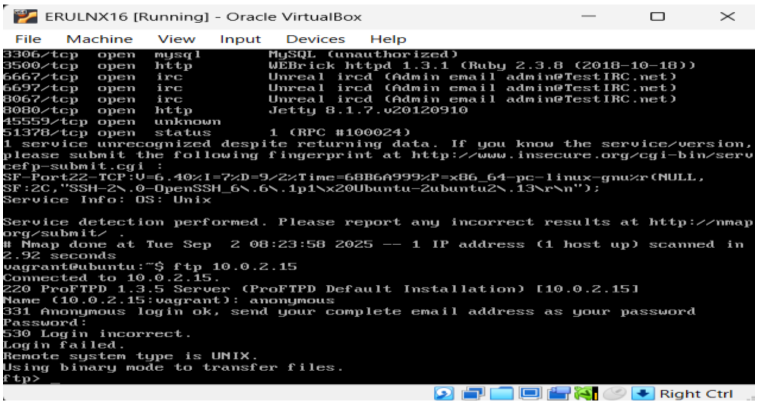
```
Ubuntu 14.04 LTS ubuntu tty1

ubuntu login: vagrant
Password:
Last login: Tue Sep  2 08:18:05 UTC 2025 on tty1
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-g

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

vagrant@ubuntu:~$ _
```


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

```
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\x20Ubuntu-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:~$ _
```

1. **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
Right Ctrl

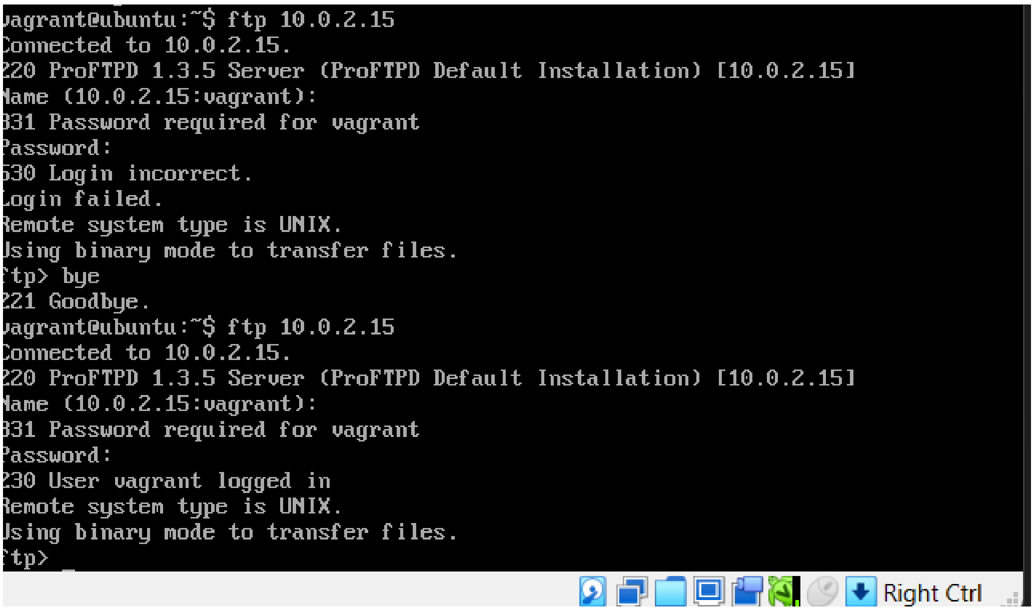
```
3306/tcp  open  mysql       MySQL (unauthorized)
3500/tcp  open  http        WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
6667/tcp  open  irc         Unreal ircd (Admin email admin@TestIRC.net)
6697/tcp  open  irc         Unreal ircd (Admin email admin@TestIRC.net)
8067/tcp  open  irc         Unreal 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: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\x20Ubuntu-2ubuntu2\.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.



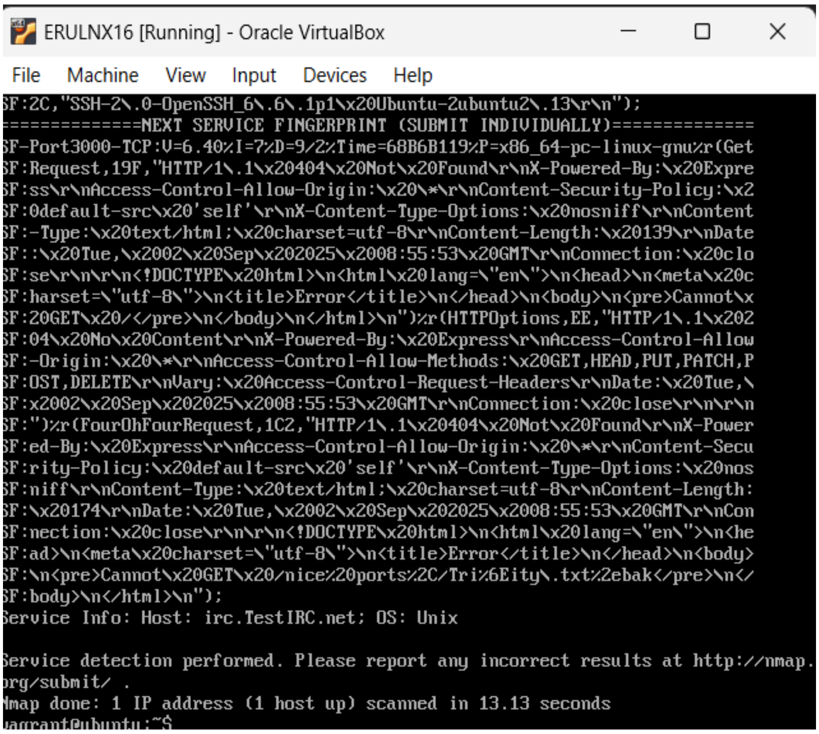
```
vagrant@ubuntu:~$ ftp 10.0.2.15
Connected to 10.0.2.15.
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.0.2.15]
Name (10.0.2.15:vagrant):
331 Password required for vagrant
Password:
530 Login incorrect.
Login failed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>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

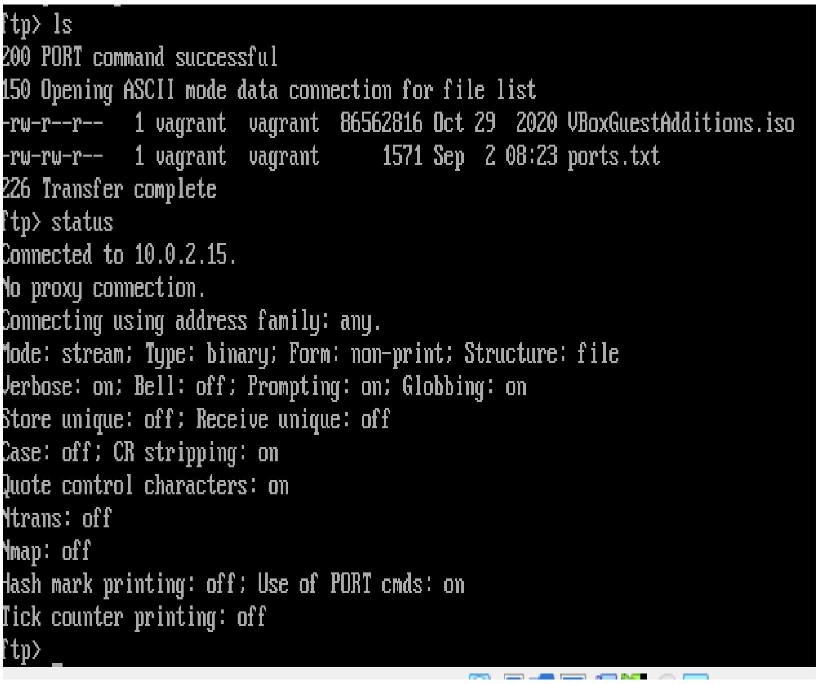
- Connected via the built-in FTP service.
- Commands tested:
  - ls
  - get <filename>
- **Observation:**
  - FTP server allowed login.
  - Limited functionality; ls and options like ls -a were invalid due to server restrictions.
  - Only minimal files were visible.

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

Screenshot 3: FTP session showing login success.



```
SF:2C,"SSH-2\.0-OpenSSH_6\.6\.1p1\x20Ubuntu-2ubuntu2\.13\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port3000-TCP:V=6.40%I=7%D=9/2%Time=68B6B119%P=x86_64-pc-linux-gnu%r(Get
SF:Request,19F,"HTTP/1\.1\x20404\x20Not\x20Found\r\nX-Powered-By:\x20Expre
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=\"en\">\n<head>\n<meta\x20c
SF:harset=\"utf-8\">\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\x202
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,\
SF:x2002\x20Sep\x202025\x2008:55:53\x20GMT\r\nConnection:\x20close\r\n\r\n
SF:")%r(FourOhFourRequest,1C2,"HTTP/1\.1\x20404\x20Not\x20Found\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=\"en\">\n<he
SF:ad>\n<meta\x20charset=\"utf-8\">\n<title>Error</title>\n</head>\n<body>
SF:\n<pre>Cannot\x20GET\x20/nice%20ports%2C/Tri%6Eity\.txt%2ebak</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:~$
```



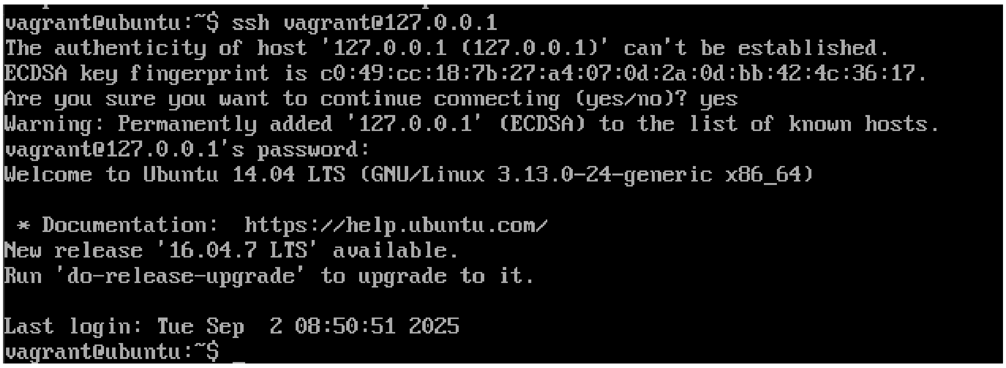
```
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-r--r--    1 vagrant  vagrant  86562816 Oct 29  2020 VBoxGuestAdditions.iso
-rw-rw-r--    1 vagrant  vagrant      1571 Sep  2 08:23 ports.txt
226 Transfer complete
ftp> status
Connected to 10.0.2.15.
No proxy 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
Ntrans: off
Nmap: off
Hash mark printing: off; Use of PORT cmds: on
Tick counter printing: off
ftp> _
```

Step 3 – Port Scanning with Nmap

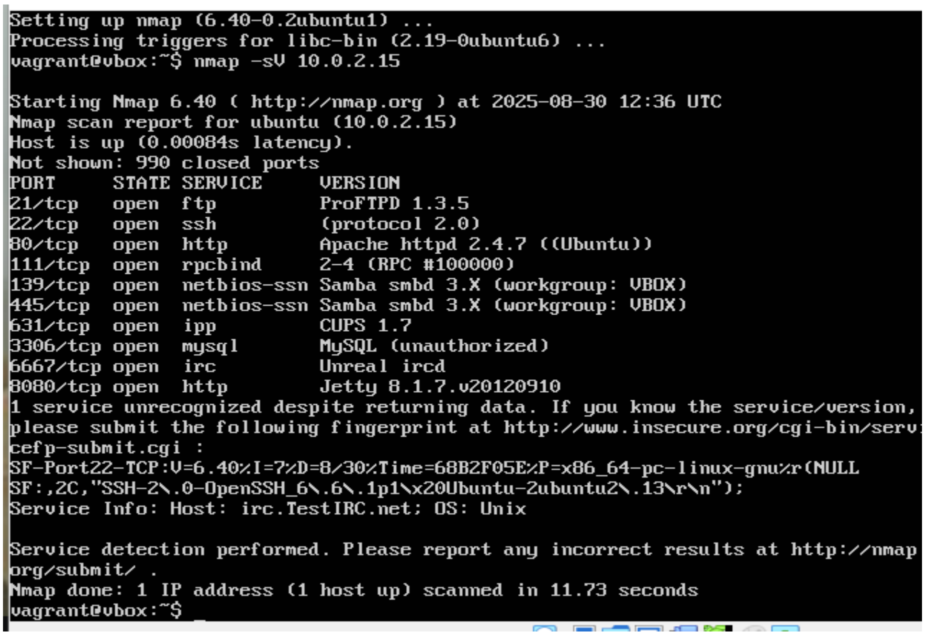
- Opened a terminal in the VM.
- Ran a local scan to discover services:
- nmap -sV 127.0.0.1
- **Observation:** Several open ports and services were detected, including:
  - FTP (port 21)
  - SSH (port 22)
  - HTTP (port 80 or 8080)
- The Nmap scan output was saved to port.txt.

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/serv
cefp-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\.1p1\x20Ubuntu-2ubuntu2\.13\r\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

The assessment of the target system revealed several active services that were identified during scanning and enumeration.

- **FTP (Port 21):** The FTP service was found to allow login with an empty username and the default password vagrant. This represents a significant weakness in authentication, as it permits unauthorized users to gain access to the service without proper credentials. While the functionality of the FTP service appeared limited, the ability to authenticate in this manner could allow attackers to probe deeper or use the access as a foothold for further attacks. Therefore, this issue is categorized as a medium severity vulnerability.
- **SSH (Port 22):** The SSH service was detected running with its default configuration. While no immediate vulnerability was confirmed, an exposed SSH service may be susceptible to brute-force login attempts or exploitation if weak credentials are used. This represents a potential risk but not an immediate compromise, and hence it is classified as a low severity observation.
- **HTTP (Port 80/8080):** A web service was also identified running on the system. The presence of an active HTTP server suggests the possibility of web application vulnerabilities such as outdated software, misconfigurations, or injection flaws. Without further detailed exploitation, it cannot be confirmed if such vulnerabilities exist, but the service itself presents a possible attack surface. For this reason, it has been rated as a medium severity observation.

Notes:

The most critical finding in this assessment is the insecure FTP configuration, as it provides a direct pathway for unauthorized access. While SSH and HTTP were also discovered, the scope of this assessment focused primarily on discovery and initial analysis, rather than in-depth exploitation of each service. Further testing could uncover additional weaknesses in these areas.

Conclusion

The ERULNX16 virtual machine was successfully deployed and assessed. The most critical finding was the insecure FTP configuration that allowed login with weak credentials. Additional services, including SSH and HTTP, were discovered and represent potential attack surfaces for further exploitation. Overall, the VM demonstrated clear security weaknesses, with FTP being the most immediate concern..