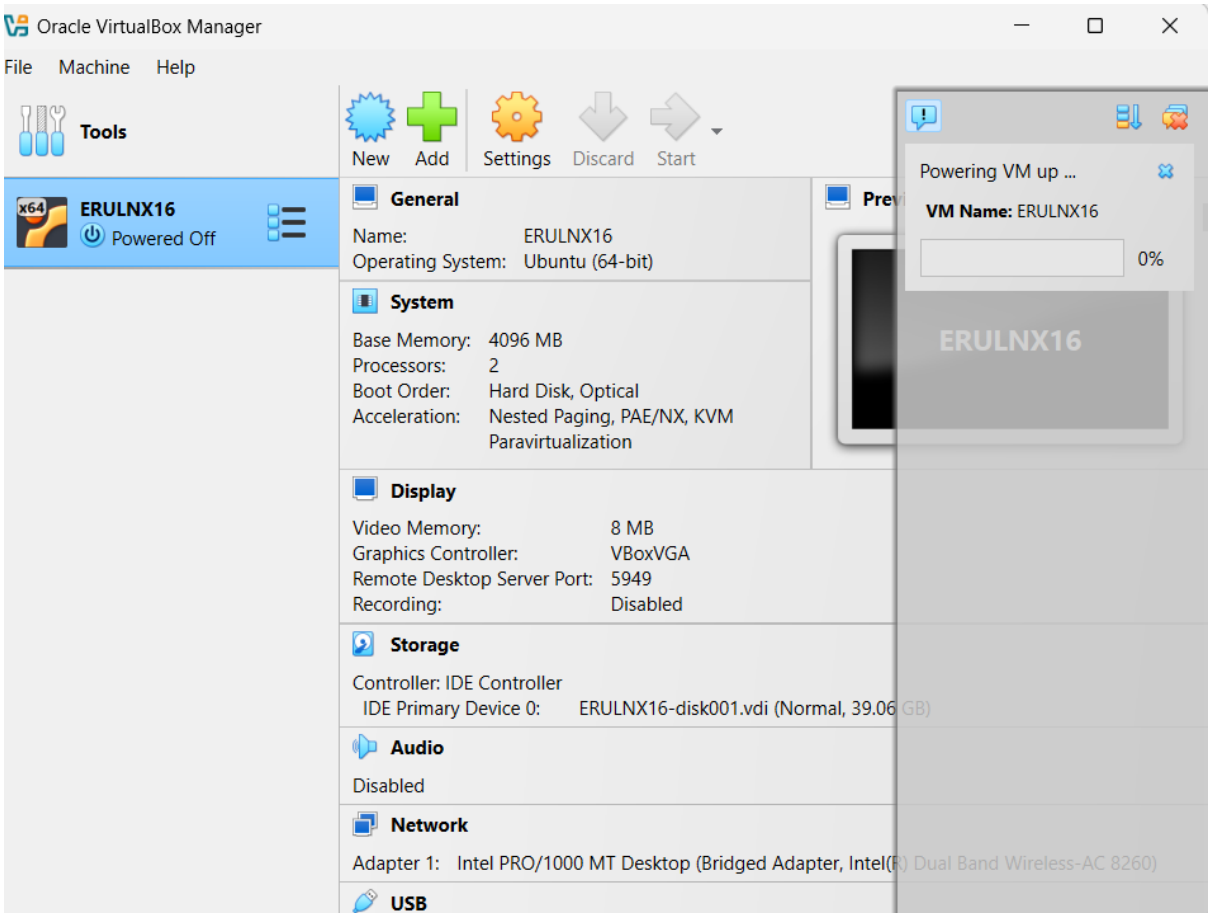
Introduction

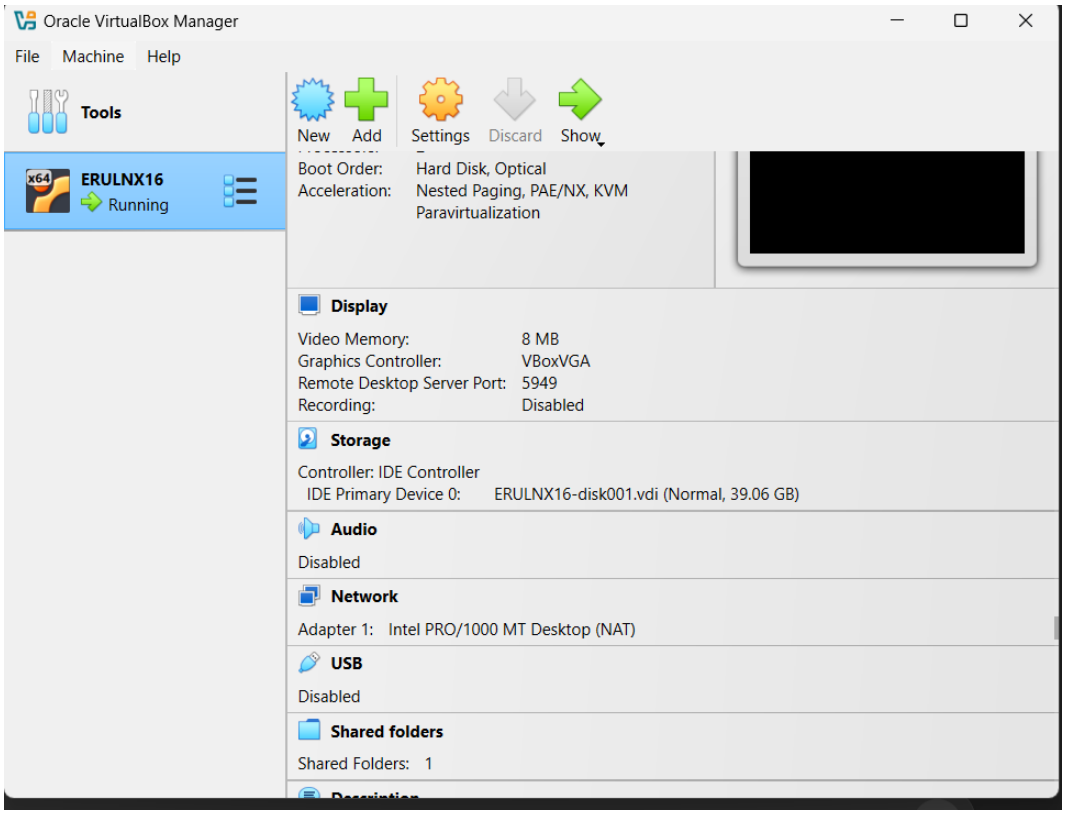
This report documents the process of assessing a virtual machine provided as part of Task 4. The goal was to identify potential vulnerabilities, explore services, and record findings in a professional format. The assessment was conducted in a controlled environment using VirtualBox.

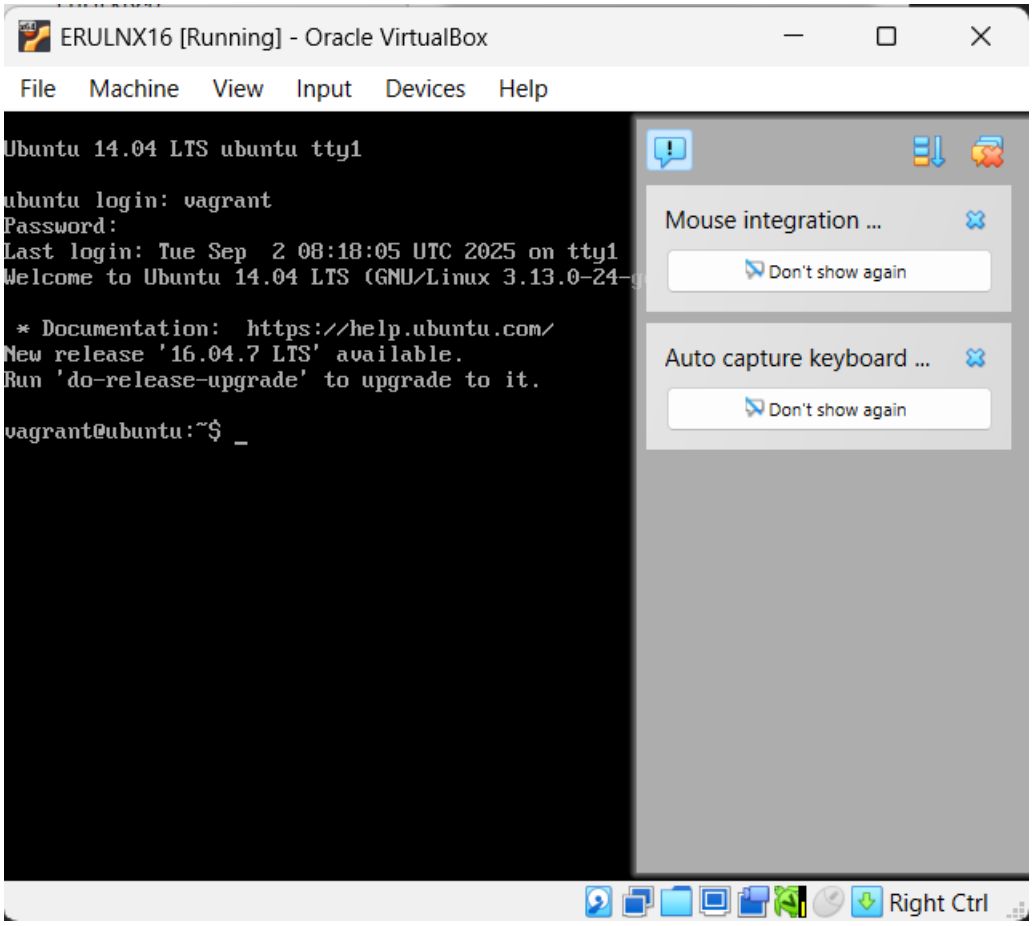
Environment Setup

1. **VM Host:** VirtualBox

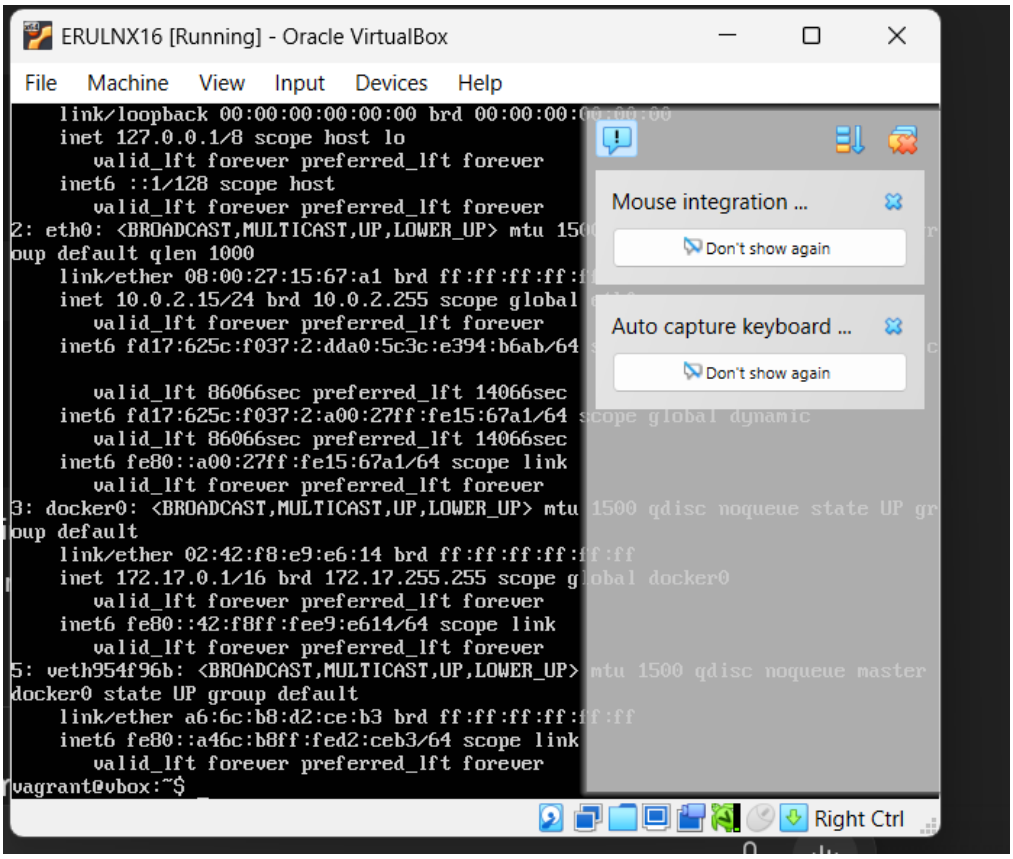


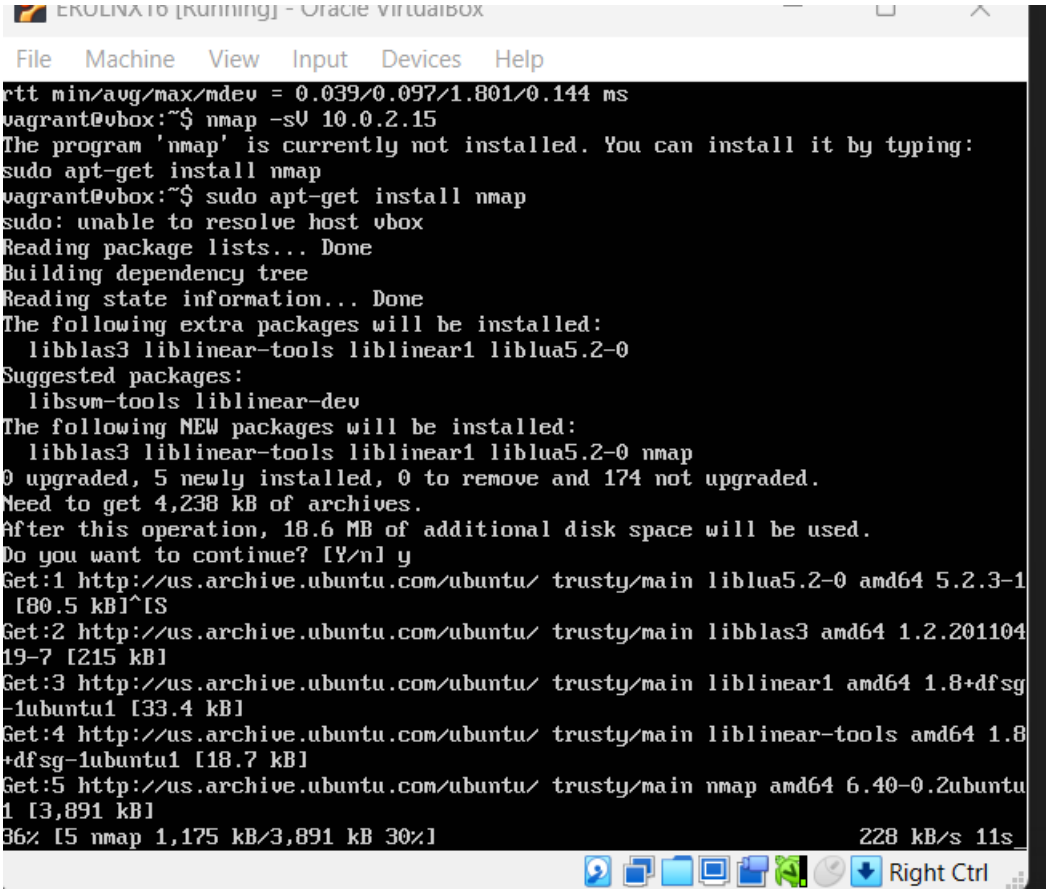
2. **VM File:** Provided OVA file

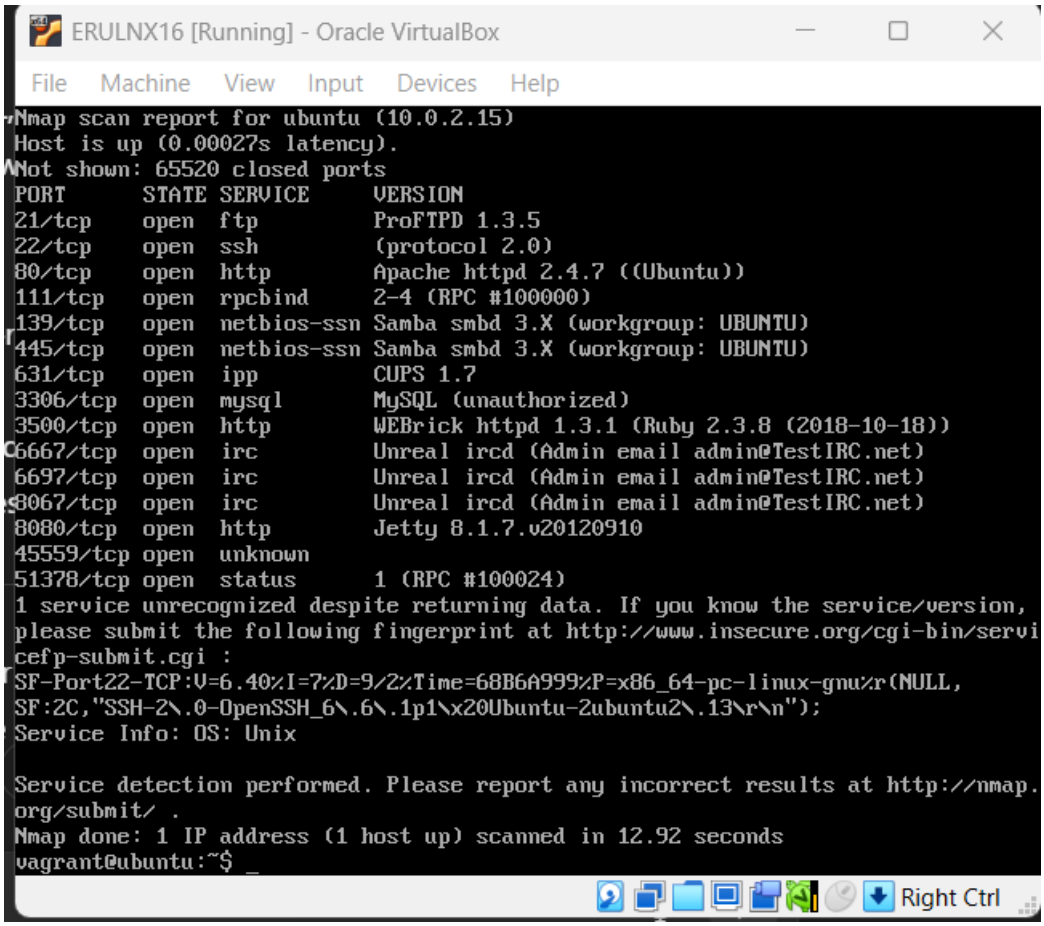




3. **VM IP Address:** 10.0.2.15

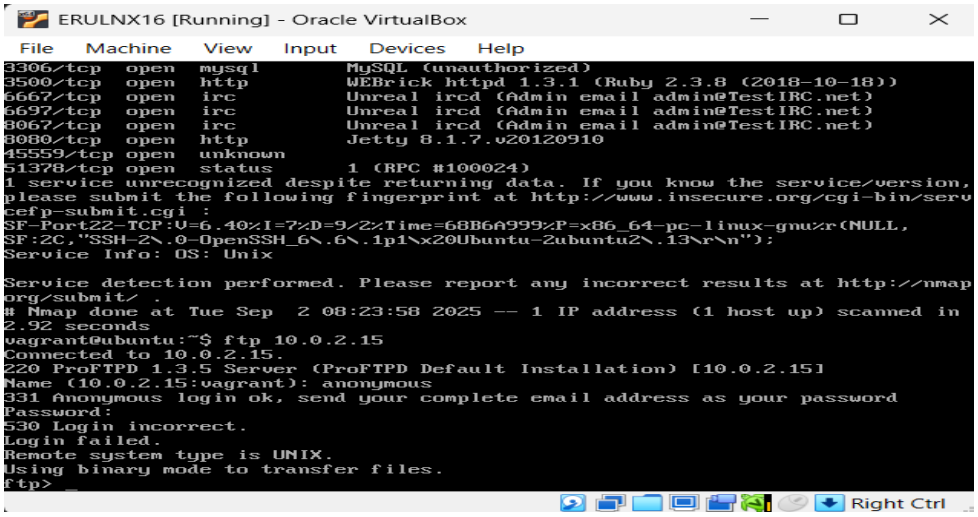






4. **Login Credentials:**
    - Username: (empty)
    - Password: vagrant

Screenshot 1: VM running in VirtualBox with login screen.

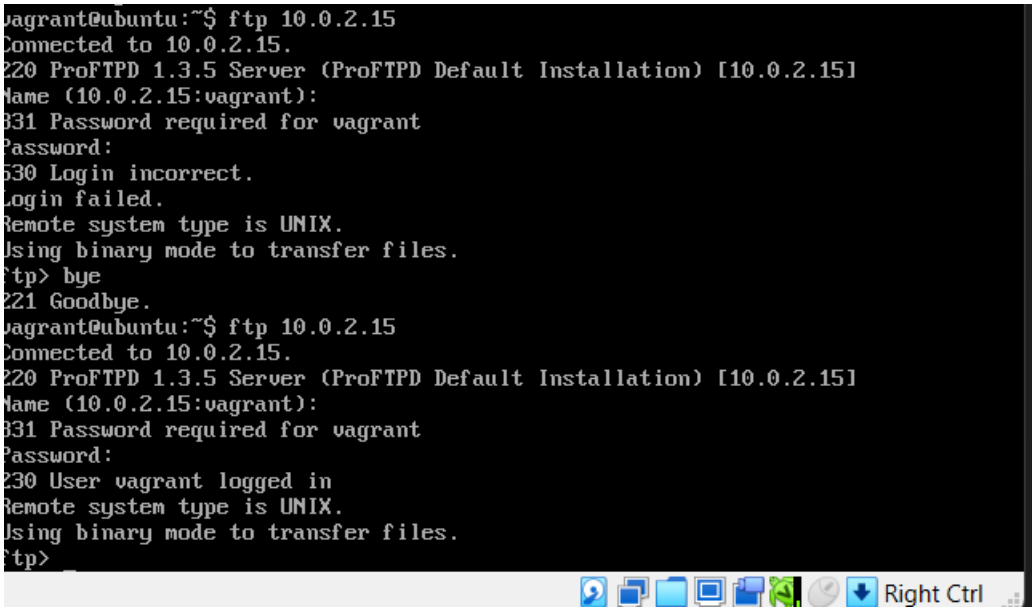


Step 1 – Logging into the VM

- 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.



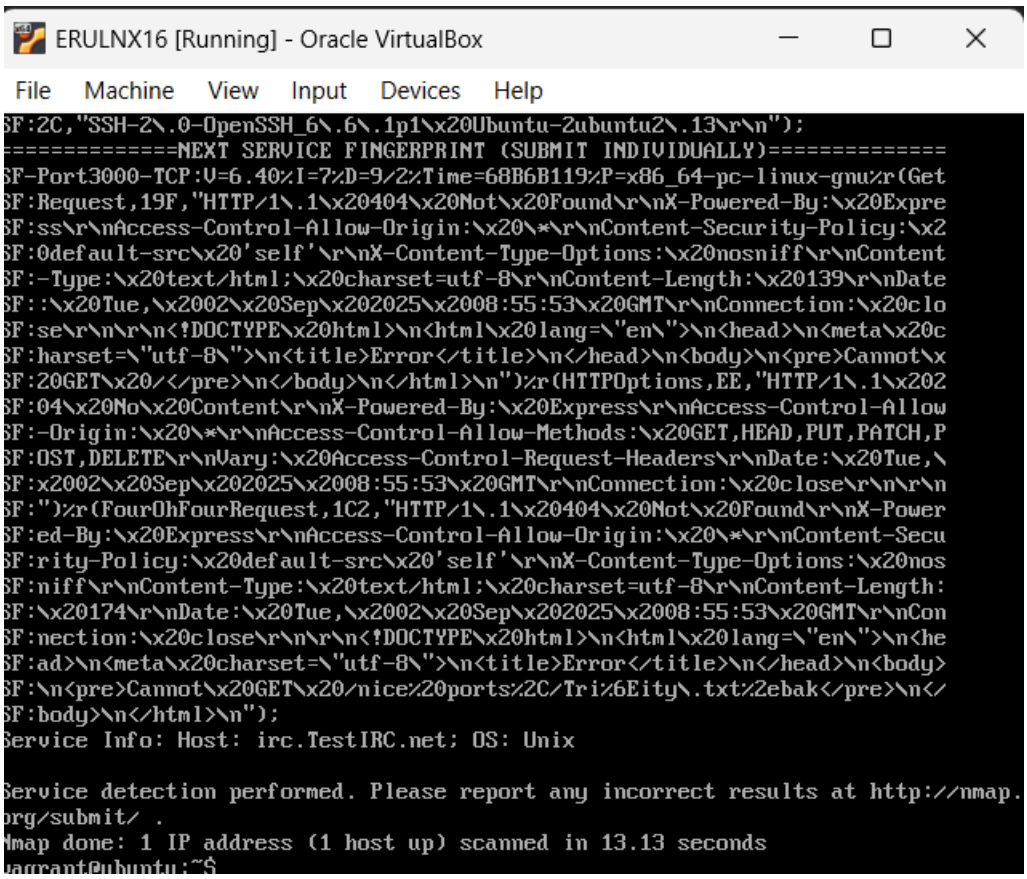
Step 2 – FTP Exploration

- 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.



```
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/servi
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

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.