SOC Analysis Report

Nmap Network Reconnaissance & Vulnerability Identification Lab

Analyst: Srishti
Date: 14 Jan 2026
Lab Type: SOC mini project/ Blue Team
Tools Used: Nmap
Environment: Virtual Lab (Kali Linux & Metasploitable)

1. Executive Summary

This report presents the results of a network reconnaissance and vulnerability identification exercise conducted using **Nmap** in a controlled lab environment. The objective was to identify exposed services, open ports, vulnerability detection, and potential security risk from a defensive (SOC) perspective.

On the reconnaissance on Metasploitable2 target system identifies 23 open ports, increasing the risk of compromise. Several exposed services were found outdated, exposed critical remote code execution vulnerabilities, or insecure by design. A critical risk was identified on **port 1524**, associated with a known backdoor service that allows unauthenticated access and requires immediate remediation.

Additionally, the assessment revealed the presence of a vsFTPd 2.3.4 backdoor vulnerability **(CVE-2011-2523)**, a confirmed remote root shell which allows complete remote access with no user interaction. Multiple services were observed using superseded cryptographic protocols, increasing susceptibility to **man-in-the-middle (MITM)** and downgrade attacks. Web-facing services also exhibited weaknesses indicative of poor input validation, potentially exposing the application to **SQL injection–based attacks**.

Overall, the system demonstrates a high-risk security posture, highlighting the importance of continuous monitoring, service hardening, and early detection of reconnaissance activity by SOC teams.

2. Objective & Scope

2.1 Objective

The objective of this assessment was to perform a controlled network reconnaissance exercise in order to identify exposed services, open ports, and potential security risks on the target system. The activity was analyzed from a Security Operations Center (SOC) perspective to understand how reconnaissance behavior contributes to an organization's overall attack surface.

Specific objectives of this assessment included:

- Identify open TCP ports and running network services.
- Detects outdated, misconfigured, or insecure services that can be a potential risk.

- Assess potential vulnerability.
- Analyze findings from a SOC analyst's perspective.
- Evaluation of reconnaissance activity for detection and monitoring by SOC teams.
- Provide actionable security recommendations to improve defensive posture.

2.2 Scope

This assessment was conducted within a controlled and authorized lab environment to evaluate exposed network services and potential security risks observable during the reconnaissance phase of an attack.

Environment Details:

- **Scanning Host:** Kali Linux (controlled scanning system)
- **Target System:** Metasploitable 2 (intentionally vulnerable virtual machine)
- **Network Type:** NAT
- **Authorization:** All activities were performed with explicit authorization within a lab environment

Systems/IPs Included:

Kali Linux: 192.168.139.129
Metasploitable 2: 192.168.139.128

Out Of Scope:

- Active exploitation of identified vulnerabilities
- Credential-based attacks (brute-force or password spraying)
- Denial-of-Service (DoS) testing
- Web application exploitation or payload execution
- Post-exploitation activities

2.3 Tools Used

The following tools were utilized during the reconnaissance and analysis phase of this assessment. All tools were used in a controlled and authorized lab environment and evaluated from a Security Operations Center (SOC) perspective.

2.3.1. Nmap (Network Mapper)

- **Purpose:** Network discovery and service enumeration
- **Usage:** Identification of live hosts, open ports, running services, and service versions
- **SOC Relevance:**
  a) Commonly used by threat actors during the reconnaissance phase
  b) Generates identifiable scan patterns detectable by IDS/IPS and SIEM platforms
  c) Helps SOC analysts understand exposed attack surfaces and prioritize remediation

2.3.2. Kali Linux

- **Purpose:** Security testing and analysis platform
- **Usage:** Served as the controlled scanning host for executing reconnaissance activities
- **SOC Relevance:**
  a) Widely used in red-team and adversary simulations
  b) Enables SOC teams to replicate attacker reconnaissance behavior for detection tuning

2.3.3. Metasploitable 2

- **Purpose:** Intentionally vulnerable target system
- **Usage:** Functioned as the assessed host for evaluating exposed services and vulnerabilities
- **SOC Relevance:**
    a) Simulates real-world insecure configurations
    b) Allows SOC analysts to observe how vulnerable systems appear during reconnaissance

3. Methodology

3.1 Reconnaissance Approach

The reconnaissance phase was conducted to identify exposed network services, open ports, and system characteristics that could be exploited by an adversary during the early stages of an attack. This activity was performed in a controlled and authorized lab environment and analyzed from a **defensive Security Operations Center (SOC) perspective**.

The approach followed a layered scanning methodology, beginning with low-noise discovery techniques and progressing to more detailed mapping. Initial scans focused on identifying live hosts and open TCP ports, followed by service and version detection to assess potential security risks associated with outdated or vulnerable system activities. Limited OS fingerprinting and default script execution were used to enhance visibility while maintaining controlled scan intensity.

All reconnaissance activity was logged and analyzed to understand how such scanning behavior would appear from a monitoring and detection standpoint within a SOC environment.

3.2 Scan Types and Commands Executed

a) Ping Scan

Command: (nmap -sn 192.168.233.0/24 | grep "Nmap scan report")
Purpose: Finding live hosts, Identifying unknown systems, filtering noise

b) Basic Port Scanning

Command: (nmap 192.168.139.128)
Purpose: Identify open TCP ports, Detect exposed services

c) Service & Version Detection

Command: (nmap -sV 192.168.139.128)
Purpose: Identify running services and their versions, Map services to known vulnerabilities

d) Operating System Detection

Command: (nmap -O 192.168.139.128)
Purpose: Identify the operating system and kernel version

e) Combined Scan (OS + Services + Vulnerabilities)
Command: (nmap -sV -O --script vuln 192.168.139.128)
Purpose: Detect services, OS, and known vulnerabilities, and Run NSE vulnerability scripts

f) FTP Vulnerability Scan (vsFTPd Backdoor)
Command: (nmap -sV -p 21 --script ftp-vsftpd-backdoor 192.168.139.128)
Purpose: Detect **CVE-2011-2523,** Confirm exploitable vsFTPd 2.3.4 backdoor

g) SMB Vulnerability Script Scan
Command: (nmap --script smb-vuln* -p 445 192.168.139.128)
Purpose: Check for known SMB-related vulnerabilities, Validate Windows exposure

h) Output Saving
Command: (nmap -sV -O --script vuln 192.168.139.128 -oA metasplotable_recon)
Purpose: save results in:

- `.nmap` (human readable)
- .xml (tool ingestion)
- .gnmap (grepable)

4. Key Observations

a) **Host Availability**

- The target system **192.168.139.128** was confirmed **alive and reachable** within the local network.
- Network latency was very low, indicating the host was on the **same subnet.**

b) **Excessive Open Ports**

Multiple TCP ports were found open, including:

a) FTP (21)
b) SSH (22)
c) Telnet (23)
d) SMTP (25)
e) HTTP (80)
f) SMB (139, 445)
g) Database services (MySQL 3306, PostgreSQL 5432)
h) Remote services (VNC 5900, RMI 1099, IRC 6667, Tomcat 8180)

c) Outdated & Vulnerable Service Versions

Identified outdated services known to contain vulnerabilities:

a) vsFTPd 2.3.4
b) Apache HTTPD 2.2.8
c) OpenSSH 4.7p1
d) MySQL 5.0.51a
e) PostgreSQL 8.3.x

d) Critical FTP Backdoor Vulnerability

- FTP service running vsFTPd 2.3.4 was confirmed vulnerable
- Vulnerability identified: CVE-2011-2523
- Backdoor allows remote root shell access

e) Default Root Bind Shell Detected

Port 1524/tcp exposed a bind shell running as root.

f) SMB File Sharing Exposure

- SMB services (ports 139 & 445) were accessible.
- Samba service running with minimal restrictions.

5. Risk Analysis

a) vsFTPd 2.3.4 Backdoor (CVE-2011-2523)

- **Affected Port:** 21/TCP
- **Attack Vector:** Network
- **Privileges Required:** None (no user interaction)
- **CVSS Base Score:** 10.0(critical)
- **Reason:** Allows unauthenticated remote attackers to gain full root access to the system.
- **Likelihood:** Public exploit available with no authentication required (Very High)
- **Impact:** Remote root shell access with Full system compromise (Severe)
- **MITRE ATT&CK Mapping:**

  a) Initial Access: T1190 – Exploit Public-Facing Application
  b) Execution: T1059 – Command and Scripting Interpreter
  c) Privilege Escalation: T1068 – Exploitation for Privilege Escalation

b) Root Bind Shell Exposure

- **Affected Port:** 1524/TCP
- **Attack Vector:** Network
- **Privileges Required:** None (no user interaction)
- **Impact:** Full system compromise
- **CVSS Base Score:** 9.8 (Critical)
- **Reason:** Direct root shell accessible over the network without authentication.
- **Likelihood:** No authentication required with Direct shell access (Very High)
- **MITRE ATT&CK Mapping:**

  a) Initial Access: T1059 – Command and Scripting Interpreter
  b) Execution: T1547 – Boot or Logon Autostart Execution
  c) Privilege Escalation: T1068 – Exploitation for Privilege Escalation

c) Insecure Remote Access Services (Telnet, rsh)

- **Affected Port:** 23, 512–514/TCP
- **Attack Vector:** Network
- **Privileges Required:** Low (no user interaction)

- **Impact:** Credential interception and remote access
- **CVSS Base Score:** 8.2 (High)
- **Reason:** Use of plaintext protocols enables credential theft and session hijacking.
- **Likelihood:** Plaintext credentials, Easy to sniff on local network (High)
- **MITRE ATT&CK Mapping:**
  a) Credential Access: T1040 – Network Sniffing
  b) Lateral Movement: T1021 – Remote Services

d) SMB Service Exposure (Samba 3.x)

- **Affected Port:** 139, 445/TCP
- **Attack Vector:** Network
- **Privileges Required:** None (no user interaction)
- **Impact:** Information disclosure and lateral movement
- **CVSS Base Score:** 7.5 (High)
- **Reason:** Outdated Samba versions are commonly exploited for file access and privilege escalation.
- **Likelihood:** Frequently targeted service, and Outdated version (Medium to High)
- **MITRE ATT&CK Mapping:**
  a) Lateral Movement: T1021.002 – SMB/Windows Admin Shares
  b) Discovery: T1083 – File and Directory Discovery

6. Recommendations

Based on the findings of this reconnaissance and vulnerability identification exercise, the following recommendations are proposed to reduce the attack surface, mitigate identified risks, and strengthen the organization's overall security posture.

a) Service Hardening and Exposure Reduction

- Disable unnecessary and insecure services such as **Telnet** and **FTP**.
- Restrict access to critical services using firewall rules and network segmentation.
- Ensure only required ports are exposed and accessible

b) Patch and Update Management

- Upgrade or replace outdated and vulnerable services, including **vsFTPd 2.3.4**.
- Remove backdoor services such as the one identified on **port 1524**.
- Implement a regular patch management process to address known vulnerabilities.

c) Secure Configuration Practices

- Replace obsolete or insecure cryptographic protocols with modern, secure alternatives.
- Enforce strong authentication mechanisms and disable anonymous access where applicable.
- Apply security hardening benchmarks (e.g., CIS benchmarks).

d) SOC Monitoring and Detection Enhancements

- Implement IDS/IPS rules to detect network scanning behavior (e.g., SYN scans, service enumeration).
- Configure SIEM alerts for repeated connection attempts across multiple ports.

- Monitor logs for indicators of reconnaissance activity consistent with **MITRE ATT&CK TA0043**.

e) Continuous Security Assessment

- Conduct periodic internal vulnerability assessments and port scans.
- Maintain asset inventory and baseline normal network behavior.
- Regularly review SOC detection rules and alert effectiveness.

7. Conclusion

The network reconnaissance and vulnerability identification exercise conducted using Nmap successfully identified multiple exposed services and critical security weaknesses on the target system. The assessment revealed an excessively large attack surface due to numerous open ports, insecure legacy services, and outdated software versions.

Two critical vulnerabilities, including an exploitable **vsFTPd 2.3.4 backdoor (CVE-2011-2523)** and an exposed **root bind shell**, were identified, both of which allow unauthenticated attackers to gain full system control. Additionally, several high-risk misconfigurations such as insecure remote access services (Telnet and rsh), exposed SMB services, and publicly accessible database services further increased the likelihood of compromise.

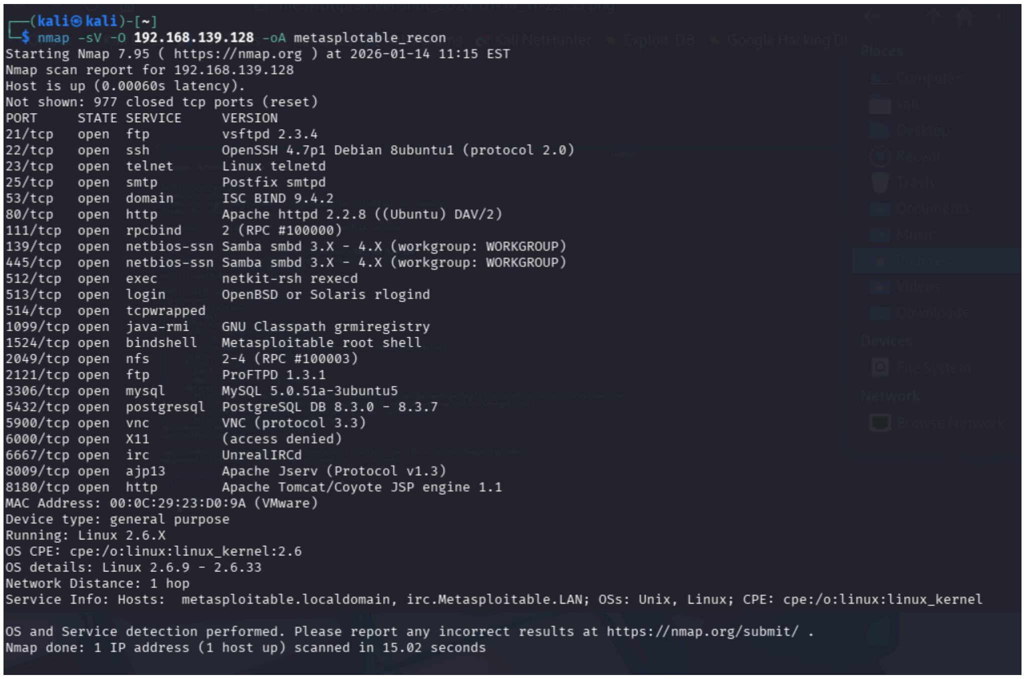
The findings were prioritized based on **severity, exploitability, and potential impact**, aligned with standard SOC triage practices and mapped to relevant **MITRE ATT&CK techniques**. While the target system was intentionally vulnerable for lab purposes, the identified issues reflect common real-world misconfigurations that continue to be exploited in production environments.

Overall, this assessment demonstrates the effectiveness of Nmap as a reconnaissance and vulnerability identification tool and highlights the importance of proper service hardening, patch management, and network segmentation to reduce organizational risk. This lab reinforced foundational SOC skills in network discovery, vulnerability analysis, risk prioritization, and security reporting.

8. Appendix

8.1 Key Evidence Screenshots

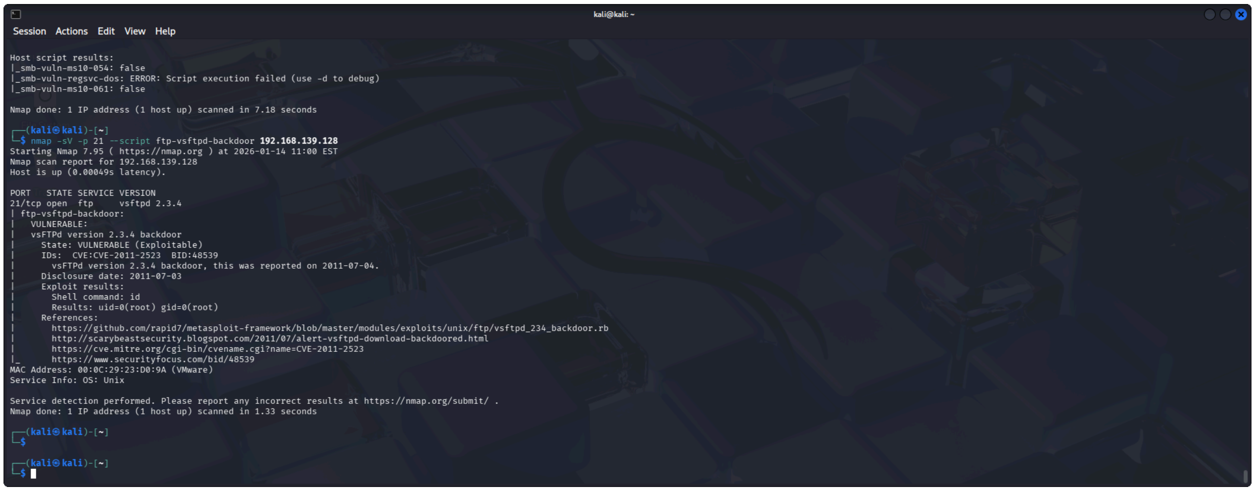
a) Screenshot of OS detection results



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -O 192.168.139.128 -oA metasplotable_recon
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-14 11:15 EST
Nmap scan report for 192.168.139.128
Host is up (0.00060s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:23:D0:9A (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.02 seconds
```

b) Screenshot of vsFTPd backdoor vulnerability detection



```
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-061: false

Nmap done: 1 IP address (1 host up) scanned in 7.18 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 21 --script ftp-vsftpd-backdoor 192.168.139.128
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-14 11:00 EST
Nmap scan report for 192.168.139.128
Host is up (0.00049s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      https://www.securityfocus.com/bid/48539
MAC Address: 00:0C:29:23:D0:9A (VMware)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.33 seconds

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$ 
```

8.2 Scan Outputs

- **Nmap scan output (.nmap):** https://drive.google.com/file/d/1-PX22AMnNltoYP4I-uAd9XAkGJMaNVP3/view?usp=sharing
- **Nmap scan output (.xml):** https://drive.google.com/file/d/1BqZvIhfdXfanUtMD4h7OLDTPgj_V2NH9/view?usp=sharing