# PRACTICAL REPORT : Vulnerability Exploitation Using Nmap, Metasploit, and OWASP ZAP

## Aim / Objective

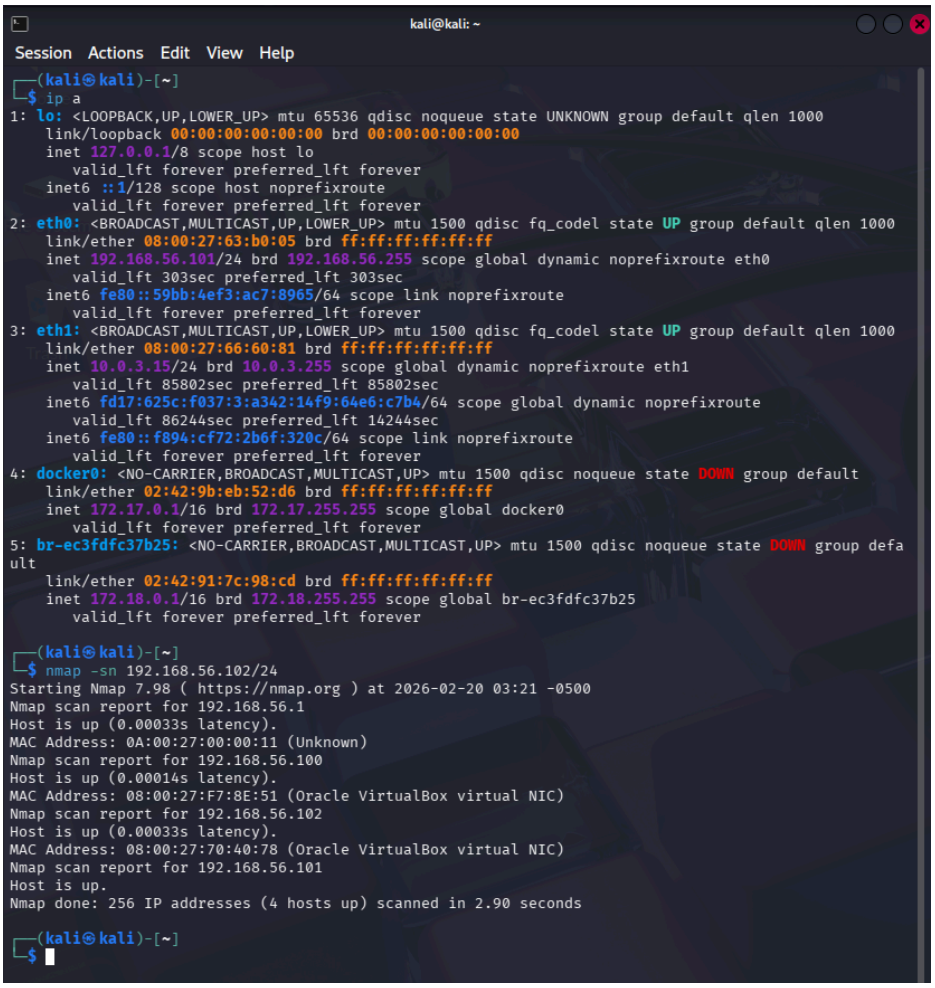
The aim of this practical is to identify, analyze, and exploit vulnerabilities present in a deliberately vulnerable system using penetration testing tools. The objective is to understand real-world attack techniques, assess their impact, and recommend suitable remediation measures.

## Tools and Technologies Used

| Tool | Purpose |
|---|---|
| Kali Linux | Attacking system |
| Metasploitable | Vulnerable target system |
| Nmap | Network and vulnerability scanning |
| Metasploit Framework | Exploitation and post-exploitation |
| OWASP ZAP | Web application security scanning |
| VirtualBox | Virtualization platform |

# Lab Environment

- **Attacker Machine**: Kali Linux
- **Target Machine**: Metasploitable
- **Target IP Address**: `192.168.56.102`
- **Network Mode**: Host-Only Adapter
- **Architecture**: Virtualized environment



# Methodology

The penetration testing process was carried out in a structured manner consisting of environment setup, reconnaissance, vulnerability identification, exploitation, post-exploitation, web application assessment, and reporting.

### ❖ Environment Setup and Target Identification

Initially, both the attacker and target virtual machines were configured in a controlled lab environment using VirtualBox. A Host-Only network adapter was selected to ensure isolation from external networks while allowing internal communication.

The target machine's IP address was identified and connectivity was verified to ensure a stable testing environment before proceeding with further assessments.

**Problem Faced:**

- Attacker machine could not communicate with the target system.

**Cause:**

- Network adapter mismatch between virtual machines.

**Solution:**

- Both machines were configured to use Host-Only Adapter mode, restoring connectivity.

### ❖ Network and Service Enumeration Using Nmap

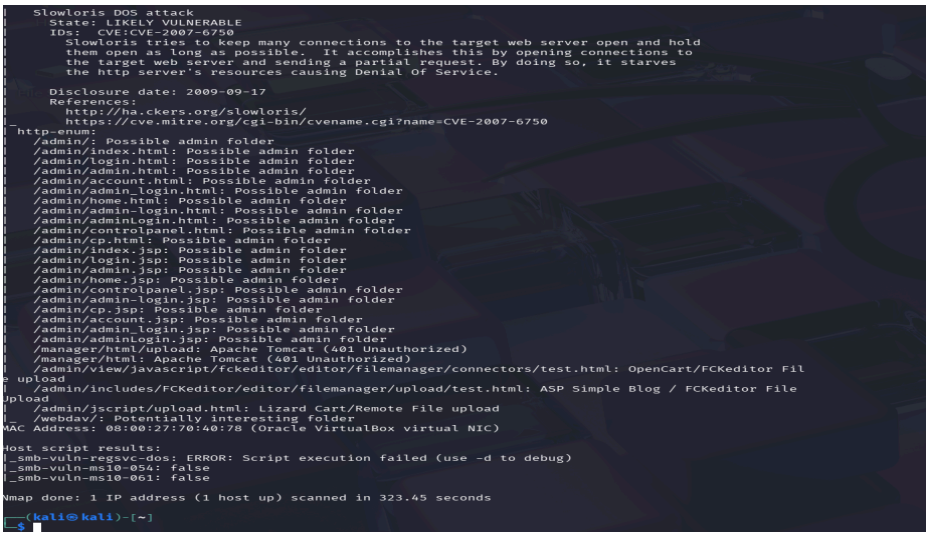
Once connectivity was established, network scanning and service enumeration were performed using Nmap to identify open ports, running services, and known vulnerabilities.

**Command Executed:**

nmap -sV --script vuln 192.168.56.102

This scan performed:

- Detection of open TCP ports
- Service version identification
- Execution of vulnerability detection scripts

**Findings:**

| Port | Service | Status |
|---|---|---|
| 21 | FTP (vsFTPd 2.3.4) | Open |
| 22 | SSH | Open |
| 23 | Telnet | Open |
| 25 | SMTP | Open |
| 80 | HTTP | Open |
| 443 | HTTPS | Open |

Multiple vulnerabilities were detected, including outdated services, insecure protocols, and known exploits.

### ❖ Vulnerability Identification and Analysis

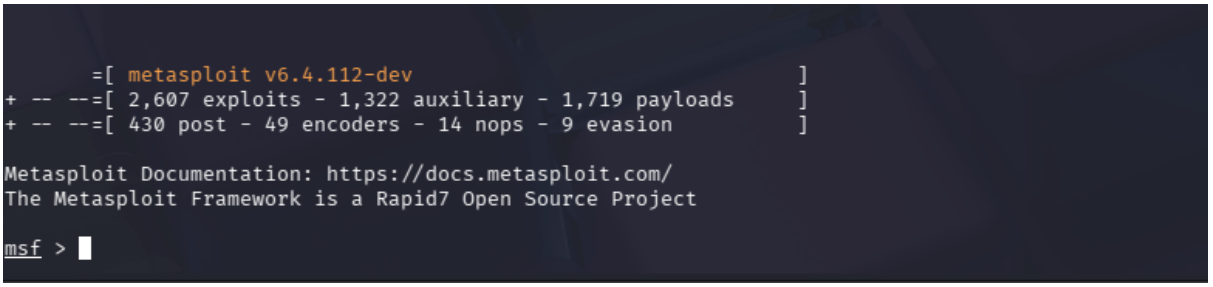
From the Nmap results, vulnerabilities were analyzed based on severity and exploitability. The most critical vulnerability identified was:

| Vulnerability | CVE ID | Severity |
|---|---|---|
| vsFTPd 2.3.4 Backdoor | CVE-2011-2523 | Critical |

This vulnerability allows an attacker to gain unauthenticated root access due to a malicious backdoor embedded in the FTP service.

### ❖ Exploitation Using Metasploit

To exploit the identified vulnerability, the Metasploit Framework was used.



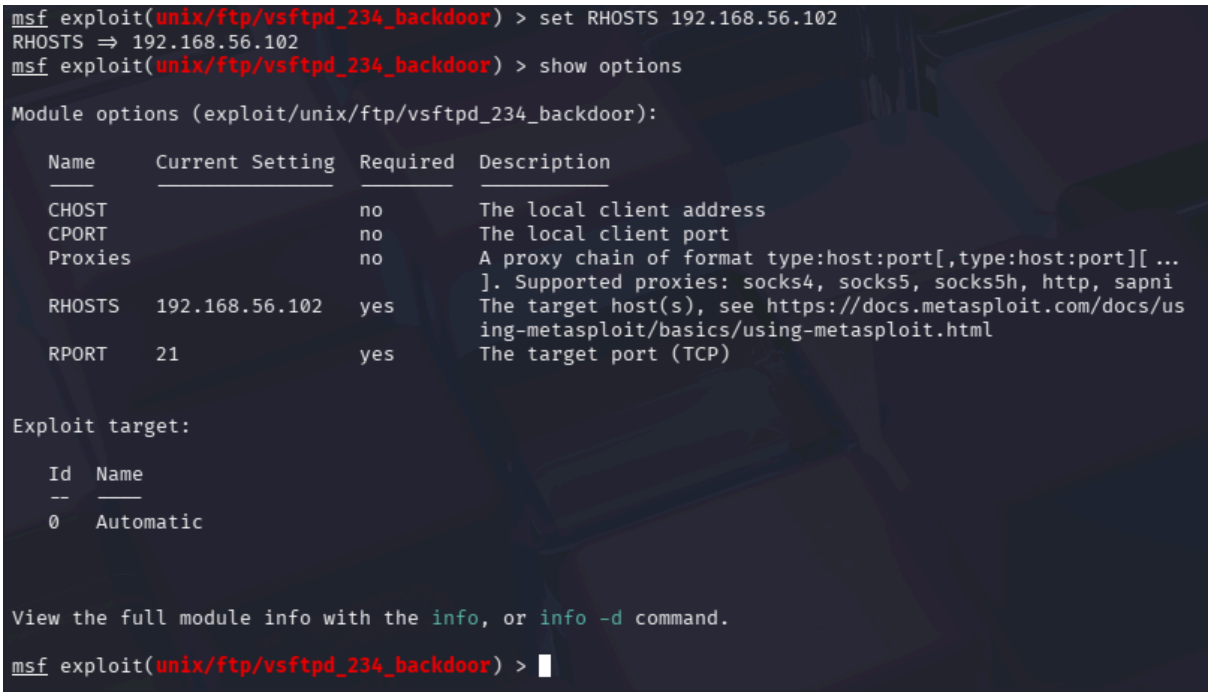

**Steps Performed:**

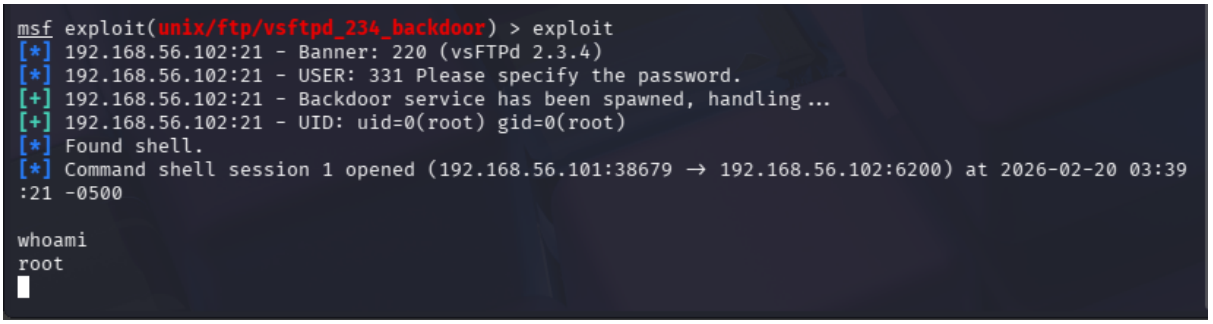
msfconsole

use exploit/unix/ftp/vsftpd_234_backdoor

set RHOSTS 192.168.56.102

exploit




**Result:**

- Backdoor service spawned successfully
- Command shell session opened
- Root-level access obtained

**Problem Faced:**

- Exploit initially failed to execute.

**Cause:**

- Metasploit database was not initialized.

**Solution:**

msfdb init

After initialization, exploitation succeeded.

## ❖ Post-Exploitation

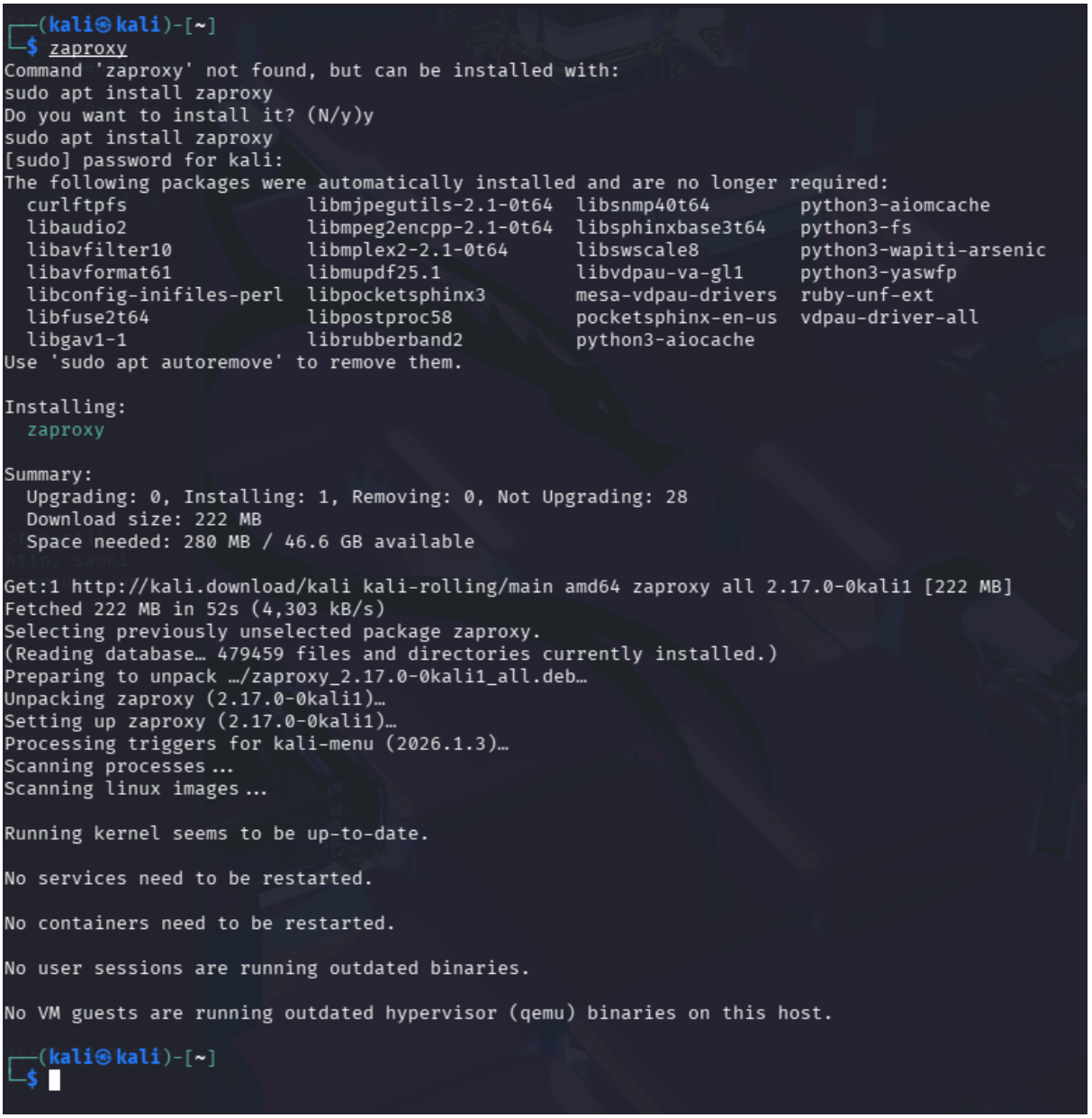
After successful exploitation, post-exploitation steps were carried out to verify privileges and assess system compromise.

- Root access was confirmed using system commands.
- Critical system directories were accessible.
- Full system control was achieved.

This demonstrates the severe impact of outdated and vulnerable services.

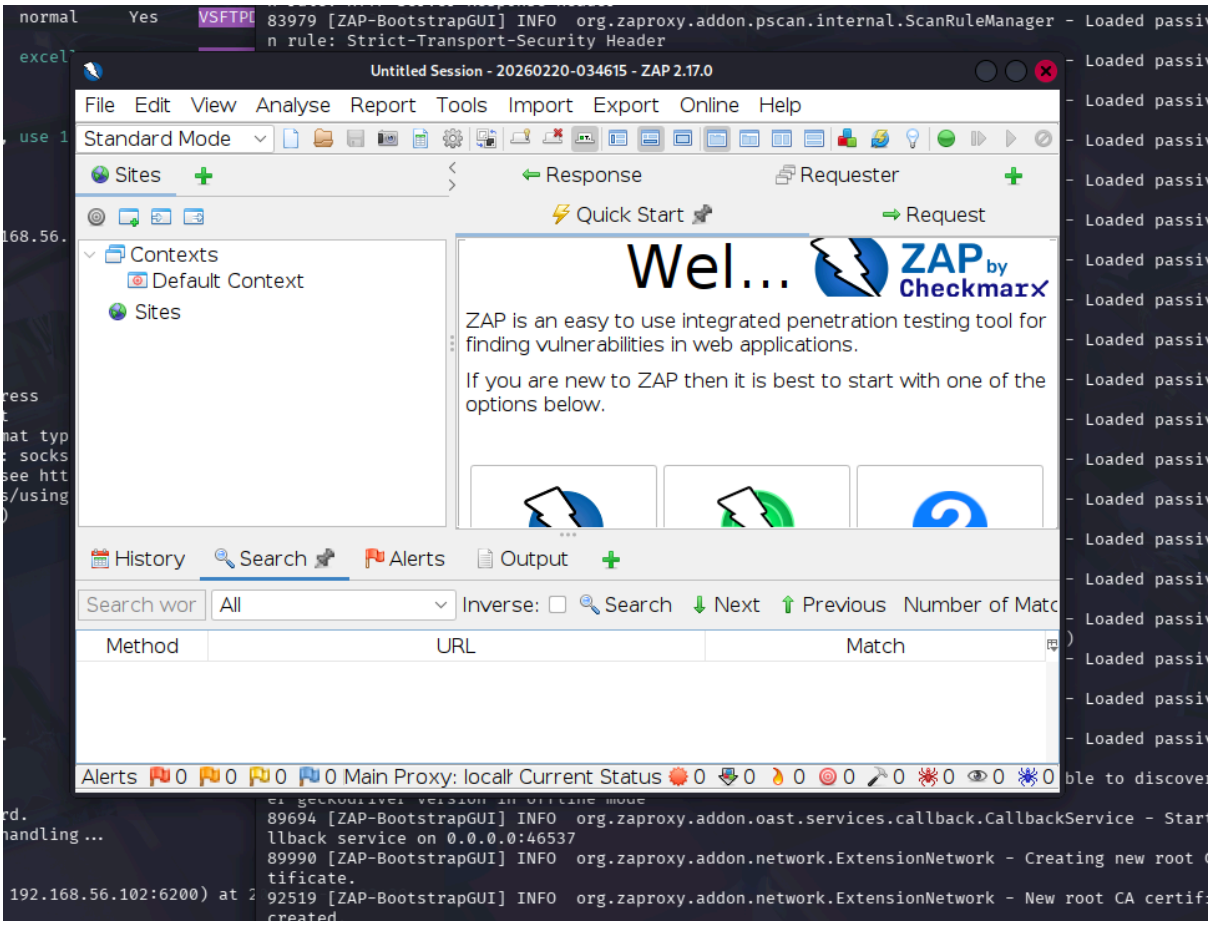
## ❖ Web Application Vulnerability Assessment Using OWASP ZAP

A web application security assessment was conducted using OWASP ZAP on the HTTP service running on the target system.



**Scan Type:**

- Passive Scan
- Active Scan




**Vulnerabilities Identified:**

| Risk Level | Vulnerability |
|---|---|
| High | Cross-Site Scripting (XSS) |

| | |
|---|---|
| Medium | Missing Security Headers |
| Medium | Directory Listing Enabled |
| Low | Cookies without HttpOnly Flag |

**Problem Faced:**

- Initial scan returned no vulnerabilities.

**Cause:**

- Incorrect target URL configuration.

**Solution:**

- Corrected the target URL and enabled active scanning.

## ❖ Impact Analysis

Successful exploitation resulted in:

- Complete system compromise
- Unauthorized root access

- Potential data theft and manipulation
- Service disruption (DoS)
- Web application exploitation

---

## ❖ Vulnerability Summary Table

| Vulnerability | CVE ID | CVSS Score | Description |
|---|---|---|---|
| vsFTPd Backdoor | CVE-2011-2523 | 10.0 | Unauthenticated root access |
| SSL POODLE | CVE-2014-3566 | 7.5 | SSL information disclosure |
| Slowloris DoS | CVE-2007-6750 | 7.8 | Denial of Service |
| XSS | N/A | 6.1 | Client-side script execution |

## Mitigation and Recommendations

1. Update and patch all outdated services
2. Disable insecure protocols such as FTP and Telnet
3. Use secure alternatives like SFTP and SSH
4. Apply firewall rules and IDS/IPS
5. Enforce strong authentication mechanisms
6. Regular vulnerability scanning and penetration testing
7. Implement secure HTTP headers

## Conclusion

This practical successfully demonstrated how insecure and outdated system configurations can lead to full system compromise. The exploitation of the vsFTPd 2.3.4 backdoor resulted in root-level access, highlighting the importance of regular patching, service hardening, and proactive security monitoring. The exercise reinforced real-world penetration testing methodologies and defensive best practices.

## Result

**The vulnerable system was successfully scanned, exploited, and analyzed, and appropriate remediation measures were recommended.**