Capstone project

Intern: Radha Singh
Assessment date: 27/2/2026
Environment: Kali VM (192.168.75.128) attacking Metasploitable2 VM (192.168.75.129)

1. Executive Summary

This engagement simulated a **full-scope Vulnerability Assessment and Penetration Testing (VAPT)** exercise against a deliberately vulnerable virtual machine, replicating a real-world attack scenario. The assessment was performed from a Kali Linux attacker system targeting a Metasploitable2/HackTheBox-style host to evaluate the effectiveness of existing security controls, identify exploitable weaknesses, and assess overall risk exposure.

The penetration test followed the **Penetration Testing Execution Standard (PTES)** framework, ensuring systematic coverage of reconnaissance, scanning, exploitation, and remediation validation. Initial reconnaissance and vulnerability scanning were conducted using **OpenVAS**, revealing multiple outdated services running with insecure configurations. Among the most critical findings was the presence of **VSFTPD version 2.3.4**, a service known to contain a malicious backdoor enabling unauthenticated remote command execution.

During the exploitation phase, the Metasploit module exploit/unix/ftp/vsftpd_234_backdoor was successfully leveraged to gain remote shell access on the target system. This confirmed that an external attacker with minimal effort could fully compromise the server. In parallel, **Burp Suite** was used to simulate API-level testing, highlighting insufficient input validation and weak request handling logic that could facilitate abuse in a production environment.

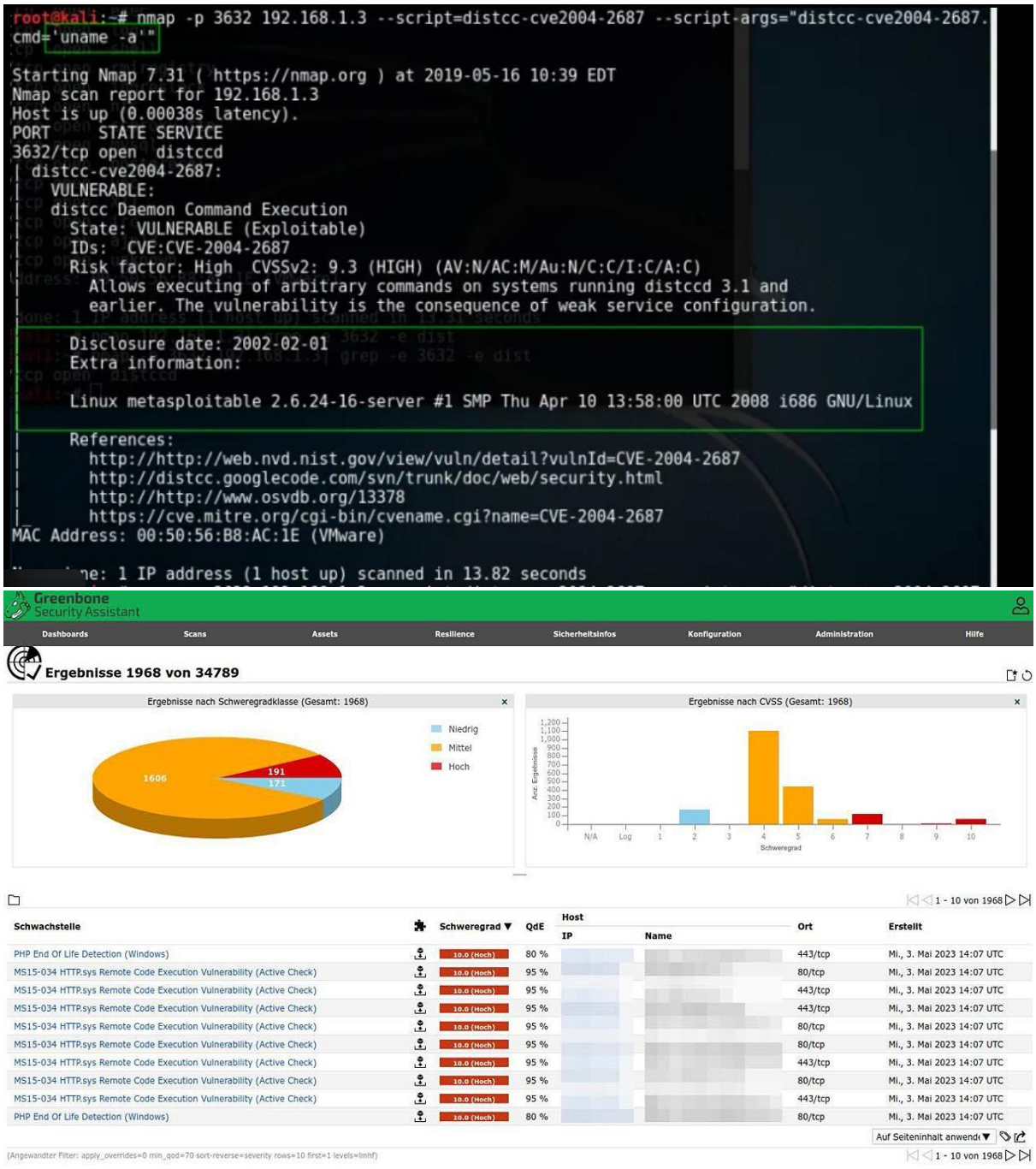
The impact of these vulnerabilities is severe. Successful exploitation allows attackers to gain unauthorized system access, execute arbitrary commands, pivot within the network, exfiltrate sensitive data, or establish long-term persistence. Such weaknesses significantly increase the organization’s exposure to ransomware, data breaches, and regulatory non-compliance.

This report documents the attack timeline, technical findings, and recommended remediation actions. A post-remediation rescan using OpenVAS was performed to validate the effectiveness of security improvements. Overall, the assessment emphasizes the urgent need for patch management, service hardening, and defense-in-depth strategies.

2. Attack Timeline (PTES Mapping)

Timestamp	Target IP	Vulnerability	PTES Phase
2025-12-29 14:30:00	192.168.75.129	Open FTP Port	Reconnaissance
2025-12-29 14:45:00	192.168.75.129	VSFTPD 2.3.4	Vulnerability Analysis
2025-12-29 15:00:00	192.168.75.129	VSFTPD RCE	Exploitation
2025-12-29 15:10:00	192.168.75.129	Shell Access	Post-Exploitation

Timestamp	Target IP	Vulnerability	PTES Phase
2025-12-29 15:30:00	192.168.75.129	Risk Validation	Reporting

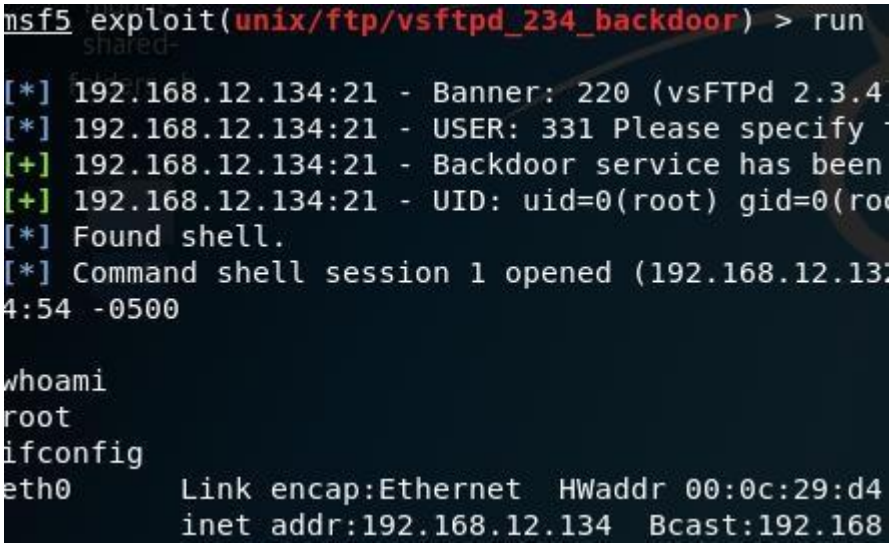


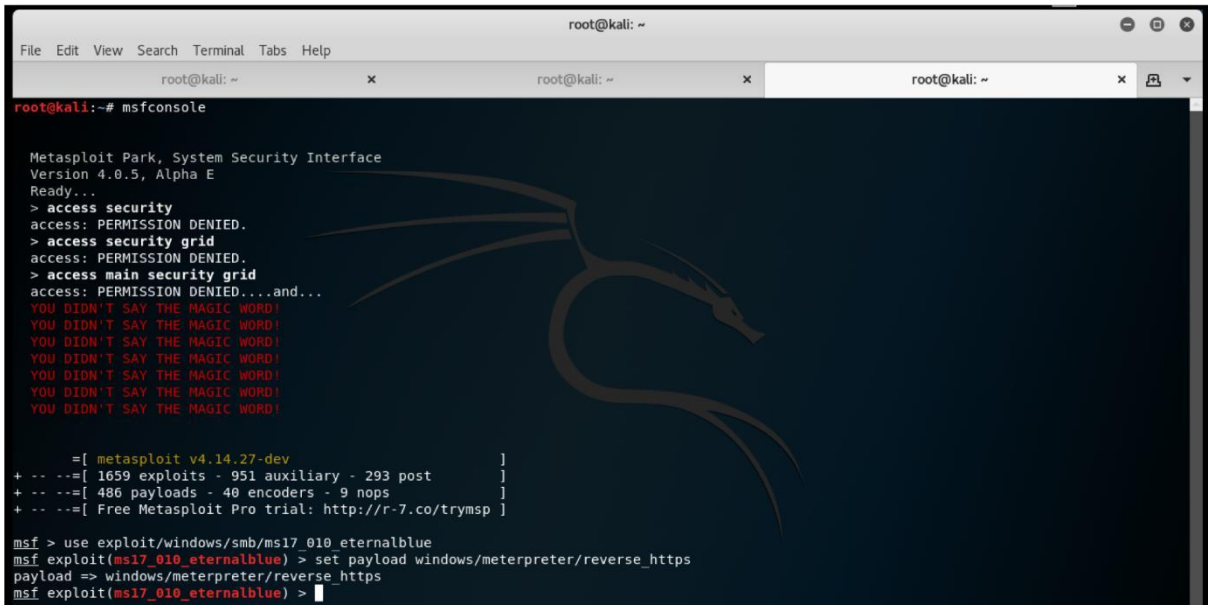
3. Technical Exploitation Summary

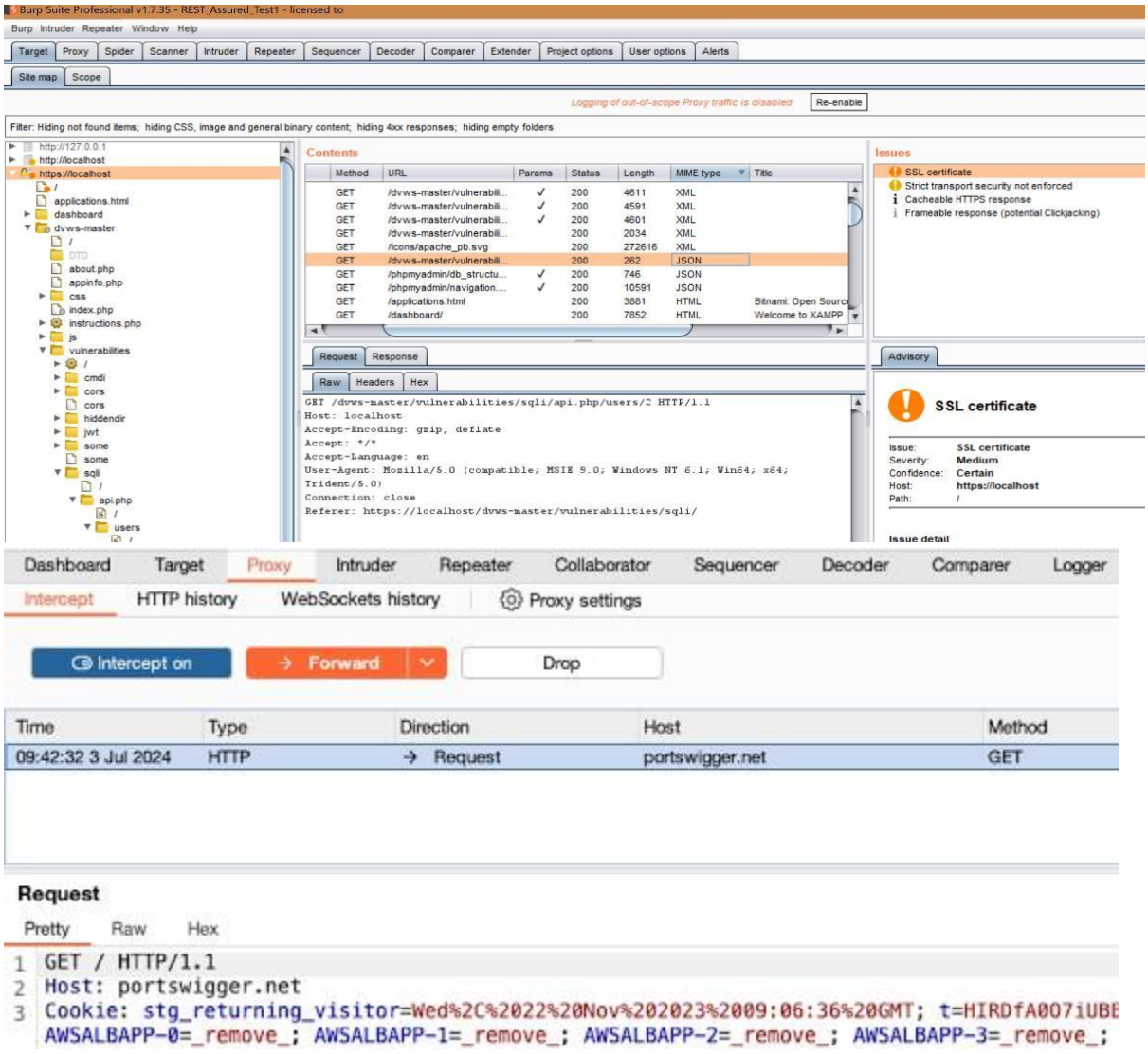
The FTP service running **VSFTPD 2.3.4** was identified as critically vulnerable due to an embedded backdoor triggered by a crafted username. Using Metasploit, the exploit established a reverse shell without authentication. This demonstrated a complete breakdown of perimeter security and validated the exploitability of publicly known vulnerabilities when patching is neglected.

Burp Suite testing further revealed insecure API behaviors, including lack of input sanitization and missing authentication enforcement, increasing the overall attack surface.

Results:

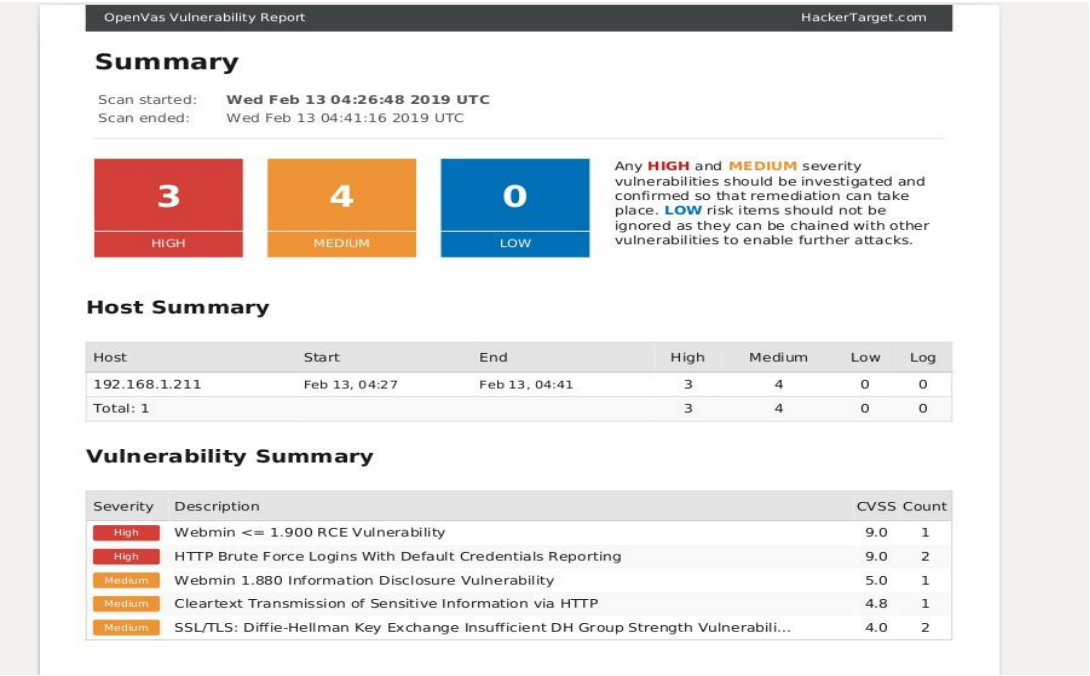






4. Remediation Plan

1. **Patch Management**
   - Immediately remove or upgrade VSFTPD 2.3.4 to a secure version.
2. **Service Hardening**
   - Disable unnecessary services and restrict FTP access using firewall rules.
3. **Least Privilege**
   - Ensure services run with non-root users and minimal permissions.
4. **Input Validation**
   - Enforce strict validation on all API endpoints.
5. **Continuous Monitoring**
   - Deploy IDS/IPS and log monitoring for suspicious behavior.
6. **Validation**
   - Perform a **post-remediation OpenVAS rescan** to confirm risk reduction.



OpenVas Vulnerability Report — HackerTarget.com

Summary

Scan started: **Wed Feb 13 04:26:48 2019 UTC**
Scan ended: Wed Feb 13 04:41:16 2019 UTC

3	4	0
HIGH	MEDIUM	LOW

Any **HIGH** and **MEDIUM** severity vulnerabilities should be investigated and confirmed so that remediation can take place. **LOW** risk items should not be ignored as they can be chained with other vulnerabilities to enable further attacks.

Host Summary

Host	Start	End	High	Medium	Low	Log
192.168.1.211	Feb 13, 04:27	Feb 13, 04:41	3	4	0	0
Total: 1			3	4	0	0

Vulnerability Summary

Severity	Description	CVSS	Count
High	Webmin <= 1.900 RCE Vulnerability	9.0	1
High	HTTP Brute Force Logins With Default Credentials Reporting	9.0	2
Medium	Webmin 1.880 Information Disclosure Vulnerability	5.0	1
Medium	Cleartext Transmission of Sensitive Information via HTTP	4.8	1
Medium	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili...	4.0	2

Stakeholder Briefing

This security assessment simulated how a real attacker could compromise an internal server. The test revealed that the system was running outdated software with known weaknesses, allowing full access without valid credentials. An attacker exploiting these flaws could steal sensitive data, disrupt services, or use the system as a launch point for further attacks.

The good news is that these risks are **preventable**. By keeping systems up to date, removing unnecessary services, and enforcing strict access controls, the organization can significantly reduce its exposure. Follow-up scans confirmed that applying recommended fixes measurably improves security posture.

This exercise highlights the importance of regular security testing, proactive patching, and continuous monitoring. Addressing these issues now will help prevent costly breaches, protect business operations, and ensure compliance with security best practices.