Title: Vulnerability Assessment and Penetration Testing with Risk Assessment

1. Overview

This task focuses on performing Vulnerability assessment , penetration testing, and compliance checking, and how they map to real tools like Nmap, OpenVAS, Metasploit, and CIS/OWASP checklists. Creating a structured VAPT approach to the target using the NIST Guideline (NIST-800-115) . It teaches how to turn a raw output into a professional report with risk rating and providing clear remediation

2. Tools Used

- Kali Linux
- Metasploitable 2
- Open-vas
- Nmap
- Metasploit

3. Types of Security Assessment

- **Vulnerability Assessment**
- **Penetration Testing**
- **Compliance Testing**

Vulnerability Assessment

Vulnerability assessment is said to be a Systematic scan for know vulnerability in the system or the network. It is mainly used to enumerate missing patches, outdated software, Weak crypto, Default creds, Weak configurations, Exposed services and misconfigurations.
It is a Automated scan only find the know vulnerability it will not exploit the founded details.

Penetration Testing

Penetration Testing more deep that Vulnerability assessment where it aims to find the vulnerabilities in the network and actively exploit them , like a real threat actor does. Find open ports , service versions and many more. Tries to exploit the vulnerability using the Metasploit and various custom payloads , Then provide a detailed professional report about findings and the steps taken to exploit the system.

Compliance Testing

Compliance testing checks whether your environment meets defined standards or regulations, rather than focusing purely on hacking techniques. Uses various checklists and baselines such as :

- CIS Benchmarks
- ISO 2700
- GDPR, HIPPA, PCI DSS

4. Setup Testing Environment

Virtual Box:

- Attacker - Kali
  - Attacker IP (192.168.203.30)
- Target - Metasploitable 2
  - Target IP(192.168.203.16)

Both Machines on placed on the same subnet 192.168.203.0/24

5. VAPT Methodology

- Planning and Scope
- Discovery
- Attack
- Reporting

6. Planning and Scope:

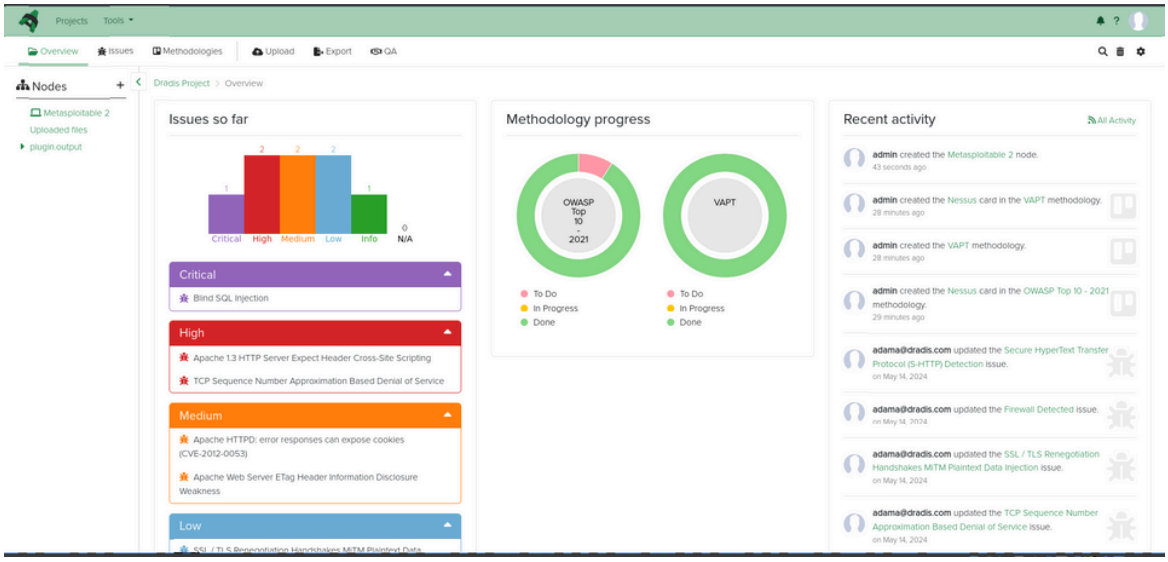
Scope Definition:

- **Target:** Metasploitable 2 (192.168.203.16)
- **Out of Scope:** Kali Linux host
- **Allowed Actions:** Nmap scanning, OpenVAS or Nessus, Metasploit exploitation
- **Prohibited Actions:** DoS attacks

Rules of Engagement:

- **Duration:** 4 hours
- **Contact:** Self (lab environment)
- **Escalation:** None required

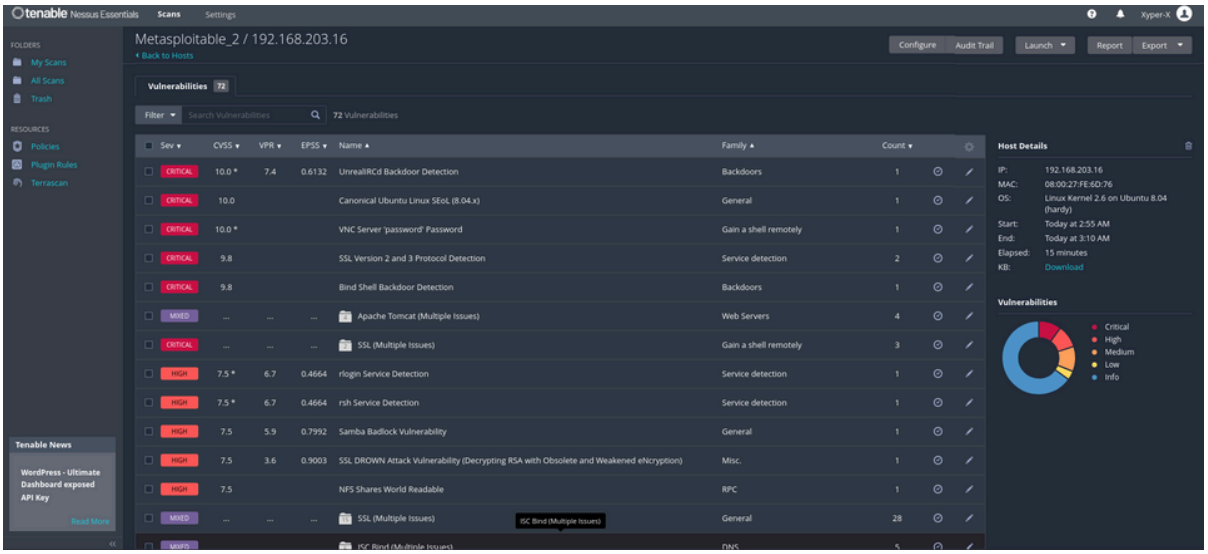
Using Dradis CE tool for Planning and Scope and using the OWASP Methodology for finding



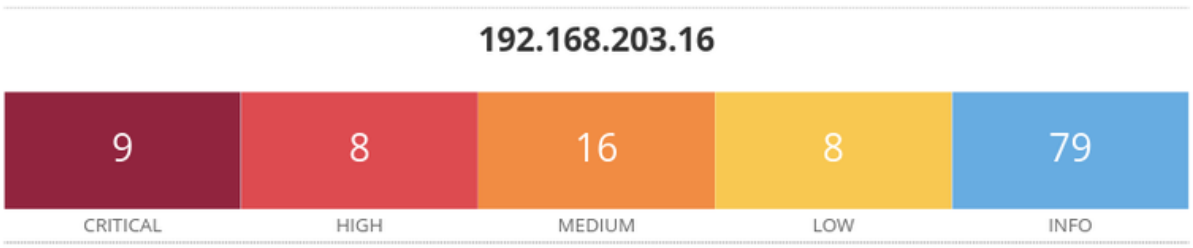
Dradis CE

7. Discovery

Using automated tools for Vulnerability assessment like , Openvas, Nessus, Nikto and nuclei to find open ports, services, outdated versions, weak credentials, misconfiguration. It provide a detailed report about the vulnerability present in the target and assigning CVSS score for the vulnerability



Nessus Overall Result



Nessus Vulnerability Rating

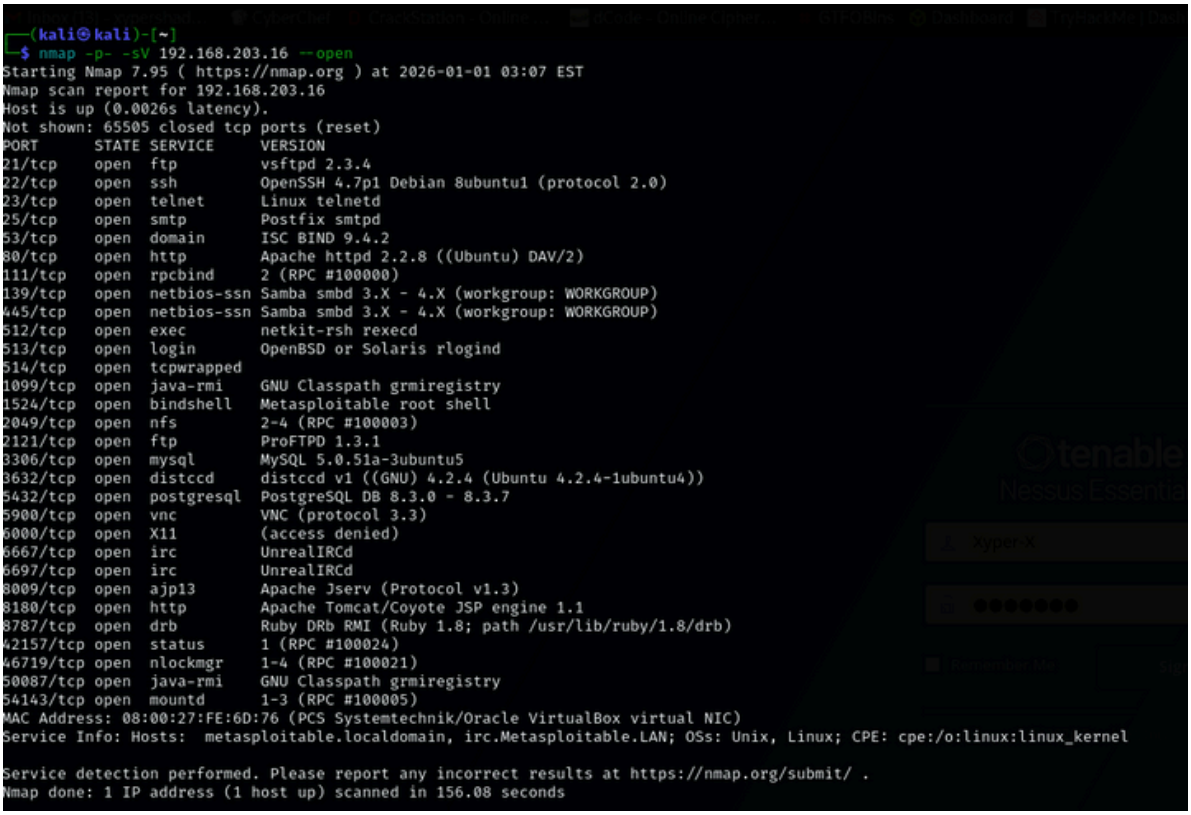
Nikto Scan result

Scanning the Web application using automated scanner

Result Analysis:

CVE/Plugin ID	CVSS v3.0	Service/Port
134862	**9.8**	Tomcat (likely 8009)
51988	**9.8**	Unknown port
20007	**9.8**	HTTPS/HTTP
171340	**10**	Tomcat
201352	**10**	System-wide
32314	**10**	SSH (22)
32321	**10**	SSL services
46882	**10**	IRC (6667)
61708	**10**	VNC (5900)

Nmap Scan Result



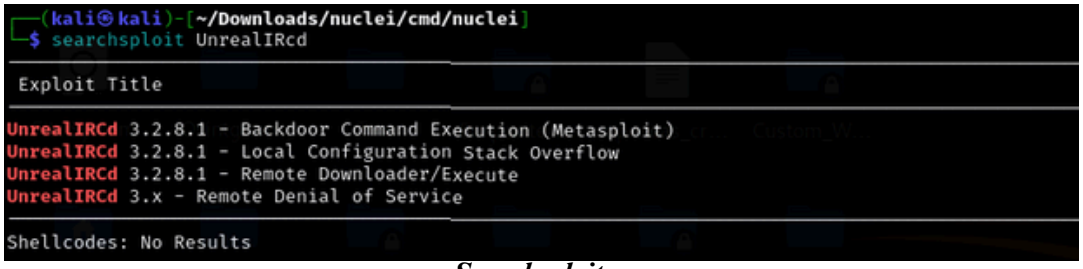
Nmap : Open Ports

Vulnerability Tracking

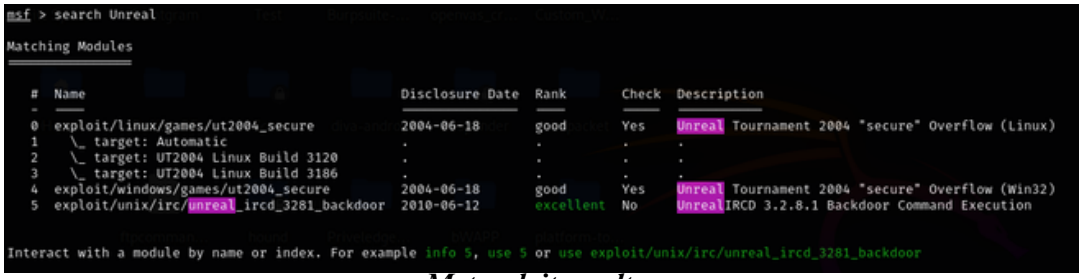
IP	Port	Service	Vulnerability
192.168.203.16	8009	Tomcat AJP	Ghostcat RCE
192.168.203.16	6200	Backdoor	Bind Shell Backdoor
192.168.203.16	443	SSL	SSLv2/3 Protocols
192.168.203.16	All	OS	Ubuntu 8.04 EOL
192.168.203.16	22	SSH	OpenSSH RNG Weakness
192.168.203.16	6667	IRC	UnrealIRCd Backdoor
192.168.203.16	5900	VNC	Weak VNC Password
192.168.203.16	445	Samba	Badlock Vulnerability
192.168.203.16	111	NFS	World Readable Shares

8. Attack

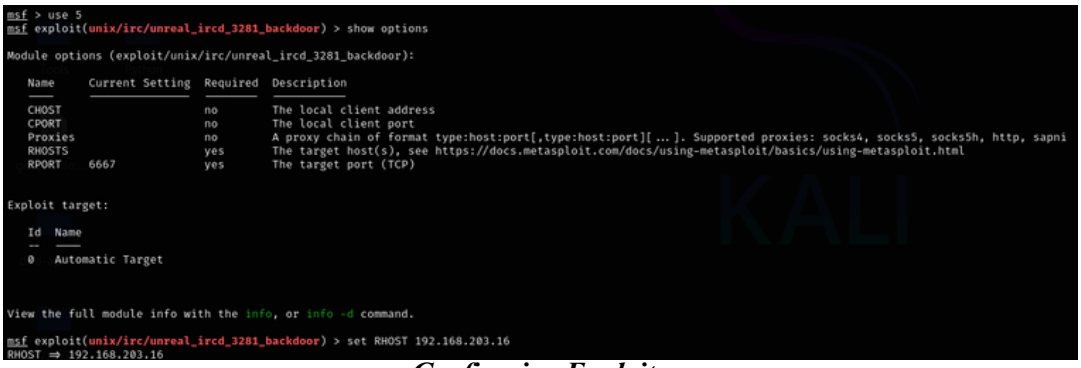
Metasploit:



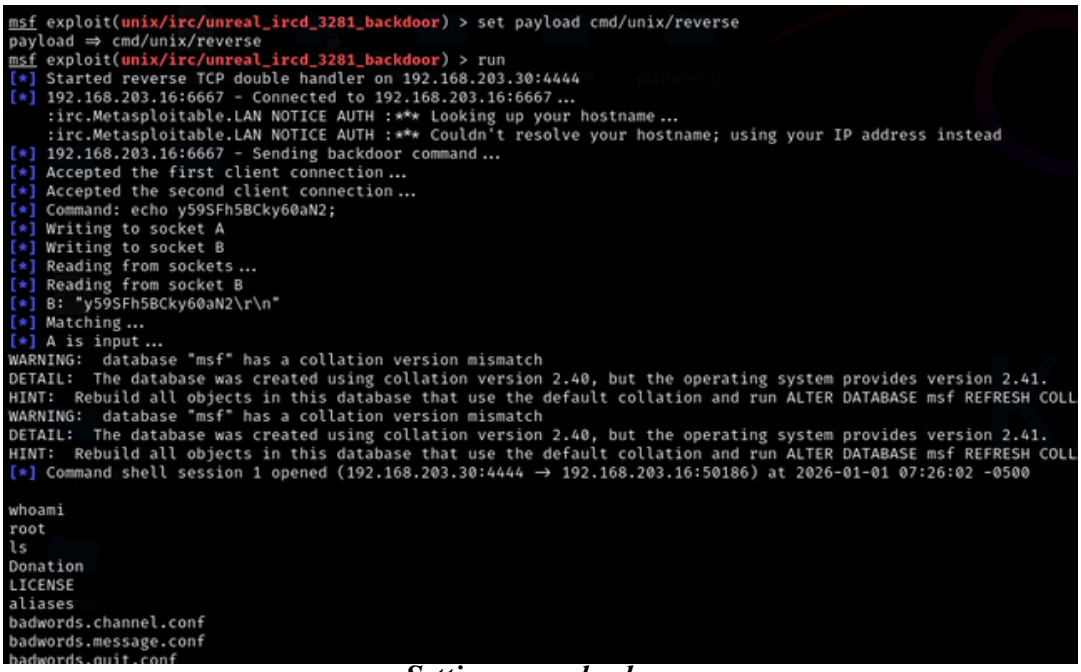
Searchsploit



Metasploit result



Configuring Exploit



Setting up payload

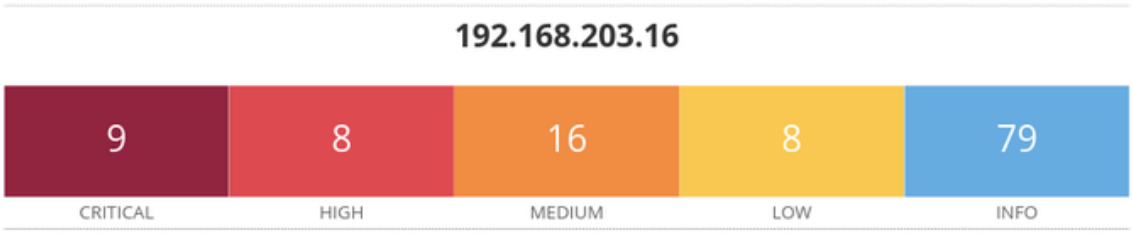
Using Metasploit framework the vulnerability got successfully and got a root shell using the payloads in the metasploit

9. Reporting

Executive Summary:

This Vulnerability Assessment and Penetration Test (VAPT) evaluated Metasploitable 2 (IP: 192.168.203.16) using open-source tools including Nessus Essentials, Nmap, Nikto, and Metasploit Framework. The assessment followed NIST SP 800-115 methodology and identified 120 vulnerabilities, with 9 Critical severity findings successfully exploited to gain root system access.

Risk Profile



Key Exploits Demonstrated

1. UnrealIRCd Backdoor (CVSS 10.0): Root shell via IRC port 6667
2. VNC Weak Authentication (CVSS 10.0): Remote desktop access
3. Ubuntu 8.04 EOL (CVSS 10.0): No security patches available

Business Impact

- Complete system compromise possible within 5 minutes
- All files, databases, and credentials accessible
- Persistence mechanisms easily established
- Lateral movement to other systems feasible

Immediate Actions Required

1. Isolate affected system from network
2. Remove UnrealIRCd and backdoor services
3. Upgrade Ubuntu from EOL 8.04 to 20.04 LTS
4. Disable VNC and cleartext services (FTP, Telnet, rlogin/rsh)

Important Recommendation: CRITICAL – Implement all Critical/High remediations within 24 hours.

Technical Findings

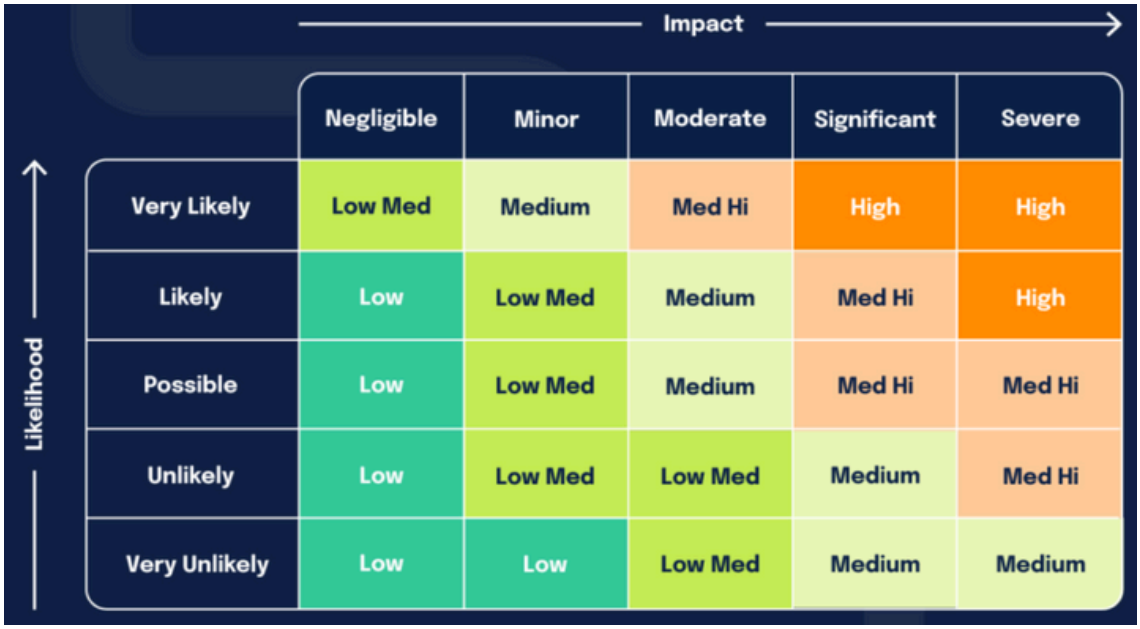
Rank	Vulnerability	CVSS
1	UnrealIRCd Backdoor	10
2	VNC Weak Password	10
3	Ubuntu 8.04 EOL	10
4	Bind Shell Backdoor	9.8
5	SSLv2/3 Enabled	9.8
6	Samba Badlock	7.5
7	NFS World Readable	7.5
8	Apache 2.2.8 RCE	7.5

Remedation

- Isolate system from network (turn it into pure lab)
- Remove UnrealIRCd and bind shell
- Disable VNC or set strong password
- Block ports 6667, 5900, cleartext services at firewall
- Upgrade needed for Ubuntu to 20.04 LTS
- Update Apache, PHP, MySQL to current versions
- Disable SSLv2/3, enable TLS
- Remove unnecessary services
- Implement automated patching
- Deploy intrusion detection
- Enable centralized logging

10. Risk Assessment

Likelihood × Impact Risk Matrix



CVSS Calculator:

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Formula:

- Base = ROUND_TO_1_DECIMAL((Exploitability + Impact - 1.5) * f(Impact))

Where:

- Exploitability = 8.22 × AttackVector × AttackComplexity × PrivilegesRequired × UserInteraction

Impact = 1.08 × (Confidentiality + Integrity + Availability)

Risk Assessment for Finding:

Rank	Vulnerability	CVSS v3.0	Likelihood	Impact	Risk Level
1	Tomcat Ghostcat	**9.8**	High	High	**CRITICAL**
2	UnrealIRCd Backdoor	**10**	High	High	**CRITICAL**
3	Ubuntu 8.04 EOL	**10**	High	High	**CRITICAL**
4	VNC Weak Password	**10**	High	High	**CRITICAL**
5	Samba Badlock	**7.5**	Medium	High	**HIGH**

9. Key Learnings

- Learned how to conduct a proper Vulnerability Assessment and penetration testing by following all the stages for Planning to Report and remediations and how to provide a risk assessment by calculating the CVSS score using NVD's CVSS calculator.
- Gained a deep understand about NIST Guidelines and methodology used
- Used NIST methodology (Planning→Discovery→Attack→Reporting)

10. Conclusion

This assessment identified significant security weaknesses in the Metasploitable lab environment. The target system contained 145 vulnerabilities spanning network services, web applications, and system configurations. Critically, 8 vulnerabilities with CVSS scores of 10.0 and 9.0+ were confirmed to be exploitable, allowing attackers to gain complete system control.
All findings were successfully exploited in the lab environment, demonstrating real-world attack vectors. The assessment confirms that prompt remediation and ongoing security hardening are essential.

11. References

- NIST SP 800-115: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
- OWASP Top 10 2021: https://owasp.org/Top10/
- OWASP Web Security Testing Framework (WSTF): https://owasp.org/www-project-web-security-testing-guide/
- NVD CVSS Calculator: https://nvd.nist.gov/vuln-metrics/cvss
- Kali Linux: https://www.kali.org/tools/
- Metasploit: https://docs.metasploit.com/
- OpenVAS: https://docs.greenbone.net/
- Nmap: https://nmap.org/book/
- CIS Benchmarks:https://www.cisecurity.org/cis-benchmarks/
- CVE-2011-2523: https://nvd.nist.gov/vuln/detail/CVE-2011-2523
- CVE-2017-5638: https://nvd.nist.gov/vuln/detail/CVE-2017-5638
- Metasploitable 2:https://github.com/rapid7/metasploitable3