Vulnerability Assessment and Penetration Testing (VAPT) Report

Client: X Company
Consultant: [Your Name]
Date: [Insert Date]

1. Executive Summary

This Vulnerability Assessment and Penetration Test (VAPT) was conducted on two company-owned servers — Venus and Napping — hosted in a controlled VulnHub environment. The objective was to identify exploitable vulnerabilities, simulate real-world attacks, and assess the resilience of the systems against unauthorized access. Both systems were found to contain multiple critical vulnerabilities, including: - Use of default/weak credentials. - Insecure web application design (input handling & authentication flaws). - Sensitive information disclosure (encoded credentials in traffic). - Privilege escalation vulnerabilities (CVE-2021-4034 Polkit, misconfigured sudo). Overall Risk Rating: Critical – Immediate remediation required.

2. Scope of Engagement

Systems Tested: - Venus (VulnHub) - Napping (VulnHub) IP Addresses: Discovered via local network reconnaissance. Testing Period: [Insert Dates] Testing Type: Internal Black-Box Penetration Test. Tools Used: - nmap - netdiscover / arp-scan - gobuster - Burp Suite - Hydra - CyberChef - LinPEAS - CVE exploit scripts (CVE-2021-4034) - SSH client - netcat

3. Methodology

Testing followed a hybrid approach combining OWASP Testing Methodology and PTES phases: 1. Reconnaissance – Network scanning & service enumeration using netdiscover, nmap. 2. Enumeration – Directory brute-forcing (gobuster), credential interception, traffic analysis. 3. Exploitation – Login bypass, brute force attacks (hydra), decoding credentials, exploiting CVEs. 4. Privilege Escalation – Local enumeration (linpeas), misconfigured sudo, CVE exploitation. 5. Post-Exploitation – Accessing flags, persistence tests. 6. Reporting – Documenting vulnerabilities, risks, and remediation recommendations.

4. Vulnerability Findings

Venus – Key Vulnerabilities

#	Vulnerability	Severity	Description	Recommendation
1	Default credentials	Critical	Weak/default passwords allowed initial access.	Implement strong password policy, disable d
2	Encoded credentials in HTTP traffic	High	BurpSuite revealed Base64/ROT13-encoded passwords.	Use salted hashing for password storage, en
3	CVE-2021-4034 (Polkit)	Critical	Local privilege escalation to root.	Patch Polkit to latest version, restrict shell ac

Napping – Key Vulnerabilities

#	Vulnerability	Severity	Description	Recommendation
1	Default credentials during signup	High	Weak account creation process without restrictions.	Implement account lockout policy and passw
2	Reverse shell via malicious HTML payload	High	JavaScript payload redirected victim to attacker's server.	Sanitize user input and disable unsafe HTML
3	Misconfigured sudo allowing virtual shell escape	Critical	sudo /usr/bin/vim -c ':!/bin/sh' granted root.	Restrict sudo permissions and monitor user c

5. Remediation Recommendations

For Both Servers: - Change all default credentials immediately. - Enforce password complexity and rotation policies. - Apply latest security patches for OS and software packages. - Limit user privileges following the principle of least privilege. - Monitor authentication logs for suspicious activity. Specific to Venus: - Patch Polkit (CVE-2021-4034). - Avoid storing or transmitting passwords in reversible encoding. Specific to Napping: - Restrict sudo permissions. - Sanitize all HTML/JavaScript inputs. - Disable execution of system commands from text editors.

6. Conclusion

The assessment revealed multiple high-risk vulnerabilities in both Venus and Napping servers. Exploitation allowed full compromise of both systems, including root-level access, representing a complete breach scenario. Immediate remediation is necessary before deployment into a production environment.