Finalized Penetration Test Report (for DC-1)

Penetration Testing Report

Target: DC-1 (Vulnerable CTF Machine)
Tester: Elebe Kehinde (kenny@kali)
Date: April 27, 2025

Executive Summary

This penetration test focused on identifying and exploiting vulnerabilities within the DC-1 machine.
The assessment revealed critical security flaws that allowed an unauthenticated attacker to execute remote code and escalate privileges to full administrative (root) control of the system.

The primary risks identified were:

- Remote Code Execution via Drupal CMS ("Drupalgeddon2" vulnerability).
- Privilege Escalation via SUID misconfiguration on /usr/bin/find.

Immediate corrective actions are strongly recommended to secure the system.

2.0 Methodology

Phase	Description
Reconnaissance	Network discovery using Nmap scanning.
Enumeration	Service identification and version fingerprinting.
Vulnerability Analysis	Mapped identified services against known vulnerabilities.
Exploitation	Gained unauthorized access through Drupalgeddon2.
Privilege Escalation	Leveraged SUID misconfigurations for root access.
Post-Exploitation	System enumeration and data exfiltration simulation.

3.0 Findings

3.1. Critical Finding: Remote Code Execution (Drupalgeddon2)

- **CVE-ID:** CVE-2018-7600
- **Affected Service:** Drupal 7.x CMS
- **Risk Level:** Critical
- **Impact:** Full remote code execution without authentication.

Proof of Concept:

- Exploited via Metasploit module exploit/unix/webapp/drupal_drupalgeddon2.
- Achieved a Meterpreter shell as www-data.

3.2. Critical Finding: Local Privilege Escalation via SUID Binary

- **Vulnerability:** Misconfigured SUID on /usr/bin/find
- **Risk Level:** High
- **Impact:** Local privilege escalation to root.

Proof of Concept:

- Ran find . -exec /bin/sh \; -quit.
- Elevated privileges from www-data to root.

4. Recommendations

Vulnerability	Recommended Fix
Drupalgeddon2	Update Drupal CMS to latest supported version and apply security patches immediately. Implement Web Application Firewall (WAF) protections.
SUID Misconfiguration	Remove unnecessary SUID bits using chmod u-s /usr/bin/find. Conduct regular file permissions audits.
General Hardening	Enforce least privilege principle. Monitor and audit user activity. Apply continuous vulnerability management.

5. Conclusion

The vulnerabilities discovered pose a severe risk to system confidentiality, integrity, and availability.
Without proper remediation, an attacker could fully compromise the DC-1 server and pivot to additional assets.

Urgent action is recommended to patch identified issues, reconfigure system permissions, and enhance network defenses.

6. Appendix (Screenshots and Logs)

- Nmap Host Discovery and Port Scan
- Drupalgeddon2 Exploit Logs
- Meterpreter Session Capture
- Root Shell Validation (whoami, id)
- Dumped /etc/shadow (optional if performed)