# Metasploitable2 Vulnerability Assessment & Exploitation

Penetration Testing Case Study

*Completed as part of a penetration testing subject during my Bachelor of Cybersecurity, La Trobe University*

## Overview

This project documents a full vulnerability assessment and exploitation exercise performed against Metasploitable2, an intentionally vulnerable Linux target, in an isolated virtual lab. The engagement covers reconnaissance, service enumeration, web application scanning, vulnerability prioritisation, multi-vector exploitation, persistence, and password cracking, demonstrating the complete offensive security lifecycle from initial scan to full system compromise.

## Objectives

- Enumerate all open services and identify the target's attack surface using Nmap and Nikto
- Prioritise discovered vulnerabilities using CVSS scoring and public exploit availability
- Exploit the target via multiple independent attack paths to demonstrate real-world attacker methodology
- Establish persistence on the compromised host
- Recover plaintext credentials from captured password hashes

## Lab Environment

Kali Linux was used as the attacking machine against Metasploitable2 (10.0.2.3), an intentionally vulnerable Linux 2.6.9–2.6.33 target running Samba 3.0.20-Debian and a wide range of outdated, exploitable services. All testing was conducted in an isolated virtual lab on personal hardware.

## Phase 1: Reconnaissance & Service Enumeration (Nmap)

A full Nmap port scan was run against the target to map its complete attack surface before any exploitation was attempted.

*Figure 1a — Nmap scan showing open ports including FTP (21), SSH (22), Telnet (23), SMTP (25), DNS (53), and HTTP/Apache 2.2.8 (80)*

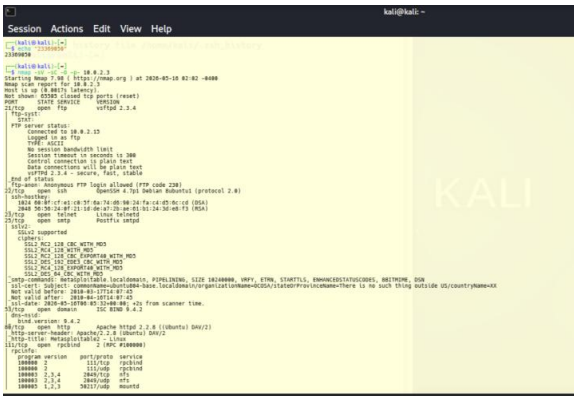



*Figure 1b — Additional open ports identified: Samba (139/445), bindshell (1524), MySQL (3306), distccd (3632), VNC (5900), UnrealIRCd (6667), Apache Tomcat (8180)*


*Figure 1c — OS fingerprinting confirming Linux 2.6.9–2.6.33 running Samba 3.0.20-Debian*


The scan revealed an unusually large attack surface for a single host  a mix of legacy, end-of-life services with well-documented public exploits, several of which are exploitable without authentication.

## Phase 2: Web Application Scanning (Nikto)

Nikto was used to assess the web services running on port 80 and to enumerate the DVWA (Damn Vulnerable Web Application) instance hosted on the target.

*Figure 2 — Nikto scan against port 80 identifying Apache 2.2.8, PHP 5.2.4, HTTP TRACE, phpMyAdmin exposure, and directory indexing*

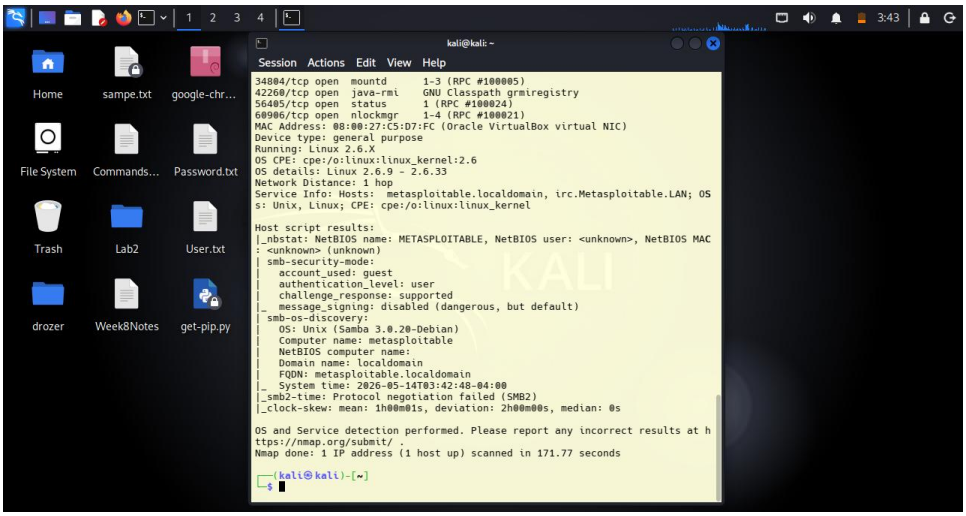



*Figure 3 — Nikto scan against DVWA confirming CVE-2012-1823 (PHP remote code execution) and CVE-2014-3704 (SQL injection)*

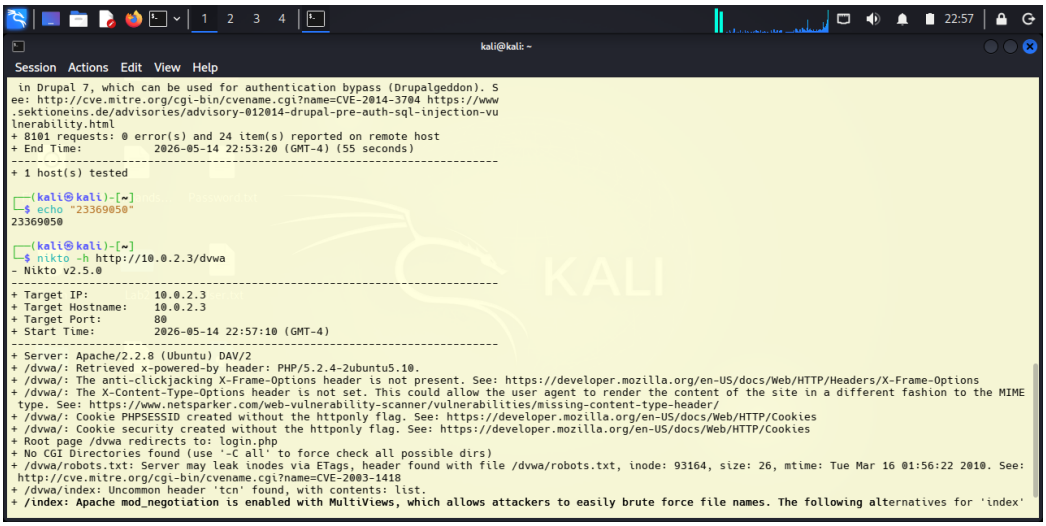
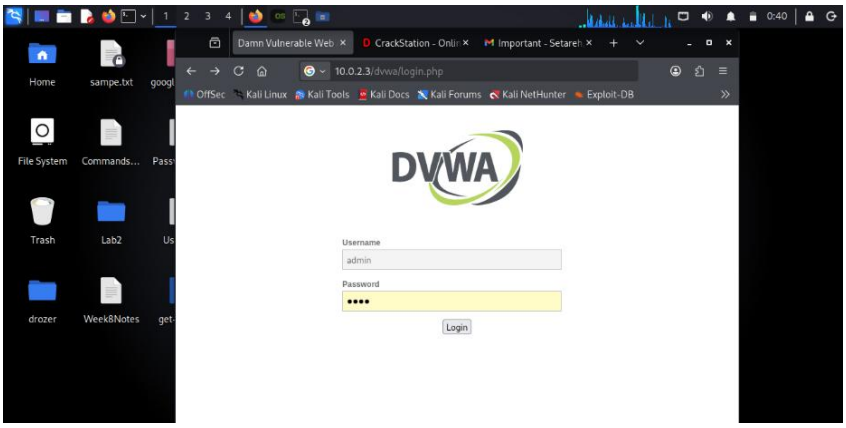



*Figure 4 — Additional DVWA findings: directory indexing on /dvwa/config/ and an exposed admin login page*




Nikto identified multiple web application misconfigurations layered on top of the already vulnerable network services, including security misconfiguration (HTTP TRACE enabled, phpinfo.php exposed), broken access control (directory indexing), cryptographic failures (SSLv2 enabled, cookies missing the HttpOnly flag), and SQL injection.

## Phase 3 — Vulnerability Prioritisation & Risk Register

Every service identified during recon was cross-referenced against known CVEs and scored by CVSS severity and public exploit availability to decide which vulnerabilities to pursue first.

| # | Service | Port | CVE ID | Description | CVSS | Public Exploit |
|---|---|---|---|---|---|---|
| 1 | vsftpd 2.3.4 | 21 | CVE-2011-2523 | Backdoor command execution | 10.0 | Yes — Metasploit |
| 2 | Samba 3.0.20 | 445 | CVE-2007-2447 | Remote command execution | 10.0 | Yes — Metasploit |
| 3 | Apache 2.2.8 | 80 | CVE-2017-7679 | Buffer overflow | 9.8 | Yes — Exploit-DB |
| 4 | distccd | 3632 | CVE-2004-2687 | Remote command execution | 9.3 | Yes — Metasploit |
| 5 | UnrealIRCd | 6667 | CVE-2010-2075 | Backdoor command execution | 7.5 | Yes — Metasploit |
| 6 | PHP 5.2.4 | 80 | CVE-2012-1823 | Remote code execution | 7.5 | Yes — Exploit-DB |
| 7 | OpenSSH 4.7p1 | 22 | CVE-2008-0166 | Weak key generation | 7.8 | Yes — Exploit-DB |
| 8 | MySQL 5.0.51a | 3306 | CVE-2008-0226 | Remote code execution | 7.5 | Yes — Exploit-DB |

### Risk Posture Analysis

Overall posture: very poor — the environment runs multiple end-of-life services with public exploits, default credentials, and no meaningful access controls.

Greatest attack paths: the vsftpd 2.3.4 backdoor (CVE-2011-2523) on port 21 and the Samba 3.0.20 vulnerability (CVE-2007-2447) on port 445 both allow unauthenticated remote code execution via a single Metasploit module — no prior access required.

Vulnerability chaining: these flaws could be chained to achieve full compromise:

- Gain initial access via the vsftpd 2.3.4 backdoor on port 21
- Enumerate the system to identify further services
- Access phpMyAdmin using default credentials to extract database contents
- Escalate to root using the distccd vulnerability
- Establish persistence via the root bindshell already listening on port 1524

Notably, port 1524 has a root shell listening by default — meaning full compromise is achievable simply by connecting to it, without exploiting a single CVE.

## Phase 4: Exploitation

### Method 1: PHP CGI Argument Injection

The php_cgi_arg_injection exploit was used to gain a Meterpreter session on the target.

*Figure 5 — Nmap scan confirming Metasploitable2 OS and multiple vulnerable services*

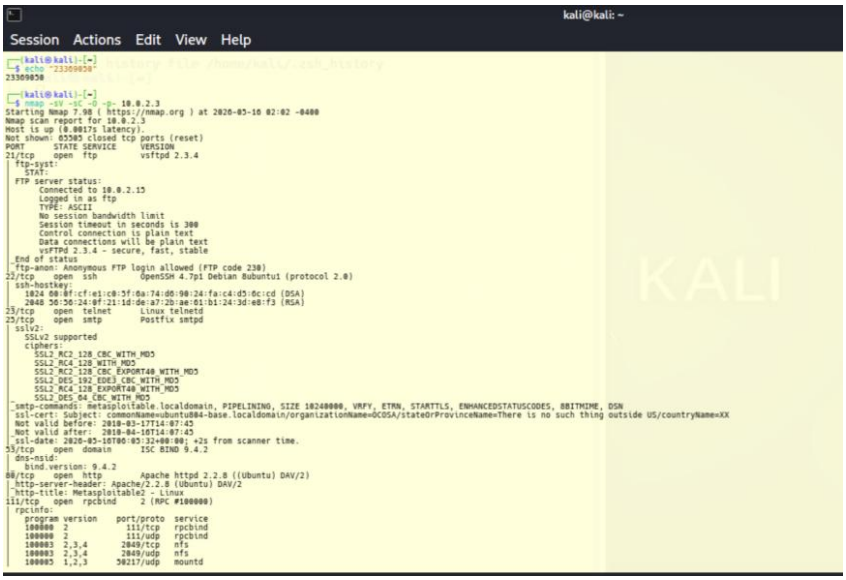
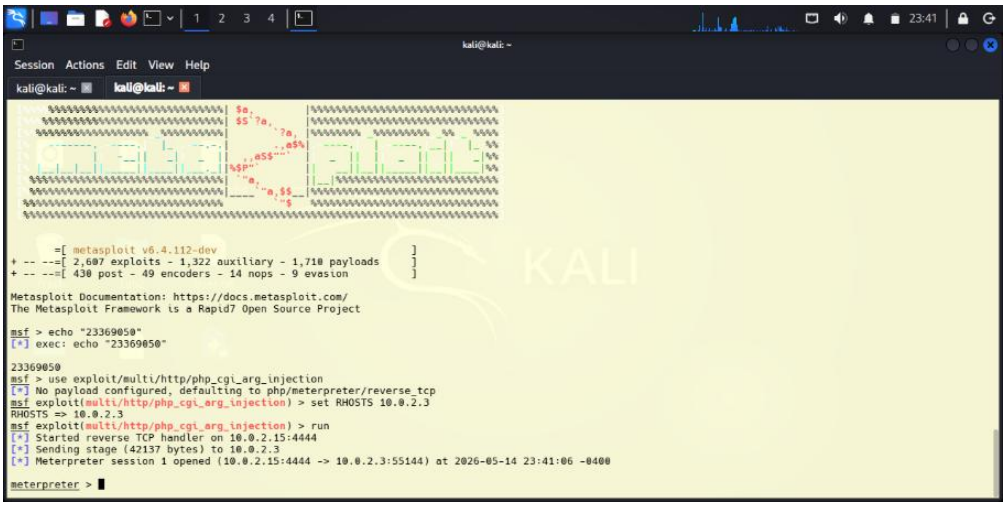


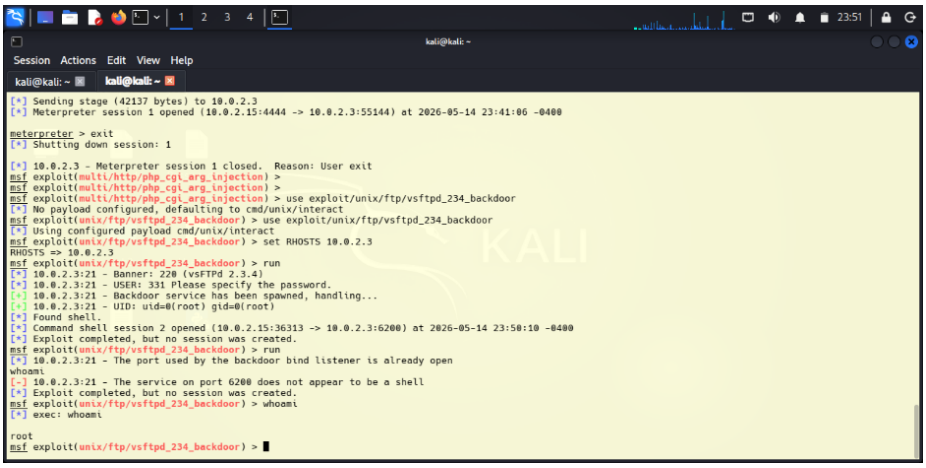

*Figure 6 — PHP CGI argument injection exploit successfully opens a Meterpreter session on 10.0.2.3*




### Method 2: vsftpd 2.3.4 Backdoor

The vsftpd 2.3.4 backdoor (CVE-2011-2523) was exploited independently to obtain root access.

*Figure 7 — vsftpd 2.3.4 backdoor exploit successfully executed, confirming root access (whoami / uid=0(root) gid=0(root))*




## Phase 5: Persistence

With root access confirmed, a backdoor account was created and log evidence was cleared to demonstrate a full post-exploitation persistence workflow.

*Figure 8 — Backdoor account created via useradd, password set, auth.log and syslog cleared*

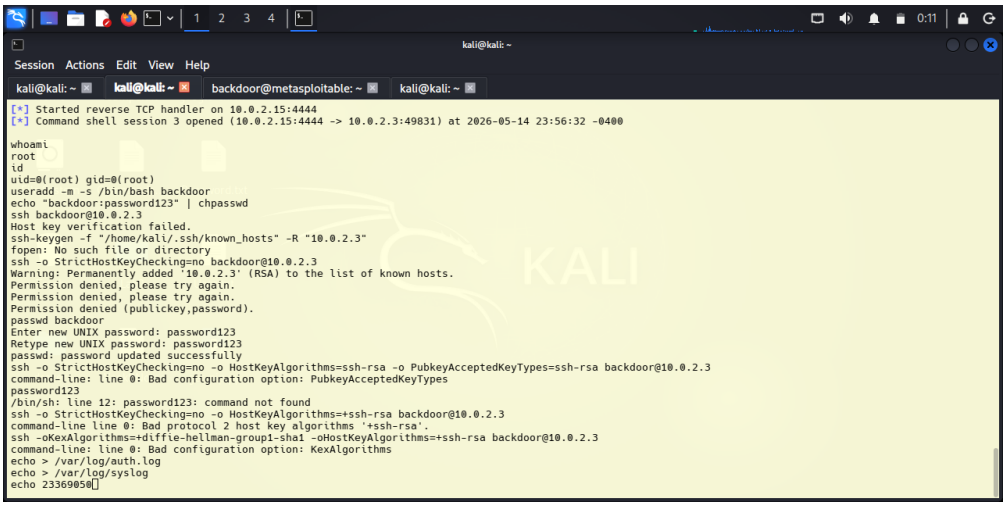
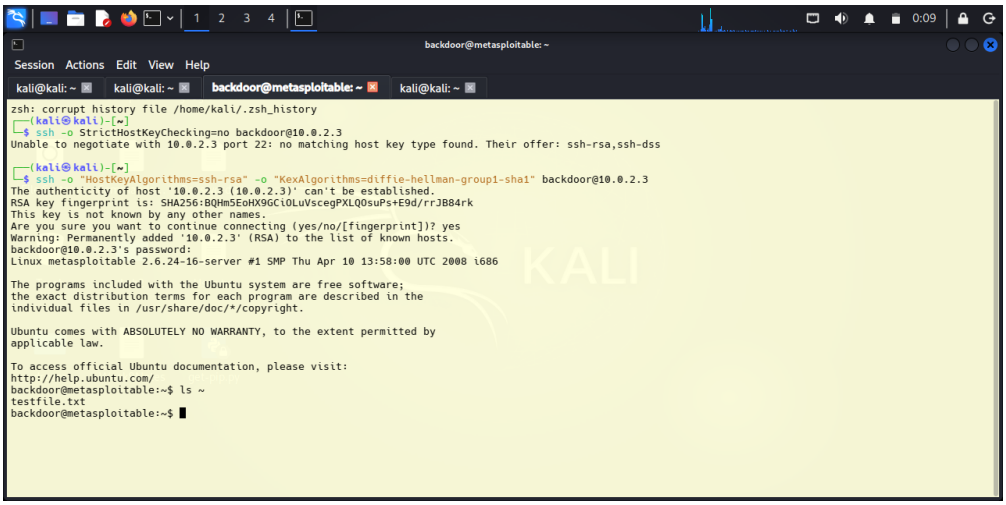



*Figure 9 — Successful SSH login to Metasploitable2 as the backdoor user from the Kali attack machine*


*Figure 10 — testfile.txt successfully transferred from Kali to Metasploitable2, confirmed in the backdoor user's home directory*




## Phase 6: Password Cracking (Ophcrack & CrackStation)

SAM file hashes recovered from the target were loaded into Ophcrack and cross-checked against CrackStation to recover plaintext credentials.

*Figure 11 — Ophcrack loaded with Administrator and John SAM file hashes (XP rainbow tables unavailable for download)*

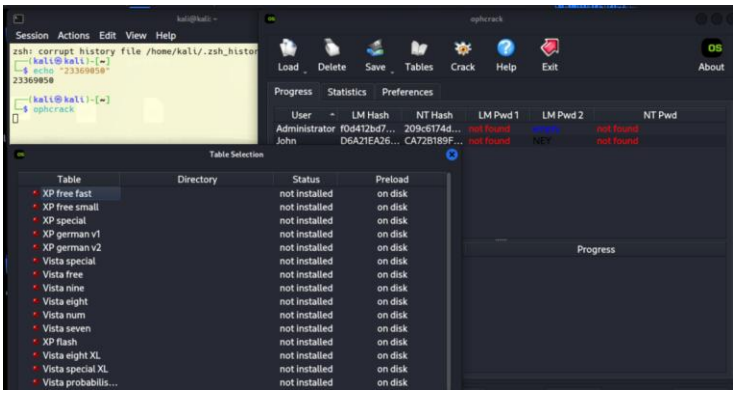
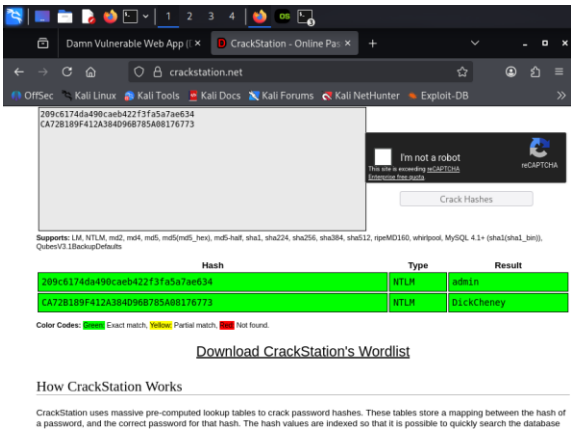


*Figure 12 — CrackStation successfully cracked both NTLM hashes — Administrator: admin | John: DickCheney*




## Key Findings

- Identified 8+ critical and high-severity vulnerabilities across network and web services, all with public exploits
- Achieved root-level compromise through two independent exploitation paths (PHP CGI injection and vsftpd backdoor)
- Established persistent access via a backdoor user account and verified it with a live SSH login
- Cracked both recovered NTLM password hashes using Ophcrack and CrackStation
- Demonstrated a complete offensive lifecycle: recon → enumeration → prioritisation → exploitation → persistence → credential recovery

## Tools & Technologies

| Tool | Purpose |
|---|---|
| Kali Linux | Attacker machine |
| Nmap | Network reconnaissance and service enumeration |
| Nikto | Web application vulnerability scanning |
| Metasploit | Exploitation framework (vsftpd backdoor, PHP CGI injection) |
| Meterpreter | Post-exploitation shell and session management |
| Ophcrack | Rainbow-table based password cracking |
| CrackStation | Online hash lookup / password recovery |
| Metasploitable2 | Intentionally vulnerable target machine |
| DVWA | Vulnerable web application (SQL injection, RCE testing) |

## Summary

This project demonstrates the full offensive security lifecycle against a deliberately vulnerable environment: from initial reconnaissance and CVSS-based risk prioritisation through to multi-vector exploitation, persistence, and password recovery. It highlights practical use of industry-standard tooling (Nmap, Nikto, Metasploit, Ophcrack) and reinforces the importance of patching end-of-life services, enforcing strong credential policies, and disabling unnecessary default services in production environments.

*Conducted entirely in an isolated virtual lab environment on personal hardware. No external systems were targeted.*