VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT) REPORT

1. Executive Summary

This Vulnerability Assessment and Penetration Testing (VAPT) activity was conducted on an authorized TryHackMe target system to identify security weaknesses using open-source security tools. The assessment focused on network service enumeration, web server configuration analysis, and manual validation of identified findings.

The assessment identified multiple medium- and high-risk security issues, including exposed network services, missing HTTP security headers, service version disclosure, and a critical exposure of a backup archive file accessible without authentication. These weaknesses could allow an attacker to gain sensitive information and potentially compromise the target system.

1.1Scope and Authorization

- Target Type: Authorized TryHackMe Vulnerable Machine
- Target IP Address: 10.49.170.172
- Testing Type: Black-box Assessment
- Access Method: OpenVPN (TryHackMe VPN)
- Authorization: Explicitly permitted for educational purposes under the TryHackMe platform

1.2Environment Setup

Attacker System

- Operating System: Kali Linux
- Tools Environment: Default Kali Linux toolset

Target System

- Operating System: Linux-based server (Kernel 4.15 detected)
- Web Server: nginx 1.24.0 (Ubuntu)
- Network Services: SSH, HTTP

1.3Tools Used

Tool	Purpose
Nmap	Network discovery and service enumeration
Nikto	Web server vulnerability and misconfiguration scanning
Nuclei	Template-based vulnerability and configuration detection
curl	Manual validation of exposed files and services
Web Browser	Manual verification and observation
OpenVPN	Secure access to authorized lab environment

Methodology Followed

The assessment followed a standard VAPT lifecycle, aligned with industry best practices:

1. Reconnaissance
2. Service Enumeration
3. Vulnerability Scanning
4. Manual Validation
5. Risk Classification
6. Documentation and Reporting

All testing activities were conducted strictly within a controlled and authorized lab environment.

2. Reconnaissance and Enumeration

2.1 Nmap Scan Command Used:

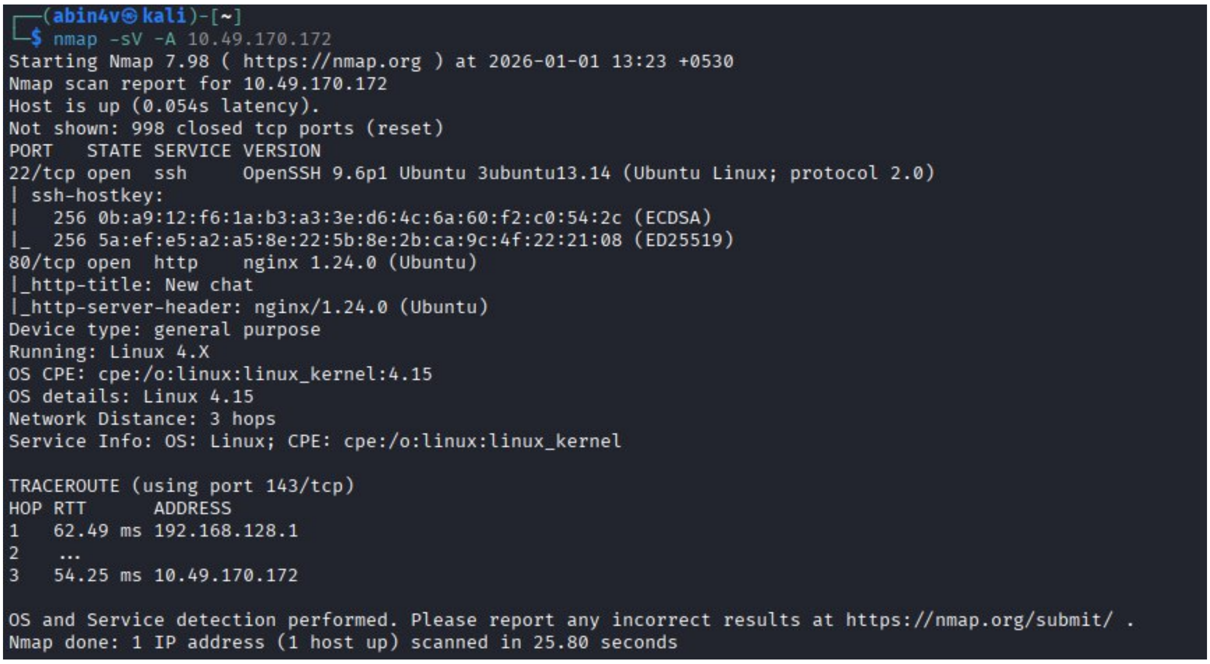
```
nmap -sV -A 10.49.170.172
```

Observations

- Host was reachable and active
- Two open TCP ports were identified
- SSH and HTTP services were exposed
- Service version and OS information were disclosed

Identified Open Ports

Port	Service	Version	Risk
22/tcp	SSH	OpenSSH 9.6p1 (Ubuntu)	Medium
80/tcp	HTTP	nginx 1.24.0 (Ubuntu)	Medium



```
┌──(abin4v㉿kali)-[~]
└─$ nmap -sV -A 10.49.170.172
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-01 13:23 +0530
Nmap scan report for 10.49.170.172
Host is up (0.054s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 0b:a9:12:f6:1a:b3:a3:3e:d6:4c:6a:60:f2:c0:54:2c (ECDSA)
|_  256 5a:ef:e5:a2:a5:8e:22:5b:8e:2b:ca:9c:4f:22:21:08 (ED25519)
80/tcp open  http    nginx 1.24.0 (Ubuntu)
|_http-title: New chat
|_http-server-header: nginx/1.24.0 (Ubuntu)
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 3 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 143/tcp)
HOP RTT      ADDRESS
1   62.49 ms 192.168.128.1
2   ...
3   54.25 ms 10.49.170.172

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.80 seconds
```

Figure 1: Nmap output showing open ports and service versions

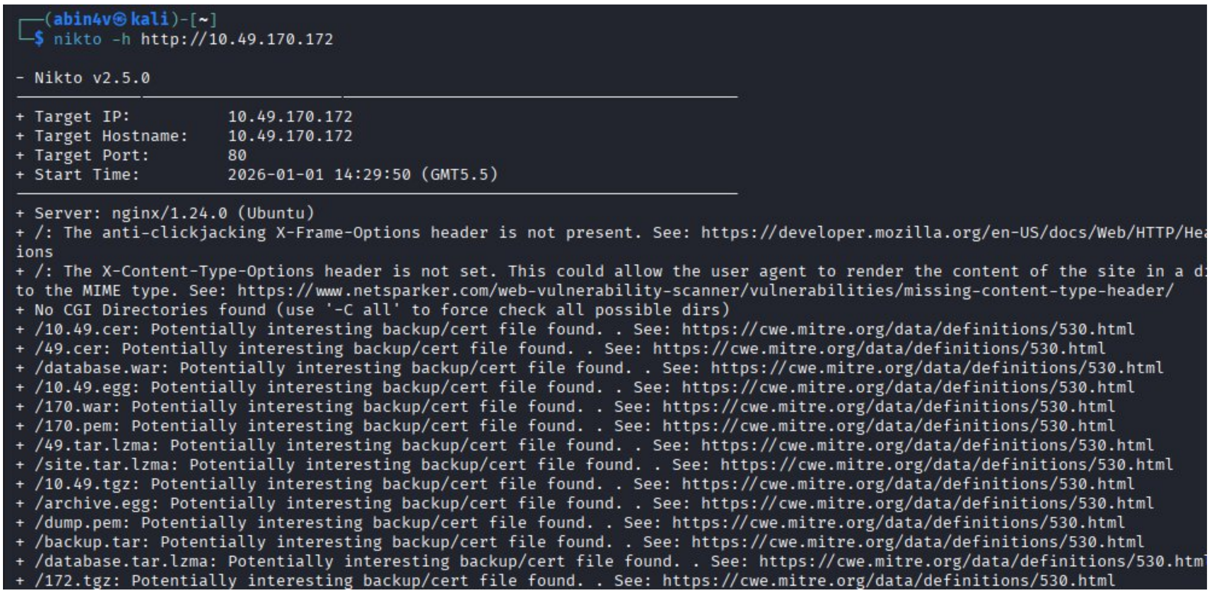
2.2 Web Vulnerability Assessment (Nikto)

Nikto was used to identify common web server misconfigurations and insecure settings.

Nikto Command Used:
nikto -h http://10.49.170.172

Findings

- Missing X-Frame-Options header
- Missing X-Content-Type-Options header
- nginx version disclosure through HTTP headers
- Presence of predictable backup and archive file names
- Potential information leakage through server headers



```
┌──(abin4v㉿kali)-[~]
└─$ nikto -h http://10.49.170.172

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.49.170.172
+ Target Hostname:    10.49.170.172
+ Target Port:        80
+ Start Time:         2026-01-01 14:29:50 (GMT5.5)
---------------------------------------------------------------------------
+ Server: nginx/1.24.0 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/He
ions
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a d
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)
+ /10.49.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /49.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /10.49.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /170.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /170.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /49.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /10.49.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /dump.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.htm
+ /172.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
```

Figure 2: Nikto scan results showing missing security headers and backup file indicators

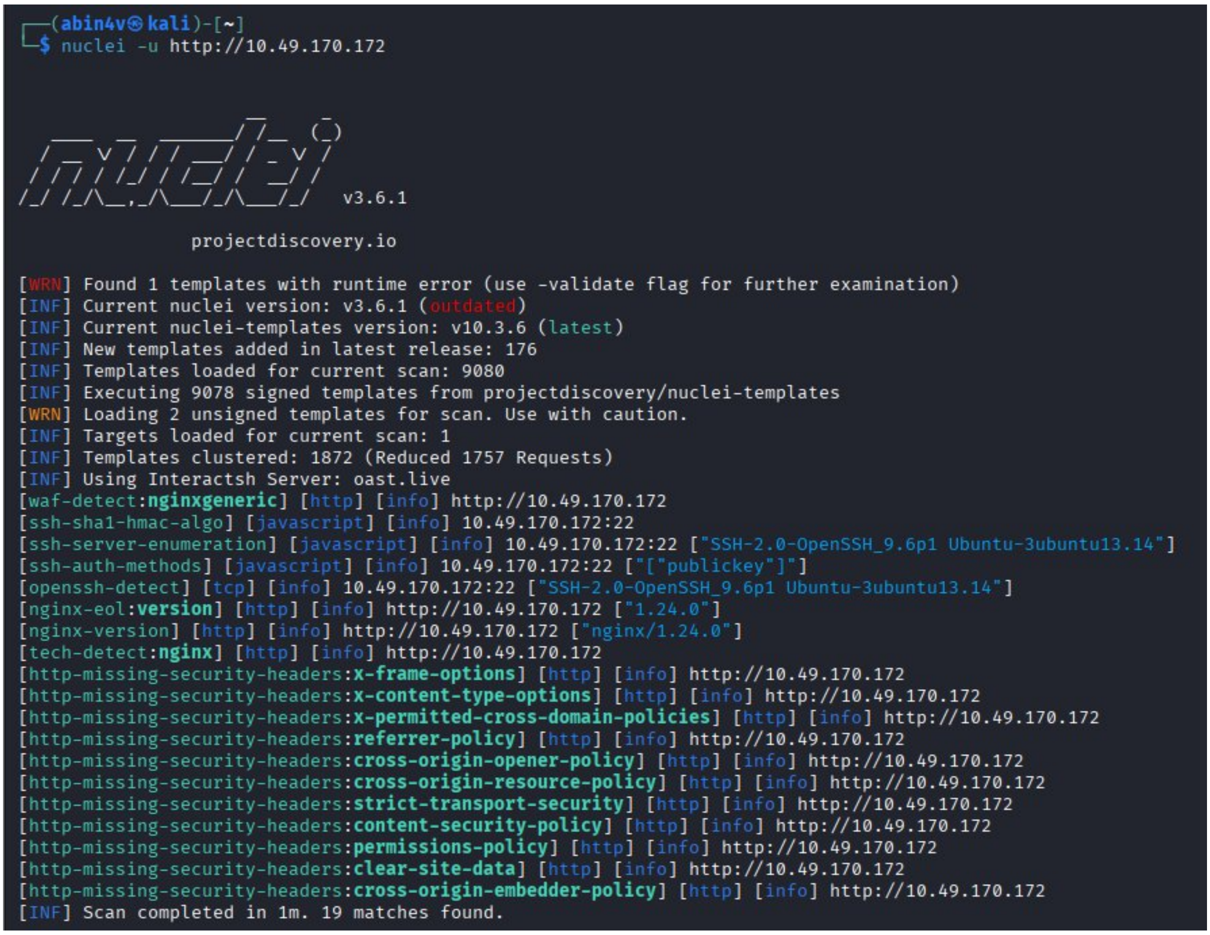
2.3 Automated Vulnerability Scanning (Nuclei)

Nuclei was executed to validate findings and identify known misconfigurations using updated templates.
Command Used:
nuclei -u http://10.49.170.172

Results

- Missing multiple HTTP security headers (CSP, HSTS, Referrer-Policy, Permissions-Policy)

- SSH banner enumeration confirmed
- nginx version disclosure confirmed
- No critical CVE-based vulnerabilities detected via templates



```
┌──(abin4v㉿kali)-[~]
└─$ nuclei -u http://10.49.170.172


                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.6.1

                projectdiscovery.io

[WRN] Found 1 templates with runtime error (use -validate flag for further examination)
[INF] Current nuclei version: v3.6.1 (outdated)
[INF] Current nuclei-templates version: v10.3.6 (latest)
[INF] New templates added in latest release: 176
[INF] Templates loaded for current scan: 9080
[INF] Executing 9078 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 2 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 1872 (Reduced 1757 Requests)
[INF] Using Interactsh Server: oast.live
[waf-detect:nginxgeneric] [http] [info] http://10.49.170.172
[ssh-sha1-hmac-algo] [javascript] [info] 10.49.170.172:22
[ssh-server-enumeration] [javascript] [info] 10.49.170.172:22 ["SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.14"]
[ssh-auth-methods] [javascript] [info] 10.49.170.172:22 ["["publickey"]"]
[openssh-detect] [tcp] [info] 10.49.170.172:22 ["SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.14"]
[nginx-eol:version] [http] [info] http://10.49.170.172 ["1.24.0"]
[nginx-version] [http] [info] http://10.49.170.172 ["nginx/1.24.0"]
[tech-detect:nginx] [http] [info] http://10.49.170.172
[http-missing-security-headers:x-frame-options] [http] [info] http://10.49.170.172
[http-missing-security-headers:x-content-type-options] [http] [info] http://10.49.170.172
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://10.49.170.172
[http-missing-security-headers:referrer-policy] [http] [info] http://10.49.170.172
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://10.49.170.172
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://10.49.170.172
[http-missing-security-headers:strict-transport-security] [http] [info] http://10.49.170.172
[http-missing-security-headers:content-security-policy] [http] [info] http://10.49.170.172
[http-missing-security-headers:permissions-policy] [http] [info] http://10.49.170.172
[http-missing-security-headers:clear-site-data] [http] [info] http://10.49.170.172
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://10.49.170.172
[INF] Scan completed in 1m. 19 matches found.
```

Figure 3: Nuclei output confirming security header and version disclosure findings

Manual Validation of Critical Finding

Exposed Backup Archive File

Manual validation was performed to confirm the existence of a potentially sensitive backup file.

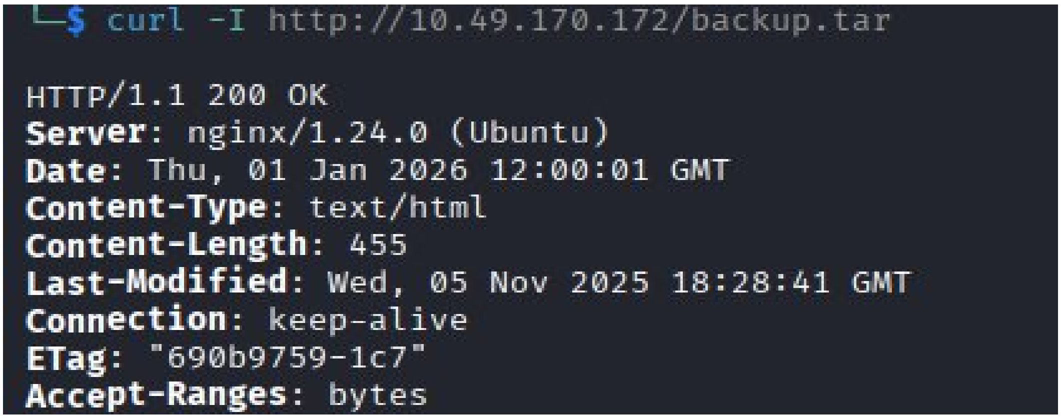
Command Used:
curl -I http://10.49.170.172/backup.tar

2.4 Observation

- The server returned an HTTP/1.1 200 OK response
- This confirms the backup archive file is publicly accessible without authentication

Impact:

Backup files may contain sensitive information such as credentials, configuration files, or database data, which could lead to full system compromise.



```
└─$ curl -I http://10.49.170.172/backup.tar

HTTP/1.1 200 OK
Server: nginx/1.24.0 (Ubuntu)
Date: Thu, 01 Jan 2026 12:00:01 GMT
Content-Type: text/html
Content-Length: 455
Last-Modified: Wed, 05 Nov 2025 18:28:41 GMT
Connection: keep-alive
ETag: "690b9759-1c7"
Accept-Ranges: bytes
```

Figure 4: HTTP header response confirming exposed backup archive file

3. Risk Assessment (CVSS-Based)

Factor	Value
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality Impact	High
Integrity Impact	High
Availability Impact	Low
Overall Severity	High (Approx. CVSS 8.6)

3.1 Summary of Findings

ID	Vulnerability	Severity	Tool Used	Status
V-01	SSH service exposed	Medium	Nmap	Identified
V-02	nginx version disclosure	Low	Nmap / Nikto / Nuclei	Identified
V-03	Missing HTTP security headers	Medium	Nikto / Nuclei	Identified
V-04	Exposed backup archive file	Critical	Nikto / curl	Confirmed

4.3CVSS Justification

Exposed Backup File

- Attack Vector: Network
- Privileges Required: None
- User Interaction: None
- Confidentiality Impact: High
- Integrity Impact: High
- Availability Impact: Low

3.2 Recommendations

1. Remove backup files from web-accessible directories
2. Store backups securely outside the web root
3. Implement proper file permission restrictions
4. Configure HTTP security headers (CSP, HSTS, X-Frame-Options)
5. Harden SSH configuration (disable root login, key-based authentication)
6. Minimize service version disclosure
7. Regularly update and patch system services
8. Perform periodic vulnerability assessments

Conclusion

The assessment successfully identified several configuration weaknesses and one critical security issue related to exposed sensitive backup files. While automated tools highlighted misconfigurations, manual validation confirmed the most severe risk, emphasizing the importance of combining automated scanning with manual verification. Implementing the recommended mitigations will significantly strengthen the security posture of the target system.

References

- OWASP Top 10
- NIST SP 800-115
- Nmap Documentation
- Nikto Documentation
- Nuclei Documentation