01
Vulnerability Scanning Lab

Objective

To identify, assess, and prioritize vulnerabilities on the target host using standard scanning tools.

Tools Used

- Nmap: Network discovery and port scanning.
- OpenVAS: Comprehensive vulnerability scanning and reporting.
- Nikto: Web server vulnerability assessment

Methodology

Nmap Scan:

- Performed TCP/UDP port scans on the target host.
- Identified open ports and running services.

OpenVAS Scan:

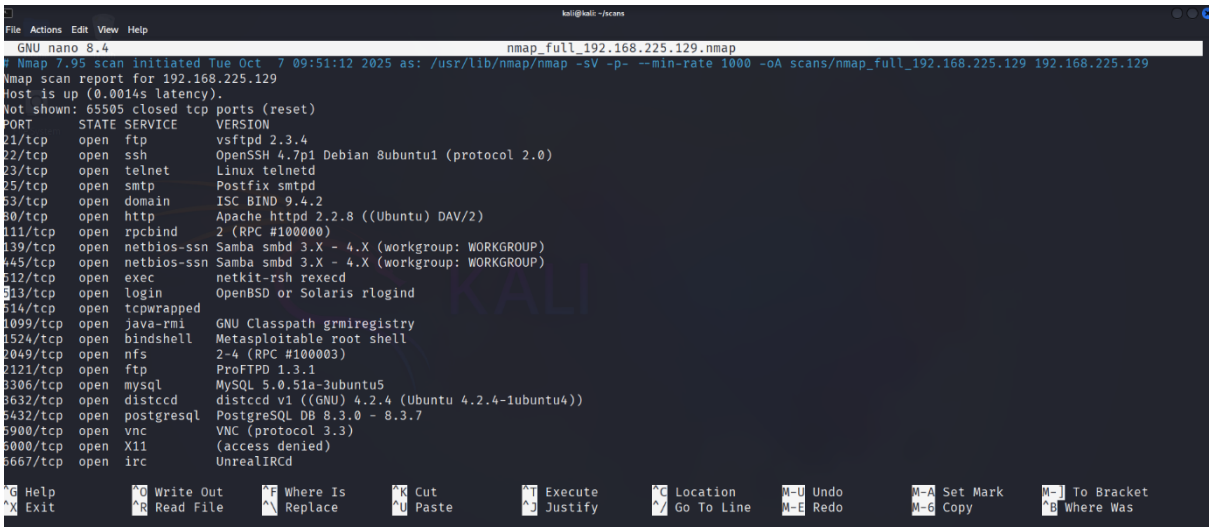
- Configured and launched full system scan.
- Prioritized vulnerabilities based on CVSS scores.
- Exported in csv format detailed results for documentation.

Nikto Scan:

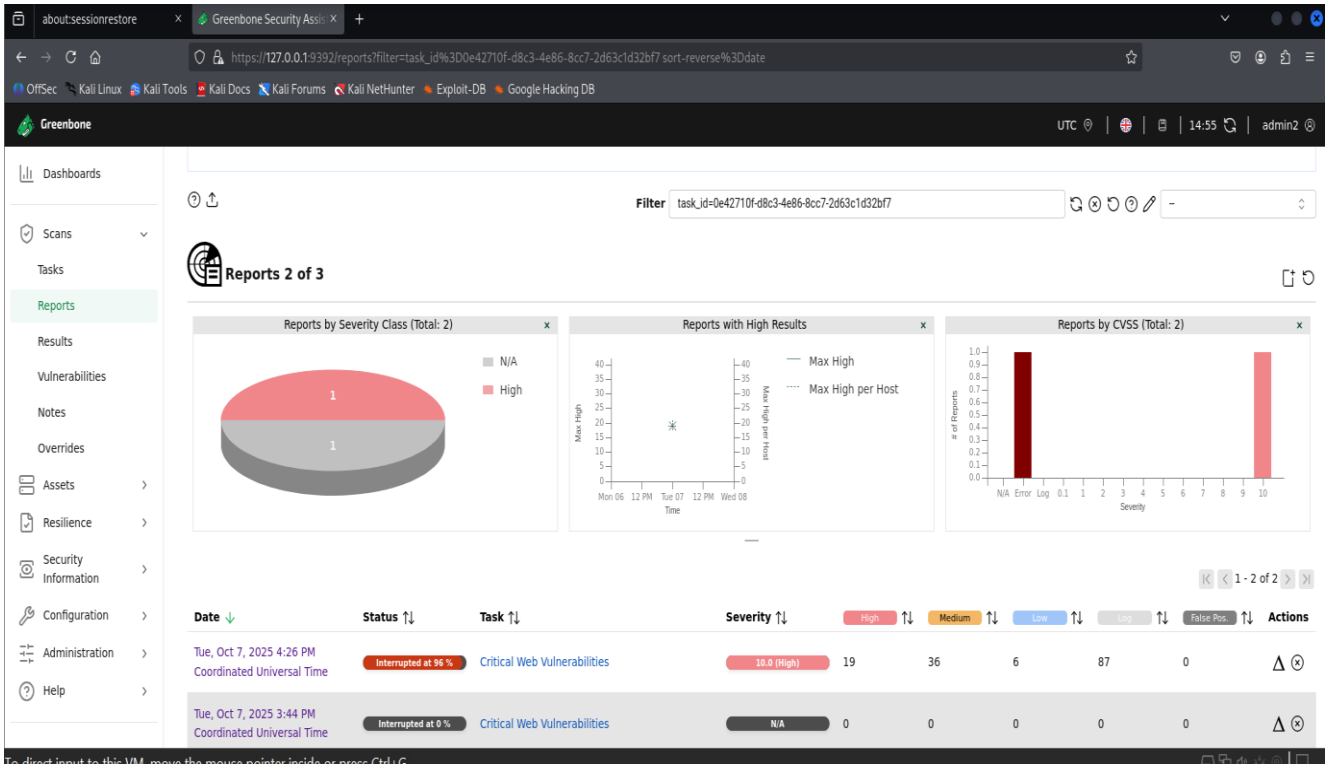
- Scanned web server endpoints for misconfigurations, default files, and known vulnerabilities.
- Generated a report in csv format

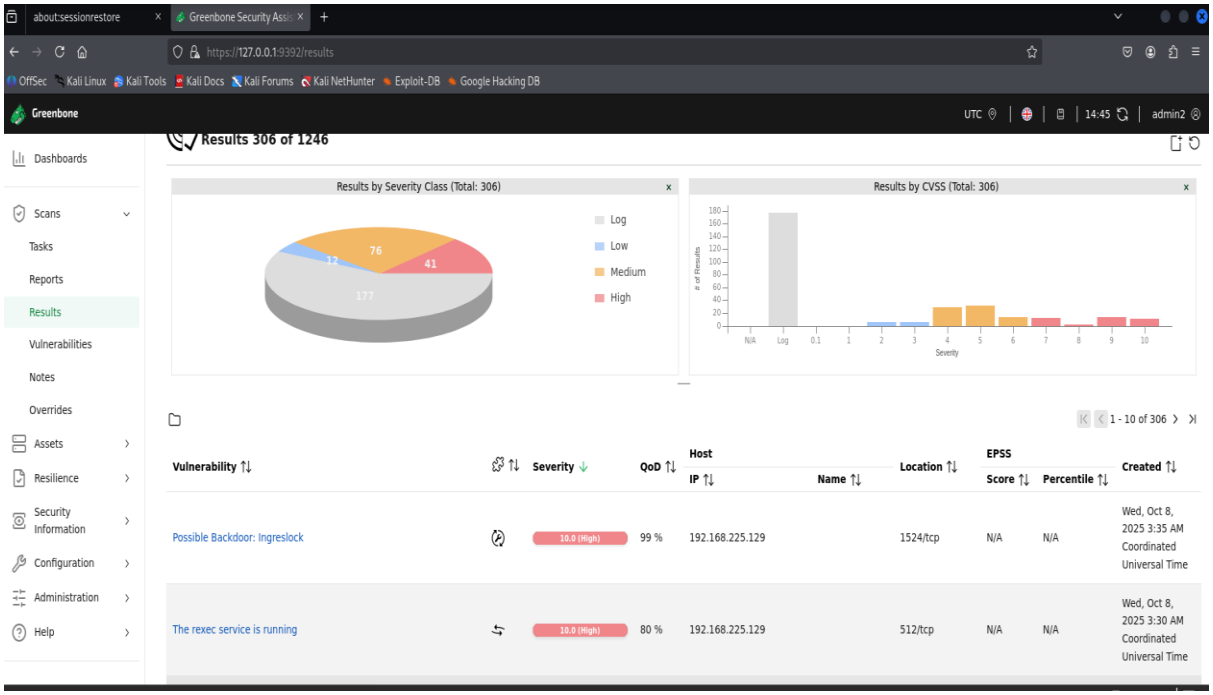
Result

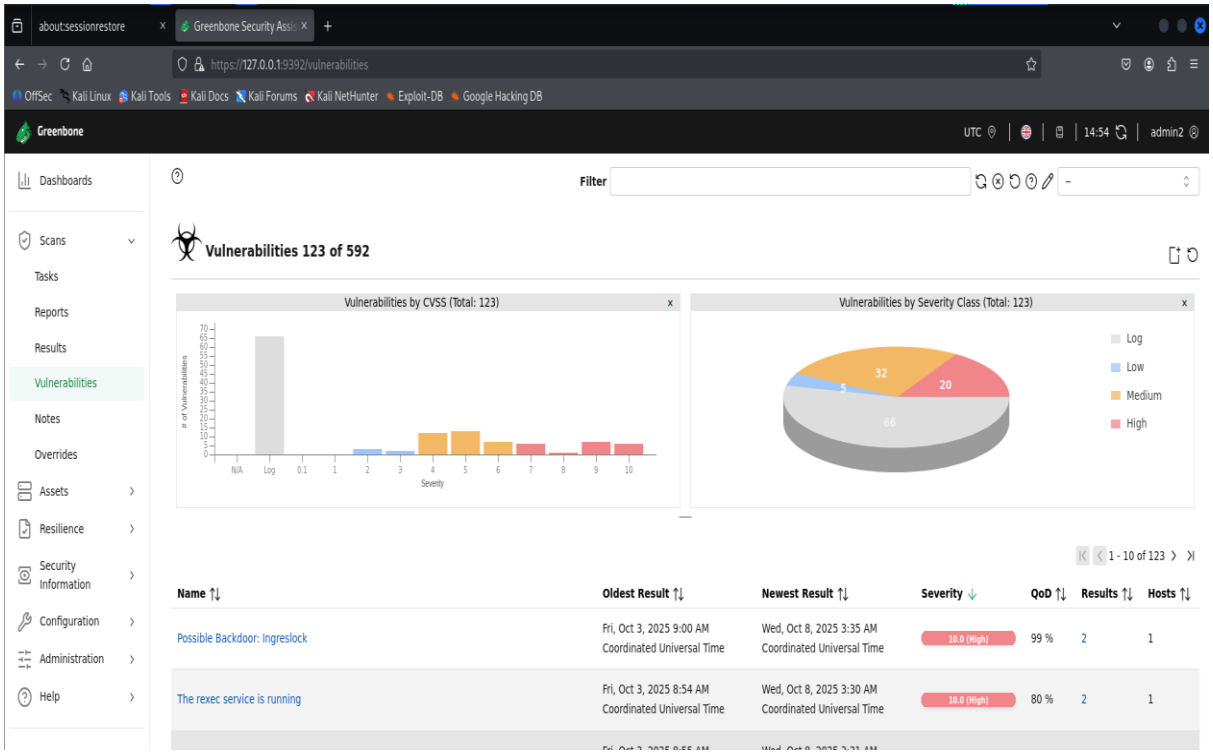
Nmap:



Openvas:




about:sessionrestore
Greenbone Security Assis
https://127.0.0.1:9392/results
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Greenbone
UTC 14:45 admin2
Dashboards
Scans
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Assets
Resilience
Security Information
Configuration
Administration
Help
Results 306 of 1246
Results by Severity Class (Total: 306)
Log
Low
Medium
High
76
12
41
177
Results by CVSS (Total: 306)
# of Results
Severity
1 - 10 of 306
Vulnerability
Severity
QoD
Host
IP
Name
Location
EPSS
Score
Percentile
Created
Possible Backdoor: Ingreslock
10.0 (High)
99 %
192.168.225.129
1524/tcp
N/A
N/A
Wed, Oct 8, 2025 3:35 AM Coordinated Universal Time
The rexec service is running
10.0 (High)
80 %
192.168.225.129
512/tcp
N/A
N/A
Wed, Oct 8, 2025 3:30 AM Coordinated Universal Time


about:sessionrestore
Greenbone Security Assis
https://127.0.0.1:9392/vulnerabilities
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Greenbone
UTC 14:54 admin2
Dashboards
Filter
Scans
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Assets
Resilience
Security Information
Configuration
Administration
Help
Vulnerabilities 123 of 592
Vulnerabilities by CVSS (Total: 123)
# of Vulnerabilities
Severity
Vulnerabilities by Severity Class (Total: 123)
Log
Low
Medium
High
32
20
5
66
1 - 10 of 123
Name
Oldest Result
Newest Result
Severity
QoD
Results
Hosts
Possible Backdoor: Ingreslock
Fri, Oct 3, 2025 9:00 AM Coordinated Universal Time
Wed, Oct 8, 2025 3:35 AM Coordinated Universal Time
10.0 (High)
99 %
2
1
The rexec service is running
Fri, Oct 3, 2025 8:54 AM Coordinated Universal Time
Wed, Oct 8, 2025 3:30 AM Coordinated Universal Time
10.0 (High)
80 %
2
1

Nikto:

```
┌──(kali㉿kali)-[~]
└─$ nikto -h  http://192.168.225.129 -output scans/nikto_192.168.225.129.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.225.129
+ Target Hostname:    192.168.225.129
+ Target Port:        80
+ Start Time:         2025-10-08 01:29:55 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to th
e MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives
for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY
 strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY
 strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY
 strings. See: OSVDB-12184
```

```
kali@kali: ~   kali@kali: ~/scans
for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY
 strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY
 strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY
 strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY
 strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue De
c  9 12:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:          2025-10-08 01:30:21 (GMT-4) (26 seconds)
```

Track results in a table:

ScanID	Vulnerability	CVSS Score	Priority	Host
1	rlogin Passwordless Login	10	Critical	192.168.225.129
2	TWiki XSS and Command Execution Vulnerabilities	10	Critical	192.168.225.129
3	Possible Backdoor: Ingreslock	10	Critical	192.168.225.129
4	The rexec service is running	10	Critical	192.168.225.129
5	Operating System (OS) End of Life (EOL) Detection	10	Critical	192.168.225.129
6	Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities	10	Critical	192.168.225.129
7	MySQL / MariaDB Default Credentials (MySQL Protocol)	9.8	Critical	192.168.225.129
8	Apache Tomcat AJP RCE Vulnerability (Ghostcat) - Active Check	9.8	Critical	192.168.225.129
9	PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check	9.8	Critical	192.168.225.129
10	vsftpd Compromised Source Packages Backdoor Vulnerability	9.8	Critical	192.168.225.129

11	vsftpd Compromised Source Packages Backdoor Vulnerability	9.8	Critical	192.168.225.129
12	DistCC RCE Vulnerability (CVE-2004-2687)	9.3	Critical	192.168.225.129
13	VNC Brute Force Login	9	Critical	192.168.225.129
14	PostgreSQL Default Credentials (PostgreSQL Protocol)	9	Critical	192.168.225.129
15	UnrealIRCd Authentication Spoofing Vulnerability	8.1	High	192.168.225.129
16	rsh Unencrypted Cleartext Login	7.5	High	192.168.225.129
17	FTP Brute Force Logins With Default Credentials Reporting	7.5	High	192.168.225.129
18	Test HTTP dangerous methods	7.5	High	192.168.225.129
19	FTP Brute Force Logins With Default Credentials Reporting	7.5	High	192.168.225.129
20	The rlogin service is running	7.5	High	192.168.225.129
21	Java RMI Server Insecure Default Configuration RCE Vulnerability - Active Check	7.5	High	192.168.225.129

22	SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	7.4	High	192.168.225.129
23	Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability	6.8	Medium	192.168.225.129
24	TWiki Cross-Site Request Forgery Vulnerability (Sep 2010)	6.8	Medium	192.168.225.129
25	Anonymous FTP Login Reporting	6.4	Medium	192.168.225.129
26	jQuery < 1.9.0 XSS Vulnerability	6.1	Medium	192.168.225.129
27	TWiki < 6.1.0 XSS Vulnerability	6.1	Medium	192.168.225.129
28	Samba 3.0.0 <= 3.0.25rc3 MS-RPC Remote Shell Command Execution Vulnerability - Active Check	6	Medium	192.168.225.129
29	TWiki CSRF Vulnerability	6	Medium	192.168.225.129
30	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	5.9	Medium	192.168.225.129
31	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	5.9	Medium	192.168.225.129
32	SSL/TLS: Report Weak Cipher Suites	5.9	Medium	192.168.225.129

33	HTTP Debugging Methods (TRACE/TRACK) Enabled	5.8	Medium	192.168.225.129
34	Weak Host Key Algorithm(s) (SSH)	5.3	Medium	192.168.225.129
35	Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	5.3	Medium	192.168.225.129
36	SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits	5.3	Medium	192.168.225.129
37	SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits	5.3	Medium	192.168.225.129
38	phpinfo() Output Reporting (HTTP)	5.3	Medium	192.168.225.129
39	awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check	5	Medium	192.168.225.129
40	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	5	Medium	192.168.225.129
41	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	5	Medium	192.168.225.129
42	/doc directory browsable	5	Medium	192.168.225.129
43	Check if Mailserver answer to VRFY and EXPN requests	5	Medium	192.168.225.129

44	SSL/TLS: Certificate Expired	5	Medium	192.168.225.129
45	SSL/TLS: Certificate Expired	5	Medium	192.168.225.129
46	QWikiwiki directory traversal vulnerability	5	Medium	192.168.225.129
47	FTP Unencrypted Cleartext Login	4.8	Medium	192.168.225.129
48	Cleartext Transmission of Sensitive Information via HTTP	4.8	Medium	192.168.225.129
49	FTP Unencrypted Cleartext Login	4.8	Medium	192.168.225.129
50	Telnet Unencrypted Cleartext Login	4.8	Medium	192.168.225.129
51	VNC Server Unencrypted Data Transmission	4.8	Medium	192.168.225.129
52	jQuery < 1.6.3 XSS Vulnerability	4.3	Medium	192.168.225.129
53	Weak Encryption Algorithm(s) Supported (SSH)	4.3	Medium	192.168.225.129
54	SSL/TLS: RSA Temporary Key Handling RSA_EXPORT Downgrade Issue (FREAK)	4.3	Medium	192.168.225.129

55	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3	Medium	192.168.225.129
56	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3	Medium	192.168.225.129
57	phpMyAdmin error.php Cross Site Scripting Vulnerability	4.3	Medium	192.168.225.129
58	Apache HTTP Server httpOnly Cookie Information Disclosure Vulnerability	4.3	Medium	192.168.225.129
59	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4	Medium	192.168.225.129
60	SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4	Medium	192.168.225.129
61	SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4	Medium	192.168.225.129
62	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4	Medium	192.168.225.129
63	SSL/TLS: DHE_EXPORT MITM Security Bypass Vulnerability (LogJam)	3.7	Low	192.168.225.129
64	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	3.4	Low	192.168.225.129
65	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	3.4	Low	192.168.225.129

66	Weak MAC Algorithm(s) Supported (SSH)	2.6	Low	192.168.225.129
67	TCP Timestamps Information Disclosure	2.6	Low	192.168.225.129
68	ICMP Timestamp Reply Information Disclosure	2.1	Low	192.168.225.129

Conclusion:

The vulnerability scanning lab highlighted significant security gaps on the target host, including critical backdoors, outdated software, weak credentials, and remote code execution vectors. Using Nmap, OpenVAS, and Nikto provided a comprehensive assessment of open services, exposed vulnerabilities, and potential attack paths. The findings emphasize the importance of prioritizing remediation based on severity, enforcing strong authentication, keeping software up-to-date, and minimizing unnecessary services. Overall, the lab reinforced the need for regular, proactive vulnerability assessments to reduce the attack surface and strengthen the organization's security posture.