

1. Objective

The goal of this task was to assess the security posture of the local machine using Nessus Essentials. The exercise involved performing a vulnerability scan, analyzing discovered weaknesses, and documenting the most critical findings with appropriate remediation strategies.

2. Tools Used

- **Nessus Essentials** (by Tenable)
- **Operating System:** Kali Linux
- **Scan Type:** Basic Network Scan

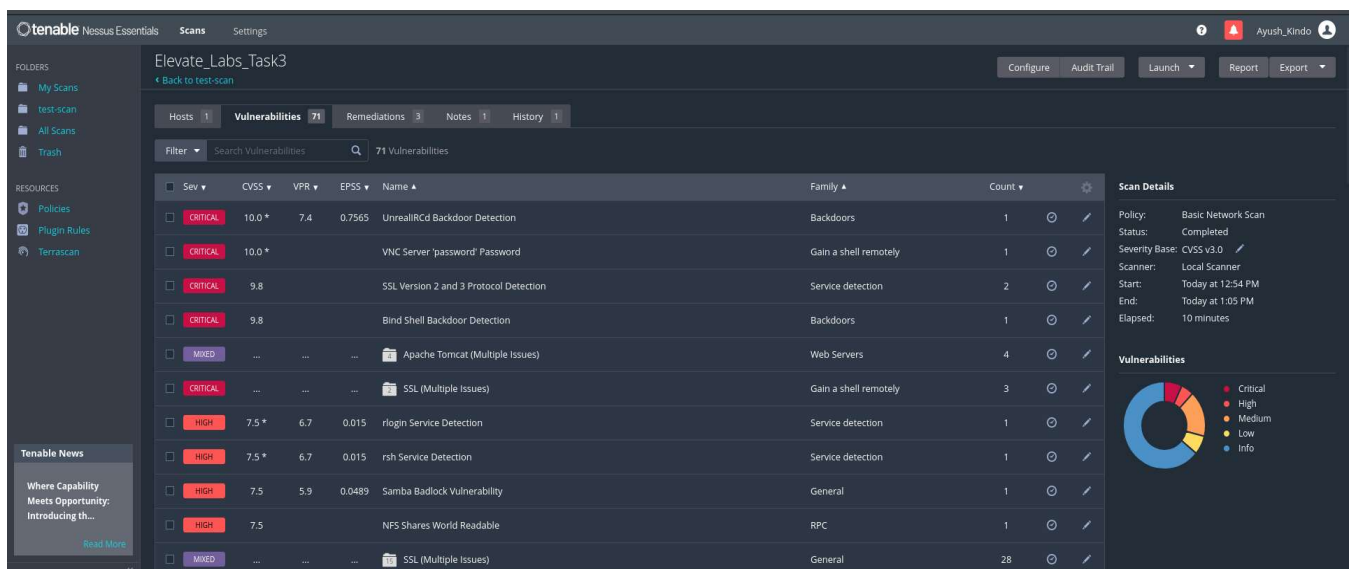
3. Starting the Nessus

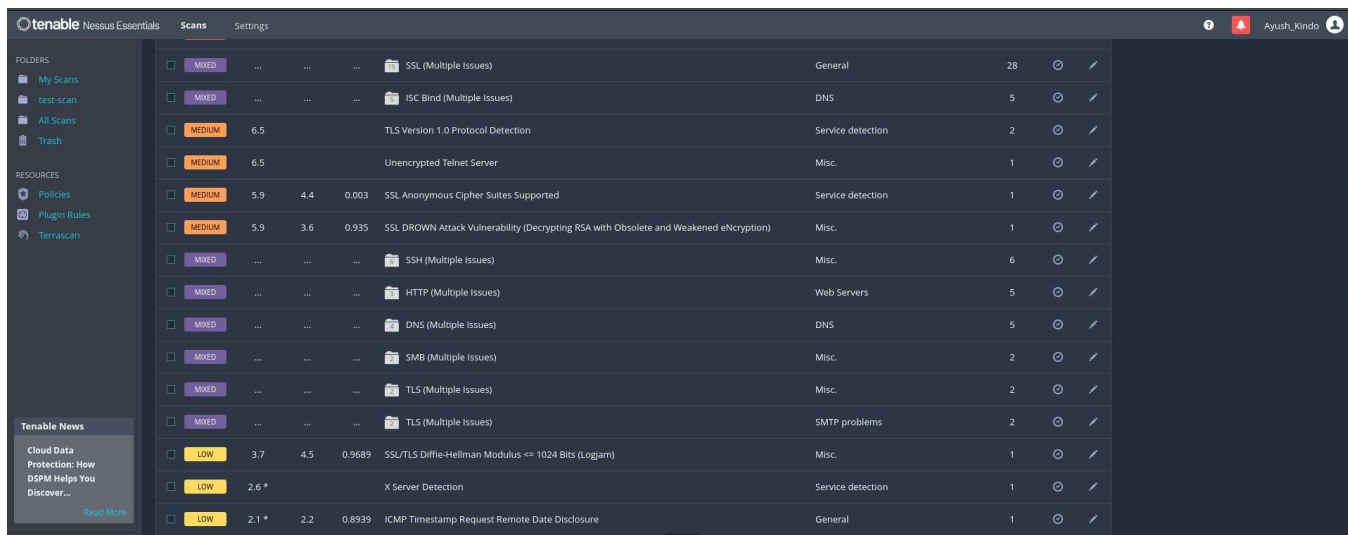
```
(ayush@kali)-[~/Downloads]
$ service nessusd start

(ayush@kali)-[~/Downloads]
$ service nessusd status
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
   Active: active (running) since Thu 2025-05-29 12:27:29 IST; 6s ago
     Invocation: 1701eb5ebf974ecbb1df40f04311dc50
       Main PID: 517814 (nessus-service)
         Tasks: 18 (limit: 6960)
        Memory: 299.4M (peak: 299.6M)
           CPU: 6.102s
        CGroup: /system.slice/nessusd.service
                └─517814 /opt/nessus/sbin/nessus-service -q
                  └─517819 nessusd -q

May 29 12:27:29 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
```

4. Key Findings and Vulnerabilities





The screenshot shows the Tenable Nessus Essentials interface. The left sidebar contains 'FOLDERS' (My Scans, test-scan, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Tenable News). The main area is titled 'Scans' and displays a table of vulnerabilities. The table has columns for severity, CVSS scores, description, category, and count. The vulnerabilities listed include SSL (Multiple Issues), ISC Bind (Multiple Issues), TLS Version 1.0 Protocol Detection, Unencrypted Telnet Server, SSL Anonymous Cipher Suites Supported, SSL DROWN Attack Vulnerability, SSH (Multiple Issues), HTTP (Multiple Issues), DNS (Multiple Issues), SMB (Multiple Issues), TLS (Multiple Issues), and SMTP problems. Some vulnerabilities are marked as 'LOW' or 'MEDIUM'.

Severity	CVSS	Description	Category	Count
MIXED		SSL (Multiple Issues)	General	28
MIXED		ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5	TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	6.5	Unencrypted Telnet Server	Misc.	1
MEDIUM	5.9	SSL Anonymous Cipher Suites Supported	Service detection	1
MEDIUM	5.9	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eEncryption)	Misc.	1
MIXED		SSH (Multiple Issues)	Misc.	6
MIXED		HTTP (Multiple Issues)	Web Servers	5
MIXED		DNS (Multiple Issues)	DNS	5
MIXED		SMB (Multiple Issues)	Misc.	2
MIXED		TLS (Multiple Issues)	Misc.	2
MIXED		TLS (Multiple Issues)	SMTP problems	2
LOW	3.7	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	1
LOW	2.6 *	X Server Detection	Service detection	1
LOW	2.1 *	ICMP Timestamp Request Remote Date Disclosure	General	1

5. Detailed Analysis and Remediations

1. UnrealIRCd Backdoor Detection (CVSS: 10.0)

Remediation:

This vulnerability signifies that a trojanized version of UnrealIRCd has been installed.

Immediately uninstall UnrealIRCd, verify the legitimacy of downloaded packages via checksums or GPG signatures, and reinstall from a trusted official source. Conduct a full malware scan and investigate for lateral movement or persistence.

2. VNC Server 'password' Password (CVSS: 10.0)

Remediation:

Change the default password to a complex, randomly generated one. Ensure VNC access is restricted by IP address using firewall rules. Additionally, configure VNC to use encrypted sessions to prevent credential interception.

3. SSL Version 2 and 3 Protocol Detection (CVSS: 9.8)

Remediation:

Edit the server's SSL/TLS configuration to disable SSLv2 and SSLv3 protocols. Only TLS 1.2 and 1.3 should be enabled. Test the configuration using SSL Labs or OpenSSL to ensure secure settings.

4. Bind Shell Backdoor Detection (CVSS: 9.8)

Remediation:

This is a serious threat indicating the presence of a backdoor. Kill any suspicious listening processes immediately. Run a malware analysis and restore system integrity via backups or clean reinstall. Rotate all credentials and audit logs for compromise.

5. Apache Tomcat (Multiple Issues)

Remediation:

Upgrade Apache Tomcat to the latest stable version. Review configuration files to disable unneeded services and secure the admin console. Use strong authentication and enforce HTTPS for all Tomcat interfaces.

6. SSL (Multiple Issues)

Remediation:

Audit the SSL configuration and disable weak ciphers like RC4 and 3DES. Enforce forward secrecy by enabling ECDHE cipher suites. Acquire a certificate from a trusted CA and regularly renew and monitor its validity.

7. rlogin Service Detection (CVSS: 7.5)

Remediation:

Disable rlogin service if not explicitly required. rlogin transmits data unencrypted and is deprecated. Replace with SSH and enforce key-based authentication.

8. rsh Service Detection (CVSS: 7.5)

Remediation:

Remove rsh services as they are outdated and insecure. Implement SSH as a secure replacement, and configure firewall rules to block port 514 if not in use.

9. Samba Badlock Vulnerability (CVSS: 7.5)

Remediation:

Update Samba to the version that patches the Badlock vulnerability. Restrict access to the Samba service using ACLs and firewalls, and monitor logs for unauthorized access.

10. NFS Shares World Readable

Remediation:

Restrict read/write access on NFS shares using `/etc/exports` and enforce `root_squash`. Apply user-based permissions and firewall rules to limit access to trusted hosts only.

6. Conclusion

The vulnerability scan revealed several critical issues, primarily related to backdoors, weak encryption, and insecure remote access services. Each has been reviewed with corresponding mitigation steps. This exercise highlighted the importance of continuous monitoring, patch management, and secure configurations in system hardening.

7. Closing the Nessus

```
(ayush@kali)~[/Downloads]
$ service nessusd stop

(ayush@kali)~[/Downloads]
$ service nessusd status
o nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
   Active: inactive (dead)

May 29 12:27:29 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
May 29 12:28:20 kali nessus-service[517819]: Cached 304 plugin libs in 243msec
May 29 12:28:20 kali nessus-service[517819]: Cached 304 plugin libs in 126msec
May 29 14:32:09 kali systemd[1]: Stopping nessusd.service - The Nessus Vulnerability Scanner...
May 29 14:32:09 kali systemd[1]: nessusd.service: Killing process 536647 (nessusd) with signal SIGKILL.
May 29 14:32:10 kali systemd[1]: nessusd.service: Deactivated successfully.
May 29 14:32:10 kali systemd[1]: Stopped nessusd.service - The Nessus Vulnerability Scanner.
May 29 14:32:10 kali systemd[1]: nessusd.service: Consumed 5min 57.064s CPU time, 1.7G memory peak.
```