🔍 Internal Lab – Vulnerability Assessment on Metasploitable using Nessus

- Environment: Conducted on a local virtual lab setup with Kali Linux as the scanning machine and Metasploitable 2 as the target vulnerable host.
- Objective: To identify and assess security vulnerabilities in Metasploitable using Nessus Essentials.
- Scanning Tool: Tenable Nessus (https://www.tenable.com/products/nessus)

🔧 Scan Configuration

- Scan Template: Basic Network Scan
- Target IP: 192.168.15.130
- Scan Type: Default
- Scan Duration: ~20 minutes
- Scanner Version: Nessus Essentials

📊 Summary of Findings (From Complete List Of Vulnerabilities By Host Report)

Severity	Count
Critical	9
High	6
Medium	21
Low	8
Info	80
Total	124

🛡️ Critical Vulnerabilities Identified

1. Apache Tomcat AJP Connector Request Injection (Ghostcat) – Allows unauthenticated file read/RCE
2. Bind Shell Backdoor Detection – Remote shell access without authentication

3. SSL Version 2 and 3 Protocol Detection – Weak and outdated encryption protocols enabled
4. Canonical Ubuntu Linux SEoL – OS is no longer supported
5. UnrealIRCd Backdoor Detection – Known backdoored version allows arbitrary command execution
6. VNC Server Weak Password (`password`) – Easily guessable login credentials
Insert 2–3 relevant screenshots showing these issues

📌 Additional Observations (From Detailed Vulnerabilities By Host Report)

- rlogin and rsh Services Enabled: Enable cleartext credential transfers
- Outdated Apache Tomcat Version (≤ 5.5.x) – Unsupported and vulnerable to many exploits
- DNS Zone Transfer Enabled (AXFR) – Can leak internal network structure
- TRACE / TRACK Methods Allowed – HTTP debugging features may leak information
- Samba Badlock Vulnerability – Allows privilege escalation on SMB
Insert key screenshots showing highlighted plugin output

📎 PDF Reports

- [🔗Complete List Of Vulnerabilities By Host
- [🔗 Detailed Vulnerabilities By Host

📌 Recommendations

- Disable insecure services like rlogin, rsh, telnet, and FTP
- Upgrade deprecated services (e.g., Tomcat, Ubuntu 8.04, OpenSSH) to supported versions
- Implement strong password policies across all exposed services
- Disable outdated SSL/TLS protocols and weak cipher suites
- Harden DNS configurations to prevent cache snooping and zone transfers