

Vulnerability Assessment Briefing

By Mahad Mohamood

A dark blue diagonal gradient bar that starts from the bottom left and extends towards the top right, covering the lower half of the slide.

Executive Summary

This briefing covers the vulnerability assessment performed on critical devices within our network: a Windows 11 machine and a Linux Server. The assessment, conducted using OpenVAS/GVM, revealed two key vulnerabilities related to timestamp information disclosure:

- TCP Timestamps Information Disclosure
- ICMP Timestamp Reply Information Disclosure

These vulnerabilities are categorized as low severity but have potential implications for system profiling and further exploitation.

Key Findings

1. **TCP Timestamps Information Disclosure**

- Windows 11: Exposes system uptime, potentially revealing reboot patterns.
- Linux Server: Exposes system uptime, which may indicate operational stability.
- Significance: TCP timestamps, used for performance metrics, can be exploited to infer system behavior.

2. **ICMP Timestamp Reply Information Disclosure**

- Linux Server: Reveals detailed internal clock settings and timing data.
- Significance: ICMP timestamps can be used to synchronize attacks or exploit time-based vulnerabilities.

Recommendations

1. Disable TCP Timestamps

- Windows: Execute `netsh int tcp set global timestamps=disabled`.
- Linux: Add `net.ipv4.tcp_timestamps = 0` to `/etc/sysctl.conf` and apply with `sysctl -p`.

2. Disable ICMP Timestamp Replies

- Action: Configure the Linux Server to block ICMP timestamp replies through system settings or firewall rules.

3. Regular Updates and Patching

- Action: Implement routine updates and patches for all systems to address vulnerabilities.

4. Monitor Network Traffic

- Action: Set up monitoring tools to detect unusual ICMP or TCP traffic patterns.

5. Review and Strengthen Firewall Rules

- Action: Update firewall rules to block unnecessary TCP and ICMP traffic.

Importance of Recommendations

- Immediate Impact: Disabling timestamps directly mitigates the current vulnerabilities.
- Long-Term Security: Regular updates and proactive monitoring are essential for ongoing security.
- Proactive Measures: Monitoring and firewall adjustments help detect and prevent future threats.

Conclusion

Expected Outcomes:

- Improved security posture by addressing information disclosure vulnerabilities.
- Reduced risk of attackers leveraging timestamp data.
- Strengthened overall resilience against potential threats.

Next Steps:

- Implement recommended actions.
- Schedule follow-up assessment to verify effectiveness.
- Continue monitoring and updating security measures.