Network Vulnerability Assessment Report

1. Executive Summary:

This Network Vulnerability Assessment Report provides an overview of the vulnerabilities identified in the XYZ Company's network infrastructure. The assessment aimed to identify potential weaknesses and propose mitigation strategies to enhance the overall security posture. The following report outlines five critical vulnerabilities, their associated risks, and recommended mitigation plans.

2. Vulnerabilities:

2.1: Outdated Software

Description: The network contains outdated software versions, which may have known vulnerabilities that could be exploited by attackers.

Risk: Unauthorized access, data breaches, and system compromise.

Mitigation Plan:
- Regularly update and patch all software components.
- Implement a centralized patch management system.
- Conduct periodic vulnerability scans to identify and address outdated software.

2.2: Weak Passwords

Description: Weak and easily guessable passwords are in use, posing a significant risk to unauthorized access.

Risk: Unauthorized access, privilege escalation, and potential data breaches.

Mitigation Plan:
- Enforce strong password policies.
- Implement multi-factor authentication (MFA) for critical systems.
- Conduct regular password audits and user education programs.

2.3: Unsecured Network Devices

Description: Some network devices have default or weak configurations, making them susceptible to exploitation.

Risk: Unauthorized access, device compromise, and network disruption.

Mitigation Plan:
- Change default credentials on all network devices.
- Implement strict access controls for network device management.
- Regularly review and update device configurations.

2.4: Insufficient Network Segmentation

Description: The network lacks proper segmentation, allowing unrestricted lateral movement for potential attackers.

Risk: Unauthorized access to sensitive data, lateral movement, and increased attack surface.

Mitigation Plan:
- Implement network segmentation to isolate critical assets.
- Enforce strict access controls based on the principle of least privilege.
- Regularly review and update segmentation rules.

2.5: Lack of Network Monitoring

Description: Inadequate network monitoring capabilities hinder the timely detection of suspicious activities.

Risk: Delayed detection of security incidents, allowing attackers to operate undetected.

Mitigation Plan:
- Deploy intrusion detection and prevention systems.
- Implement real-time monitoring of network logs and traffic.
- Establish an incident response plan for swift action in case of a security incident.

3. Recommendations:

3.1. Conduct regular penetration testing to identify and address emerging vulnerabilities.

3.2. Implement network-wide encryption for sensitive data in transit.

3.3. Establish a comprehensive security awareness training program for employees.

3.4. Regularly review and update the incident response plan to address evolving threats.

3.5. Engage in continuous monitoring of emerging security threats and updates.

4. Conclusion:

The Network Vulnerability Assessment has identified critical vulnerabilities within the XYZ Company's network infrastructure. By implementing the proposed mitigation plans and recommendations, the organization can significantly enhance its security posture, reduce the risk of unauthorized access, and better protect sensitive data. Regular monitoring, timely updates, and employee training are essential components of a robust cybersecurity strategy.

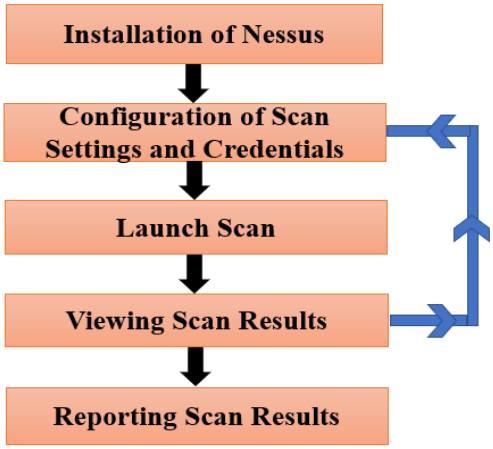
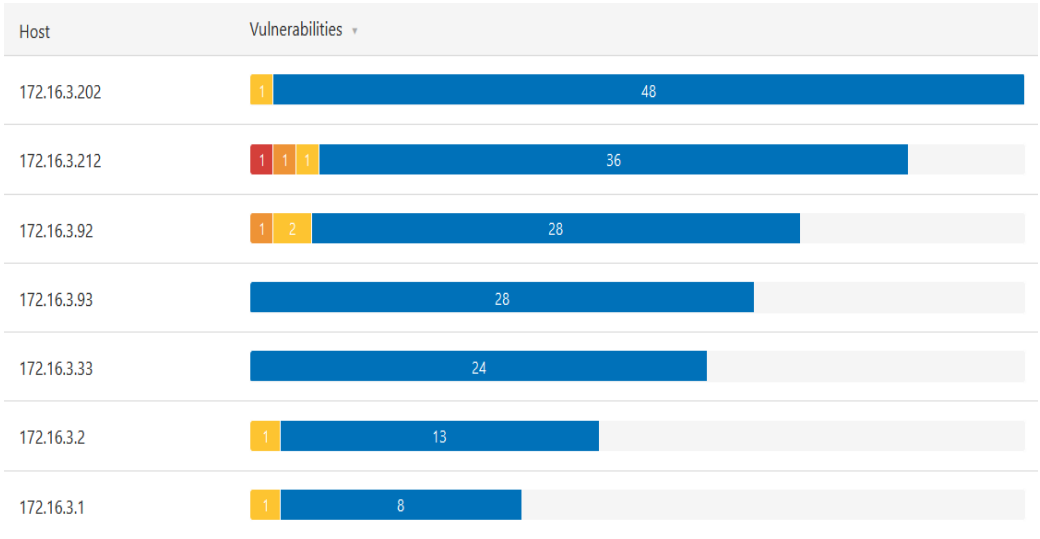
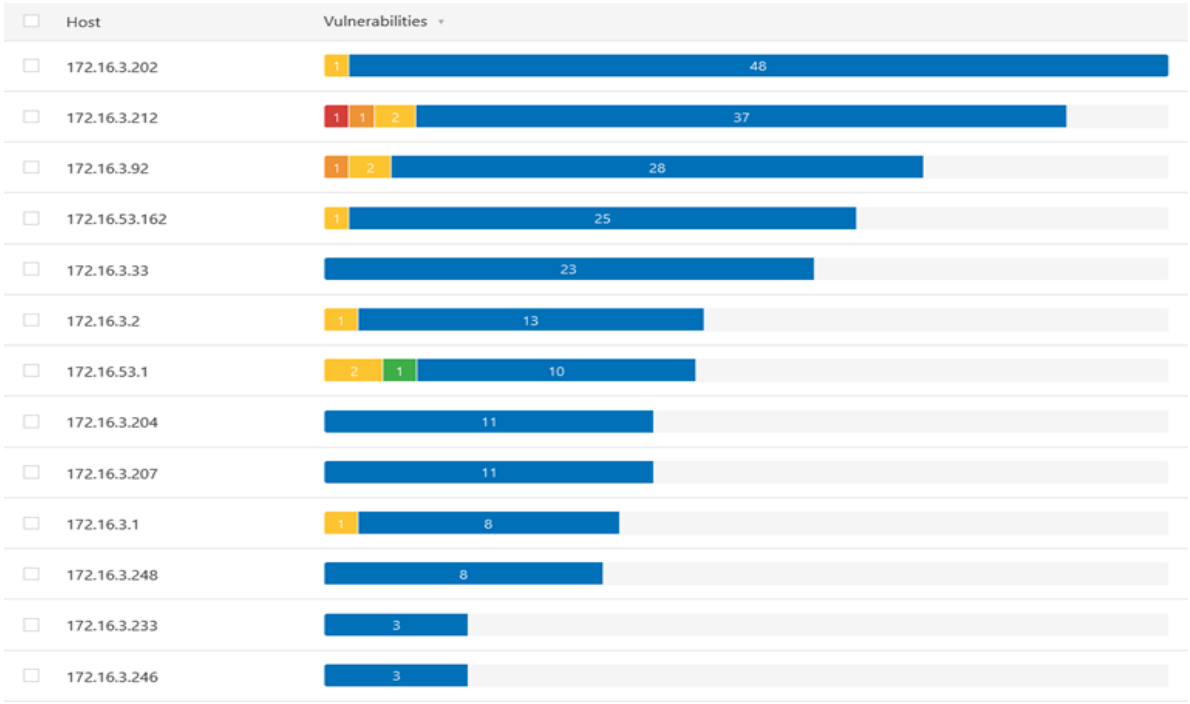


Fig 1. Network Scanning Steps using NESSUS





Hosts 7 | **Vulnerabilities** 34 | VPR Top Threats | History 1

Filter | Search Vulnerabilities | **34** Vulnerabilities

Sev	Name	Family	Count
MIXED	4 Microsoft Windows (Multiple Issues)	Windows	6
MIXED	6 SNMP (Multiple Issues)	SNMP	6
MEDIUM	Unencrypted Telnet Server	Misc.	3
MEDIUM	SMB Signing not required	Misc.	2
MEDIUM	RomPager HTTP Referer Header XSS	CGI abuses : XSS	1
INFO	Nessus SNMP Scanner	Port scanners	28
INFO	DCE Services Enumeration	Windows	26
INFO	Nessus SYN scanner	Port scanners	23
INFO	6 SMB (Multiple Issues)	Windows	18
INFO	3 HTTP (Multiple Issues)	Web Servers	9
INFO	Service Detection	Service detection	8

172.16.3.212

CRITICAL	HIGH	MEDIUM	LOW	INFO
1	1	1	0	23

Vulnerabilities Total: 26

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)