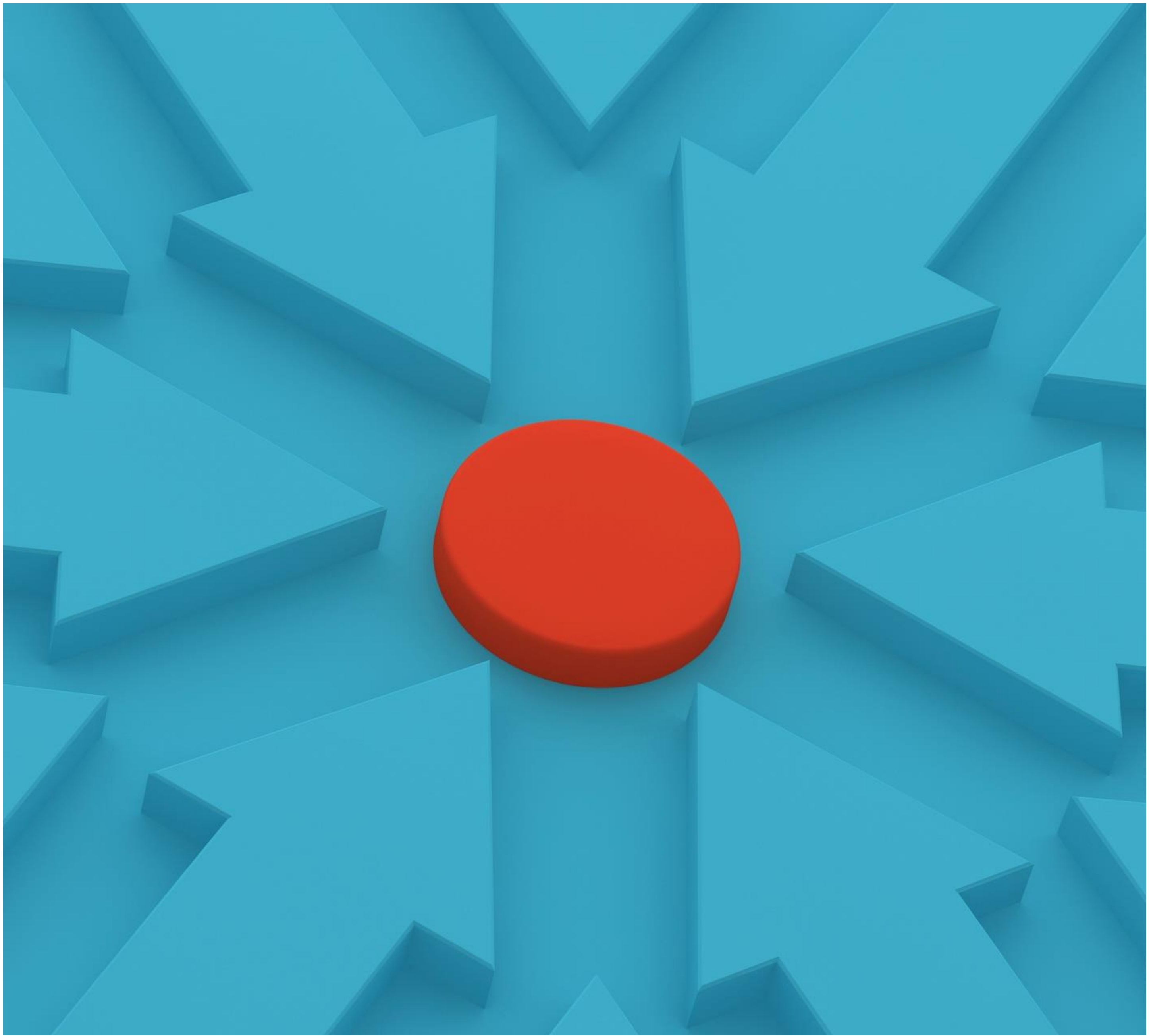

VULNERABILITY ASSESSEMENT

ACME COMPANY HEADQUATERS

ROAD RUNNER CORPORATION

soc@roadrunner.com

VULNERABILITY ASSESSMENT OVERVIEW

Executive Summary

This report outlines a detailed plan to address vulnerabilities identified in our recent vulnerability scans on the ACME headquarters network. The scans conducted using Nessus uncovered 287 vulnerabilities across 18 hosts spanning three subnets: the Internal LAN, DMZ, and SOC networks. The most vulnerable hosts are 192.168.20.222, 192.168.10.210, and 192.168.10.1, with 110, 32, and 22 vulnerabilities respectively. This report presents a comprehensive, risk-based remediation strategy, prioritizing vulnerabilities based on severity, frequency of occurrence, and the required time for mitigation. The remediation plan is divided into the critical, high, medium, and low risks, with recommendations provided for each.

Network Overview

1. Internal LAN (192.168.10.0/24)
2. DMZ (192.168.20.0/24)
3. SOC Network (192.168.30.0/24)

Total Vulnerabilities Detected

- Critical: 6
- High: 5
- Medium: 24
- Low: 20
- Informational: 232

Most Vulnerable Hosts

1. **192.168.20.222**
   - 110 vulnerabilities
2. **192.168.10.210**
   - 32 vulnerabilities
3. **192.168.10.1**
   - 22 vulnerabilities

PRIORITIZED MITIGATION PLAN

Critical Vulnerabilities

These vulnerabilities need to have immediate mitigation within 24-48 hours. These pose the highest risk to security and operations. They include issues with Apache Tomcat, OpenSSH, SSL/TLS and VNC. Most of which came from the 192.168.20.222 host in the DMZ network. Once these have either been remediated or have had compensating controls put in place, you can start focusing on the high risks.

Apache Tomcat Ghostcat Vulnerability (CVE-2020-1938)

Risk: Critical (CVSS 9.8)
Affected Systems: 192.168.20.222
Frequency: 1 instance
Mitigation: Upgrade Apache Tomcat to the latest stable version
Team: Web Application Team
Time Estimate: 2-3 days

Steps to Remediate:

1. Test the upgrade in a staging environment
2. Schedule a maintenance window
3. Backup current configuration
4. Perform the upgrade
5. Validate functionality
6. Update documentation

SSL/TLS Protocol Vulnerabilities

Risk: Critical (CVSS 9.8)
Affected Systems: 192.168.20.222
Frequency: Multiple instances
Mitigation:

- Disable SSL v2/v3
- Enforce TLS 1.2+
- Implement proper certificate management

Team: Network Security Team
Time Estimate: 3-4 days

Steps to Remediate:

1. Inventory all SSL/TLS-enabled services
2. Develop a standardized secure configuration
3. Test in a non-production environment

4. Deploy changes in batches
5. Validate each batch
6. Update security policies and documentation

Debian OpenSSH/OpenSSL Random Number Generator Weakness

Risk: Critical (CVSS 10.0)

Affected Systems: 192.168.20.222

Frequency: 2 instances

Mitigation: Apply latest security patches

- Potentially regenerate cryptographic keys

Team: Systems Administration Team

Time Estimate: 2-3 days

Steps to Remediate:

1. Identify all affected systems
2. Test patches in a staging environment
3. Schedule maintenance windows
4. Apply patches and reboot systems
5. Verify patch application
6. Assess the need for key regeneration
7. If necessary, regenerate and distribute new keys

VNC Server Default Password

Risk: Critical (CVSS 10.0)

Affected Systems: 192.168.20.222

Frequency: 1 instance

Mitigation: Change default password

- Implement strong authentication (MFA)

Team: Systems Administration Team

Time Estimate: 4-6 hours

Steps to Remediate:

1. Generate a strong, unique password
2. Change the VNC server password
3. Update password management system
4. Notify authorized users of the change
5. Consider implementing two-factor authentication for VNC access

High Risk Vulnerabilities

These vulnerabilities need to be addressed within 3-5 days or as soon as the critical risks are addressed. These are also mostly on the 192.168.20.222 host but are also seen in a variety of other hosts in the network.

NFS Shares World Readable

Risk: High (CVSS 7.5)
Affected Systems: 192.168.20.222
Frequency: 1 instance
Mitigation: Implement proper access controls on NFS shares
Team: Systems Administration Team
Time Estimate: 1-2 days

Steps to Remediate:

1. Audit current NFS share configurations
2. Identify necessary access levels for each share
3. Implement least-privilege access controls
4. Test access for authorized and unauthorized users
5. Update documentation and monitoring

Samba Badlock Vulnerability

Risk: High (CVSS 7.5)
Affected Systems: 192.168.20.222
Frequency: 1 instance
Mitigation: Apply security patches or upgrade Samba
Team: Systems Administration Team
Time Estimate: 1-2 days

Steps to Remediate:

1. Identify the specific Samba version in use
2. Obtain and test appropriate patches
3. Schedule maintenance window
4. Apply patches or perform upgrade
5. Validate Samba functionality
6. Update security baseline documentation

rsh Service Detection

Risk: High (CVSS 7.5)
Affected Systems: 192.168.20.222
Frequency: 1 instance
Mitigation: Disable rsh service and replace with secure an alternative
Team: Systems Administration Team
Time Estimate: 4-6 hours

Steps to Remediate:

1. Identify any critical dependencies on rsh
2. Plan migration to secure alternatives (e.g., SSH)
3. Disable rsh service
4. Remove rsh-related packages
5. Update firewall rules to block rsh ports
6. Validate that rsh is no longer accessible

ISC BIND Service Vulnerabilities

Risk: High (CVSS 8.6)
Affected Systems: 192.168.20.222
Frequency: 1 instance
Mitigation: Upgrade BIND to the latest stable version
Team: Network Administration Team
Time Estimate: 2-3 days

Steps to Remediate:

1. Review current BIND configuration
2. Test upgrade in a non-production environment
3. Schedule maintenance window
4. Backup current configuration
5. Perform the upgrade
6. Validate DNS functionality
7. Update monitoring and documentation

Medium & Low Risk Vulnerabilities

Medium and low vulnerabilities pose less immediate risk but should still be remediated. It is recommended that these be remediated or have compensating controls put in place within 1-2 weeks.

DNS Server Cache Snooping

Risk: Medium (CVSS 5.3)
Affected Systems: 192.168.20.1, 192.168.10.1
Mitigation: Configure DNS servers to prevent cache snooping
Team: Network Security Team
Time Estimate: 2-3 days

Steps to Remediate:

1. Access DNS server configuration
2. Disable cache snooping
3. Implement access controls
4. Test configuration
5. Document changes

SMB Signing Not Required

Risk: Medium (CVSS 5.3)
Affected Systems: 192.168.20.222, 192.168.10.210
Mitigation: Enable SMB signing on all relevant hosts
Team: System Administration Team
Time Estimate: 2-3 days

Steps to Remediate:

1. Access group policy management
2. Create or edit group policy object
3. Enable SMB signing
4. Apply changes
5. Reboot and refresh policies
6. Document Changes

SSH Terrapin Prefix Truncation Weakness

Risk: Medium (CVSS 5.9)
Affected Systems: 192.168.10.210
Mitigation: Update SSH configurations
Team: Network Security Team
Time Estimate: 1-2 days

Steps to Remediate:

- Access SSH configuration
- Edit SSH configuration files
- Update configuration to not allow root login and to not use DNS
- Restart SSH service
- Test configuration
- Document Changes

ICMP Timestamp Request Remote Date Disclosure

Risk: Low (CVSS 2.1)
Affected Systems: All hosts
Mitigation: Configure firewalls to block ICMP timestamp requests
Team: Network Security Team
Time Estimate: 1 week

Steps to Remediate:

- Access firewall configuration
- Create new firewall rule to block incoming ICMP timestamp requests
- Apply changes
- Test the new firewall rule by monitoring logs
- Document changes

FINAL THOUGHTS

The vulnerability assessment of ACME headquarters' network has identified 287 vulnerabilities across various hosts and subnets, with critical and high-risk vulnerabilities requiring immediate remediation. The most vulnerable host, 192.168.20.222, has multiple critical issues, requiring the most attention by far.

A prioritized remediation strategy has been established, focusing on addressing critical vulnerabilities within 24-48 hours, high-risk vulnerabilities within 3-5 days, and medium and low-risk vulnerabilities within 1-2 weeks. Each vulnerability has specific remediation steps assigned to the appropriate teams.

To enhance security and reduce the risk of exploitation, it is essential to implement the recommended mitigation strategies promptly. Ongoing vulnerability management, including regular scans and updates, will be critical in maintaining a robust cybersecurity posture and protecting sensitive data. Collaboration among the Network Security, System Administration, and Network Administration teams will be vital for achieving these objectives.