Cybersecurity Risk Assessment

Title: Cybersecurity Risk Assessment For KTDA Network System.

Prepared by: Loyd Kinoti

Date: 15/09/2024

Contact Information: loyd5kinoti@gmail.com

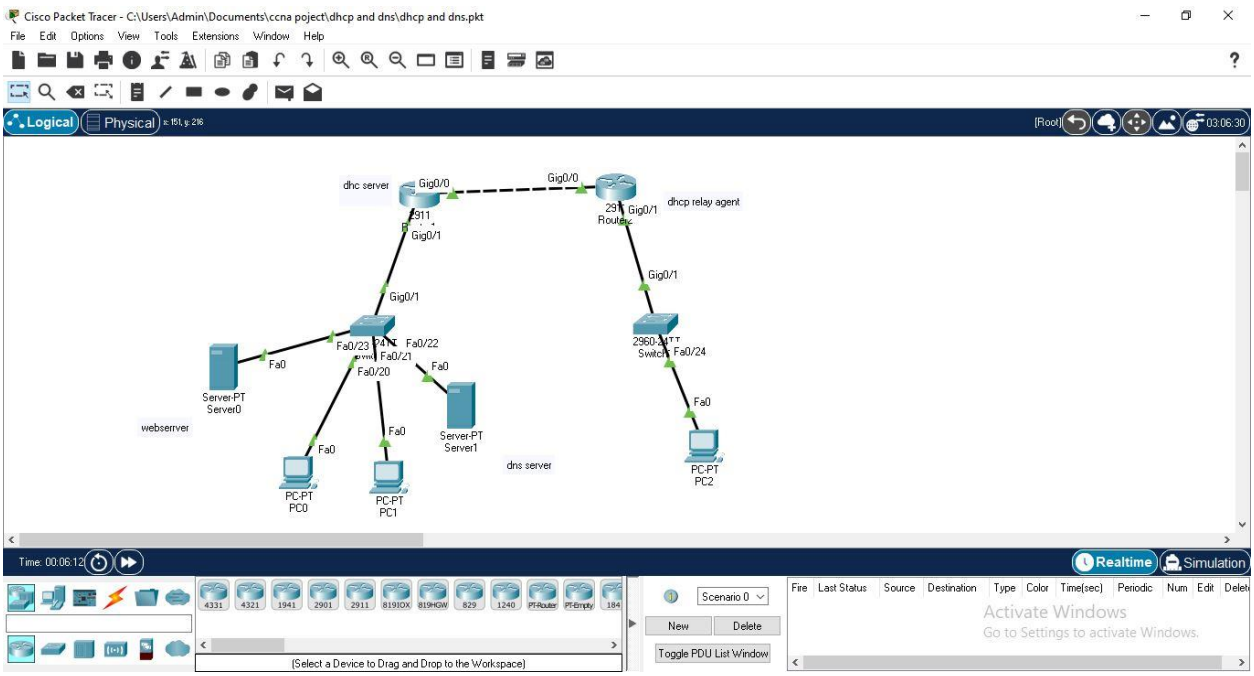
TABLE OF CONTENTS

1) Threat Identification.

a) Sample network setup for assessment.

I designed and implemented a simulated network for KTDA, a tea processing company in Kenya that manages tea purchasing and operational transactions. This network was meticulously configured to mirror the company's actual systems, allowing for comprehensive assessment and evaluation. I have attached the configured network.

b) Potential threats and vulnerabilities within the system.



Here are five major potential threats and vulnerabilities in the system:

1. DHCP Spoofing:

- A rogue DHCP server could be introduced, potentially allowing attackers to provide malicious IP configurations to clients, leading to traffic interception or redirection.

2. DNS Poisoning:

- The DNS server could be vulnerable to DNS spoofing or poisoning, where attackers redirect legitimate traffic to malicious sites, compromising the integrity of the network.

3. Lack of Network Segmentation:

- Without proper network segmentation (e.g., VLANs), the entire network could be compromised if an attacker gains access to any one device, allowing lateral movement across the network.

4. No Firewall Protection:

- The absence of visible firewall configurations between internal servers and external traffic makes the network vulnerable to attacks from external threats, such as unauthorized access or denial-of-service (DoS) attacks.

5. Unsecured Web Server:

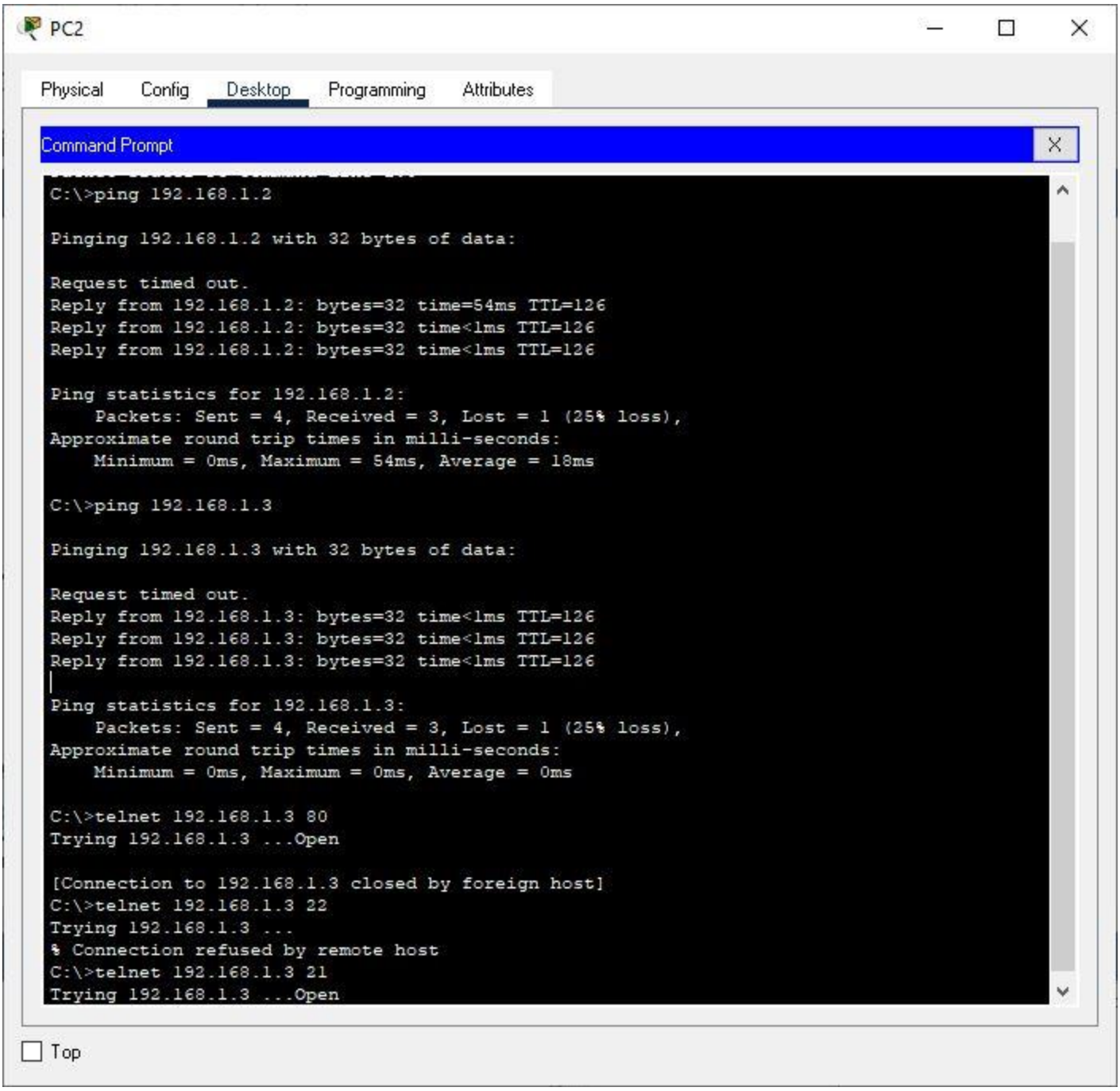
- The web server may be exposed to the internet without proper security measures, such as HTTPS encryption, leaving it vulnerable to attacks like data breaches, defacement, or DDoS.

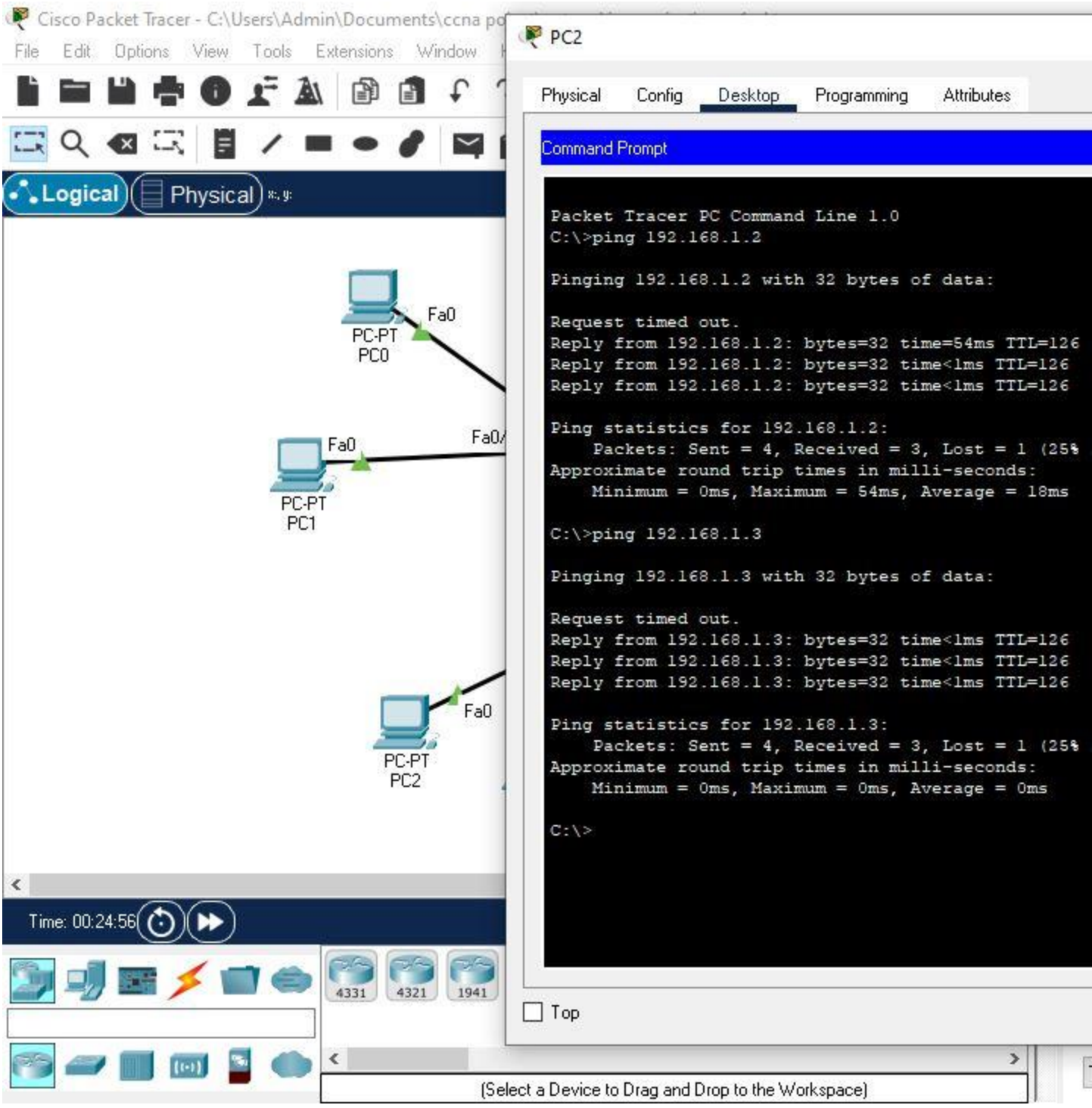
2) Vulnerability Scanning.

a) Cybersecurity tools used to conduct vulnerability scans.

I utilized Cisco Packet Tracer to simulate network environments and execute commands analogous to those used by cybersecurity tools such as Nmap and Nessus. This approach allowed me to perform vulnerability assessments and analyze network security by emulating scanning and probing techniques similar to those offered by these industry-standard tools.

b) Identified vulnerabilities, their severity, and potential impact


PC2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.2: bytes=32 time=54ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 54ms, Average = 18ms
C:\>ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
Ping statistics for 192.168.1.3:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>telnet 192.168.1.3 80
Trying 192.168.1.3 ...Open
[Connection to 192.168.1.3 closed by foreign host]
C:\>telnet 192.168.1.3 22
Trying 192.168.1.3 ...
% Connection refused by remote host
C:\>telnet 192.168.1.3 21
Trying 192.168.1.3 ...Open
Top



The following vulnerabilities, their severity, and potential impacts can be identified:

1. Packet Loss during Ping (192.168.1.2 and 192.168.1.3)

Severity: Medium

The network experiences a 25% packet loss during pings to both 192.168.1.2 and 192.168.1.3. This could indicate network congestion, a misconfigured network device, or faulty hardware.

Impact: Reduced network performance and unreliable connectivity. It could also indicate a potential attack (e.g., a DoS attack) or faulty equipment that could eventually result in a network outage.

2. Open Telnet Port (192.168.1.3:21)

Severity: High

The Telnet protocol is open and accessible on port 21 of 192.168.1.3. Telnet is an outdated protocol that transmits data in plain text, making it highly vulnerable to eavesdropping and man-in-the-middle attacks.

Impact: Attackers could intercept login credentials and gain unauthorized access to the device, leading to full system compromise.

3. Open HTTP Port (192.168.1.3:80)

Severity: High

Port 80 (HTTP) is open, but the connection is closed by the foreign host. The presence of this port indicates the system is hosting a web service. However, without HTTPS (port 443), the traffic is unencrypted, leaving it vulnerable to sniffing attacks.

Impact: Attackers could intercept sensitive data transmitted over HTTP or exploit known vulnerabilities in the web service to gain access to the server.

4. Connection Refused on Port 22 (SSH)

Severity: Medium

Port 22 (SSH) refused the connection, which may indicate SSH is not properly configured or there is a security mechanism in place to block access.

Impact: While SSH is more secure than Telnet, improper configuration could prevent legitimate remote management. If SSH is accessible without strong credentials, it could become a target for brute-force attacks.

5. Intermittent Connectivity

Severity: Medium

The intermittent "request timed out" responses in the ping tests suggest network instability, which could be due to misconfiguration, network overload, or potential attacks (such as a DoS).

Impact: Unreliable communication between network devices can lead to disruptions in service, delayed responses, or failures in critical applications.

3) Risk Analysis:

a) Identified vulnerabilities in terms of their potential risks to the system.

Vulnerability	Risk	Potential Impact	Likelihood
Packet Loss During Ping	Medium	Degraded performance, potential network outage due to congestion or DoS	Medium
Open Telnet Port	High	Eavesdropping, full system compromise, unauthorized access to sensitive data	High
Open HTTP Port	High	Data interception, web server compromise, exposure to attacks	High
Connection Refused on SSH Port	Medium	Improper remote management, potential brute-force attacks	Medium
Intermittent Connectivity	Medium	Unreliable network performance, potential service disruption	Medium

b) Prioritized vulnerabilities based on their severity and likelihood of exploitation.

The following vulnerabilities have been prioritized based on their severity and the likelihood of exploitation, starting from the most critical to the least critical:

1. Open Telnet Port (192.168.1.3:21)

Severity: High

Likelihood of Exploitation: High

Reason for Priority:

Telnet transmits data in plain text, making it extremely vulnerable to eavesdropping, credential theft, and man-in-the-middle attacks.

Attackers commonly target open Telnet ports, and the consequences of unauthorized access could result in a complete system compromise.

Action: Disable Telnet immediately and replace it with a more secure protocol like SSH.

2. Open HTTP Port (192.168.1.3:80)

Severity: High

Likelihood of Exploitation: High

Reason for Priority:

HTTP transmits data unencrypted, making any sensitive information (e.g., login credentials or business data) vulnerable to interception.

Web services running on port 80 are attractive targets for attackers, especially if they are not upgraded to HTTPS.

Action: Transition the service to HTTPS by implementing SSL/TLS certificates and secure web communication.

3. Packet Loss During Ping (192.168.1.2 and 192.168.1.3)

Severity: Medium

Likelihood of Exploitation: Medium

Reason for Priority:

Packet loss can indicate performance issues that, if left unchecked, may lead to system instability or network outages.

While less immediately exploitable by attackers, network degradation could facilitate Denial-of-Service (DoS) attacks.

Action: Investigate and resolve the root cause of packet loss (e.g., misconfigured network devices or faulty hardware).

4. Intermittent Connectivity

Severity: Medium

Likelihood of Exploitation: Medium

Reason for Priority:

Intermittent connectivity suggests network instability, which could lead to service disruptions and downtime.

Although not directly exploitable, it could be indicative of misconfigurations or underlying attacks like DoS.

Action: Review network configurations and traffic patterns, and ensure network devices are functioning properly.

5. Connection Refused on SSH Port (192.168.1.3:22)

Severity: Medium

Likelihood of Exploitation: Medium

Reason for Priority:

SSH is generally secure but could be vulnerable if misconfigured (e.g., weak credentials, improper access control).

The refusal of connection may indicate a configuration issue, but it also prevents legitimate access to remote management.

Action: Ensure that SSH is properly configured with strong credentials and access controls, and verify that legitimate users can access the system as needed.

Prioritized Vulnerabilities:

1. **Open Telnet Port** (High severity, High likelihood)
2. **Open HTTP Port** (High severity, High likelihood)
3. **Packet Loss During Ping** (Medium severity, Medium likelihood)
4. **Intermittent Connectivity** (Medium severity, Medium likelihood)
5. **Connection Refused on SSH Port** (Medium severity, Medium likelihood)

4) Mitigation Strategies:

a) Mitigation strategies for high-risk vulnerabilities.

The following are detailed mitigation strategies for the high-risk vulnerabilities identified in the KTDA network setup. These strategies aim to reduce or eliminate the risk of exploitation.

I. Open Telnet Port (192.168.1.3:21)

Telnet is an outdated protocol that transmits data in plain text, making it highly vulnerable to eavesdropping, credential theft, and man-in-the-middle attacks.

Priority:High

Mitigation Strategy:

1. Disable Telnet Services

- **Immediate Action:** Disable Telnet entirely to prevent unauthorized access. In most modern systems, Telnet should no longer be used, especially in production environments.

2. Replace Telnet with SSH:

- SSH (Secure Shell) provides encrypted communication and is a secure alternative to Telnet.

3. Restrict SSH Access:

- Use firewall rules or access control lists (ACLs) to restrict SSH access to trusted IP addresses only. This limits exposure to potential attackers.

4. Use Strong Authentication Methods:

- Enforce key-based authentication rather than password-based authentication to prevent brute-force attacks.

5. Monitor SSH Access:

- Enable logging for all SSH access attempts and review logs regularly to detect unusual activity.

II. Open HTTP Port (192.168.1.3:80)

HTTP transmits data unencrypted, making it vulnerable to data interception, sniffing attacks, and MITM attacks.

Priority:**High**

Mitigation Strategy:

1. Migrate to HTTPS (SSL/TLS):

- **Immediate Action:** Install an SSL/TLS certificate to secure web traffic and redirect all HTTP requests to HTTPS.

- **Obtain an SSL Certificate:** Use a free service like **Let's Encrypt** or purchase a certificate from a certificate authority (CA).

2. **Enforce HTTPS (Redirection):**

- Configure the web server (e.g., Apache, Nginx) to automatically redirect all HTTP traffic to HTTPS to ensure data encryption during transmission.

3. Regularly Patch and Update Web Server:

- Keep the web server and any web applications running on it up-to-date with the latest security patches to reduce the risk of exploitation from known vulnerabilities.

4. Implement Security Headers:

- Add security headers like **HTTP Strict Transport Security (HSTS)** to force browsers to only communicate over HTTPS.

5. Conduct Regular Vulnerability Scanning:

- Use tools like Nessus or OpenVAS to conduct routine vulnerability scans on the web server to identify any emerging vulnerabilities.

Summary of High-Risk Mitigation:

Vulnerability	Mitigation Actions	Priority
Open Telnet Port	- Disable Telnet entirely. - Replace with SSH. - Restrict SSH access to trusted IPs. - Use key-based authentication.	**High**
Open HTTP Port	- Install SSL/TLS certificates. - Redirect HTTP traffic to HTTPS.	**High**

Vulnerability	Mitigation Actions	Priority
	- Keep web server updated. - Use security headers.	

b) Suggest recommendations to address identified risks effectively.

To address the identified vulnerabilities and risks, the following recommendations are provided to improve the security and stability of the system:

1. Address Packet Loss

Recommendation:

- Investigate the root cause of the packet loss by analyzing network devices, connections, and traffic patterns.

- Check hardware for faults (such as bad cables or malfunctioning switches/routers).

- Review the network configuration to ensure devices are properly connected and routes are optimized.

- Monitor for potential DoS attacks by using network traffic analysis tools.

- Increase network capacity or optimize bandwidth allocation if the issue is due to congestion.

2. Close or Secure Telnet (Port 21)

Recommendation:

- Disable Telnet on all devices and replace it with SSH (Secure Shell) for secure remote access. SSH encrypts communication, ensuring that sensitive data like credentials are not transmitted in plain text.

- Enforce strong password policies and use key-based authentication for SSH to prevent brute-force attacks.

- Restrict access to SSH by configuring access control lists (ACLs) and firewall rules to limit who can connect remotely to the system.

3. Implement HTTPS (Port 80 Security)

- Recommendation:

- Upgrade the web service on `192.168.1.3` from HTTP to HTTPS (Port 443). HTTPS ensures all communication between users and the server is encrypted, preventing data interception.

- Obtain a valid SSL certificate and configure it on the server to encrypt traffic.

- Implement HTTP-to-HTTPS redirection so that users attempting to connect over HTTP are automatically redirected to the encrypted connection.

4. Secure SSH Access (Port 22)

Recommendation:

- Ensure SSH is properly configured to allow legitimate remote access while preventing unauthorized connections.

- Implement rate limiting to prevent brute-force attacks, and enforce strong password policies or SSH key-based authentication.

- Use two-factor authentication (2FA) an added layer of security.

- Apply firewall rules to limit SSH access to specific IP addresses, and monitor failed login attempts.

5. Improve Network Stability

Recommendation:

- Conduct regular network monitoring using tools like Wireshark, SolarWinds, or Nagios to detect potential performance issues and bottlenecks.

- Implement Quality of Service (QoS) policies to prioritize critical traffic and ensure that important services have sufficient bandwidth.

- Ensure firmware updates are applied to all networking equipment to fix known bugs and security vulnerabilities.

- Set up network redundancy where possible to prevent single points of failure.

6. Harden Firewall and ACLs

Recommendation:

- Review and update firewall rules to ensure only necessary ports are open, and block unused or vulnerable ports (such as Telnet or unsecured services).

- Implement Access Control Lists (ACLs) to restrict access to critical services based on IP addresses and device roles.

- Use Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor network traffic for suspicious activity and automatically block threats.

7**. Regular Vulnerability Assessments and Patching**

Recommendation:

- Conduct regular vulnerability scans using tools like Nessus or OpenVAS to identify new risks and ensure prompt patching.

- Apply security patches and updates to all software and hardware as soon as they are released to close known vulnerabilities.