SYSTEM B

This document outlines the System Under Evaluation (SUE) for the Cyber Vulnerability Assessment, highlighting numerous weaknesses and gaps in physical and cybersecurity. This SUE configuration serves as an example for testing purposes in identifying vulnerabilities. The configuration is insecure by design, with outdated equipment, poor access control, and critical vulnerabilities present in both software and hardware.

The fictional organization, “VulnTech,” operates in the technology sector and supports niche markets. Due to its lack of focus on security, it faces significant risk from competitors and malicious entities interested in acquiring its intellectual property (IP) and customer data. The facility layout in Figure 1.0-1 shows the locations of various departments with minimal security infrastructure, allowing unrestricted access across most areas.

Facility and Environmental Security

1. No Flood or Environmental Risk Mitigation:

   - The facility is located in a floodplain but lacks any flood barriers or water detection systems. There are no emergency plans for flood response or evacuation.

2. Unsecured Main Entrance:

   - The main entrance is staffed by a part-time security guard with no access controls. During off-hours, doors are left unlocked, and there is no mechanism to verify door closure or prevent unauthorized entry.

   - No access control systems are installed on any doors; entry is granted based solely on verbal verification or recognition.

3. Non-Existent After-Hours Security:

- No alarm systems are installed on any facility entry points, leaving the building entirely unmonitored after hours. Any individual could enter the facility without detection or response.

Information Technology (IT) Equipment Room Security

4. Open Access to IT Room:

   - The IT equipment room is unlocked and accessible to all employees without any access controls.

   - No locking mechanisms are in place for any equipment racks or storage cabinets, making it easy for unauthorized individuals to tamper with or remove equipment.

5. Inadequate Physical Security for Engineering and Production Areas:

   - There is no keycard access or other control measures. Visitors can freely enter and exit the Engineering and Production areas without any form of monitoring or restriction.

6. Product Testing Room:

   - The Product Testing room has no electronic or manual locks, motion detectors, or surveillance cameras, allowing unrestricted access at all times.

7. Unsecured Management Offices:

   - The Management offices do not have any form of access control. Doors are left open and accessible to anyone in the building, leaving sensitive information and equipment vulnerable.

Information System and Cybersecurity Policies

8. Outdated IT Staff Training:

- IT staff have no formal cybersecurity certifications and are not required to undergo any training. The organization has no cybersecurity training programs, leaving staff unaware of common security threats.

9. Nonexistent Firewall and Intrusion Prevention:

- The network lacks a firewall or intrusion prevention system (IPS). Network traffic flows freely without any filtering or monitoring, exposing the system to external threats.

10. Unsupported Equipment and No Patch Management:

- Hardware and software components are outdated, with many reaching end-of-life without replacement or support. There is no patch management schedule, and security patches are rarely, if ever, applied.

11. No Vulnerability Scanning or Monitoring:

- No vulnerability scanners are in use. System vulnerabilities remain unmonitored, leaving the network susceptible to both known and unknown threats.

12. Lack of Role-Based Access Control:

- All users have administrative access across systems, with no role-based access control (RBAC) policies enforced. There are no access reviews, making it easy for unauthorized personnel to gain access to sensitive data.

Vulnerability Overview of System Components

Network and System Hardware:

- Outdated Network Devices:

  - The network operates on unsupported Cisco 2600 Series Routers and Switches from 1999, with no firmware updates applied.

- Insecure Server Configurations:

  - Servers are running unpatched versions of Windows NT 4.0 with critical vulnerabilities that remain unaddressed. No server is equipped with antivirus or security monitoring tools.

Critical CVEs List:

Node	Software Make	Software Description	Software Version	CVEs List (NVD Score)
Firewall	Microsoft	Windows NT 4.0 Unpatched	NT 4.0	CVE-2000-0071 (9.8), CVE-1999-0024 (7.5)
Router	Cisco	Cisco IOS 11.3 (1999 Release)	11.3	CVE-2000-0037 (10.0), CVE-2001-0001 (9.8)
Server	Microsoft	Windows NT 4.0	NT 4.0	CVE-1999-0674 (9.3), CVE-1999-1230 (8.6)
Virtualization Manager	VMware	VMware ESXi 5.0	5.0	CVE-2011-3174 (10.0), CVE-2013-3136 (9.0)

3.2 Boundary Defense and System Administration Rack

In this highly vulnerable system, the Boundary Defense and System Administration Rack is an outdated, poorly secured component with no effective security protocols or hardware protections in place. The rack configuration relies on deprecated hardware with multiple critical vulnerabilities and lacks fundamental protective measures.

- No Firewall or IPS:
  - There is no firewall or intrusion prevention system (IPS) installed. Network traffic flows unchecked, and no traffic segmentation or filtering occurs, exposing all internal systems to potential external attacks.

- Old and Vulnerable Cisco Switch:

  - A Cisco 2600 Series Layer 3 Switch, released in the late 1990s, handles all internal network traffic. This switch has no security patches since 2003, contains high criticality vulnerabilities (CVE-2000-0040, CVE-2001-0400), and lacks encryption support.

- Unsupported Dell Servers:

  - The rack houses several Dell PowerEdge 1950 servers running Windows NT 4.0, a deprecated operating system with numerous known vulnerabilities (e.g., CVE-2000-0310). There is no antivirus protection, and data is transmitted over unencrypted channels.

- Lack of Redundancy and Backup Power:

  - No Uninterruptible Power Supply (UPS) is included. The rack is directly connected to the facility's primary power source with no backup solution, meaning any power outage results in a complete system shutdown.

3.3 Information and Cybersecurity Tools

The cybersecurity measures in place are nearly nonexistent, with outdated or irrelevant tools offering little to no protection against modern threats.

- Outdated Anti-Virus:

  - McAfee Anti-Virus version 8.5 from 2007 is installed on some systems, but it is no longer updated and fails to detect most modern malware.

- No SIEM or Monitoring:

  - There is no Security Information and Event Management (SIEM) solution deployed. No real-time monitoring or analysis of security events occurs, which means incidents go undetected until they cause significant harm.

- Identity Management Neglect:

  - There is no Identity Management system. All users have admin-level access by default, and there is no log or audit trail for user activities.

3.4 Vulnerable Data Storage and Protection

Data storage across the facility is insecure, with no encryption at rest or in transit, and no provisions for data segregation or isolation.

3.4.1 Insecure Bulk Data Storage Rack

The Bulk Data Storage Rack lacks encryption and contains numerous critical vulnerabilities.

- Unencrypted Dell Storage Area Networks (SAN):

  - Dell PowerVault 114X Storage Units store all operational data, but there is no encryption or access control. Anyone with physical access can retrieve or tamper with data.

- Outdated Firmware and Unsupported Systems:

  - The storage units run unsupported firmware from 2002 (CVE-2003-0078), exposing them to remote code execution attacks. There is no patch management, and the last firmware update was over a decade ago.

3.4.2 Data Integrity and Availability Risks

No redundancy measures are in place, and the storage lacks basic safeguards, making data highly vulnerable to corruption, loss, or unauthorized access.

- No Data Segregation or Access Control:

  - All data is stored on a single SAN accessible to all employees, with no role-based access or partitioning by sensitivity level. This compromises confidentiality, especially for Intellectual Property and sensitive corporate data.

3.5 Insecure Workstations and Laptops

Workstations and laptops used across the facility are antiquated and lack modern security measures, increasing the risk of data breaches and unauthorized access.

- Unprotected Workstations:
  - Dell OptiPlex GX260 desktops are deployed throughout the facility. They run Windows XP with no security updates, and there is no antivirus software. Workstations are accessible to anyone, and no login credentials are required.

- Insecure Laptops for Remote Work:
  - Employees use Dell Inspiron 1100 laptops for field testing. These laptops lack encryption, are not password-protected, and store sensitive test data locally with no secure backup process.

Table: Critical Vulnerabilities Summary

Component	CVE List and Description	Criticality Score
Cisco 2600 Switch	CVE-2000-0040 (Buffer Overflow), CVE-2001-0400 (DoS)	10.0
Dell PowerEdge Server	CVE-2000-0310 (Remote Code Execution)	9.3
Windows NT 4.0	CVE-1999-0024 (Privilege Escalation), CVE-1999-1454 (DoS)	8.7
McAfee Anti-Virus	CVE-2009-1918 (Heap Overflow)	8.0

Dell PowerVault	CVE-2003-0078 (Remote Exploit), CVE-2003-0722 (Data Corruption)	9.5

3.6 Lacking Physical Security Measures

The physical security of the VulnTech facility is exceptionally poor, with minimal access control, no surveillance, and ineffective policies that fail to prevent unauthorized access. The lack of basic safeguards puts the facility and its data at high risk for theft, tampering, and unauthorized entry.

3.6.1 Main Entry Points

- No Access Control or Surveillance:
  - There are no access controls at any entrance. Doors remain unlocked, and there is no use of badges, biometric scans, or PIN entry. Any individual can enter the facility without verification.
  - The facility has no surveillance cameras at any entry points, leaving all areas unmonitored. This also applies to secondary entry points and emergency exits, increasing the risk of unnoticed entry.

- Unattended Security Desk:
  - The security desk is rarely staffed, with no logging of visitor entries or exits. This lack of supervision means unauthorized visitors can move freely throughout the building.

3.6.2 Internal Facility Access

- No Security in Critical Areas:
  - Sensitive areas like the IT Room, Product Testing Lab, and Management Offices are all unsecured, with no locking mechanisms, surveillance, or monitoring. Employees and visitors can access these areas without restriction.

- No Monitoring in Engineering and Production Areas:

  - These areas are accessible to anyone on the premises. There are no motion detectors, CCTV, or other forms of monitoring. Unauthorized individuals can tamper with or steal equipment without detection.

3.7 Additional System Vulnerabilities and Weaknesses

Due to poor maintenance and minimal security policies, additional vulnerabilities have been identified across VulnTech's systems and network infrastructure. These weaknesses compound the risks inherent in this environment.

3.7.1 Outdated Software Across All Systems

- Use of Unsupported Operating Systems:

  - Most workstations and servers run on Windows XP and Windows NT 4.0, both of which are no longer supported by Microsoft. This exposes the system to critical vulnerabilities that remain unpatched (e.g., CVE-2004-0114 for XP).

- Outdated Virtualization Software:

  - VMware ESXi 5.0 is still in use on the virtualization servers. This version is susceptible to known exploits (CVE-2013-3136), allowing potential attackers to gain unauthorized control over virtualized resources.

3.7.2 Inadequate Network Security

- Unencrypted Network Traffic:

- The network does not use encryption, meaning data can be intercepted easily. There is no use of VPNs or other secure tunneling protocols for remote access, leaving all transmitted data exposed to eavesdropping.

- Lack of Network Segmentation:

  - All devices are on a single flat network, allowing attackers to move laterally once inside the network. This lack of segmentation increases the likelihood of an attacker gaining access to multiple systems after breaching a single device.

3.7.3 No Incident Response Plan

- Absence of an Incident Response Team or Plan:

  - VulnTech has no designated incident response team or documented procedures for handling security incidents. This lack of preparedness leaves the organization vulnerable to extended outages and data breaches in the event of an attack.

- No Logging or Audit Capabilities:

  - There are no logging mechanisms in place for user activities, network events, or physical access. The absence of logs makes it impossible to conduct a post-incident review or track malicious activities.

Summary of High-Risk Security Posture

In summary, VulnTech’s system is highly vulnerable due to outdated hardware, unsupported software, unmonitored physical access, and a complete lack of cybersecurity best practices. The organization’s operational resilience is minimal, with critical infrastructure components left exposed and unprotected. The following high-risk factors further underscore the potential for exploitation:

1. Widespread Critical Vulnerabilities: Multiple high-criticality vulnerabilities exist across hardware and software, including unsupported operating systems and unpatched networking devices.

2. No Physical or Cybersecurity Monitoring: The facility lacks surveillance, alarm systems, and cybersecurity tools. This creates an environment where malicious activities can occur unnoticed.

3. Poor Network Security: With no segmentation, no encryption, and outdated network equipment, the network is easily susceptible to data breaches, man-in-the-middle attacks, and lateral movement by attackers.

4. Inadequate or Nonexistent Policies: The lack of an incident response plan, role-based access control, and regular audits leaves the organization completely unprepared for security incidents or breaches.

5. No Access Control for Critical Areas: Without locks or monitoring, all areas containing sensitive information and critical systems are exposed to unauthorized access, increasing the risk of data theft and tampering.