COMPREHENSIVE RISK ASSESSMENT AND MITIGATION PLAN FOR METASPLOITABLE 2: A SHOWCASE OF CYBERSECURITY SKILLS

A SHOWCASE OF CYBERSECURITY SKILLS

This project presents a detailed risk assessment and mitigation plan for the Metasploitable 2 virtual machine, demonstrating key cybersecurity skills and methodologies. The objective of this project is to identify, evaluate, and address vulnerabilities within a simulated environment, following the ISO 27001 framework. This assessment is a practical demonstration of my ability to conduct penetration tests, analyse risks, and implement effective security measures.

Disclaimer: This project is intended for educational and demonstration purposes only. The findings and methods detailed in this report are based on a controlled, simulated environment and should not be applied to real-world systems without proper authorization and professional oversight. The techniques and vulnerabilities discussed are specific to the Metasploitable 2 machine and may not be applicable to other systems. By showcasing this project, I aim to highlight my proficiency in cybersecurity practices and my commitment to improving security postures in any professional setting.

7/18/2024

RISK ASSESSMENT REPORT

SCOPE OF THE RISK ASSESSMENT

INTRODUCTION

This risk assessment is conducted for TechSecure Inc., a cybersecurity firm specializing in training, penetration testing, and security consulting. The assessment focuses on the Metasploitable 2 virtual machine, which is utilized within the organization for cybersecurity training and internal testing purposes. This document outlines the risks, threats, vulnerabilities, and mitigation strategies associated with the services running on the Metasploitable 2 machine.

SCOPE

The scope of this risk assessment includes the following components:

1. **Assessment Target**:
    - **Virtual Machine**: Metasploitable 2
    - **IP Address**: 10.0.2.4
    - **Operating Environment**: TechSecure Inc.'s training and internal testing network
2. **Services Assessed:**
    - **Open ports and their corresponding services**
3. **Assets**:
    - **Training Infrastructure**: Virtual machines and training modules used for cybersecurity exercises
    - **Client Data**: Sensitive information from clients used in training scenarios
    - **Internal Networks**: Includes servers, workstations, and network devices supporting daily operations
4. **Risk Appetite**: **TechSecure Inc.** has a low risk appetite, prioritizing the protection of client data and maintaining high levels of trust and security. This assessment aims to identify and mitigate vulnerabilities that could compromise the integrity, confidentiality, and availability of critical assets.
5. **Objectives:**
    - **Identify Vulnerabilities**: Discover and document vulnerabilities present in the Metasploitable 2 virtual machine.
    - **Assess Risks**: Evaluate the potential impact and likelihood of exploitation of identified vulnerabilities.
    - **Recommend Mitigations**: Provide actionable recommendations to mitigate identified risks and enhance the security posture of the training infrastructure
    - **Ensure Compliance**: Align with industry best practices and regulatory requirements relevant to cybersecurity training environments.
6. **Exclusions:**

- This assessment does not cover other virtual machines, servers, or network devices outside the specified training environment.
- Third-party applications and services not running on the Metasploitable 2 machine are excluded.

ASSET INVENTORY:

METASPLOITABLE 2 MACHINE:

- Description: A deliberately vulnerable Linux virtual machine used for security training and testing
- IP Address: 10.0.2.4
- Purpose: Testing and training environment for penetration testing and cybersecurity exercises.

SERVICES RUNNING ON METASPLOITABLE 2

Port	Service	Version
21	FTP	220 (vsFTPd 2.3.4)
22	SSH	OpenSSH 4.7p1 Debian 8ubuntu1
23	Telnet	Linux telnetd
53	DNS	ISC BIND 9.4.2
80	HTTP	Apache httpd 2.2.8
111	RCPBind	2 (RPC #100000)
139	NetBIOS-SSN	Samba smbd 3.X - 4.X
445	NetBIOS-SSN	Samba smbd 3.X - 4.X
512	exec	netkit-rsh rexecd
513	login	OpenBSD or Solaris rlogind
513	Shell	OpenBSD or Solaris rshd
1099	Java RMI Registry	GNU Classpath grmiregistry
1524	ingreslock Backdoor	Metasploitable root shell
2049	NFS	2-4 (RPC #100003)
2121	ccproxy-ftp	220 ProFTPD 1.3.1 Server (Debian) [::ffff:10.0.2.4]
3306	MySQL	MySQL 5.0.51a
3632	distccd	DistCC 2.18.3
5432	PostgreSQL	PostgreSQL DB 8.3.0 - 8.3.7

THREAT ANALYSIS OF OPEN PORTS AND SERVICES: IDENTIFYING RISKS

Port 21 FTP vsftpd 2.3.4:

Port		Service	Version
21		FTP	vsFTPd 2.3.4
Threats identified	**Vulnerabilities Found**	**Risk/CVSS Score**	**References**
Backdoor command execution (CVE-2011-2523)	Unauthorized access (anonymous login), FTP bounce attacks	Critical 10.0	NIST ExploitDB: vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)

EXPLANATION:

Threats identified:

- Backdoor command execution (CVE-2011-2523): This vulnerability allows attackers to execute arbitrary commands on the FTP server, compromising its security.
- Unauthorized access (anonymous login), FTP bounce attacks: These are common threats associated with FTP services, where anonymous access can lead to unauthorized file access, and FTP bounce attacks can be used to bypass security measures.

Vulnerabilities Found:

- Unauthorized access (anonymous login): vsFTPd 2.3.4 allows anonymous access by default, which can lead to unauthorized data access.
- FTP bounce attacks: The FTP service may be vulnerable to bounce attacks, where an attacker can use the server to connect to other servers indirectly.

Risk Level:

- High: The presence of the CVE-2011-2523 vulnerability with a CVSS Base Score of 10.0 poses a significant risk to the confidentiality, integrity, and availability of the FTP service and potentially the entire system.

References:

- **CVE-2011-2523:** Detailed vulnerability information and severity rating from NIST.
- **ExploitDB:** Lists an exploit targeting vsFTPd 2.3.4 for backdoor command execution (Metasploit), indicating active exploitation potential.

Port 22 SSH OpenSSH 4.7p1 Debian 8ubuntu1

<table>
<tr><th colspan="4">Port</th><th colspan="4">Service</th><th colspan="4">Version</th></tr>
<tr><td colspan="4">22</td><td colspan="4">SSH</td><td colspan="4">OpenSSH 4.7p1 Debian 8ubuntu1</td></tr>
<tr><th colspan="3">Threats identified</th><th colspan="3">Vulnerabilities Found</th><th colspan="3">Risk/CVSS Score</th><th colspan="3">References</th></tr>
<tr><td colspan="3">CVE-2023-51385.</td><td colspan="3">CVE-2023-51385: OS command injection might occur if a username or hostname contains shell metacharacters, and is referenced by an expansion token.</td><td colspan="3">Critical
9.8</td><td colspan="3">NIST</td></tr>
<tr><td colspan="3">CVE-2023-51384.</td><td colspan="3">Destination constraints in ssh-agent are incompletely applied, potentially affecting the security of PKCS#11-hosted private keys.</td><td colspan="3">Medium
5.5</td><td colspan="3">NIST</td></tr>
</table>

EXPLANATION:

Threats identified:

- CVE-2023-51385: OS command injection might occur if a username or hostname contains shell metacharacters, and is referenced by an expansion token.
- CVE-2023-51384: Destination constraints in ssh-agent are incompletely applied, potentially affecting the security of PKCS#11-hosted private keys.

Vulnerabilities Found:

CVE-2023-51385:

- The issue arises when usernames or hostnames contain shell metecharacters (special characters used in command shells).
- These metacharacters are not properly sanitised or escaped when referenced by an expansion token.
- Expansion tokens are typically used in configuration files or scripts to dynamically insert value

Impact:

- Execute unauthorised commands on the system
- Elevate privileges
- Access sensitive information
- Potentially take control of the system

CVE-2023-51384:

- PKCS#11 is a standard for cryptographic token s, often used for storing private keys securely.
- Ssh-agent is supposed to apply contraints on which destinations (servers) can use these keys
- The vulnerability suggests that these constrains are not fully enforced, potentially allowing keys to be used for unintended destinations.

Impact:

- Use private keys for unauthorised destinations
- Potentially impersonate the key owner on unintended systems
- Bypass security measures intended to limit key usage

Risk Level:

CVE-2023-51385:

- Critical
- High impact on confidentiality, integrity and availability.

CVE-2023-51384:

- Medium
- High impact on confidentiality
- Medium impact on integrity and availability.

References:

- **CVE-2023-51385, CVE-2023-51384:** Detailed vulnerability information and severity rating from NIST.
- **NVD.NIST.GOV:** Detailed vulnerability information.

Port 23 Telnet Linux telnetd

<table>
<tr><th colspan="4">Port</th><th colspan="4">Service</th><th colspan="4">Version</th></tr>
<tr><td colspan="4">23</td><td colspan="4">Telnet</td><td colspan="4">Linux telnetd</td></tr>
<tr><th colspan="3">Threats identified</th><th colspan="3">Vulnerabilities Found</th><th colspan="3">Risk/CVSS Score</th><th colspan="3">References</th></tr>
<tr><td colspan="3">CVE-2022-1039</td><td colspan="3">The weak password on the web user interface can be exploited via HTTP or HTTPS.</td><td colspan="3">Critical
Score: 9.6</td><td colspan="3">NIST</td></tr>
</table>

EXPLANATION:

Threats identified:

CVE-2022-1039: The weak password on the web user interface can be exploited via HTTP or HTTPS/

Vulnerabilities Found:

The weak password on the web user interface can be exploited via HTTP or HTTPS. Once such access has been obtained, the other passwords can be changed. The weak password on Linux accounts can be accessed via SSH or Telnet, the former of which is by default enabled on trusted interfaces. While the SSH service does not support root login, a user logging in using either of the other Linux accounts may elevate to root access using the su command if they have access to the associated password.

Risk Level:

- Critical
- Critical impact on confidentiality, integrity and availability.

References:

- **CVE-2022-1039:** Detailed vulnerability information and severity rating from NIST.

Port 53 DNS SC BIND 9.4.2

Port	Service	Version
53	DNS	ISC BIND 9.4.2

Threats identified	Vulnerabilities Found	Risk/CVSS Score	References
CVE-2008-4163	Allows remote attackers to cause a denial of service	High 7.8	Nvd.nist.gov

EXPLANATION:

Threats identified:

CVE-2008-4163

Vulnerabilities Found:

Unspecified vulnerability in ISC BIND 9.3.5-P2-W1, 9.4.2-P2-W1, and 9.5.0-P2-W1 on Windows allows remote attackers to cause a denial of service (UDP client handler termination) via unknown vectors.

Risk Level:

- High
- No impact on confidentiality and integrity
- Critical impact on availability

References:

- **CVE-20008-4163:** Detailed vulnerability information and severity rating from NIST.

Port 80 HTTP Apache httpd 2.2.8

<table>
<tr><th colspan="4">Port</th><th colspan="4">Service</th><th colspan="4">Version</th></tr>
<tr><td colspan="4">80</td><td colspan="4">HTTP</td><td colspan="4">Apache httpd 2.2.8</td></tr>
<tr><th colspan="3">Threats identified</th><th colspan="3">Vulnerabilities Found</th><th colspan="3">Risk/CVSS Score</th><th colspan="3">References</th></tr>
<tr><td colspan="3">CVE-2008-2364</td><td colspan="3">Version 2.2.8 does not limit number of forwarded interim responses allowing remote HTTP servers to cause a DoS</td><td colspan="3">Medium
5.0</td><td colspan="3">Nvd.nist.org</td></tr>
</table>

EXPLANATION:

Threats identified:

CVE-2008-2364

Vulnerabilities Found:

The ap_proxy_http_process_response function in mod_proxy_http.c in the mod_proxy module in the Apache HTTP Server 2.0.63 and 2.2.8 does not limit the number of forwarded interim responses, which allows remote HTTP servers to cause a denial of service (memory consumption) via a large number of interim responses.

Risk Level:

- Medium
- No impact on confidentiality and integrity
- partial impact on availability

References:

- **CVE-20008-2364:** Detailed vulnerability information and severity rating from NIST.

Port 111 RCPBind 2 (RPC #100000)

Port	Service	Version
80	HTTP	Apache httpd 2.2.8

Threats identified	Vulnerabilities Found	Risk/CVSS Score	References
CVE-2022-47562	Vulnerability in the RCPbind service running on UDP port (111), allowing a remote attacker to create a denial of service (DoS) condition.	High 7.5	Nvd.nist.org

EXPLANATION:

Threats identified:

CVE-2022-47562

Vulnerabilities Found:

Vulnerability in the RCPbind service running on UDP port (111), allowing a remote attacker to create a denial of service (DoS) condition.

Impact:

- Disrupt the RCPBind service
- Potentially affect other RPC-dependent service
- Cause system instability or unresponsiveness

Risk Level:

- High
- No impact on confidentiality and integrity
- High impact on availability

References:

- **CVE-2022-47562:** Detailed vulnerability information and severity rating from NIST.

Port 139 NetBios-SSN Samba smbd 3.X - 4.X

Port	Service	Version
139	NetBios-SSN	Samba smbd 3.X - 4.X

Threats identified	Vulnerabilities Found	Risk/CVSS Score	References
CVE-2015-5252	Allows remote attackers to bypass intended file-access restrictions via a symlinks that points outside of a share.	High 7.2	Nvd.nist.org

EXPLANATION:

Threats identified:

CVE-2015-5252: vfs.c in smbd in Samba 3.x and 4.x before 4.1.22, 4.2.x before 4.2.7, and 4.3.x before 4.3.3, when share names with certain substring relationships exist, allows remote attackers to bypass intended file-access restrictions via a symlink that points outside of a share.

Vulnerabilities Found:

vfs.c in smbd in Samba 3.x and 4.x before 4.1.22, 4.2.x before 4.2.7, and 4.3.x before 4.3.3, when share names with certain substring relationships exist, allows remote attackers to bypass intended file-access restrictions via a symlink that points outside of a share.

Impact:

If exploited, an attacker could:

- Access files and directories that should be exploited.
- Potentially read, modify or delete sensitive data outside the intended share.
- Escalate privileges within the system.

Risk Level:

- High
- Low impact on confidentiality and integrity
- No impact on availability

References:

- **CVE-2015-5252:** Detailed vulnerability information and severity rating from NIST.

Port 512 exec netkit-rsh rexecd

Port	Service	Version
512	exec	netkit-rsh rexecd

Threats identified	Vulnerabilities Found	Risk/CVSS Score	References
CVE-2023-38336	Allows command injection via filenames because /bin/bash/sh is used by susytem.	Critical 9.8	Nvd.nist.org

EXPLANATION:

Threats identified:

netkit-rcp in rsh-client 0.17-24 allows command injection via filenames because /bin/sh is used by susystem, a related issue to CVE-2006-0225, CVE-2019-7283, and CVE-2020-15778.

Vulnerabilities Found:

The vulnerability exists in the netkit-rcp component, which is part of the rsh-client package. It allows for command injection through filenames due to the use of /bin/sh by the system function.

Impact:

If successfully exploited, an attacker could:

- Execute arbitrary commands with the privileges of the user running netkit-rcp
- Gain unauthorised access to the system
- Modify or delete files
- Potentially escalate privileges if netkit-rcp is run with elevated permissions.

Risk Level:

- High
- High impact on confidentiality, integrity and availability

References:

- **CVE-2023-38336:** Detailed vulnerability information and severity rating from NIST.

Port 513 Login OpenBSD or Solaris rlogind

Port	Service	Version
513	Login	OpenBSD or Solaris rlogind

Threats identified	Vulnerabilities Found	Risk/CVSS Score	References
CVE-2008-4247	Allows users to conduct remote attackers to conduct cross-site request forgery amd execute arbitrary FTP commands	High 7.5	Nvd.nist.org

EXPLANATION:

Threats identified:

CVE-2008-4247: ftpd in OpenBSD 4.3, FreeBSD 7.0, NetBSD 4.0, Solaris, and possibly other operating systems interprets long commands from an FTP client as multiple commands, which allows remote attackers to conduct cross-site request forgery (CSRF) attacks and execute arbitrary FTP commands via a long ftp:// URI that leverages an existing session from the FTP client implementation in a web browser.

The primary threats associated with this CVE:

1. **Cross-Site Request Forgery (CSRF)**
2. **Execution of arbitrary FTP commands**

Vulnerabilities Found:

The vulnerability comes from how the FTPD interprets long commands received from an FTP client:

- Ftpd incorrectly processes long commands by splitting them into multiple commands
- This behaviour can be exploited through specialty crafted long ftp:// URLs.

Impact:

If successfully exploited, an attacker could:

- Execute unauthorised FTP commands on the server
- Perform actions on behalf of the authenticated user without their knowledge or consent.
- Potentially access, modify or delete files on the FTP server

- Compromise the integrity and confidentiality of data stored on the FTP server

Risk Level:

- High
- partial impact on confidentiality, integrity and availability as it could lead to compromise of data.

References:

- **CVE-:** Detailed vulnerability information and severity rating from NIST.
-

Port 1099 Java RMI Registry GNU Classpath grmregistry

Port	Service	Version
1099	Java RMI Registry	GNU Classpath grmregistry

Threats identified	Vulnerabilities Found	Risk/CVSS Score	References
CVE-2023-37895	Allows remote code execution due to how java allows objects to be serialized and deserialised.	Critical 9.8	Nvd.nist.org

EXPLANATION:

Threats identified:

Vulnerability in the Apache Jackrabbit web application and standalone server allows attackers to execute arbitrary code remotely through a Java object deserialization flaw. This affects versions up to 2.20.10 (stable) and 2.21.17 (unstable). The vulnerability is rooted in the use of the commons-beanutils component, which contains a class that can be exploited for remote code execution (RCE) over RMI (Remote Method Invocation).

Vulnerabilities Found:

- **Java Object Deserialization:** Java allows objects to be serialized and deserialized, which means converting objects to a byte stream and reconstructing them back into objects. If untrusted data is deserialized, it can lead to remote code execution.
- **RMI (Remote Method Invocation):** RMI allows remote communication between Java programs. Jackrabbit's RMI interface is vulnerable because it uses commons-beanutils, which has a class exploitable through deserialization.
- **Commons-beanutils:** This library contains utility classes for manipulating Java beans and is included in Jackrabbit. It has known vulnerabilities in handling deserialization that can be exploited.

Impact:

- **Remote Code Execution (RCE):** Attackers can execute arbitrary code on the server running Jackrabbit by exploiting the deserialization vulnerability via RMI.
- **Exposure:** The mere presence of an exploitable class on the classpath can be sufficient for exploitation, even if Jackrabbit itself is not directly vulnerable anymore.

Risk Level:

- High
- High impact on confidentiality, integrity and availability

References:

- **CVE-2023-37895:** Detailed vulnerability information and severity rating from NIST.

Port 1524 ingresslock backdoor Metasploitable root shell

Port	Service	Version
1524	Ingreslock Backdoor xinetd (Extended Internet Services Daemon)	Metasploitable root shell

Threats identified	Vulnerabilities Found	Risk/CVSS Score	References
Backdoor	Unauthorized root access via a backdoor	Critical 9	Nvd.nist.org

EXPLANATION:

Threats identified:

The Ingreslock backdoor on port 1524 in Metasploitable 2 is a well-known security vulnerability that allows unauthorized users to gain root access to the system with minimal effort. This port is intentionally left open to demonstrate the dangers of improperly secured services and backdoors.

Vulnerabilities Found:

- **Ingreslock Backdoor:** The Ingreslock service on port 1524 is configured to allow remote access through a backdoor. This backdoor is implemented via the xinetd daemon, which manages Internet-based services on Unix-like systems.
- **xinetd Daemon:** xinetd is a more secure replacement for inetd, the Internet services daemon. It provides access control, logging, and resource management for services.
- **Backdoor Implementation:** In the case of Metasploitable 2, xinetd is configured to listen on port 1524 for connections. When a connection is made, the service provides a shell with root privileges.

Impact:

- Root Access: The backdoor provides root-level access to the attacker, which means they have complete control over the system.

- Privilege Escalation: Since the backdoor bypasses any authentication mechanisms, it represents a critical security flaw.
- Ease of Exploitation: The simplicity of the exploit (just using a netcat command) means that even low-skilled attackers can gain root access.

Risk Level:

- High
- High impact on confidentiality, integrity and availability as it allows root access to the machine thus allowing the attacker to do as they please

References:

- NMAP, Penetration Test conducted

Port 3306 MySQL MySQL 5.0.51a

Port	Service	Version
3306	MySQL	MySQL 5.0.51a

Threats identified	Vulnerabilities Found	Risk/CVSS Score	References
CVE-2009-4484	Stack-based Buffer Overflow	High 7.5	Nvd.nist.org

EXPLANATION:

Threats identified:

Multiple stack-based buffer overflows in the CertDecoder::GetName function in src/asn.cpp in TaoCrypt in yaSSL before 1.9.9, as used in mysqld in MySQL 5.0.x before 5.0.90, MySQL 5.1.x before 5.1.43, MySQL 5.5.x through 5.5.0-m2, and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption and daemon crash) by establishing an SSL connection and sending an X.509 client certificate with a crafted name field, as demonstrated by mysql_overflow1.py and the vd_mysql5 module in VulnDisco Pack Professional 8.11. NOTE: this was originally reported for MySQL 5.0.51a.

Vulnerabilities Found:

- This vulnerability is a stack-based buffer overflow in the CertDecoder::GetName function.
  - The vulnerability occurs in the TaoCrypt library used by yaSSL, which is an SSL/TLS library.

Impact:

- **Arbitrary Code Execution**: The crafted certificate can cause a buffer overflow, allowing the attacker to execute arbitrary code on the server.
- **Denial of Service**: The buffer overflow can also cause memory corruption, leading to a crash of the MySQL daemon (mysqld), resulting in a denial of service.

Risk Level:

- High
- Partial impact to confidentiality, Integrity and Availability.
- High score due to its exploitability score which is a 10.0.

References:

- **CVE-2009-4484:** Detailed vulnerability information and severity rating from NIST.

Port 5432 PostgreSQL PostgreSQL DB 8.3.0-8.3.7

<table>
<tr><th colspan="4">Port</th><th colspan="4">Service</th><th colspan="4">Version</th></tr>
<tr><td colspan="4">5432</td><td colspan="4">PostgreSQL</td><td colspan="4">PostgreSQL DB 8.3.0 - 8.3.7</td></tr>
<tr><th colspan="3">Threats identified</th><th colspan="3">Vulnerabilities Found</th><th colspan="3">Risk/CVSS Score</th><th colspan="3">References</th></tr>
<tr><td colspan="3">CVE-2009-0922</td><td colspan="3">Allows remote authenticated users to cause a denial of service</td><td colspan="3">Medium
4.0</td><td colspan="3">Nvd.nist.org</td></tr>
</table>

EXPLANATION:

Threats identified:

CVE-2009-0922: PostgreSQL before 8.3.7, 8.2.13, 8.1.17, 8.0.21, and 7.4.25 allows remote authenticated users to cause a denial of service (stack consumption and crash) by triggering a failure in the conversion of a localized error message to a client-specified encoding, as demonstrated using mismatched encoding conversion requests.

Vulnerabilities Found:

Denial of service (DoS) caused by memory corruption in the intarray contrib module.

Impact:

- Arbitrary Code Execution: Exploiting the memory corruption may allow an attacker to execute arbitrary code on the server.
- Denial of Service: The memory corruption can cause the PostgreSQL server to crash, resulting in a denial of service.

Risk Level:

- Medium
- No impact to Confidentiality and Integrity and partial impact to Availability.

References:

- **CVE-2009-0922:** Detailed vulnerability information and severity rating from NIST.

IMPACT ON ORGANIZATION: ASSESSING THE IMPACT OF THE VULNERABILITIES ON THE ORGANIZATION

Critical Impact Considerations:

- **Data Confidentiality:** Unauthorized data access and exfiltration.
- **Data Integrity:** Modification or deletion of sensitive data.
- **Service Availability:** Disruption of critical services affecting business operations.

Likelihood Determination:

Likelihood is based on the exploitability scores from CVE databases and the probability of exploitation given the existing security controls and threat landscape.

Port	Service & Version	Impact	Likelihood of Occurrence	Reason
21	FTP/220 (vsFTPd 2.3.4)	High	High	Unauthenticated remote attackers can upload files leading to potential data exfiltration and system compromise.
22	SSH/ OpenSSH 4.7p1 Debian 8ubuntu1	High	High	2023-51385 allows OS command injection with a sore of 9.8, leading to unauthorised command execution.
23	Telnet/ Linux telnetd	High	High	CVE-2022-1039 exploits weak passwords, allowing full system control and password changes via HTTP/HTTPS.
53	DNS/ ISC BIND 9.4.2	High	Medium	CVE-2008-4163 allows DoS, disrupting DNS services and impacting service availability.
80	HTTP/ Apache httpd 2.2.8	Medium	Medium	CVE-2008-2364 allows DoS by forwarding interim responses, impacting service availability.
111	RCPBind/2 (RPC #100000)	High	Medium	CVE-2022-47562 allows DoS, impacting RPC-dependent services and causing system instability.
139	NetBIOS-SSN / Samba smbd 3.X -	High	Medium	CVE-2015-5252 allows file-access restrictions bypass via symlinks, potentially leading to

	4.X			unauthorized data access.
445	NetBIOS-SSN/ Samba smbd 3.X - 4.X	High	Medium	Same as port 139, due to the use of Samba smbd services.
512	Exec/netkit-rsh rexecd	Critical	High	CVE-2023-38336 allows command injection via filenames, leading to unauthorized command execution.
513	Login/ OpenBSD or Solaris rlogind	Critical	High	Remote code execution through weak configurations, impacting system control and data integrity.
1099	Java RMI Registry/ GNU Classpath grmiregistry	High	Medium	Potential for remote code execution through insecure RMI registry configurations.
1524	ingreslock Backdoor/ Metasploitable root shell	Critical	High	Direct access to a root shell, leading to full system control and data manipulation.
3306	MySQL	High	Medium	CVE-2009-4484 allows buffer overflow, leading to arbitrary code execution or DoS.
5432	PostgreSQL	Medium	Medium	CVE-2009-0922 allows DoS through memory corruption, impacting database availability.

RISK MITIGATION AND TREATMENT PLAN

INTRODUCTION

The purpose of this mitigation and treatment plan is to address the vulnerabilities identified within the system, Metasploitable 2, with the goal of protecting confidentiality, integrity, and availability. Client data and network infrastructure are of utmost importance, and the strategies outlined below aim to protect these assets.

The main objectives of the plan:

- To reduce risk to a degree which limits the exposure and exploitability of vulnerabilities found,
- Comply with security policies and standards (ISO 27001).
- Protect information assets and client data.

Key Findings:

- Majority of vulnerabilities found are of critical and high impact nature which have a high impact on Confidentiality, Integrity and Availability.
- Many vulnerabilities are due to outdated versions of services.
- Vulnerabilities were identified through a combination of a Penetration Testing, Nmap scans and CVE databases.

Port	Service & Version	Strategy
21	FTP/220 (vsFTPd 2.3.4)	Upgrade vsFTPd to the latest version. Disable anonymous FTP if not needed.
22	SSH/ OpenSSH 4.7p1 Debian 8ubuntu1	Upgrade OpenSSH to the latest version. Use strong authentication methods and restrict root login.
23	Telnet/ Linux telnetd	Disable Telnet service and replace with SSH.
53	DNS/ ISC BIND 9.4.2	Upgrade BIND to the latest stable version. Implement DNSSEC to improve DNS security.
80	HTTP/ Apache httpd 2.2.8	Upgrade Apache to the latest version. Apply necessary patches and disable unused modules.
111	RCPBind/2 (RPC #100000)	Upgrade RPC services and apply security patches. Restrict RPC services to trusted networks.
139		Upgrade Samba to the latest version. Configure

	NetBIOS-SSN / Samba smbd 3.X - 4.X	file permissions and restrict access.
445	NetBIOS-SSN/ Samba smbd 3.X - 4.X	Same as port 139, due to the use of Samba smbd services.
512	Exec/netkit-rsh rexecd	Disable the rsh service. Replace with more secure alternatives such as SSH.
513	Login/ OpenBSD or Solaris rlogind	Disable rlogind service and replace with SSH.
1099	Java RMI Registry/ GNU Classpath grmiregistry	Upgrade Java and configure secure RMI registry settings. Restrict access to the registry.
1524	ingreslock Backdoor/ Metasploitable root shell	Remove the backdoor shell or restrict access to trusted users. Monitor for unauthorized access.
3306	MySQL	Upgrade MySQL to the latest version. Implement strong authentication and encryption for connections.
5432	PostgreSQL	Upgrade PostgreSQL to the latest version. Apply necessary patches and configure secure settings.

Approach to Risk Mitigation:

- Due to many of the vulnerabilities being outdated versions of services and well documented CVE details, the approach was to update, replace or close services to ensure the protection of assets.
- Vulnerabilities were prioritized based on CVE details and CVSS scores and the impact to Confidentiality, Integrity and Availability.

MITIGATION STRATEGIES:

The mitigation strategies include a combination of technical controls and process improvements:

- Upgrading Software Versions: Ensure all software and services are updated to their latest stable versions to mitigate known vulnerabilities.
- Applying Security Patches: Regularly apply security patches to address newly discovered vulnerabilities.
- Disabling Vulnerable Services: Disable or remove services that are not needed or are inherently insecure, such as Telnet and rsh.
- Implementing Stronger Authentication Mechanisms: Enforce the use of strong passwords and multi-factor authentication where possible.

- Configuring Secure Settings: Apply secure configurations to services, such as enabling encryption, restricting access, and hardening server settings.

RISK TREATMENT PLAN:

The risk treatment plan details specific actions, responsible parties, and timelines:

- Upgrading vsFTPd: Update to the latest version and disable anonymous access. Responsible: IT Operations. Timeline: Immediate.
- Upgrading OpenSSH: Update to the latest version and restrict root login. Responsible: IT Security. Timeline: Immediate.
- Disabling Telnet: Replace Telnet with SSH. Responsible: IT Operations. Timeline: Immediate.
- Upgrading BIND: Update to the latest version and implement DNSSEC. Responsible: Network Team. Timeline: Within one month.
- Upgrading Apache: Update to the latest version, apply patches, and disable unused modules. Responsible: Web Team. Timeline: Within one month.
- Monitoring and Regular Audits: Continuous monitoring for new threats and regular security audits. Responsible: IT Security. Timeline: Ongoing.

EXPECTED OUTCOMES:

The implementation of this plan is expected to:

- Significantly reduce the risk of security breaches by addressing critical and high-impact vulnerabilities.
- Enhance the overall security posture of SecureTech Solutions, ensuring better protection of client data and network infrastructure.
- Ensure compliance with ISO 27001 standards, demonstrating a commitment to security and risk management.
- Create a proactive security culture within the organization, with continuous improvements and updates to address new vulnerabilities.

CONTINUOUS MONITORING AND IMPROVEMENT:

To maintain and improve security:

- Conduct ongoing vulnerability scans and penetration tests to identify new vulnerabilities.
- Regularly update software and services to mitigate newly discovered vulnerabilities.
- Perform regular security audits and reviews to ensure compliance with security policies and standards.
- Keep security policies and procedures up-to-date and ensure staff are trained on security best practices.