Analysis the security of Metasploitable 2

2023

CROCUS

Table of Contents

Introduction

Strong cybersecurity measures are crucial in the linked world of today, where information technology is the foundation of many different sectors. It is critical to comprehend possible weaknesses and assess the efficacy of security solutions as organizations work to defend their systems and preserve sensitive data.

This research seeks to carry out a thorough security analysis of Metasploitable 2, a virtual computer made specifically susceptible for penetration testing and security evaluations. Cybersecurity experts frequently utilise Metasploitable 2 as a teaching and research tool, which enables them to comprehend the techniques used by attackers and create effective defences.

The goal of this investigation is to pinpoint all of Metasploitable 2's security flaws and offer mitigation tactics to strengthen its overall security posture. We can learn a lot about actual attack scenarios by investigating the flaws in this system that are meant to be vulnerable. This will make it easier for us to protect against comparable threats.

In order to safeguard crucial infrastructure and sensitive data, we undertook this security study of Metasploitable 2 in an effort to better understand the possible vulnerabilities related to weak systems and the OSI protocol. In the end, the report's conclusions will aid in the creation of more effective security protocols and support organizations in their efforts to create a safe and resilient online environment.

By doing this security research of Metasploitable 2, we hope to better understand the possible hazards connected with weak systems and improve our capacity to safeguard sensitive information and vital infrastructure. In the end, the report's conclusions will aid in the creation of more effective security protocols and support organisations in their efforts to create a safe and resilient online environment.

Overview

Overview: The project's goal is to examine the security of Metasploitable 2, a virtual machine that is intentionally susceptible and used for security audits and penetration testing. The project tries to uncover and examine the flaws in Metasploitable 2 as well as the hazards that might result from them. It also makes suggestions for enhancing the system's security posture.

Methodology for Security Analysis

System Setup: The first step in conducting a security study is to create a controlled environment. In order to do this, the Metasploitable 2 virtual machine must be installed on a secure network segment or in a closed lab setting.

Backup and recovery: For Metasploitable 2, implement a regular backup method. The ability to swiftly restore the system to a known safe state is ensured by keeping current backups in the event of a successful attack or system compromise.

Recommendations and Mitigation Techniques: In order to strengthen Metasploitable 2's security, a number of recommendations and mitigation techniques are put forth based on the vulnerabilities found and the threats they pose. To reduce the risks detected, these suggestions can include updating vulnerable software, putting in place secure settings, network segmentation, and other recommended practices.

Documentation and Reporting: Finally, a thorough report summarizing the findings, methodology, vulnerabilities found, and suggested corrective measures is produced. The study is a resource that stakeholders may use to better understand Metasploit able 2's security posture and to guide their choices for enhancing its overall security.

Exploitation and penetration testing: In this stage, ethical hacking methods are used to take advantage of the vulnerabilities found and break into the Metasploitable 2 system. To mimic real-world attack scenarios and evaluate the system's resistance to such attacks, a variety of penetration testing tools are used, such as Metasploit Framework.

Metasploitable 2 installation process and network configuration

Description

Metasploitable 2 Installation Process:

The installation process of Metasploitable 2 involves the following steps:

Step 1: Virtualization Environment Setup:

- Install a virtualization software such as VMware Workstation or VirtualBox on the host machine.
- Ensure that the host machine meets the minimum system requirements for the virtualization software.

Step 2: Metasploitable 2 Image Download:

- Obtain the Metasploitable 2 virtual machine image from a reliable source.
- The image is typically available in the form of an OVA (Open Virtualization Archive) file.

Step 3: Importing the Metasploitable 2 Image:

- Open the virtualization software and create a new virtual machine.
- Choose the option to import an existing virtual machine and select the Metasploitable 2 OVA file.
- Follow the on-screen instructions to complete the import process.

Step 4: Virtual Machine Configuration:

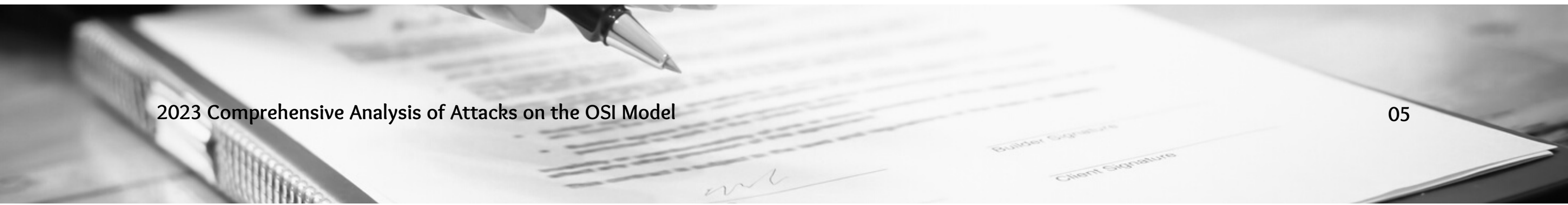
- Configure the virtual machine settings according to the desired specifications.
- Allocate sufficient resources such as CPU, memory (RAM), and storage to the Metasploitable 2 virtual machine.
- Adjust any other settings as needed, such as networking and display options.

Step 5: Powering on the Virtual Machine:

- Start the Metasploitable 2 virtual machine within the virtualization software.
- The virtual machine will boot up and initiate the necessary configurations.

Step 6: Completing the Installation:

- Once the virtual machine has booted up, the installation process is complete.
- The Metasploitable 2 environment is now ready for use.



Network Configuration:
Network configuration for Metasploitable 2 involves setting up the network connectivity and addressing within the virtual machine. The steps are as follows:

Step 1: Network Adapter Settings:

- Access the settings of the Metasploitable 2 virtual machine within the virtualization software.
- Configure the network adapter type to either Bridged Networking or NAT, based on requirements.
- Bridged Networking: Allows the virtual machine to be directly connected to the physical network, obtaining an IP address from the DHCP server.
- NAT (Network Address Translation): Enables the virtual machine to share the host machine's IP address and access the network through it.

Step 2: IP Address Assignment:

- Determine the IP addressing scheme to be used for the Metasploitable 2 virtual machine.
- Assign a static IP address to the virtual machine within the chosen network configuration.

Step 3: Network Testing:

- Verify the network configuration by testing connectivity from the host machine and other machines in the network.
- Ensure that the Metasploitable 2 virtual machine can communicate with other machines and access the internet if necessary.

Remediation actions:

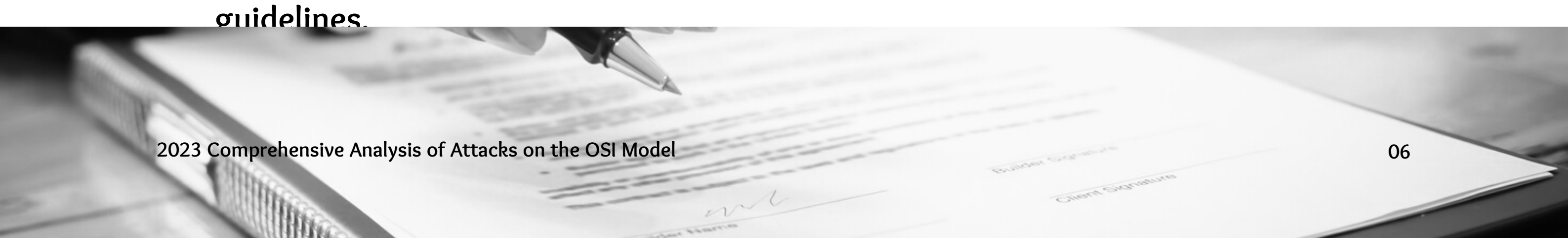
- Weak or default credentials:
- Change all default credentials for services and accounts.
- Implement strong password policies and enforce regular password changes.

Outdated software versions:

- Update the operating system and all installed software to the latest versions.
- Apply security patches and updates promptly.

Insecure configurations:

- Review and modify configurations to follow best practices and security guidelines.



Unnecessary or insecure services:

- Identify and disable or remove any unnecessary services running on the system.
- Disable unnecessary ports and protocols.

conclusion and recommendations for improving the security posture of metasplotable 2.

Regularly update and patch:

- Keep the operating system and all software up to date with the latest security patches and updates.
- Apply updates promptly to address known vulnerabilities.

Strong authentication and access controls:

- Change default credentials for all services and accounts.
- Implement strong password policies and enforce regular password changes.

Vulnerability management:

- Regularly conduct vulnerability assessments and penetration tests to identify and address weaknesses.
- Use security tools to scan and identify vulnerabilities.

Security awareness and training:

- Conduct security awareness training for users to educate them about security practices and potential risks.
- Teach users how to identify and report suspicious activities or potential vulnerabilities.

Network Scanning using Nmap

Using Nmap, network scanning is the process of looking at a network to find open ports, active services, and potential security holes. The following details the steps needed in using Nmap to scan a network:

Use Nmap to do a network scan:

Nmap (Network Mapper) is a strong and flexible network scanning tool. Normally, you would enter the target IP address or IP range that you wish to scan before starting the network scan. To gather replies from the hosts on the target network, Nmap sends several sorts of probes or packets. Nmap can learn which ports are open and what services are using them by examining the answers.

Find open ports and active services:

After starting a network scan, Nmap sends packets to various ports on the target IP address or IP range. Nmap's analysis of the replies it receives allows it to determine which ports are open. A service that is accessible and listening on a port is said to have an open port. Nmap also identifies the services that are active on those ports by analysing the hosts' answers. An HTTP service may be active, for instance, if port 80 is open.

Identify possible Metasploitable 2 vulnerabilities:

A virtual machine (VM) called Metasploitable 2 is used for testing and training using security tools and procedures. Using Nmap, you may locate the open ports and operating services on Metasploitable 2, and then you can compare this data to known vulnerabilities related to those services. Nmap offers a vulnerability database that may be compared to the found services. You may do this to find possible flaws that could be used in future penetration tests or security analyses.

When the network scan is launched:

Nmap sends packets to various ports on the target IP address or IP range to identify open ports and active services. Nmap can determine which ports are open by examining the answers it receives. An open port means a service is available and listening on that port. By analysing the hosts' answers, Nmap can also ascertain the services that are active on those ports. A operating HTTP service, for instance, can be indicated by port 80 being open.

In conclusion, network scanning with Nmap entails starting a scan to find open ports and active services, using the information gleaned to spot potential security holes on a particular target (like Metasploitable 2), and utilising Nmap scripts to gather more data and carry out particular tasks associated with the services and vulnerabilities discovered.

Vulnerability Assessment using Nessus:

The process of performing a vulnerability assessment with Nessus entails employing the vulnerability scanner to find security flaws in a target system. The following are the key considerations while doing a vulnerability assessment with Nessus:

Install and configure Nessus: The host machine's Nessus has to be installed and set up first. A popular vulnerability scanner that can be installed on several operating systems is Nessus. The essential login information and scanning parameters will be configured throughout the installation and configuration procedure.

Decide on the intended system: You must choose the target system for your vulnerability assessment in this stage. In this instance, "Metasploitable 2," a purposefully vulnerable virtual computer frequently used for security testing, is mentioned in the sample.

Configure the scan: After choosing the target system, you must set up the Nessus scan. The target system's IP address or hostname must be specified, the type of scan (such as a quick network scan or a more thorough web application scan), and any special parameters or preferences must be defined.

Run the vulnerability scan: After configuring the scan, Nessus may be used to launch the vulnerability scan. The scan will thoroughly examine the target system to look for known security flaws, configuration errors, weak passwords, and other problems. To find possible holes, Nessus uses a variety of techniques include port scanning, service discovery, and vulnerability testing.

Examine the scan findings: Nessus delivers a thorough report with the scan results when the vulnerability scan is finished. The found vulnerabilities, their severity (such as low, medium, high, or critical), and any potential effects on the target system's security are all covered in this report.

Prioritise and fix vulnerabilities: Using the data in the Nessus scan report, you must examine the discovered vulnerabilities and rank them according to their seriousness and probable consequences. High severity and critical vulnerabilities should be fixed right away, but lesser severity problems may be handled more methodically.

Mitigate vulnerabilities: You may begin the process of resolving the detected security concerns after prioritizing the vulnerabilities. To fix the vulnerabilities found, this may entail installing patches, upgrading software, altering settings, changing passwords, or putting extra security measures in place.

Conduct frequent vulnerability assessments: As new vulnerabilities are consistently found, vulnerability assessment is a continuous activity. To protect the security of your systems and keep current with the most recent threats and vulnerabilities, it is advised to frequently carry out vulnerability assessments using Nessus or other tools.

Using Nessus to analyze vulnerabilities aids organizations in finding and fixing security flaws in their systems, lowering the risk of prospective attacks and enhancing overall security posture.

Nmap scan results, highlighting open ports, services, and potential vulnerabilities.

An Nmap scan results in a thorough report that gives you important details about the target system or network. The report is divided into many sections, and the following are the critical details to consider while examining the Nmap scan findings, paying particular attention to open ports, services, and potential vulnerabilities:

Port 21

ftp-vsftpd-backdoor: (vsFTPd version 2.3.4 backdoor) IDs:CVE:CVE-2011-2523

A security flaw known as CVE-2011-2523 enables an attacker to obtain unauthorized access to a machine running the vulnerable version of vsFTPd. Unknown party purposely placed the backdoor code into the vsFTPd source code, potentially jeopardizing the security of computers running the vulnerable version.

Port 22

CVE-2010-4478

OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-2010-4252.

Port 80
SQL vulnerable, csrf vulnerable on admin page
CSRF: CSRF is an attack where an attacker tricks a user into performing unintended actions on a web application by exploiting their authenticated session.
SQL Injection: SQL injection is a vulnerability that allows attackers to manipulate a web application's database by injecting malicious SQL code through user input.

Port 445

SMB Message Signing vulnerable.
SMB (Server Message Block) message signing vulnerability refers to a security weakness in the SMB protocol, which is used for file and printer sharing in Windows networks. The vulnerability allows an attacker to bypass the message signing mechanism, which is intended to ensure the integrity and authenticity of SMB communications.

Port 1099

Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.

The default configuration of RMI (Remote Method Invocation) registry allows loading classes from remote URLs, which can potentially result in remote code execution. This means that if the RMI registry is not properly secured, an attacker can exploit this vulnerability to execute arbitrary code on the remote system. It is crucial to properly configure and secure the RMI registry to prevent unauthorized access and potential remote code execution.

Port 2121

Pro ftp vulnerable

If enabled in ProFTPD, the mod_copy extension enables unauthenticated attackers to read and write arbitrary files using the

SITE CPFR
SITE CPTO

instructions. If the machine additionally runs a web server that supports PHP, this might result in the execution of arbitrary commands.

PostgreSQL, 9.2.x before 9.2.4, 9.1.x before 9.1.9, 9.0.x before 9.0.13, 8.4.x before 8.4.17, and 8.3.x before 8.3.23 generates insecure temporary files with predictable filenames, which has unspecified impact and attack vectors related to "graphical installers for Linux and Mac OS X."

Nessus vulnerability assessment findings, including identified vulnerabilities and severity levels.

Nessus is a well-known vulnerability assessment tool that searches networks and computer systems to find security flaws. The programme delivers thorough results, including information on vulnerabilities that have been found and how serious they are. The following are the key conclusions from Nessus vulnerability assessments:

Host Information: The findings often begin with the target system's IP address, hostname, operating system, and other pertinent information.

Vulnerability summary: of the vulnerabilities discovered during the evaluation is given in this section. It could consist of a breakdown of the types and total numbers of vulnerabilities that have been found.

Severity Levels: Nessus classifies vulnerabilities into several severity categories according to the danger they provide. Depending on the vulnerability categorization system being used, there might be several severity levels, but the most frequent ones are Critical, High, Medium, Low, and Informational. Each vulnerability is given a severity rating to show how much it might compromise the security of the system.

Vulnerability Details: Specific information about each detected vulnerability is provided in this section. Name, description, and links to more resources are all included for the vulnerability. The impacted software or systems, the possible effects of the vulnerability, and the procedures to mitigate or fix the problem may also be included in the information.

Exploitability: Nessus may try to ascertain whether the vulnerabilities discovered are exploitable, which means they might be exploited to compromise the system or obtain unauthorised access. Prioritising remedial actions is made easier by the information.

Recommended Actions: Nessus frequently offers suggestions or corrective measures to resolve the discovered vulnerabilities. These suggestions frequently involve fixes, configuration adjustments, or other steps to lessen the risks brought on by the vulnerabilities.

Compliance Checks: Nessus can run compliance tests in accordance with a variety of security best practises and standards, including CIS benchmarks, HIPAA, PCI DSS, and others. The findings can reveal non-compliant setups or behaviours that need to be changed to satisfy the necessary compliance requirements.

False Positives: Nessus occasionally detects vulnerabilities that do not pose a threat to system security. We refer to these as false positives. Users may be able to distinguish between true vulnerabilities and false positives using the results' information regarding possible false positives.

Historical Data: Nessus offers historical data that customers may utilize to follow changes in vulnerability over time. Monitoring security posture and gauging the success of remedial activities may both be done with the use of this data.

Nessus assists users in understanding security vulnerabilities in their systems, prioritizing remedial efforts, and enhancing overall security posture by providing these results in the vulnerability assessment reports.

Conclusion and suggestions for enhancing Metasploitable 2's security stance.

The virtual computer known as Metasploitable 2 was created with the intention of being intentionally susceptible. Even if its flaws are on purpose, it's crucial to take the right steps to adequately protect it and reduce any hazards. Here are some findings and suggestions for strengthening Metasploitable 2's security posture:

Regular Updates and Patching: Maintain Metasploitable 2's compatibility by applying the most recent security updates and patches. This lessens the possibility of exploitation while addressing any known vulnerabilities.

Network segmentation: Use a firewall or a virtual network to isolate Metasploitable 2 from the rest of your network. If an attacker manages to hack Metasploitable 2, this makes it difficult for them to access other computers.

Disable Unneeded Services: Look through the services Metasploitable 2 is currently using and turn off any that are unnecessary. As a result, the attack surface is reduced and the likelihood of exploitation is decreased.

Strong Authentication: Ensure that each Metasploitable 2 user account has a strong, one-of-a-kind password. Combining capital and lowercase letters, numerals, and special characters is acceptable. Do not use weak or default credentials.

Network Monitoring: Detect any abnormal activity or prospective attacks against Metasploitable 2 by using network monitoring tools. Monitoring makes it possible to quickly identify security events and respond to them.

Intrusion Detection and Prevention Systems (IDPS): Deploy an IDPS to monitor network traffic and identify any malicious activity or attempted attacks. Intrusion Detection and Prevention Systems (IDPS). This assists in thwarting successful assaults and gives warnings for any security lapses.

Scan: Conduct regular vulnerability checks on Metasploitable 2 to find any vulnerabilities or incorrect setups. To improve security, address the discovered vulnerabilities right away.

Security Awareness and Training: Inform users and administrators using Metasploitable 2 about security best practises, such as avoiding dubious links or email attachments, utilising secure surfing techniques, and being aware of the dangers of using insecure systems.

Backup and recovery: For Metasploitable 2, implement a regular backup method. The ability to swiftly restore the system to a known safe state is ensured by keeping current backups in the event of a successful attack or system compromise.

By putting these procedures in place, you may considerably strengthen Metasploitable 2's security posture and lower the danger of exploitation. A controlled and secure environment is essential while using Metasploitable 2 to avoid any unwanted repercussions, like as mistakenly exposing susceptible systems to the internet.

Overview

This report presents an overview of the objectives and methodology for a minor project centered on the setup and security analysis of Metasploitable 2. The project's primary focus involves the installation of Metasploitable 2, network scanning using Nmap, vulnerability assessments utilizing Nessus, and the subsequent generation of a comprehensive report encompassing identified vulnerabilities and recommended remediation actions.

1. Objectives:

The core objectives of the project are as follows:

Installation of Metasploitable 2:

To set up and configure Metasploitable 2 on a designated virtualization platform, ensuring a stable and functional environment for subsequent security assessments.

Network Scanning using Nmap:

Conduct a thorough network scan using Nmap, targeting Metasploitable 2, to identify open ports, services, and potential vulnerabilities that may exist within the system.

Vulnerability Assessments using Nessus:

Utilize Nessus, a renowned vulnerability scanner, to perform comprehensive assessments of Metasploitable 2. This process will help identify and evaluate potential security weaknesses, misconfigurations, and outdated software within the environment.

Generation of a Comprehensive Report:

Develop a comprehensive report encompassing identified vulnerabilities, their descriptions, severity levels, and potential impacts on the system's security. Additionally, provide recommended remediation actions to mitigate the identified vulnerabilities effectively.