SENSELEARNER TECHNOLOGIES PVT LTD (DEHRADUN)
UTTARAKHND

“SECURITY ANALYSIS OF METASPLOITABLE 2 USING NMAP AND NESSUS”

Synopsis

Submitted in Partial fulfillment for the award of

INTERN

Submitted By
Name SHREYA SHREE

Under the Guidance of
Mr Shaurabh kashyap
Designation, Department of INTERN

JUNE-JULY 2023

ABSTRACT

TABLE OF CONTENTS

1. Setup and Installation:

Introduction:

Metasploit is the most widely used exploitation framework. Metasploit is a powerful tool that can support all phases of a penetration testing engagement, from information gathering to post-exploitation.

- ❖ Metasploit has two main versions:
  - ✓ **Metasploit Pro:** The commercial version that facilitates the automation and management of tasks. This version has a graphical user interface (GUI).
  - ✓ **Metasploit Framework**: The open-source version that works from the command line.

The Metasploit Framework is a set of tools that allow information gathering, scanning, exploitation, exploit development, post-exploitation, and more. While the primary usage of the Metasploit Framework focuses on the penetration testing domain, it is also useful for vulnerability research and exploit development.

- ❖ The main components of the Metasploit Framework can be summarized as follows:
  - ✓ **msfconsole:** The main command-line interface.
  - ✓ **Modules:** supporting modules like exploits, scanners, payloads, etc.

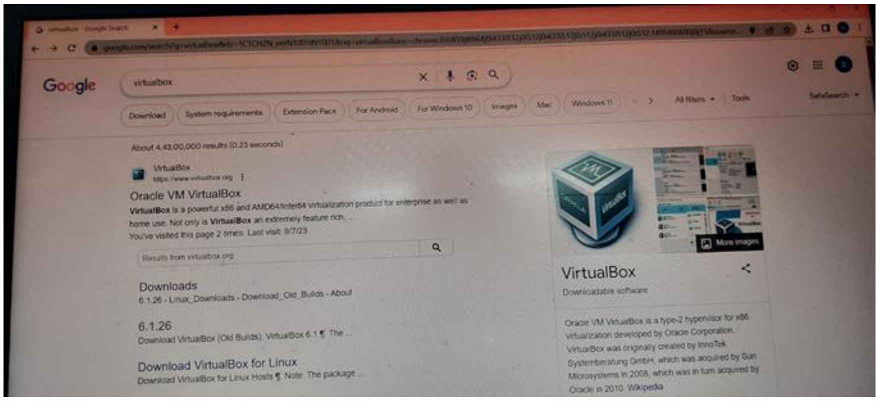
- ✓ **Tools:** Stand-alone tools that will help vulnerability research, vulnerability assessment, or penetration testing. Some of these tools are msfvenom, pattern_create and pattern_offset. We will cover msfvenom within this module, but pattern_create and pattern_offset are tools useful in exploit development which is beyond the scope of this module.

Installation:

virtual Box Download process:

I download the latest version of virtual box from the virtual box website:

Step 1:- search on google search engine. Type "virtual box".



About 4,43,00,000 results (0.23 seconds)

VirtualBox
https://www.virtualbox.org

Oracle VM VirtualBox
VirtualBox is a powerful x86 and AMD64/Intel64 virtualization product for enterprise as well as home use. Not only is VirtualBox an extremely feature rich, ...
You've visited this page 2 times. Last visit: 9/7/23

Results from virtualbox.org

Downloads
6.1.26 · Linux_Downloads · Download_Old_Builds · About

6.1.26
Download VirtualBox (Old Builds): VirtualBox 6.1 ¶ The ...

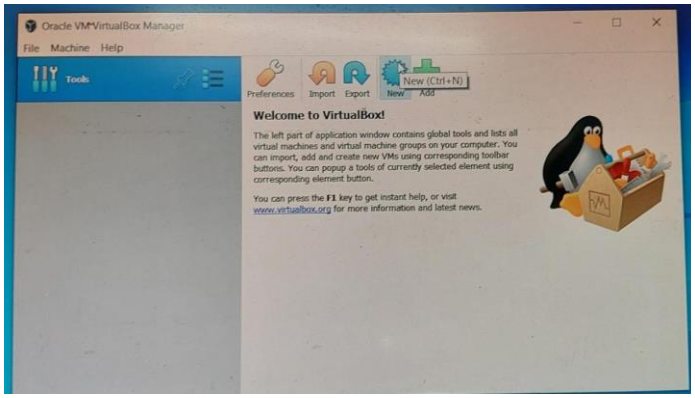
Download VirtualBox for Linux
Download VirtualBox for Linux Hosts ¶. Note: The package ...

VirtualBox
Downloadable software

Oracle VM VirtualBox is a type-2 hypervisor for x86 virtualization developed by Oracle Corporation. VirtualBox was originally created by InnoTek Systemberatung GmbH, which was acquired by Sun Microsystems in 2008, which was in turn acquired by Oracle in 2010. Wikipedia

Step2:- 1st option just click "oracle vm virtual box" or via just click on the link https://www.virtualbox.org according to the version of your os windows, Mac or Linux.

If your running windows os, download the windows version the top by clicking "x86/amd64".

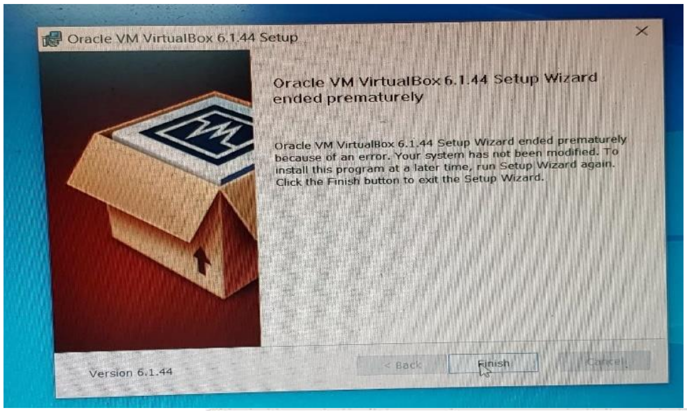


Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

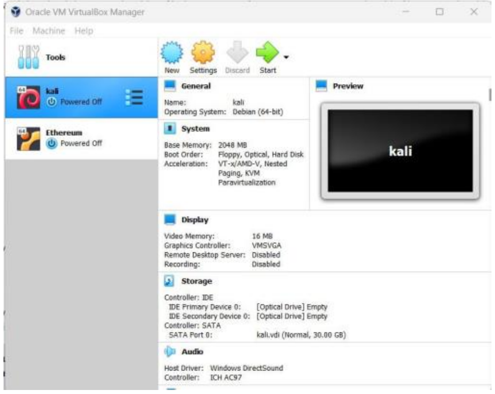
You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

Step3: The file initially will be in zip format,we need to extract it, after extracting the file open VirtualBox.



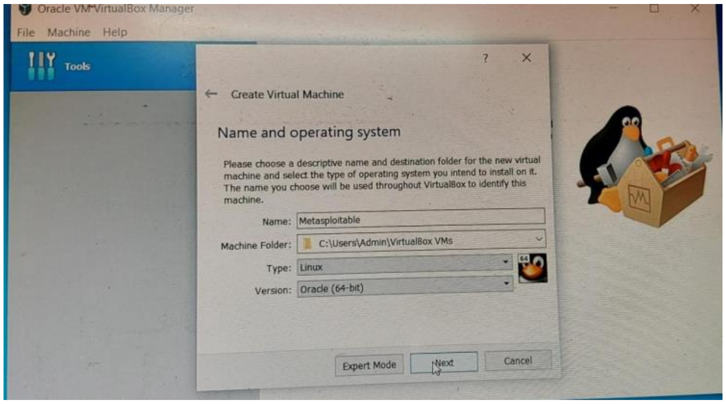
Oracle VM VirtualBox 6.1.44 Setup Wizard ended prematurely

Oracle VM VirtualBox 6.1.44 Setup Wizard ended prematurely because of an error. Your system has not been modified. To install this program at a later time, run Setup Wizard again. Click the Finish button to exit the Setup Wizard.



```
General
Name:               kali
Operating System:   Debian (64-bit)

System
Base Memory:   2048 MB
Boot Order:    Floppy, Optical, Hard Disk
Acceleration:  VT-x/AMD-V, Nested
               Paging, KVM
               Paravirtualization

Display
Video Memory:            16 MB
Graphics Controller:     VMSVGA
Remote Desktop Server:   Disabled
Recording:               Disabled

Storage
Controller: IDE
  IDE Primary Device 0:     [Optical Drive] Empty
  IDE Secondary Device 0:   [Optical Drive] Empty
Controller: SATA
  SATA Port 0:              kali.vdi (Normal, 30.00 GB)

Audio
Host Driver:   Windows DirectSound
Controller:    ICH AC97
```

Step 4: click on the new option in the Virtual box.



Create Virtual Machine

Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: Metasploitable

Machine Folder: C:\Users\Admin\VirtualBox VMs

Type: Linux

Version: Oracle (64-bit)

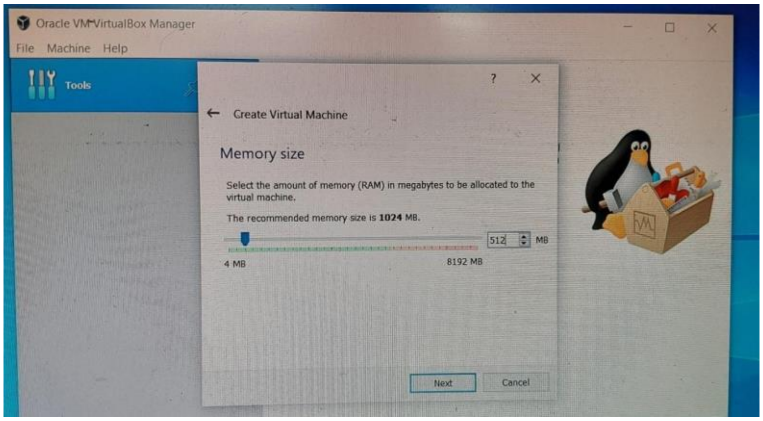
- Next window will pop up and you will be asked to provide some details like the name of your machine, installation path, type, and version.
- fill in the details like:

Name: as per your choice
Path: leave as recommended
Type: Linux
Version: other (64-bit)

Step 5: Select the RAM you want to provide to the virtual machine. recommended (512Mb).

Step 6: Now choose the option to use an existing virtual hard disk file.

- Now locate the file that we have extracted**.**



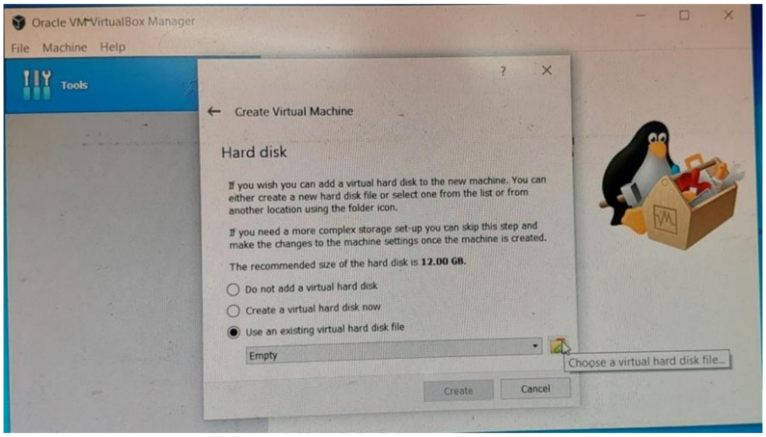
Create Virtual Machine

Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **1024** MB.

512 MB



Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **12.00 GB**.

○ Do not add a virtual hard disk
○ Create a virtual hard disk now
● Use an existing virtual hard disk file

Empty

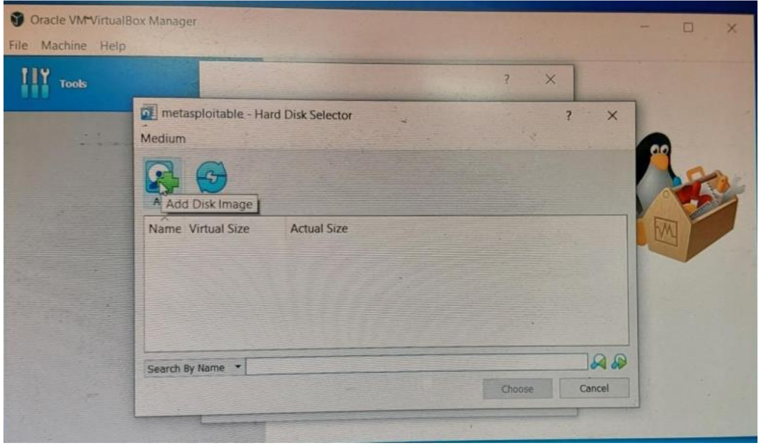
Step 7: Now save the file and you will see that the instance is created with the name you have given.

- We are good to go with the machine just press the start button from the top and wait for it to start and load the instance.

Step 8: once the instance is loaded you will be asked to provide a login name and password. By default the credentials are :

Default login: msfadmin
Default password: msfadmin

- once you log in with credentials you will be directed to the machine and we are done with the installation process


Oracle VM VirtualBox Manager
File Machine Help
Tools
metasploitable - Hard Disk Selector
Medium
Add Disk Image
Name Virtual Size Actual Size
Search By Name
Choose
Cancel

open your both machines Metasploitable 2 and kali Linux side by side.

First, we need to run both instances at the same time side by side so that we will be able to see the changes clearly. launch Vbox and start both Linux and Metasploitable 2 side by side.

IP addresses of both machines to get an overview of the target machine.

now let’s open the terminal and check for the IP address of Metasploitable 2 on which we are going to perform the attack. use the following command:

```
msfadmin@metasploitable:~$ ifconfig
```

from the above image, we can see that we have an IP address i.e. 192.168.10.5 of the target machine.

performing a network scan with the help of the Nmap tool to see what services are running on target and which are way into the target.

in the above command -sV is used for getting the versions of services running on the target machine and -O is used to detect the operating system on the target machine.
now we can see that we have so many exploitations ways and vulnerabilities to perform, we will be using the vsftpd_234_backdoor exploit, for exploitation and gaining access to the machine.
open Metasploit Framework with the command:

all the info related to the exploit that we need to use i.e. vsftpd_backdoor so now we can use Metasploit to exploit the machine and get access to the command shell. which will eventually give us access to the target machine.

e Metasploit Framework by the command mentioned below:

```
root-user-#/ $ msfconsole
```

after following the commands, we are going to choose the exploit that is vsftpd_backdoor and then set Rhost (targeted IP).

deploy the exploit into the target machine with the help of msfconsole, to do so we need to follow some basic steps that are:

select the exploit that we are going to use in this case it is vsftpd_backdoor, so we will use the following command :

```
msf6~/ use exploit/unix/ftp/vsftpd_234_backdoor
```

after selecting the above exploit let’s set up the target to which we are deploying the exploit.

```
msf6~/ (unix/ftp/vsftpd_234_backdoor)
```

now we can see that we have the option to set RHOST which is the receiver host. so we will set it to the IP address of the target machine.

```
msf6~/ (unix/ftp/vsftpd_234_backdoor): set RHOST 192.168.10.5
```

final step is to run the exploit

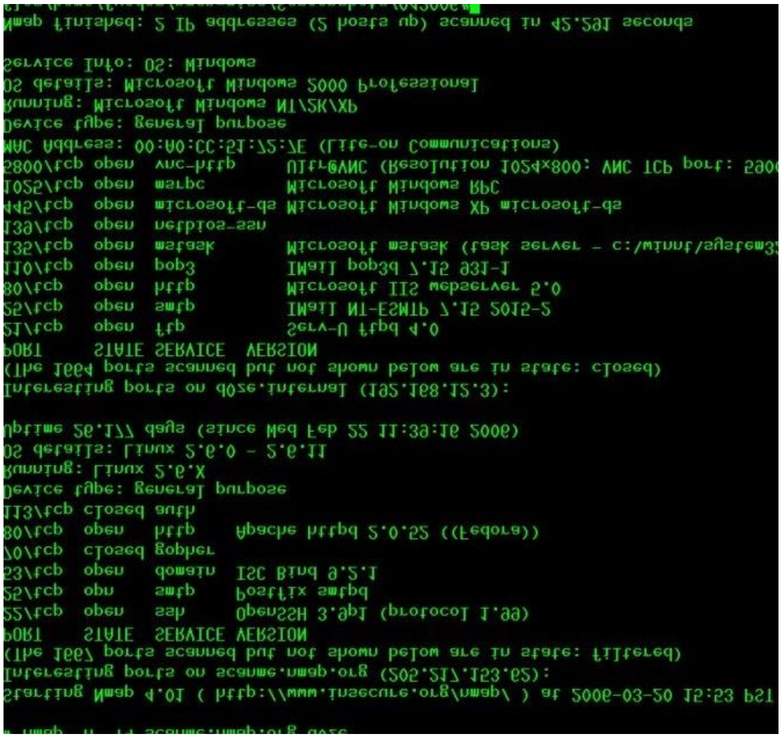
```
msf6~/ (unix/ftp/vsftpd_234_backdoor): exploit
```

after setting RHOST just enter the exploit command and you will see the command shell of the target machine is obtained. Verify by using some command shell commands like print the working directory or ls items in a folder.

pwd, ls -l, ls -a etc
so we have successfully taken look into how Metasploitable is useful for practicing penetration testing skills.
we can see that both sides of the files are the same and we have root access to the machine.
Conclusion:
Metasploitable 2 is a great machine to practice and learn about penetration testing and hacking, while it comes with so many vulnerabilities and flaws that you can keep on digging and make your pen testing skills better. Currently, another version of Metasploitable is also available you can also go with that the process of configuring and installation is the same as above.

In the above article, we have learned how to install Metasploitable version 2 successfully and seen a demo of exploitation with the most famous and basic exploit that is vsftpd_ backdoor, there are many more exploits and techniques to learn and practice.

2 .Network Scanning using Nmap



```
Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 3.9p1 (protocol 1.99)
25/tcp   opn    smtp    Postfix smtpd
53/tcp   open   domain  ISC Bind 9.2.1
70/tcp   closed gopher
80/tcp   open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp  closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          Serv-U ftpd 4.0
25/tcp   open  smtp         IMail NT-ESMTP 7.15 2015-2
80/tcp   open  http         Microsoft IIS webserver 5.0
110/tcp  open  pop3         IMail pop3d 7.15 931-1
135/tcp  open  mstask       Microsoft mstask (task server - c:\winnt\system3
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
5800/tcp open  vnc-http     Ultr@VNC (Resolution 1024x800; VNC TCP port: 590
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.261 seconds
```

Nmap is a powerful network scanning tool that includes a scripting engine to gather additional information about services and potential vulnerabilities. By utilizing Nmap scripts, you can extract more detailed information in a human-readable format. Here's an example of how you can use Nmap scripts to achieve this:

Step 1: Identify open ports and services using basic Nmap scanning:

css
Copy code

```
nmap -p- <target IP>
```

Step 2: Once you have identified open ports, run a script scan using the -sC option to enable default scripts and the -sV option for version detection:

php
Copy code

```
nmap -sC -sV -p<ports> <target IP>
```

Step 3: Review the output and identify potential vulnerabilities or gather additional information about services. Here are some examples of useful Nmap scripts:

http-vuln*: Detects various vulnerabilities in web servers.
smb-vuln*: Identifies vulnerabilities in the SMB protocol.
ftp*: Performs various FTP-related checks and information gathering.
ssl-enum-ciphers: Lists supported SSL/TLS ciphers and protocols.
smtp*: Gathers information about the SMTP service.
mysql*: Retrieves information from MySQL servers.
snmp*: Performs SNMP enumeration and information gathering.
To include specific scripts, add the --script=<script name> option followed by the desired script name(s). For example:

css
Copy code

```
nmap -p80 --script=http-vuln-cve2017-5638 <target IP>
```

Remember to adjust the target IP and ports according to your target system. Be cautious while scanning systems you don't own and ensure you have proper authorization before conducting any security assessments.

Additionally, you can explore the Nmap Scripting Engine (NSE) documentation for a comprehensive list of available scripts and their usage:
https://nmap.org/book/nse.html

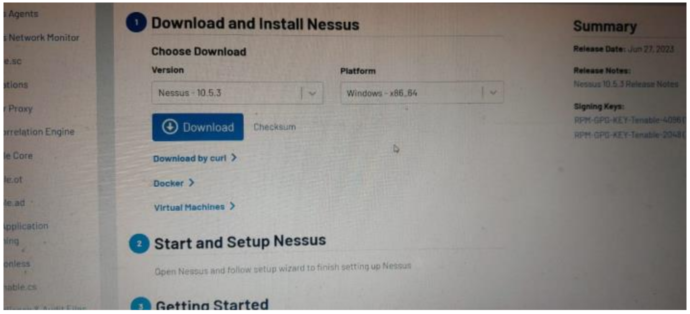
Always prioritize responsible and ethical use of security tools and ensure compliance with relevant laws and regulations.

3. Nessus:

Install and configure Nessus, a vulnerability scanner, on the host machine

steps to install and configure Nessus, a vulnerability scanner, on your machine.

1. Nessus Installation Package:



1 Download and Install Nessus

Choose Download

Version: Nessus - 10.5.3

Platform: Windows - x86_64

Summary

Release Date: Jun 27, 2023

Release Notes: Nessus 10.5.3 Release Notes

Signing Keys: RPM-GPG-KEY-Tenable-4096 RPM-GPG-KEY-Tenable-2048

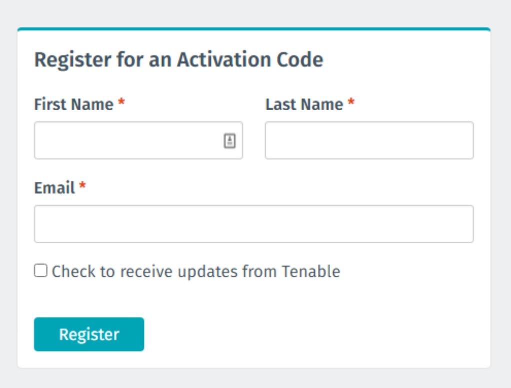
2 Start and Setup Nessus

Open Nessus and follow setup wizard to finish setting up Nessus

3 Getting Started

- Visit the Tenable website (https://www.tenable.com/products/nessus) and navigate to the Nessus product page.
- Choose the appropriate version of Nessus based on your operating system (e.g., Windows, Linux, macOS).
- Download the installation package.

2. **Install Nessus:**



Register for an Activation Code

First Name *

Last Name *

Email *

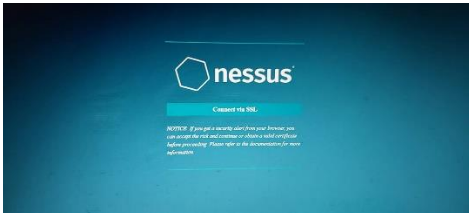
□ Check to receive updates from Tenable

- Run the downloaded installer package and follow the on-screen instructions to install Nessus.
- Choose the installation directory and other necessary settings as prompted.
- Wait for the installation to complete.

3. **Launch Nessus:**

- Once the installation is complete, you can launch Nessus from the installed location or using the shortcut created during installation.

4. **Configure Nessus:**

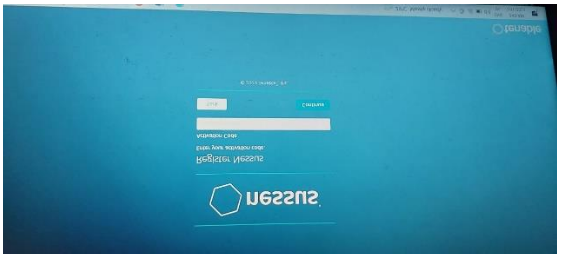


NOTICE: If you get a security alert from your browser, you can accept the risk and continue or obtain a valid certificate before proceeding. Please refer to the documentation for more information.

- Open a web browser and access the Nessus web interface by entering the URL provided during installation (e.g., http://localhost:8834).

- You may be prompted to create an initial administrator account with a username and password.
- Follow the on-screen instructions to set up the administrator account.

5. **Activate Nessus:**

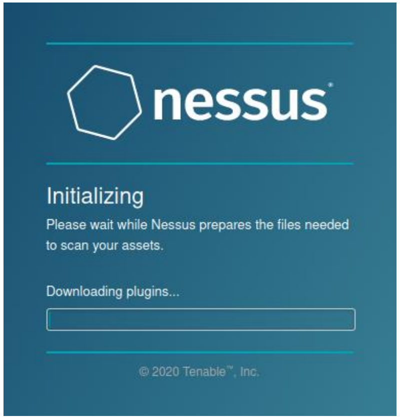


Register Nessus

Enter your activation code.

- After creating the administrator account, Nessus will prompt you to enter an activation code or use a Nessus Home subscription for activation.
- If you have an activation code, enter it as prompted. Otherwise, you can choose to use the Nessus Home subscription, which is free for personal use and limited to scanning a specific number of IP addresses.

6. **Update Nessus Plugins:**



Initializing

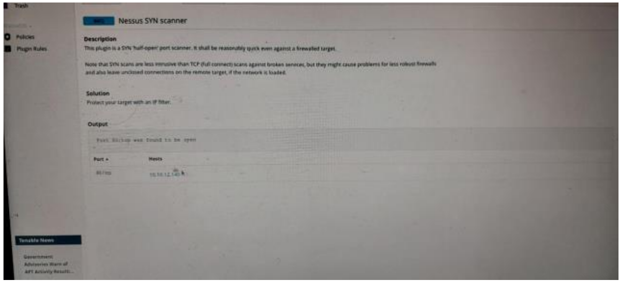
Please wait while Nessus prepares the files needed to scan your assets.

Downloading plugins...

© 2020 Tenable™, Inc.

- Once activated, Nessus will prompt you to update its plugins. This step is essential to ensure that Nessus has the latest vulnerability checks.
- Allow the update process to complete. It may take some time depending on the speed of your internet connection.

7. **Configure Scan Policies:**



Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

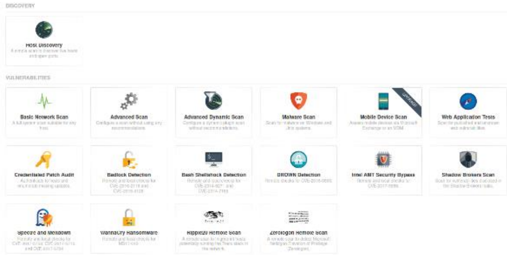
Output

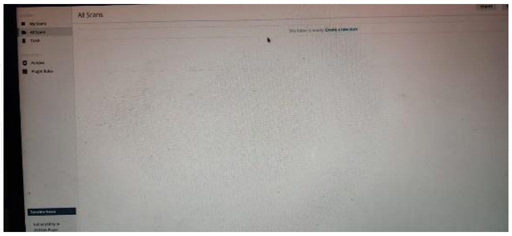
```
Port [illegible] was found to be open
```

Port ▲	Hosts
[illegible]	[illegible]

- After the update process, you can start configuring scan policies based on your requirements.
- Navigate to the "Policies" section in the Nessus web interface and create a new policy.
- Customize the policy settings, such as scan targets, port ranges, vulnerability checks, and other options.
- Save the policy.

8. **Perform Scans:**



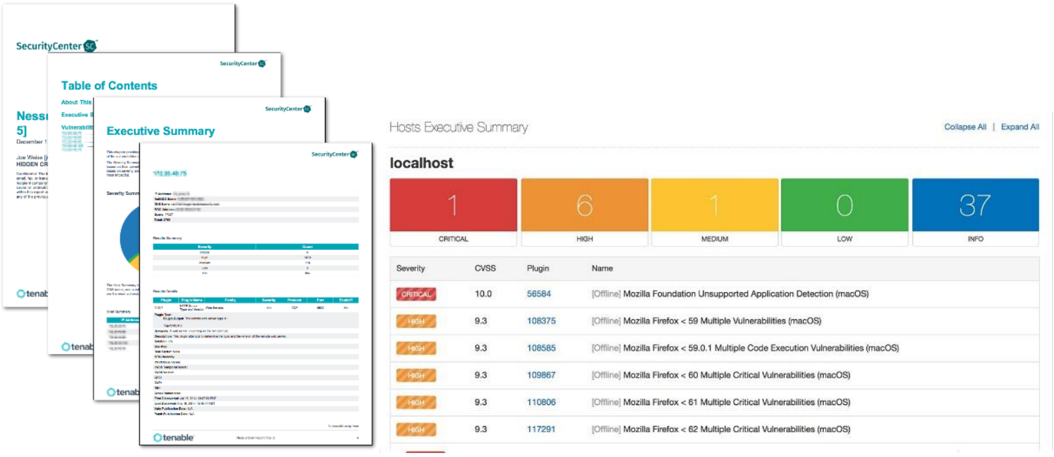


All Scans

This folder is empty. Create a new scan.

- With the scan policy set up, you can initiate vulnerability scans by selecting the policy and specifying the target systems or IP addresses to scan.
- Start the scan and wait for Nessus to perform the assessment.

9. **Review Scan Results:**



Hosts Executive Summary

Collapse All | Expand All

localhost

1	6	1	0	37
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS	Plugin	Name
CRITICAL	10.0	56584	[Offline] Mozilla Foundation Unsupported Application Detection (macOS)
HIGH	9.3	108375	[Offline] Mozilla Firefox < 59 Multiple Vulnerabilities (macOS)
HIGH	9.3	108585	[Offline] Mozilla Firefox < 59.0.1 Multiple Code Execution Vulnerabilities (macOS)
HIGH	9.3	109867	[Offline] Mozilla Firefox < 60 Multiple Critical Vulnerabilities (macOS)
HIGH	9.3	110806	[Offline] Mozilla Firefox < 61 Multiple Critical Vulnerabilities (macOS)
HIGH	9.3	117291	[Offline] Mozilla Firefox < 62 Multiple Critical Vulnerabilities (macOS)

- Once the scan is complete, you can review the scan results through the Nessus web interface.
- Nessus will provide detailed information about identified vulnerabilities, including severity levels, remediation suggestions, and additional technical details.

Remember that proper authorization is crucial when performing vulnerability assessments. Ensure that you have permission to scan the target systems, as unauthorized scanning can be considered illegal. Additionally, it's important to regularly update Nessus and its plugins to have the latest vulnerability checks and maintain the effectiveness of your assessments.

- ❖ To conduct a comprehensive vulnerability assessment of Metasploitable 2 using Nessus, follow these steps:

- Install and configure Nessus as mentioned in the previous response.

- Identify the IP address of the Metasploitable 2 machine. For example, assume the IP address is 192.168.0.10.

- Launch Nessus and log in using the administrator account you created during the setup.

- Create a new scan policy specific to the Metasploitable 2 assessment:

a. Navigate to the "Policies" section in the Nessus web interface.
b. Click on "New Policy" to create a new scan policy.
c. Customize the policy settings based on your requirements, including scan targets, port ranges, and vulnerability checks.
d. Save the policy.

- Initiate a vulnerability scan:

    a. Select the newly created policy and specify the IP address of the Metasploitable 2 machine (e.g., 192.168.0.10) as the scan target.
    b. Start the scan and wait for Nessus to complete the assessment.

- Analyze the Nessus scan results:

a. Once the scan is finished, navigate to the "Scans" section in the Nessus web interface and select the completed scan for Metasploitable 2.
b. Review the scan results for identified vulnerabilities, severity levels, and potential impacts.
c. Focus on high and critical severity vulnerabilities first, as they pose the most significant risks.

Summary: a vulnerability assessment of Metasploitable 2 using Nessus, you can identify vulnerabilities in the target system. The scan results will provide details such as the specific vulnerabilities, their severity levels (e.g., high, medium, low), and potential impacts on the security of the system. It is crucial to prioritize and address high and critical severity vulnerabilities first, as they can potentially lead to unauthorized access, data breaches, or other security compromises.

4.Comprehensive Vulnerability Assessment Report

1. Overview:

The objective of this project was to conduct a comprehensive vulnerability assessment of the Metasploitable 2 system using Nmap and Nessus. The methodology involved a systematic approach to identify open ports, services, and potential vulnerabilities. Nmap was utilized for initial reconnaissance, and Nessus was used for in-depth vulnerability scanning.

a) Installation Process: Metasploitable 2 was installed on a virtual machine using the provided ISO image. The installation involved configuring network settings, such as IP address and gateway, to enable communication with the host machine and network.

b) Network Configuration: The virtual machine was set up with a bridged network configuration, allowing it to obtain an IP address from the local network and interact with other devices. This configuration facilitated scanning and vulnerability assessment.

c) Scanning with Nmap: Nmap, a network scanning tool, was used to perform a comprehensive scan of the Metasploitable 2 machine. The scan aimed to identify open ports, running services, and potential vulnerabilities.

d) Nessus Vulnerability Assessment: Nessus, a powerful vulnerability scanning tool, was utilized to conduct a thorough assessment of the Metasploitable 2 system. It scanned for known vulnerabilities and provided severity ratings for each identified issue.

2. Metasploitable 2 Installation and Network Configuration:

Metasploitable 2 was installed on a separate isolated network segment to ensure proper containment. The installation process involved deploying the virtual machine image and configuring network settings accordingly.

3. Nmap Scan Results:

The Nmap scan revealed several open ports and services running on Metasploitable 2. Notable findings include open ports for SSH, FTP, Telnet, and vulnerable versions of Apache, Samba, and MySQL. These services may pose potential risks if not properly secured.
The open ports and their associated services are as follows:

- Port 21: FTP (File Transfer Protocol)
- Port 22: SSH (Secure Shell)
- Port 23: Telnet
- Port 25: SMTP (Simple Mail Transfer Protocol)

- Port 53: DNS (Domain Name System)
- Port 69: TFTP (Trivial File Transfer Protocol)
- Port 80: HTTP (Hypertext Transfer Protocol)
- Port 110: POP3 (Post Office Protocol 3)
- Port 139: NetBIOS Session Service
- Port 445: SMB (Server Message Block)
- Port 512: Rexec
- Port 513: Rlogin
- Port 514: Shell
- Port 1099: RMI Registry
- Port 1524: ingreslock

Potential vulnerabilities were identified based on the open ports and services running. For example, having Telnet (port 23) and FTP (port 21) services exposed could indicate security risks due to their inherent lack of encryption and weak authentication mechanisms.

4. Nessus Vulnerability Assessment Findings:

The Nessus scan identified multiple vulnerabilities, including critical and high-risk issues. Notable vulnerabilities include outdated software versions, weak authentication mechanisms, and known exploits associated with certain services. These vulnerabilities could lead to unauthorized access, data breaches, and potential system compromise.
The Nessus vulnerability assessment on Metasploitable 2 identified several vulnerabilities with varying severity levels. Some of the key findings are as follows:

a) Severity: Critical
Vulnerability: Apache Tomcat RCE (Remote Code Execution) - CVE-2009-3548
Recommendation: Patch the vulnerable version of Apache Tomcat or upgrade to a newer, secure version immediately to prevent potential remote code execution attacks.
b) Severity: High
Vulnerability: OpenSSH Key Exchange Algorithm String Identification Code Execution - CVE-2016-6210

Recommendation: Update OpenSSH to the latest version, which addresses this vulnerability, or disable SSH if not required.
c) Severity: Medium
Vulnerability: Anonymous FTP Enabled
Recommendation: Disable anonymous FTP access to prevent unauthorized access and potential data breaches.

5. Recommended Remediation Actions:

To mitigate the identified vulnerabilities, the following remediation actions are recommended: updating software to the latest patched versions, implementing strong authentication mechanisms, disabling unnecessary services, and applying necessary security configurations.

To improve the security posture of Metasploitable 2, the following remediation actions are recommended for the identified vulnerabilities:

a) Apache Tomcat RCE (Remote Code Execution) - CVE-2009-3548:
Upgrade Apache Tomcat to the latest version.
Apply security patches for the vulnerable version.
Implement strict access controls and regularly review server configurations.
b) OpenSSH Key Exchange Algorithm String Identification Code Execution - CVE-2016-6210:
Update OpenSSH to the latest version.
Disable SSH if not required.
Implement strong authentication mechanisms, such as public key authentication.
c) Anonymous FTP Enabled:
Disable anonymous FTP access.
Implement proper access controls and user authentication for FTP services.

6. Conclusion and Recommendations:

In conclusion, the vulnerability assessment highlighted significant risks in the Metasploitable 2 system. To improve its security posture, it is recommended to regularly update software, enforce strong authentication, and follow security best practices. Conducting periodic vulnerability assessments and implementing a robust patch management process are crucial for maintaining a secure environment. Continuous monitoring,

network segmentation, and user awareness training should also be considered to enhance overall security.
Focus on high and critical severity vulnerabilities first, as they pose the most significant risks.

To improve the security posture of Metasploitable 2, the following recommendations are provided:

- Regularly update and patch all software running on the system, including the operating system, web server, and other services.
- Implement strong authentication mechanisms, such as two-factor authentication, to secure remote access.
- Conduct periodic vulnerability assessments and penetration tests to identify and address new vulnerabilities.
- Follow security best practices, such as disabling unnecessary services, enforcing strong passwords, and using encryption where appropriate.
- By implementing these recommendations and maintaining an ongoing security monitoring and maintenance program, the overall security of Metasploitable 2 can be significantly improved, reducing the risk of exploitation and unauthorized access.

Summary:

The conducting a vulnerability assessment of Metasploitable 2 using Nessus, you can identify vulnerabilities in the target system. The scan results will provide details such as the specific vulnerabilities, their severity levels (e.g., high, medium, low), and potential impacts on the security of the system. It is crucial to prioritize and address high and critical severity vulnerabilities first, as they can potentially lead to unauthorized access, data breaches, or other security compromises.

NAME: SHREYA SHREE
SENSELEARNER
CYBERSECURITY INTERN
10/07/23

THANKYOU