MIS 311

INFORMATION SECURITY SYSTEMS DESIGN and APPLICATIONS

NESSUS VULNERABILITY SCANNER

Name/ Last Name: EDANUR ŞEN

Student Number: 18030411023

Instructor's Name: SAFA BURAK GÜRLEYEN

Submission Date: June 2021

Nessus is a security vulnerability scanning program with many users around the world. Nessus Professional, Nessus Manager, Nessus Home and Nessus Cloud editions are available. It provides the detection of security vulnerabilities and malware in physical, virtual and cloud environments.

The penetration service, which includes activities such as auditing IT infrastructures in terms of security and identifying security levels and closing the gaps, ensures that institutions are prepared and resistant to cyber attacks. In this way, cybersecurity professionals who perform penetration tests ensure that the vulnerable points of the system are repaired and security tightened when a real attack is encountered, by thinking like a hacker and applying infiltration and hijacking scenarios to the system and trying all the methods that the attackers can try.

Licensed or open-source tools are used in penetration tests, and all vulnerabilities are identified and corrected as much as possible by applying manual tests specific to the institution as well as automated scanning tools.

Nessus, one of the most important tools used in internal network penetration tests, contains plugins consisting of pieces of code simulating various attack techniques used by cybercriminals in its database and by applying them on the devices to be scanned, it reveals the vulnerabilities they have.

Nessus provides comprehensive reporting on the vulnerabilities of the target devices according to criteria such as which operating system is running on the devices, which services are running on which ports, the vulnerabilities of the operating system and services, the vulnerabilities of software components and network protocols, and the compliance requirements. Nessus provides the ability to sort and filter the vulnerabilities it detects in the system according to many different criteria, allowing to better understand the vulnerabilities.

WHY NESSUS?

If you are familiar with other network vulnerability scanners, you might be wondering what advantages Nessus has over them. Key points include:

- Unlike other scanners, Nessus does not make assumptions about your server configuration (such as assuming that port 80 must be the only web server) that can cause other scanners to miss real vulnerabilities.

- Nessus is very extensible, providing a scripting language for you to write tests specific to your system once you become more familiar with the tool. It is also provides a plugin interface, and many free plugins are available from the Nessus plugin site. These plugs are often specific to detecting a common virus or vulnerability.

- Up to date information about new vulnerabilities and attacks. The Nessus team updates the list of what vulnerabilities to check for on a daily basis in order to minimize the window between an exploit appearing in the wild, and you being able to detect it with Nessus.

- Open-source: Nessus is open source, meaning it costs nothing, and you are free to see and modify the source as you wish.

- Patching Assistance: When Nessus detects a vulnerability, it is also most often able to suggest the best way you can mitigate the vulnerability.

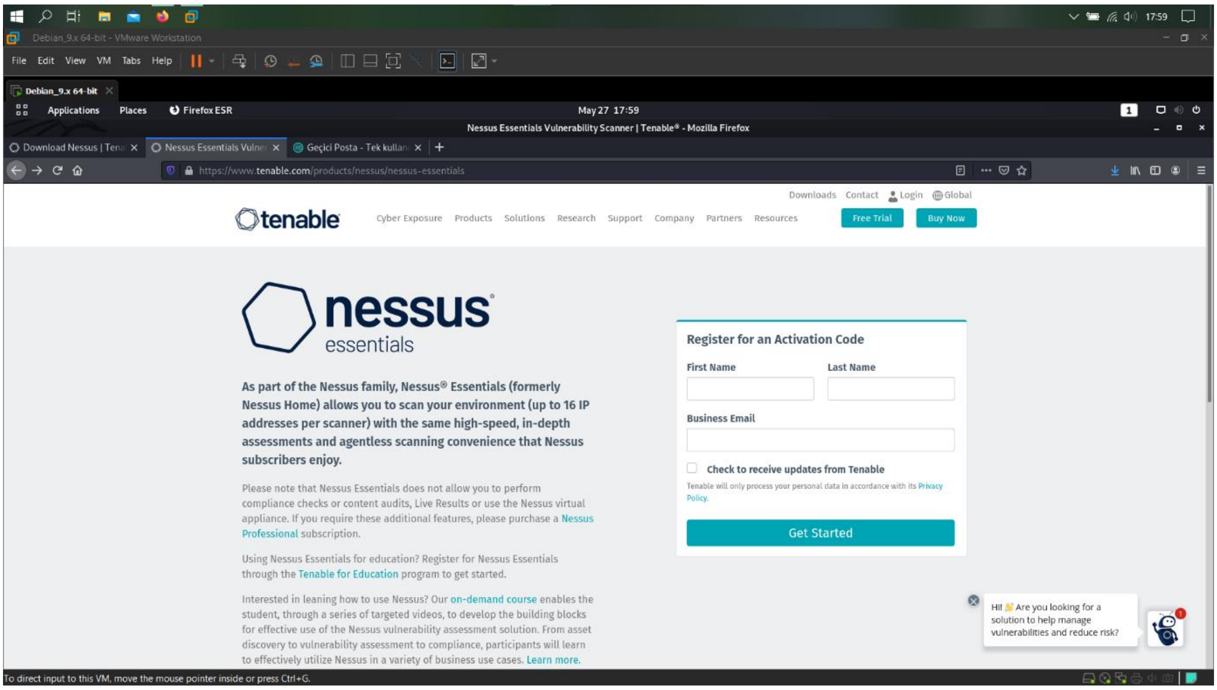
HOW NESSUS WORKS?

To learn how Nessus and other port-scanning security tools work, it is necessary to understand different services (such as a web server, SMTP server, FTP server, etc.) are accessed on a remote server. Most high-level network traffic, such as email, web pages, etc reach a server via a high-level protocol that is transmitted reliably by a TCP stream. To keep different streams from interfering with each other, a computer divides it is physical connection to the network into thousands of logical paths, called ports. So if you want to talk to a web server on a given machine, you would connect to port #80 (the standard HTTP port), but if you wanted to connect to an SMTP server on that same machine you would instead connect to port #25.

Each computer has thousands of ports, all of which may or may not have services (ie: a server for a specific high-level protocol) listening on them. Nessus works by testing each port on a computer, determining what service it is running, and then testing this service to make sure there are no vulnerabilities in it that could be used by a hacker to carry out a malicious attack. Nessus is called a "remote scanner" because it does not need to be installed on a computer for it to test that computer. Instead, you can install it on only one computer and test as many computers as you would like.

INSTALLATION

1- Firstly, register by going to "https://www.tenable.com/products/nessus/nessus-essentials". After the registration is completed, an activation code will be sent to your e-mail address. We will use this code during the installation phase.


Debian_9.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Debian_9.x 64-bit
Applications Places Firefox ESR
May 27 17:59
Nessus Essentials Vulnerability Scanner | Tenable® - Mozilla Firefox
Download Nessus | Tena
Nessus Essentials Vulne
Geçici Posta - Tek kullan
https://www.tenable.com/products/nessus/nessus-essentials
Downloads Contact Login Global
tenable
Cyber Exposure Products Solutions Research Support Company Partners Resources
Free Trial
Buy Now
nessus essentials
Hi! 👋 Are you looking for a solution to help manage vulnerabilities and reduce risk?
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
17:59

As part of the Nessus family, Nessus® Essentials (formerly Nessus Home) allows you to scan your environment (up to 16 IP addresses per scanner) with the same high-speed, in-depth assessments and agentless scanning convenience that Nessus subscribers enjoy.

Please note that Nessus Essentials does not allow you to perform compliance checks or content audits, Live Results or use the Nessus virtual appliance. If you require these additional features, please purchase a Nessus Professional subscription.

Using Nessus Essentials for education? Register for Nessus Essentials through the Tenable for Education program to get started.

Interested in leaning how to use Nessus? Our on-demand course enables the student, through a series of targeted videos, to develop the building blocks for effective use of the Nessus vulnerability assessment solution. From asset discovery to vulnerability assessment to compliance, participants will learn to effectively utilize Nessus in a variety of business use cases. Learn more.

Register for an Activation Code

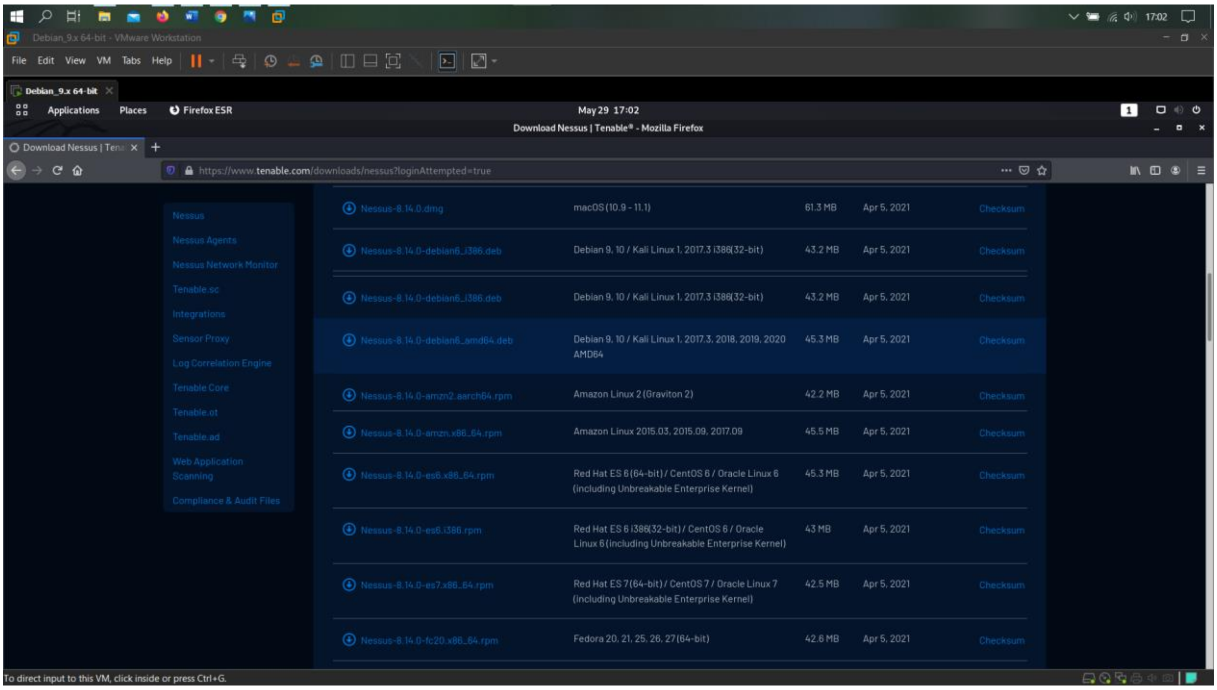
First Name
Last Name
Business Email

□ Check to receive updates from Tenable

Tenable will only process your personal data in accordance with its Privacy Policy.

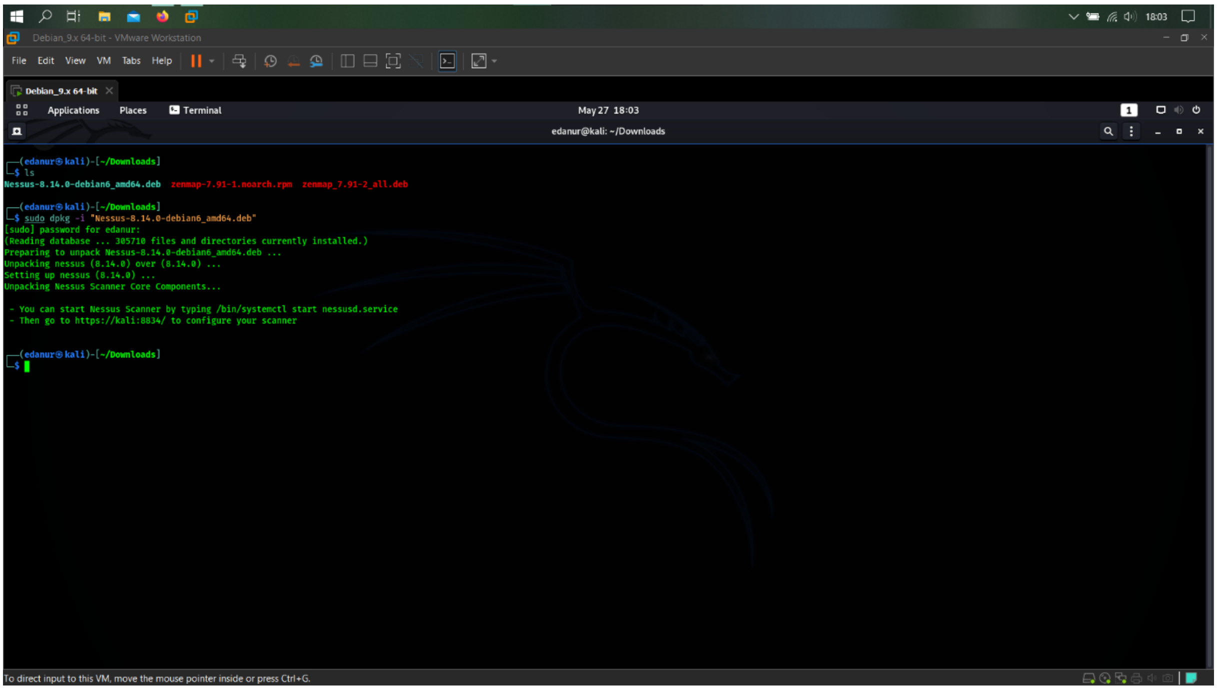
Get Started

2- Then, you go to "https://www.tenable.com/downloads/nessus?loginAttempted=true" and download the Nessus version suitable for your operating system.


Debian_9.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Debian_9.x 64-bit
Applications Places Firefox ESR
May 29 17:02
Download Nessus | Tenable® - Mozilla Firefox
Download Nessus | Tena
https://www.tenable.com/downloads/nessus?loginAttempted=true
Nessus
Nessus Agents
Nessus Network Monitor
Tenable.sc
Integrations
Sensor Proxy
Log Correlation Engine
Tenable Core
Tenable.ot
Tenable.ad
Web Application Scanning
Compliance & Audit Files
To direct input to this VM, click inside or press Ctrl+G.
17:02

Nessus-8.14.0.dmg	macOS (10.9 - 11.1)	61.3 MB	Apr 5, 2021	Checksum
Nessus-8.14.0-debian6_i386.deb	Debian 9, 10 / Kali Linux 1, 2017.3 i386(32-bit)	43.2 MB	Apr 5, 2021	Checksum
Nessus-8.14.0-debian6_i386.deb	Debian 9, 10 / Kali Linux 1, 2017.3 i386(32-bit)	43.2 MB	Apr 5, 2021	Checksum
Nessus-8.14.0-debian6_amd64.deb	Debian 9, 10 / Kali Linux 1, 2017.3, 2018, 2019, 2020 AMD64	45.3 MB	Apr 5, 2021	Checksum
Nessus-8.14.0-amzn2.aarch64.rpm	Amazon Linux 2 (Graviton 2)	42.2 MB	Apr 5, 2021	Checksum
Nessus-8.14.0-amzn.x86_64.rpm	Amazon Linux 2015.03, 2015.09, 2017.09	45.5 MB	Apr 5, 2021	Checksum
Nessus-8.14.0-es6.x86_64.rpm	Red Hat ES 6 (64-bit) / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel)	45.3 MB	Apr 5, 2021	Checksum
Nessus-8.14.0-es6.i386.rpm	Red Hat ES 6 i386(32-bit) / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel)	43 MB	Apr 5, 2021	Checksum
Nessus-8.14.0-es7.x86_64.rpm	Red Hat ES 7 (64-bit) / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel)	42.5 MB	Apr 5, 2021	Checksum
Nessus-8.14.0-fc20.x86_64.rpm	Fedora 20, 21, 25, 26, 27 (64-bit)	42.6 MB	Apr 5, 2021	Checksum

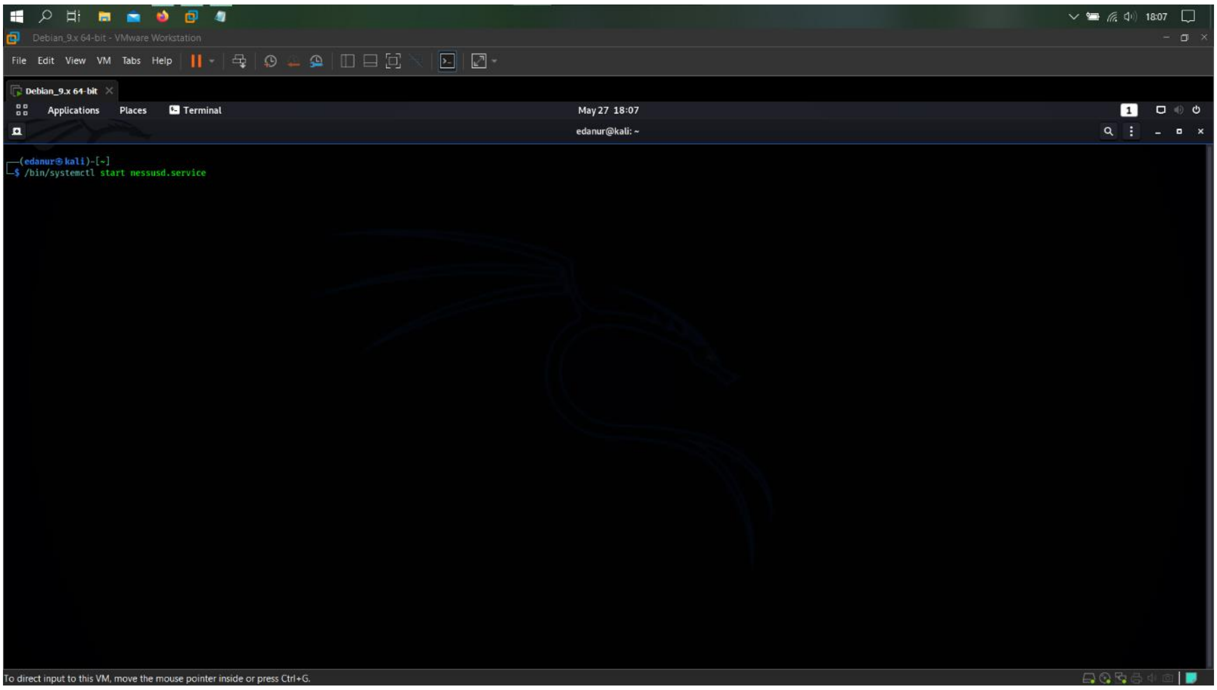
3- In the next step, we go to the terminal and install the version we downloaded.



```
┌──(edanur㉿kali)-[~/Downloads]
└─$ ls
Nessus-8.14.0-debian6_amd64.deb  zenmap-7.91-1.noarch.rpm  zenmap_7.91-2_all.deb

┌──(edanur㉿kali)-[~/Downloads]
└─$ sudo dpkg -i "Nessus-8.14.0-debian6_amd64.deb"
[sudo] password for edanur:
(Reading database ... 305710 files and directories currently installed.)
Preparing to unpack Nessus-8.14.0-debian6_amd64.deb ...
Unpacking nessus (8.14.0) over (8.14.0) ...
Setting up nessus (8.14.0) ...
Unpacking Nessus Scanner Core Components...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://kali:8834/ to configure your scanner


┌──(edanur㉿kali)-[~/Downloads]
└─$ 
```

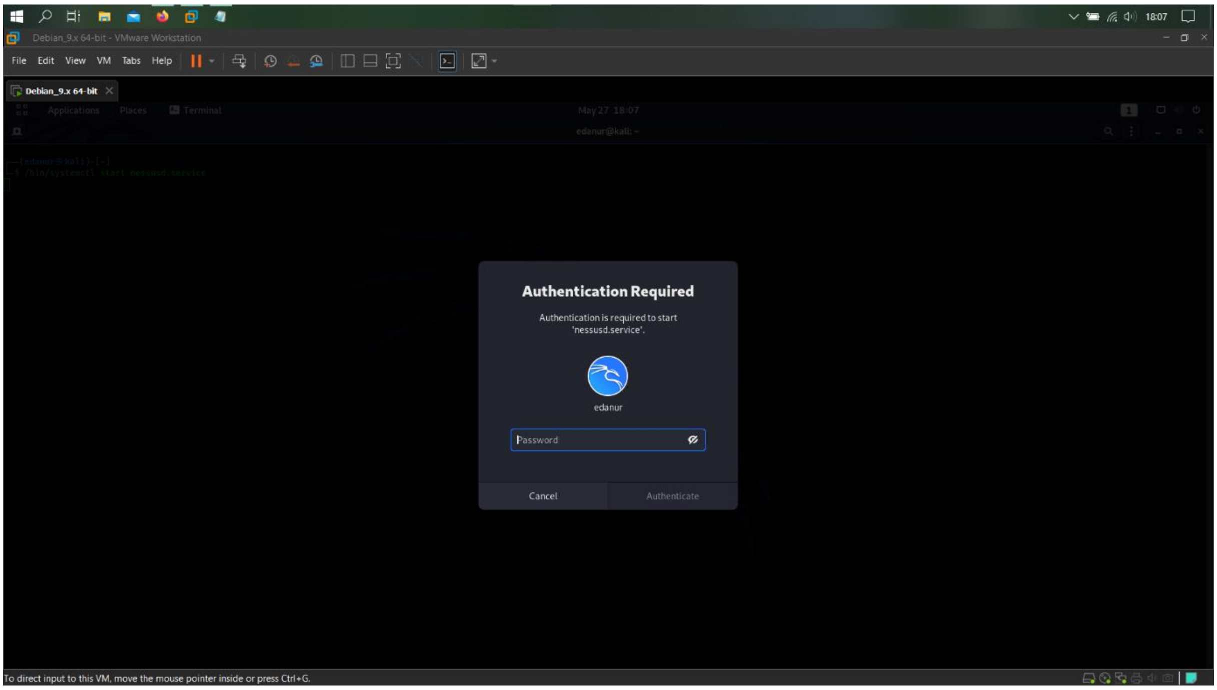
Debian_9.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Debian_9.x 64-bit
Applications Places Terminal
May 27 18:03
edanur@kali: ~/Downloads
18:03
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

4- Then, write the command to the terminal that allows us to start the Nessus service.



```
┌──(edanur㉿kali)-[~]
└─$ /bin/systemctl start nessusd.service
```

Debian_9.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Debian_9.x 64-bit
Applications Places Terminal
May 27 18:07
edanur@kali: ~
18:07
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



```
┌──(edanur㉿kali)-[~]
└─$ /bin/systemctl start nessusd.service
```

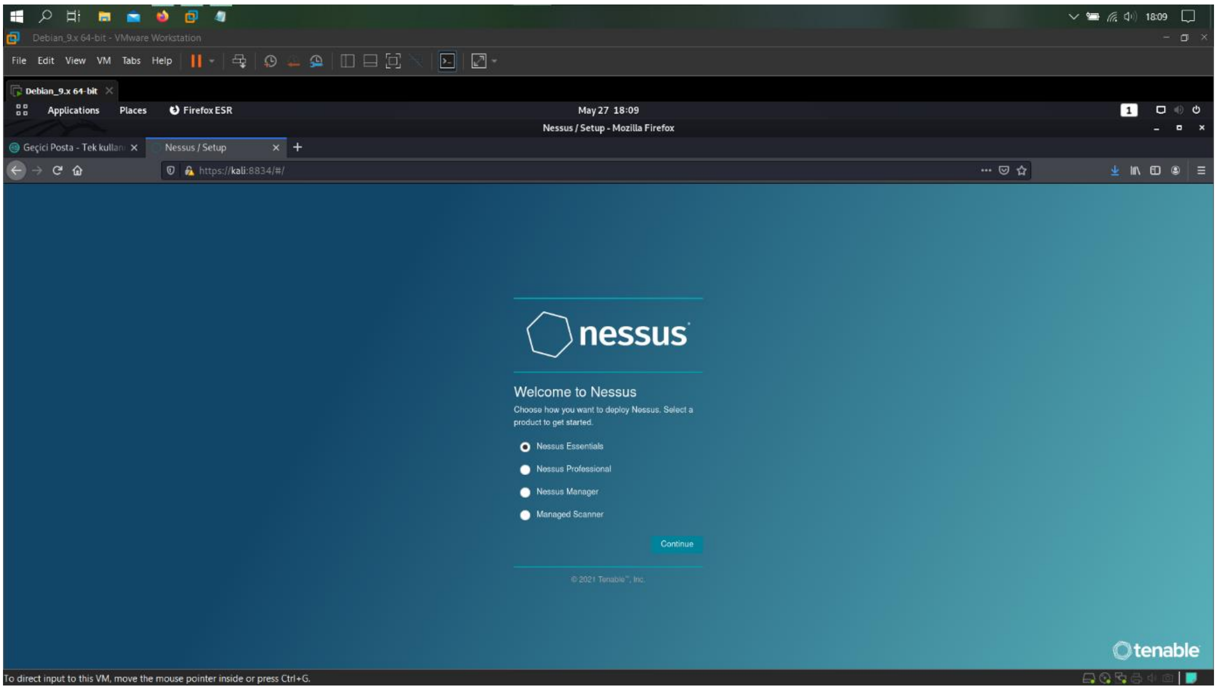
Authentication Required

Authentication is required to start 'nessusd.service'.

edanur

Debian_9.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Debian_9.x 64-bit
Applications Places Terminal
May 27 18:07
edanur@kali: ~
Password
Cancel
Authenticate
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
18:07

5- In the next step, open a new web browser and write the connection port given at the end of the installation "https://kali:8834/" in the browser opened and log in to Nessus. Then, choose Nessus Essentials, the free version, and continue.



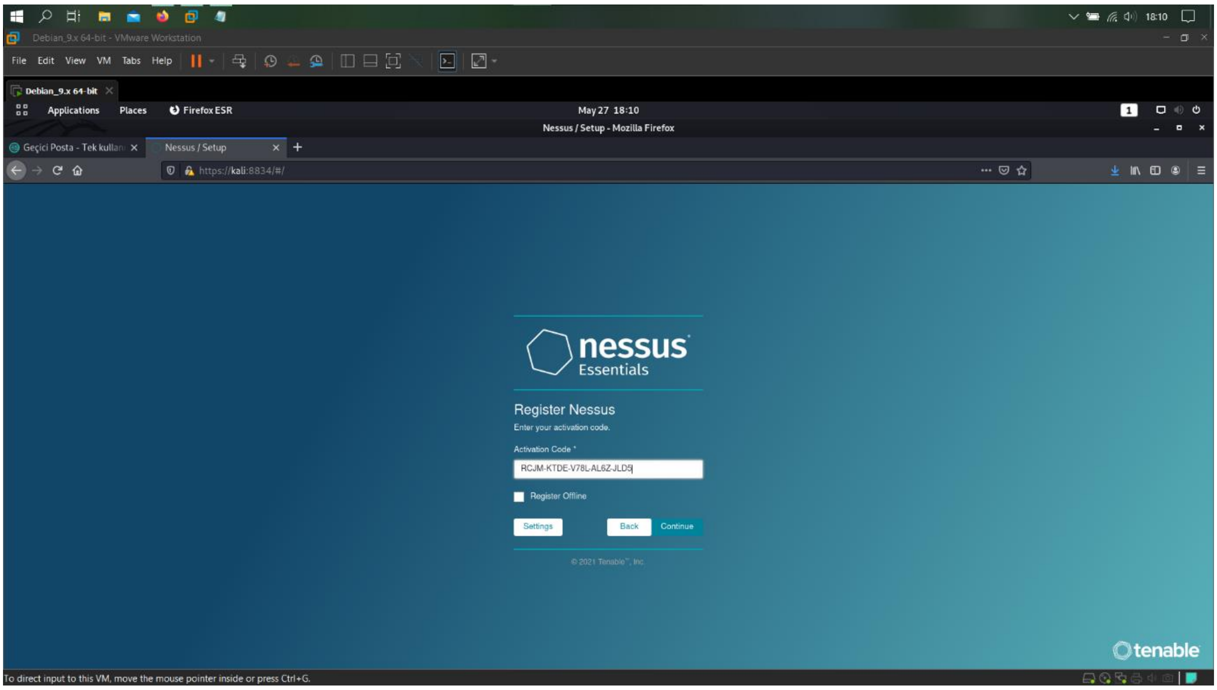
Welcome to Nessus

Choose how you want to deploy Nessus. Select a product to get started.

- ● Nessus Essentials
- ○ Nessus Professional
- ○ Nessus Manager
- ○ Managed Scanner

Debian_9.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Debian_9.x 64-bit
Applications Places Firefox ESR
May 27 18:09
Nessus / Setup - Mozilla Firefox
Geçici Posta - Tek kullan
Nessus / Setup
https://kali:8834/#/
nessus
Continue
© 2021 Tenable™, Inc.
tenable
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
18:09

6- In this step, you enter the activation code given when you registered with Nessus. Then, you are creating your user account.



Debian_9.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Applications Places Firefox ESR
May 27 18:10
Nessus / Setup - Mozilla Firefox
Geçici Posta - Tek kullan
Nessus / Setup
https://kali:8834/#/
nessus Essentials
Settings
Back
Continue
© 2021 Tenable™, Inc.
tenable
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

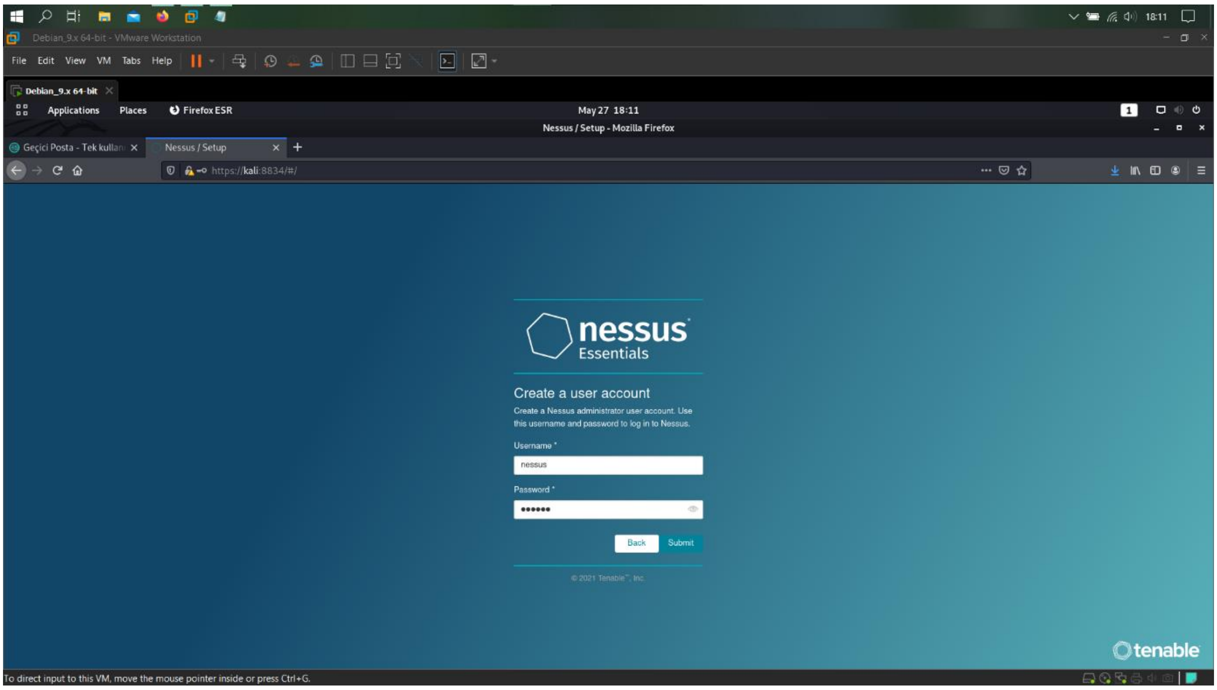
Register Nessus

Enter your activation code.

Activation Code *

RCJM-KTDE-V78L-AL6Z-JLD5

□ Register Offline



Debian_9.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Applications Places Firefox ESR
May 27 18:11
Nessus / Setup - Mozilla Firefox
Geçici Posta - Tek kullan
Nessus / Setup
https://kali:8834/#/
nessus Essentials
Back
Submit
© 2021 Tenable™, Inc.
tenable
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Create a user account

Create a Nessus administrator user account. Use this username and password to log in to Nessus.

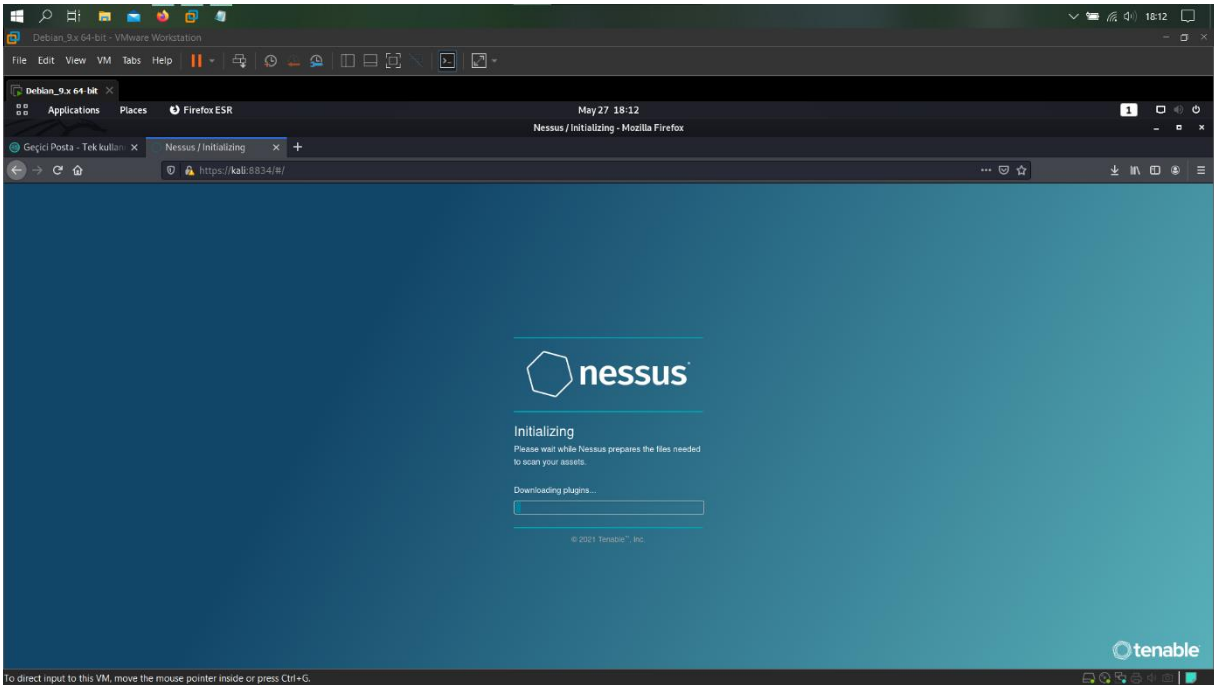
Username *

nessus

Password *

••••••

7- In this step, Nessus downloads some required plugins and the installation is complete.

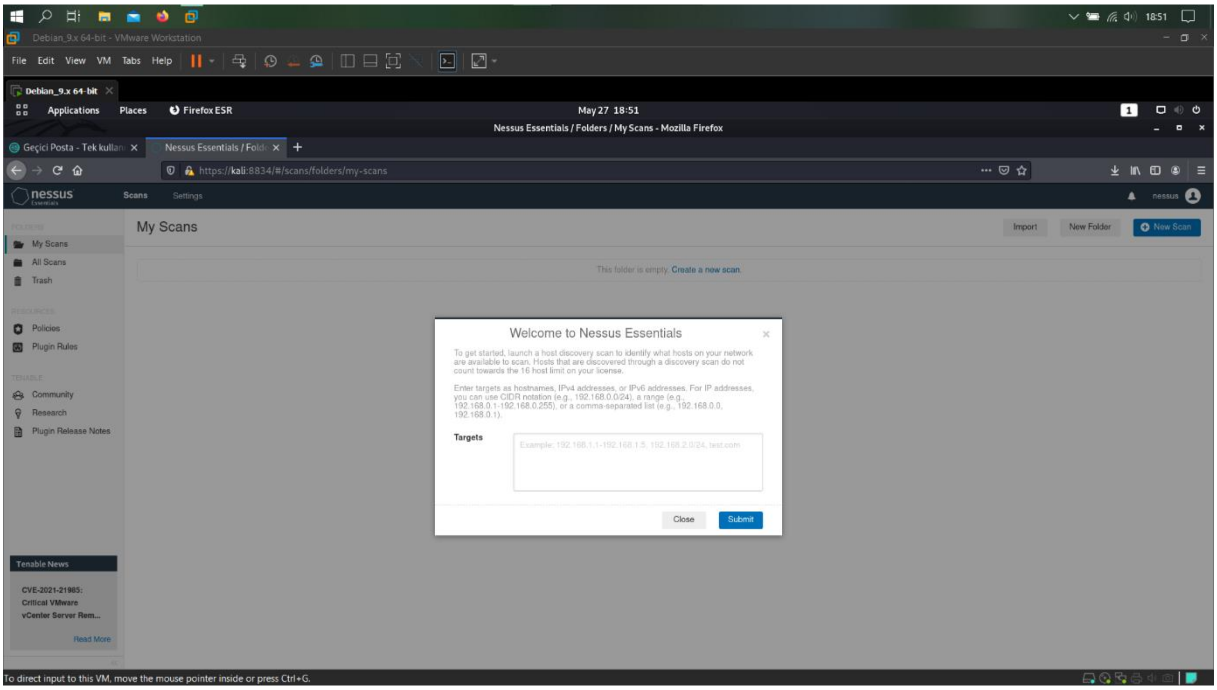


Debian_9.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Debian_9.x 64-bit
Applications Places Firefox ESR
May 27 18:12
Nessus / Initializing - Mozilla Firefox
Geçici Posta - Tek kullan
Nessus / Initializing
https://kali:8834/#/
nessus
© 2021 Tenable™, Inc.
tenable
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
18:12

Initializing

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

Downloading plugins...



Debian_9.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Debian_9.x 64-bit
Applications Places Firefox ESR
May 27 18:51
Nessus Essentials / Folders / My Scans - Mozilla Firefox
Geçici Posta - Tek kullan
Nessus Essentials / Fold
https://kali:8834/#/scans/folders/my-scans
nessus Essentials
Scans
Settings
nessus
My Scans
All Scans
Trash
Policies
Plugin Rules
Community
Research
Plugin Release Notes
Tenable News
CVE-2021-21985: Critical VMware vCenter Server Rem...
Read More
Import
New Folder
New Scan
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
18:51

My Scans

This folder is empty. Create a new scan.

Welcome to Nessus Essentials

To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets: Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

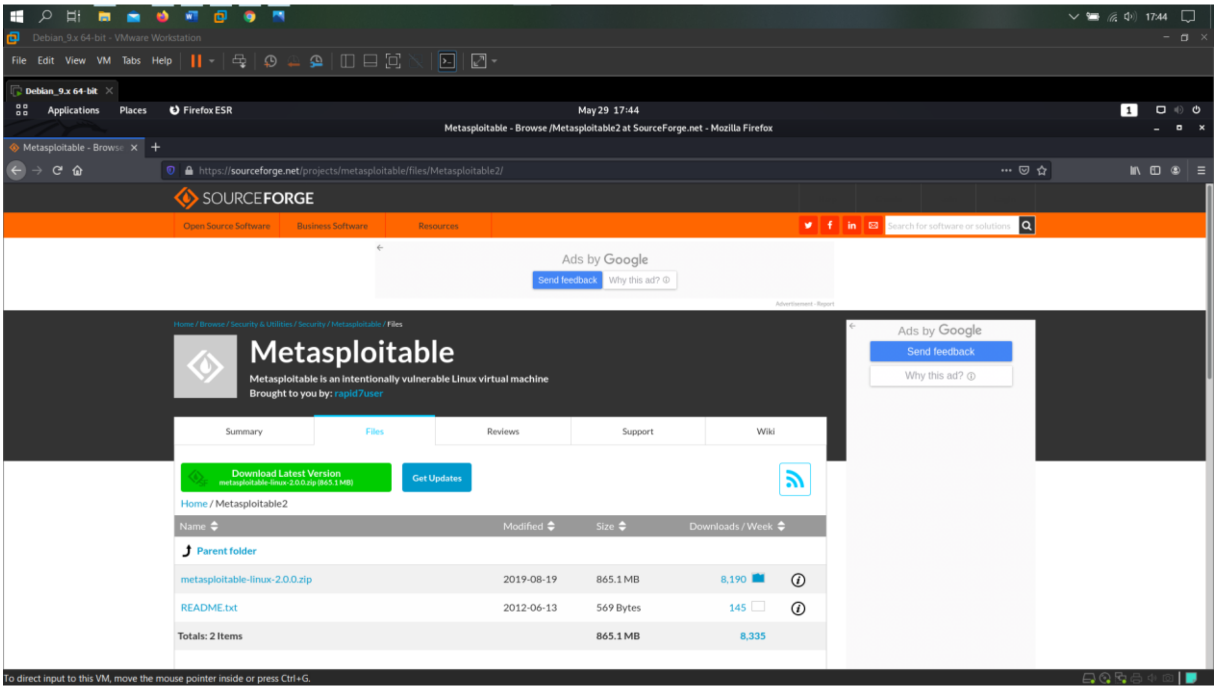
Close Submit

METASPLOITABLE-2

Metasploitable2 is a test environment created for use in hands-on penetration testing training and security research. A vulnerable test environment is needed in cyber security trainings, Metasploitable2 application can be used for this.

DOWNLOADING and SETTING UP METASPLOITABLE-2

1- First of all, go to "https://sourceforge.net/projects/metasploitable/files/Metasploitable2/" and perform the download process. The compressed file is about 800 MB and can take a while to download over a slow connection. After you have downloaded the Metasploitable 2 file, you will need to unzip the file to see it is contents.



Debian_9.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Applications Places Firefox ESR
May 29 17:44
Metasploitable - Browse /Metasploitable2 at SourceForge.net - Mozilla Firefox
SOURCEFORGE
Open Source Software
Business Software
Resources
Summary
Files
Reviews
Support
Wiki
Download Latest Version
Get Updates

https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

Home / Browse / Security & Utilities / Security / Metasploitable / Files

Metasploitable

Metasploitable is an intentionally vulnerable Linux virtual machine
Brought to you by: rapid7user

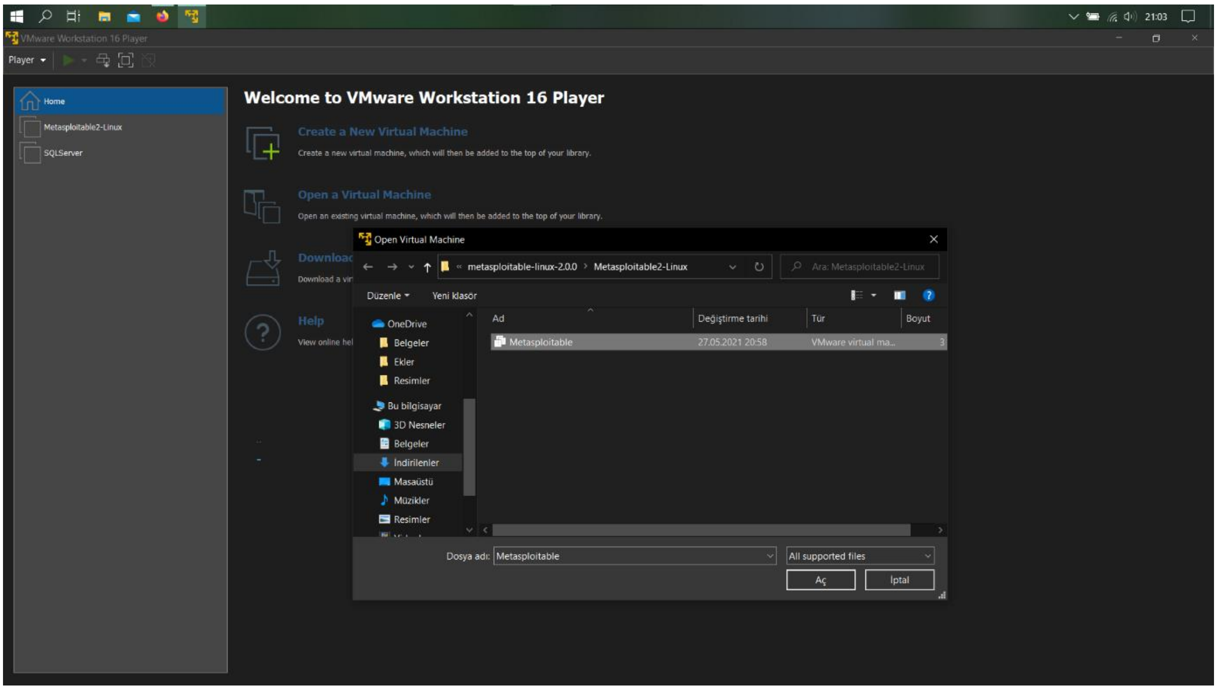
metasploitable-linux-2.0.0.zip (865.1 MB)

Home / Metasploitable2

Name	Modified	Size	Downloads / Week
Parent folder			
metasploitable-linux-2.0.0.zip	2019-08-19	865.1 MB	8,190
README.txt	2012-06-13	569 Bytes	145
Totals: 2 Items		865.1 MB	8,335

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

2- Next, open your virtualization platform and click Open a Virtual Machine to install Metasploitable2 that you downloaded. Then, run it with VMWare Player.



Create a new virtual machine, which will then be added to the top of your library.

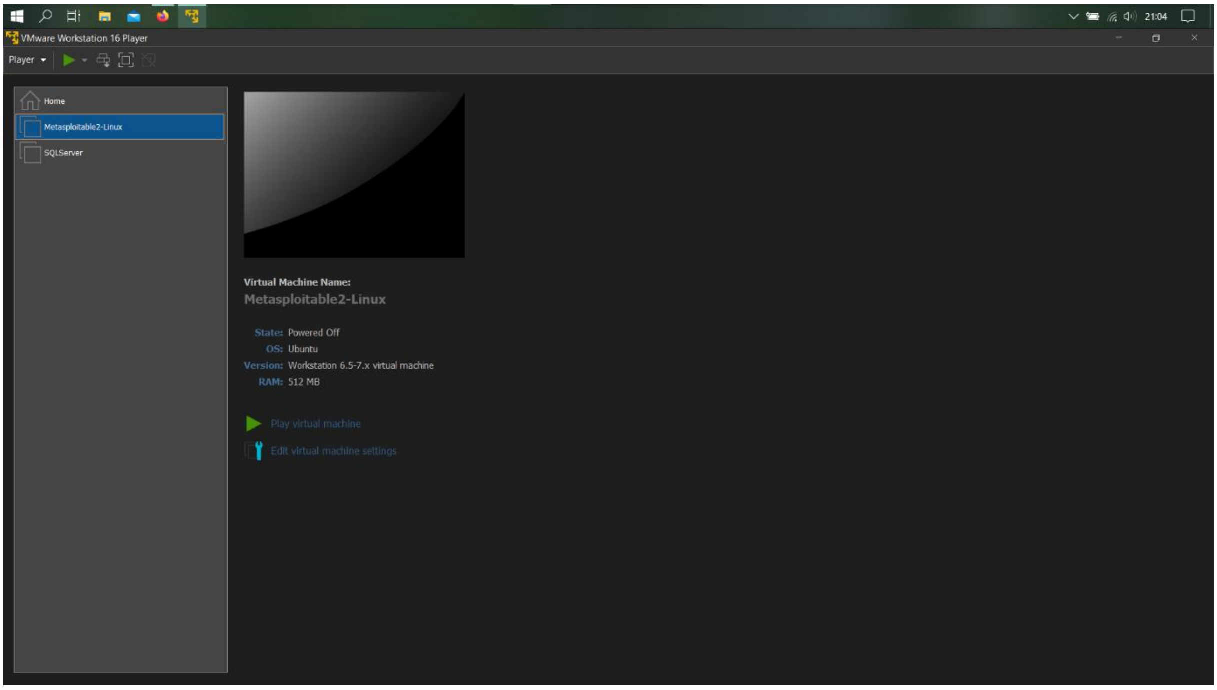
Open an existing virtual machine, which will then be added to the top of your library.

View online hel

Download a vir

Metasploitable 27.05.2021 20:58 VMware virtual ma...

Dosya adı: Metasploitable



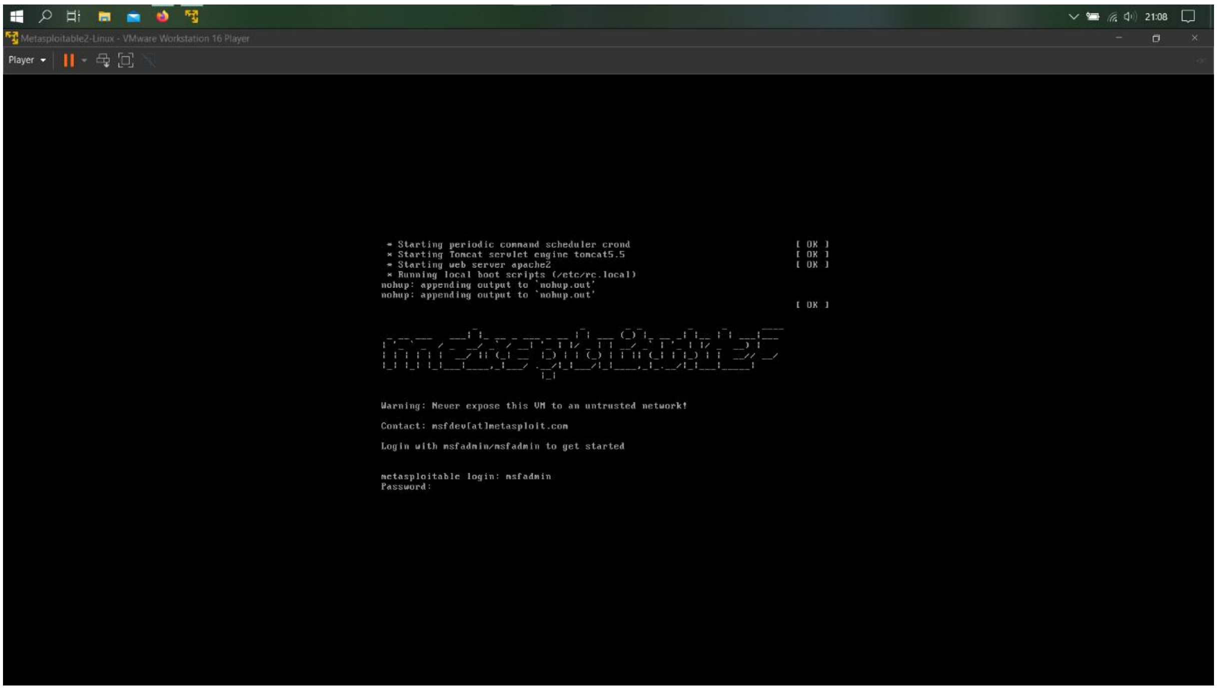
Virtual Machine Name:
Metasploitable2-Linux

State: Powered Off
OS: Ubuntu
Version: Workstation 6.5-7.x virtual machine
RAM: 512 MB

3- The user name and password are entered to log in on the screen that appears after the installation.

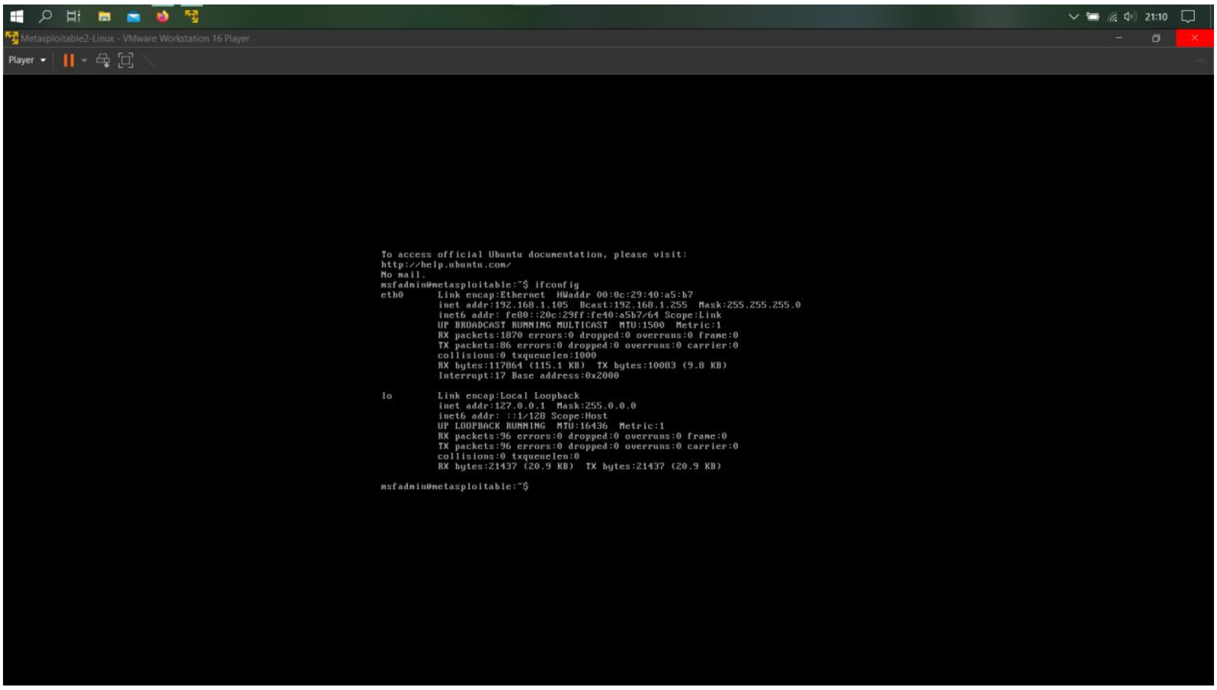
-User Name: *msfadmin*

-Password: *msfadmin*



```
 * Starting periodic command scheduler crond                          [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                           [ OK ]
 * Starting web server apache2                                        [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                      [ OK ]

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
```

4- In the next step, type “ifconfig” command on the command line to find out the IP address assigned to the machine and other details about the virtual machine. That is all. Now we can start hacking :)

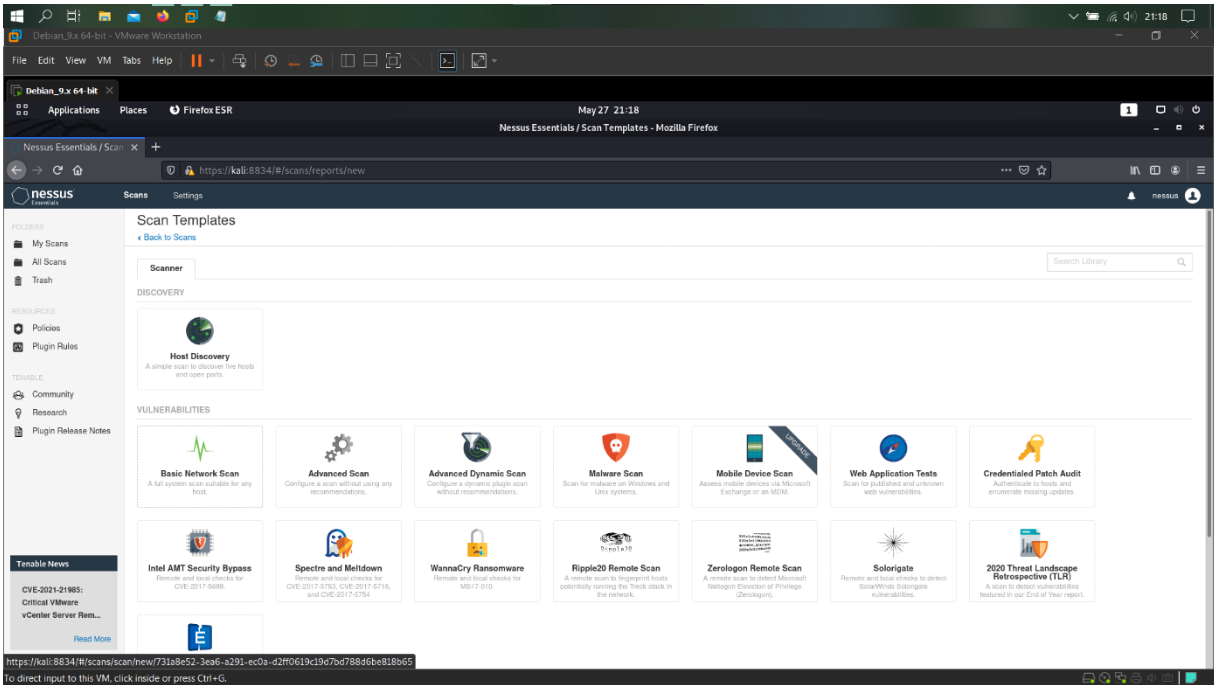


```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:40:a5:b7
          inet addr:192.168.1.105  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe40:a5b7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1870 errors:0 dropped:0 overruns:0 frame:0
          TX packets:86 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:117864 (115.1 KB)  TX bytes:10083 (9.8 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$
```

SCENARIO

In this project, I will scan for vulnerabilities on Metasploitable2 using Nessus. Latter, I will infiltrate the machine using one of the vulnerabilities I found.

1- Firstly, I open Nessus and select the "Basic Network Scan" option.



Scan Templates
‹ Back to Scans

DISCOVERY

Host Discovery
A simple scan to discover live hosts and open ports.

VULNERABILITIES

Basic Network Scan
A full system scan suitable for any host.

Advanced Scan
Configure a scan without using any recommendations.

Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.

Malware Scan
Scan for malware on Windows and Unix systems.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests
Scan for published and unknown web vulnerabilities.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.

Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

WannaCry Ransomware
Remote and local checks for MS17-010.

Ripple20 Remote Scan
A remote scan to fingerprint hosts potentially running the Treck stack in the network.

Zerologon Remote Scan
A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).

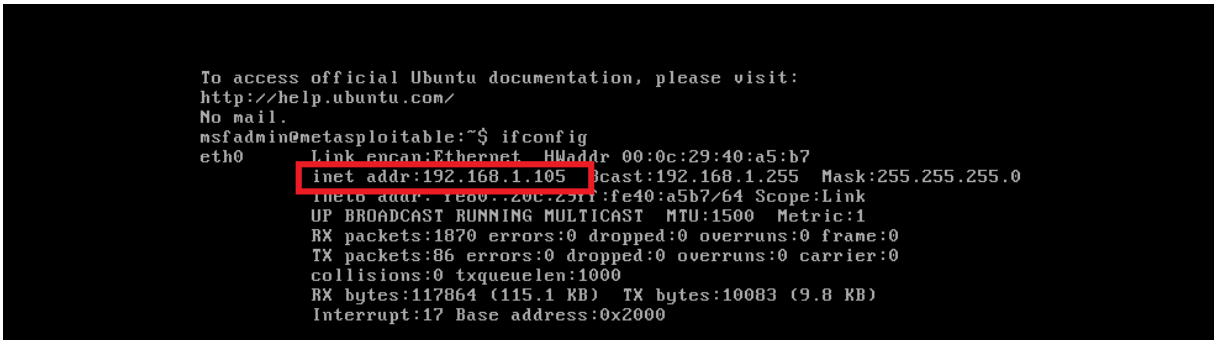
Solorigate
Remote and local checks to detect SolarWinds Solorigate vulnerabilities.

2020 Threat Landscape Retrospective (TLR)
A scan to detect vulnerabilities featured in our End of Year report.

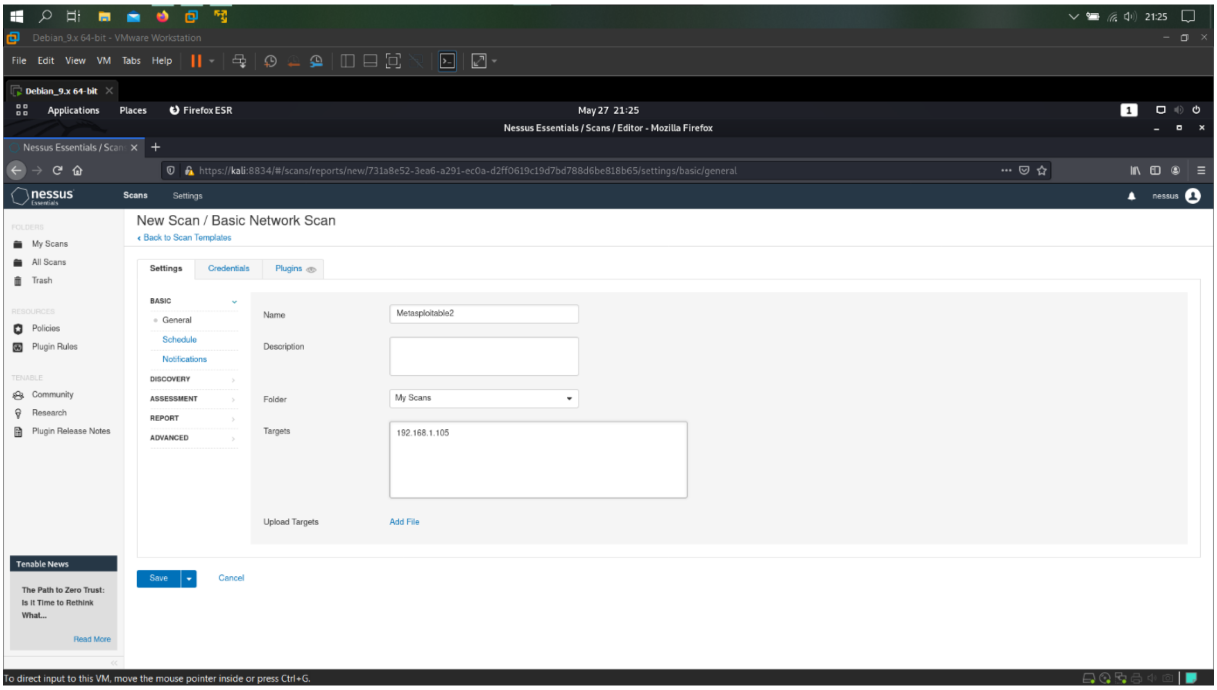
https://kali:8834/#/scans/scan/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65

To direct input to this VM, click inside or press Ctrl+G.

2- Then, I specify the name for the scanning process and write the IP of the target machine. After these steps, I launch the scanning process.



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:40:a5:b7
          inet addr:192.168.1.105  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe40:a5b7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1870 errors:0 dropped:0 overruns:0 frame:0
          TX packets:86 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:117864 (115.1 KB)  TX bytes:10083 (9.8 KB)
          Interrupt:17 Base address:0x2000
```



Debian_9.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Applications Places Firefox ESR
May 27 21:25
Nessus Essentials / Scans / Editor - Mozilla Firefox
https://kali:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/basic/general
nessus
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
TENABLE
Community
Research
Plugin Release Notes
Tenable News
The Path to Zero Trust: Is it Time to Rethink What...
Read More
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Save
Cancel
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

New Scan / Basic Network Scan

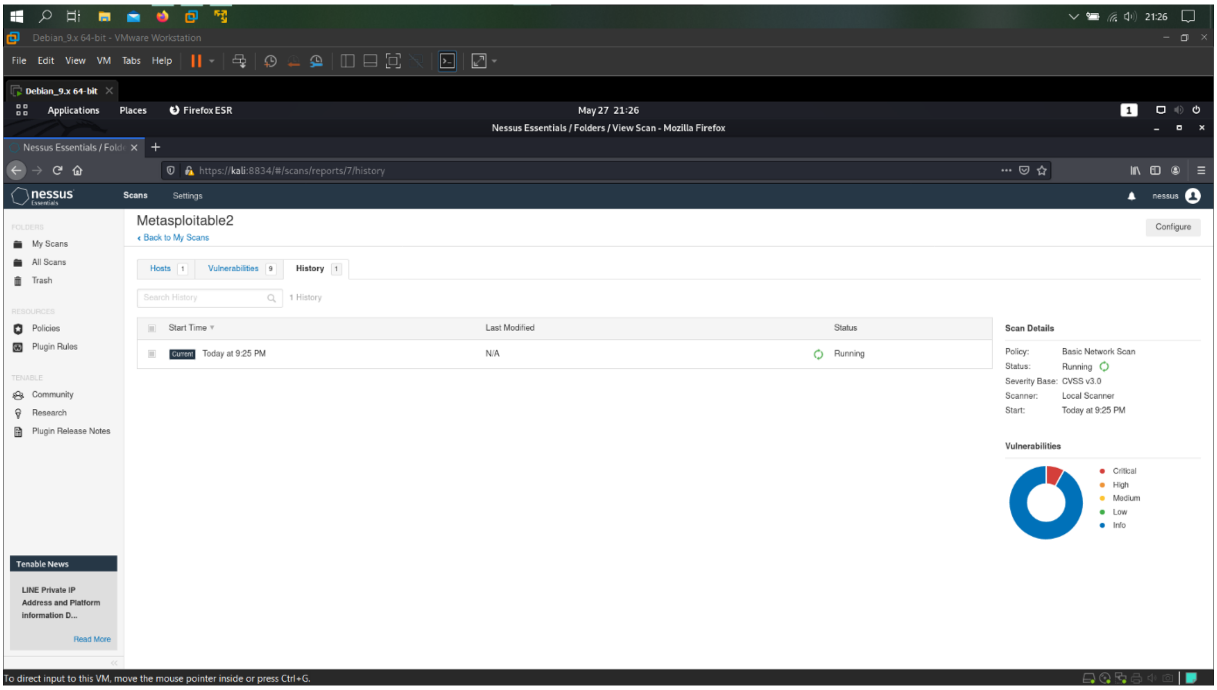
Name: Metasploitable2

Description:

Folder: My Scans

Targets: 192.168.1.105

Upload Targets: Add File



Debian_9.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Applications Places Firefox ESR
May 27 21:26
Nessus Essentials / Folders / View Scan - Mozilla Firefox
https://kali:8834/#/scans/reports/7/history
nessus
Scans
Settings
Configure
Back to My Scans
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
TENABLE
Community
Research
Plugin Release Notes
Tenable News
LINE Private IP Address and Platform Information D...
Read More
Hosts 1
Vulnerabilities 9
History 1
Search History
1 History
Critical
High
Medium
Low
Info
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Metasploitable2

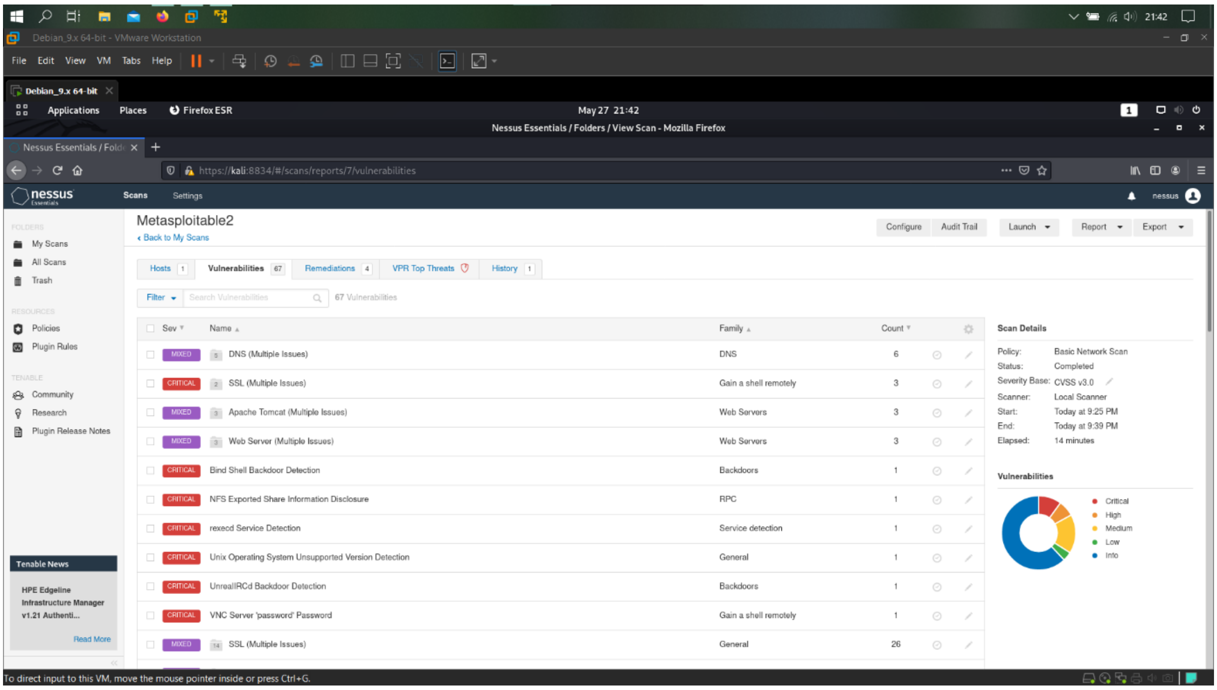
Start Time	Last Modified	Status
Current Today at 9:25 PM	N/A	Running

Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 9:25 PM

Vulnerabilities

3- In this step, we see that the scanning process is finished and the vulnerabilities are listed according to their degree.



Nessus Essentials / Folders / View Scan - Mozilla Firefox

https://kali:8834/#/scans/reports/7/vulnerabilities

Metasploitable2

‹ Back to My Scans

Hosts 1 | Vulnerabilities 67 | Remediations 4 | VPR Top Threats | History 1

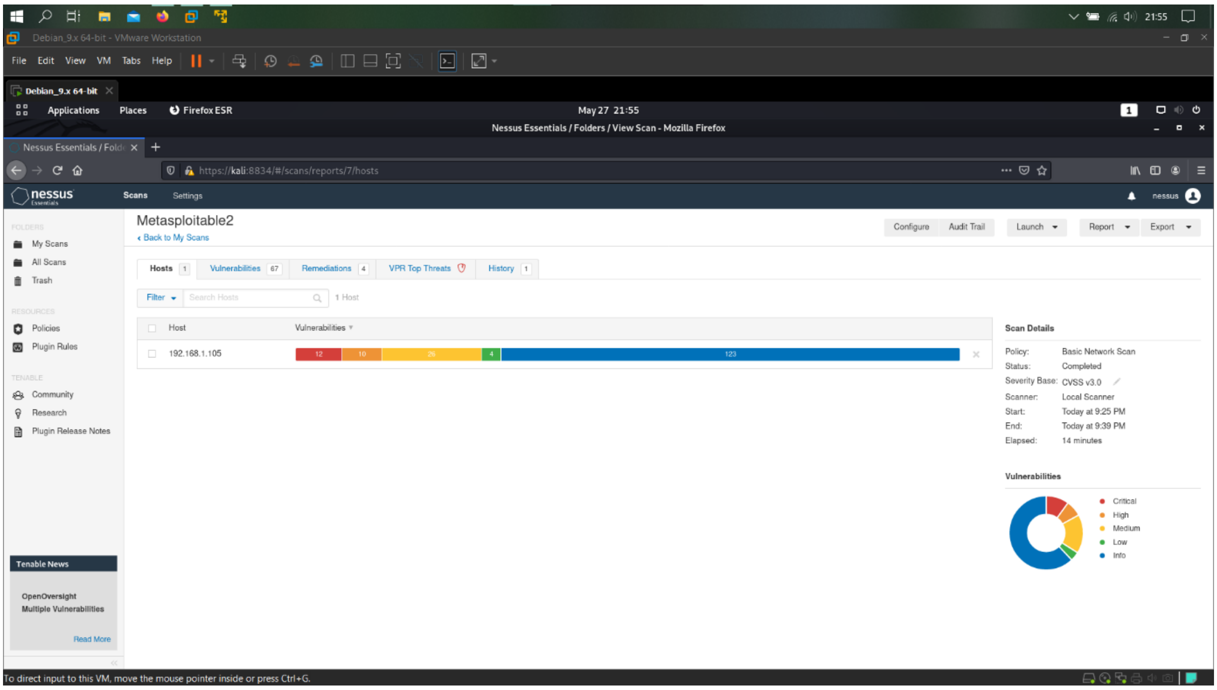
67 Vulnerabilities

☐	Sev	Name	Family	Count
☐	MIXED	5 DNS (Multiple Issues)	DNS	6
☐	CRITICAL	2 SSL (Multiple Issues)	Gain a shell remotely	3
☐	MIXED	3 Apache Tomcat (Multiple Issues)	Web Servers	3
☐	MIXED	3 Web Server (Multiple Issues)	Web Servers	3
☐	CRITICAL	Bind Shell Backdoor Detection	Backdoors	1
☐	CRITICAL	NFS Exported Share Information Disclosure	RPC	1
☐	CRITICAL	rexecd Service Detection	Service detection	1
☐	CRITICAL	Unix Operating System Unsupported Version Detection	General	1
☐	CRITICAL	UnrealIRCd Backdoor Detection	Backdoors	1
☐	CRITICAL	VNC Server 'password' Password	Gain a shell remotely	1
☐	MIXED	14 SSL (Multiple Issues)	General	26

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 9:25 PM
End: Today at 9:39 PM
Elapsed: 14 minutes

Vulnerabilities



Nessus Essentials / Folders / View Scan - Mozilla Firefox

https://kali:8834/#/scans/reports/7/hosts

Metasploitable2

‹ Back to My Scans

Hosts 1 | Vulnerabilities 67 | Remediations 4 | VPR Top Threats | History 1

1 Host

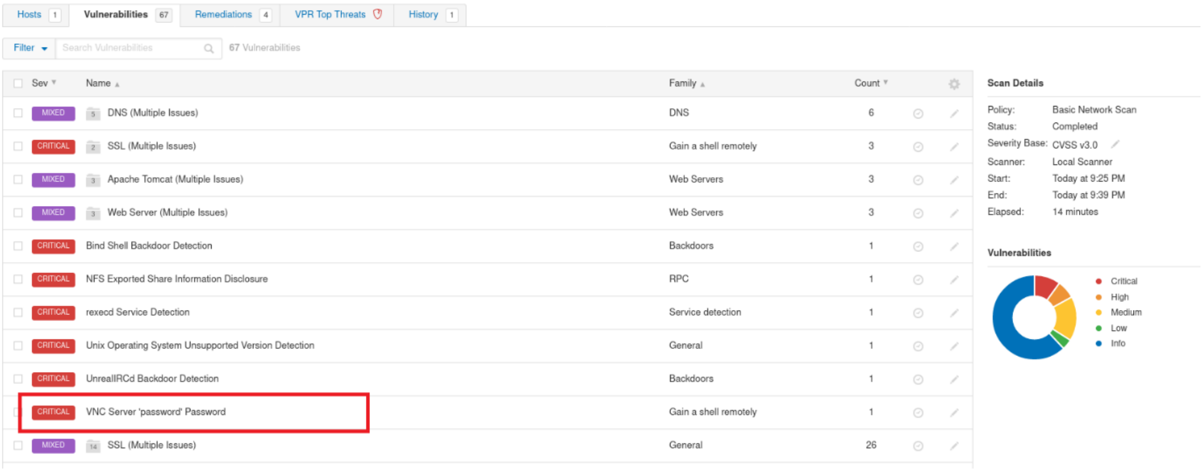
☐	Host	Vulnerabilities
☐	192.168.1.105	12 · 10 · 26 · 4 · 123

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 9:25 PM
End: Today at 9:39 PM
Elapsed: 14 minutes

Vulnerabilities

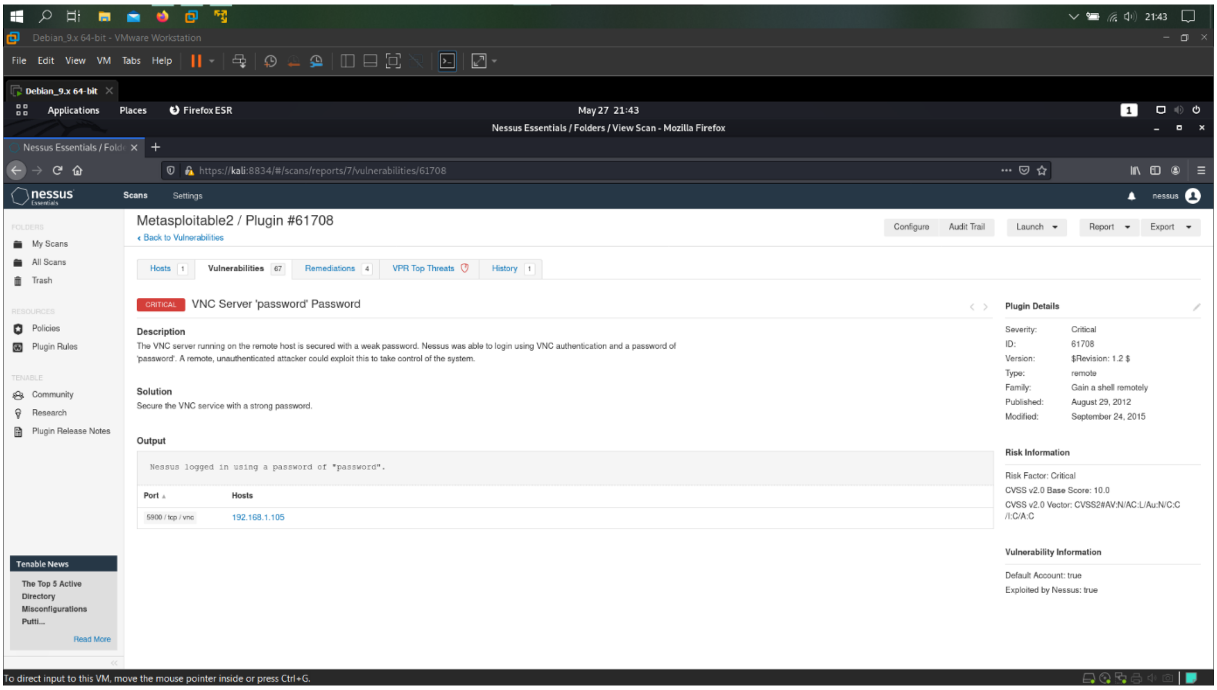
4- In this step, I choose VNC Server 'password' Password from the vulnerabilities listed. The definition of the vulnerability and the degree of risk are given on the screen by Nessus. In the next step, I will try to infiltrate the machine using this vulnerability.



Sev	Name	Family	Count
MIXED	5 DNS (Multiple Issues)	DNS	6
CRITICAL	2 SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	3 Apache Tomcat (Multiple Issues)	Web Servers	3
MIXED	3 Web Server (Multiple Issues)	Web Servers	3
CRITICAL	Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	rexecd Service Detection	Service detection	1
CRITICAL	Unix Operating System Unsupported Version Detection	General	1
CRITICAL	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	VNC Server 'password' Password	Gain a shell remotely	1
MIXED	14 SSL (Multiple Issues)	General	26

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 9:25 PM
End:	Today at 9:39 PM
Elapsed:	14 minutes


Debian_9.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Debian_9.x 64-bit
Applications Places Firefox ESR
May 27 21:43
Nessus Essentials / Folders / View Scan - Mozilla Firefox
https://kali:8834/#/scans/reports/7/vulnerabilities/61708
nessus
Scans Settings
My Scans
All Scans
Trash
Policies
Plugin Rules
Community
Research
Plugin Release Notes
Tenable News
The Top 5 Active Directory Misconfigurations Putti...
Read More
Configure Audit Trail Launch Report Export
Hosts 1 Vulnerabilities 67 Remediations 4 VPR Top Threats History 1
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Metasploitable2 / Plugin #61708

‹ Back to Vulnerabilities

CRITICAL VNC Server 'password' Password

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Output

```
Nessus logged in using a password of "password".
```

Port	Hosts
5900 / tcp / vnc	192.168.1.105

Plugin Details

Severity:	Critical
ID:	61708
Version:	$Revision: 1.2 $
Type:	remote
Family:	Gain a shell remotely
Published:	August 29, 2012
Modified:	September 24, 2015

Risk Information

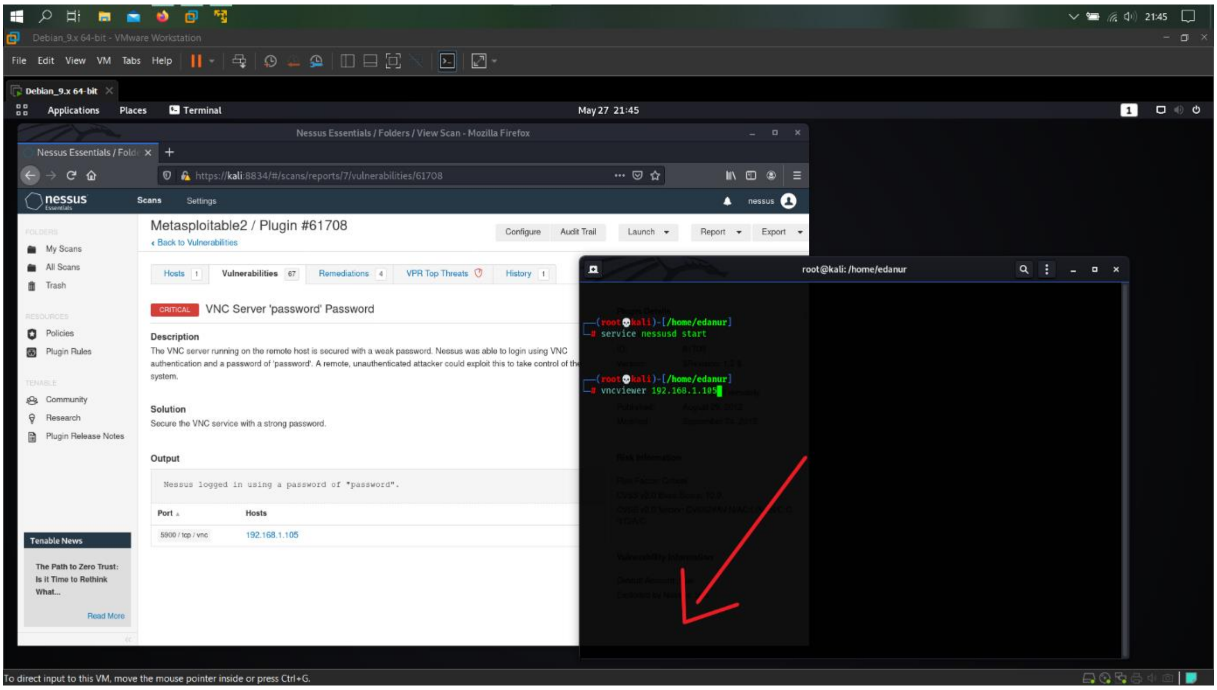
Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

Default Account: true
Exploited by Nessus: true

5- I open the command line. To run the VNC viewer client, I type the command "vncviewer" and then enter the destination IP address. I press enter and in the password query I type the password ("password") that Nessus found.

- VNC runs the VNC client (VNC viewer) program on a computer on a network. Thus, it provides interaction with the VNC server (VNC server) on another network server. As a result of this interaction, it sees the remote computer's screen and provides desktop access with keyboard and mouse movements.



Nessus Essentials / Folders / View Scan - Mozilla Firefox

https://kali:8834/#/scans/reports/7/vulnerabilities/61708

Metasploitable2 / Plugin #61708

CRITICAL VNC Server 'password' Password

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of th system.

Solution

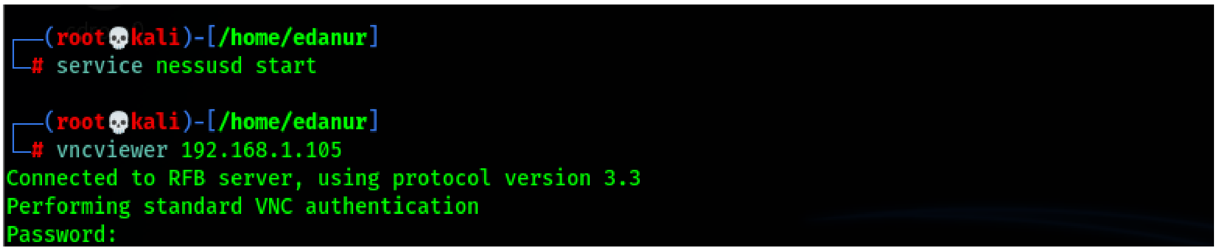
Secure the VNC service with a strong password.

Output

```
Nessus logged in using a password of "password".
```

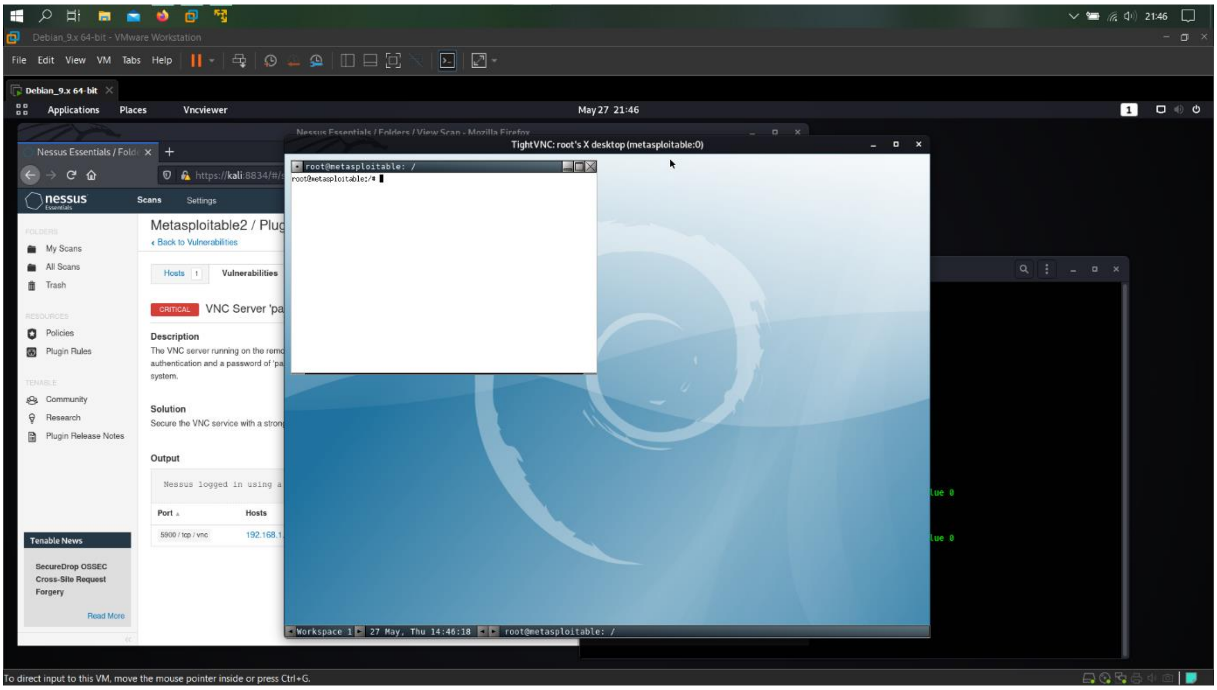
Port	Hosts
5900 / tcp / vnc	192.168.1.105

```
┌──(root💀kali)-[/home/edanur]
└─# service nessusd start

┌──(root💀kali)-[/home/edanur]
└─# vncviewer 192.168.1.105
```



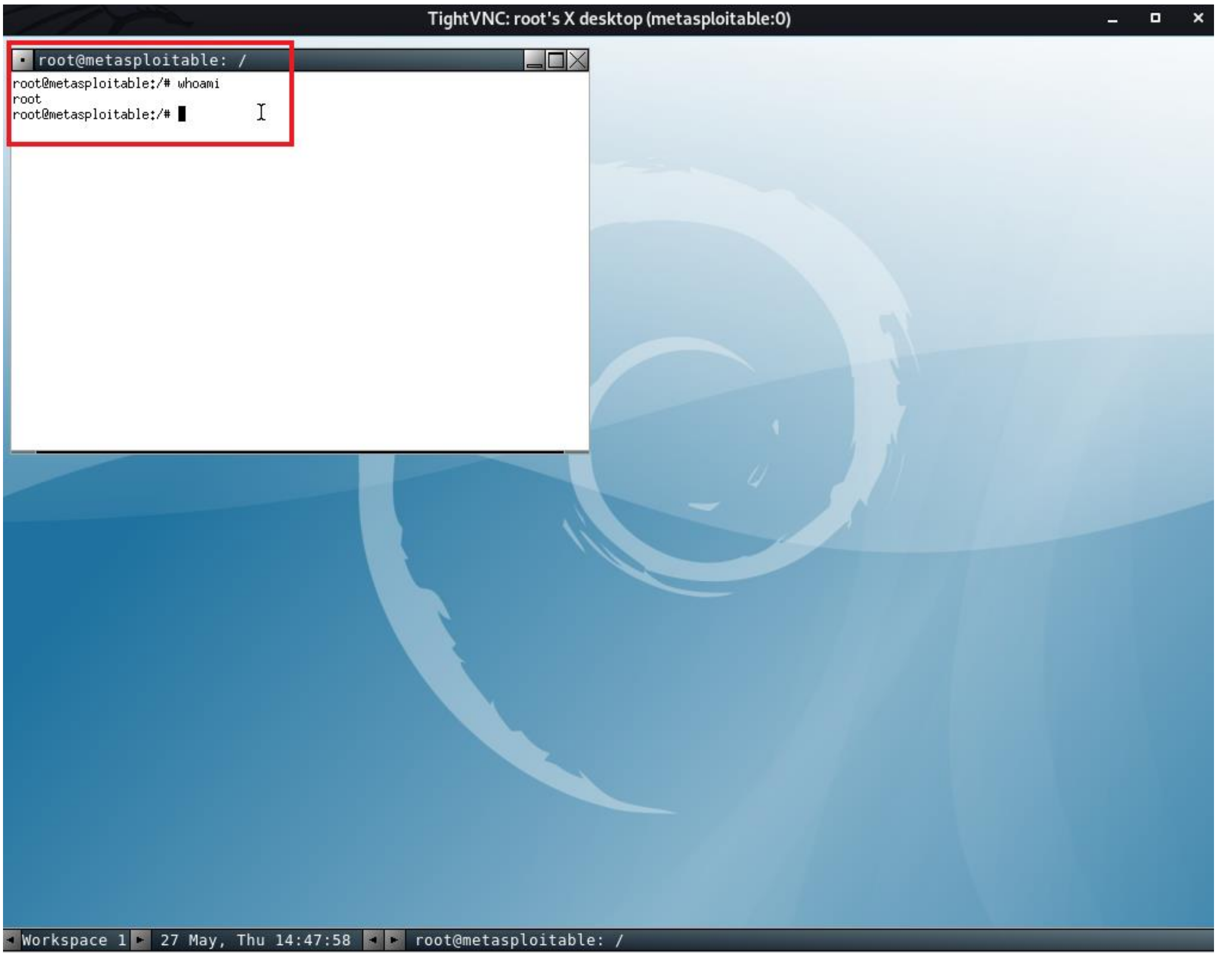
```
┌──(root💀kali)-[/home/edanur]
└─# service nessusd start

┌──(root💀kali)-[/home/edanur]
└─# vncviewer 192.168.1.105
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
```

6- As you can see, VNC viewer worked and I reached the opposite machine. Here, I ask "who am i" and see that I have access to the machine as root. So, now I can do whatever I want in the system.

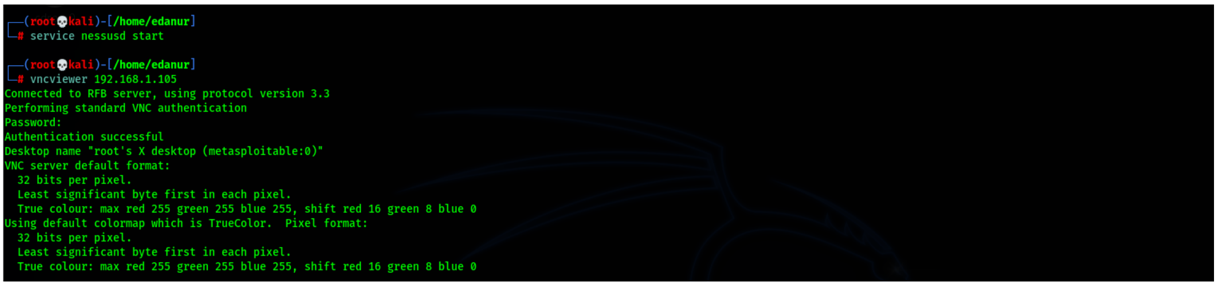


TightVNC: root's X desktop (metasploitable:0)

```
root@metasploitable:/#
```



```
root@metasploitable:/# whoami
root
root@metasploitable:/# 
```



```
┌──(root💀kali)-[/home/edanur]
└─# service nessusd start

┌──(root💀kali)-[/home/edanur]
└─# vncviewer 192.168.1.105
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

CONCLUSION

In this study, I scanned the target machine for vulnerability using Nessus, an open source vulnerability scanning software. For vulnerability scanning, I chose Metasploitable2, a test environment created to be used in hands-on penetration testing trainings. At the beginning of the work, I showed what Nessus and Metasploitable2 are and how they are set up. Next, I followed the steps required by my scenario and finally exploited a vulnerability found on the target machine.

Nessus, as far as I have experienced, is an easy to install, clear user interface and very useful security software due to its features. As seen in the study, you can scan for security vulnerabilities on your computer by using Nessus and take the necessary precautions according to the vulnerabilities. On the other hand, you can scan for vulnerabilities on a target machine and exploit them according to the vulnerabilities found. And it should be noted that Nessus is not a complete security solution, rather it is one small part of a good security strategy. Nessus does not actively prevent attacks, it is only a tool that checks your computers to find vulnerabilities that hackers could exploit. It is up to the system administrator to patch these vulnerabilities in order to create a security solution.

REFERENCES:

Çolak, F. (September, 2019). Nessus Nedir ve Ne Amaçla Kullanılır? *Fatih Çolak Bilişim Blog*. Retrieved June 9, 2021, from https://www.fatihcolak.com.tr/nessus-nedir-ve-ne-amacla-kullanilir.html

Nessus. *Tenable*. Retrieved June 9, 2021, from https://www.tenable.com/products/nessus

Wendlandt, D. Nessus: A security vulnerability scanning tool. *Carnegie Mellon University*. Retrieved June 9, 2021, from https://www.cs.cmu.edu/~dwendlan/personal/nessus.html