Task 6

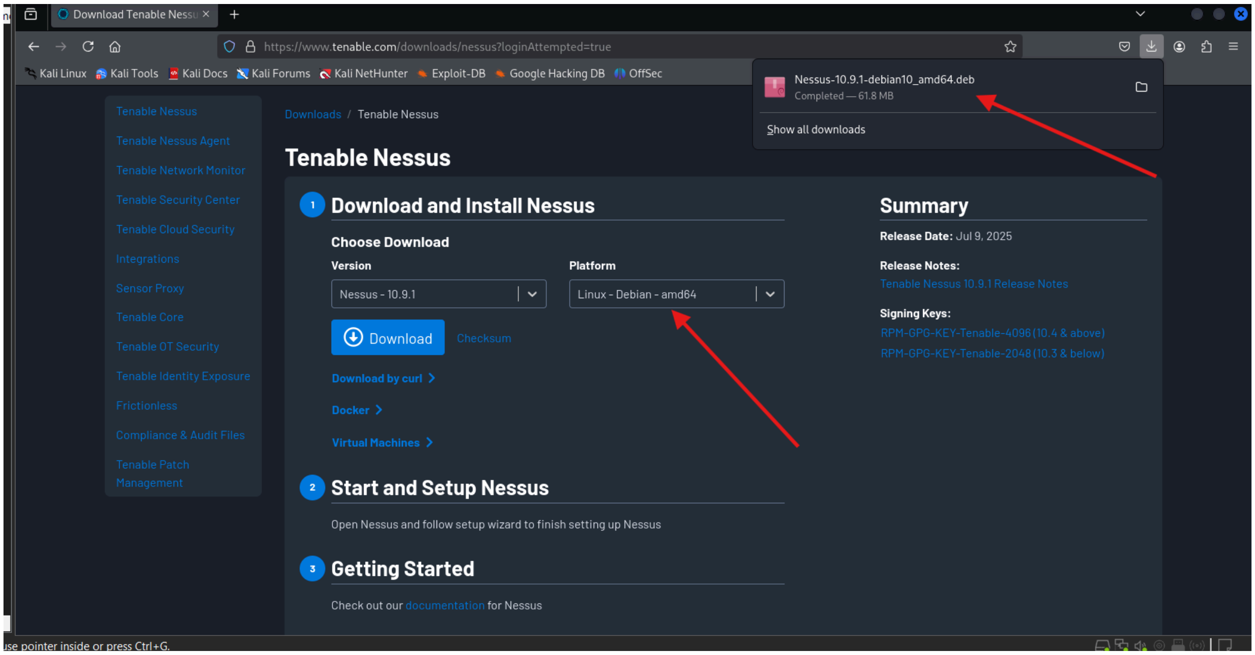
🎯 Installing and Configuring Nessus on Kali Linux:

✅ Step 1: Download Nessus

1-Go to the official Nessus download page:
👉 https://www.tenable.com/downloads/nessus
2-Under the **Linux** section, choose **Debian** (because Kali is Debian-based).

3-Click **Download** and wait for the `.deb` file to finish downloading.

Example file name: `Nessus-10.9.1-debian10_amd64.deb`



Nessus-10.9.1-debian10_amd64.deb
Completed — 61.8 MB

Tenable Nessus

1 Download and Install Nessus

Choose Download

Version: Nessus - 10.9.1

Platform: Linux - Debian - amd64

Summary

Release Date: Jul 9, 2025

Release Notes: Tenable Nessus 10.9.1 Release Notes

Signing Keys: RPM-GPG-KEY-Tenable-4096 (10.4 & above) RPM-GPG-KEY-Tenable-2048 (10.3 & below)

2 Start and Setup Nessus

Open Nessus and follow setup wizard to finish setting up Nessus

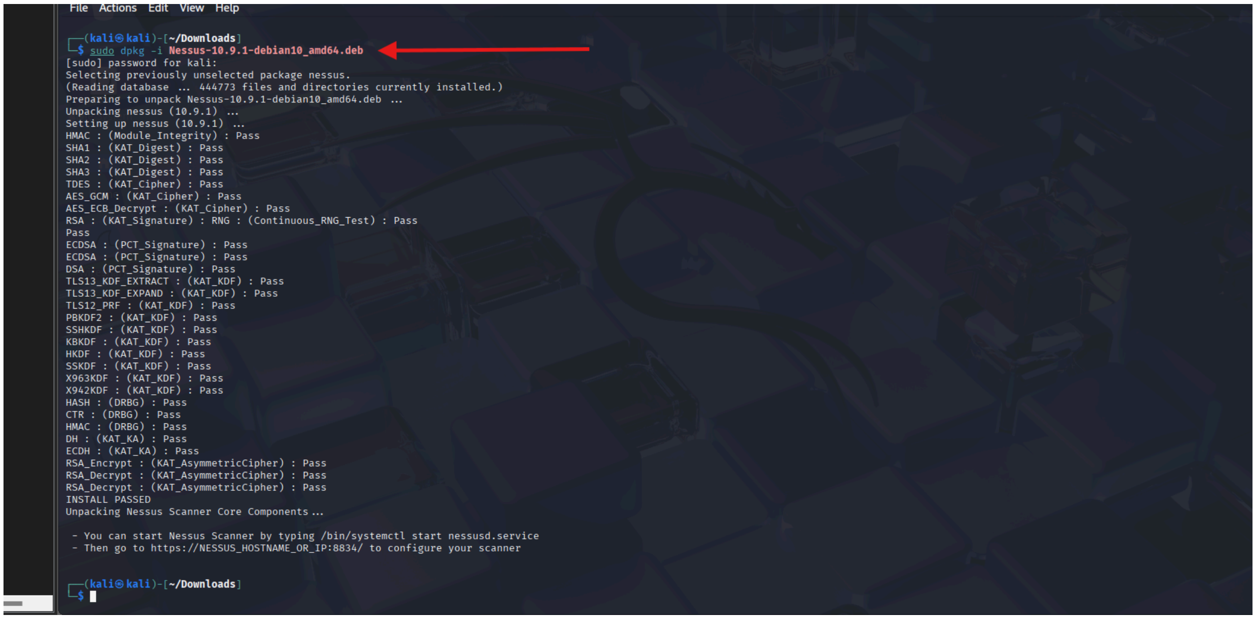
3 Getting Started

Check out our documentation for Nessus

✅ Step 2: Install Nessus:

Once the file is downloaded, open your terminal and run:

👉 sudo dpkg -i Nessus-10.9.1-debian10_amd64.deb



```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo dpkg -i Nessus-10.9.1-debian10_amd64.deb
[sudo] password for kali:
Selecting previously unselected package nessus.
(Reading database ... 444773 files and directories currently installed.)
Preparing to unpack Nessus-10.9.1-debian10_amd64.deb ...
Unpacking nessus (10.9.1) ...
Setting up nessus (10.9.1) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components...

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


┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

✅ Step 3: Start Nessus Service:

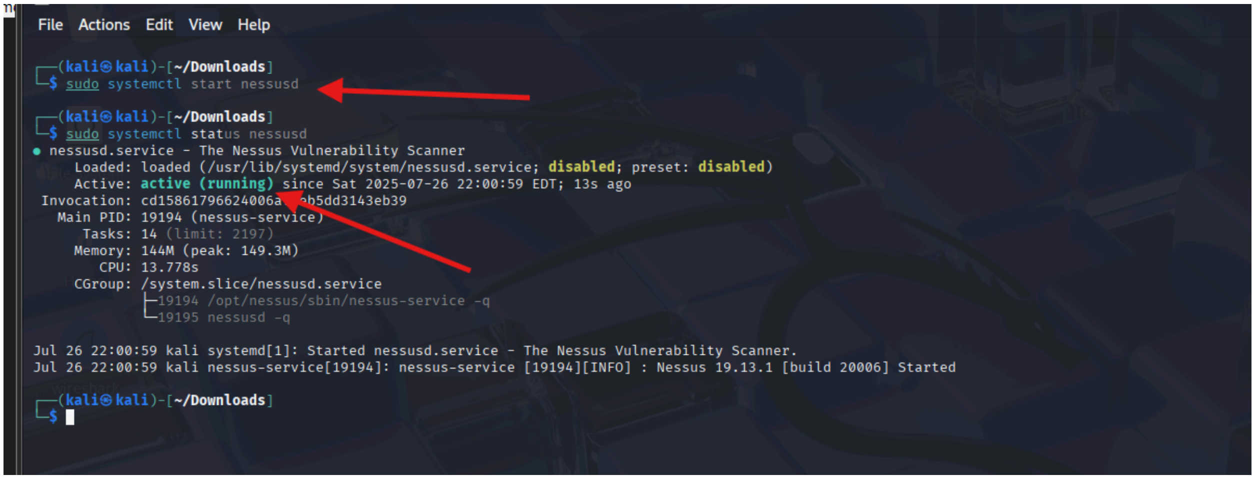
To start the Nessus service, use:

👉 sudo systemctl start nessusd

To **check if Nessus is running**, use:

👉 sudo systemctl status nessusd

You should see something like `active (running)` in green.



```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl start nessusd

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
     Active: active (running) since Sat 2025-07-26 22:00:59 EDT; 13s ago
 Invocation: cd15861796624006a  eb5dd3143eb39
   Main PID: 19194 (nessus-service)
      Tasks: 14 (limit: 2197)
     Memory: 144M (peak: 149.3M)
        CPU: 13.778s
     CGroup: /system.slice/nessusd.service
             ├─19194 /opt/nessus/sbin/nessus-service -q
             └─19195 nessusd -q

Jul 26 22:00:59 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Jul 26 22:00:59 kali nessus-service[19194]: nessus-service [19194][INFO] : Nessus 19.13.1 [build 20006] Started

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

✅ Step 4: Get Activation Code (Registration):

1-Go to the Nessus Essentials registration page:

👉 **https://www.tenable.com/products/nessus/nessus-essentials**

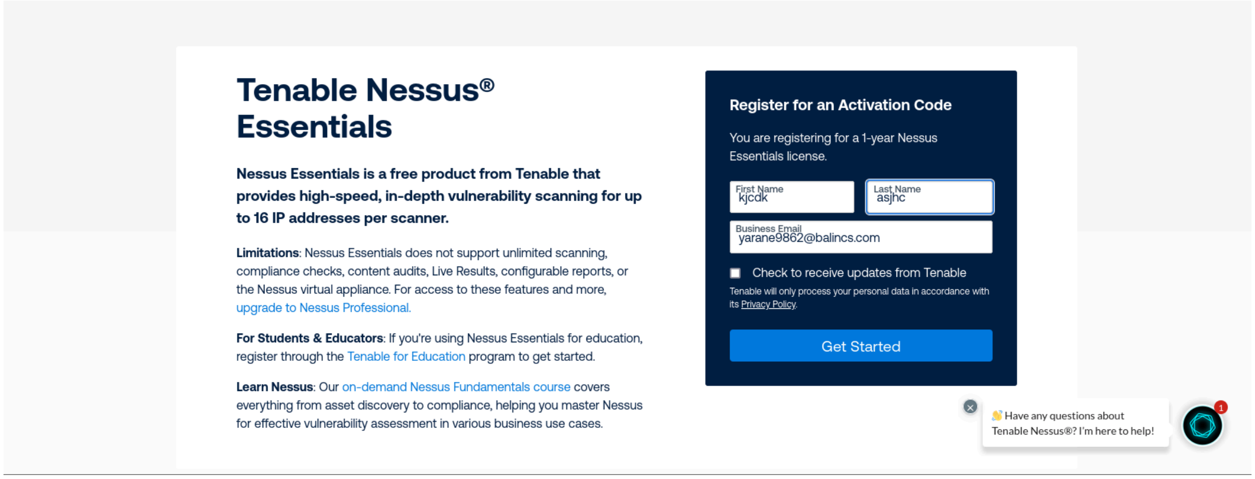
*** This page asks for a business email. If you don't have one, you can use a temporary email:**

2- go to 👉 https://temp-mail.org

3-Enter the temporary email, then check your inbox at temp-mail.org to find:

"Your activation code for Nessus Essentials"

4-Save this code, you'll use it in the web interface.



Tenable Nessus® Essentials

Nessus Essentials is a free product from Tenable that provides high-speed, in-depth vulnerability scanning for up to 16 IP addresses per scanner.

Limitations: Nessus Essentials does not support unlimited scanning, compliance checks, content audits, Live Results, configurable reports, or the Nessus virtual appliance. For access to these features and more, upgrade to Nessus Professional.

For Students & Educators: If you're using Nessus Essentials for education, register through the Tenable for Education program to get started.

Learn Nessus: Our on-demand Nessus Fundamentals course covers everything from asset discovery to compliance, helping you master Nessus for effective vulnerability assessment in various business use cases.

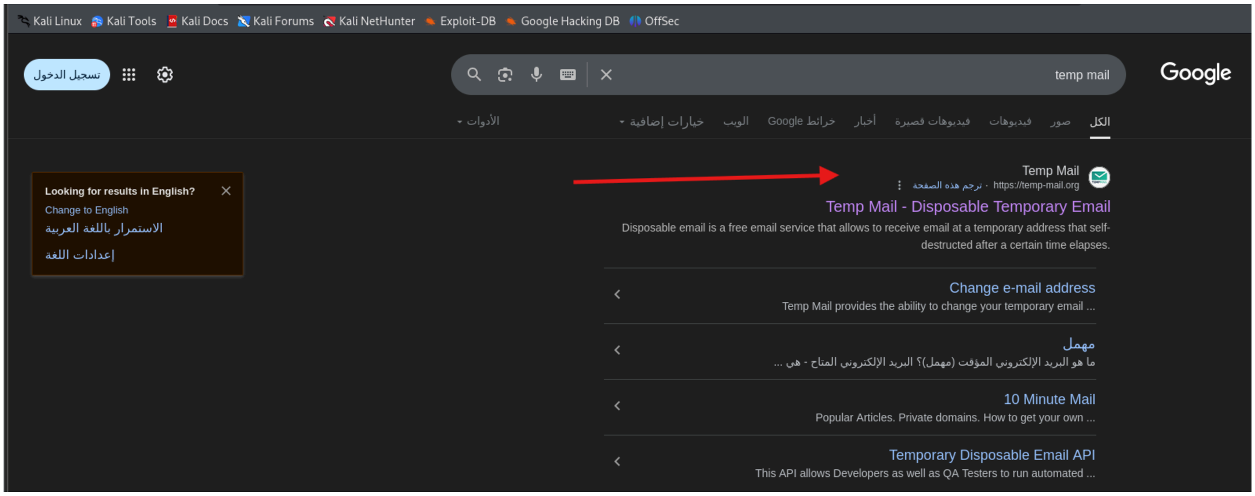
Register for an Activation Code

You are registering for a 1-year Nessus Essentials license.

First Name: kjcdk
Last Name: asjhc
Business Email: yarane9862@balincs.com

□ Check to receive updates from Tenable

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



Looking for results in English?

Change to English

الاستمرار باللغة العربية

إعدادات اللغة

Temp Mail

https://temp-mail.org · ترجم هذه الصفحة

Temp Mail - Disposable Temporary Email

Disposable email is a free email service that allows to receive email at a temporary address that self-destructed after a certain time elapses.

Change e-mail address

Temp Mail provides the ability to change your temporary email ...

مهمل

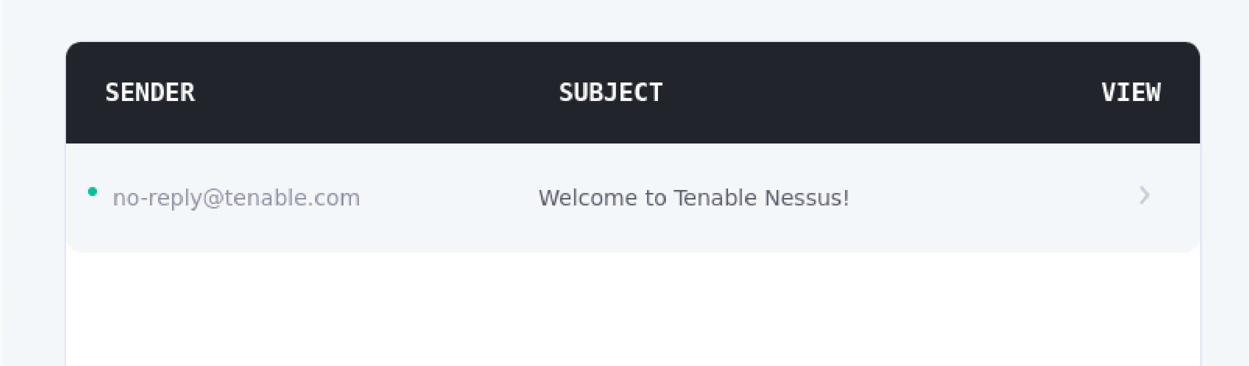
ما هو البريد الإلكتروني المؤقت (مهمل)؟ البريد الإلكتروني المتاح - هي ...

10 Minute Mail

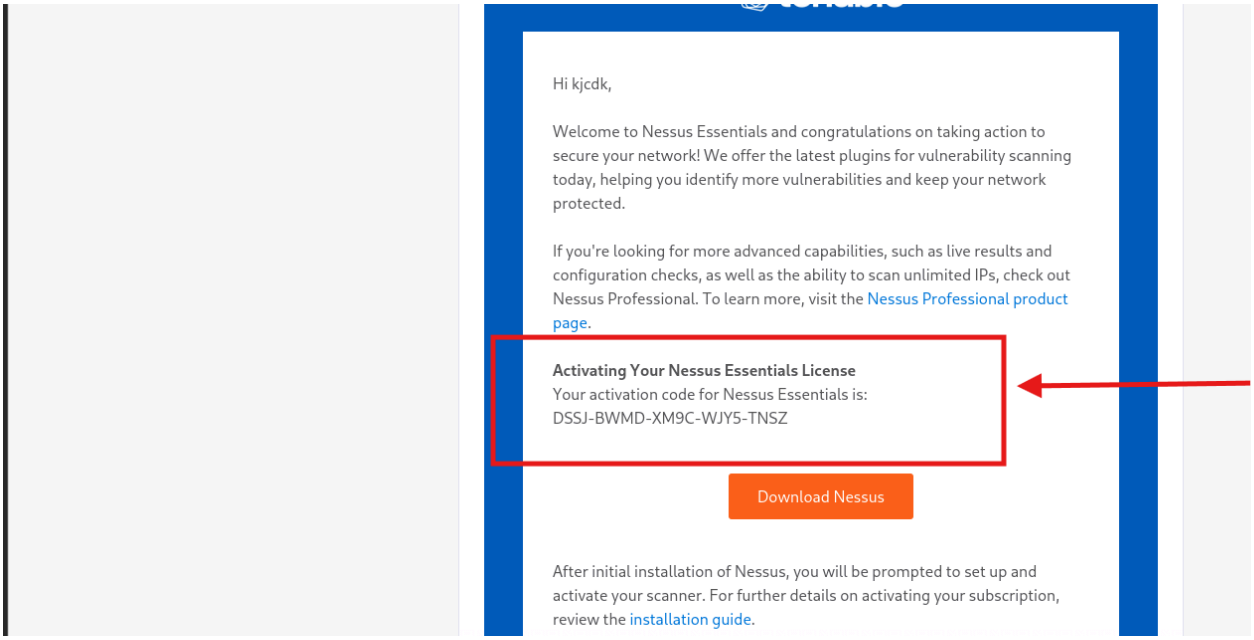
Popular Articles. Private domains. How to get your own ...

Temporary Disposable Email API

This API allows Developers as well as QA Testers to run automated ...



SENDER	SUBJECT	VIEW
● no-reply@tenable.com	Welcome to Tenable Nessus!	›



Hi kjcdk,

Welcome to Nessus Essentials and congratulations on taking action to secure your network! We offer the latest plugins for vulnerability scanning today, helping you identify more vulnerabilities and keep your network protected.

If you're looking for more advanced capabilities, such as live results and configuration checks, as well as the ability to scan unlimited IPs, check out Nessus Professional. To learn more, visit the Nessus Professional product page.

Activating Your Nessus Essentials License

Your activation code for Nessus Essentials is:

DSSJ-BWMD-XM9C-WJY5-TNSZ

After initial installation of Nessus, you will be prompted to set up and activate your scanner. For further details on activating your subscription, review the installation guide.

✅ Step 5: Access the Nessus Web Interface:

Open your browser and go to:

👉 **https://localhost:8834**

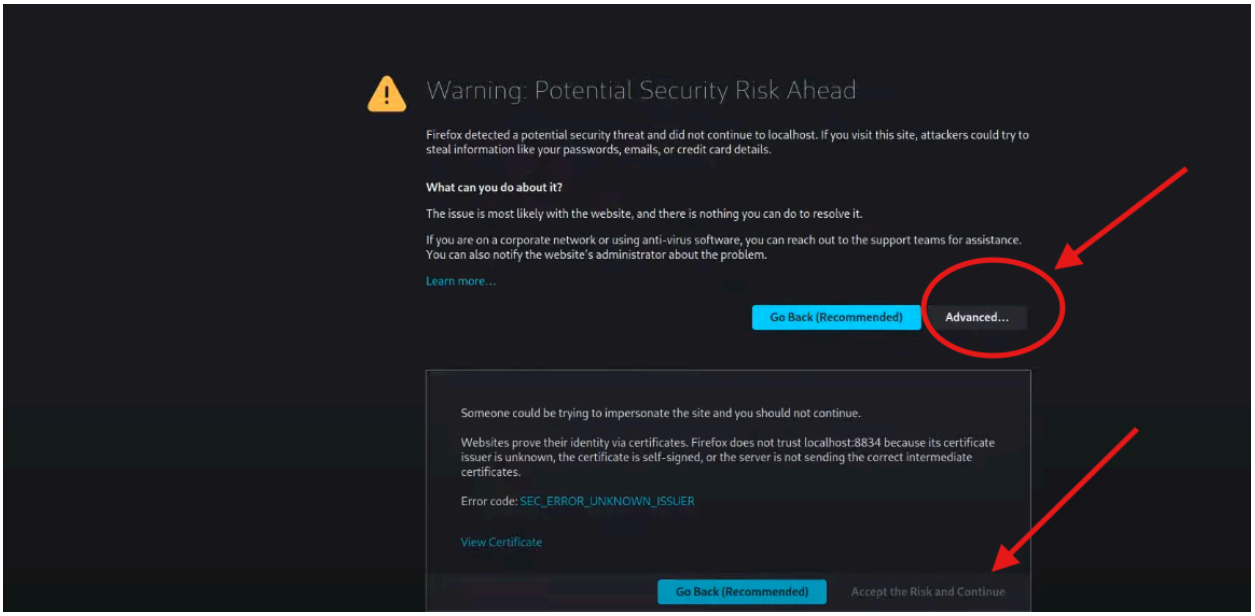
You may get a **warning about SSL**, click **“Advanced”** → **Proceed anyway**.

Choose **Nessus Essentials** as the product.

Enter the **activation code** from earlier.

Create a username and password for your Nessus login.

Nessus will now download and configure necessary plugins — this may take 20–40 minutes. Be patient!



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to localhost. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

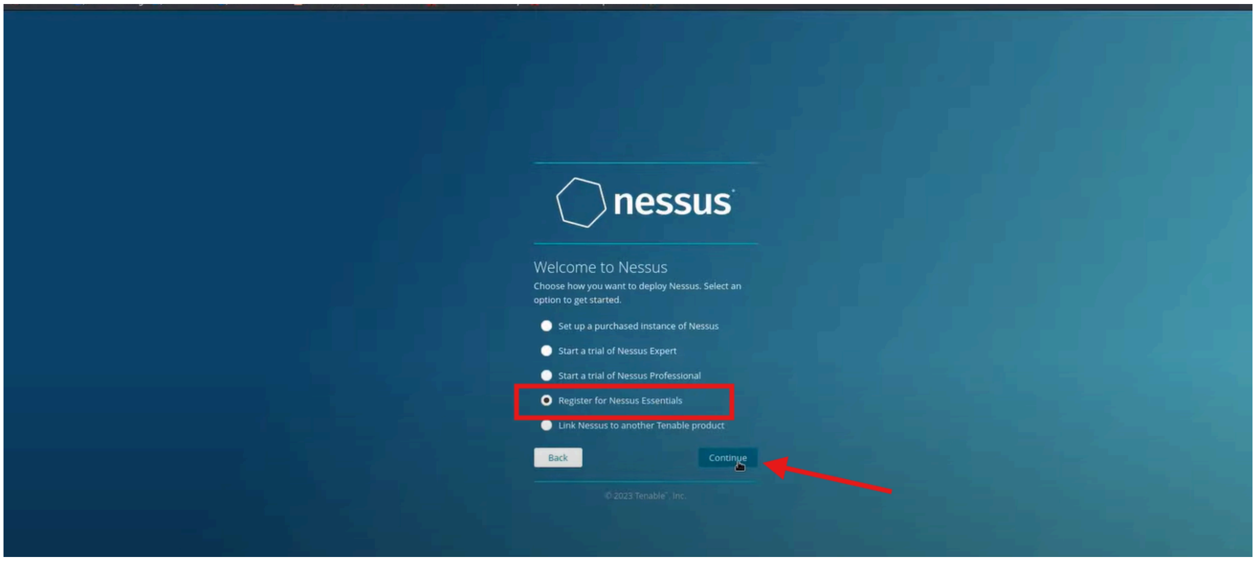
The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust localhost:8834 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

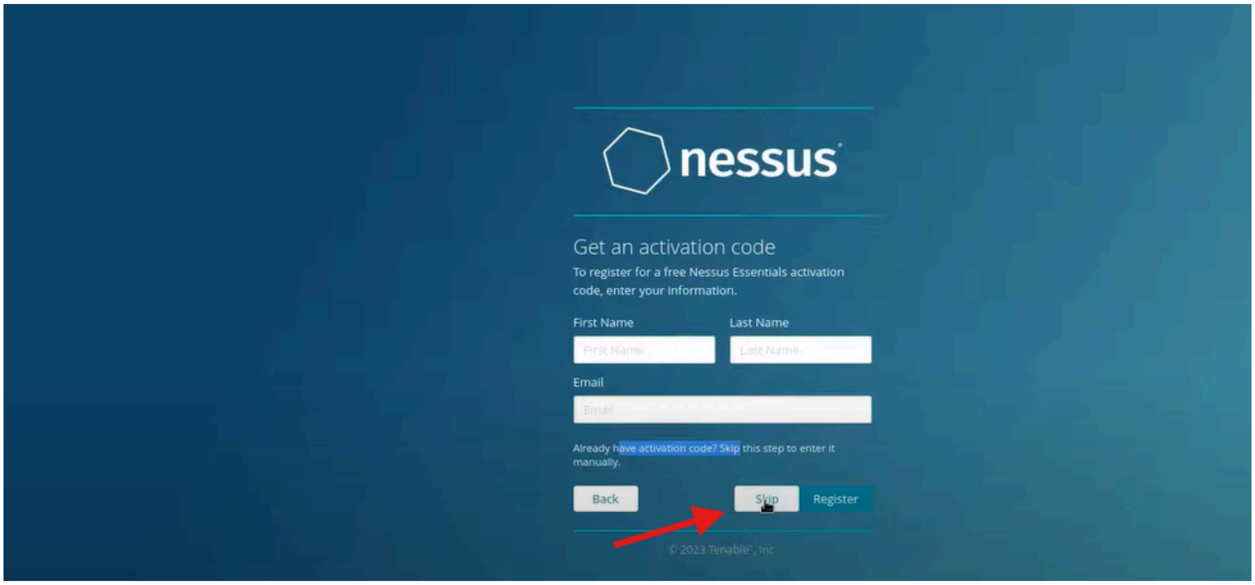
Error code: SEC_ERROR_UNKNOWN_ISSUER



Welcome to Nessus

Choose how you want to deploy Nessus. Select an option to get started.

- ○ Set up a purchased instance of Nessus
- ○ Start a trial of Nessus Expert
- ○ Start a trial of Nessus Professional
- ● Register for Nessus Essentials
- ○ Link Nessus to another Tenable product



Get an activation code

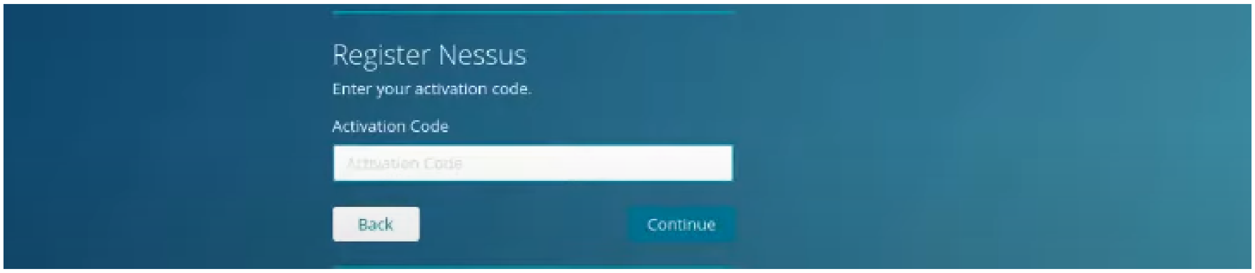
To register for a free Nessus Essentials activation code, enter your information.

First Name: First Name

Last Name: Last Name

Email: Email

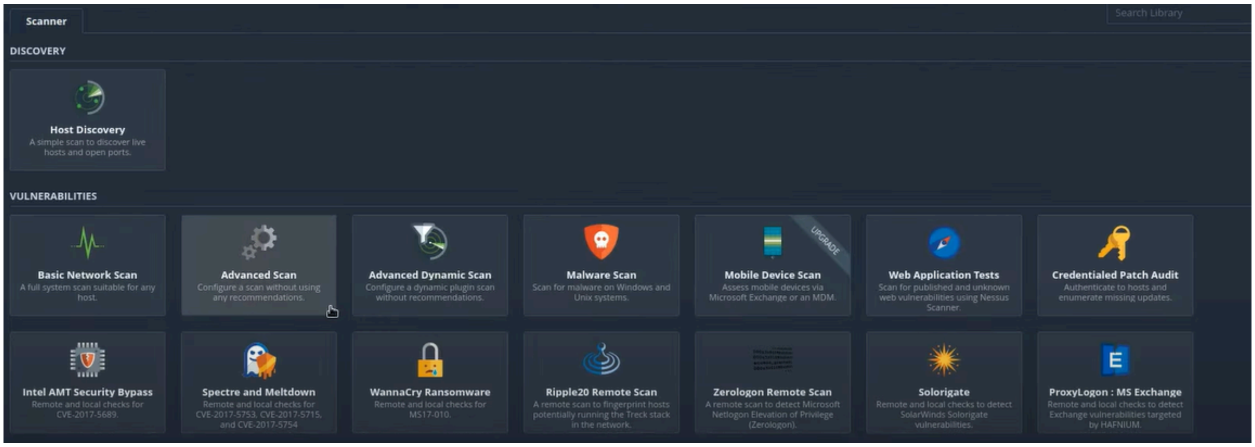
Already have activation code? Skip this step to enter it manually.



Register Nessus

Enter your activation code.

Activation Code: Activation Code



Scanner

Search Library

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.

UPGRADE

Web Application Tests Scan for published and unknown web vulnerabilities using Nessus Scanner.

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.

ProxyLogon : MS Exchange Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.

🎉 Final Step: Start Scanning and Exploiting Metasploitable2

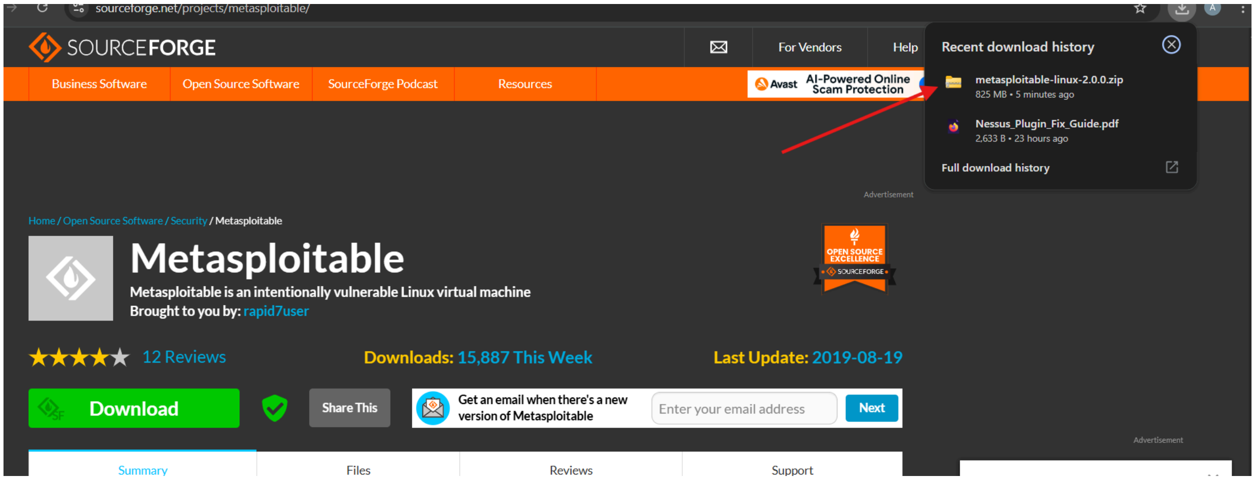
✅ Step 1: Download Metasploitable2:

1-Go to this link to download Metasploitable2:

👉 https://sourceforge.net/projects/metasploitable/

2-After downloading the ZIP file:

- Extract the VM files.
- Open the VM using **VMware** or **VirtualBox**.



sourceforge.net/projects/metasploitable/

SOURCEFORGE

For Vendors Help

Business Software Open Source Software SourceForge Podcast Resources

Avast AI-Powered Online Scam Protection

Recent download history

metasploitable-linux-2.0.0.zip
825 MB • 5 minutes ago

Nessus_Plugin_Fix_Guide.pdf
2,633 B • 23 hours ago

Full download history

Advertisement

Home / Open Source Software / Security / Metasploitable

Metasploitable

Metasploitable is an intentionally vulnerable Linux virtual machine

Brought to you by: rapid7user

OPEN SOURCE EXCELLENCE SOURCEFORGE

★★★★★ 12 Reviews

Downloads: 15,887 This Week

Last Update: 2019-08-19

Download

Share This

Get an email when there's a new version of Metasploitable

Enter your email address

Next

Advertisement

Summary Files Reviews Support

✅ Step 2: Check the Metasploitable2 IP Address:

Login using:

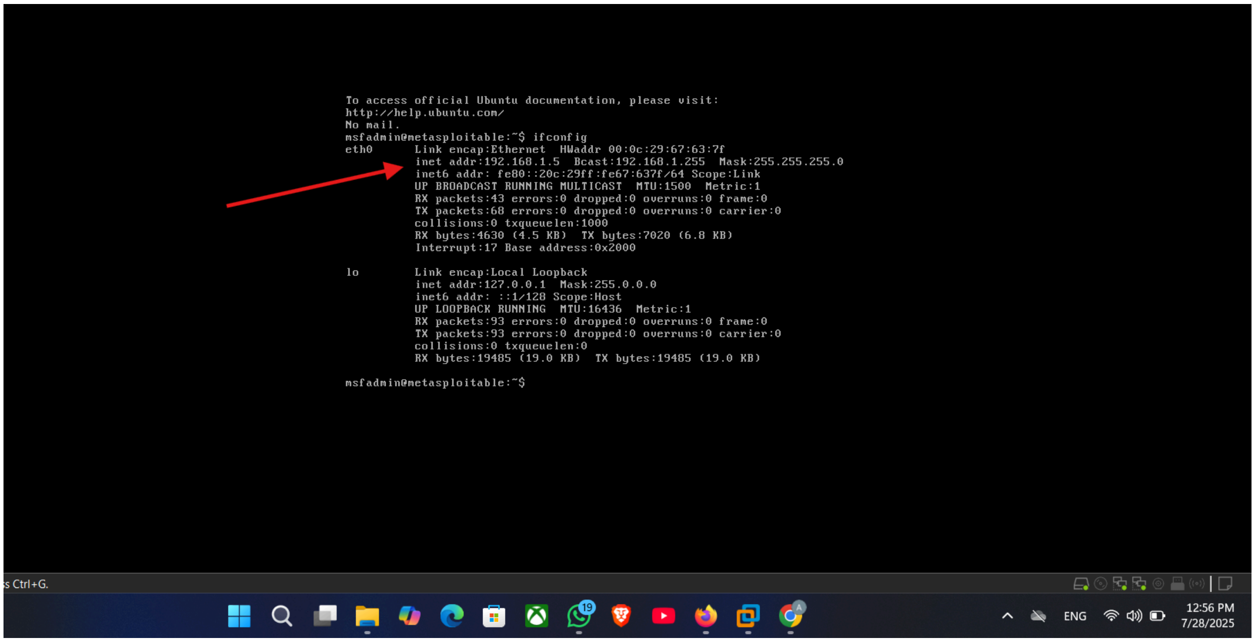
Username: `msfadmin`
Password: `msfadmin`

Run this command to get the IP: 👉 `ifconfig`

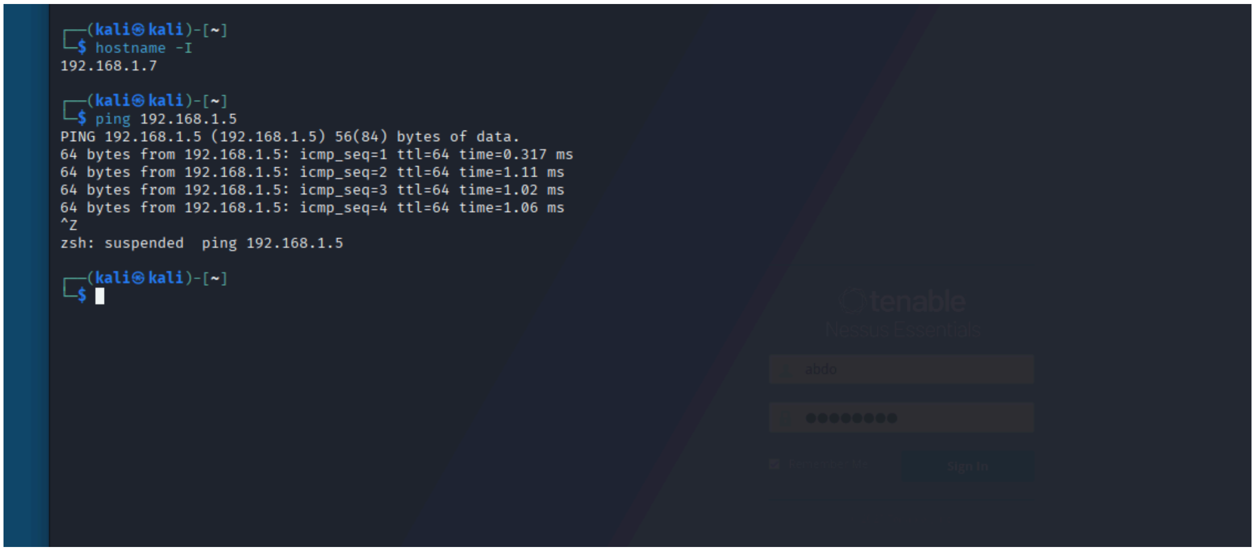
Make sure the **IP address** is in the **same subnet** as your Kali Linux machine (e.g., 192.168.x.x).

From Kali, ping the Metasploitable2 machine to confirm it's reachable:

👉 `ping <target-ip>`



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:67:63:7f
          inet addr:192.168.1.5  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe67:637f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4630 (4.5 KB)  TX bytes:7020 (6.8 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:93 errors:0 dropped:0 overruns:0 frame:0
          TX packets:93 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19485 (19.0 KB)  TX bytes:19485 (19.0 KB)

msfadmin@metasploitable:~$
```



```
┌──(kali㉿kali)-[~]
└─$ hostname -I
192.168.1.7

┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.5
PING 192.168.1.5 (192.168.1.5) 56(84) bytes of data.
64 bytes from 192.168.1.5: icmp_seq=1 ttl=64 time=0.317 ms
64 bytes from 192.168.1.5: icmp_seq=2 ttl=64 time=1.11 ms
64 bytes from 192.168.1.5: icmp_seq=3 ttl=64 time=1.02 ms
64 bytes from 192.168.1.5: icmp_seq=4 ttl=64 time=1.06 ms
^Z
zsh: suspended  ping 192.168.1.5

┌──(kali㉿kali)-[~]
└─$ █
```

✅ Step 3: Start a New Scan:

1- Choose Basic Network Scan

2- Set the Target IP to the IP of the Metasploitable2 machine

Under **Credentials**:

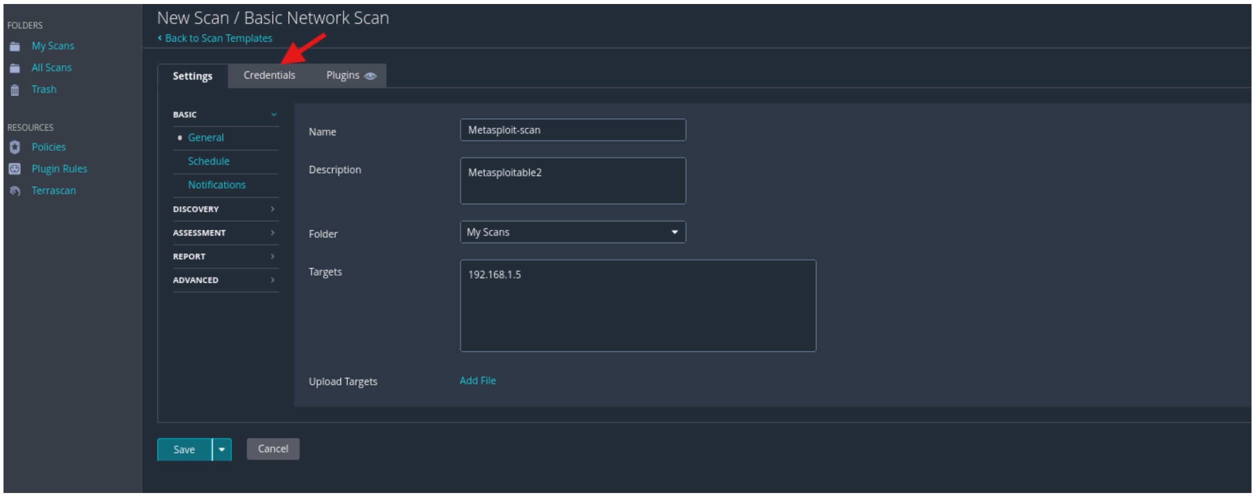
👉 Choose **SSH**

Enter:

👉 **Username:** `msfadmin`

👉 **Password:** `msfadmin`

Click **Save**, then **Launch the scan**.



New Scan / Basic Network Scan

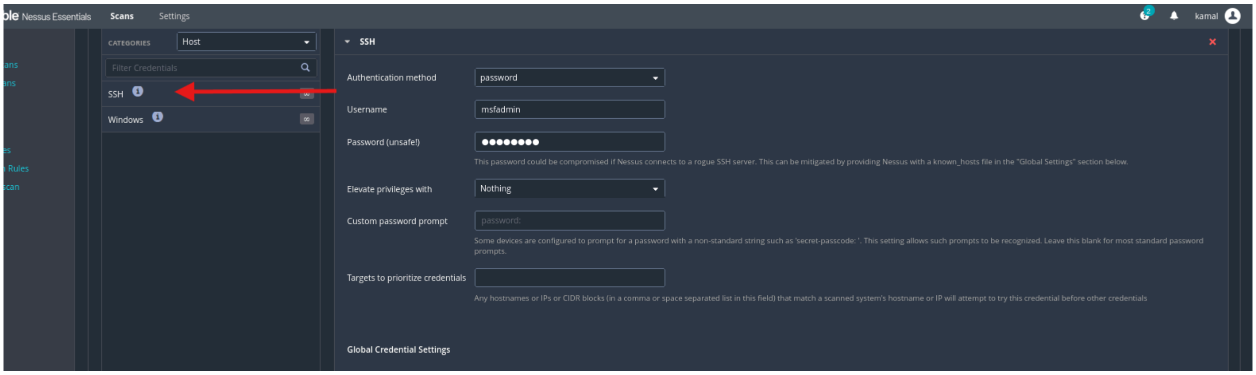
Name: Metasploit-scan

Description: Metasploitable2

Folder: My Scans

Targets: 192.168.1.5

Upload Targets: Add File



SSH

Authentication method: password

Username: msfadmin

Password (unsafe!): ●●●●●●●●

This password could be compromised if Nessus connects to a rogue SSH server. This can be mitigated by providing Nessus with a known_hosts file in the "Global Settings" section below.

Elevate privileges with: Nothing

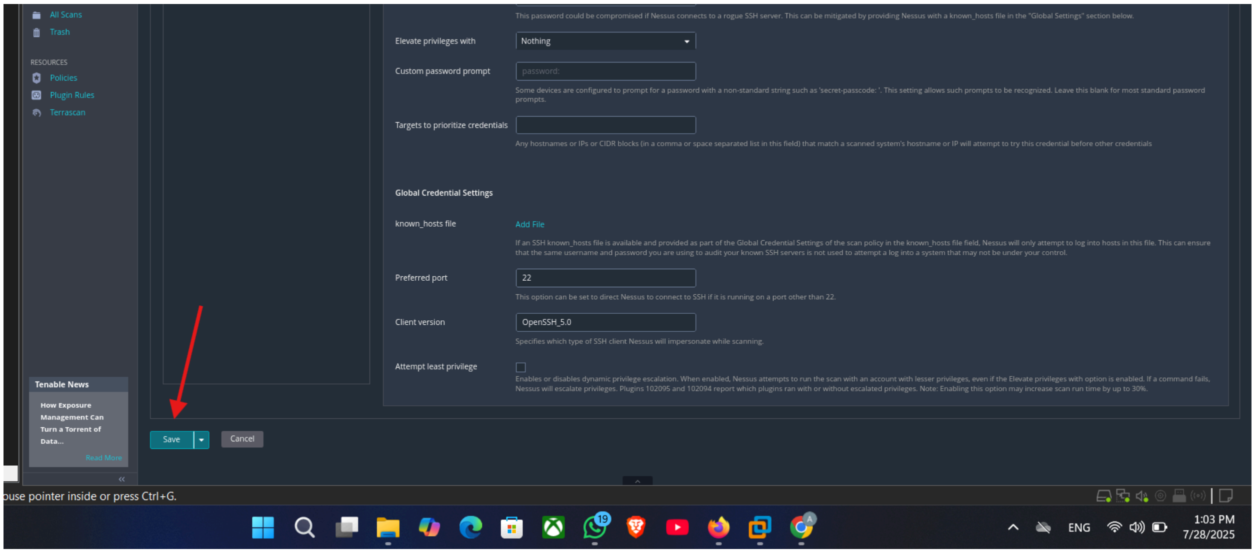
Custom password prompt: password:

Some devices are configured to prompt for a password with a non-standard string such as 'secret-passcode: '. This setting allows such prompts to be recognized. Leave this blank for most standard password prompts.

Targets to prioritize credentials:

Any hostnames or IPs or CIDR blocks (in a comma or space separated list in this field) that match a scanned system's hostname or IP will attempt to try this credential before other credentials

Global Credential Settings



This password could be compromised if Nessus connects to a rogue SSH server. This can be mitigated by providing Nessus with a known_hosts file in the "Global Settings" section below.

Elevate privileges with: Nothing

Custom password prompt: password:

Some devices are configured to prompt for a password with a non-standard string such as 'secret-passcode: '. This setting allows such prompts to be recognized. Leave this blank for most standard password prompts.

Targets to prioritize credentials:

Any hostnames or IPs or CIDR blocks (in a comma or space separated list in this field) that match a scanned system's hostname or IP will attempt to try this credential before other credentials

Global Credential Settings

known_hosts file: Add File

If an SSH known_hosts file is available and provided as part of the Global Credential Settings of the scan policy in the known_hosts file field, Nessus will only attempt to log into hosts in this file. This can ensure that the same username and password you are using to audit your known SSH servers is not used to attempt a log into a system that may not be under your control.

Preferred port: 22

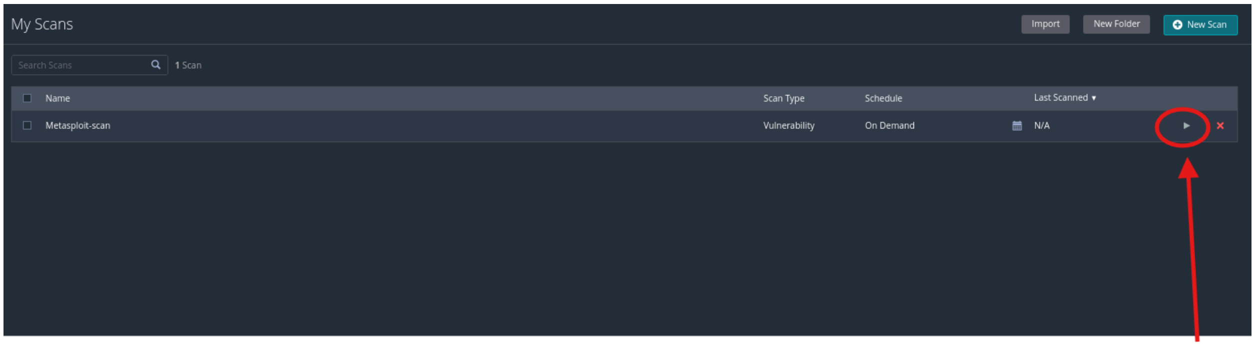
This option can be set to direct Nessus to connect to SSH if it is running on a port other than 22.

Client version: OpenSSH_5.0

Specifies which type of SSH client Nessus will impersonate while scanning.

Attempt least privilege: □

Enables or disables dynamic privilege escalation. When enabled, Nessus attempts to run the scan with an account with lesser privileges, even if the Elevate privileges with option is enabled. If a command fails, Nessus will escalate privileges. Plugins 102095 and 102094 report which plugins ran with or without escalated privileges. Note: Enabling this option may increase scan run time by up to 30%.



My Scans

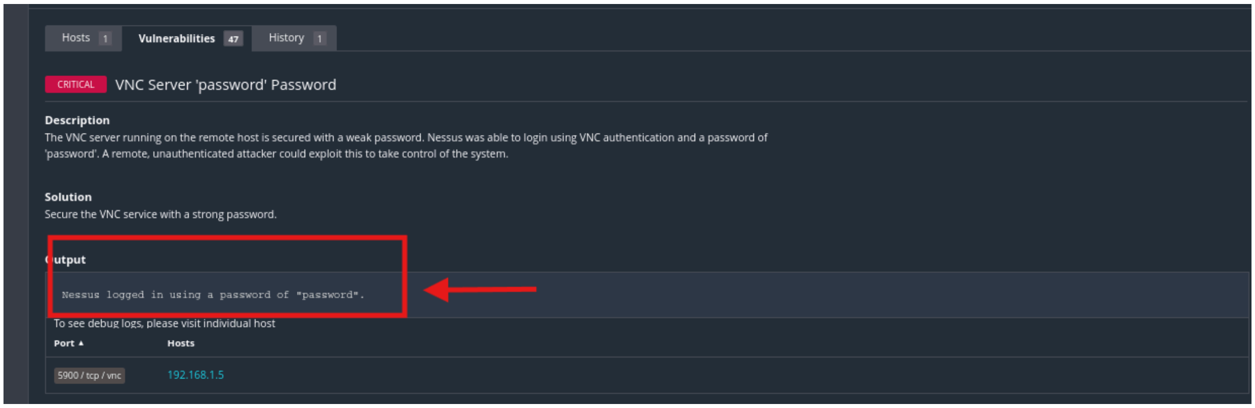
1 Scan

☐	Name	Scan Type	Schedule	Last Scanned ▾
☐	Metasploit-scan	Vulnerability	On Demand	N/A

✅ Step 4: Identify the Critical Vulnerability:

Once the scan finishes, Nessus will list vulnerabilities.

The VNC server has a weak or default password. **Password:** `password` .



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".
```

To see debug logs, please visit individual host

Port ▲	Hosts
5900 / tcp / vnc	192.168.1.5

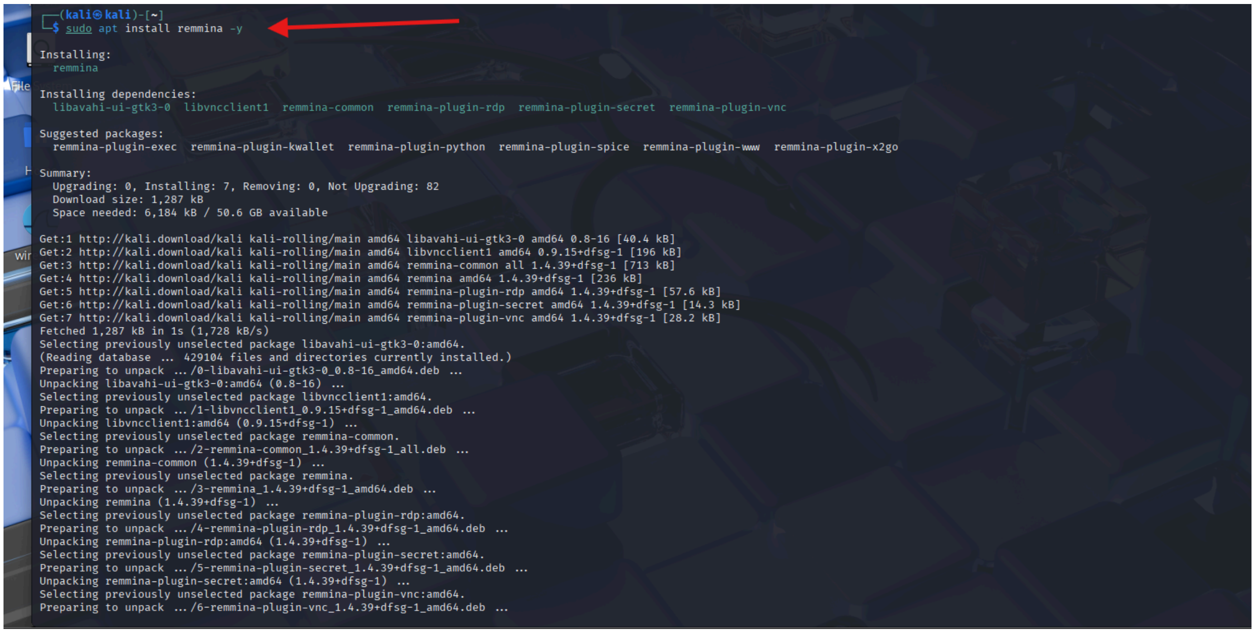
✅ Step 5: Exploit the VNC Vulnerability Using Remmina:

Step A: Install Remmina (if not already installed)

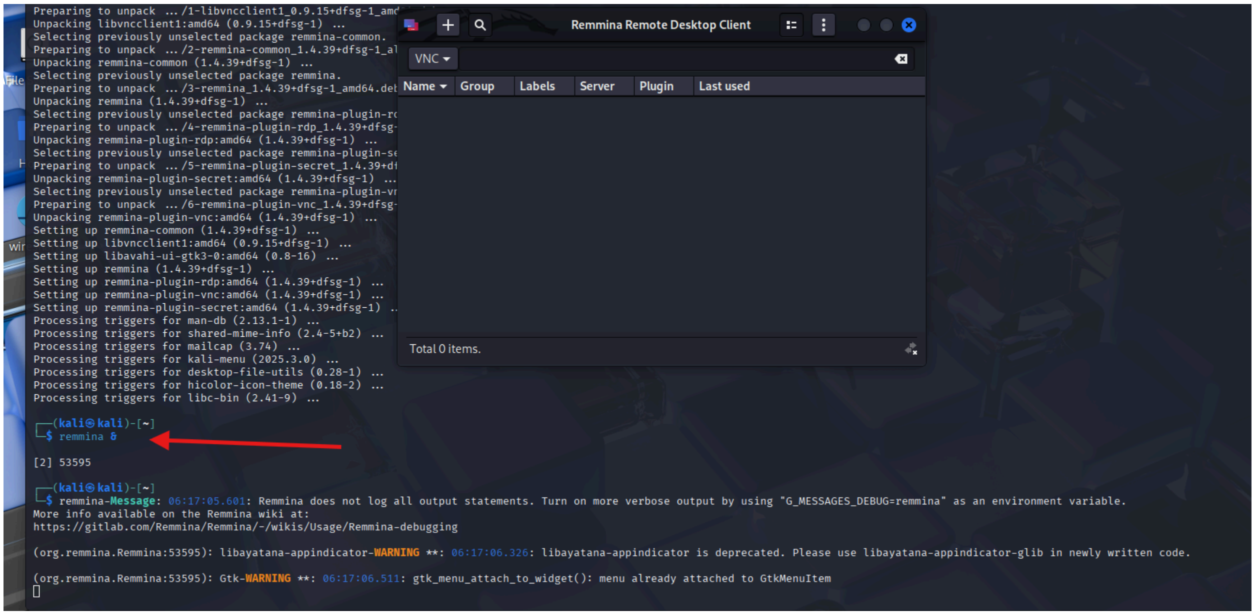
👉 **sudo apt install remmina -y**

Step B: Launch Remmina:

👉 remmina &



```
┌──(kali㉿kali)-[~]
└─$ sudo apt install remmina -y

Installing:
  remmina

Installing dependencies:
  libavahi-ui-gtk3-0  libvncclient1  remmina-common  remmina-plugin-rdp  remmina-plugin-secret  remmina-plugin-vnc

Suggested packages:
  remmina-plugin-exec  remmina-plugin-kwallet  remmina-plugin-python  remmina-plugin-spice  remmina-plugin-www  remmina-plugin-x2go

Summary:
  Upgrading: 0, Installing: 7, Removing: 0, Not Upgrading: 82
  Download size: 1,287 kB
  Space needed: 6,184 kB / 50.6 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 libavahi-ui-gtk3-0 amd64 0.8-16 [40.4 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libvncclient1 amd64 0.9.15+dfsg-1 [196 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 remmina-common all 1.4.39+dfsg-1 [713 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 remmina amd64 1.4.39+dfsg-1 [236 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 remmina-plugin-rdp amd64 1.4.39+dfsg-1 [57.6 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 remmina-plugin-secret amd64 1.4.39+dfsg-1 [14.3 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 remmina-plugin-vnc amd64 1.4.39+dfsg-1 [28.2 kB]
Fetched 1,287 kB in 1s (1,728 kB/s)
Selecting previously unselected package libavahi-ui-gtk3-0:amd64.
(Reading database ... 429104 files and directories currently installed.)
Preparing to unpack .../0-libavahi-ui-gtk3-0_0.8-16_amd64.deb ...
Unpacking libavahi-ui-gtk3-0:amd64 (0.8-16) ...
Selecting previously unselected package libvncclient1:amd64.
Preparing to unpack .../1-libvncclient1_0.9.15+dfsg-1_amd64.deb ...
Unpacking libvncclient1:amd64 (0.9.15+dfsg-1) ...
Selecting previously unselected package remmina-common.
Preparing to unpack .../2-remmina-common_1.4.39+dfsg-1_all.deb ...
Unpacking remmina-common (1.4.39+dfsg-1) ...
Selecting previously unselected package remmina.
Preparing to unpack .../3-remmina_1.4.39+dfsg-1_amd64.deb ...
Unpacking remmina (1.4.39+dfsg-1) ...
Selecting previously unselected package remmina-plugin-rdp:amd64.
Preparing to unpack .../4-remmina-plugin-rdp_1.4.39+dfsg-1_amd64.deb ...
Unpacking remmina-plugin-rdp:amd64 (1.4.39+dfsg-1) ...
Selecting previously unselected package remmina-plugin-secret:amd64.
Preparing to unpack .../5-remmina-plugin-secret_1.4.39+dfsg-1_amd64.deb ...
Unpacking remmina-plugin-secret:amd64 (1.4.39+dfsg-1) ...
Selecting previously unselected package remmina-plugin-vnc:amd64.
Preparing to unpack .../6-remmina-plugin-vnc_1.4.39+dfsg-1_amd64.deb ...
```

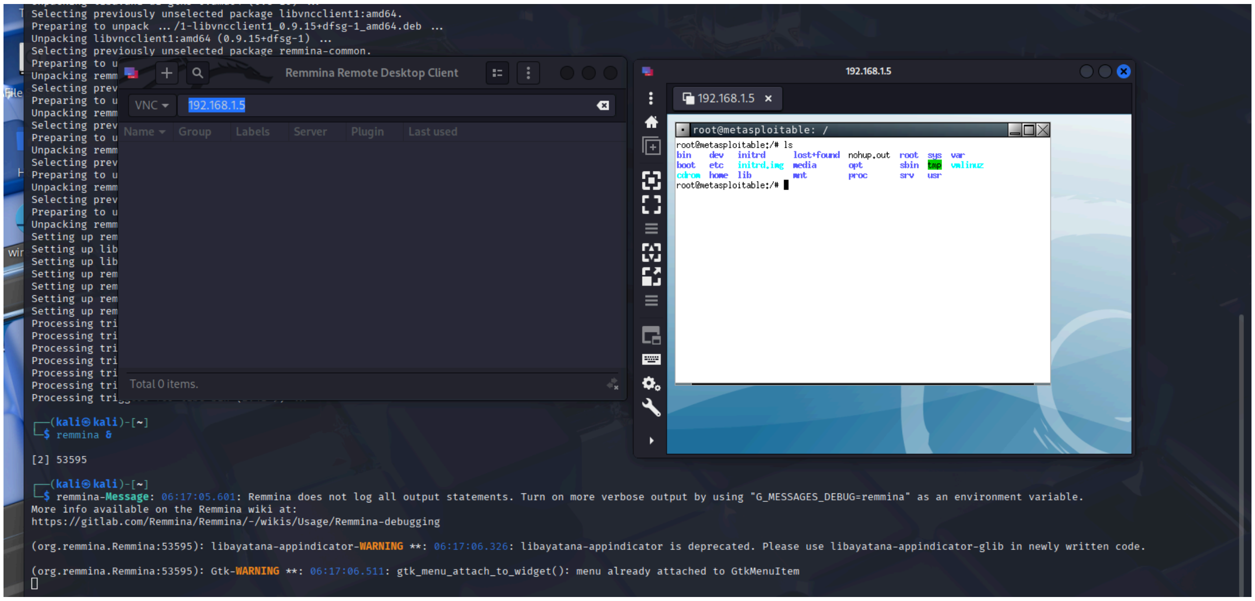


```
Preparing to unpack .../1-libvncclient1_0.9.15+dfsg-1_amd
Unpacking libvncclient1:amd64 (0.9.15+dfsg-1) ...
Selecting previously unselected package remmina-common.
Preparing to unpack .../2-remmina-common_1.4.39+dfsg-1_al
Unpacking remmina-common (1.4.39+dfsg-1) ...
Selecting previously unselected package remmina.
Preparing to unpack .../3-remmina_1.4.39+dfsg-1_amd64.deb
Unpacking remmina (1.4.39+dfsg-1) ...
Selecting previously unselected package remmina-plugin-rc
Preparing to unpack .../4-remmina-plugin-rdp_1.4.39+dfsg-
Unpacking remmina-plugin-rdp:amd64 (1.4.39+dfsg-1) ...
Selecting previously unselected package remmina-plugin-se
Preparing to unpack .../5-remmina-plugin-secret_1.4.39+df
Unpacking remmina-plugin-secret:amd64 (1.4.39+dfsg-1) ...
Selecting previously unselected package remmina-plugin-vr
Preparing to unpack .../6-remmina-plugin-vnc_1.4.39+dfsg-
Unpacking remmina-plugin-vnc:amd64 (1.4.39+dfsg-1) ...
Setting up remmina-common (1.4.39+dfsg-1) ...
Setting up libvncclient1:amd64 (0.9.15+dfsg-1) ...
Setting up libavahi-ui-gtk3-0:amd64 (0.8-16) ...
Setting up remmina (1.4.39+dfsg-1) ...
Setting up remmina-plugin-rdp:amd64 (1.4.39+dfsg-1) ...
Setting up remmina-plugin-vnc:amd64 (1.4.39+dfsg-1) ...
Setting up remmina-plugin-secret:amd64 (1.4.39+dfsg-1) .
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for shared-mime-info (2.4-5+b2) ...
Processing triggers for mailcap (3.74) ...
Processing triggers for kali-menu (2025.3.0) ...
Processing triggers for desktop-file-utils (0.28-1) ...
Processing triggers for hicolor-icon-theme (0.18-2) ...
Processing triggers for libc-bin (2.41-9) ...

┌──(kali㉿kali)-[~]
└─$ remmina &

[2] 53595

┌──(kali㉿kali)-[~]
└─$ remmina-Message: 06:17:05.601: Remmina does not log all output statements. Turn on more verbose output by using "G_MESSAGES_DEBUG=remmina" as an environment variable.
More info available on the Remmina wiki at:
https://gitlab.com/Remmina/Remmina/-/wikis/Usage/Remmina-debugging

(org.remmina.Remmina:53595): libayatana-appindicator-WARNING **: 06:17:06.326: libayatana-appindicator is deprecated. Please use libayatana-appindicator-glib in newly written code.

(org.remmina.Remmina:53595): Gtk-WARNING **: 06:17:06.511: gtk_menu_attach_to_widget(): menu already attached to GtkMenuItem
```

Step C: Connect to the Vulnerable VNC Server (Metasploitable2)

In Remmina:

👉 **Protocol:** VNC 👉 **Server/IP:** Use the Metasploitable2 IP 👉 **Password:** `password`



```
Selecting previously unselected package libvncclient1:amd64.
Preparing to unpack .../1-libvncclient1_0.9.15+dfsg-1_amd64.deb ...
Unpacking libvncclient1:amd64 (0.9.15+dfsg-1) ...
Selecting previously unselected package remmina-common.
Preparing to u
Unpacking remm
Selecting prev
Preparing to u
Unpacking remm
Selecting prev
Preparing to u
Unpacking remm
Selecting prev
Preparing to u
Unpacking remm
Selecting prev
Preparing to u
Unpacking remm
Setting up rem
Setting up lib
Setting up lib
Setting up rem
Setting up rem
Setting up rem
Setting up rem
Processing tri
Processing tri
Processing tri
Processing tri
Processing tri
Processing tri
Processing tri

┌──(kali㉿kali)-[~]
└─$ remmina &

[2] 53595

┌──(kali㉿kali)-[~]
└─$ remmina-Message: 06:17:05.601: Remmina does not log all output statements. Turn on more verbose output by using "G_MESSAGES_DEBUG=remmina" as an environment variable.
More info available on the Remmina wiki at:
https://gitlab.com/Remmina/Remmina/-/wikis/Usage/Remmina-debugging

(org.remmina.Remmina:53595): libayatana-appindicator-WARNING **: 06:17:06.326: libayatana-appindicator is deprecated. Please use libayatana-appindicator-glib in newly written code.

(org.remmina.Remmina:53595): Gtk-WARNING **: 06:17:06.511: gtk_menu_attach_to_widget(): menu already attached to GtkMenuItem
```

```
root@metasploitable: /
root@metasploitable:/# ls
bin     dev   initrd      lost+found  nohup.out  root  sys  var
boot    etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom   home  lib         mnt         proc       srv   usr
root@metasploitable:/# 
```

🎯 Task Complete!