EDUNET FOUNDATION-Class Exercise

LAB 1- Vulnerability detection in Raspberry-PI via IP address

1. Understanding Vulnerability

In the realm of cybersecurity, a vulnerability refers to a weakness or flaw in a system, network, software, or application that can be exploited by cyber attackers to compromise the confidentiality, integrity, or availability of data or resources. Vulnerabilities can exist in various forms and may arise due to design flaws, incorrect configurations, software bugs, or lack of security controls. Here's a detailed explanation of vulnerabilities:

Types of Vulnerabilities:

- **Software Vulnerabilities:** These vulnerabilities exist in software applications or operating systems and can range from coding errors to misconfigurations that could be exploited by attackers.
- **Hardware Vulnerabilities:** Weaknesses present in hardware components, such as microprocessors or networking devices, that can be targeted for exploitation.
- **Human Factor:** Vulnerabilities can also stem from human actions, such as weak passwords, social engineering attacks, or lack of security awareness.

Common Examples:

- **Buffer Overflow:** A common software vulnerability where an application writes more data to a buffer than it can hold, potentially allowing attackers to execute malicious code.
- **SQL Injection:** Occurs when attackers inject malicious SQL queries into input fields, exploiting vulnerabilities in web applications to access or manipulate databases.
- **Cross-Site Scripting (XSS):** Allows attackers to inject malicious scripts into web pages viewed by other users, compromising their data or session information.

Impact of Vulnerabilities:

- **Data Breaches:** Exploiting vulnerabilities can lead to unauthorized access to sensitive data like user credentials, financial information, or intellectual property.
- **Service Disruption:** Attackers can leverage vulnerabilities to disrupt services or systems, causing downtime and operational disruptions.
- **Financial Loss**: Organizations can face financial repercussions due to the costs associated with addressing security incidents, legal implications, and damage to reputation.

Mitigation Strategies:

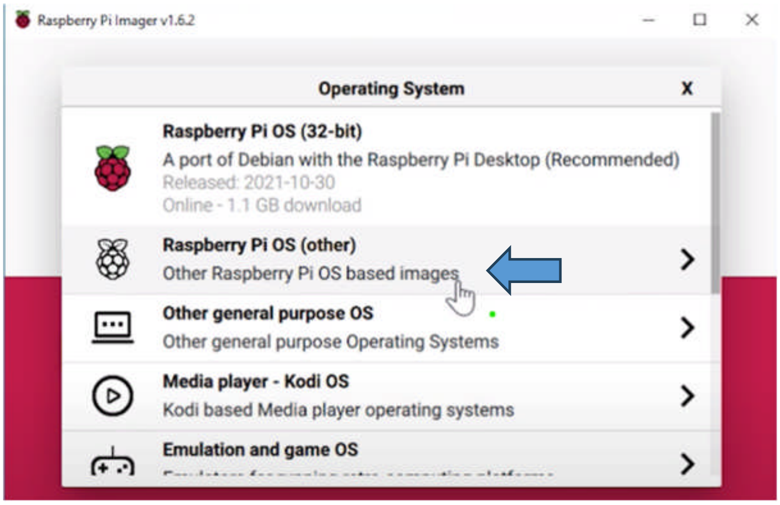
- **Patch Management**: Regularly applying security patches and updates to software and systems to address known vulnerabilities.
- **Vulnerability Scanning**: Conducting regular vulnerability assessments and scans to identify and remediate security weaknesses proactively.
- **Secure Coding Practices**: Implementing secure coding guidelines and best practices to reduce the likelihood of introducing vulnerabilities during the development process.

Note: Understanding vulnerabilities is essential for organizations and individuals alike to proactively address security risks and strengthen their cybersecurity posture against potential threats.

Disclaimer: The content is curated for educational purposes only.

Let’s Look how to find the vulnerability in anyone’s network through IP-addresses:

Step-1



Raspberry Pi Imager v1.6.2

Operating System

Raspberry Pi OS (32-bit)
A port of Debian with the Raspberry Pi Desktop (Recommended)
Released: 2021-10-30
Online - 1.1 GB download

Raspberry Pi OS (other)
Other Raspberry Pi OS based images

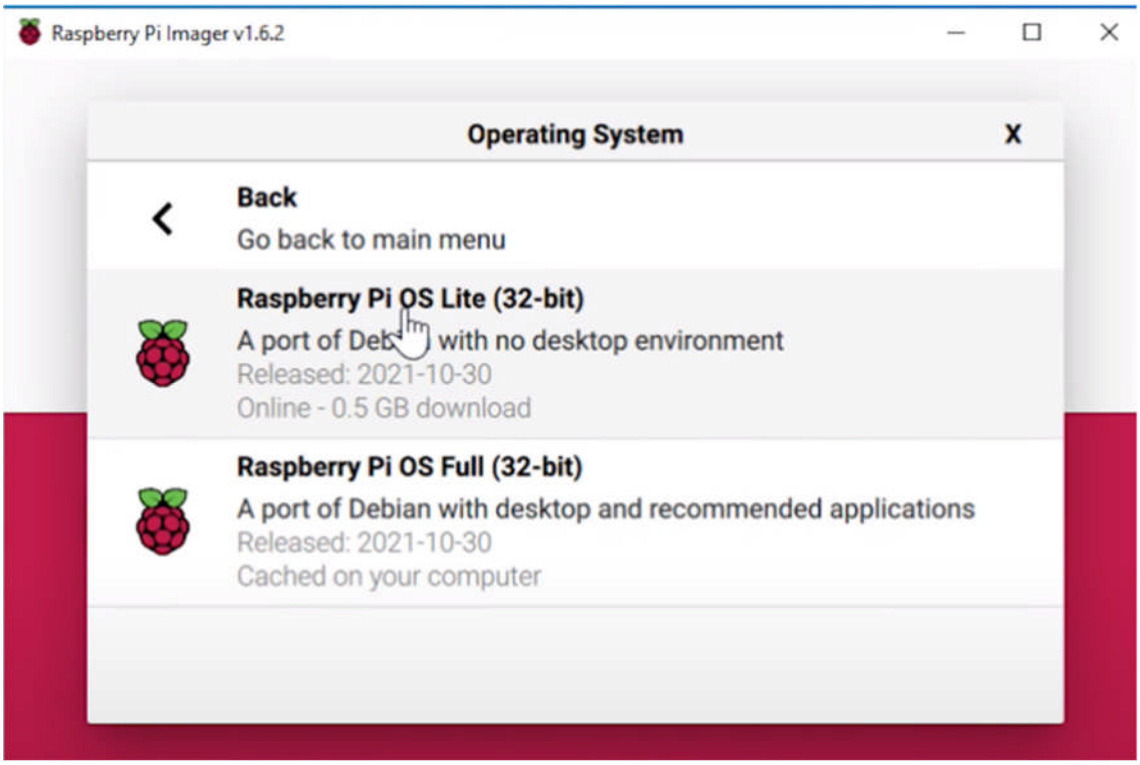
Other general purpose OS
Other general purpose Operating Systems

Media player - Kodi OS
Kodi based Media player operating systems

Emulation and game OS

Step-2

Click on OS Lite(32-bit) A port of Debian with no desktop environment



Raspberry Pi Imager v1.6.2

Operating System

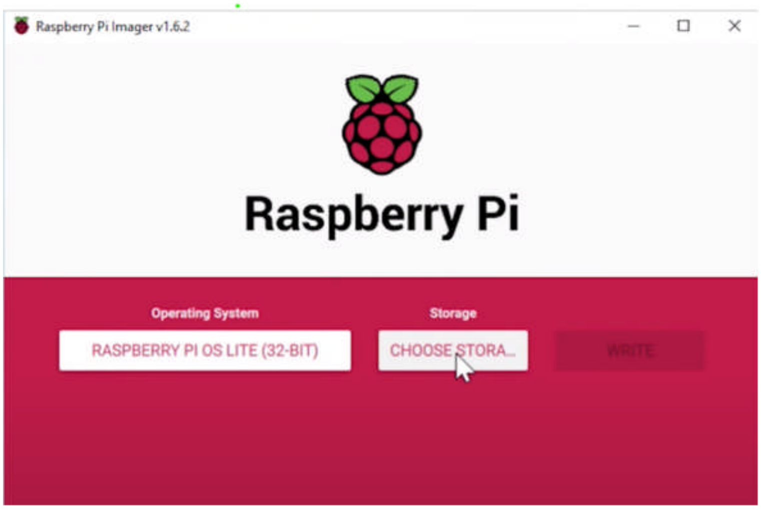
Back
Go back to main menu

Raspberry Pi OS Lite (32-bit)
A port of Debian with no desktop environment
Released: 2021-10-30
Online - 0.5 GB download

Raspberry Pi OS Full (32-bit)
A port of Debian with desktop and recommended applications
Released: 2021-10-30
Cached on your computer

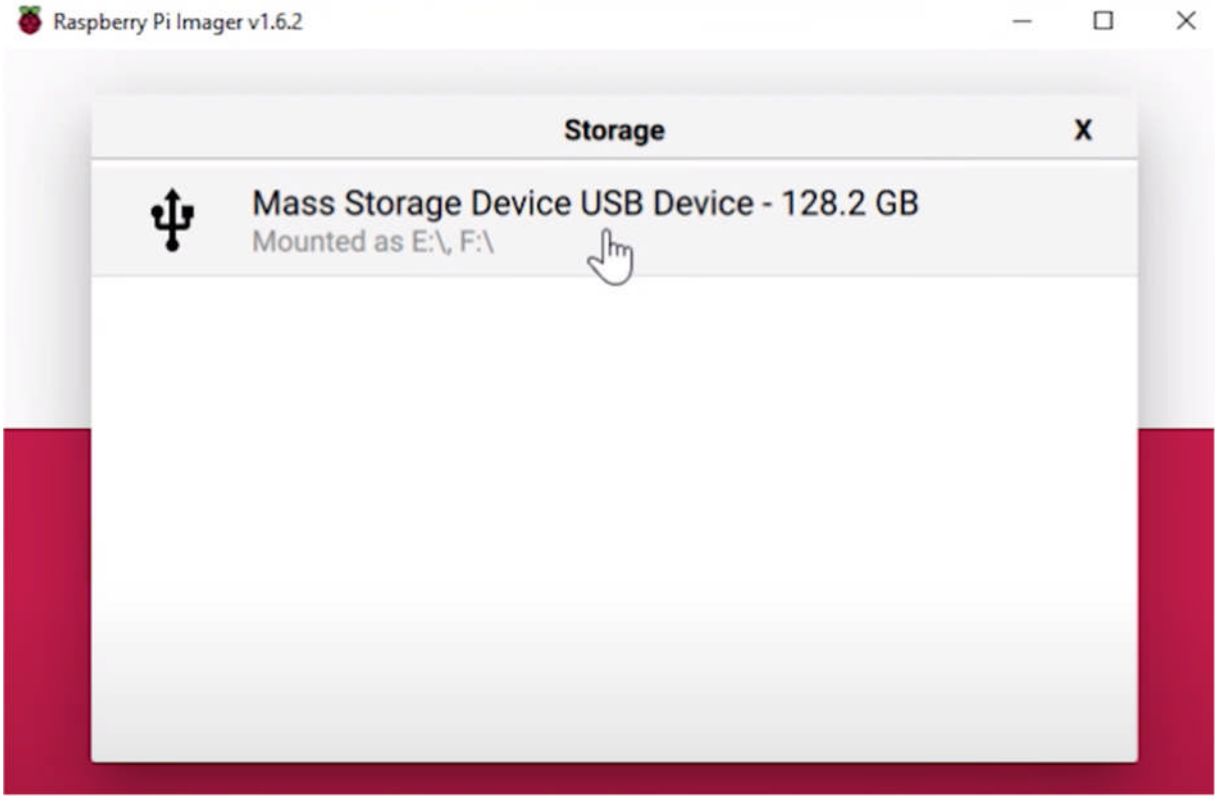
Step-3:

Click on choose storage



Step-4

click on USB Device

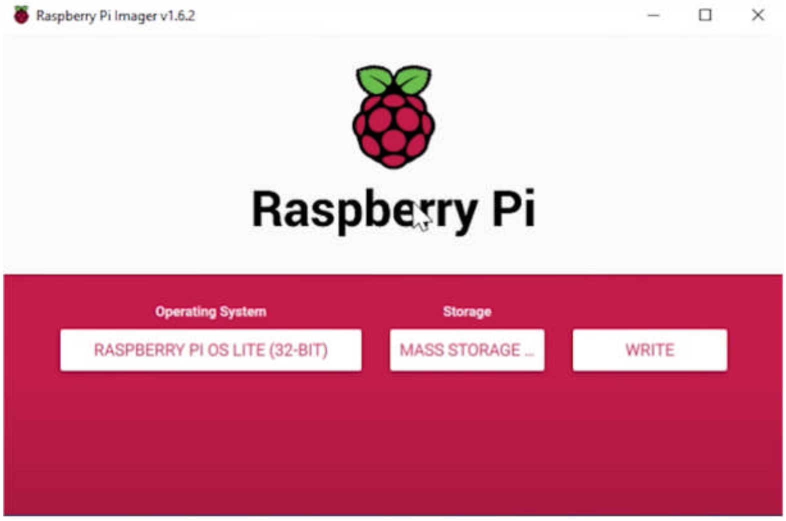


Mass Storage Device USB Device - 128.2 GB
Mounted as E:\, F:\

Step-5

Most important: “Do not click” Anywhere

- Now Press “**cntrl + shift + x**”

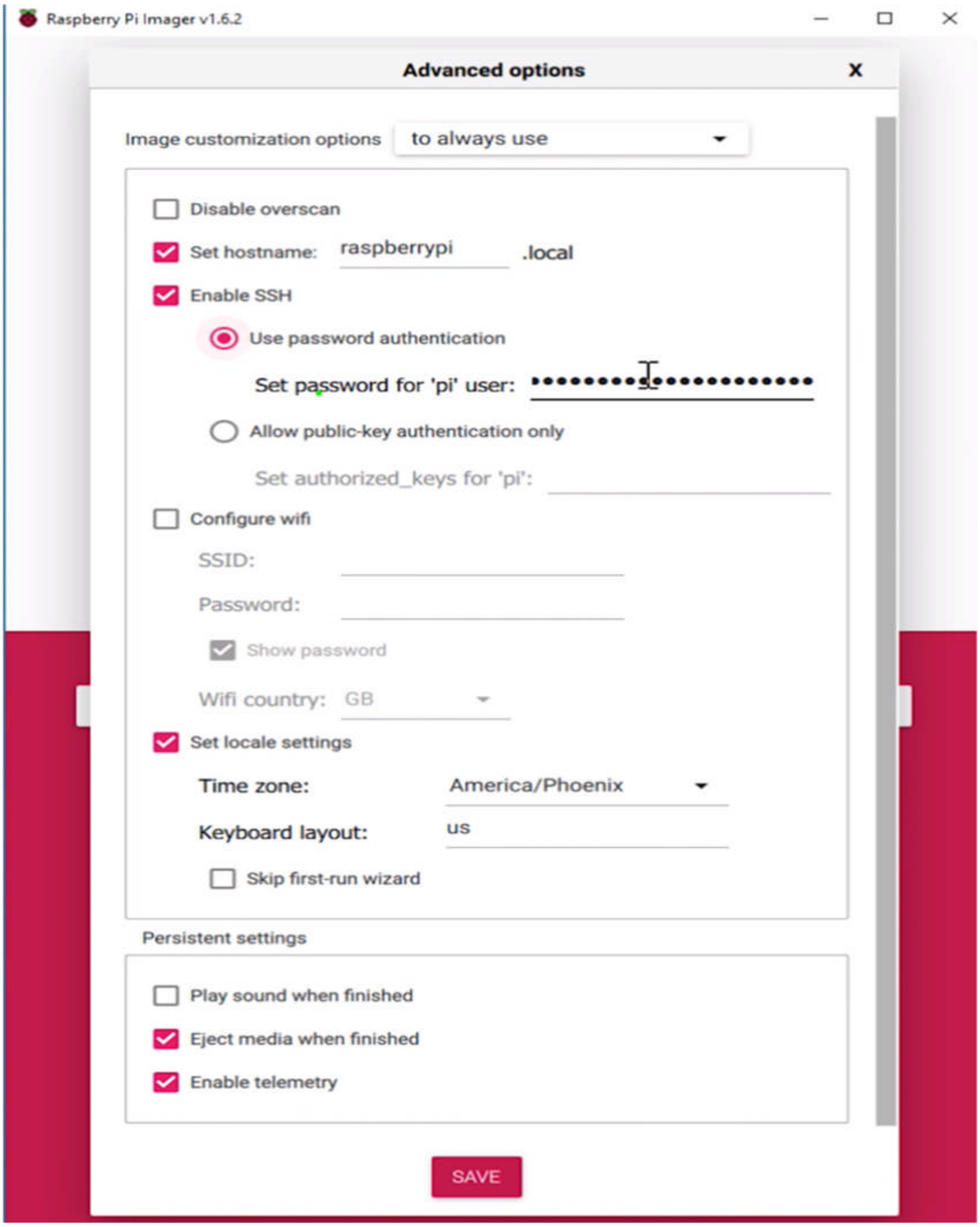


Step-6

Then advanced option window will pop up, where you can see many options out of which we have to remember hostname and password

1. Set hostname: raspberrypi
2. Set Password: pi
3. Others Set as follows(like checkbox)
4. Click **Save**

Disclaimer: The content is curated for educational purposes only.



Advanced options

Image customization options: to always use

- □ Disable overscan
- ☑ Set hostname: raspberrypi .local
- ☑ Enable SSH
  - ● Use password authentication
    - Set password for 'pi' user: ••••••••••••••••••••••
  - ○ Allow public-key authentication only
    - Set authorized_keys for 'pi':
- □ Configure wifi
  - SSID:
  - Password:
  - ☑ Show password
  - Wifi country: GB
- ☑ Set locale settings
  - Time zone: America/Phoenix
  - Keyboard layout: us
  - □ Skip first-run wizard

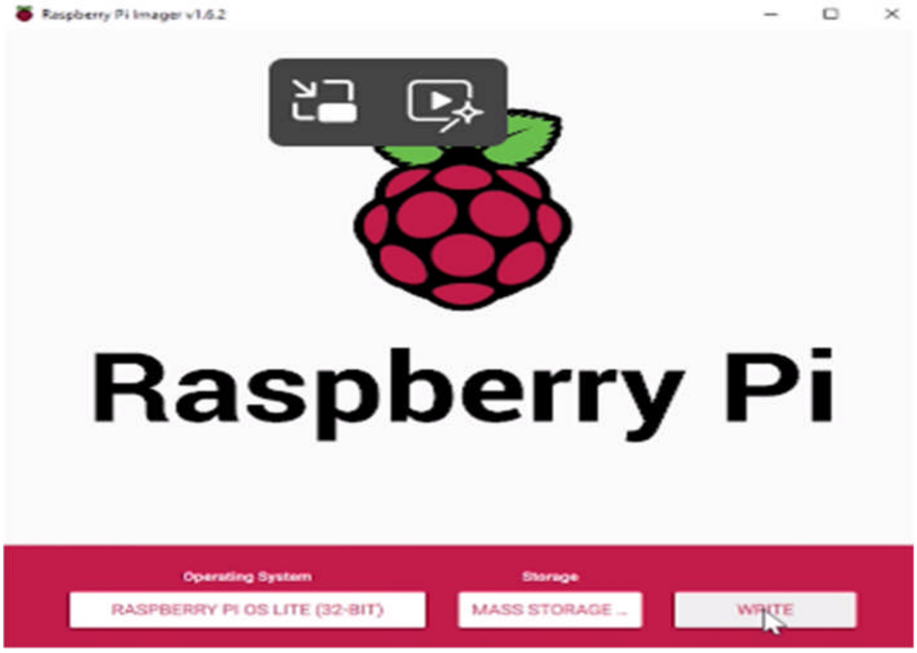
Persistent settings

- □ Play sound when finished
- ☑ Eject media when finished
- ☑ Enable telemetry

Step-7

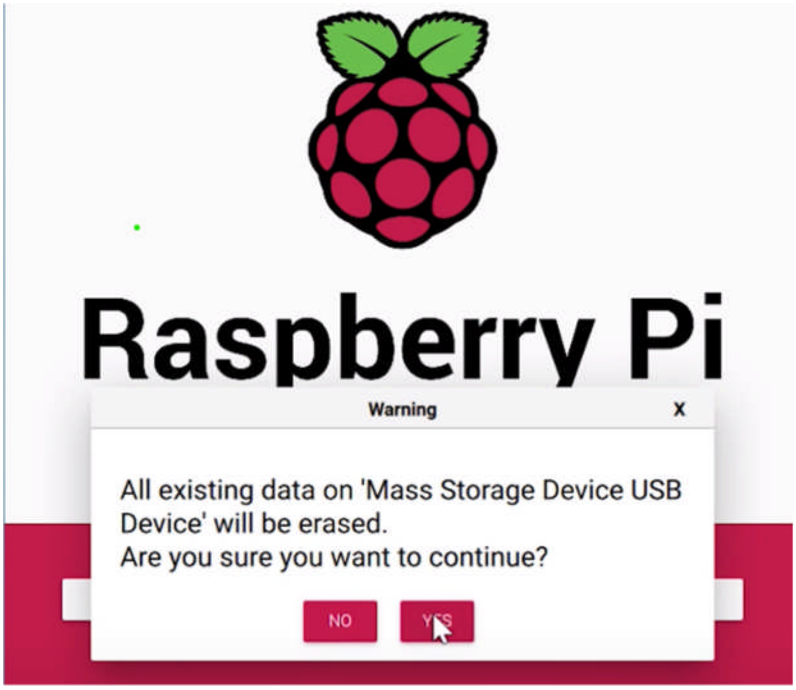
Now click on **WRITE**

Disclaimer: The content is curated for educational purposes only.
© Edunet Foundation. All rights reserved.



Step-8

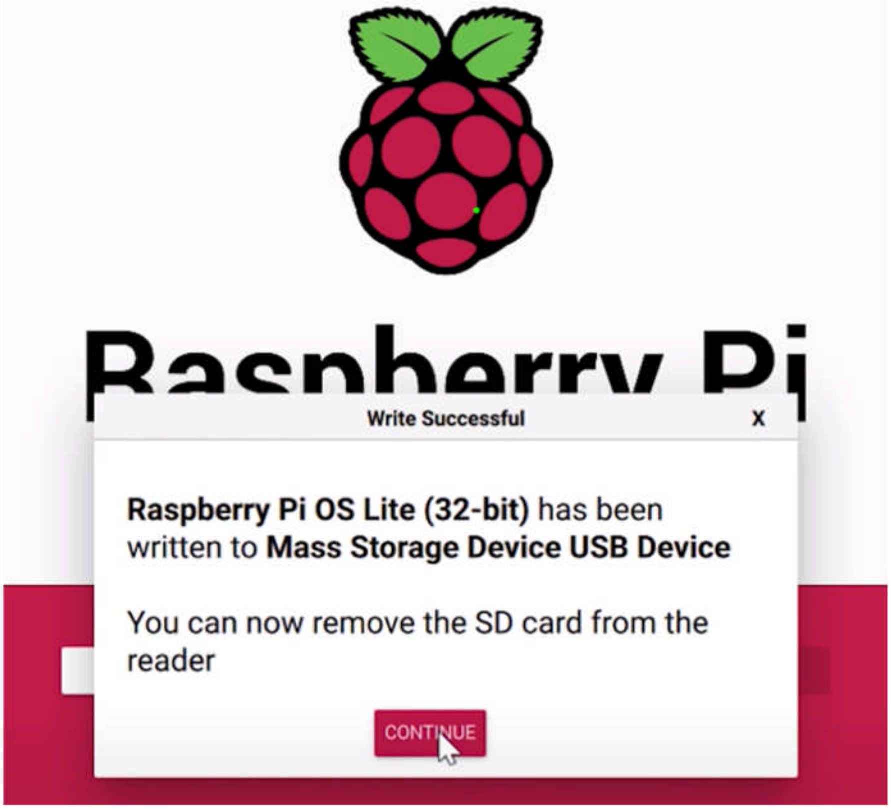
Click on **“YES”**



All existing data on 'Mass Storage Device USB Device' will be erased.
Are you sure you want to continue?

Step-9

Click on **Continue**



Write Successful

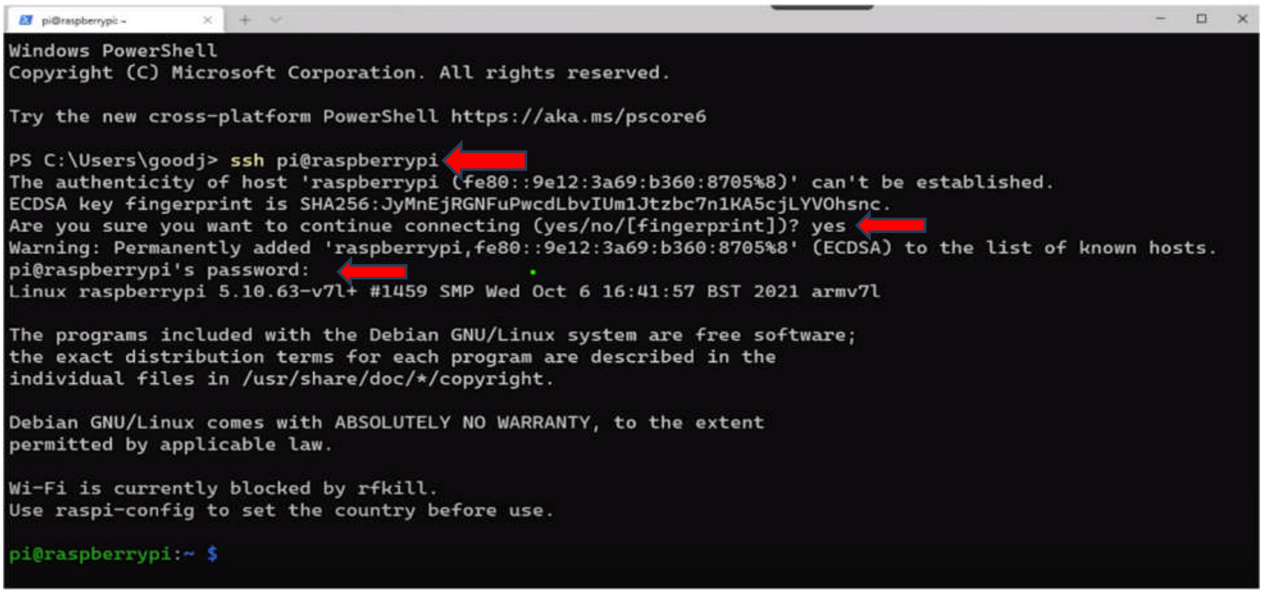
Raspberry Pi OS Lite (32-bit) has been written to **Mass Storage Device USB Device**

You can now remove the SD card from the reader

Step-10

1. Open you **“Windows powershell command”**
2. Type command **“ ssh pi@raspberrypi”**
3. Type: **Yes**
4. Password: **pi**

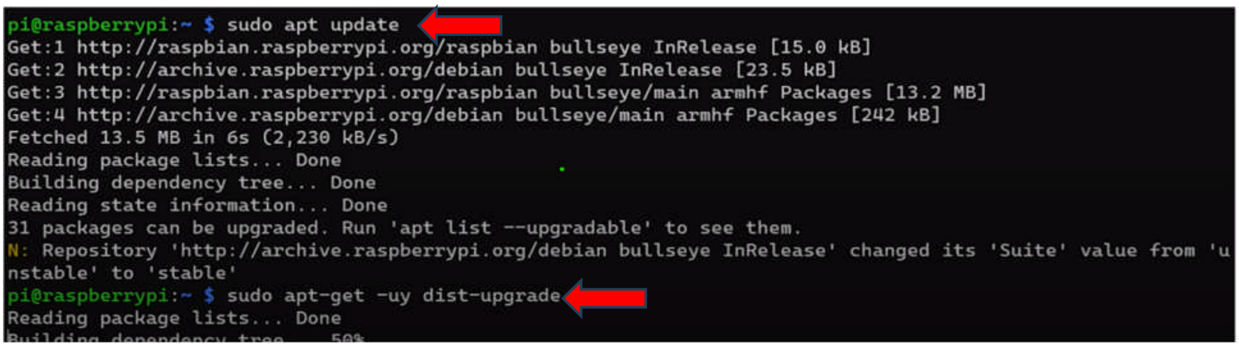
Disclaimer: The content is curated for educational purposes only.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\goodj> ssh pi@raspberrypi
The authenticity of host 'raspberrypi (fe80::9e12:3a69:b360:8705%8)' can't be established.
ECDSA key fingerprint is SHA256:JyMnEjRGNFuPwcdLbvIUm1Jtzbc7n1KA5cjLYVOhsnc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'raspberrypi,fe80::9e12:3a69:b360:8705%8' (ECDSA) to the list of known hosts.
pi@raspberrypi's password:
Linux raspberrypi 5.10.63-v7l+ #1459 SMP Wed Oct 6 16:41:57 BST 2021 armv7l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Wi-Fi is currently blocked by rfkill.
Use raspi-config to set the country before use.

pi@raspberrypi:~ $
```

Step-11:

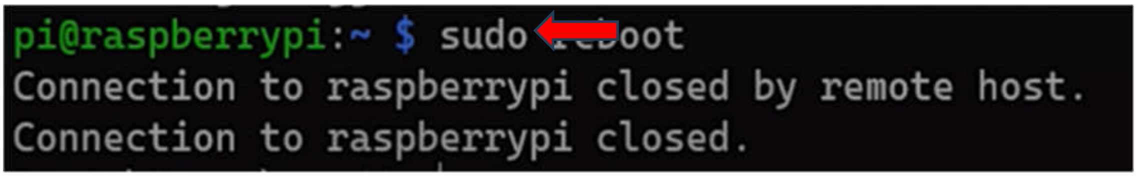
write following command shown in image



```
pi@raspberrypi:~ $ sudo apt update
Get:1 http://raspbian.raspberrypi.org/raspbian bullseye InRelease [15.0 kB]
Get:2 http://archive.raspberrypi.org/debian bullseye InRelease [23.5 kB]
Get:3 http://raspbian.raspberrypi.org/raspbian bullseye/main armhf Packages [13.2 MB]
Get:4 http://archive.raspberrypi.org/debian bullseye/main armhf Packages [242 kB]
Fetched 13.5 MB in 6s (2,230 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
31 packages can be upgraded. Run 'apt list --upgradable' to see them.
N: Repository 'http://archive.raspberrypi.org/debian bullseye InRelease' changed its 'Suite' value from 'u
nstable' to 'stable'
pi@raspberrypi:~ $ sudo apt-get -uy dist-upgrade
Reading package lists... Done
Building dependency tree... 50%
```

Step-12:

write following command shown in image and close the connection now.

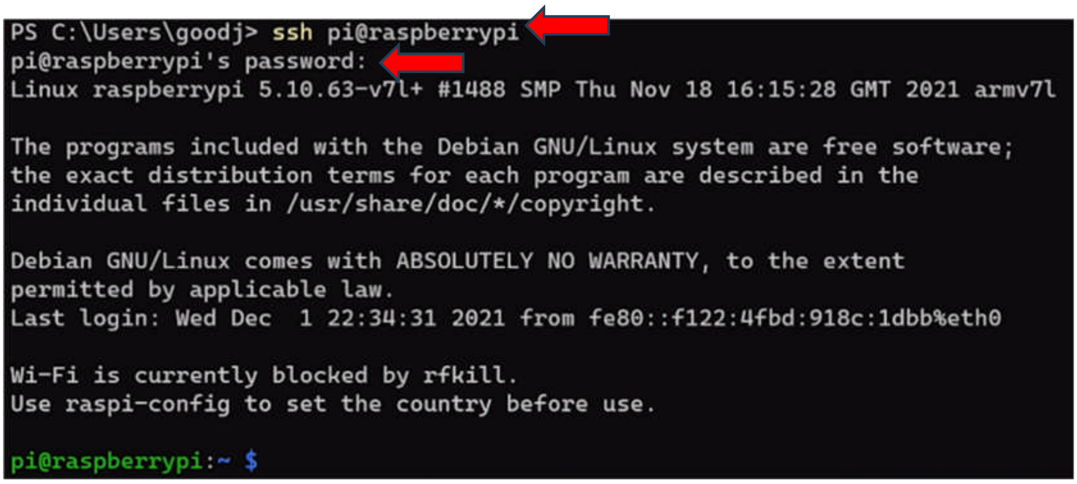


```
pi@raspberrypi:~ $ sudo reboot
Connection to raspberrypi closed by remote host.
Connection to raspberrypi closed.
```

Disclaimer: The content is curated for educational purposes only.
© Edunet Foundation. All rights reserved.

Step-13:

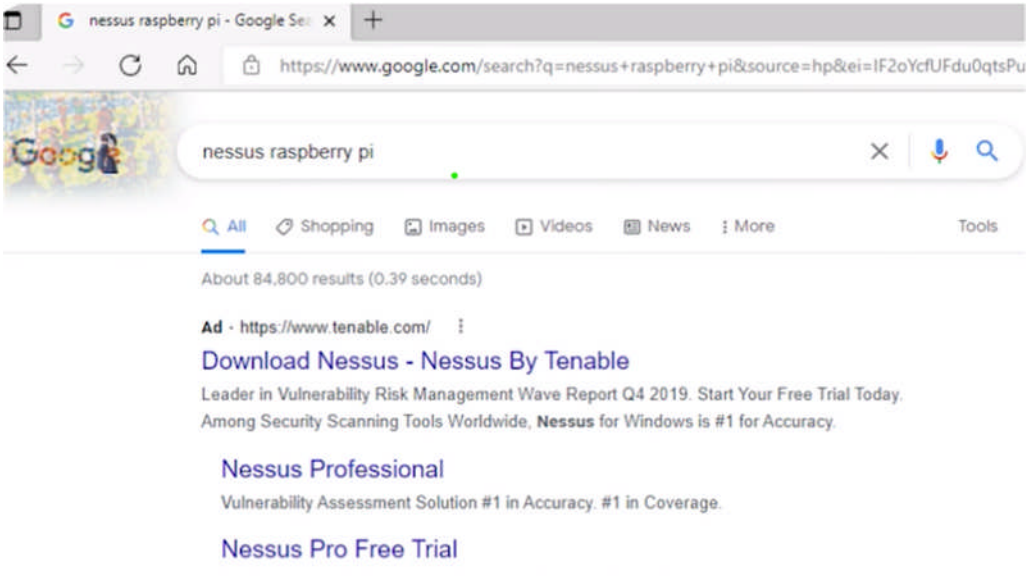
1. We are out of the **raspberrypi**
2. In windows powershell write following command shown in image



```
PS C:\Users\goodj> ssh pi@raspberrypi
pi@raspberrypi's password:
Linux raspberrypi 5.10.63-v7l+ #1488 SMP Thu Nov 18 16:15:28 GMT 2021 armv7l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Dec  1 22:34:31 2021 from fe80::f122:4fbd:918c:1dbb%eth0

Wi-Fi is currently blocked by rfkill.
Use raspi-config to set the country before use.

pi@raspberrypi:~ $
```

Step-14

In your browser search **nessus raspberry pi**



nessus raspberry pi - Google Se
https://www.google.com/search?q=nessus+raspberry+pi&source=hp&ei=IF2oYcfUFdu0qtsPu
nessus raspberry pi
All
Shopping
Images
Videos
News
More
Tools

About 84,800 results (0.39 seconds)

Ad · https://www.tenable.com/

Download Nessus - Nessus By Tenable

Leader in Vulnerability Risk Management Wave Report Q4 2019. Start Your Free Trial Today. Among Security Scanning Tools Worldwide, **Nessus** for Windows is #1 for Accuracy.

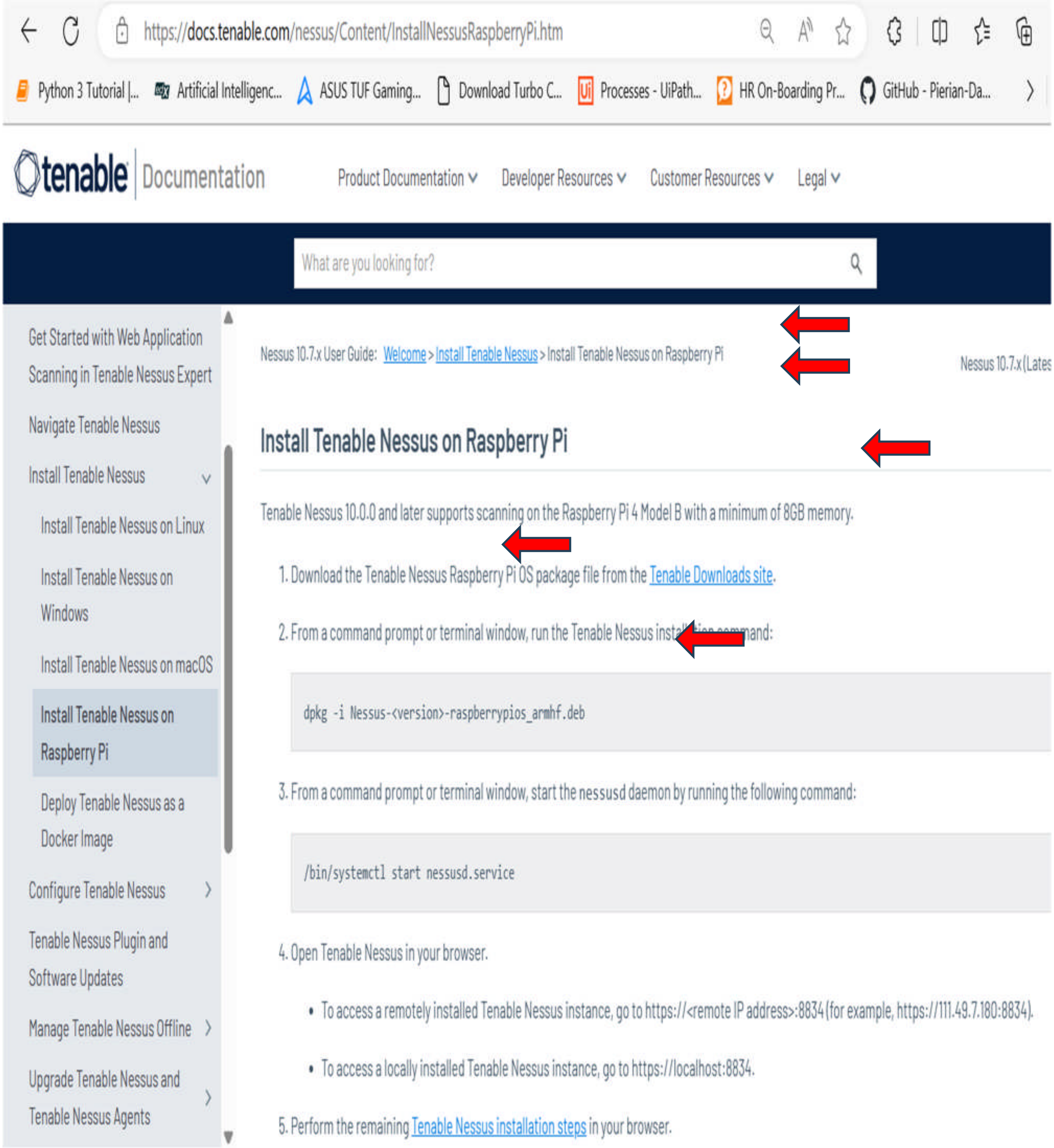
Nessus Professional

Vulnerability Assessment Solution #1 in Accuracy. #1 in Coverage.

Nessus Pro Free Trial

Step-15

1. Now we have to follow these five steps one by one (with command)
2. Click on **Tenable Downloads site** in new window


https://docs.tenable.com/nessus/Content/InstallNessusRaspberryPi.htm
Python 3 Tutorial |...
Artificial Intelligenc...
ASUS TUF Gaming...
Download Turbo C...
Processes - UiPath...
HR On-Boarding Pr...
GitHub - Pierian-Da...
tenable Documentation
Product Documentation
Developer Resources
Customer Resources
Legal
What are you looking for?
Get Started with Web Application Scanning in Tenable Nessus Expert
Navigate Tenable Nessus
Install Tenable Nessus
Install Tenable Nessus on Linux
Install Tenable Nessus on Windows
Install Tenable Nessus on macOS
Install Tenable Nessus on Raspberry Pi
Deploy Tenable Nessus as a Docker Image
Configure Tenable Nessus
Tenable Nessus Plugin and Software Updates
Manage Tenable Nessus Offline
Upgrade Tenable Nessus and Tenable Nessus Agents
Nessus 10.7.x User Guide: Welcome > Install Tenable Nessus > Install Tenable Nessus on Raspberry Pi
Nessus 10.7.x (Lates

Install Tenable Nessus on Raspberry Pi

Tenable Nessus 10.0.0 and later supports scanning on the Raspberry Pi 4 Model B with a minimum of 8GB memory.

1. Download the Tenable Nessus Raspberry Pi OS package file from the Tenable Downloads site.
2. From a command prompt or terminal window, run the Tenable Nessus installation command:

```
dpkg -i Nessus-<version>-raspberrypios_armhf.deb
```

3. From a command prompt or terminal window, start the nessusd daemon by running the following command:

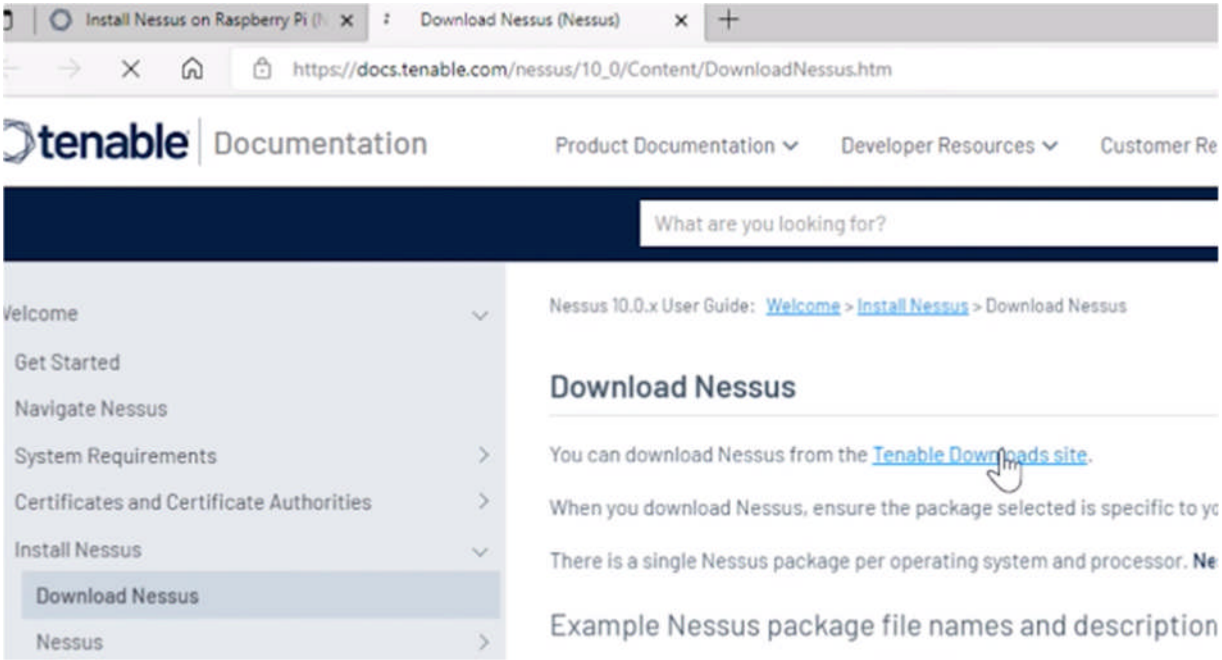
```
/bin/systemctl start nessusd.service
```

4. Open Tenable Nessus in your browser.
   - To access a remotely installed Tenable Nessus instance, go to https://<remote IP address>:8834 (for example, https://111.49.7.180:8834).
   - To access a locally installed Tenable Nessus instance, go to https://localhost:8834.
5. Perform the remaining Tenable Nessus installation steps in your browser.

Disclaimer: The content is curated for educational purposes only.
© Edunet Foundation. All rights reserved.

Step-16

Click on download



Nessus 10.0.x User Guide: Welcome > Install Nessus > Download Nessus

Download Nessus

You can download Nessus from the Tenable Downloads site.

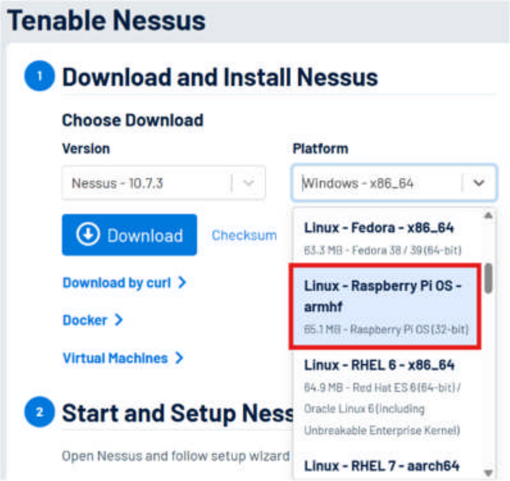
When you download Nessus, ensure the package selected is specific to yo

There is a single Nessus package per operating system and processor. Ne

Example Nessus package file names and description

Step-17

1. **Platform: Choose from the dropdown menu**
2. click on **red rectangle box** option
3. **Version:** Leave it as at is.(by default)



Tenable Nessus

Download and Install Nessus

Choose Download

Version: Nessus - 10.7.3

Platform: Windows - x86_64

Linux - Fedora - x86_64 — 63.3 MB - Fedora 38 / 39 (64-bit)

Linux - Raspberry Pi OS - armhf — 65.1 MB - Raspberry Pi OS (32-bit)

Linux - RHEL 6 - x86_64 — 64.9 MB - Red Hat ES 6 (64-bit) / Oracle Linux 6 (including Unbreakable Enterprise Kernel)

Linux - RHEL 7 - aarch64

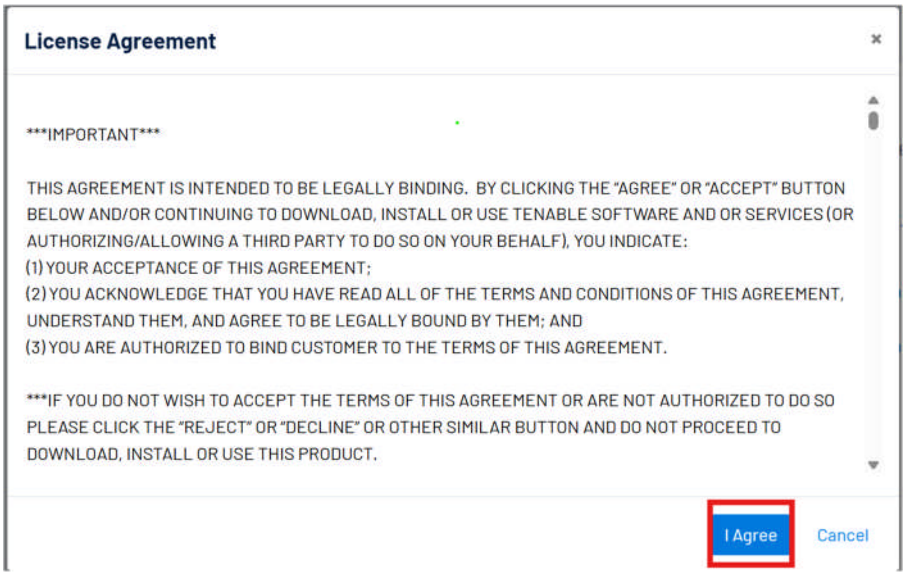
Start and Setup Ness

Open Nessus and follow setup wizard

Disclaimer: The content is curated for educational purposes only.
© Edunet Foundation. All rights reserved.

Step-18

Click on **Agree**



License Agreement

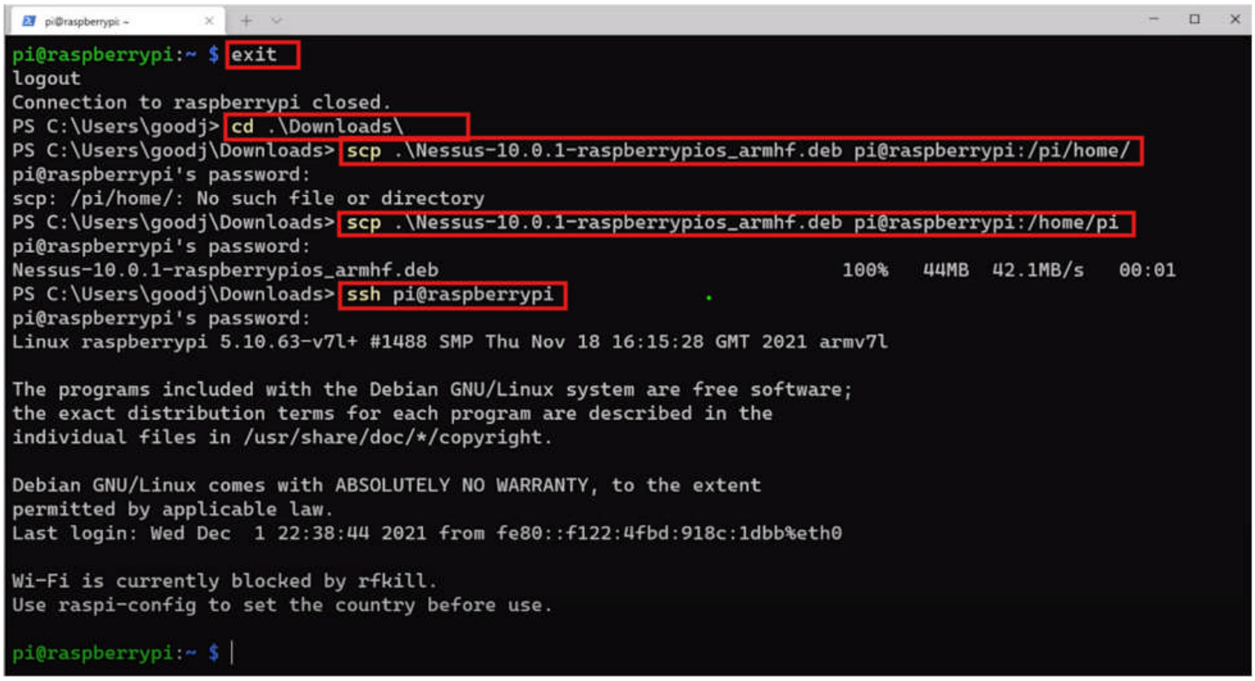
IMPORTANT

THIS AGREEMENT IS INTENDED TO BE LEGALLY BINDING. BY CLICKING THE "AGREE" OR "ACCEPT" BUTTON BELOW AND/OR CONTINUING TO DOWNLOAD, INSTALL OR USE TENABLE SOFTWARE AND OR SERVICES (OR AUTHORIZING/ALLOWING A THIRD PARTY TO DO SO ON YOUR BEHALF), YOU INDICATE:
(1) YOUR ACCEPTANCE OF THIS AGREEMENT;
(2) YOU ACKNOWLEDGE THAT YOU HAVE READ ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, UNDERSTAND THEM, AND AGREE TO BE LEGALLY BOUND BY THEM; AND
(3) YOU ARE AUTHORIZED TO BIND CUSTOMER TO THE TERMS OF THIS AGREEMENT.

***IF YOU DO NOT WISH TO ACCEPT THE TERMS OF THIS AGREEMENT OR ARE NOT AUTHORIZED TO DO SO PLEASE CLICK THE "REJECT" OR "DECLINE" OR OTHER SIMILAR BUTTON AND DO NOT PROCEED TO DOWNLOAD, INSTALL OR USE THIS PRODUCT.

Step-19

1. We are in our raspberrypi type **"exit"** command that will logout RPI.
2. Now you are in local computer copy the path of downloaded nessus and paste here after command: **cd .\path**
3. Type **"scp .\filename:/pi/home/", it will show you no such directory**
4. Then again type "**scp .\filename:/home/pi"** (look carefully it's **home/pi** now)
5. Now again activate raspberrypi type: **ssh pi@raspberrypi**
6. Now you can see in green color you RPI connected successfully.



```
pi@raspberrypi:~ $ exit
logout
Connection to raspberrypi closed.
PS C:\Users\goodj> cd .\Downloads\
PS C:\Users\goodj\Downloads> scp .\Nessus-10.0.1-raspberrypios_armhf.deb pi@raspberrypi:/pi/home/
pi@raspberrypi's password:
scp: /pi/home/: No such file or directory
PS C:\Users\goodj\Downloads> scp .\Nessus-10.0.1-raspberrypios_armhf.deb pi@raspberrypi:/home/pi
pi@raspberrypi's password:
Nessus-10.0.1-raspberrypios_armhf.deb                                 100%    44MB  42.1MB/s   00:01
PS C:\Users\goodj\Downloads> ssh pi@raspberrypi
pi@raspberrypi's password:
Linux raspberrypi 5.10.63-v7l+ #1488 SMP Thu Nov 18 16:15:28 GMT 2021 armv7l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Dec  1 22:38:44 2021 from fe80::f122:4fbd:918c:1dbb%eth0

Wi-Fi is currently blocked by rfkill.
Use raspi-config to set the country before use.

pi@raspberrypi:~ $ |
```

Step-22

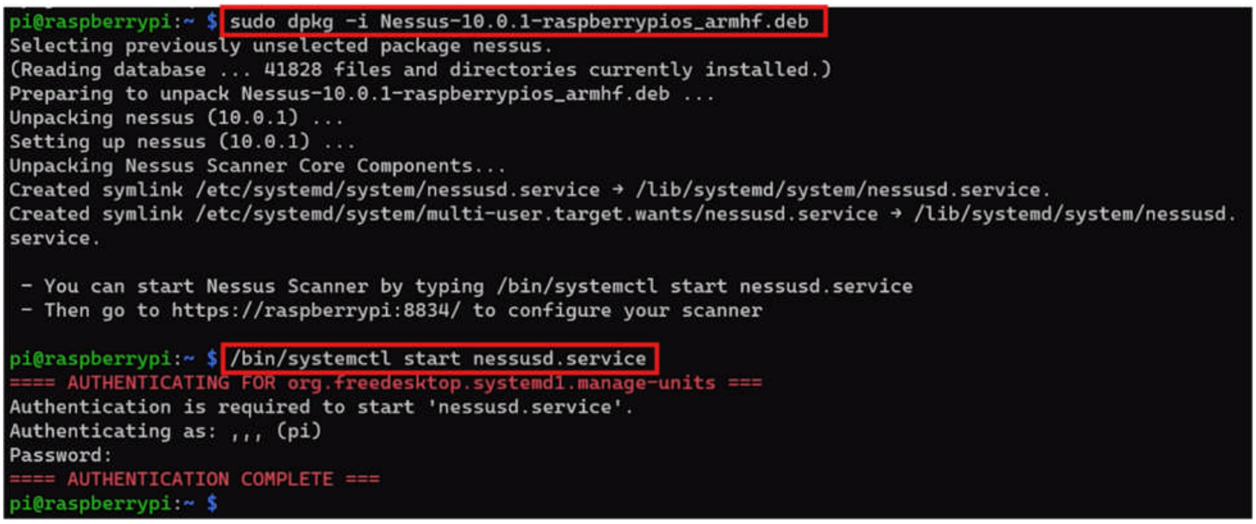
Now type the following in the image (Copy your nessus **filename** from download)

1. Type command: **sudo dpkg -i <filename>**

   “sudo dpkg -i Nessus-10.7.3-raspberrypios_armhf.deb”

   or put you current version e.g. Nessus 10.7.3 or latest.

2. Type command: **/bin/systemctl start nessusd.service**

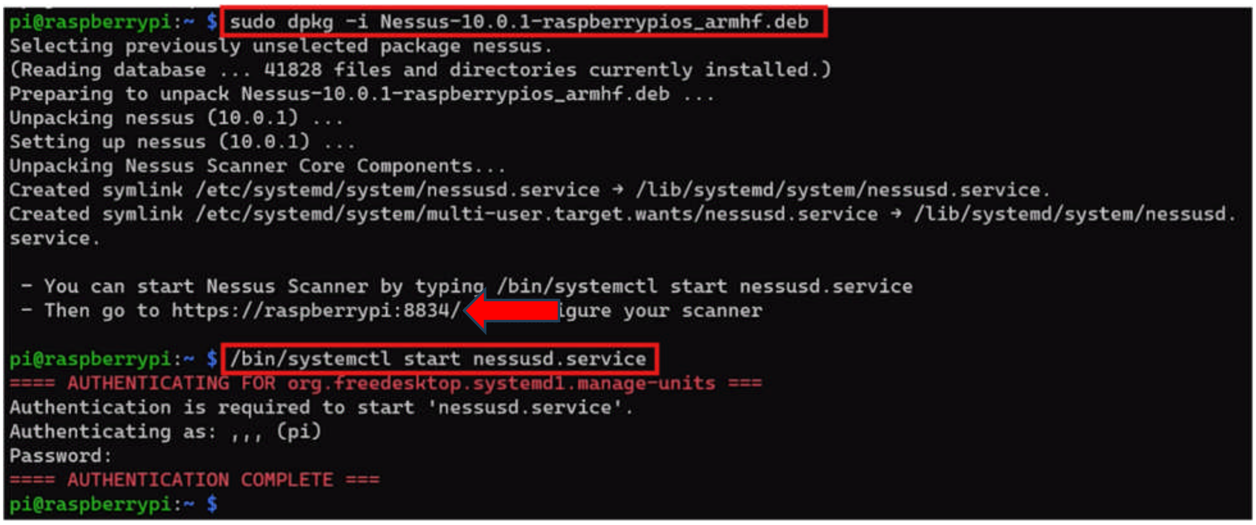


```
pi@raspberrypi:~ $ sudo dpkg -i Nessus-10.0.1-raspberrypios_armhf.deb
Selecting previously unselected package nessus.
(Reading database ... 41828 files and directories currently installed.)
Preparing to unpack Nessus-10.0.1-raspberrypios_armhf.deb ...
Unpacking nessus (10.0.1) ...
Setting up nessus (10.0.1) ...
Unpacking Nessus Scanner Core Components...
Created symlink /etc/systemd/system/nessusd.service → /lib/systemd/system/nessusd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/nessusd.service → /lib/systemd/system/nessusd.
service.

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

pi@raspberrypi:~ $ /bin/systemctl start nessusd.service
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to start 'nessusd.service'.
Authenticating as: ,,, (pi)
Password:
==== AUTHENTICATION COMPLETE ===
pi@raspberrypi:~ $
```

3. RPI authentication completed.

Step-23

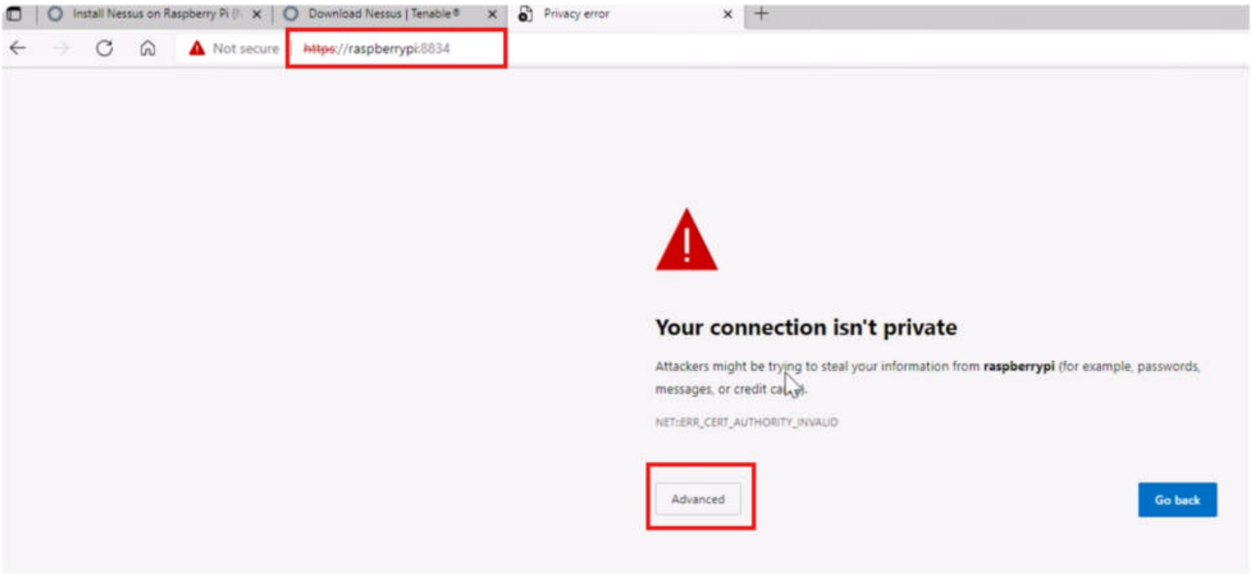
You will get to know that we have: **https://raspberrypi:8834/**



```
pi@raspberrypi:~ $ sudo dpkg -i Nessus-10.0.1-raspberrypios_armhf.deb
Selecting previously unselected package nessus.
(Reading database ... 41828 files and directories currently installed.)
Preparing to unpack Nessus-10.0.1-raspberrypios_armhf.deb ...
Unpacking nessus (10.0.1) ...
Setting up nessus (10.0.1) ...
Unpacking Nessus Scanner Core Components...
Created symlink /etc/systemd/system/nessusd.service → /lib/systemd/system/nessusd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/nessusd.service → /lib/systemd/system/nessusd.
service.

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

pi@raspberrypi:~ $ /bin/systemctl start nessusd.service
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to start 'nessusd.service'.
Authenticating as: ,,, (pi)
Password:
==== AUTHENTICATION COMPLETE ===
pi@raspberrypi:~ $
```

Step-24

1. Open the browser paste this above url. (**https://raspberrypi:8834/)**
2. Click on advanced option.



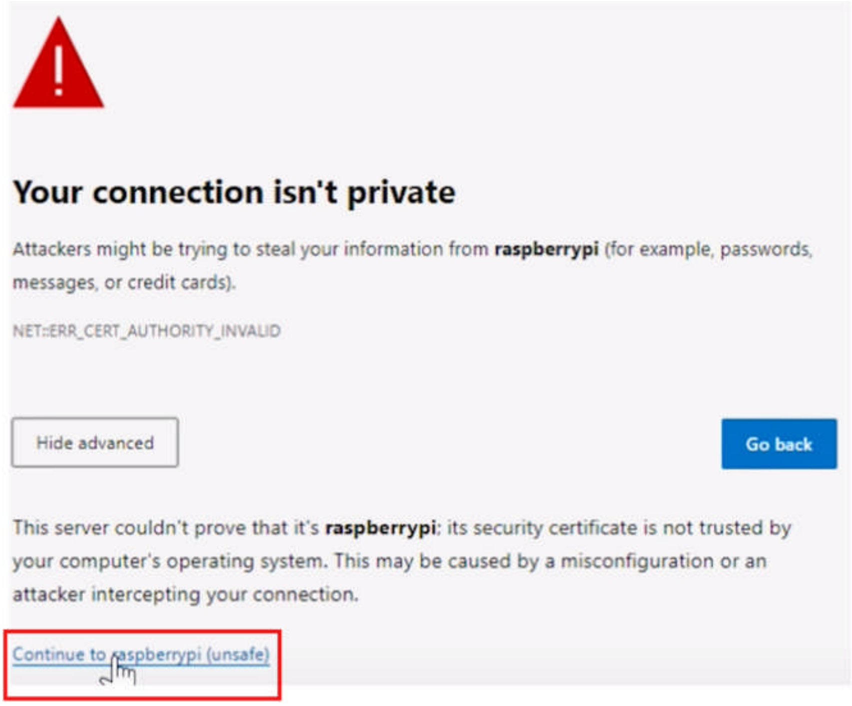
Your connection isn't private

Attackers might be trying to steal your information from **raspberrypi** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_AUTHORITY_INVALID

Step-25

Click on continue



Your connection isn't private

Attackers might be trying to steal your information from **raspberrypi** (for example, passwords, messages, or credit cards).

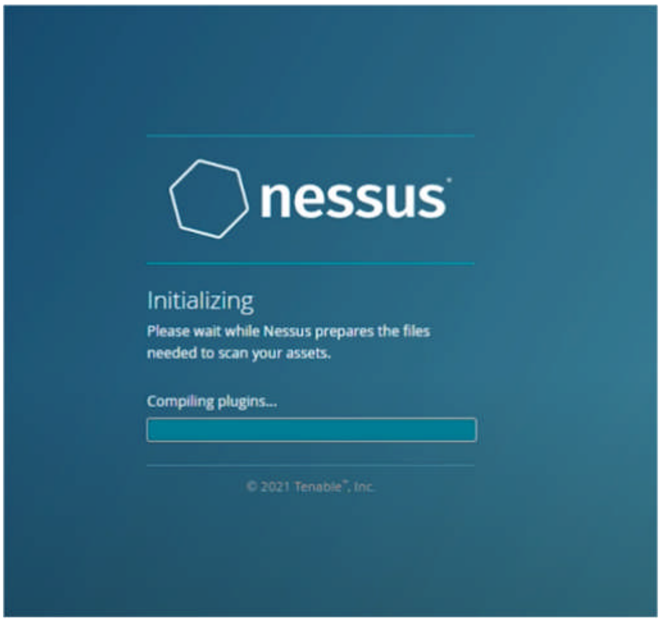
NET::ERR_CERT_AUTHORITY_INVALID

This server couldn't prove that it's **raspberrypi**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Continue to raspberrypi (unsafe)

Step-26

1. Click on Nessus essential plugins
2. Click on continue



Initializing

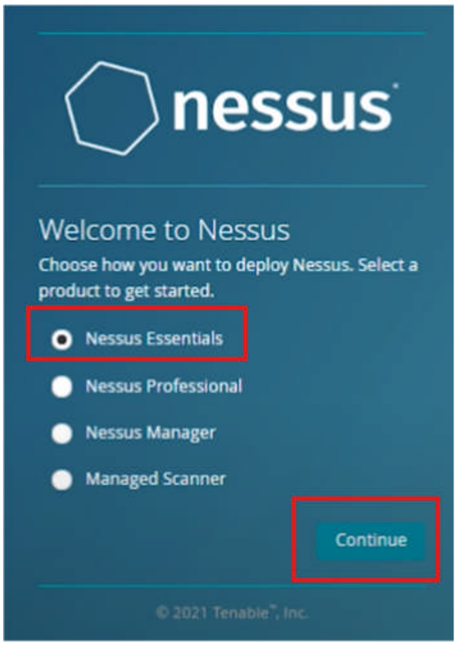
Please wait while Nessus prepares the files needed to scan your assets.

Compiling plugins...

© 2021 Tenable®, Inc.

Step-27

3. Click on Nessus essential plugins
4. Click on continue



nessus

Welcome to Nessus

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

● Nessus Essentials

○ Nessus Professional

○ Nessus Manager

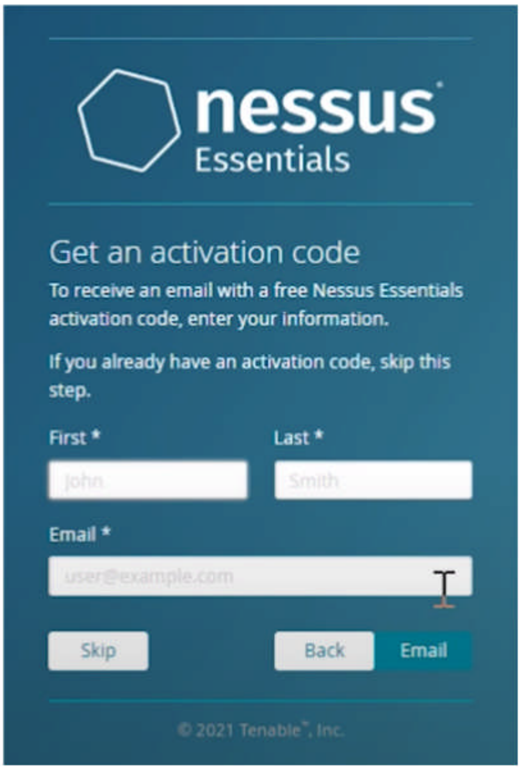
○ Managed Scanner

Continue

© 2021 Tenable™, Inc.

Step-28

Fill your details



nessus Essentials

Get an activation code

To receive an email with a free Nessus Essentials activation code, enter your information.

If you already have an activation code, skip this step.

First * John

Last * Smith

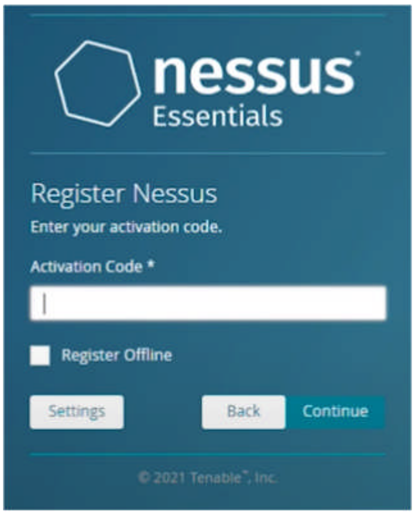
Email * user@example.com

Skip Back Email

© 2021 Tenable™, Inc.

Step-29

Check your mail and paste activation code here



nessus Essentials

Register Nessus

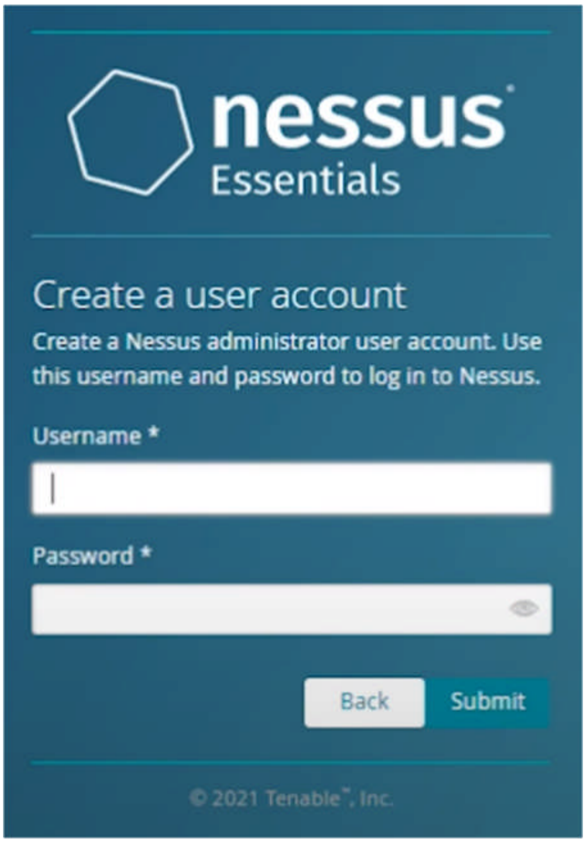
Enter your activation code.

Activation Code *

□ Register Offline

Step-30

Now set username and password



nessus Essentials

Create a user account

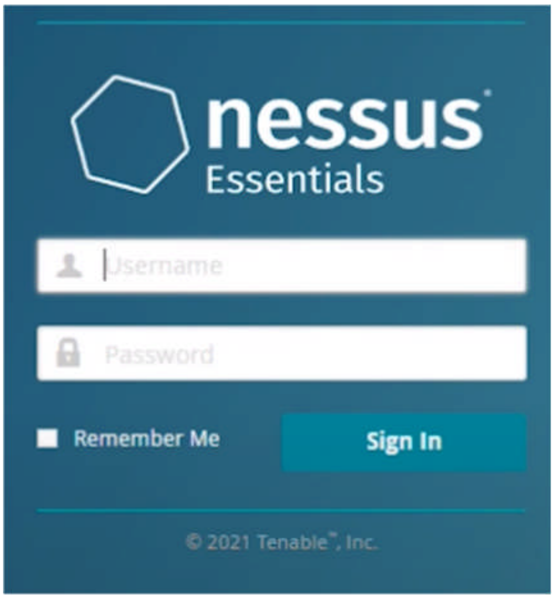
Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username *

Password *

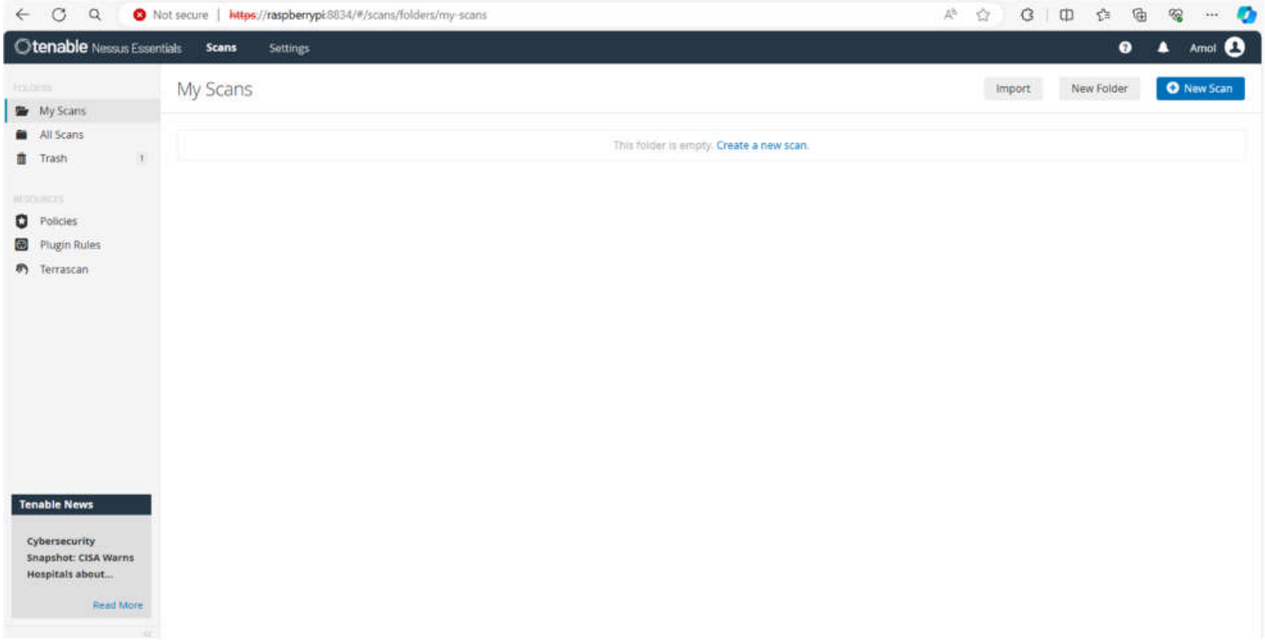
Step-31

Sign in now



Step-32

Click on **New scan**

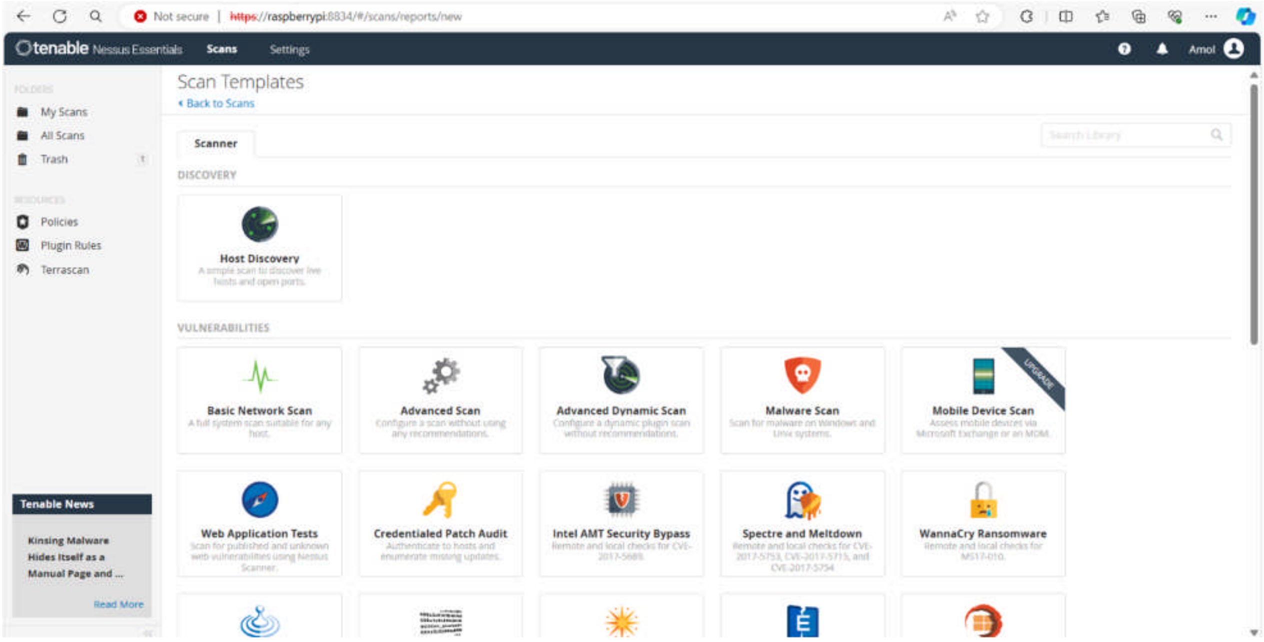


This folder is empty. Create a new scan.

Cybersecurity Snapshot: CISA Warns Hospitals about...

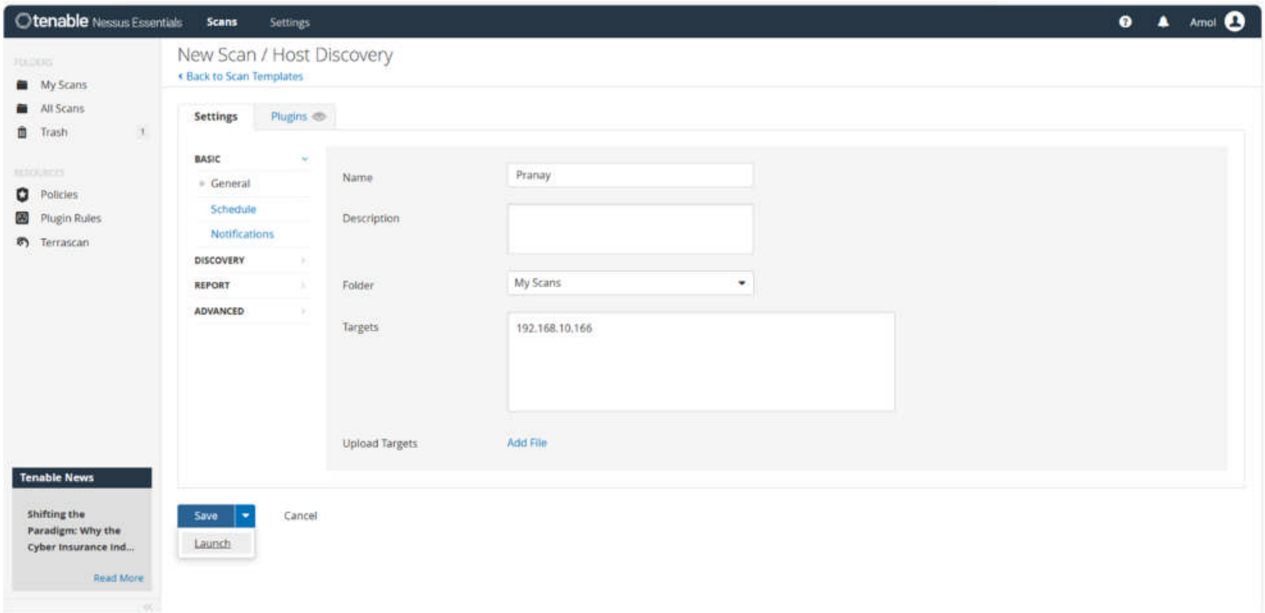
Step-33

Click on **host discovery**



Step-34

- Fill the information.
- Fill the IP address of the device of which you want to find vulnerability.



Name: Pranay

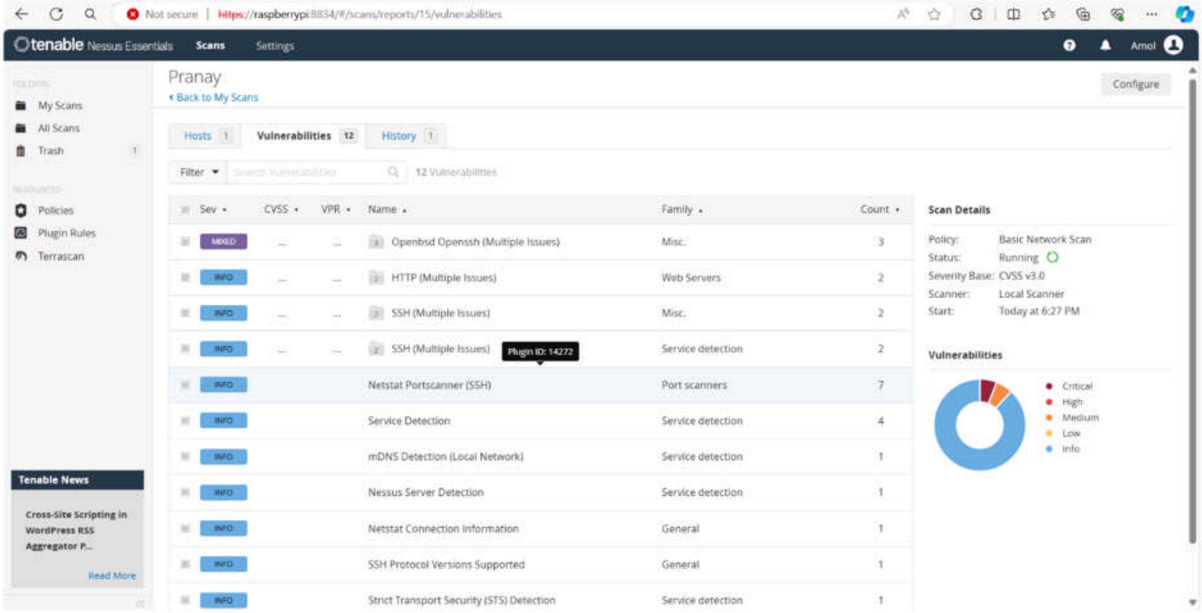
Description:

Folder: My Scans

Targets: 192.168.10.166

Step-35

Here on Clicking vulnerabilities on the top, we can see all vulnerabilities according to different types.



Not secure | https://raspberrypi:8834/#/scans/reports/15/vulnerabilities

Pranay

‹ Back to My Scans

12 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
MIXED	...	...	3 Openbsd Openssh (Multiple Issues)	Misc.	3
INFO	...	...	2 HTTP (Multiple Issues)	Web Servers	2
INFO	...	...	2 SSH (Multiple Issues)	Misc.	2
INFO	...	...	2 SSH (Multiple Issues) Plugin ID: 14272	Service detection	2
INFO			Netstat Portscanner (SSH)	Port scanners	7
INFO			Service Detection	Service detection	4
INFO			mDNS Detection (Local Network)	Service detection	1
INFO			Nessus Server Detection	Service detection	1
INFO			Netstat Connection Information	General	1
INFO			SSH Protocol Versions Supported	General	1
INFO			Strict Transport Security (STS) Detection	Service detection	1

Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:27 PM

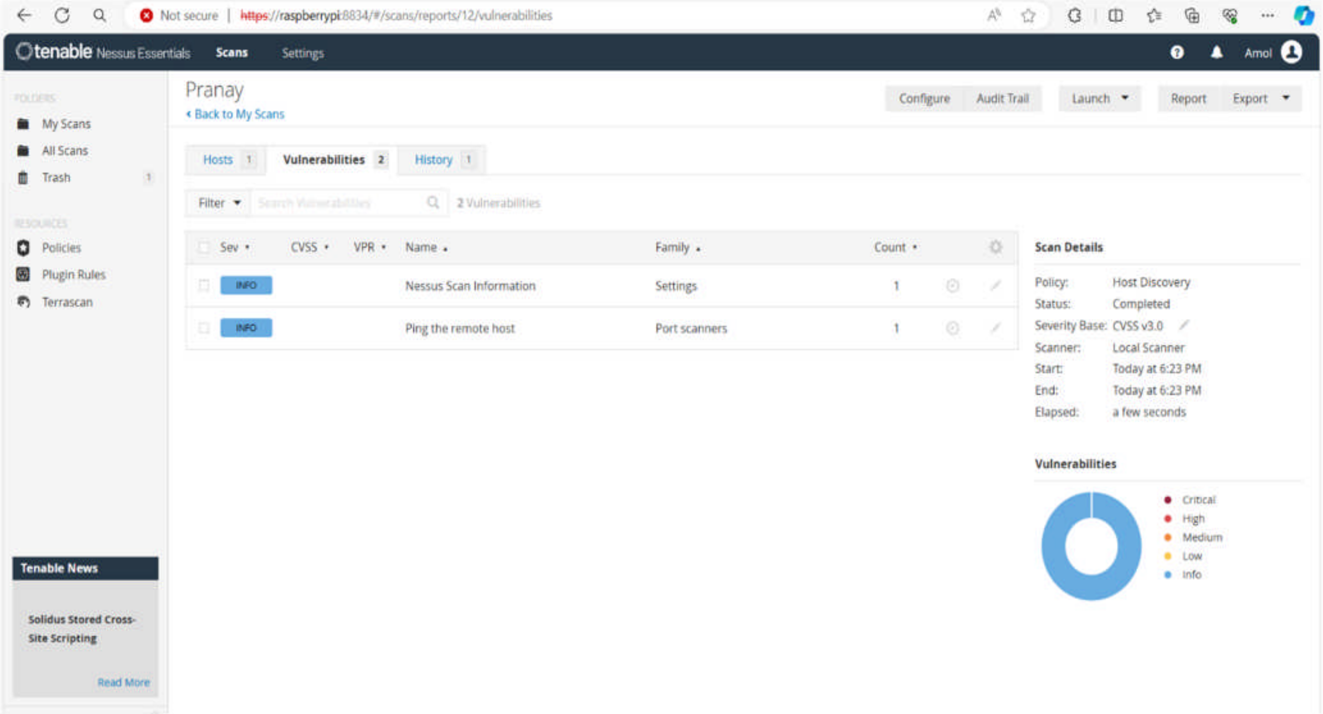
Vulnerabilities

Tenable News

Cross-Site Scripting in WordPress RSS Aggregator P...

Read More

- **Here scanning completed!**
- **Here** on Clicking vulnerabilities on the top, we can see all vulnerabilities according to different types.



Not secure | https://raspberrypi:8834/#/scans/reports/12/vulnerabilities

Pranay

‹ Back to My Scans

2 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
INFO			Nessus Scan Information	Settings	1
INFO			Ping the remote host	Port scanners	1

Scan Details

Policy: Host Discovery
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:23 PM
End: Today at 6:23 PM
Elapsed: a few seconds

Vulnerabilities

Tenable News

Solidus Stored Cross-Site Scripting

Read More

- **Here** on Clicking vulnerabilities on the top, we can see all vulnerabilities according to different types.
- We have done with the practical. We found vulnerability in the device via IP address using Nessus scanner.