Enumerate a Network with Kali and Zenmap

Contents

Time required: 30 minutes

How to Create Screenshots: Please use the Windows Snip and Sketch Tool or the Snipping Tool. Paste a screenshot of just the program you are working on. If you are snipping a virtual machine, make sure your focus is outside the virtual machine before you snip.

1. Press and hold down the **Windows key** & **Shift**, then type **S.** This brings up the on-screen snipping tool.
2. Click and Drag your mouse around whatever you want to snip.
3. Release the mouse button. This places the snip into the Windows Clipboard.
4. Go into Word or wherever you want to paste the snip. Hold down **CTRL**, then type **V** to paste the snip.

Lab Description

One of the first steps of penetration testing or doing a security audit is to find out what devices are on the network.

DANGER ZONE: Make sure that you own the devices you perform a scan on. If you are performing this scan on a device or network you do not own, make sure to get a written consent from the owner of the device to avoid legal issues.

You have permission to scan the network in D1.

Installing Zenmap in Kali Linux

Zenmap is a graphical user interface for the command line tool nmap.

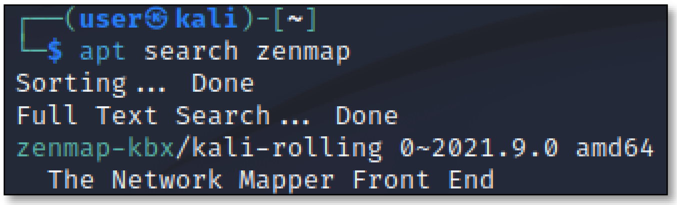
1. In a Kali Linux terminal session, update Kali.

```
# Update the packages list
sudo apt update

# Perform the update
sudo apt dist-upgrade -y
```

2. Do an apt-search for ZenMap

```
apt search zenmap
```



```
┌──(user㉿kali)-[~]
└─$ apt search zenmap
Sorting... Done
Full Text Search... Done
zenmap-kbx/kali-rolling 0~2021.9.0 amd64
  The Network Mapper Front End
```

3. Install **zenmap-kbx**

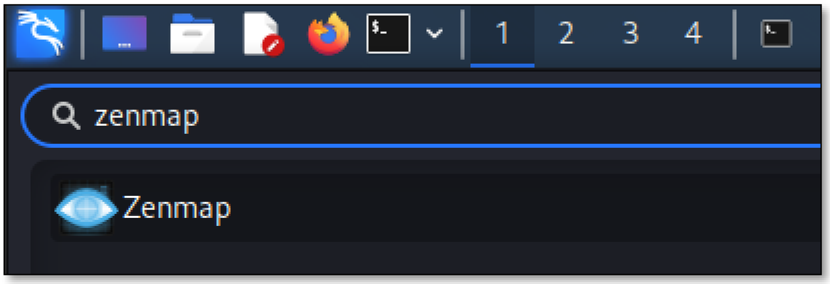
```
sudo apt install zenmap-kbx -y
```

Zenmap In Kali Linux

1. In the Kali Linux VM → Go to **Machine** menu → **Settings** → **Network**. Make sure you are attached to the Bridged Adapter.
2. In a Kali Linux terminal session type **ip a**
   Use this information to figure out your network Target. For example: If your IP address was 192.168.1.106, and your subnet mask is 255.255.255.0, then your network Target is 192.168.1.1-254 or 192.168.1.0/24
3. **Insert a screenshot showing your IP address.**

Click or tap here to enter text.

4. Go to the Kali start menu → type **zenmap**

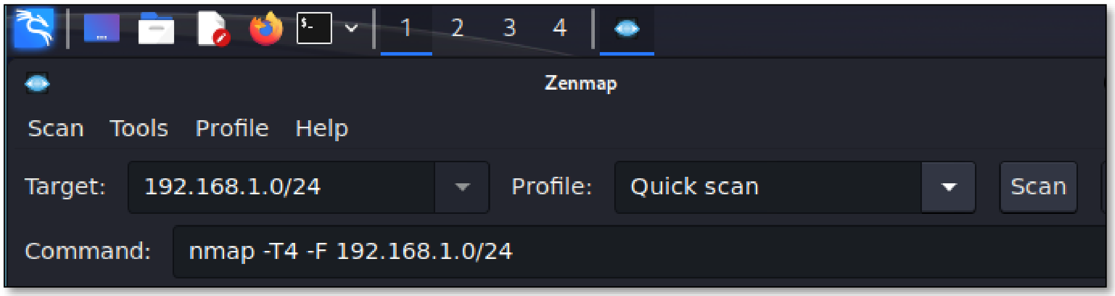


zenmap

5. Click **Zenmap**. You should see the following.

6. **Target**: Put in your network information.

7. By Profile: choose **Quick scan**.

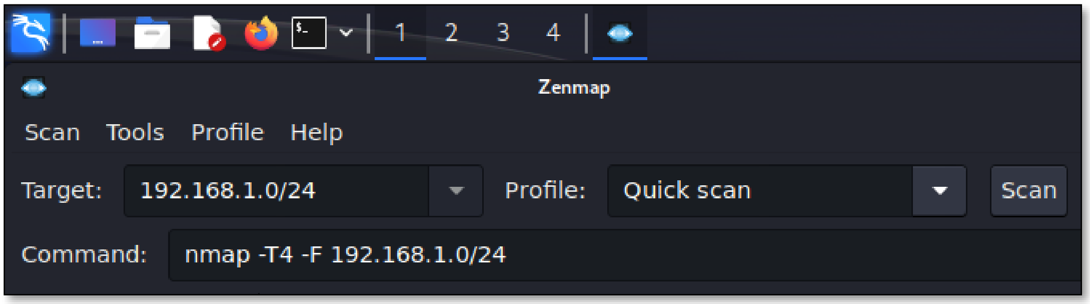


Target: 192.168.1.0/24

Profile: Quick scan

Command: nmap -T4 -F 192.168.1.0/24

8. Click **Scan**.



Target: 192.168.1.0/24

Profile: Quick scan

Command: nmap -T4 -F 192.168.1.0/24

9. **Insert a screenshot of the results of your scan:**

Click or tap here to enter text.

10. **How many IP addresses were scanned?**

Click or tap here to enter text.

11. **How many hosts are up?**

Click or tap here to enter text.

12. Choose a host with open ports reported, use the Ports/Hosts tab to list the ports and services.

13. What type of information is available?

Click or tap here to enter text.

14. Choose the host details tab.

15. What type of information is available?

Click or tap here to enter text.

16. Can you figure out which machine is the one you are scanning from?

Click or tap here to enter text.

17. What other information is provided?

Click or tap here to enter text.

18. Insert a screenshot of the host details of one of your hosts.

Click or tap here to enter text.

Windows Zenmap Install

You can use your local Windows computer or a VM on a bridged adapter.

1. Go to www.nmap.org.
2. Go to **Microsoft Windows binaries**.
3. Download and install **Latest stable release self-installer.**

Scan Localhost

Let’s start by scanning our local computer.

localhost refers to a network address that points to the current device or computer that you are working on. It is often represented as **127.0.0.1** in IPv4 or "::1" in IPv6. Localhost is used to establish a connection to the device itself, allowing applications and services to communicate with each other on the same machine without going through a network, which can enhance security by keeping certain processes isolated from external networks and potential threats.

4. Run **Zenmap**.
   a. **Target:** localhost

   b. **Profile:** Quick scan plus

5. Click **Scan**.

6. **Insert a screenshot:**

Click or tap here to enter text.

Scan Local Network

1. Run **ipconfig**.

2. Use the **ipconfig** information to figure out your network **Target**.
   For example: If your IP address was 192.168.1.106, and your subnet mask is 255.255.255.0, then your network Target is 192.168.1.1-254.

3. Enter your network range in the **Target** field. Click **Scan**.

4. **Insert a screenshot:**

Click or tap here to enter text.

5. **How many IP addresses were scanned?**

Click or tap here to enter text.

6. **How many hosts are up?**

Click or tap here to enter text.

7. Choose a host with open ports reported, use the Ports/Hosts tab to list the ports and services.

8. **What type of information is available?**

Click or tap here to enter text.

9. Choose the host details tab.

10. **What type of information is available?**

Click or tap here to enter text.

11. **Can you figure out which machine is the one you are scanning from?**

Click or tap here to enter text.

12. **What other information is provided?**

Click or tap here to enter text.

13. **Insert a screenshot of the host details of one of your hosts.**

Click or tap here to enter text.

scanme.nmap.org

scanme.nmap.org or 45.33.32.156 is a public ip address provided by nmap for practicing scanning.

1. **Insert a screenshot of a regular scan of this host.**

Click or tap here to enter text.

Assignment Submission

Attach this completed document to the assignment in Blackboard.