# Enumerate a Network with Kali and Zenmap

Contents

[Enumerate a Network with Kali and Zenmap 1](#_Toc200371304)

[Lab Description 1](#_Toc200371305)

[Installing Zenmap in Kali Linux 1](#_Toc200371306)

[Zenmap In Kali Linux 2](#_Toc200371307)

[Windows Zenmap Install 4](#_Toc200371308)

[Scan Localhost 4](#_Toc200371309)

[Scan Local Network 4](#_Toc200371310)

[scanme.nmap.org 5](#_Toc200371311)

[Assignment Submission 6](#_Toc200371312)

Time required: 60 minutes

## 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****

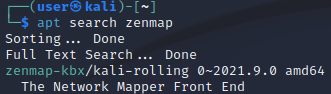
Zenmap is a graphical user interface for the command line tool nmap.

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

|  |
| --- |
| # Update the packages list  sudo apt update  # Perform the update  sudo apt dist-upgrade -y |

1. Do an apt-search for ZenMap

|  |
| --- |
| apt search zenmap |



1. Install **zenmap-kbx**

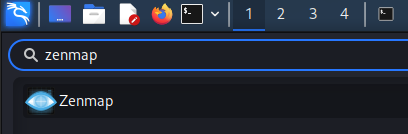
|  |
| --- |
| sudo apt install zenmap-kbx -y |

# 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.

1. Go to the Kali start menu 🡪 type **zenmap**



1. Click **Zenmap**. You should see the following.
2. **Target**: Put in your network information.
3. By Profile: choose **Quick scan**.

A screenshot of a computer

Description automatically generated

1. Click **Scan**.

A screenshot of a computer

Description automatically generated

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

Click or tap here to enter text.

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

Click or tap here to enter text.

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

Click or tap here to enter text.

1. Choose a host with open ports reported, use the Ports/Hosts tab to list the ports and services.
2. **What type of information is available?**

Click or tap here to enter text.

1. Choose the host details tab.
2. **What type of information is available?**

Click or tap here to enter text.

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

Click or tap here to enter text.

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

Click or tap here to enter text.

1. **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](http://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.

1. Run **Zenmap**.
   1. **Target:** localhost
   2. **Profile:** Quick scan plus
2. Click **Scan**.
3. **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.

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

Click or tap here to enter text.

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

Click or tap here to enter text.

1. Choose a host with open ports reported, use the Ports/Hosts tab to list the ports and services.
2. **What type of information is available?**

Click or tap here to enter text.

1. Choose the host details tab.
2. **What type of information is available?**

Click or tap here to enter text.

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

Click or tap here to enter text.

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

Click or tap here to enter text.

1. **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.