CYBERTECH AWARENESS PROGRAM

CYBERSECURITY AWARENESS AND EDUCATIONAL OUT-REACH

BURLINGTON, VT

Nmap

Network Scanner

@cybertechvt @cybertechvt cybertechvt.com

Disclaimer/Warning

The Kali Guides provided to you by the Cyber Tech Awareness team are meant for educational purposes ONLY.

The tools covered in the Kali Guides can be used for malicious purposes, but should not be used as such.

The CyberTech Awareness team and the Leahy Center for Digital Forensics and Cybersecurity is NOT responsible any malicious activity conduced with aid from these Kali Guides.

Only use this tool on domains, addresses, files and resources that you have permission to.

Brief Summary

Nmap, or **Network Mapper**, is a free and open source network discovery tool, useful to **map** networks and **scan** ports of machines on your network.

Helpful Vocabulary

IP Address:

- An Internet Protocol (IP) Address, is similar to a physical home or mailing address. All devices that are connected to the internet have a unique IP address. This allows devices to communicate and send information to specific devices using their IP address.

Domain Names:

- When you want to go a specific website, you need the IP address of the site to access it. Instead of having to remember IP addresses, you can just type in the domain that is associated with a certain IP, and it will be translated to an IP address for you.

Domain Name System(DNS)

- DNS is a network of servers that collectively knows every domain name. When a browser requests the IP address of a domain name, the server will either know the answer or will ask other servers for the IP address, until it returns the page you are looking for.

Ports:

- Ports are virtual gateways that help computers categorize and manage various types of data that they send and receive.

Operating System (OS):

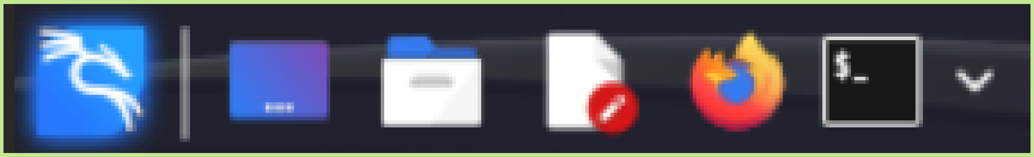
- The Operating System is core software that manages and controls system hardware and provides a platform for running applications and other software. Kali runs on the Linux OS.

Terminal:

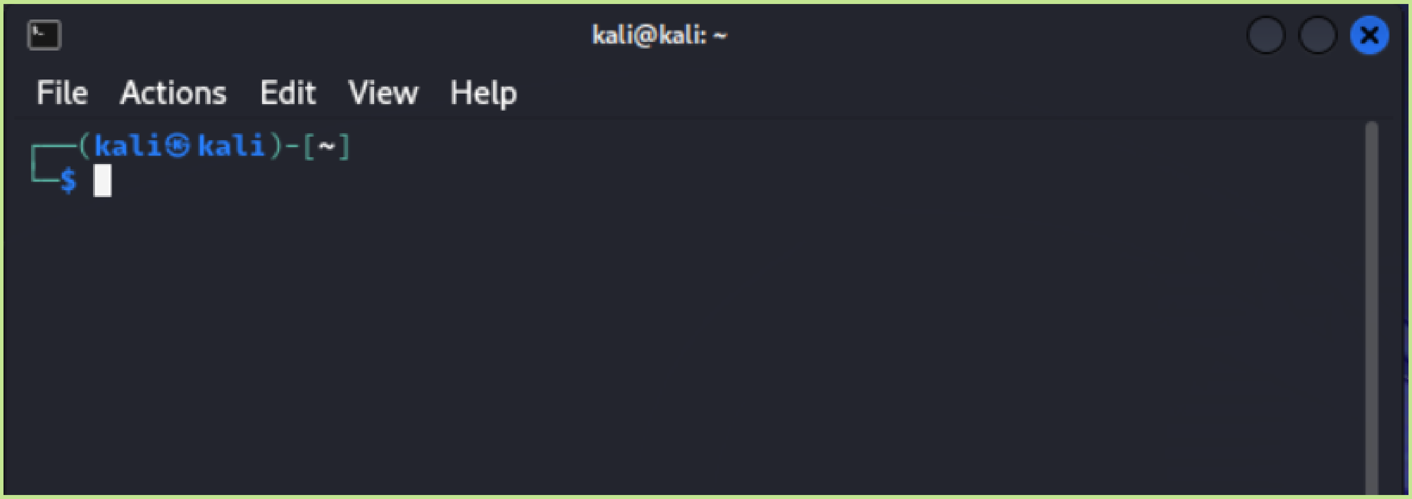
- A terminal, is a text-based interface or command-line interface (CLI) that allows a user to interact with a computer or OS by entering text commands. Users can execute commands, manage files, and perform system tasks by typing specific instructions.

How to Access Nmap Through the Terminal

In your taskbar, which should be located at the top left of your screen, click on the black box with white text that looks like "$_".



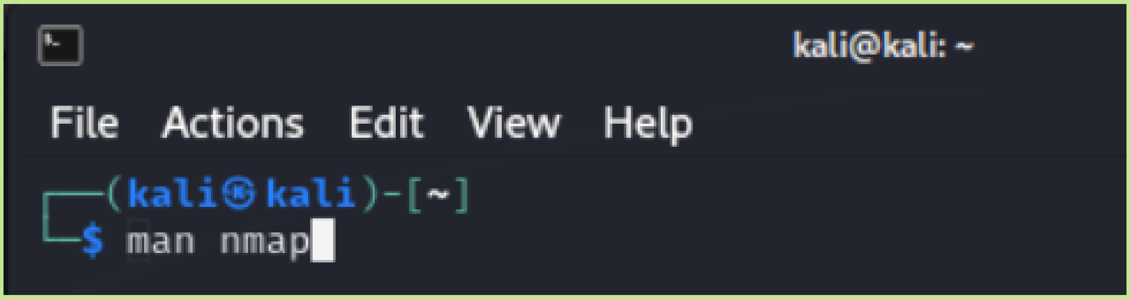
*If the black box isn't there, click on the blue dragon symbol and type "**Terminal Emulator"** into the search bar.*



```
┌──(kali㉿kali)-[~]
└─$ 
```

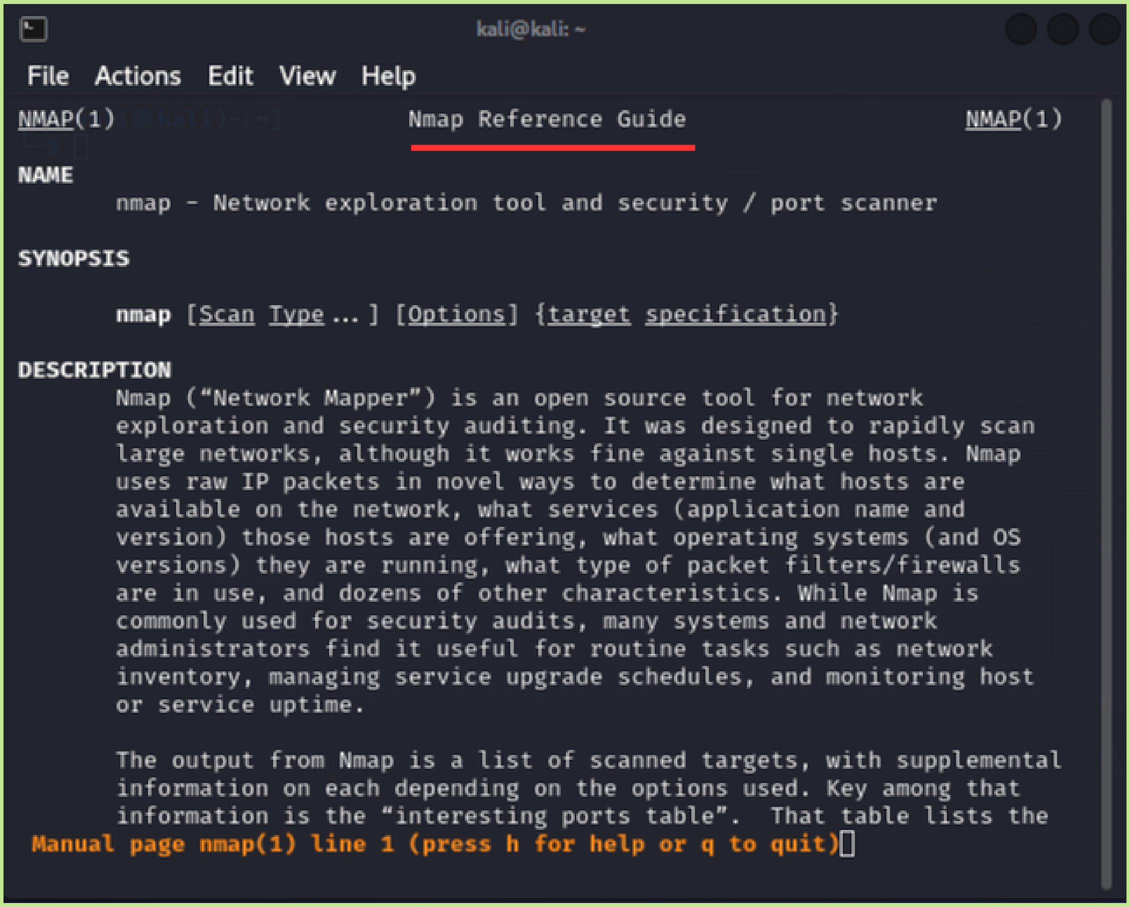
This is what the terminal looks like once it's opened. The default user is "kali@kali".

How to Find the Manual for Commands and Tools



```
┌──(kali㉿kali)-[~]
└─$ man nmap
```

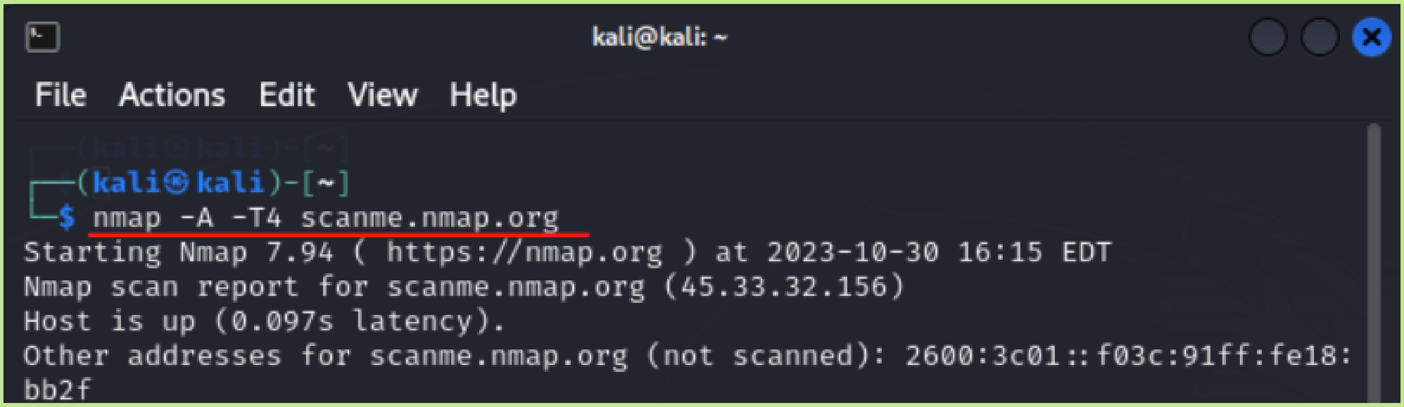
The "man" command displays the manual for the command that can be run in the terminal.



```
NMAP(1)                    Nmap Reference Guide                    NMAP(1)

NAME
       nmap - Network exploration tool and security / port scanner

SYNOPSIS

       nmap [Scan Type ...] [Options] {target specification}

DESCRIPTION
       Nmap ("Network Mapper") is an open source tool for network
       exploration and security auditing. It was designed to rapidly scan
       large networks, although it works fine against single hosts. Nmap
       uses raw IP packets in novel ways to determine what hosts are
       available on the network, what services (application name and
       version) those hosts are offering, what operating systems (and OS
       versions) they are running, what type of packet filters/firewalls
       are in use, and dozens of other characteristics. While Nmap is
       commonly used for security audits, many systems and network
       administrators find it useful for routine tasks such as network
       inventory, managing service upgrade schedules, and monitoring host
       or service uptime.

       The output from Nmap is a list of scanned targets, with supplemental
       information on each depending on the options used. Key among that
       information is the "interesting ports table".  That table lists the
 Manual page nmap(1) line 1 (press h for help or q to quit)
```

Above is the user manual for the "nmap" command

Example 1: nmap -A -T4 scanme.nmap.org



```
┌──(kali㉿kali)-[~]
┌──(kali㉿kali)-[~]
└─$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-30 16:15 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.097s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f
```

What is this command doing?

This command scans **scanme.nmap.org** and reports back the **status**, **latency**, **IPv4 and IPv6 addresses**, **open ports**, and **current OS** of the host.

nmap

- Tells the system that it's going to be using an **Nmap** command

-A

- This option **modifies** the basic nmap scan by requesting that OS and version detection, script scanning and traceroute are all applied. This will make the scan take longer but yield more data.

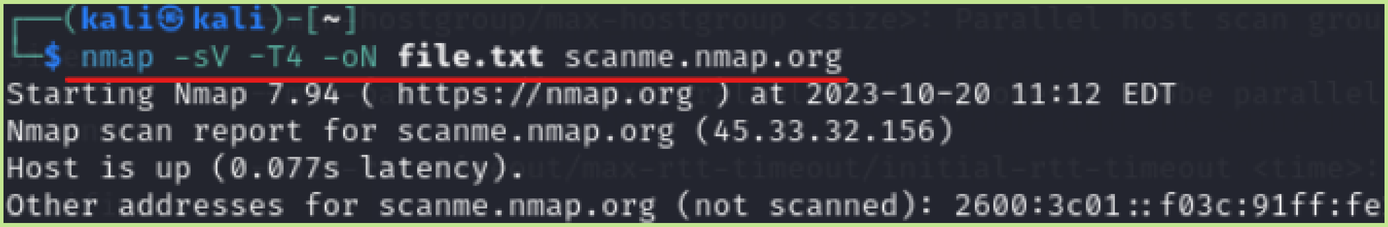
-T4

- This option changes the speed and accuracy of the scan. The -Ts goes from T0 to T5. T0 is the slowest, most hidden, and most accurate scan while T5 is the fastest, loudest, and least accurate. -T4 is almost the fastest since it's only beaten by -T5 in speed.

scanme.nmap.org

- This is the target for the nmap scan, This is a domain name rather then an IP address . You can use either a domain or an IP for a target.
  - this website is a safe way to practice scanning
  - **You should NOT scan networks if you do not have permission to.**

Example 2: nmap -sV -T4 -oN file.txt scanme.nmap.org



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -T4 -oN file.txt scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-20 11:12 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.077s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe
```

What is this command doing?

This command is using **nmap** to **probe** scanme.nmap.org's **ports** to see which services are running and which ports are open. It is also saving the results of the scan onto a file called "**file.txt**"

nmap

- Tells the system that it's going to be using an **Nmap** command.

-sV

- This option requests the scan to also **probe open ports** to find their version and service type.

-T4

- This option changes the speed and accuracy of the scan. -T4 is almost the fastest since it's only beaten by -T5 in speed (see Example 1 for more info).

-oN file.txt

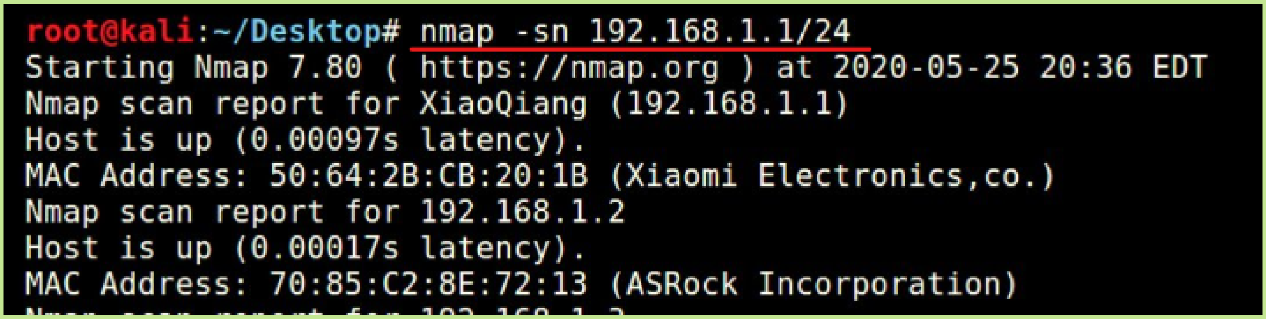
- This option requests the command to save the output from the command to a file called "file.txt".

scanme.nmap.org

- This is the target for the nmap scan, This is a domain name rather then an IP address . You can use either a domain or an IP for a target.
  - this website is a safe way to practice scanning
  - **You should NOT scan networks if you do not have permission to.**

Example 3: nmap -sn 192.168.1.1/24

*****ONLY USE THIS COMMAND ON CONNECTIONS YOU'RE AUTHORIZED TO SCAN*****



```
root@kali:~/Desktop# nmap -sn 192.168.1.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-25 20:36 EDT
Nmap scan report for XiaoQiang (192.168.1.1)
Host is up (0.00097s latency).
MAC Address: 50:64:2B:CB:20:1B (Xiaomi Electronics,co.)
Nmap scan report for 192.168.1.2
Host is up (0.00017s latency).
MAC Address: 70:85:C2:8E:72:13 (ASRock Incorporation)
Nmap scan report for 192.168.1.3
```

Credit: HackerSploit - https://www.youtube.com/HackerSploit

What is this command doing?

This command is doing a **ping** scan to all machines with the IP address through 192.168.1.1 to 192.168.1.256 to see if they're there. It will also check the **MAC address**, which gives the manufacturer details of a device.

nmap

- Tells the system that it's going to be using an **Nmap** command.

-sn

- This option restricts the scan to only a **ping scan**. This means that the ports will not be scanned or probed.

192.168.1.1/24:

- This is the target range for the scan. The /24 states that the maximum is 192.168.1.255. This makes the program interpret the range it is allowed to scan as 192.168.1.1 to 192.168.1.255.

Additional Resources:

Kali Linux Nmap Official Webpage:
https://www.kali.org/tools/nmap/

How to Use Nmap: Commands and Tutorial Guide:
https://www.varonis.com/blog/nmap-commands

Nmap: Usage and Examples:
https://nmap.org/book/osdetect-usage.html

Six Practical Use Cases for Nmap:
https://www.redhat.com/sysadmin/use-cases-nmap

Nmap Tutorial:
https://hackertarget.com/nmap-tutorial/

How to Run a Simple Nmap Scan:
https://www.wikihow.com/Run-a-Simple-Nmap-Scan