**Intro to Nmap**

**What is Nmap?**

Nmap is a free and open-source network scanner. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. We can use Nmap to scan a system and understand what weaknesses exist that an unethical hacker could potentially exploit.

More info at https://nmap.org

**Where can I use Nmap?**

* Nmap is installed into Kali by default. \*There is a cyberlabs tutorial for nmap
* You can also install nmap into your computer by downloading it from <https://nmap.org/download.html>

\*We can scan scanme.nmap.org, as it is a host that was created by the tools developers for practice.

\*\*\*\*\*DO NOT SCAN ANY NETWORKS OR HOSTS WITHOUT THE PROPER CONSENT OF THE OWNER!!!!!!\*\*\*\*\*\*

**How to use nmap on Linux**

* Open the Command Line Interface
* Call nmap by entering the following:

Nmap “*target IP/name” “additional flags”*

* For example, if I wanted to scan the website scanme.nmap.orgwe would type:

Nmap scanme.nmap.org

That’s it, that’s how you use nmap. That’s literally it. Then you read what’s on the screen.

**Task for the day:**

1. Use the command “ nmap -h”. This is the nmap help page. Find a command that seems interesting and try it out in step 3.
2. Scan “scanme.nmap.org”. What ports are open?
3. Scan the same website, but use an additional flag, such as -v. Try to understand some of the information. If you can’t, google it and read about it!

**How to use nmap on windows**

* Sorry, you’re gonna have to google that one :p