Network Scanning Tools

Module 10 | Activity 1

Introduction

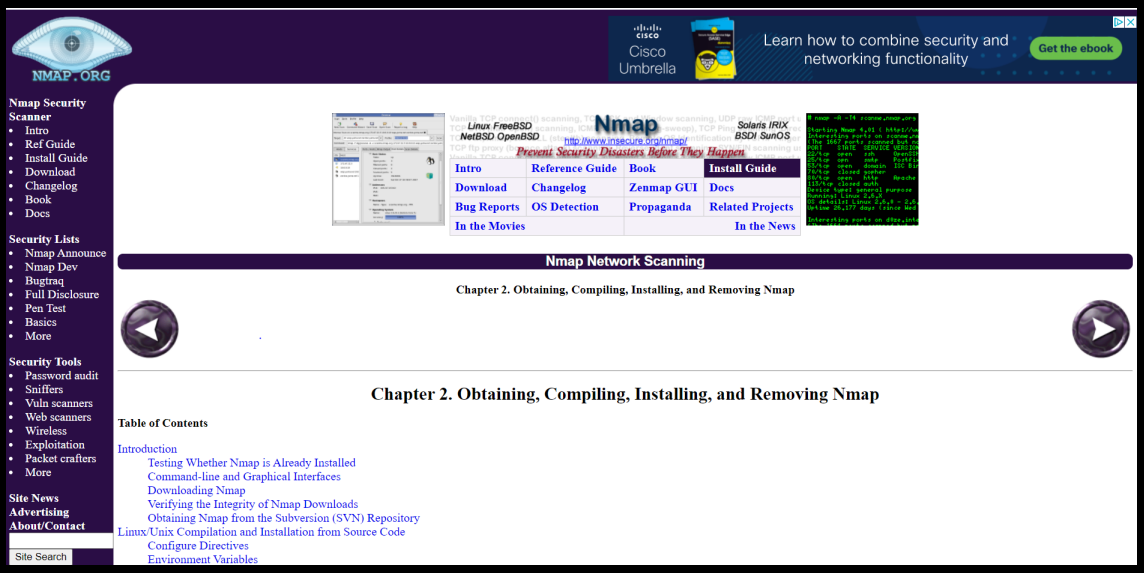
This activity will be focusing on the second step of the penetration test. Network Scanning will allow us to find potential entry ports within a network. For this activity, we will be scanning our own networks. This will be great practice for when your team will have to fix up and protect your given virtual machines for the Cyber Defence Competition. *PRECAUTIONS* DO NOT USE THIS TECHNIQUE OUTSIDE OF ISAEAGE. IT IS ILLEGAL TO SCAN ORGANIZATIONS WITHOUT AUTHORITY.

Getting Started

This activity will guide you through using one of the most common network scanning tools in linux. We will be working with Nmap. Nmap is an abbreviation for Network Mapper. Nmap is a free network scanner that can be used for host scans, port scans, and vulnerability scans. Nmap is known to be very flexible and easy to update which is why it is used by many organizations. Their

website provided very helpful instructions on how to install and test their networking software. They also provide their website as a space to practice your network scanning. Since we headed towards the end of the semester, you all should be comfortable with being about to install softwares on your own. As a team, you will be using https://nmap.org/book/install.html to install and test network scanning with the guidance below. Make sure to have a note sheet or document open to take notes.

A. As a team, pop on over to https://nmap.org/book/install.html by using the link. You should be seeing something like this.



Scroll down to wear "Introduction" and take a minute to read through it.

B. Our next step is to see if Nmap is already preinstalled in our Linux operating system. Your team should see the subtitle "Testing Whether Nmap is Already Installed" under the "Introduction". Read through and follow the steps on how to use the **nmap --version** command to check whether Nmap is installed or not. If it is not, your team will be going

through the steps to install it. If it is installed, WOOHOO! Your team will then update Nmap.

C. Now we are going to move on to the next page by pressing the right arrow at the bottom of the page. It should look a little something like this.

You will then reach the page called "Linux/Unix Compilation and Installation from Source Code". Go ahead and read the first paragraph of this section. You will learn that installing Nmap using source code is the most powerful way of installation, but binary packages are available for most operating systems. Although source code installation may be the most powerful, there is a much faster way to install and update in our virtual machine's linux operating system. Instructions on how are on the next page of the website. Click the right arrow again on the bottom of the page.

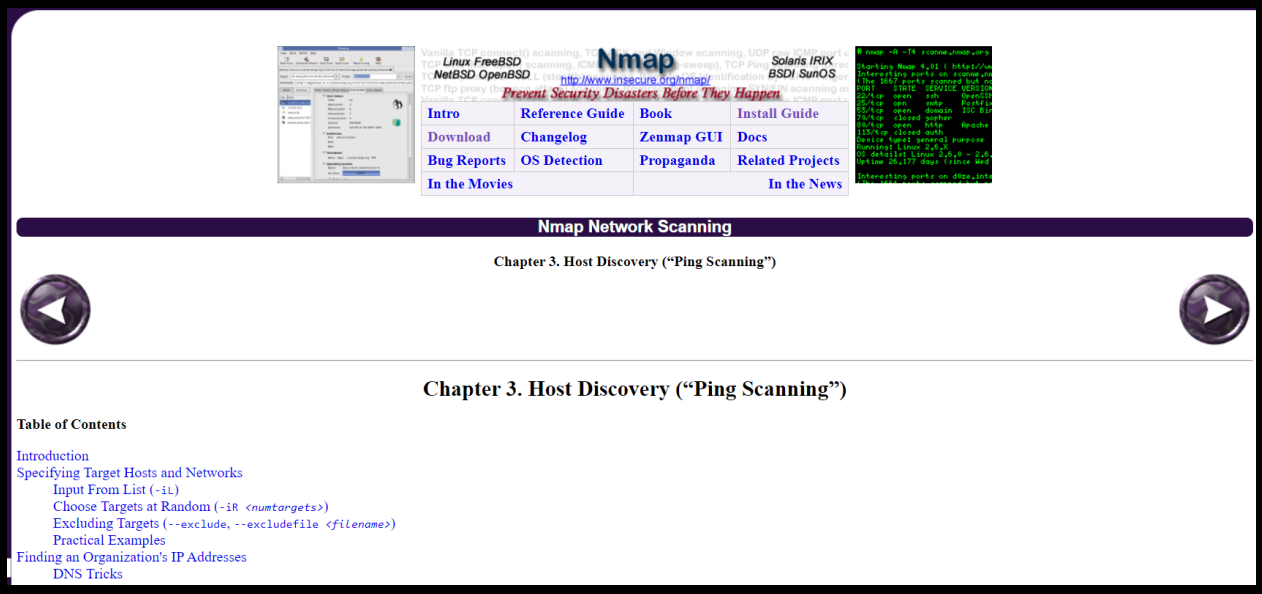
D. After clicking the right arrow, you should be sent to a page titled "Linux Distributions". Have your team take a minute to read the first paragraph. You will learn how binary packages for Linux allow for easier installation.
   a. If you recall, our virtual machines have the Debian Linux operating systems. We will need to scroll down to find the instructions on how to install Nmap for this specific system. The subtitle is called "Debian Linux and Derivatives such as Ubuntu". It may be at the very bottom of the page. Follow the instructions on how to install/update Nmap with the **sudo apt-get install nmap** command. You may have to enter your user password and press "Y" to confirm installation. The

Installation will take about two to three minutes. After nmap has been installed, run the command **nmap** to check if it installed properly. If it did, you will list everything about it.

E. CONGRATS! Nmap is successfully updated/installed on your VM. It is now time to see how it works. *Remember this is a very powerful tool, and should never be used on unauthorized websites or outside ISEAGE.*
   a. As a team, we are going to go over to the following link.

      https://nmap.org/book/host-discovery.html

      It should take you to the page titled "Chapter 3. Host Discovery ("Ping Scanning")"



Read the "Introduction" to get some background information about scanning with Nmap. Click the next arrow on the bottom of the page to reach the "Specifying Target Hosts and Networks" page. Spend a few minutes reading this carefully. It is going to tell you how to enter the specific IP addresses you would like to scan. You could have each team member read a paragraph and example each part to each other to go faster.

F. Now that you understand how to specify IP addresses, we are going to look at another important aspect of nmap scanning. Hop on over to the page titled "DNS Resolution" https://nmap.org/book/host-discovery-dns.html

   Take a moment to understand what data the DNS can tell you in a scan and what **-n**, **-R**, **--system-dns**, and **--dns-servers <server1>[,<server2>[,...]]** commands will do.

   *Try scanning by using the command **nmap scanme.nmap.org** and see what data you get.

G. Click the next arrow to get to "Host Discovery Controls". After going through the page, you should be able to describe what **-sL** , **-sn** , and **-Pn** will do to a scan.

   *Now practice these commands by adding it to the beginning of **nmap scanme.nmap.org** and see what data you receive.

H. Once again, click the next arrow to proceed to the section titled "Host Discovery Techniques". This step would be a good time for your team to spill up the work. Have each person in your group be assigned the following…
   a. TCP SYN Ping
   b. TCP ACK Ping
   c. UDP Ping
   d. ICMP Ping
   e. IP Protocol Ping
   f. ARP Scan

   Have each team member read and take notes on the important commands and information of their scans. After each member is finished, come together as a group to discuss what each scan does. Take note of each of them. Take some time to test each of these scans on **scan.me.nmao.org**.

1. Finally, have the authority to scan only your own IP addresses. Use what you have learned to scan your network with the command **nmap scanme XX.X.XX.X** and see what you get.

CONGRATS! YOU HAVE OFFICIALLY LEARNED HOW TO USE NMAP FOR NETWORK SCANNING.

**If you would like to learn a little bit more about Nmap go on over to https://nmap.org/book/history-future.html to look at the history and future of Nmap.