Hidden Target Teacher Instructions

Introduction

Welcome to your *Hidden Target* workout, in which you will exercise your ability to perform the early stages of cyber reconnaissance. When performing security tests on a system, network scanning is crucial in determining possible attack vectors a hacker could leverage to gain access to the system. Depending on the scan results, a lot can be learned about the target including any services and operating systems used along with the associated versions. For example, if attackers scanned a network and discovered that a machine on the network was running Windows 7 for the operating system, they might try using a popular exploit called *Et ernalBlue* to control and take down the system.

For this workout, you will be using a popular scanning tool, *Zenmap* (*the GUI version of Nmap),* to learn about a network and discover a hidden target.

Your Mission

- Once logged in, open the *Zenmap* application on your machine by going to *A pplications Internet Zenmap (run as root)*
- When prompted, enter the password, *Let's workout!*
- Perform a quick scan of the network, *10.1.1.0/24*

> This is known as CIDR (Classless Inter-Domain Routing) notation. It's a quick way to say, "I want to scan everything from 10.1.1.0 through 10.1.1.255. An IP address can be divided into a network portion and a host portion. The /24 refers to the number of bits used for the network, which in this case is "10.1.1". Don't worry too much about this right now.

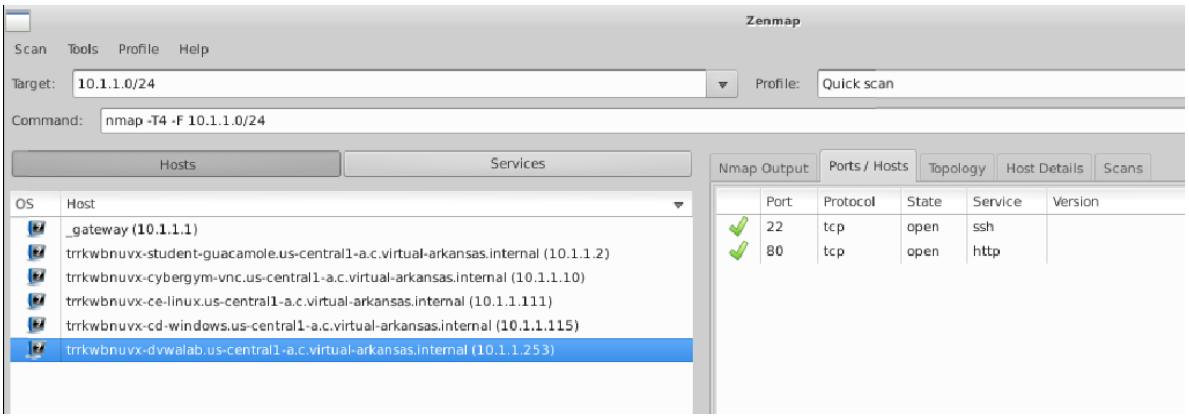
- Look for any ports that might provide you information about the hidden target. Check out this website for some common network ports to search for: https://en.wikipedia.org/wiki/Port_(computer_networking)#Common_port_numbers

Your mission is to find a host with the following secret emblem as one of its services. Then answer the following questions about the workout.

Assessment Questions:

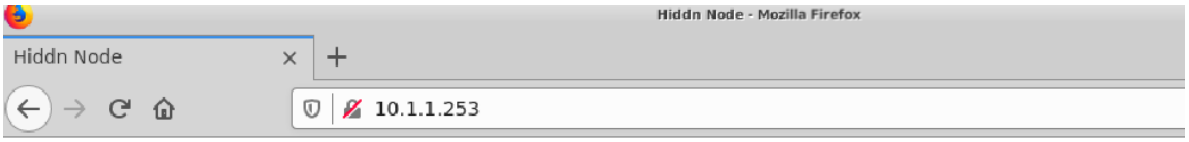
- How many *unique* IP addresses were discovered by the scan?

The following screenshot shows something similar to what the students would see. They can expand out the host frame to see the full IP addresses. You can click on each address and get the ports/hosts over to the right. In this screenshot, the target system is highlighted (IP address 10.1.1.253), and they will be looking to see port 80 as the service they need to further explore.



- What is the IP address of the hidden target?

The student will open a browser and type in http://10.1.1.253 to access the page shown below.



- What was the port number used to access the hidden target?

The port number is 80. This corresponds to TCP port 80, which they can look up and find is the default port for HTTP. Looking up the port number usage should direct them to check for the emblem using their browser.