Topic: Introduction to nmap

Objectives: After completing this activity the student will be able to:  
 1. Explain both the purpose and function of nmap 2. Run a network sweep on a target network 3. Perform both TCP connect and TCP SYN scans 4. Identify both vulnerable and protected ports on a target machine 5. Identify characteristics of a target machine

Watch the “Introduction to nmap” video (22:00).

* <http://dhsaoit.org/cyber/nmap_intro/Introduction%20to%20nmap_big/index.html>

This video is an introduction to the nmap tool and is the first of a series of modules using nmap. The video discusses the methods of five fundamental scan types used in nmap and uses a network of 4 virtual machines for the explanation. Each of the packet capture files used in the video are available for download.

After completing the video there are 5 packet capture files for download and a series of questions.

* sample pcap files:  <http://dhsaoit.org/cyber/nmap_intro/packet_captures/>
* challenge pcap files:  <http://dhsaoit.org/cyber/nmap_intro/challenge_files/>

Download the 5 packet capture files and use Wireshark to analyze the file and answer the following questions and use the 5 nmap scans types seen in the instructional video.

**Capture1.pcapng**

1. What type of scan is most-likely to have been run?   
   Click here to enter text.
2. What is the exact syntax of the command?  
   Click here to enter text.
3. What is the result of the scan?  
   Click here to enter text.
4. What are the machine types of vendors of machines seen in the scan?  
   Click here to enter text.
5. What is the MAC address of the machine that is running nmap?   
   Click here to enter text.
6. What is the IPv4 address of the machine that is running nmap?  
   Click here to enter text.
7. What is the IPv6 address of the machine that is running nmap? \*bonus question  
   Click here to enter text.
8. List the four MAC addresses of devices on the network:  
   Click here to enter text.

**capture2.pcapng:** This is an OS scan. Look at the file and answer the questions

1. What is the exact syntax of the command?  
   Click here to enter text.
2. If this is between two machines on the local network, why are there packets from other hosts?  
   Click here to enter text.
3. According to the capture file, what service(s) are responding on the target?  
   Click here to enter text.
4. Which packet numbers are checking the Telnet service?   
   Click here to enter text.

**capture3.pcapng**

1. What type of scan is most-likely to have been run?  
   Click here to enter text.
2. What is the major clue to the type of scan?   
   Click here to enter text.
3. What is the exact syntax of the command?   
   Click here to enter text.
4. According to the file, what port(s) are listening on the target?  
   Click here to enter text.

**capture4.pcapng**

1. What type of scan is most-likely to have been run?   
   Click here to enter text.
2. What is the major clue to the type of scan?   
   Click here to enter text.
3. What is the exact syntax of the command?  
   Click here to enter text.
4. What common service and port number is active on 2 of the devices, and which are the two?  
   Click here to enter text.

**capture5.pcapng:** This is a version scan. Look at the file and answer the questions

1. What is the exact syntax of the command?   
   Click here to enter text.
2. The target represents an Internet facing server, what service(s) are running on that server?   
   Click here to enter text.
3. What operating system is the target running?  
   Click here to enter text.
4. What protocol is running that shows the OS of the target?   
   Click here to enter text.
5. What is the hostname of the target?   
   Click here to enter text.
6. What protocol is running that shows the hostname of the target?  
   Click here to enter text.
7. What is the hostname of the machine running nmap?  
   Click here to enter text.
8. What service is allowing the hostname of the machine running nmap to be seen?   
   Click here to enter text.