Lab 12

Quick Qanda

- 1. What is meant by a *half-open* scan?
 - a. A scan is half open if the client does not ack the servers response.
- 2. What is the significance of a port number?
 - a. Some port numbers typically used by specific protocols. For example ssh usually uses port 22. Http uses port 80, and https uses 443.
- 3. Is there anything stopping you from running SSH on something other than port 22?
 - a. No smiley face
- 4. How could a firewall easily detect a port scan?
 - a. If someone tries port 1, then port 2, then port 3, etc. in sequential order the firewall could see that and then add them to the deny list.
- 5. In what ways could an attacker make a port scan stealthier?
 - a. The attacker could scan the ports in a random order.

Local Enumeration

It is very important to be aware of what services are running on your servers. Since there is a local firewall running, you may also want to scan from an external host to see which ports are "open" to the public.

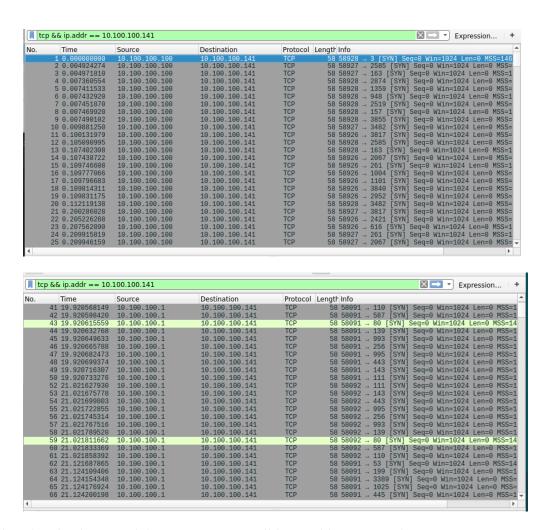
- A. Install nmap (network mapper) on node1 and main
- B. What ports are open locally on node1?
 - a. sudo nmap -sS -p1-4096 127.0.0.1
- C. Does this match the output from the SS command?

- a. Almost all of the ports match but we can see an extra port in ss. We see 53 in ss but not in nmap.
- D. Using SS, are there any UDP sockets listening?
 - a. There are no listening UDP sockets, they are all "UNCONN".

Non-local Enumeration

When you run a port scan, you are attempting to connect to the host. Many firewall appliances can detect a port scan, can you?

- 1. On node1, open Wireshark and keep an eye out for someone scanning you.
 - 1. Can you tell that your lab partner is port scanning this machine?
 - i. yes
 - 2. Is there an order to which ports are checked by nmap?
 - i. It looks pretty random
 - 3. On ports that were open, did nmap complete the three-way handshake?
 - i. No.
- 2. Meanwhile, from main, scan TCP ports 1-4096 on node1
 - 1. What ports are open?
 - i. 22, 80, 443
 - 2. Are the results different than the scan results in *Local Enumeration*?
 - i. Yea. We found less ports.
- nmap claims to have some super sneaky scan methods, look through nmap --help and try out various options
 - 1. What options did you try?
 - i. -S to spoof the source address
 - ii. --badsum to include a bogus "checksum"
 - 2. What shows up in Wireshark for each one?
 - i. When we spoofed, it showed the address we spoofed started port scanning instead of our own address. Professor Scrivnor port scanned us :(.



ii. The checksums of the messages sent did not add up correctly.