PenTest Lab Exercise Ex040 – `Wireshark`

Goal

Learn about how to use `Wireshark`.

Tasks

1. Log in to the Netlab server, schedule the PenTest Ex040 Lab, start up the lab, then log in to your Kali VM.

2. Identify your active ethernet interfaces by executing `ifconfig` or by executing `ip a`.

3. Fire up `Wireshark`.

4. Start a `Wireshark` session on your active Ethernet interface by double-clicking on the interface name on the Welcome panel.

5. Provide some data to Wireshark by executing the following command:

   ```
   traceroute -I plunder.pr0b3.com
   ```

   By way of explanation, linux `traceroute`, by default, sends UDP packets rather than an ICMP echo (partly because so many machines ignore ICMP echo). The -I parameter will cause an ICMP echo packet to be sent. Parameters to traceroute can specify other ports and protocols. Check this out by executing

   ```
   traceroute --help 2>&1 | less
   ```

   (What's that `2>&1` thing all about? BTW, when I ask such questions, it means it's important for you to find out the answer but not necessary to include in your report!)

6. Stop the `Wireshark` session by clicking the square red stop recording button. You can start a new session by clicking the blue shark-fin button. There's no need to save the packets for this assignment, but you can experiment with saving them and reloading them if you want to.

7. Take note of how many ICMP packets you find with different sources and destinations. It may help you to enter the string `ICMP` into the `Wireshark` filter input box.

   Check the TTL field in each of the packets you see sent from your host (check the Source column for your IP address). Try this several times to make sure you understand what's happening. How many pings does `traceroute` send out before it stops? Does it need to send them all? If you find any ICMP packets that you don't expect to see, inspect them to understand what's happening. There's really not much traffic on this network, so this shouldn't bog you down.

8. Use `traceroute` again to identify the path to `ns.artstailor.com`.

9. Write and submit a report about what you did in this exercise. Although this activity involves both passive and active intelligence (you're both listening and eliciting active responses), you only need to provide an attack narrative because this really isn't part of a penetration test. No Mitre ATT&CK Framework TTP is necessary.

   Explain the host responses to `traceroute` and discuss what you would do if a host did not reply to ICMP ECHO requests or to requests to other default ports. (You may want to consult the `traceroute` man page.) Don't forget that your report should answer any non-parenthesized questions asked in this exercise.

Question

Did you find a key? There was one available today.