Ex040–Wireshark

Welcome to Penetration Testing and Ethical Hacking at the University of Florida, this is pen test exercise hex 040: Wireshark. In this exercise your goal is to learn a little bit about Wireshark you can't learn everything there is to know in the context of the same exercise don't worry there's a lot to this tool.

You need to log into the net lab server get your pen test for lab log into kali VM. Once you're there you'll want to look at the interfaces that you have available to you the network interfaces you can use ifconfig or (if config, some people will say) and "ip a" these are two commands you can do to look at that you can use to look at the active network interfaces. The one you'll be looking for is the one that's 172.24.0.10 or 11. That's the active interface, that is, on the network that you're interested in. Probably eth0.

Fire up Wireshark. You can find that by, there are several ways to: you can run a command line is Wireshark you need to run you run that as sudo, I believe. You can get it from the menu as one of the sniffing tools, there are a variety of ways to start up. You need to start a Wireshark session on your active ethernet interface by double clicking the interface name on the welcome panel. And then you'll provide some data to actually capture by running a program and i'm going to ask you to run `traceroute -I plunder.pr0b3.com`. And if your network interfaces not active during all of this, it will not show up. Remember look for the spinning icon in the in the upper right corner, it takes about a minute for the router to complete its job. It delays, a little bit, it pauses when it's starting up DNS services

So the `traceroute` command sends, normally sends UDP packets, rather than ICMP ECHO. Although you may have heard of trace route uses ICMP ECHO and you know `-I` parameter will override that and use ICMP ECHO. So you'll see ICMP ECHO packets being used if you use -I.

The parameters to `traceroute` can specify different ports protocols other other possibilities, there are a number of different possibilities, you can find out about all of them by running `traceroute --help 2>1 | less`. I suggest you use the 2>1 and pipe that into less so that you can see it a

page at a time instead to interested in person, one thing about. Find out. It's worth finding out about, but don't report on it, all right?

You can stop your `Wireshark` session by clicking the square red stop-recording button looks like a stop-recording button, you can start a new session by clicking the blue shark-fin button. You don't need to save the packets, you can save them if you want to find out about `Wireshark` you can also one `Wireshark` from a file, so you get information from a file.

I want you to note how many ICMP packets you find that have different sources and destinations as a result of the trace route. It may help you to enter the string ICMP into the `Wireshark` filter by output box when that's green you've entered a usable filter and you can check the TTL, the time to live that, check that field in each of the packets that you see sent from your host to see how trace route really works. And you should try this several times to see what's happening.

How many pings does trace route send out before it stops sending? And does it need to send them all? And if you find any ICMP packets that you didn't expect to see you probably want to look at them and see what's happening. It's really, there is not much traffic on this network. There are no other users, besides you right now pretty much–and maybe some scripts that run on different machines, maybe looking for name service or other other capabilities.

So you should use `traceroute` to identify the path to ns.artstailor.com as well, and then, write and submit a report about what you did in the exercise.

The `traceroute` that you do to artstailor.com, you might consider that to be part of a pen test but i'm not going to consider it to be that at this time, so only report an attack narrative in your in your report. You don't need to provide any other information besides the attack narrative.

You should explain the host responses that `traceroute` generated. You should discuss what you would do if a host didn't reply to ICMP ECHO requests or to requests from any other of the default ports–you might want to consult the trace route man page to think about this and see what you might do.

Of course, don't forget in your report to answer any non parenthesized questions I asked in the exercise that are demands on you not suggestions for further learning.

There is a key available, you can find it. If you have questions: discord, office hours, other humans–all all good. I'll see you in the next class.