Session Three – Passive Reconnaissance with Wireshark

Passive reconnaissance aims to gather info on an adversary and their networked machines without giving away our presence. Through picking up packets on a network they use, we can work out the hosts and services they are using and potentially even glean key information from those packets.

Part 0 – Installing Wireshark

- The WireShark tool can be downloaded for all major OSs from www.wireshark.org/download.html -it is GUI based and may prompt you to download a couple of additional drivers.

Part 1 – Wireshark fundamentals

- Head to this wireshark tutorial and work through 5.2.1-5.2.6 to gain an understanding of the basic means of operating Wireshark. This will provide the foundation for the following sections.

Part 2 – Finding the juicy stuff

Even a short packet capture can generate thousands of packets so if we want to be able to perform long term cyber recon we need to be capable of sifting through that effectively. We have learnt the basics of this in Part

- Start a new packet capture and visit the cyberbulls.net website
- Filter your capture to just show packets resulting from the DNS protocol. What DNS lookups have been taking place?
- The follow stream tool is particularly useful in that allows us to track two machines exchanging packets over a given protocol.

Apply a conversation filter to one of the DNS request packets. What was the response?

Part 3 – Applying our skills to recon

With our newfound skills not only can we see host IP and services on the network but we may be able to gain critical info such as access creds via non-encrypted protocols.

- Open the telnet packet capture from the resources page. Analyse the packets contained to find the username and password of the person using the telnet protocol and the name of the website they pinged.
- Next look at the http packet capture file. What was the nature of the data being sent? Which type of HTTP request was used? (e.g. GET, POST, PUT etc.)

Part 4 – Extension - Moving on to defence

- Using your skills from last week, run a regular NMap scan against a target while running a capture on wireshark. Filter the capture for packets sent from your own IP. Can you spot the packets sent by the NMap scan?
- Work with another cyberbulls member to scan each other without saying exactly when you are doing the scan. Can you find the packets? Try it again with a stealth scan – how does that differ?