# Session Two – Reconnaissance with NMap

This session, we look at the first step in the cyber killchain – scoping out the target. Using the NMap tool we will be scanning targets to identify their network and see what services they are running – which will provide a means of attack.

## Part 0 – Installing NMap

The NMap tool can be downloaded for all major OSs from nmap.org - many linux distos such as Kali will come with it pre-installed. The tool features a command line tool and a GUI (called ZenMap) which can also be used.

## Part 1 – Basic scanning

- Use NMap to do a quick scan (-F) of the cyberbulls website – what services is it running?
- Try scanning a couple of other sites you know – what services are they running? What do those services do?

## Part 2 – Network Exploration

Using NMap by providing a domain name (URL) is great when we already know what we are looking for, but often we will want to find other machines on the network, which might not publicly announce their location.

- Perform a scan for the bbc.co.uk website – what is its IP Address?
- Modify your scan to search for a range of addresses near this IP. What other hosts on the network can you find?
    - Think about what would be a sensible range to scan. For most subnets the router is going to be on an IP of X.X.X.0, with hosts starting from X.X.X.1 going upwards.
- Find the IP Address for one of the bbc file transfer servers?
    - What service would a file transfer server be running?
    - The bbc has multiple file transfer services. Can you find any more?

## Part 3 – Probing services

Once we have found hosts on a network, the final step is to probe hosts we are interested in to find out more about them. We can use the fingerprinting tools within NMap to find out information such as the OS of the host and the version of services it is running. This will help us choose which exploit to target it with.

- Scan the cyberbulls website with version detection and OS detection enbaled.
    - Which framework is being used to run the web server (http)?
    - What type of OS is the server likely to be run on?
- Do the same for the bbc file servers identified in Part 2. What are you able to find out?

## Part 4 – Extension

At this point feel free to play around with the scanning tools and techniques you have learnt by scanning other addresses across the web (scan in moderation and stick to commercial networks rather than government bodies etc). If you want to learn even more, try the bullet points below.

- When performing cyber recon we don't want the target to know that we are scanning them. What tools does NMap have to aid with stealthy scanning? How does this affect performance?
- Some services are particularly useful to find when trying to exploit a system. Telnet is one such service. Why? What other particularly vulnerable services would provide a potential goldmine?