Session 02 – Enumeration of Target Computers

What will we be covering

Session 02 is designed to teach you the fundamentals of target enumeration, which is the process of gaining information about your target before you hack them.

The session content will be split into three different things

- Basic port scanning using Masscan
- Advanced port scanning using Nmap
- Subdirectory and subdomain enumeration with ffuf

For port scanning, we are covering both Masscan and Nmap as while Nmap has more advanced scanning functionality, Masscan is an extremely fast port scanner which can far outpace nmap. As such, people often start a scan with masscan to find open ports, then scan for details using nmap.

Starting the Session

It should be noted that for most of the planned content for this session, you will require an account on TryHackMe (https://tryhackme.com/). I have specifically selected the free content on TryHackMe for this session.

Using Masscan

For a basic understanding of how to use masscan, I would recommend experimenting with how to use masscan to scan the domain "scanme.nmap.org". You should be able to see the 4 open ports on the domain. The Github repository for masscan can be found at https://github.com/robertdavidgraham/masscan (read the README for basic documentation, or use google…). You should be able to finish this in around 20 minutes.

Using Advanced Nmap

If you have signed up for TryHackMe, you should be able to access the Nmap content at https://tryhackme.com/r/room/furthernmap. You should be able to go through the whole content within session 02. As you follow along with the theory of nmap, I recommend testing out some of the commands against the provided machine.

To start with TryHackMe, I recommend looking at how to connect your Kali VM to TryHackMe using Openvpn, instructions which can be found at https://tryhackme.com/r/access. A basic tutorial to make sure that your Openvpn software

is working can be found at https://tryhackme.com/r/room/tutorial. Make sure to read the openvpn-specific information on both links.

Using ffuf

Ffuf (Fuzz faster U fool) is a well-known enumeration tool that can be used to search for subdirectories, files, and subdomains of a website. The learning material for ffuf can be found at https://tryhackme.com/r/room/ffuf. We expect you to work on this topic and complete this during the drop-in session.

Ffuf requires that you tell it what to look for by providing it a wordlist of guesses. Generally, the seclists repository (https://github.com/danielmiessler/SecLists) is a fairly good choice, and should already be installed with Kali. You may need to look into where your copy is installed on the VM.

Assorted Reading Material

- https://allabouttesting.org/nmap-vs-masscan-which-one-is-better/ - Basic comparison of masscan and nmap
- https://nmap.org/
- https://github.com/ffuf/ffuf