Nmap Cheat Sheet

This room covered the following types of scans.

Port Scan Type	Example Command
TCP Null Scan	`sudo nmap -sN 10.10.149.1`
TCP FIN Scan	`sudo nmap -sF 10.10.149.1`
TCP Xmas Scan	`sudo nmap -sX 10.10.149.1`
TCP Maimon Scan	`sudo nmap -sM 10.10.149.1`
TCP ACK Scan	`sudo nmap -sA 10.10.149.1`
TCP Window Scan	`sudo nmap -sW 10.10.149.1`
Custom TCP Scan	`sudo nmap --scanflags URGACKPSHRSTSYNFIN 10.10.149.1`
Spoofed Source IP	`sudo nmap -S SPOOFED_IP 10.10.149.1`
Spoofed MAC Address	`--spoof-mac SPOOFED_MAC`
Decoy Scan	`nmap -D DECOY_IP,ME 10.10.149.1`
Idle (Zombie) Scan	`sudo nmap -sI ZOMBIE_IP 10.10.149.1`
Fragment IP data into 8 bytes	`-f`
Fragment IP data into 16 bytes	`-ff`

Option	Purpose
`--source-port PORT_NUM`	specify source port number
`--data-length NUM`	append random data to reach given length

These scan types rely on setting TCP flags in unexpected ways to prompt ports for a reply. Null, FIN, and Xmas scan provoke a response from closed ports, while Maimon, ACK, and Window scans provoke a response from open and closed ports.

Option	Purpose
`--reason`	explains how Nmap made its conclusion
`-v`	verbose
`-vv`	very verbose
`-d`	debugging
`-dd`	more details for debugging

Conclusion:

This was an excellent module that branched off from the basic port scans we can do and what happens if there are filters involved. This build off that into real world scenarios, as well as how to remain anonymous with our traffic and bypass things such as firewalls, or IDS using zombies or packet segmentations, such as using -ff to break out traffic into smaller segments making it harder to trace anything malicious.

Overall this module has been very interesting from both an offensive standpoint but also a defensive perspective. Because I can both see the advantages and disadvantages of both sides. Why I said that,

Offensively this is great because it allows you to bypass some security protocols, such as the IDS, or firewalls. This is important because not only does it help you go undetected but also makes it easier to cover your tracks, which is paramount to a successful attack, what is the point of an attack if you get discovered, it makes it more likely for the attack to be reversed or for you to be discovered entirely.

Defensively, this is harder to spot, because if you rely solely off a IDS or firewall it's hard to detect an attack is even occurring, but there is tools around this such as those which enable the defender to inspect data in finer detail, such as reassembling data that has been segmented to better understand the intent behind data.

Overall this has been a very big insight and I am very excited to continue this path to learn more.