NMap

Forget about **ZMap** and **UnicornScan**, they have their place. NMap is far more versatile...**Learn to use it well**.

If your command does not have at least 5 flags you are not using it correctly.

Side Note: Nessus is dumb in port/host discovery. Give it very specific tasks.

How You Run NMap is Important

- If you are NATed and use **-sS** (default) it will take your hours for a full scan of a Class C.
- If you are bridged and use **-sT** it will take 10mins for a full scan of a Class C.

NMap in Phases

Host Discovery

- Pingsweep happens by default (disable with -Pn)
- Pingsweep does 4 things. 2x ICMP 2x TCP
- Use **-PE -sP** if you know host responds to ping, this is way faster
- Get a list of live hosts by grep'ing the .gnmap for up hosts

Not all hosts respond to a ping. Discovery with common ports (21,22,80,443,445,3389,etc), a fast scan **-F or --top-ports 1000**

Ensure No Sensitive Host

- See below on "wrecking everything"

Full Scans

- You do not want to go in guns blazing with **-A**...yet
- Get a list of open ports **-p-**
- Then look into each port or set of ports bit by bit. This will reduce the risk of overloading the server, and if something breaks you know what broke it.

Service Identification

- Common Ports
- -sV and --version-all
- Google

Scan Types

- -sS: Steal Scan. Was useful back in the day, most IPS/IDS' will find this now
- -sT: Standard 3 way handshake probe, generally faster...especially on internal networks
- -sU: UDP Ports
- RTFM. Don't be a Skiddie

UDP Scans

- UDP is a fickle child, it will only respond to the correct probes/data
- -sU -sV --version-all
- Doing full scans against UDP will take a lifetime. Choose some specific common ports (53,69,161,etc) and top 100/1000

Useful Flags

- --randomize-hosts
- --top-ports 2000
- --min-hostgroup #Changes the number of hosts to scan at once
- -T4 Change the timing options
- --max-retries 2
- --proxy #Lets you scan through SSH etc

NMap Can Wreck Everything

- Some devices such POS/SCADA are fragile.
- Do an OS scan with top 20 ports to identify these
- -sS can break older OS's as they will keep the connection open for each probe

Interesting Scans

- nmap -sT --script=broadcast –nvv –oA broadcastscan #Finds some interesting ranges/hosts
- nmap -sT -nvv -Pn -p 22,139,445 -min-hostgroup 256 -T4 -max-retries 2 -oA getstarted.txt --script=smb-os-enum 10.1.1.1/23 #Quick scan at the beginning of the test to give you something to look at

SSLWrapped

- If nmap comes back with ***sslwrapped*** you need to dig deeper
- Connect with stunnel, then nmap your localhost

IPv6

- Firewalls are often neglected on IPv6. Find those holes

JumpBox/Citrix/etc

- Windows
  - PowerShell to the rescue: https://gallery.technet.microsoft.com/scriptcenter/Invoke-TSPingSweep-b71f1b9b
- Linux
  - SSH Dynmaic Port forwarding and ProxyChains
  - nmap --proxy

Overnight/Long Running Scans

- Place all IPs in a file.
- Randomise file ***sort*** **-R**. This will reduce the load on each subnet.
- Place hosts in a **for loop.** Doing them one by one also help restarting them should they fail. Will also only get output once scan is complete.
  - for ip in $(cat randomised-ip-list.txt); do nmap -nvv -Pn -sT -sV $ip -p- -oA $ip; done