Ultimate Cheat Sheet: Scanning

nmap

```
//Ping sweep
nmap -PS [IP Range]

//Service Scan
nmap -sV [ADDR]

//Service scan for UDP
nmap -sU [ADDR]

//Host protected by a firewall (no ping)
nmap -Pn [ADDR]

//Fast scan:
nmap -T5 [ADDR]

//Aggressive scan all ports
nmap -A -p- [ADDR]

//Scan for SMB Vulnerabilities
nmap --script smb-vuln* [ADDR]
nmap -p 139, 445 --script=smb-vuln* [ADDR]

//Host Discovery (no port scan only ping)
nmap -sn 10.0.0.0/24

//Scan 1024 most common ports and run default scripts
nmap -A -oA nmap [ADDR]
```

```
//Scan all ports, with a full connection scan
nmap -v -p- -sT [ADDR]

//Running nmap scripts
nmap -p [PORTS] --script=[SCRIPTNAME] [ADDR]

//Banner Grabbing
nmap -sV --script=banner [ADDR]

//TCP SYN Scan
nmap -sS [ADDR]

//TCP ACK Scan
/*You might use this scan type to identify if a host is
using a firewall, and if they are what type of
firewall rules they might be using, by determining which
ports are filtered, and on a filtered port
whether the packets are dropped or rejected.*/
nmap -sA [ADDR]

//TCP FIN Scan
/*You might use this scan type on a host with a firewall as
it is not as common for firewall rules to
block packets with the FIN flag set. It may also allow the
attacker to predict which ports have
services running on them by taking the complement of which
ports are closed.*/
nmap -sF [ADDR]

//TCP Connect scan
/*
This type of scan might be used when the user does not have
```

```
the privileges to run another TCP
scan type. This scan type does not write raw packets
instead it uses the operating system to
establish a connection with the target by using the connect
system call.
*/
nmap -sT [ADDR]

//Operating System Detection Scan
nmap -O -v [ADDR]

//Operating System Scan: show possible matches
nmap -O --osscan-guess -v [ADDR]
```

Miscellaneous

```
//ping sweep: single device
ping [ADDR]

//ping sweep: entire network: (ex. Range
192.168.0.0-192.168.0.255)
for i in {0..255}; do ping -c 192.168.0.$i | grep 'from';
done

//fping: tool for ping sweeps
//-a - force tool to show only live hosts, -g - specifies
ping sweep
fping -a -g 192.168.0.0/24
fping -a -g 192.168.0.0 192.168.0.255

//netdiscover - ARP scanner to scan for live hosts in a
```

```
network
netdiscover -r 192.168.0.0/24

//masscan with interface tun0 scan ports 1-65535 TCP and
1-65535 UDP at the rate of 1000 packets per second

masscan -e tun0 -p1-65535,U:1-65535 [IP ADDR] --rate=1000
```