Active Scanning and Vulnerability Scanning

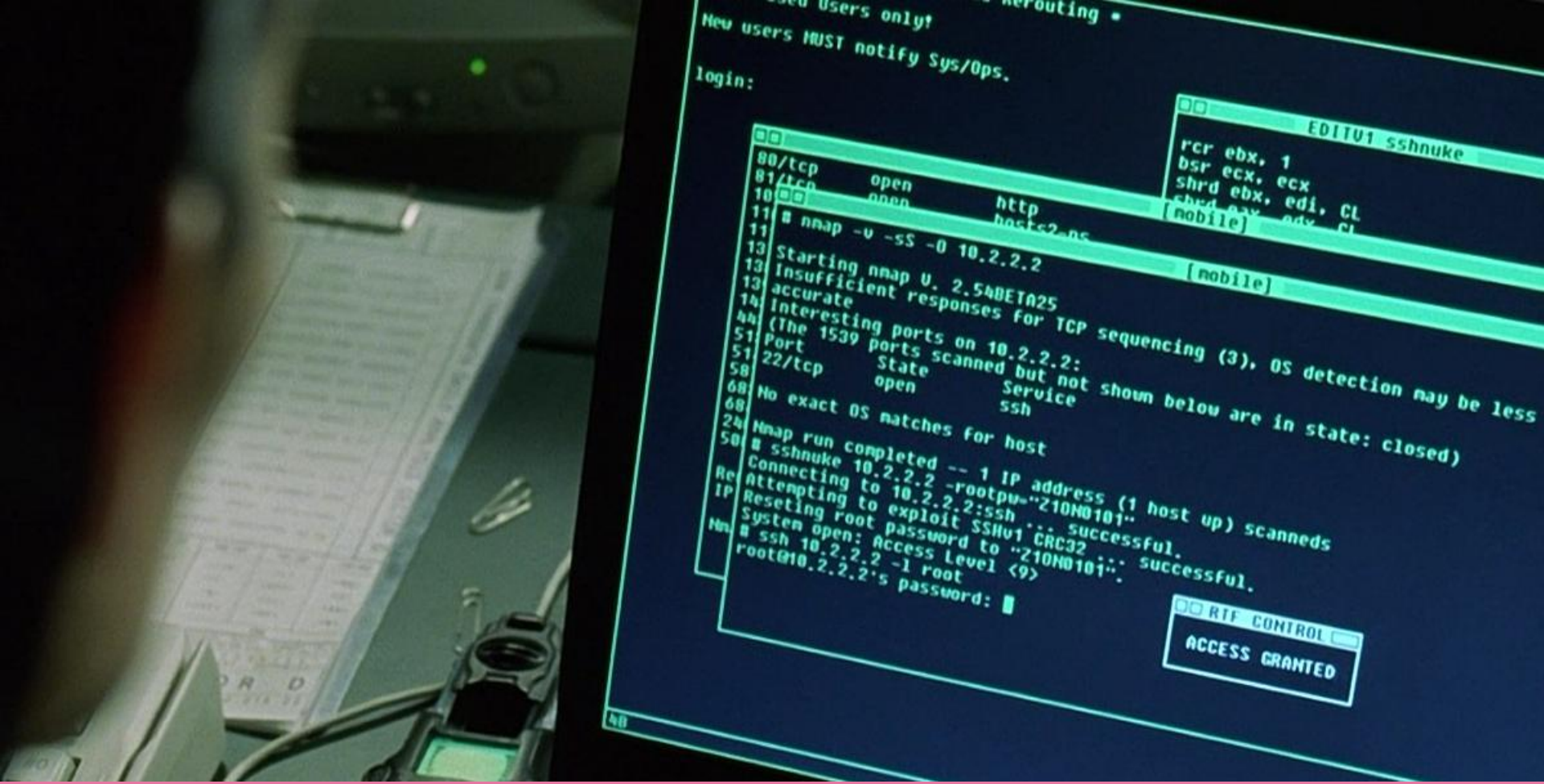
No plans survives it's first engagement with the enemy

What are active scans?

- Active scans hit actual target infrastructure
- They can be traced with decent IDS and logging
  - *Mostly*
- Helps get a clearer picture of what's really happening on a target network

Nmap

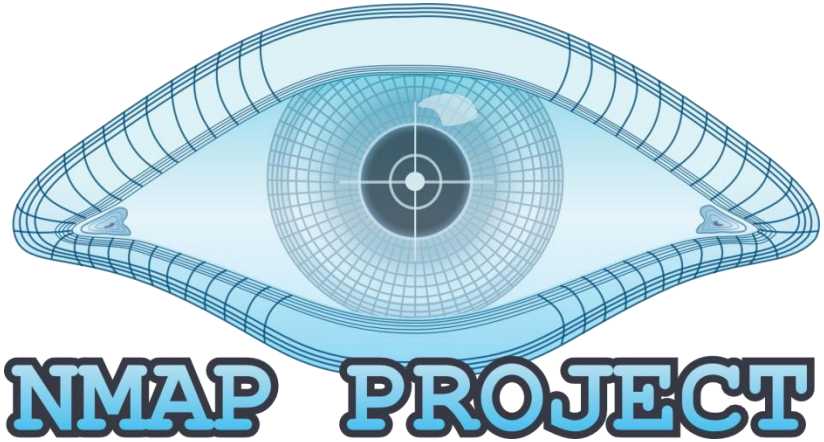
So famous, it was in the matrix



It really was!

nmap

- A network mapping utility
- Can be given a range of targets
  - Both IP and port ranges
- Attempts to determine details of devices and services at each endpoint



Different scan types

- Connect
  - Attempt a full connection
  - More easily detectable
- SYN
  - Half open scanning
  - Less detectable
- FIN scan
- Ping Scan

Version Scan

- Attempt to deterine versions of services running on a machine

```
root@kali:/demoScripts/activeScanning# ./versionScanMetasploitable.sh
Starting Nmap 7.70 ( https://nmap.org ) at 2018-08-23 16:19 EDT
Nmap scan report for 192.168.64.2
Host is up (0.00029s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:C5:DE:AD (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OS
s: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.84 seconds
```

Don’t be so loud

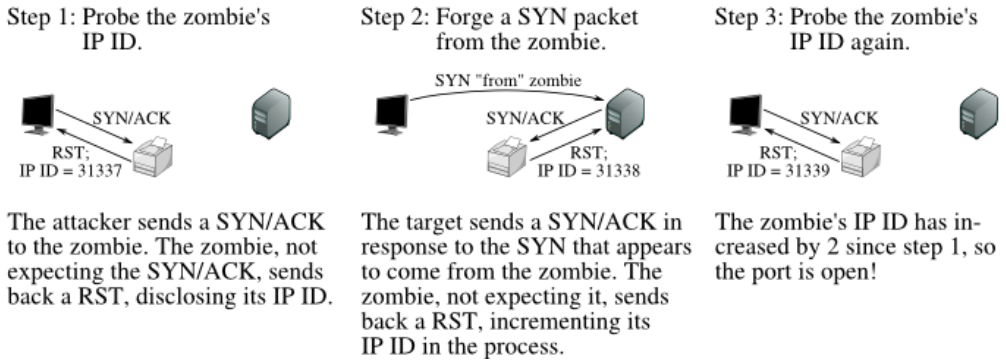
- Nmap generates a lot of traffic
  - This might trigger alarms
- Version scan has “intensity” levels
- You can set max rates and delays between probes

```
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
          directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
          <Lua scripts> is a comma-separated list of script-files or
          script-categories.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
```

Zombies are everywhere

Idle (Zombie) Scanning

- You don't have to send packets from your machine
- Based on simple packet counter implementations
  - Basic incrementing IDS
- https://nmap.org/book/idlescan.html



Finding zombies

- Must have a global request ID
- Must increment per request
- Must not have other traffic (Idle)

- Generally Printers used to be a good source
  - Simple IP stacks
  - Generally not pinged often

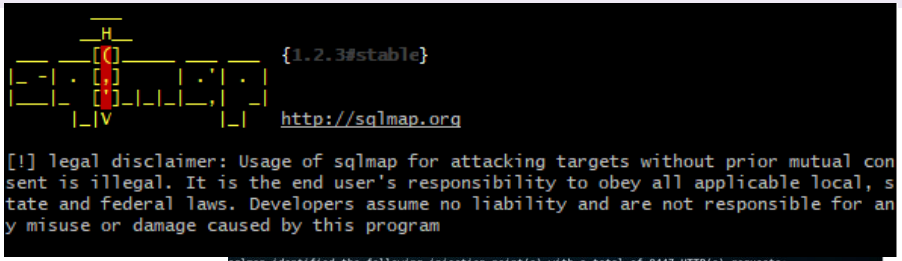
Even more in depth

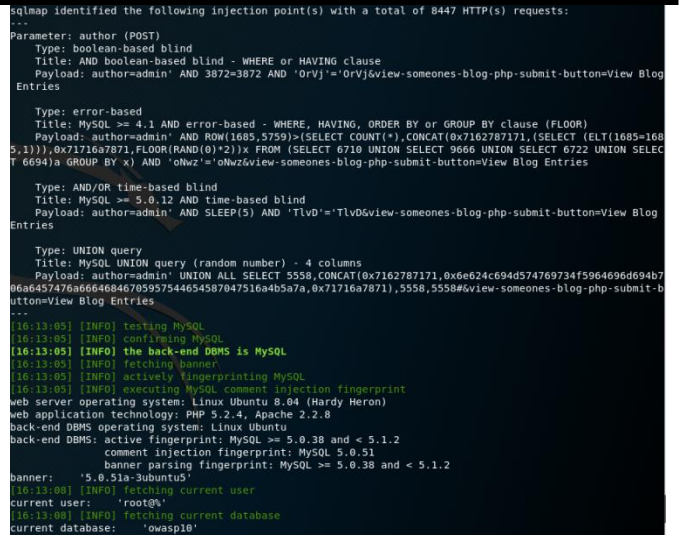
- NSE: Nmap
  - Nmap -sV -sC <target>
- Scripts can be used to discover specific vulnerabilities
  - -script=sslheartbleed.nse

Other Tools

SQL Map

- Designed to detect and abuse SQL injection vulnerabilities in a target website
- Can determine the type of database being used





Aircrack-ng and wifite

- Aircrack-ng is a suite of tools used to capture and crack data from wifi connections
- Requires a wireless card that can be put in monitor mode
  - Like promiscuous mode of the LAN world
- Wifite is a wrapper for aircrack that simplifies a lot of the process.

Available demos

- /demoScripts/activeScanning
  - fullNmapScan.sh
  - sqlmapMutilldae.sh
  - versionScanMetasploitable.sh
- They basically just run the commands for you
  - You can see some standard syntax