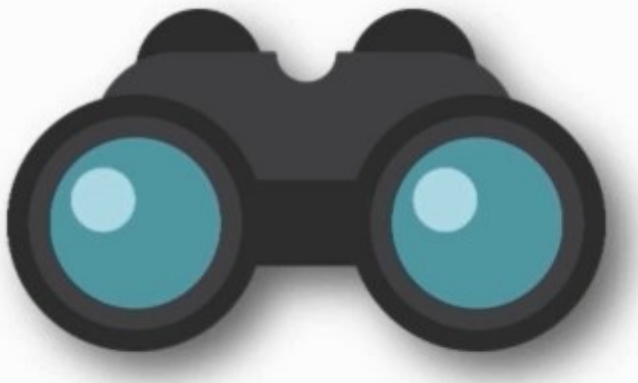
Understanding What You're Doing



- What is scanning?
- Types of scanning.
- What's the goal?
- What are techniques used?
- What tools are used?

What is Scanning?

What is Scanning?

Looking for "Live" systems.

Identifying those systems.

Discovering what ports are open or closed.

Are those systems running any services?

Types of Scanning

Network Scan

- Find all “Live” Hosts
- Possibly “see” OS’s
- Pick up IP address

Port Scan

192.168.0.15

+

HTTP

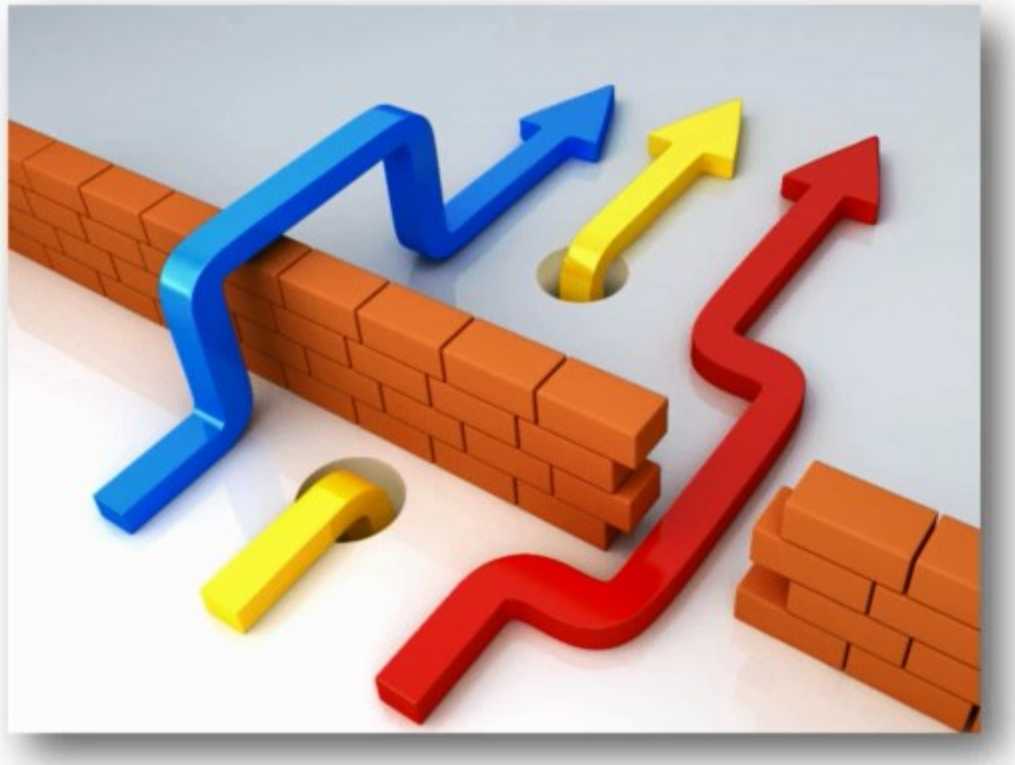
192.168.0.15:80

- What is a port?

Port Scan

- What is a port?
- 65,535 but focus on the first 1,023
- Which ports are responding?
- Which services use those ports?

Vulnerability Scan



- Identify possible threats to OS/Apps
- Identify vulnerabilities OS/Apps
- Be proactive folks!

What's the Goal?

Objectives

"Live" Hosts

IP Addresses

Open/Closed Ports

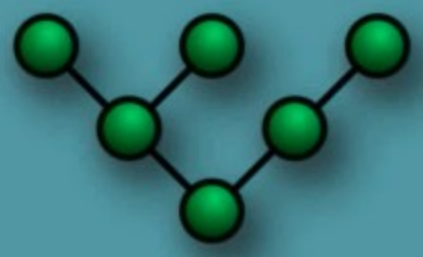
OS & Architecture

Vulnerabilities & Threats

Security Risks & Services

What Techniques Are Used?

Different Strokes for Different… Technologies



Internal or External

Not Just

Computers

Don't Forget Wifi

Banner Grabbing

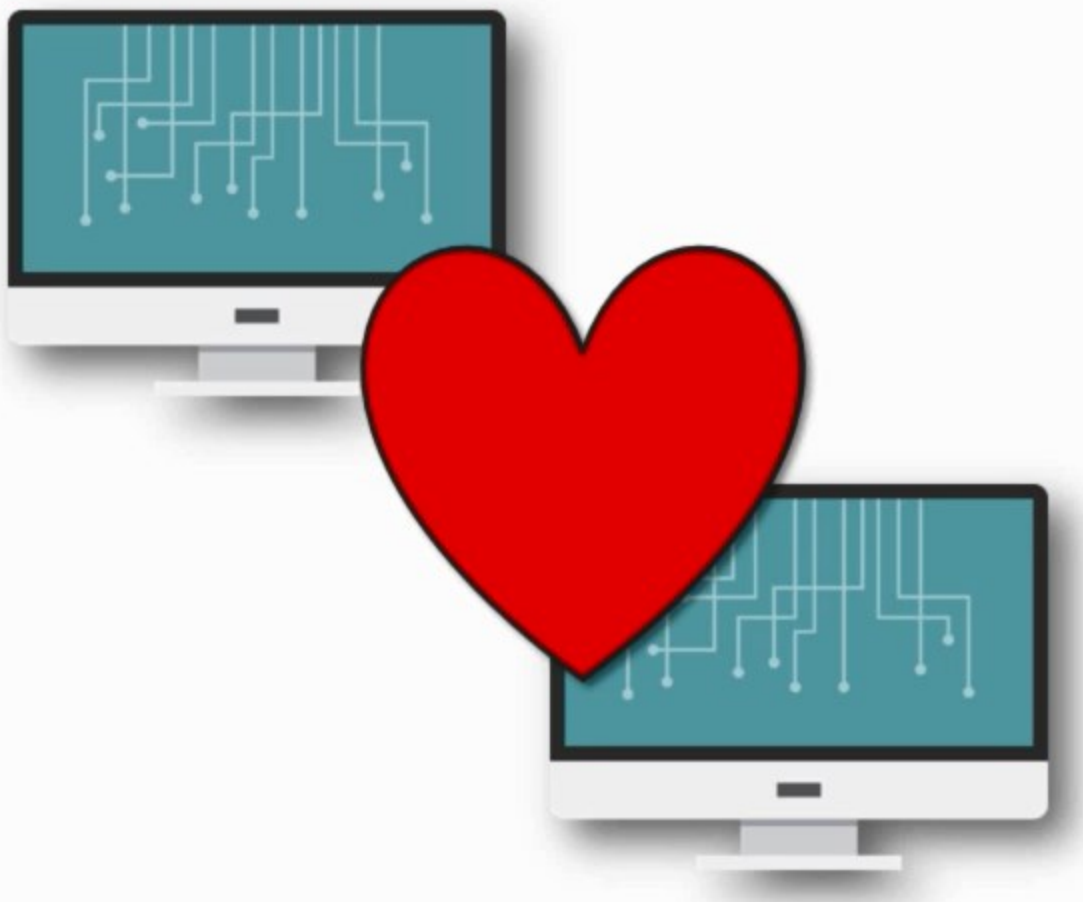
What Tools Are Used?

Oh, My… Where to Start/End?

- Command Line
- **Nmap**
- **Angry IP Scanner**
- Solarwinds
- Colasoft Ping
- Visual Ping Tester
- Ping Scanner Pro
- Ping Sweep
- Ping Monitor
- Pinkie
- PingInfoView
- PacketTrap MSP
- GFI
- SoftPerfect
- **Nessus**
- NetStumbler
- Ping Tester
- The list keeps going

TCP & UDP Communications

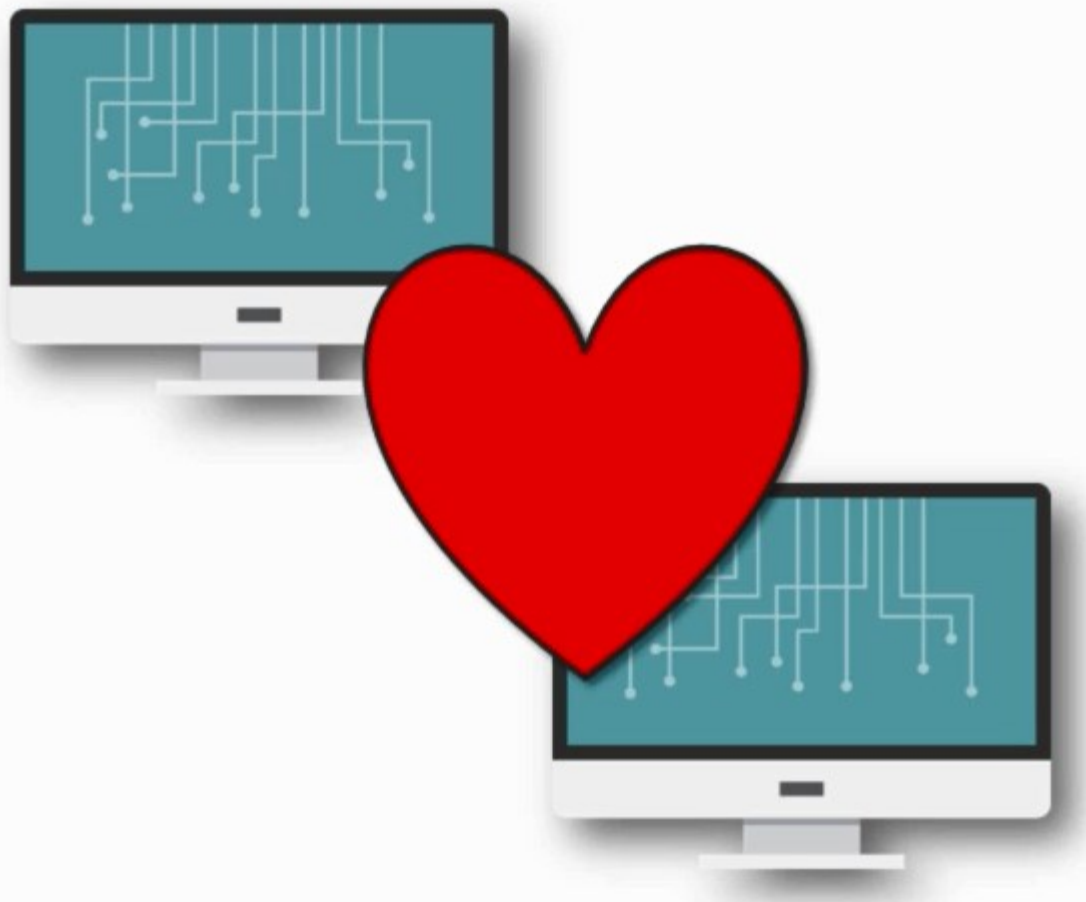
When Two Computers Love Each Other…



TCP

- Negotiate a connection
- Delivery acknowledgements
- Retransmission / error detection
- In-order delivery
- Congestion control
- Bigger headers (20 bytes)
- Bigger overhead
- Stream-oriented

When Two Computers Love Each Other…



UDP

- Connectionless based
- Smaller packets (8 bytes)
- Only 1 packet goes
- Out of order
- No congestion control
- Message-oriented

TCP Header Flags

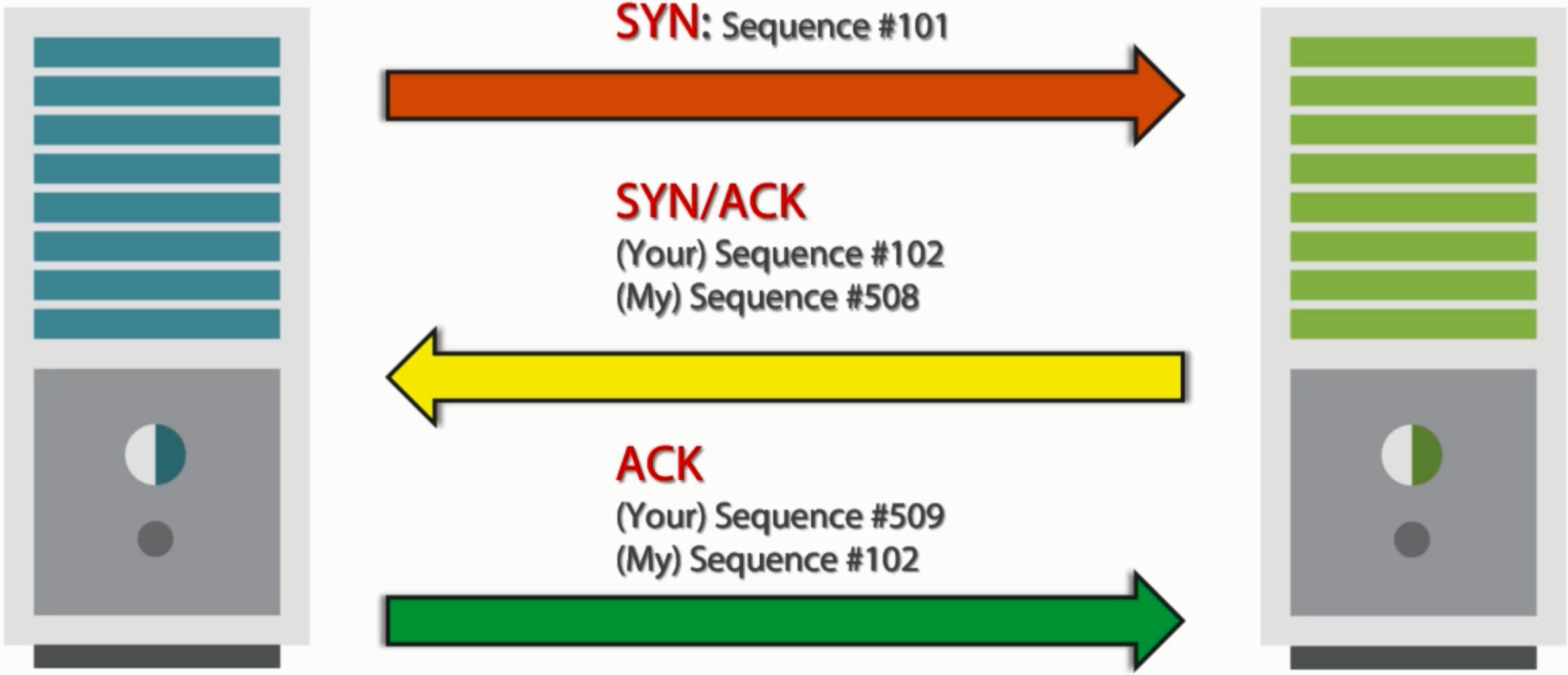
There's a Flag on the Play!

- SYN
  - Synchronize (Includes a seq #)
- ACK
  - Acknowledgement
- FIN
  - Finish

- PSH
  - Push
- URG
  - Urgent
- RST
  - Reset

Normal 3-Way Handshake

Let's Put It All Together Now



Let's Put It All Together Now

What If…

Think Outside the Box

- SYN / SYN-ACK / ACK
- FIN / ACK-FIN /ACK

- What would happen if your first packet was a SYN/ACK?
- What would happen if your first packet was a FIN?
- What would happen if you shot a gun in space?

Checking for “Live” Systems and Their Ports

It's ALIVE!

- ICMP Sweep
- Port Scan
- Firewalking

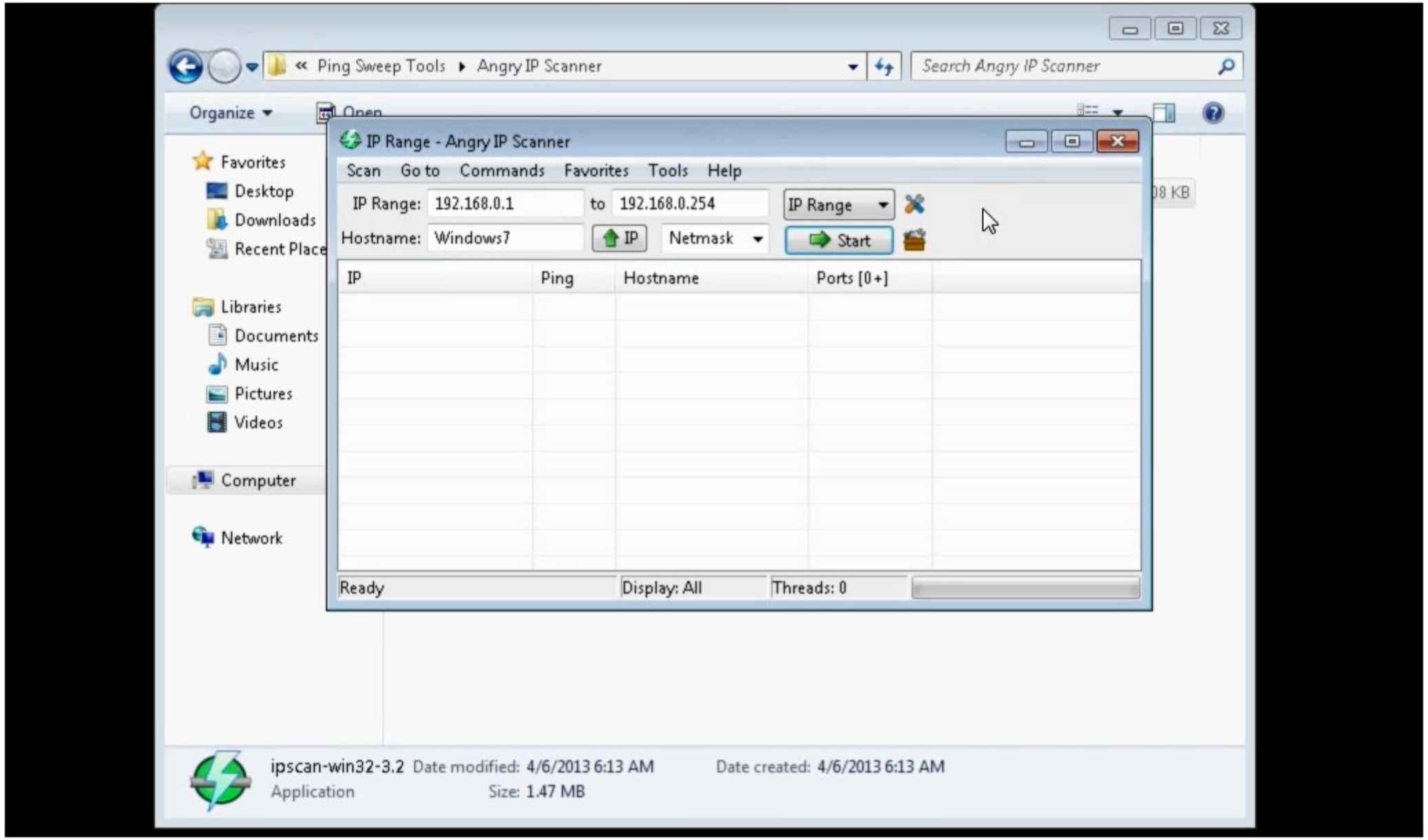
Step 1: ICMP Sweep

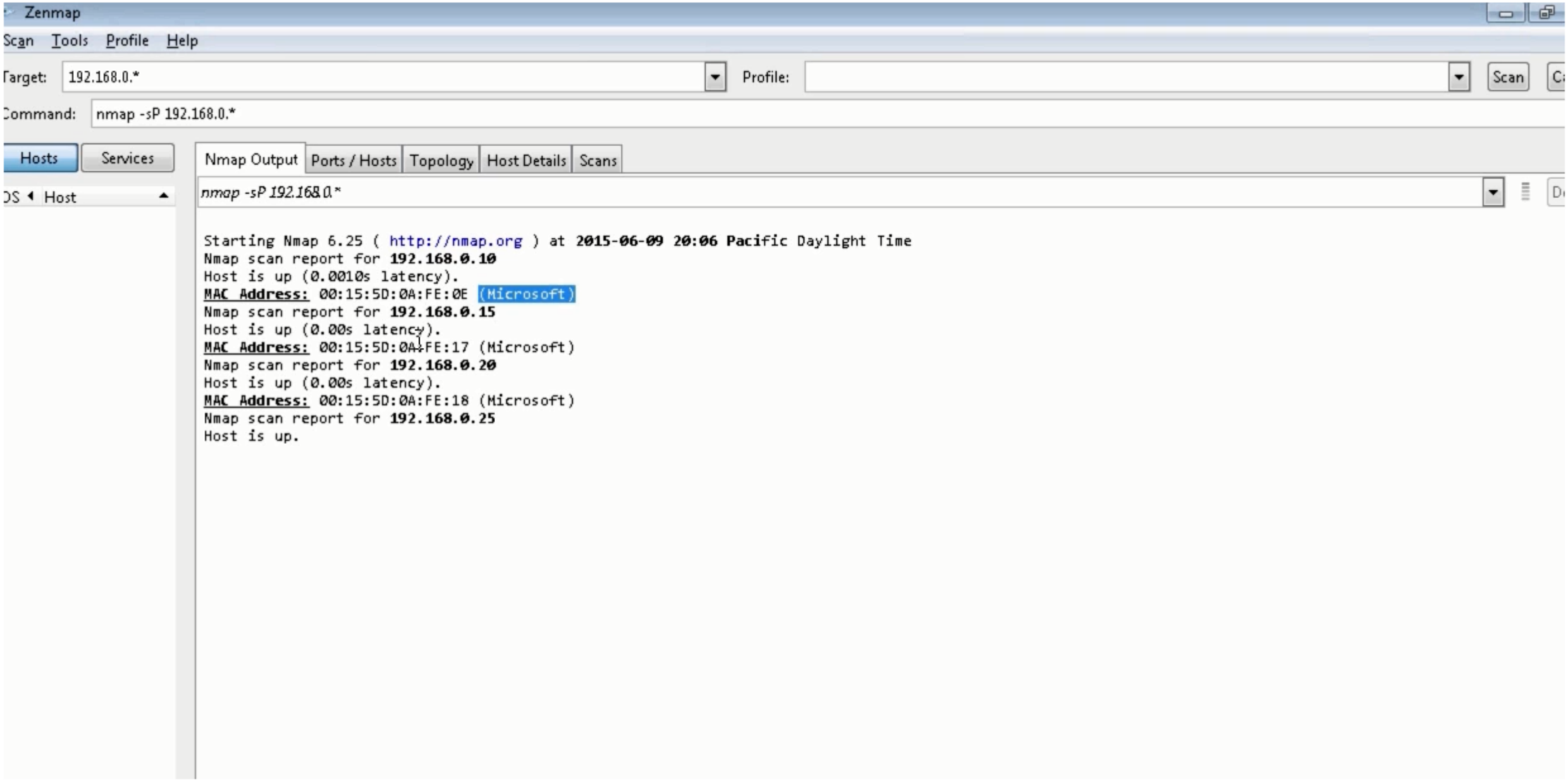
Using an ICMP Tool

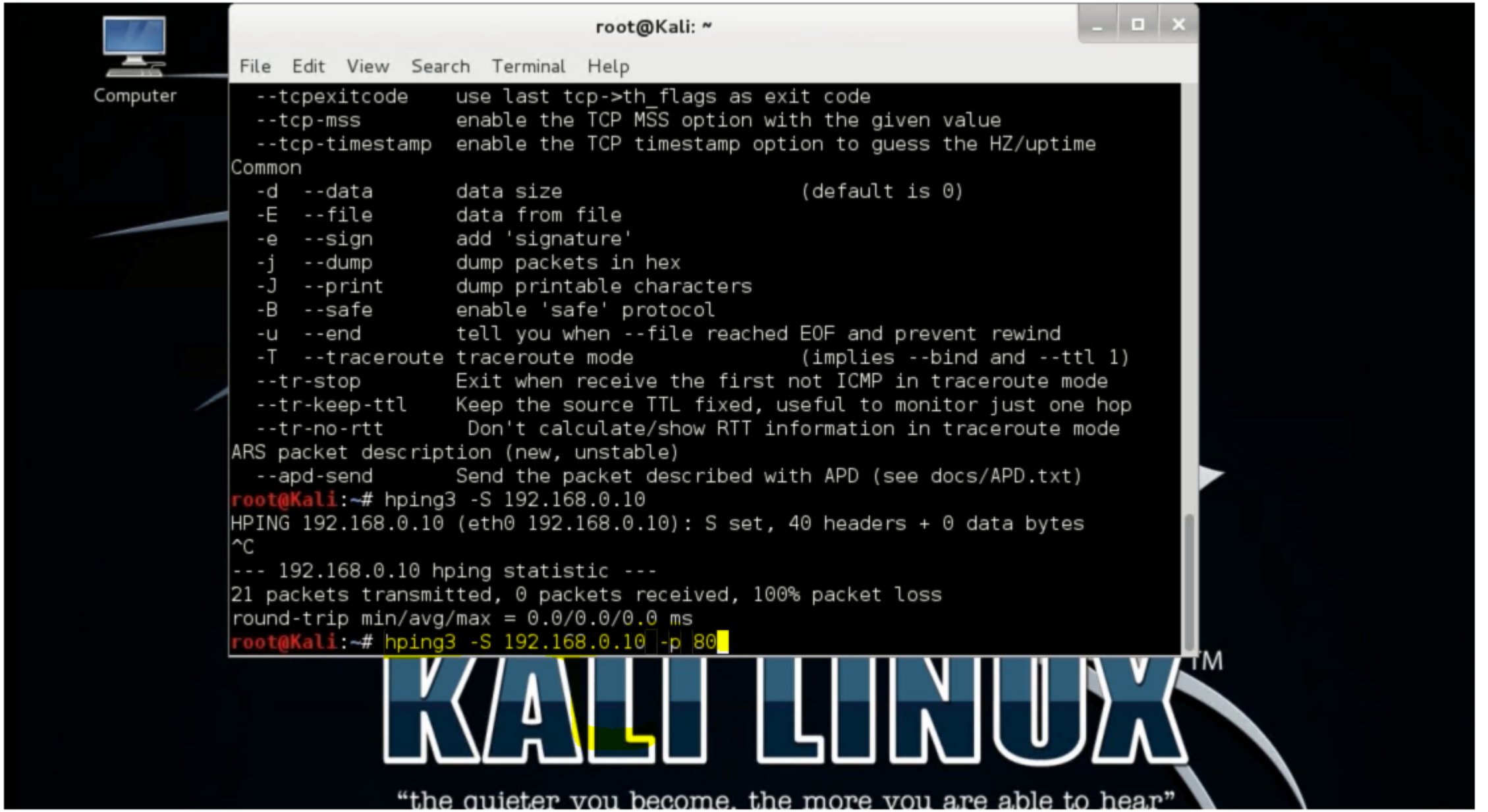
Angry IP Scanner

Nmap

Hping2/Hping3


« Ping Sweep Tools ▸ Angry IP Scanner
Search Angry IP Scanner
Organize
Open
Favorites
Desktop
Downloads
Recent Place
Libraries
Documents
Music
Pictures
Videos
Computer
Network
IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range: 192.168.0.1 to 192.168.0.254
IP Range
Hostname: Windows7
IP
Netmask
Start
IP Ping Hostname Ports [0+]
Ready
Display: All
Threads: 0
ipscan-win32-3.2 Date modified: 4/6/2013 6:13 AM
Date created: 4/6/2013 6:13 AM
Application
Size: 1.47 MB


Zenmap
Scan Tools Profile Help
Target: 192.168.0.*
Profile:
Scan
Command: nmap -sP 192.168.0.*
Hosts
Services
OS Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sP 192.168.0.*
Starting Nmap 6.25 (http://nmap.org) at 2015-06-09 20:06 Pacific Daylight Time
Nmap scan report for 192.168.0.10
Host is up (0.0010s latency).
MAC Address: 00:15:5D:0A:FE:0E (Microsoft)
Nmap scan report for 192.168.0.15
Host is up (0.00s latency).
MAC Address: 00:15:5D:0A:FE:17 (Microsoft)
Nmap scan report for 192.168.0.20
Host is up (0.00s latency).
MAC Address: 00:15:5D:0A:FE:18 (Microsoft)
Nmap scan report for 192.168.0.25
Host is up.


Computer
root@Kali: ~
File Edit View Search Terminal Help
--tcpexitcode use last tcp->th_flags as exit code
--tcp-mss enable the TCP MSS option with the given value
--tcp-timestamp enable the TCP timestamp option to guess the HZ/uptime
Common
-d --data data size (default is 0)
-E --file data from file
-e --sign add 'signature'
-j --dump dump packets in hex
-J --print dump printable characters
-B --safe enable 'safe' protocol
-u --end tell you when --file reached EOF and prevent rewind
-T --traceroute traceroute mode (implies --bind and --ttl 1)
--tr-stop Exit when receive the first not ICMP in traceroute mode
--tr-keep-ttl Keep the source TTL fixed, useful to monitor just one hop
--tr-no-rtt Don't calculate/show RTT information in traceroute mode
ARS packet description (new, unstable)
--apd-send Send the packet described with APD (see docs/APD.txt)
root@Kali:~# hping3 -S 192.168.0.10
HPING 192.168.0.10 (eth0 192.168.0.10): S set, 40 headers + 0 data bytes
^C
--- 192.168.0.10 hping statistic ---
21 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@Kali:~# hping3 -S 192.168.0.10 -p 80
KALI LINUX
"the quieter you become, the more you are able to hear"

Firewalking

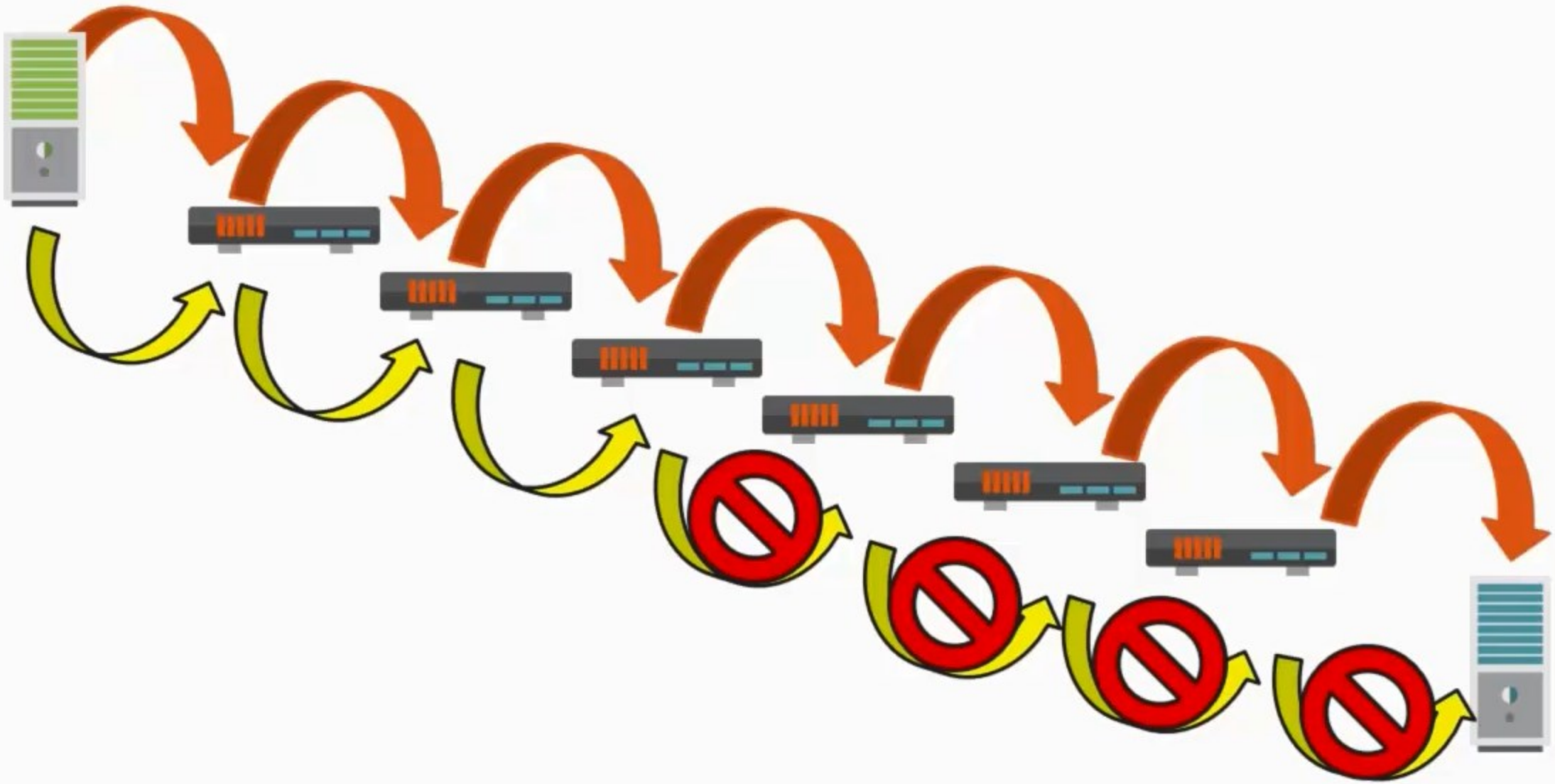
What is Firewalking?

Like traceroute, but determines whether or not a particular packet can pass from the attacker's system to the target via a packet-filtering device

What is Firewalking?

- Define a firewall's ACL (what's allowed)
- It uses the TTL
- What happens to the packet?
  - Forwarded = Open
  - Dropped = Closed

Never Give Up. Attackers Don't



Standard Traceroute

```
traceroute 192.168.0.10

traceroute to 192.168.0.10(192.168.0.10), 30 hops max, 40
byte packets

1 192.168.0.1 (192.168.0.1) 0.540 ms 0.394 ms 0.397 ms

2 192.168.0.2 (192.168.0.2) 2.455 ms 2.479 ms 2.512 ms

3 192.168.0.3 (192.168.0.3) 4.812 ms 4.780 ms 4.747 ms

4 * * *

5 * * *
```

Standard Traceroute (Add a Port)

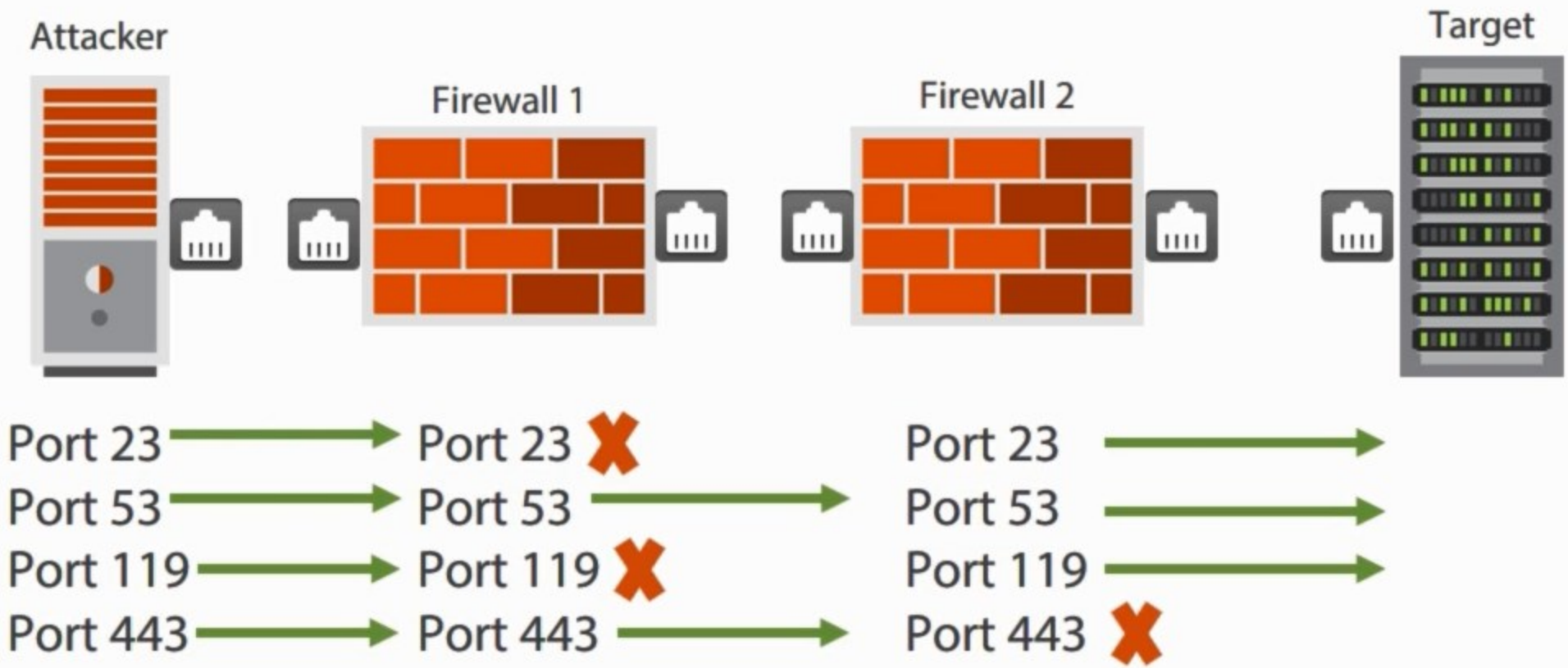
```
traceroute -p53 192.168.0.10
traceroute to 192.168.0.10(192.168.0.10), 30 hops max, 40
byte packets
1 192.168.0.1 (192.168.0.1) 0.540 ms 0.394 ms 0.397 ms
2 192.168.0.2 (192.168.0.2) 2.455 ms 2.479 ms 2.512 ms
3 192.168.0.3 (192.168.0.3) 4.812 ms 4.780 ms 4.747 ms
4 192.168.0.4 (192.168.0.4) 5.342 ms 5.304 ms 5.283 ms
5 * * *
```

Firewalk

```
firewalk -s20-100 -i eth0 -n -pTCP 192.168.0.254 192.168.0.10


Scanning Phase:
port 52: *no response*
port 53: A! open (port not listen) [192.168.0.1]
port 54: *no response*
```

Thus, You Can Firewalk Beyond



Types of Scanning

A Plethora of Scanning

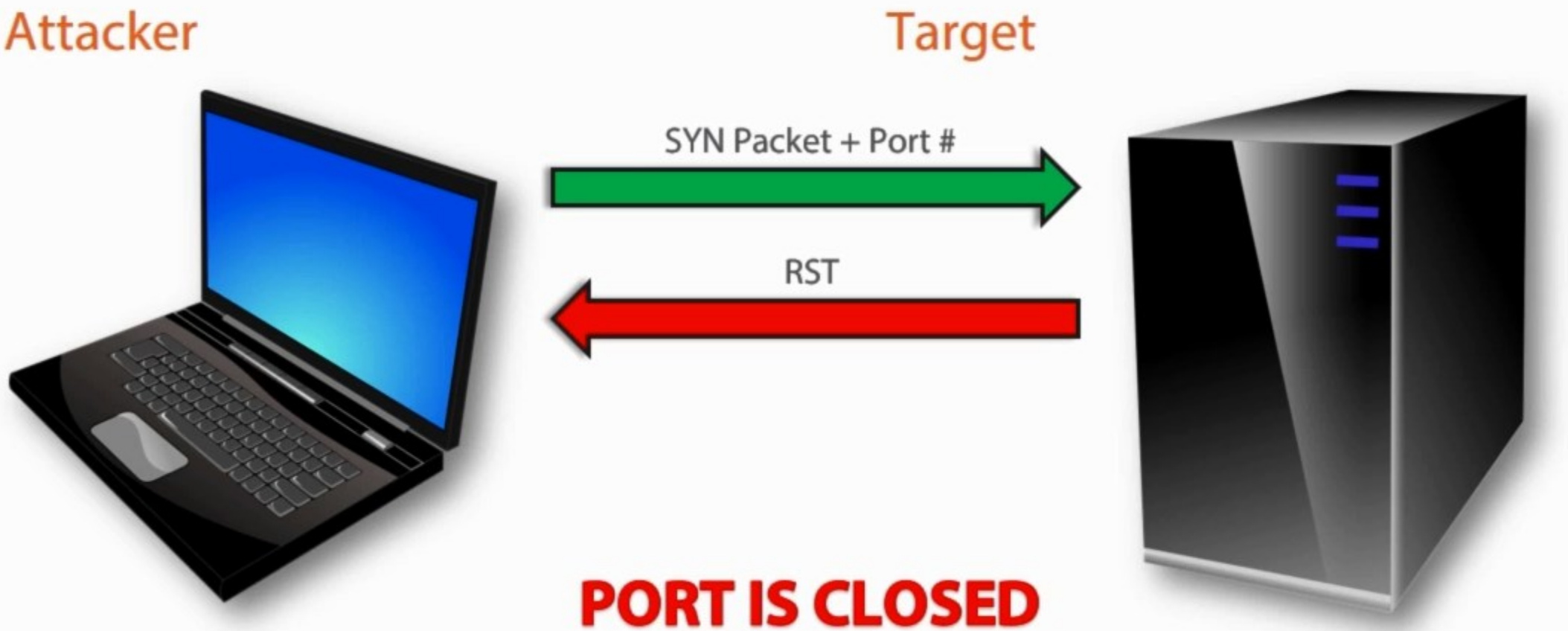
- Full Scans
- Half-open Scans
- Xmas Tree Scans
- FIN Scans
- NULL Scans

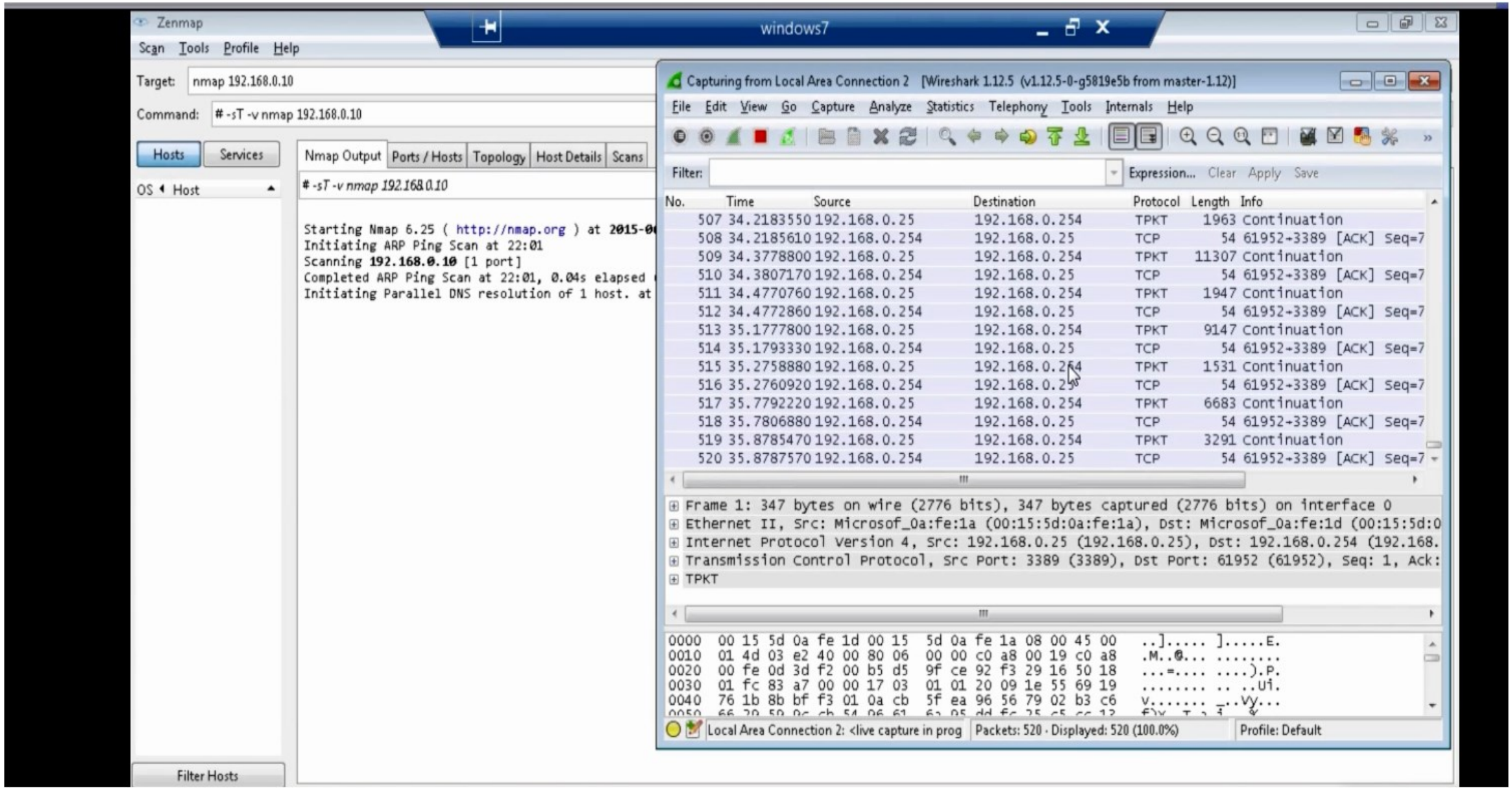
A Plethora of Scanning

- UDP Scans
- IDS Evasion Methods
- Countermeasures

Full Scan

How a Full Scan Works

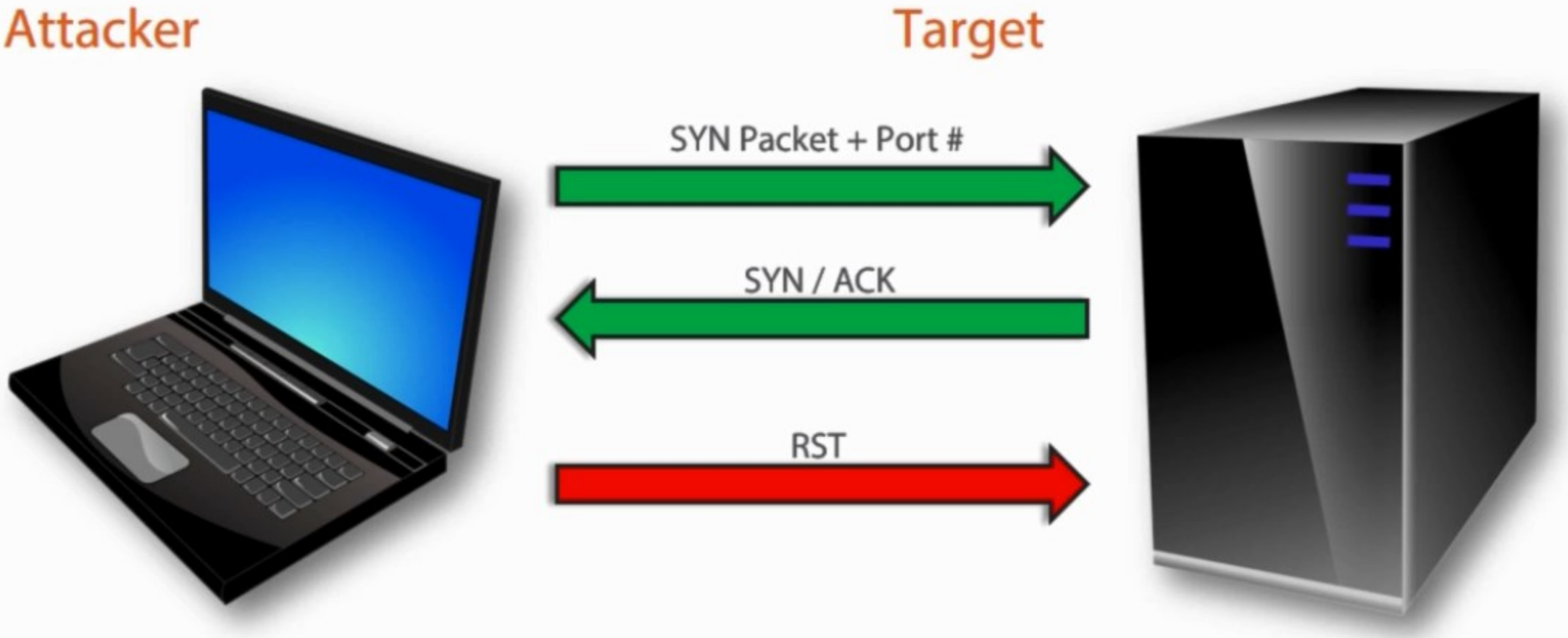



Zenmap
windows7
Scan Tools Profile Help
Target: nmap 192.168.0.10
Command: # -sT -v nmap 192.168.0.10
Hosts Services
OS Host
Filter Hosts
Nmap Output Ports / Hosts Topology Host Details Scans
-sT -v nmap 192.168.0.10
Starting Nmap 6.25 (http://nmap.org) at 2015-0
Initiating ARP Ping Scan at 22:01
Scanning 192.168.0.10 [1 port]
Completed ARP Ping Scan at 22:01, 0.04s elapsed
Initiating Parallel DNS resolution of 1 host. at
Capturing from Local Area Connection 2 [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
507 34.2183550 192.168.0.25 192.168.0.254 TPKT 1963 Continuation
508 34.2185610 192.168.0.254 192.168.0.25 TCP 54 61952→3389 [ACK] Seq=7
509 34.3778800 192.168.0.25 192.168.0.254 TPKT 11307 Continuation
510 34.3807170 192.168.0.254 192.168.0.25 TCP 54 61952→3389 [ACK] Seq=7
511 34.4770760 192.168.0.25 192.168.0.254 TPKT 1947 Continuation
512 34.4772860 192.168.0.254 192.168.0.25 TCP 54 61952→3389 [ACK] Seq=7
513 35.1777800 192.168.0.25 192.168.0.254 TPKT 9147 Continuation
514 35.1793330 192.168.0.254 192.168.0.25 TCP 54 61952→3389 [ACK] Seq=7
515 35.2758880 192.168.0.25 192.168.0.254 TPKT 1531 Continuation
516 35.2760920 192.168.0.254 192.168.0.25 TCP 54 61952→3389 [ACK] Seq=7
517 35.7792220 192.168.0.25 192.168.0.254 TPKT 6683 Continuation
518 35.7806880 192.168.0.254 192.168.0.25 TCP 54 61952→3389 [ACK] Seq=7
519 35.8785470 192.168.0.25 192.168.0.254 TPKT 3291 Continuation
520 35.8787570 192.168.0.254 192.168.0.25 TCP 54 61952→3389 [ACK] Seq=7
Frame 1: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits) on interface 0
Ethernet II, Src: Microsof_0a:fe:1a (00:15:5d:0a:fe:1a), Dst: Microsof_0a:fe:1d (00:15:5d:0
Internet Protocol Version 4, Src: 192.168.0.25 (192.168.0.25), Dst: 192.168.0.254 (192.168.
Transmission Control Protocol, Src Port: 3389 (3389), Dst Port: 61952 (61952), Seq: 1, Ack:
TPKT
0000 00 15 5d 0a fe 1d 00 15 5d 0a fe 1a 08 00 45 00 ..].....].....E.
0010 01 4d 03 e2 40 00 80 06 00 00 c0 a8 00 19 c0 a8 .M..@... ....
0020 00 fe 0d 3d f2 00 b5 d5 9f ce 92 f3 29 16 50 18 ...=.... ....).P.
0030 01 fc 83 a7 00 00 17 03 01 01 20 09 1e 55 69 19 ....Ui.
0040 76 1b 8b bf f3 01 0a cb 5f ea 96 56 79 02 b3 c6 v....... _..Vy...
Local Area Connection 2: <live capture in prog
Packets: 520 · Displayed: 520 (100.0%)
Profile: Default

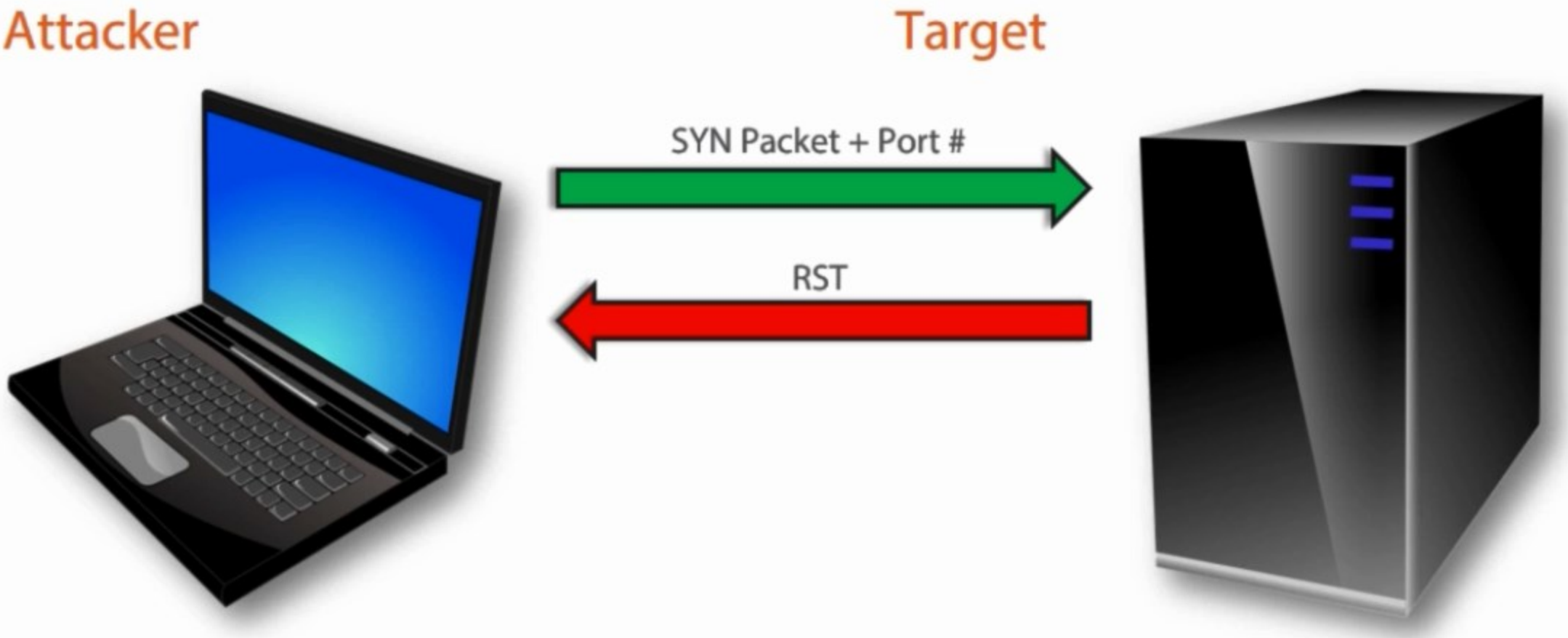
Half-open Scan

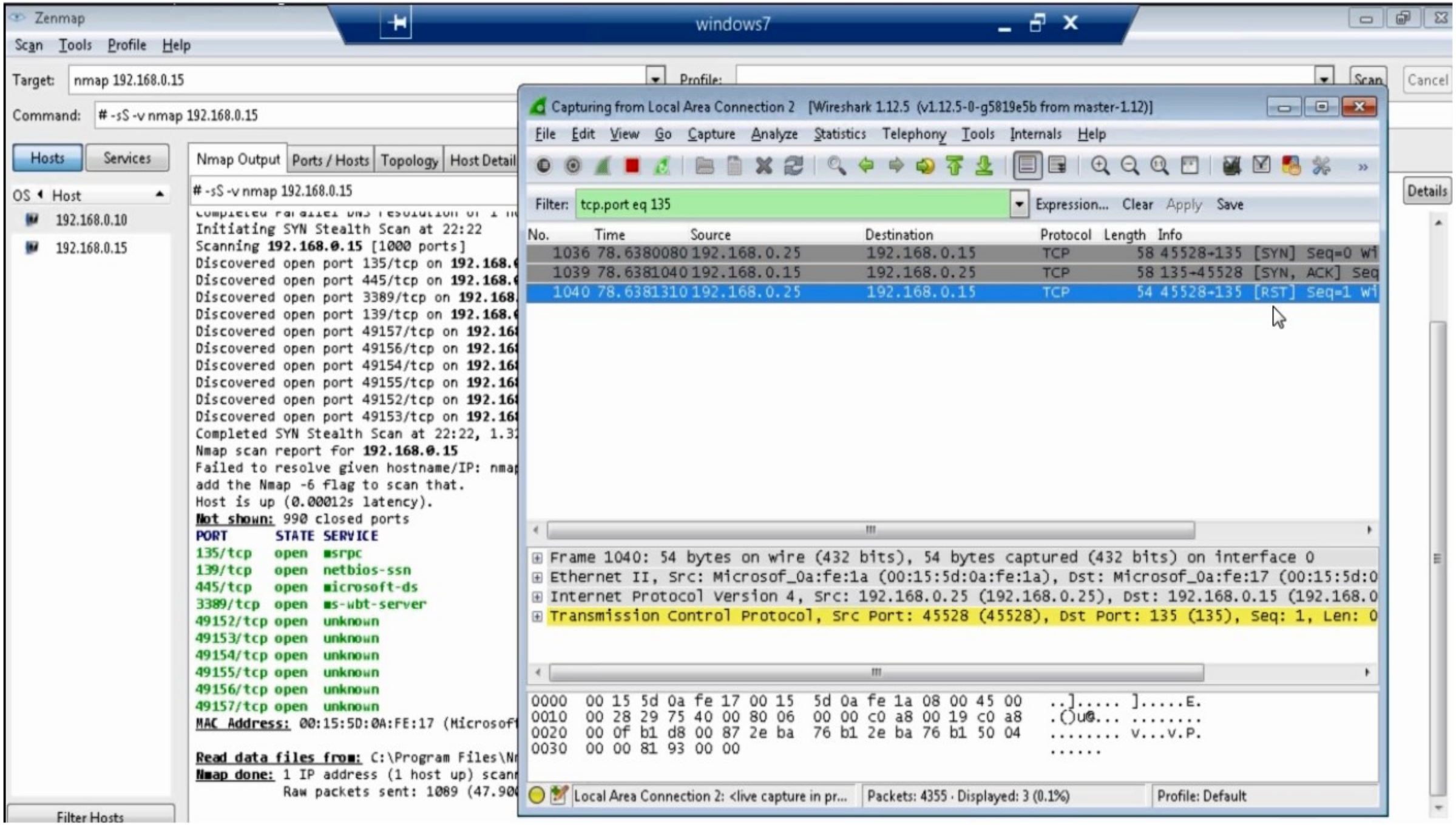
Stealth Scan

How a Half-open Scan Works



How a Half-open Scan Works

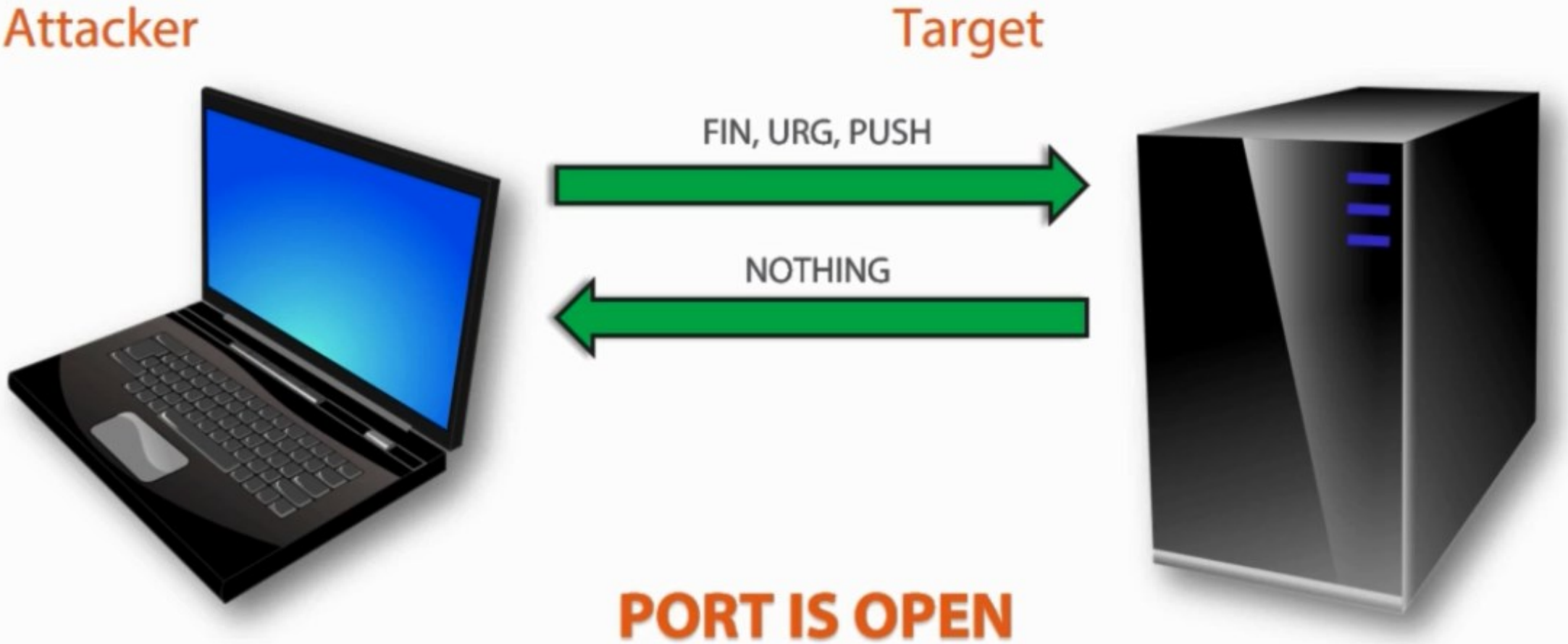



Zenmap
windows7
Scan Tools Profile Help
Target: nmap 192.168.0.15
Profile:
Scan
Cancel
Command: # -sS -v nmap 192.168.0.15
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Detail
Details
OS Host
192.168.0.10
192.168.0.15
-sS -v nmap 192.168.0.15
Initiating SYN Stealth Scan at 22:22
Scanning 192.168.0.15 [1000 ports]
Discovered open port 135/tcp on 192.168.0.15
Discovered open port 445/tcp on 192.168.0.15
Discovered open port 3389/tcp on 192.168.0.15
Discovered open port 139/tcp on 192.168.0.15
Discovered open port 49157/tcp on 192.168.0.15
Discovered open port 49156/tcp on 192.168.0.15
Discovered open port 49154/tcp on 192.168.0.15
Discovered open port 49155/tcp on 192.168.0.15
Discovered open port 49152/tcp on 192.168.0.15
Discovered open port 49153/tcp on 192.168.0.15
Completed SYN Stealth Scan at 22:22, 1.31
Nmap scan report for 192.168.0.15
Failed to resolve given hostname/IP: nmap
add the Nmap -6 flag to scan that.
Host is up (0.00012s latency).
Not shown: 990 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
49157/tcp open unknown
MAC Address: 00:15:5D:0A:FE:17 (Microsoft
Read data files from: C:\Program Files\Nm
Nmap done: 1 IP address (1 host up) scann
Raw packets sent: 1089 (47.90
Filter Hosts
Capturing from Local Area Connection 2 [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.port eq 135
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1036 78.6380080 192.168.0.25 192.168.0.15 TCP 58 45528→135 [SYN] Seq=0 Wi
1039 78.6381040 192.168.0.15 192.168.0.25 TCP 58 135→45528 [SYN, ACK] Seq
1040 78.6381310 192.168.0.25 192.168.0.15 TCP 54 45528→135 [RST] Seq=1 Wi
Frame 1040: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: Microsof_0a:fe:1a (00:15:5d:0a:fe:1a), Dst: Microsof_0a:fe:17 (00:15:5d:0
Internet Protocol Version 4, Src: 192.168.0.25 (192.168.0.25), Dst: 192.168.0.15 (192.168.0
Transmission Control Protocol, Src Port: 45528 (45528), Dst Port: 135 (135), Seq: 1, Len: 0
0000 00 15 5d 0a fe 17 00 15 5d 0a fe 1a 08 00 45 00 ..].....].....E.
0010 00 28 29 75 40 00 80 06 00 00 c0 a8 00 19 c0 a8 .()u@... ....
0020 00 0f b1 d8 00 87 2e ba 76 b1 2e ba 76 b1 50 04 .... v...v.P.
0030 00 00 81 93 00 00 ......
Local Area Connection 2: <live capture in pr...
Packets: 4355 · Displayed: 3 (0.1%)
Profile: Default

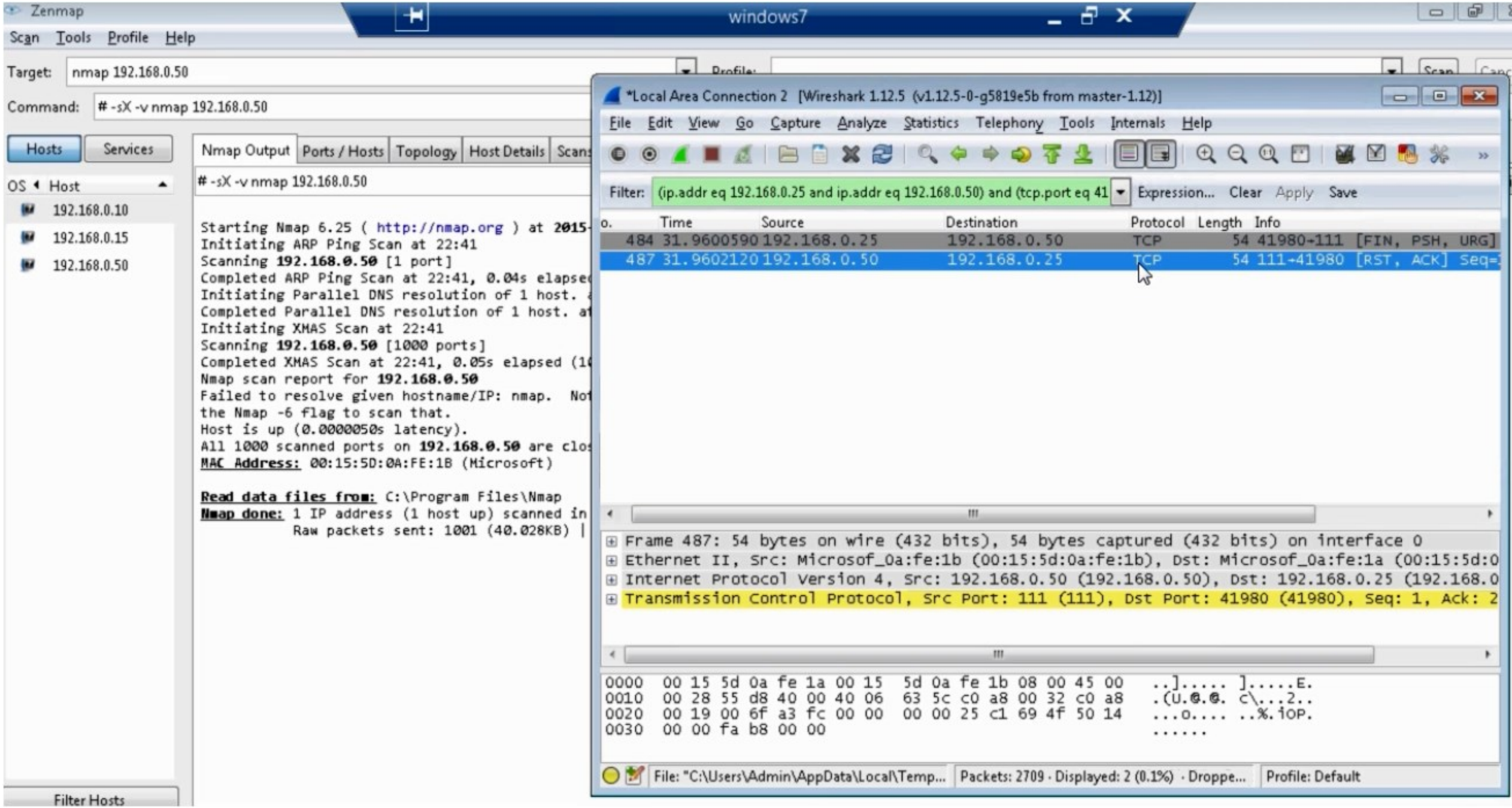
Xmas Scans

Doesn't Work on Windows

How a Xmas Scan Works



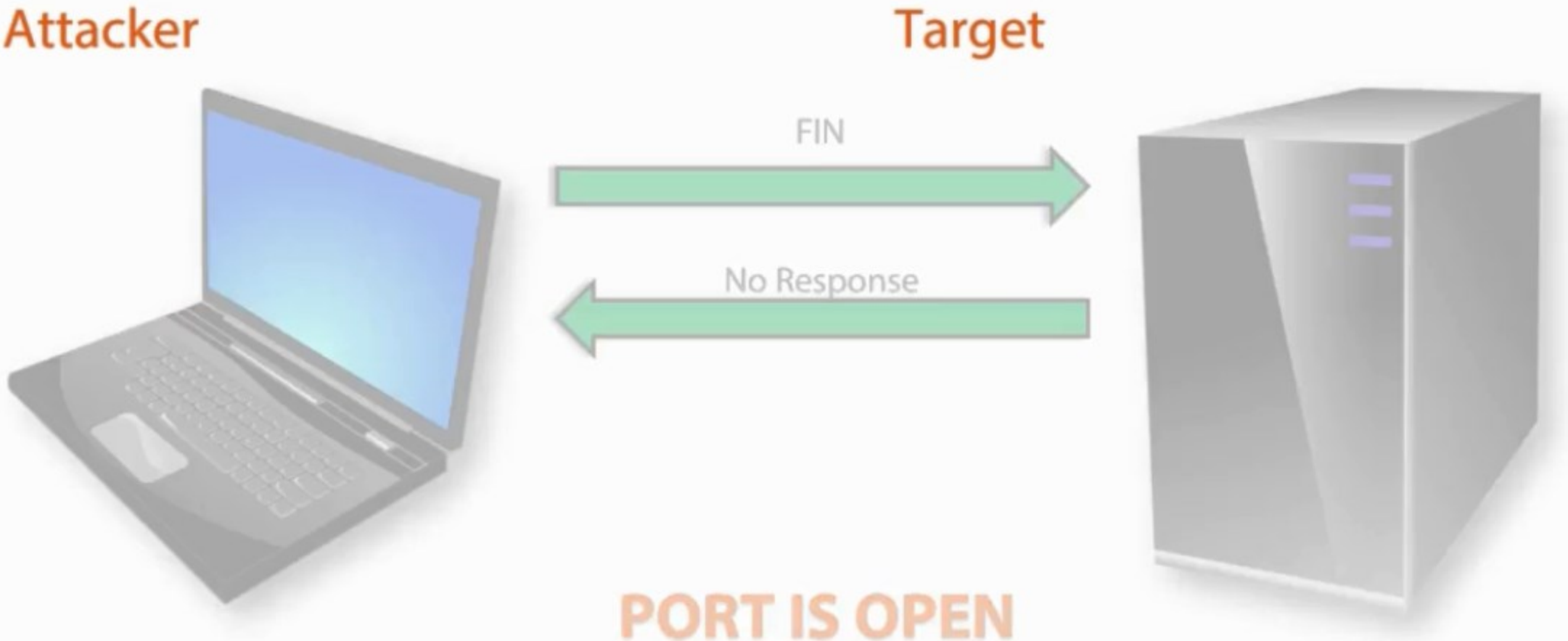
How a Xmas Scan Works


Zenmap
windows7
Scan Tools Profile Help
Target: nmap 192.168.0.50
Command: # -sX -v nmap 192.168.0.50
Hosts Services
OS Host
192.168.0.10
192.168.0.15
192.168.0.50
Filter Hosts
Nmap Output Ports / Hosts Topology Host Details Scans
-sX -v nmap 192.168.0.50
Starting Nmap 6.25 (http://nmap.org) at 2015-
Initiating ARP Ping Scan at 22:41
Scanning 192.168.0.50 [1 port]
Completed ARP Ping Scan at 22:41, 0.04s elapsed
Initiating Parallel DNS resolution of 1 host.
Completed Parallel DNS resolution of 1 host. at
Initiating XMAS Scan at 22:41
Scanning 192.168.0.50 [1000 ports]
Completed XMAS Scan at 22:41, 0.05s elapsed (1
Nmap scan report for 192.168.0.50
Failed to resolve given hostname/IP: nmap. Not
the Nmap -6 flag to scan that.
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.0.50 are clos
MAC Address: 00:15:5D:0A:FE:1B (Microsoft)
Read data files from: C:\Program Files\Nmap
Nmap done: 1 IP address (1 host up) scanned in
Raw packets sent: 1001 (40.028KB) |
*Local Area Connection 2 [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: (ip.addr eq 192.168.0.25 and ip.addr eq 192.168.0.50) and (tcp.port eq 41
Expression... Clear Apply Save
o. Time Source Destination Protocol Length Info
484 31.9600590 192.168.0.25 192.168.0.50 TCP 54 41980-111 [FIN, PSH, URG]
487 31.9602120 192.168.0.50 192.168.0.25 TCP 54 111-41980 [RST, ACK] Seq=
Frame 487: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: Microsof_0a:fe:1b (00:15:5d:0a:fe:1b), Dst: Microsof_0a:fe:1a (00:15:5d:0
Internet Protocol Version 4, Src: 192.168.0.50 (192.168.0.50), Dst: 192.168.0.25 (192.168.0
Transmission Control Protocol, Src Port: 111 (111), Dst Port: 41980 (41980), Seq: 1, Ack: 2
0000 00 15 5d 0a fe 1a 00 15 5d 0a fe 1b 08 00 45 00 ..].....].....E.
0010 00 28 55 d8 40 00 40 06 63 5c c0 a8 00 32 c0 a8 .(U.@.@. c\...2..
0020 00 19 00 6f a3 fc 00 00 00 00 25 c1 69 4f 50 14 ...o.... ..%.iOP.
0030 00 00 fa b8 00 00 ....
File: "C:\Users\Admin\AppData\Local\Temp...
Packets: 2709 · Displayed: 2 (0.1%) · Droppe...
Profile: Default

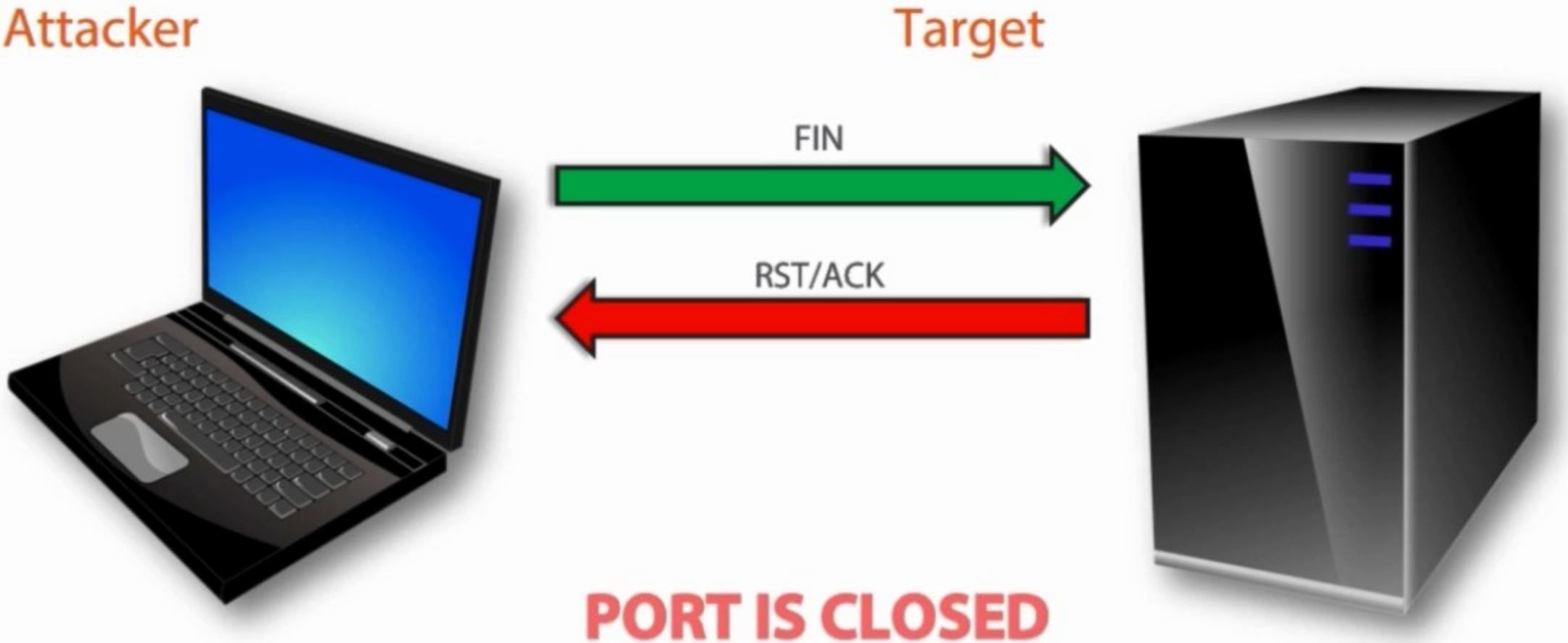
FIN Scans

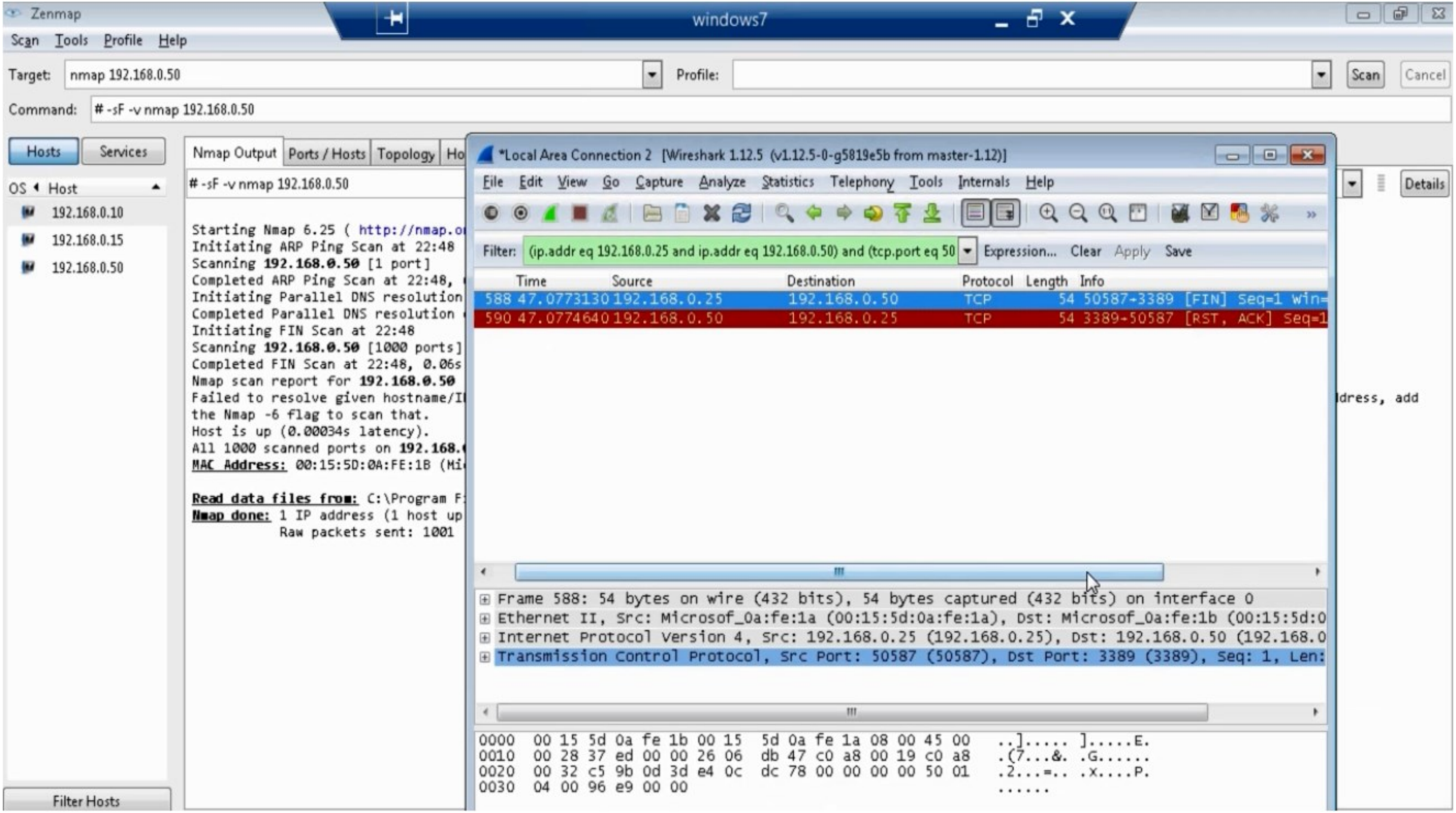
Doesn't Work on Windows

How a FIN Scan Works



How a FIN Scan Works

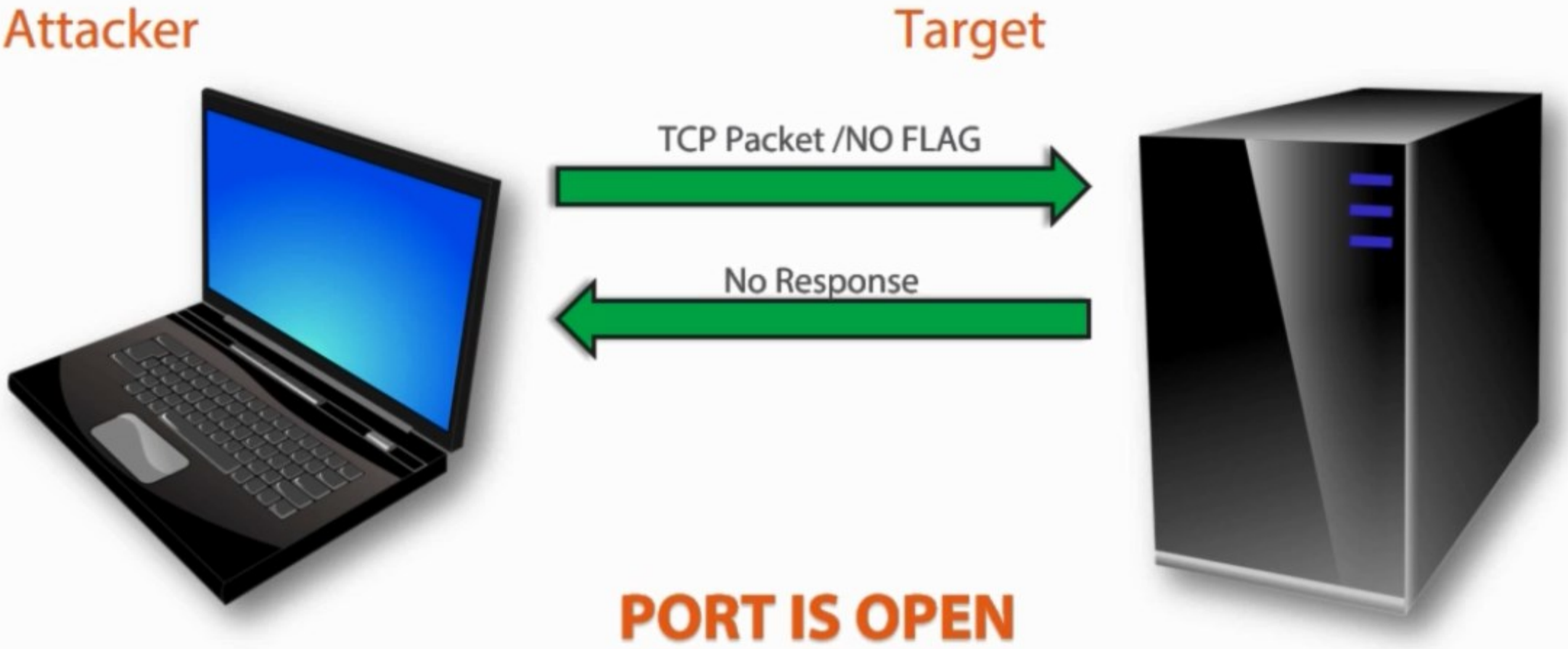



Zenmap
windows7
Scan Tools Profile Help
Target: nmap 192.168.0.50
Profile:
Scan
Cancel
Command: # -sF -v nmap 192.168.0.50
Hosts
Services
OS Host
192.168.0.10
192.168.0.15
192.168.0.50
Filter Hosts
Nmap Output
Ports / Hosts
Topology
-sF -v nmap 192.168.0.50
Starting Nmap 6.25 (http://nmap.o
Initiating ARP Ping Scan at 22:48
Scanning 192.168.0.50 [1 port]
Completed ARP Ping Scan at 22:48,
Initiating Parallel DNS resolution
Completed Parallel DNS resolution
Initiating FIN Scan at 22:48
Scanning 192.168.0.50 [1000 ports]
Completed FIN Scan at 22:48, 0.06s
Nmap scan report for 192.168.0.50
Failed to resolve given hostname/I
the Nmap -6 flag to scan that.
Host is up (0.00034s latency).
All 1000 scanned ports on 192.168.
MAC Address: 00:15:5D:0A:FE:1B (Mi
Read data files from: C:\Program F
Nmap done: 1 IP address (1 host up
Raw packets sent: 1001
*Local Area Connection 2 [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: (ip.addr eq 192.168.0.25 and ip.addr eq 192.168.0.50) and (tcp.port eq 50
Expression... Clear Apply Save
Time Source Destination Protocol Length Info
588 47.0773130 192.168.0.25 192.168.0.50 TCP 54 50587→3389 [FIN] Seq=1 Win=
590 47.0774640 192.168.0.50 192.168.0.25 TCP 54 3389→50587 [RST, ACK] Seq=1
Frame 588: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: Microsof_0a:fe:1a (00:15:5d:0a:fe:1a), Dst: Microsof_0a:fe:1b (00:15:5d:0
Internet Protocol Version 4, Src: 192.168.0.25 (192.168.0.25), Dst: 192.168.0.50 (192.168.0
Transmission Control Protocol, Src Port: 50587 (50587), Dst Port: 3389 (3389), Seq: 1, Len:
0000 00 15 5d 0a fe 1b 00 15 5d 0a fe 1a 08 00 45 00 ..].....].....E.
0010 00 28 37 ed 00 00 26 06 db 47 c0 a8 00 19 c0 a8 .(7...&. .G......
0020 00 32 c5 9b 0d 3d e4 0c dc 78 00 00 00 00 50 01 .2...=.. .x....P.
0030 04 00 96 e9 00 00 ......
Details
dress, add

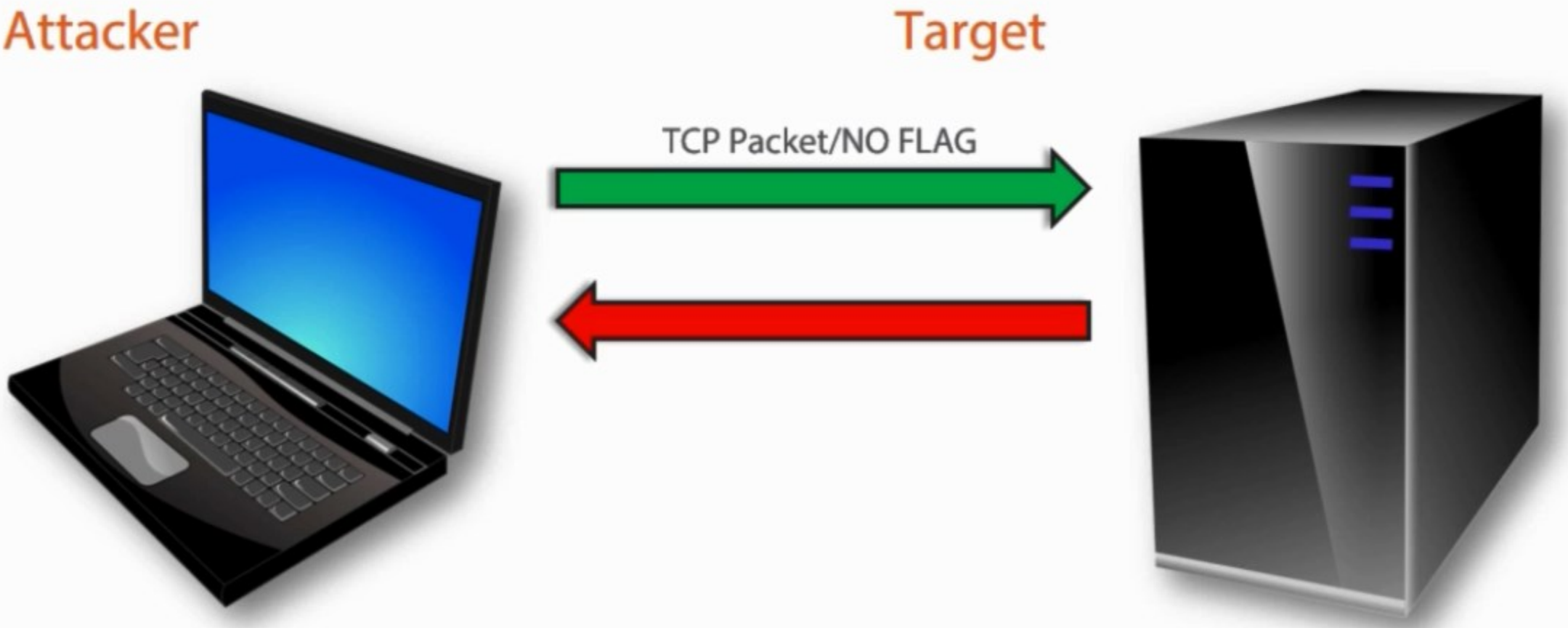
NULL Scans

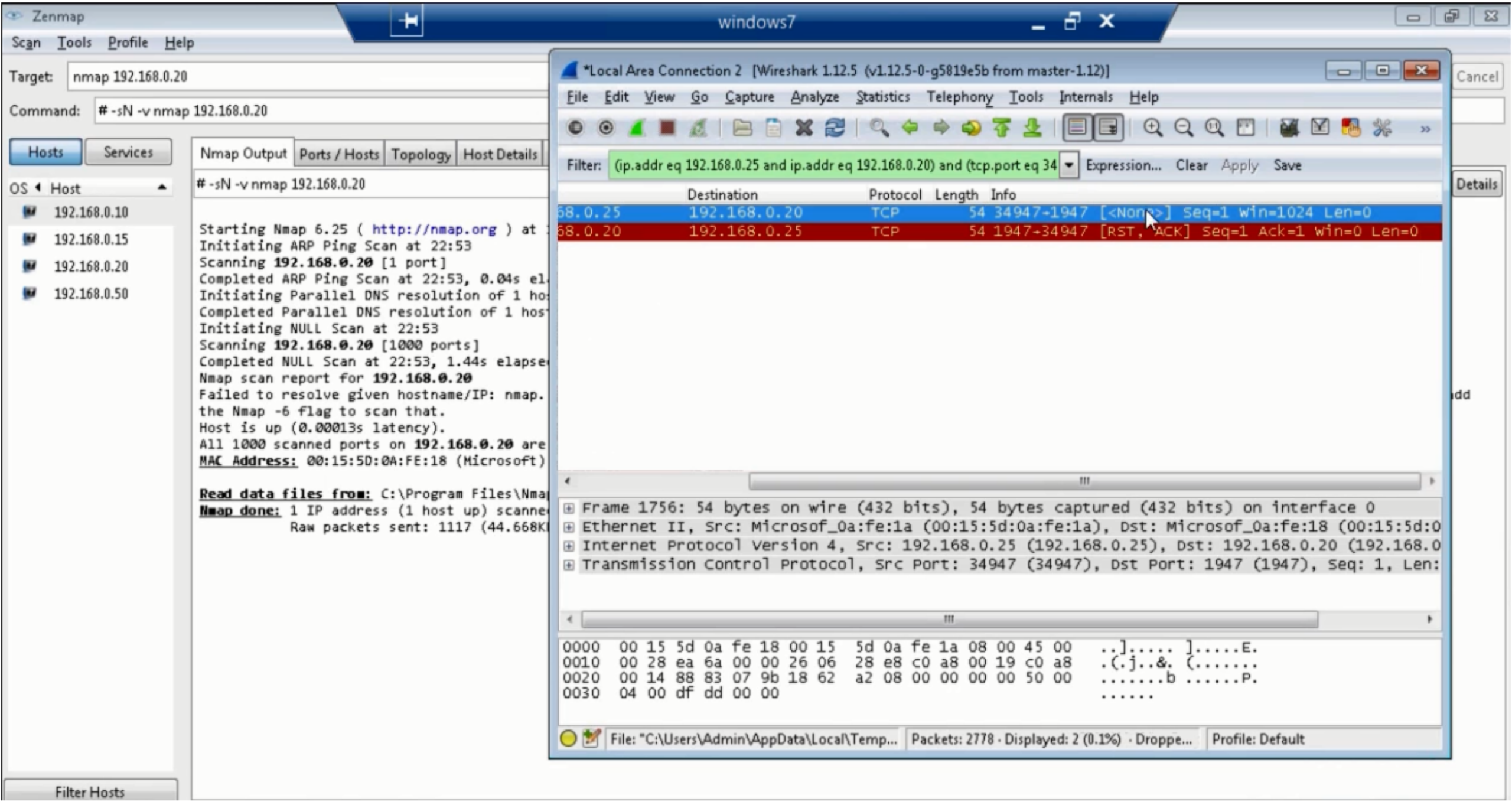
UNIX System Only

How a NULL Scan Works



How a NULL Scan Works




Zenmap
windows7
Scan Tools Profile Help
Target: nmap 192.168.0.20
Command: # -sN -v nmap 192.168.0.20
Cancel
Hosts Services
OS Host
192.168.0.10
192.168.0.15
192.168.0.20
192.168.0.50
Filter Hosts
Nmap Output Ports / Hosts Topology Host Details
-sN -v nmap 192.168.0.20
Starting Nmap 6.25 (http://nmap.org) at
Initiating ARP Ping Scan at 22:53
Scanning 192.168.0.20 [1 port]
Completed ARP Ping Scan at 22:53, 0.04s el
Initiating Parallel DNS resolution of 1 ho
Completed Parallel DNS resolution of 1 hos
Initiating NULL Scan at 22:53
Scanning 192.168.0.20 [1000 ports]
Completed NULL Scan at 22:53, 1.44s elapse
Nmap scan report for 192.168.0.20
Failed to resolve given hostname/IP: nmap.
the Nmap -6 flag to scan that.
Host is up (0.00013s latency).
All 1000 scanned ports on 192.168.0.20 are
MAC Address: 00:15:5D:0A:FE:18 (Microsoft)
Read data files from: C:\Program Files\Nma
Nmap done: 1 IP address (1 host up) scanne
Raw packets sent: 1117 (44.668K
Details
*Local Area Connection 2 [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: (ip.addr eq 192.168.0.25 and ip.addr eq 192.168.0.20) and (tcp.port eq 34
Expression... Clear Apply Save
Destination Protocol Length Info
68.0.25 192.168.0.20 TCP 54 34947→1947 [<None>] Seq=1 Win=1024 Len=0
68.0.20 192.168.0.25 TCP 54 1947→34947 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 1756: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: Microsof_0a:fe:1a (00:15:5d:0a:fe:1a), Dst: Microsof_0a:fe:18 (00:15:5d:0
Internet Protocol Version 4, Src: 192.168.0.25 (192.168.0.25), Dst: 192.168.0.20 (192.168.0
Transmission Control Protocol, Src Port: 34947 (34947), Dst Port: 1947 (1947), Seq: 1, Len:
0000 00 15 5d 0a fe 18 00 15 5d 0a fe 1a 08 00 45 00 ..].....].....E.
0010 00 28 ea 6a 00 00 26 06 28 e8 c0 a8 00 19 c0 a8 .(.j..&. (.....
0020 00 14 88 83 07 9b 18 62 a2 08 00 00 00 00 50 00 .....b ......P.
0030 04 00 df dd 00 00 ....
File: "C:\Users\Admin\AppData\Local\Temp...
Packets: 2778 · Displayed: 2 (0.1%) · Droppe...
Profile: Default

UDP Scans

Remember UDP?

No 3-way handshake!

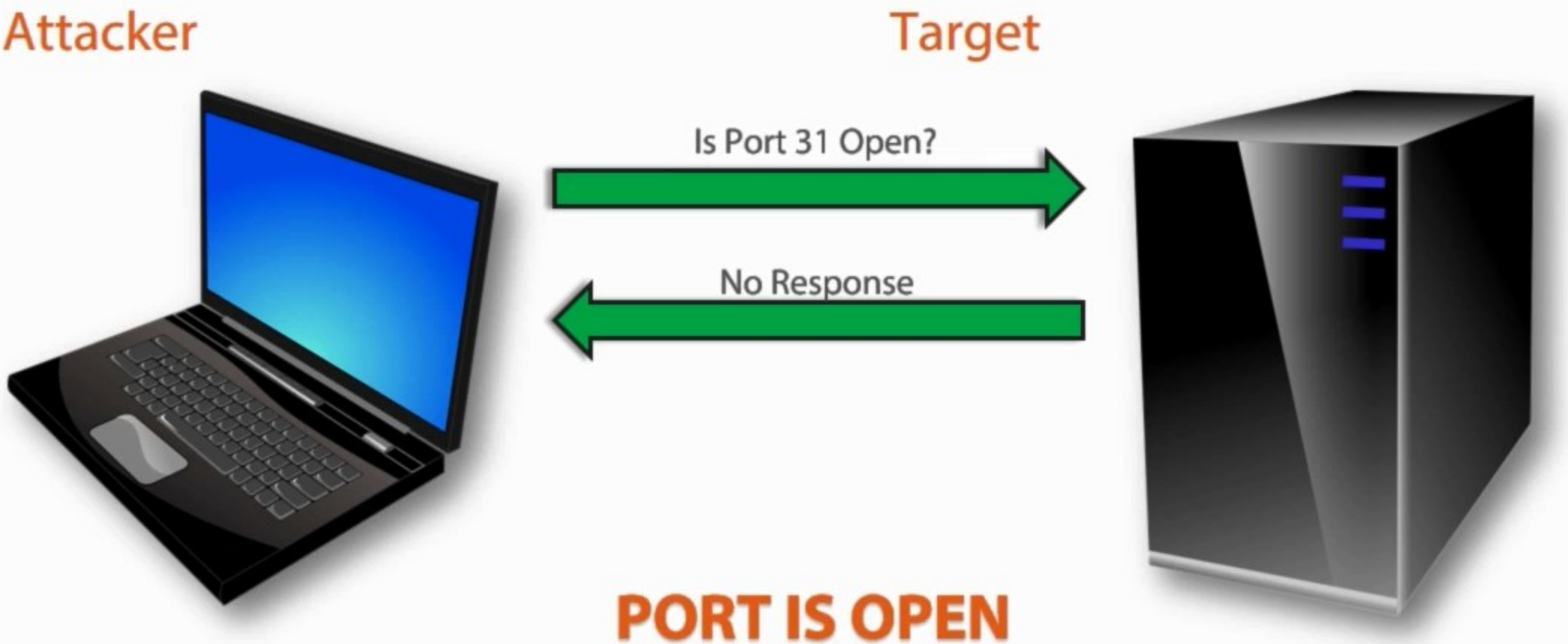
Advantages

- Harder to monitor
- No TCP overhead / # frames can be larger
- Very efficient against Windows targets

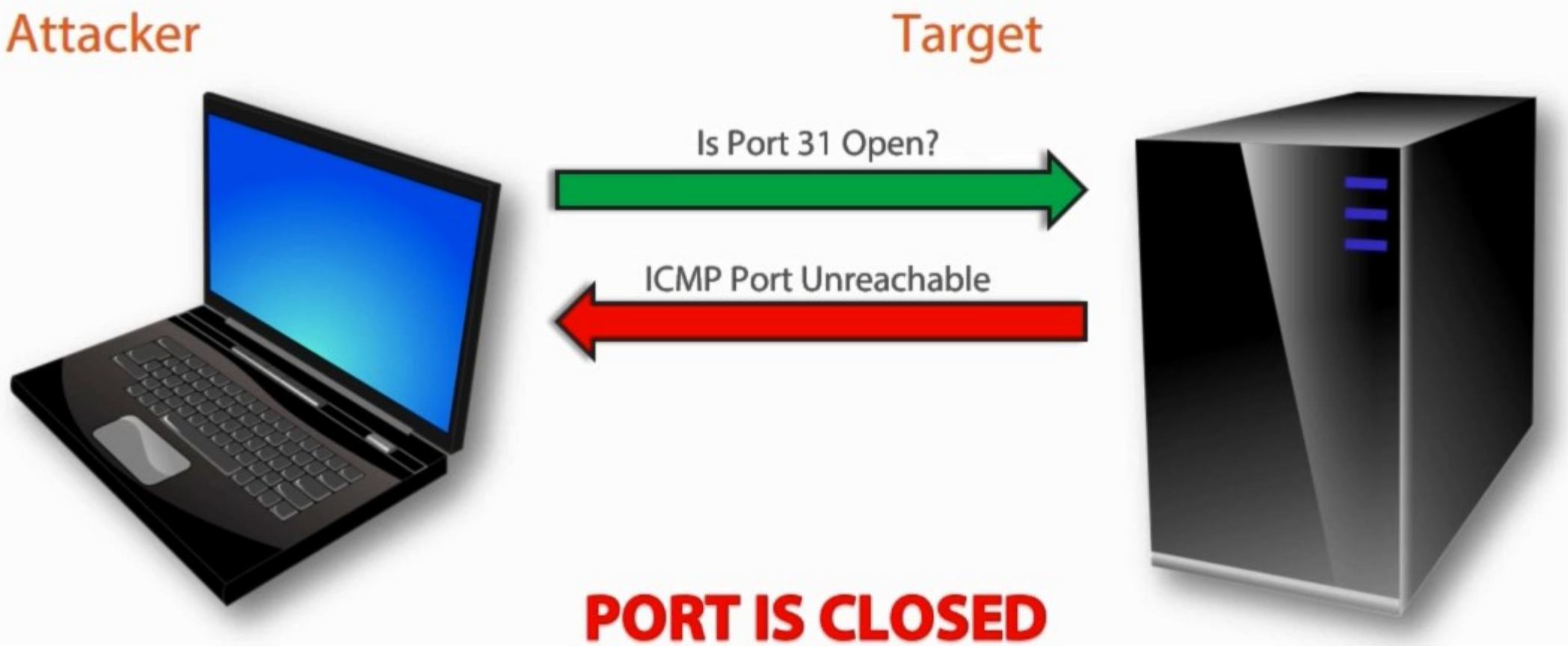
Disadvantages

- Port data only

How a UDP Scan Works



How a UDP Scan Works



IDS Evasion Methods

IDLE Scans

Uses TCP port scanning method BUT we spoof the "source address"

Advantages

Blame someone else ;-)

Disadvantages

Requires a zombie

1st Step

- Find/use a zombie
  - Send a SYN/ACK watch for the IP ID *make a note of it

Step #1 IDLE Scan

Attacker

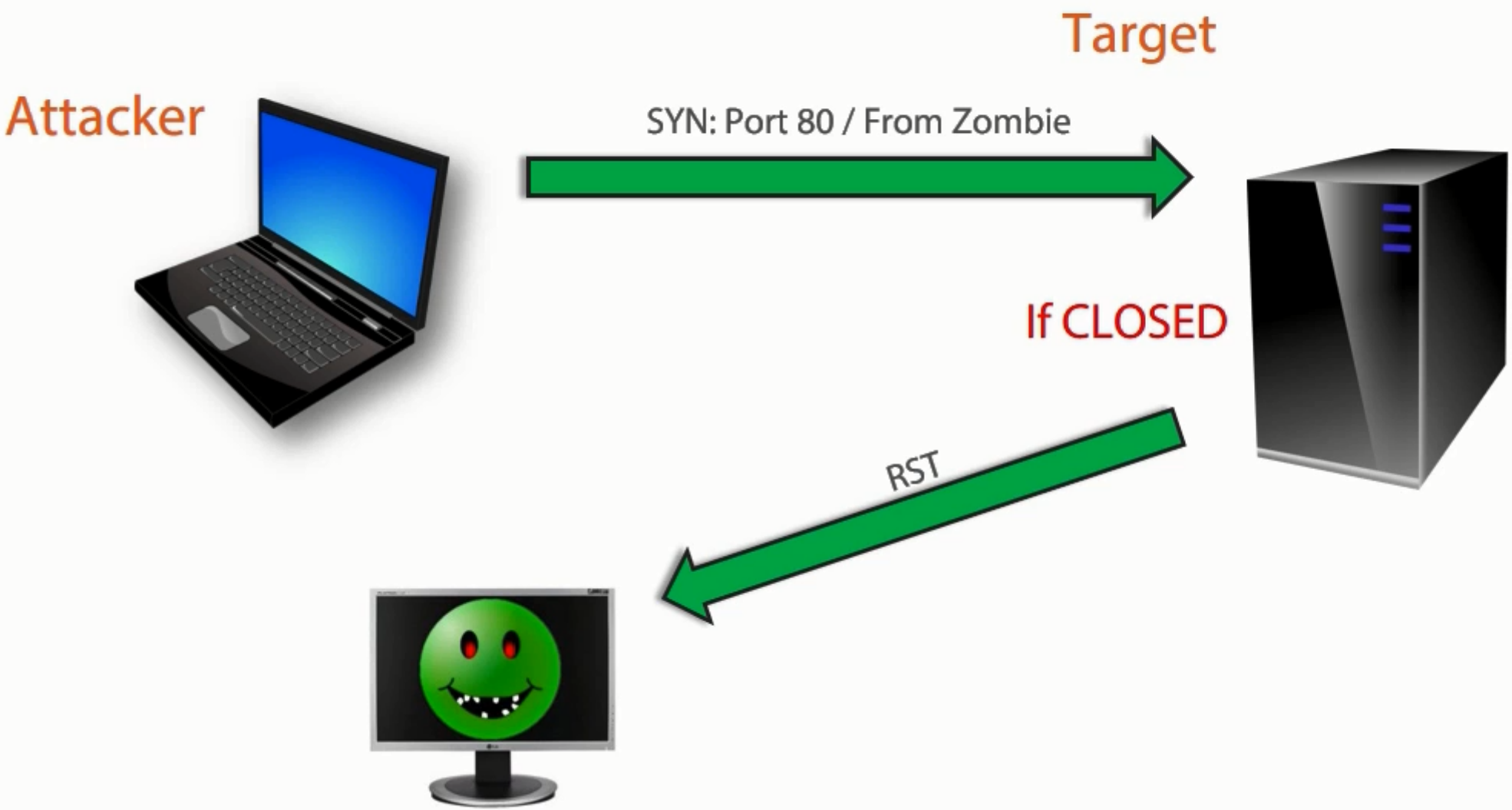
Zombie

SYN/ACK

RST / IPID=2001

PORT IS OPEN

Step #2 IDLE Scan



Step #3 IDLE Scan

Attacker

Zombie

SYN/ACK

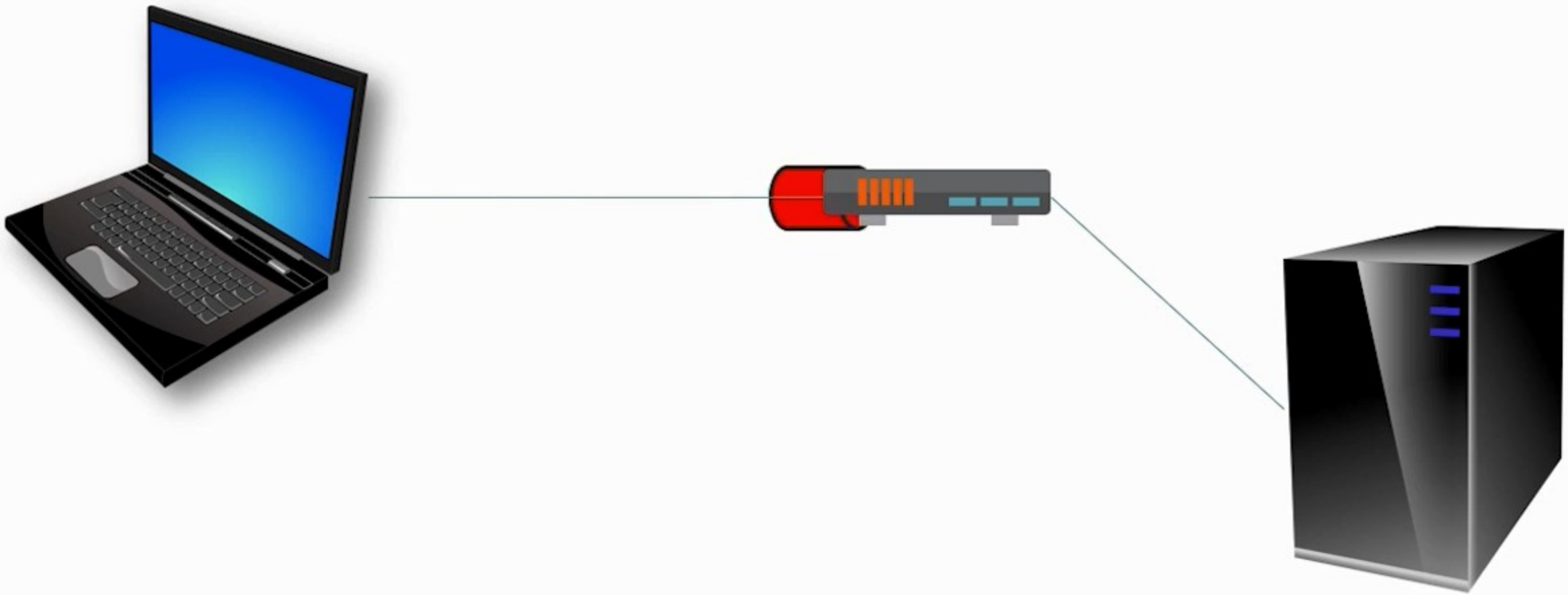
RST / IPID=2002

PORT IS CLOSED

There's Always a Way Around

- Spoof your IP and sniff the responses
- Use a proxy or pwned machine
- Fragment IP Packets
- If you're able, use source routing

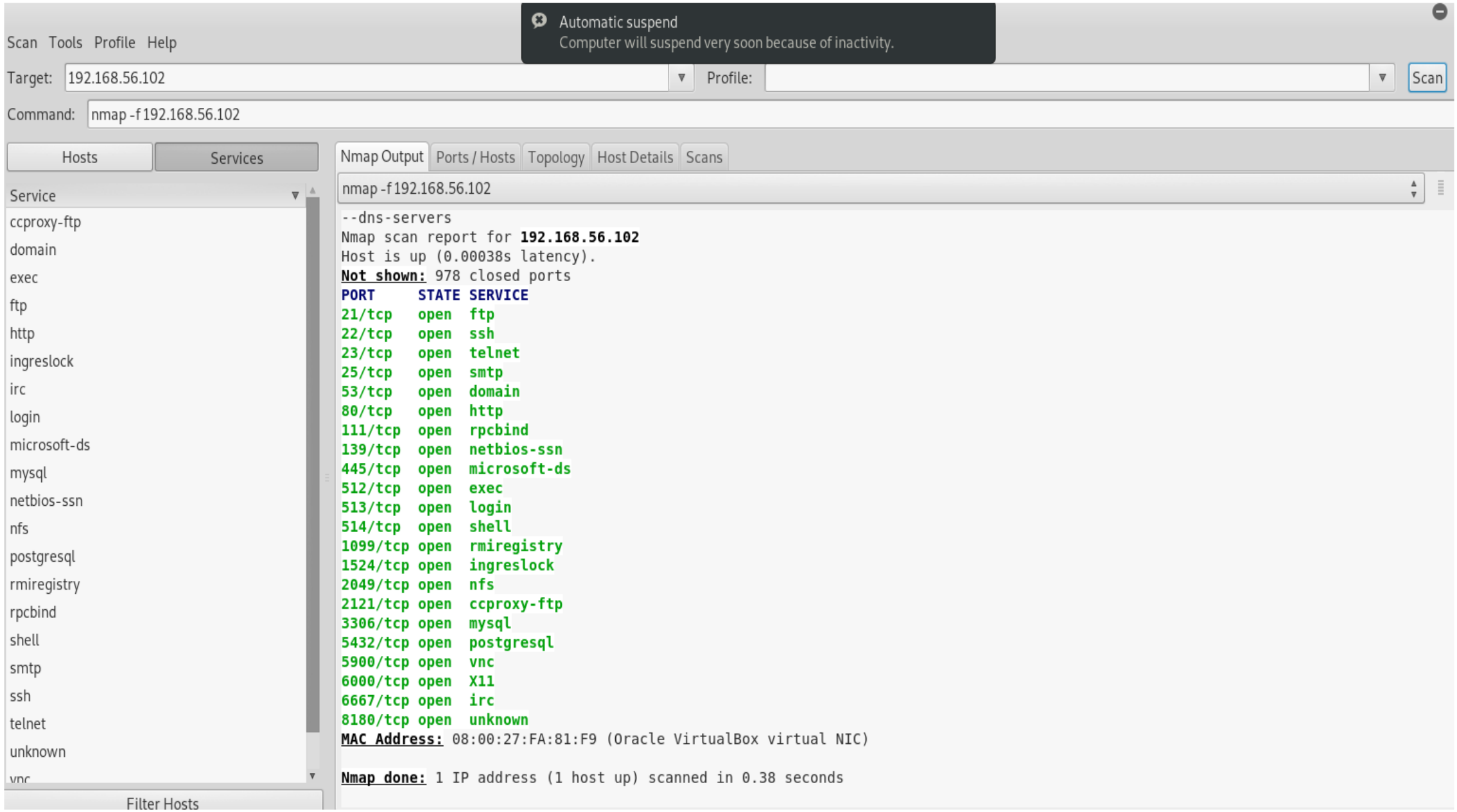
IP Fragments



Getting Around The IDS/Firewall

Nmap:

- Idle scan
- IP Fragment


Automatic suspend
Computer will suspend very soon because of inactivity.
Scan Tools Profile Help
Target: 192.168.56.102
Profile:
Scan
Command: nmap -f 192.168.56.102
Hosts
Services
Service
ccproxy-ftp
domain
exec
ftp
http
ingreslock
irc
login
microsoft-ds
mysql
netbios-ssn
nfs
postgresql
rmiregistry
rpcbind
shell
smtp
ssh
telnet
unknown
vnc
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -f 192.168.56.102
--dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00038s latency).
Not shown: 978 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8180/tcp open unknown
MAC Address: 08:00:27:FA:81:F9 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds

Countermeasures

Countermeasures

Firewalls configured to look for SYN Scans

IDS should detect Nmap/Snort

Open only require ports

Filter ICMP messages

Test your own network

Keep firewalls / IDS updated/patched

Banner Grabbing & OS Fingerprinting

Who Are You?

- O/S Fingerprinting
- Banner Grabbing
- Countermeasures

O/S Fingerprinting

Why Fingerprint?

O/S fingerprinting attempts to determine the host via packets

Know the OS…

Two Types

Active Fingerprinting

- Uses specially crafted packets
- Reponses are compared to a database of known responses
- Extremely high chance of detection

Passive Fingerprinting

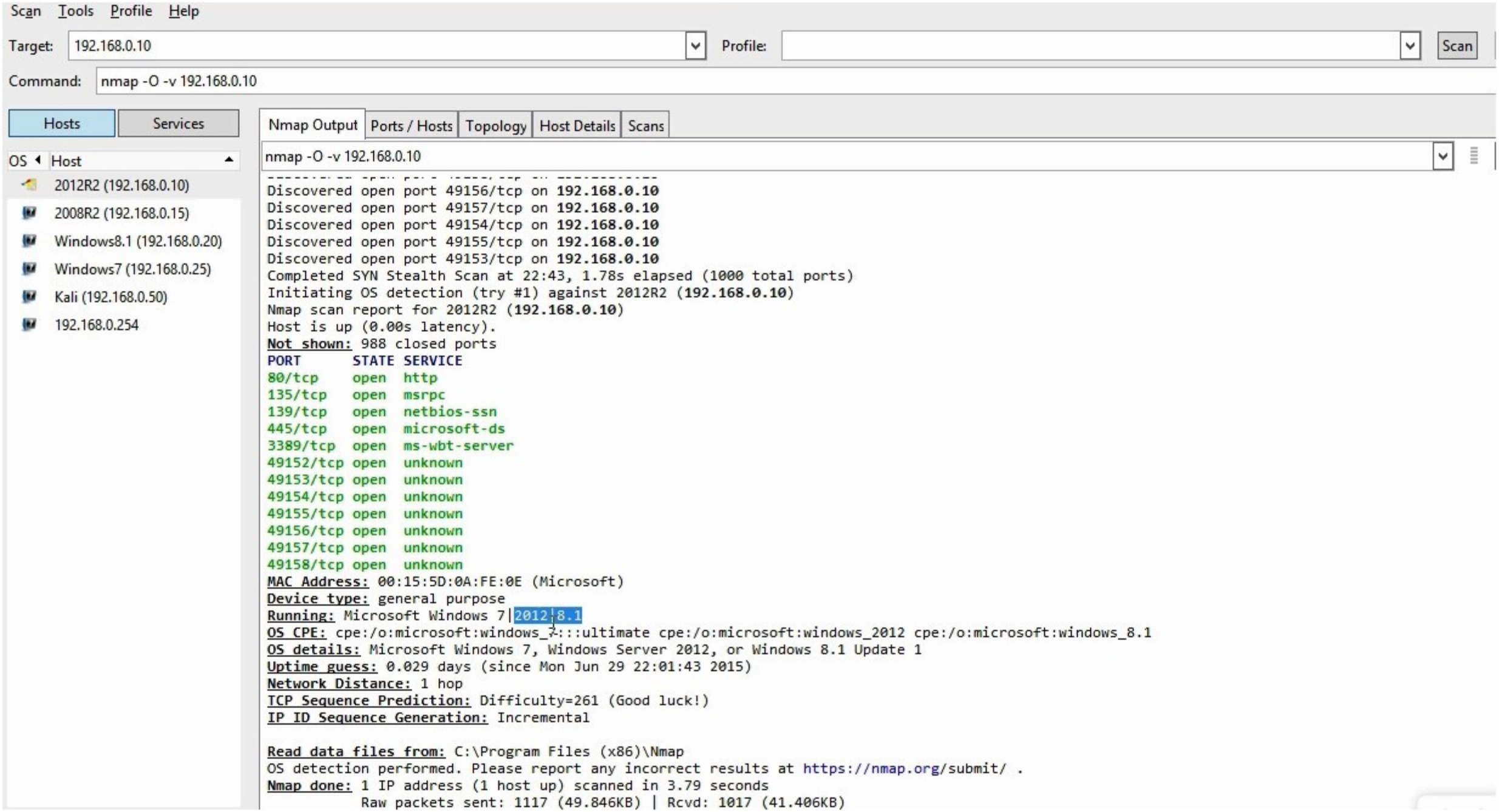
- Sniffs network traffic
- Responses are analyzed to discover any details that could ID the system
- Chances of detection are extremely low

Using Nmap

Sends various TCP/UDP

Results are compared to over 2,600 known OS's

Can resolve vendor, OS, version, device type


Scan Tools Profile Help
Target: 192.168.0.10
Profile:
Scan
Command: nmap -O -v 192.168.0.10
Hosts
Services
OS Host
2012R2 (192.168.0.10)
2008R2 (192.168.0.15)
Windows8.1 (192.168.0.20)
Windows7 (192.168.0.25)
Kali (192.168.0.50)
192.168.0.254
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -O -v 192.168.0.10
Discovered open port 49156/tcp on 192.168.0.10
Discovered open port 49157/tcp on 192.168.0.10
Discovered open port 49154/tcp on 192.168.0.10
Discovered open port 49155/tcp on 192.168.0.10
Discovered open port 49153/tcp on 192.168.0.10
Completed SYN Stealth Scan at 22:43, 1.78s elapsed (1000 total ports)
Initiating OS detection (try #1) against 2012R2 (192.168.0.10)
Nmap scan report for 2012R2 (192.168.0.10)
Host is up (0.00s latency).
Not shown: 988 closed ports
PORT STATE SERVICE
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
49157/tcp open unknown
49158/tcp open unknown
MAC Address: 00:15:5D:0A:FE:0E (Microsoft)
Device type: general purpose
Running: Microsoft Windows 7|2012|8.1
OS CPE: cpe:/o:microsoft:windows_7:::ultimate cpe:/o:microsoft:windows_2012 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1
Uptime guess: 0.029 days (since Mon Jun 29 22:01:43 2015)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Read data files from: C:\Program Files (x86)\Nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.79 seconds
Raw packets sent: 1117 (49.846KB) | Rcvd: 1017 (41.406KB)

Zenmap

Scan Tools Profile Help

Target: 192.168.0.1-254 Profile: Scan Cancel

Command: nmap 192.168.0.1-254

Hosts Services

OS Host

- 2012R2 (192.168.0.1
- 2008R2 (192.168.0.1
- Windows8.1 (192.16
- Windows7 (192.168
- Kali (192.168.0.50)
- 192.168.0.254

Nmap Output Ports / Hosts Topology Host Details Scans

nmap 192.168.0.1-254 Details

```
Starting Nmap 6.49BETA2 ( http://nmap.org ) at 2015-06-29 22:05 Mountain Daylight Time
Nmap scan report for 2012R2 (192.168.0.10)
Host is up (0.00s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
MAC Address: 00:15:5D:0A:FE:0E (Microsoft)

Nmap scan report for 2008R2 (192.168.0.15)
Host is up (0.00s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:15:5D:0A:FE:17 (Microsoft)
```

Zenmap

Scan Tools Profile Help

Target: 192.168.0.20-50 Profile: Scan Cancel

Command: nmap -O -v 192.168.0.20-50

Hosts Services

OS Host

- 2012R2 (192.168.0.10)
- 2008R2 (192.168.0.15)
- Windows8.1 (192.168.0.20)
- Windows7 (192.168.0.25)
- Kali (192.168.0.50)
- 192.168.0.254

Nmap Output Ports / Hosts Topology Host Details Scans

Closed ports: 988
Scanned ports: 1000
Up time: 2496
Last boot: Mon Jun 29 22:01:43 2015

Addresses

IPv4: 192.168.0.10
IPv6: Not available
MAC: 00:15:5D:0A:FE:0E

Hostnames

Name - Type: 2012R2 - PTR

Operating System

Name: Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1

Accuracy: 100%

Ports used

OS Classes

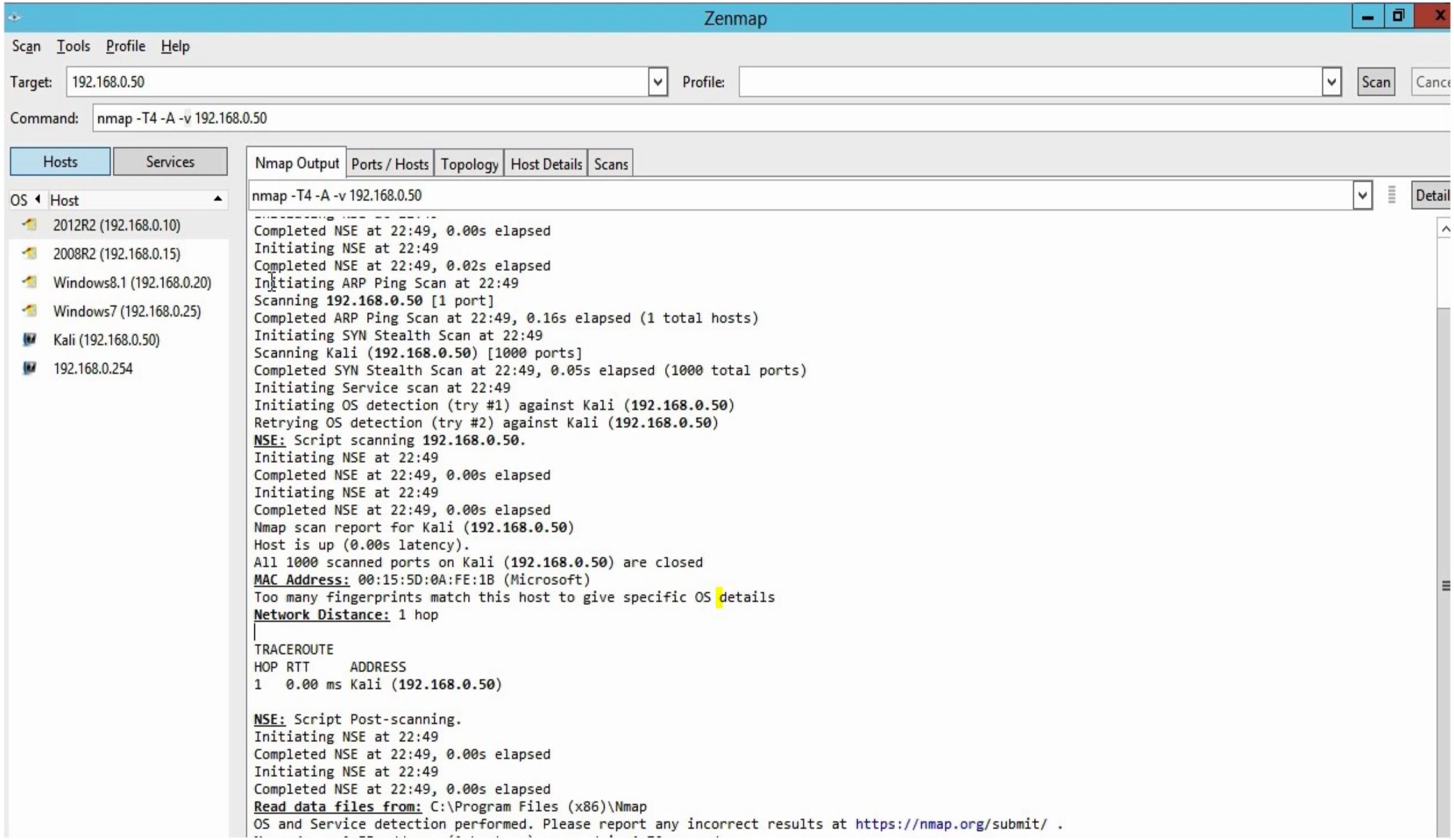
TCP Sequence

IP ID Sequence

TCP TS Sequence

Comments

notes about this machine


Zenmap
Scan Tools Profile Help
Target: 192.168.0.50
Profile:
Scan
Command: nmap -T4 -A -v 192.168.0.50
Hosts
Services
OS Host
2012R2 (192.168.0.10)
2008R2 (192.168.0.15)
Windows8.1 (192.168.0.20)
Windows7 (192.168.0.25)
Kali (192.168.0.50)
192.168.0.254
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 192.168.0.50
Completed NSE at 22:49, 0.00s elapsed
Initiating NSE at 22:49
Completed NSE at 22:49, 0.02s elapsed
Initiating ARP Ping Scan at 22:49
Scanning 192.168.0.50 [1 port]
Completed ARP Ping Scan at 22:49, 0.16s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 22:49
Scanning Kali (192.168.0.50) [1000 ports]
Completed SYN Stealth Scan at 22:49, 0.05s elapsed (1000 total ports)
Initiating Service scan at 22:49
Initiating OS detection (try #1) against Kali (192.168.0.50)
Retrying OS detection (try #2) against Kali (192.168.0.50)
NSE: Script scanning 192.168.0.50.
Initiating NSE at 22:49
Completed NSE at 22:49, 0.00s elapsed
Initiating NSE at 22:49
Completed NSE at 22:49, 0.00s elapsed
Nmap scan report for Kali (192.168.0.50)
Host is up (0.00s latency).
All 1000 scanned ports on Kali (192.168.0.50) are closed
MAC Address: 00:15:5D:0A:FE:1B (Microsoft)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 0.00 ms Kali (192.168.0.50)
NSE: Script Post-scanning.
Initiating NSE at 22:49
Completed NSE at 22:49, 0.00s elapsed
Initiating NSE at 22:49
Completed NSE at 22:49, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

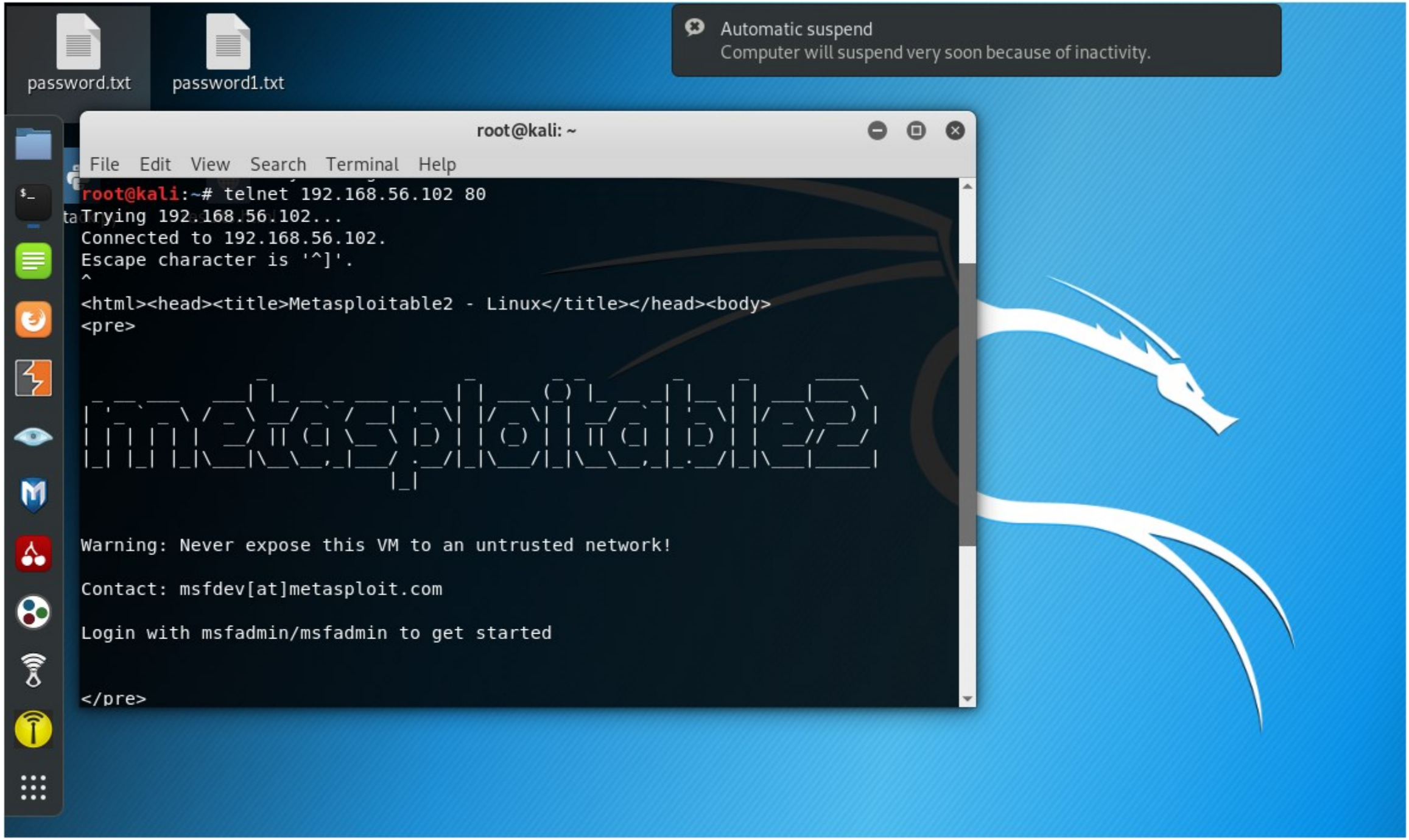
Banner Grabbing

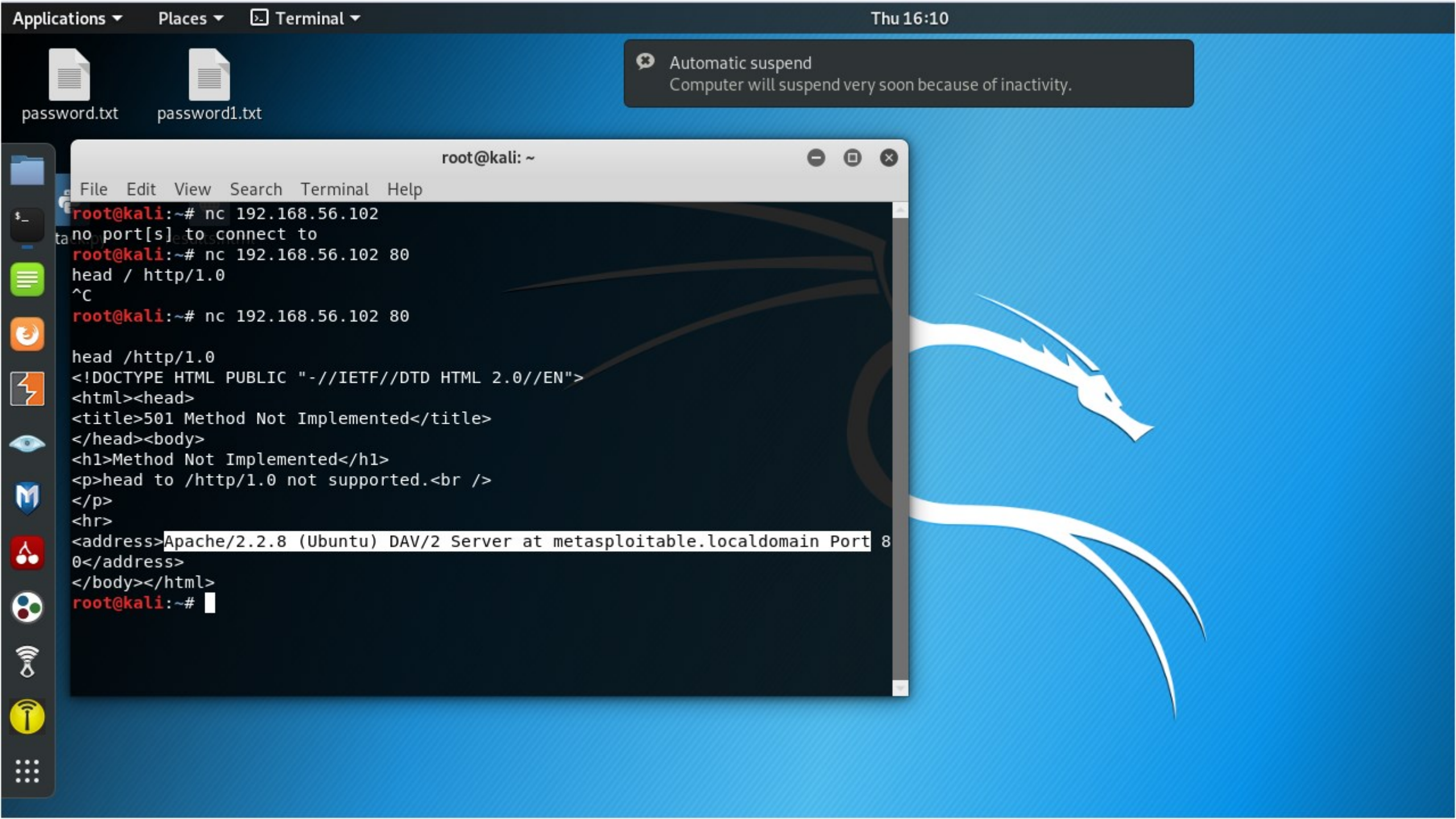
The Welcome Mat of Computers

- Welcome messages that ID software and other system info
- Normally you can use Netcat
- Xprobe
- p0f

Using Telnet and Netcat

Very active | ID a server | ID a service


password.txt
password1.txt
Automatic suspend
Computer will suspend very soon because of inactivity.
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# telnet 192.168.56.102 80
Trying 192.168.56.102...
Connected to 192.168.56.102.
Escape character is '^]'.
^
<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
</pre>


Applications
Places
Terminal
Thu 16:10
password.txt
password1.txt
Automatic suspend
Computer will suspend very soon because of inactivity.
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nc 192.168.56.102
no port[s] to connect to
root@kali:~# nc 192.168.56.102 80
head / http/1.0
^C
root@kali:~# nc 192.168.56.102 80
head /http/1.0
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>501 Method Not Implemented</title>
</head><body>
<h1>Method Not Implemented</h1>
head to /http/1.0 not supported.

<hr>
<address>Apache/2.2.8 (Ubuntu) DAV/2 Server at metasploitable.localdomain Port 8
0</address>
</body></html>
root@kali:~#

Countermeasures

Is There Anything I Can Do to Stop This?

Misdirection / fake banners

IIS lockdown tool

ServerMask

Turn off unused services

Change the ServerSignature (httpd.conf)

Speaking of httpd.conf: mod_headers

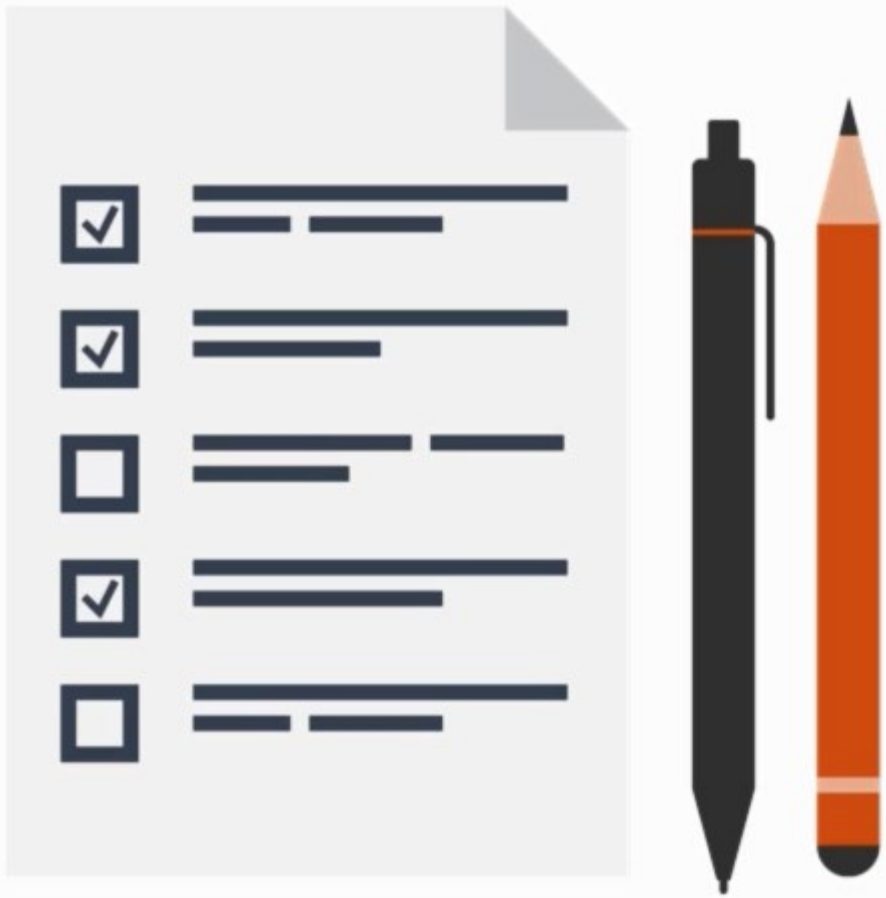
Vulnerability Scanning and Drawing Out the Network

Know Your Greatest Weakness

- What Is Vulnerability Scanning
- How Does Vulnerability Scanning Work
- Vulnerability Scanning Tools
- Why Draw Out the Network
- Tools to Help Visualize

What Is Vulnerability Scanning

The Basics



Software

Looks at

- Network systems
- Computers
- Operating systems
- Applications

Types of Scanners

Network based

- Web server scanners
- Port Scanners
- Web App Scanners

Host based

- Designed for specific hosts
- Look for signs of penetration
- Performs baselines checks

How Does Vulnerability Scanning Work

Limitations

Human judgment

It's only a snapshot

Only "known" vulnerabilities

Limitations

Parts is parts
(or plugins)

Benefits

Detect & resolving of security issues

New device / rogue systems

Verify inventory

NVD - Search

https://web.nvd.nist.gov/view/vuln/search

Sponsored by DHS/NCCIC/US-CERT

NIST National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

70912 CVE Vulnerabilities
298 Checklists
249 US-CERT Alerts
4365 US-CERT Vuln Notes
10286 OVAL Queries
104891 CPE Names

Last updated: 7/1/2015 3:59:36 PM

CVE Publication rate: 16.33

Email List

NVD provides four mailing lists to the public. For information and subscription instructions please visit NVD Mailing Lists

Workload Index

Vulnerability Workload Index: 6.67

About Us

Search CVE and CCE Vulnerability Database

(Advanced Search)

Keyword search: Search

Try a product or vendor name
Try a CVE standard vulnerability name or OVAL query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

- (•) Search All
- ( ) Search Last 3 Months
- ( ) Search Last 3 Years

Show only vulnerabilities that have the following associated resources:

- [x] Software Flaws (CVE)
- [ ] Misconfigurations (CCE), under development

- [ ] US-CERT Technical Alerts
- [ ] US-CERT Vulnerability Notes
- [ ] OVAL Queries

NVD now maps to CWE! See NVD CWE for more details.

www.us-cert.gov

The Gears of Vulnerability Scanners

1) Engine runs security check
2) Database stores results & info
3) Reporting services
4) UI

Vulnerability Scanning Tools

Some Many Choices, So Little Time

Considerations

- Updates and plugins
- Quality vs. accuracy
- Reporting options

Deployment

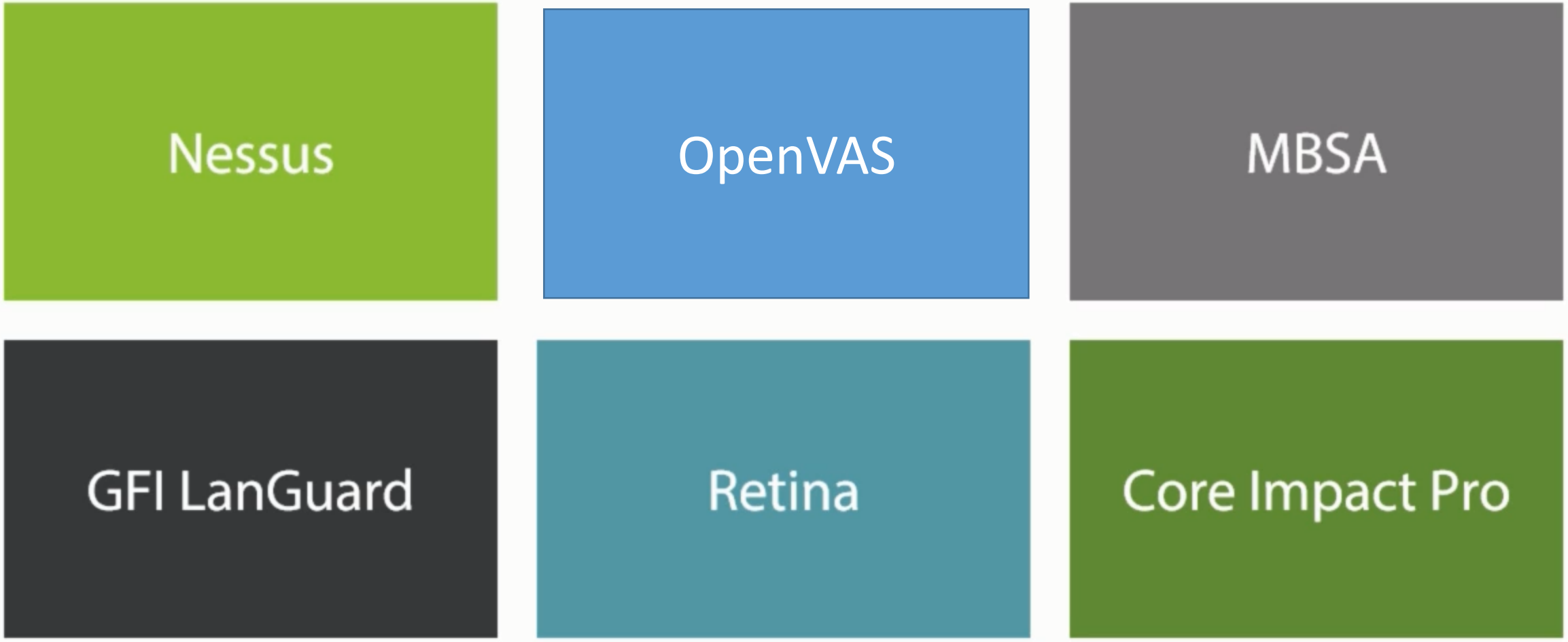
- Placement of scanner
- Port ranges
- Baseline setup
- Post scanning practices

Be Aware Of…

Possible issues

- Potential threats
- Handling results
- Policies and actions

Tools, Tools, and More Tools



https://localhost:8834/nessus6.html#/scans/5/hosts/2/vulnerabilitie Certificate error Nessus Home / Scans

Nessus Scans Policies admin

Baseline Scan

CURRENT RESULTS: TODAY AT 11:05 AM

Configure

Hosts > **192.168.0.10** > **Vulnerabilities** 28

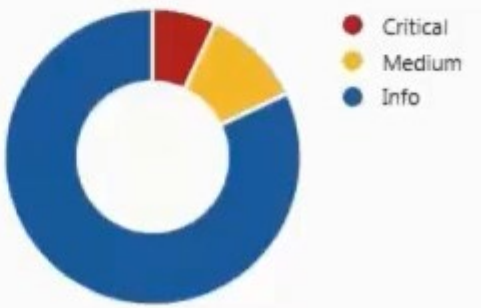
Severity	Plugin Name	Plugin Family	Count
CRITICAL	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execu...	Windows	1
CRITICAL	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execut...	Windows	1
MEDIUM	SMB Signing Required	Misc.	1
MEDIUM	SSL Certificate Cannot Be Trusted	General	1
MEDIUM	SSL Self-Signed Certificate	General	1
INFO	DCE Services Enumeration	Windows	9
INFO	Nessus SYN scanner	Port scanners	5
INFO	Microsoft Windows SMB Service Detection	Windows	2
INFO	Common Platform Enumeration (CPE)	General	1

Plugin ID: 82828

Host Details

IP:	192.168.0.10
DNS:	Server2012r2
MAC:	00:15:5d:0a:fe:0e
OS:	Microsoft Windows Server 2012 R2 Standard
Start:	Today at 11:05 AM

Vulnerabilities

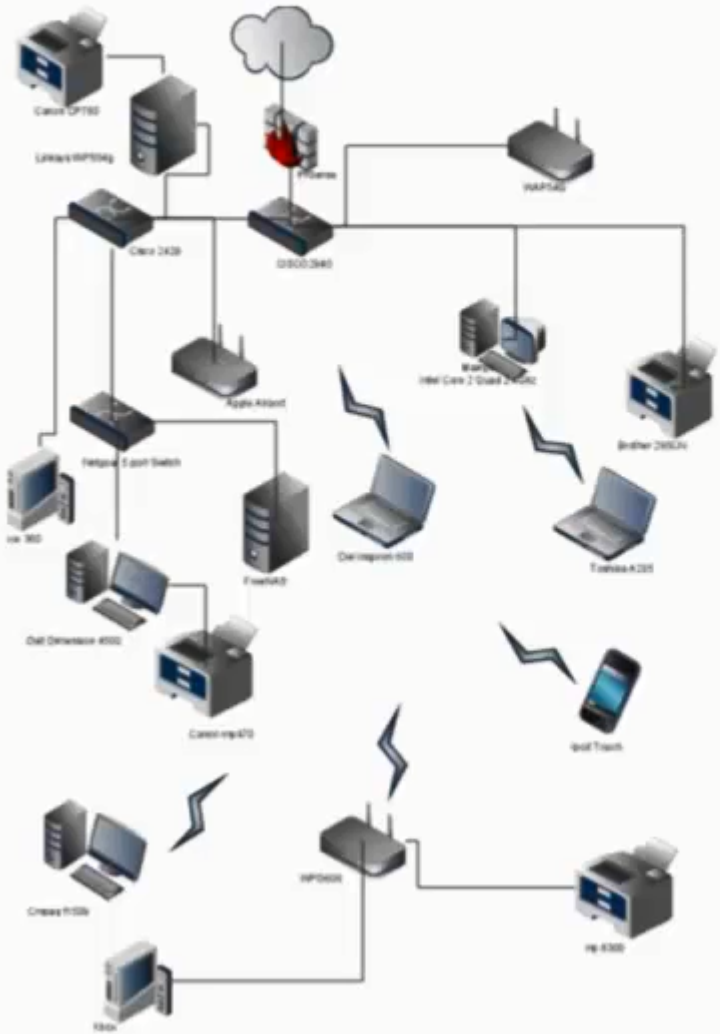


Why Draw Out the Network

Taking Notes

- You're not the only network
- Helps to visualize architecture
- Fill in the missing pieces
- Helps IT to manage their networks

What Do You See?



What does this map show?

- OS?
- Devices?
- Apps?
- Architecture?

You Say “Tomato”, I say “Tomato”

WhatsUp Gold

OpManger

NetworkView

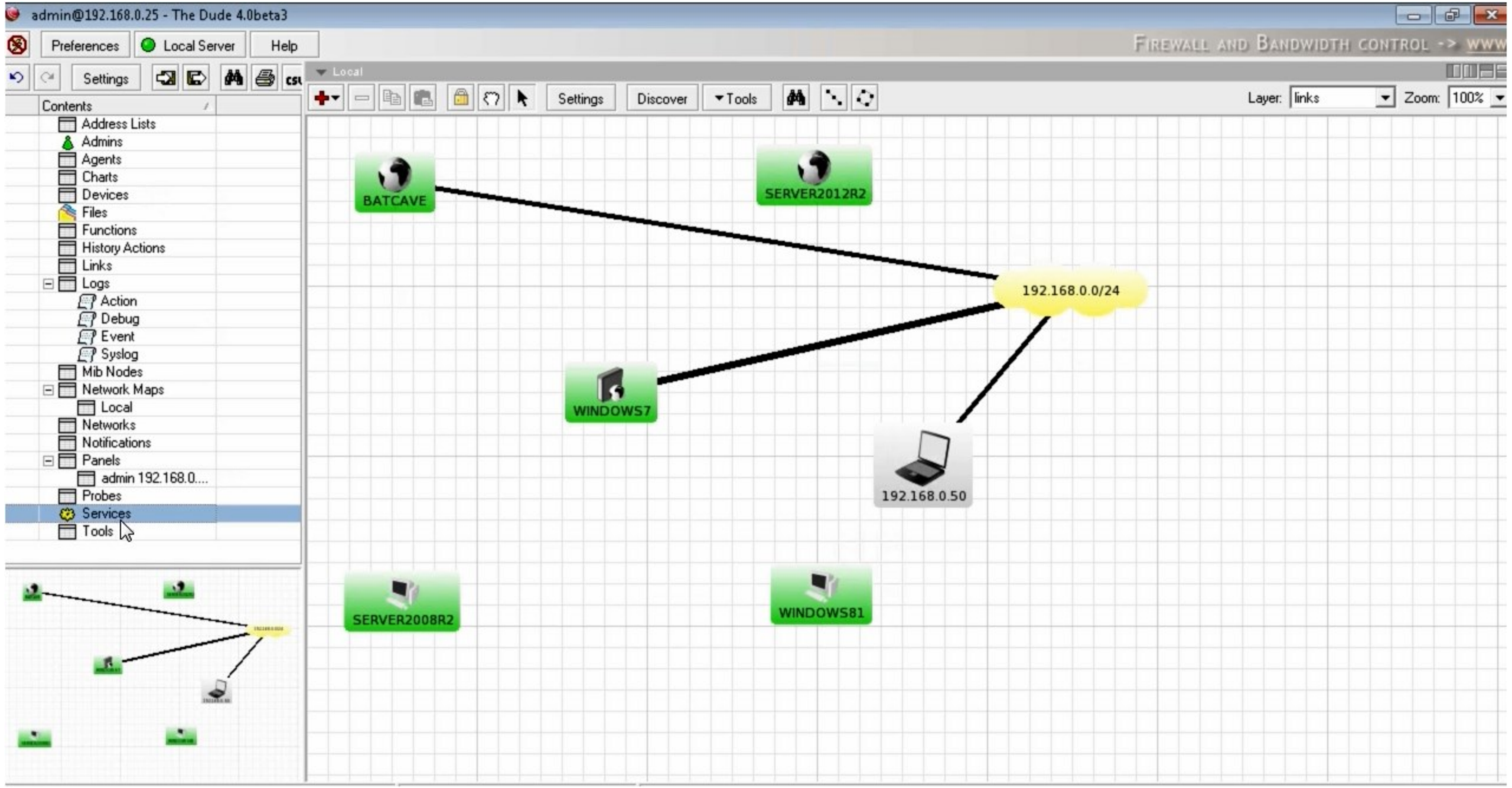
LANsurveyor

The Dude

FriendlyPinger

Mapping with The Dude

- Discovery
- Auto layout
- Customize and make notes


admin@192.168.0.25 - The Dude 4.0beta3
Preferences
Local Server
Help
Settings
Contents
Address Lists
Admins
Agents
Charts
Devices
Files
Functions
History Actions
Links
Logs
Action
Debug
Event
Syslog
Mib Nodes
Network Maps
Local
Networks
Notifications
Panels
admin 192.168.0....
Probes
Services
Tools
Local
Settings
Discover
Tools
Layer:
links
Zoom:
100%
BATCAVE
SERVER2012R2
192.168.0.0/24
WINDOWS7
192.168.0.50
SERVER2008R2
WINDOWS81