Classifying theTypes of Scanning

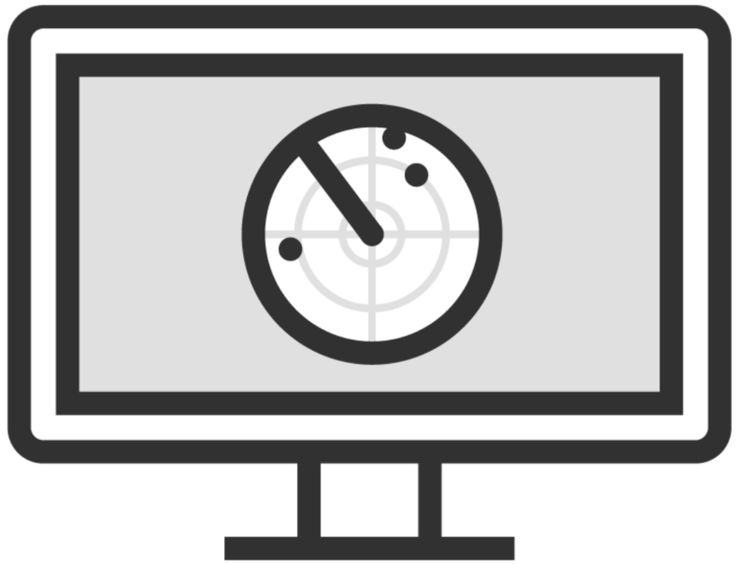
Dale Meredith
MCT/CEI/CEH/Security Dude
Owner: Wayne Technologies

:@dalemeredith :daledumbsITdown :daledumbsITdown
:dalemeredith www.daledumbsITdown.com

Scanning for life signs, Captain.

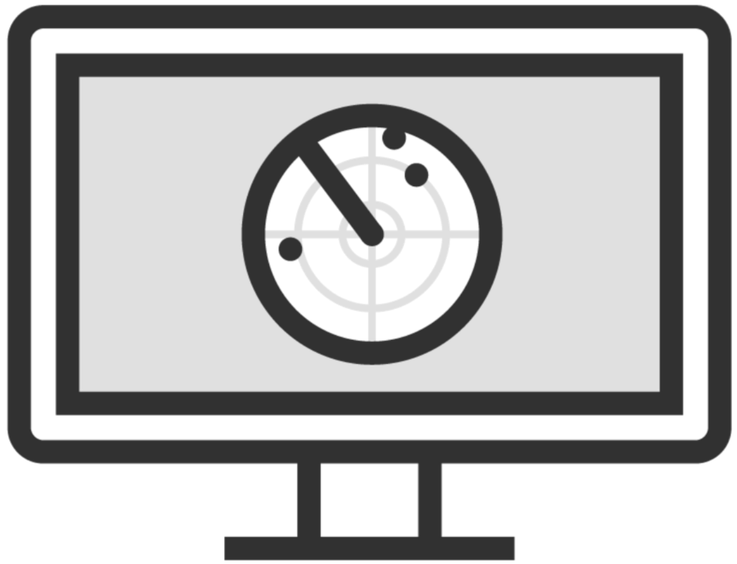
Spock

A Plethora of Scanning



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

A Plethora of Scanning



UDP Scans

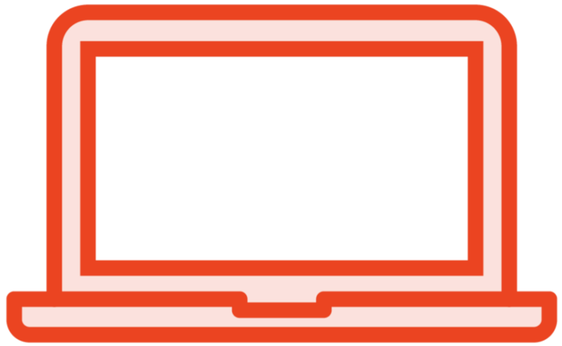
IDS Evasion Methods

Countermeasures

Full Scans

How a Full Scan Works

Attacker



SYN Packet + Port #

SYN / ACK

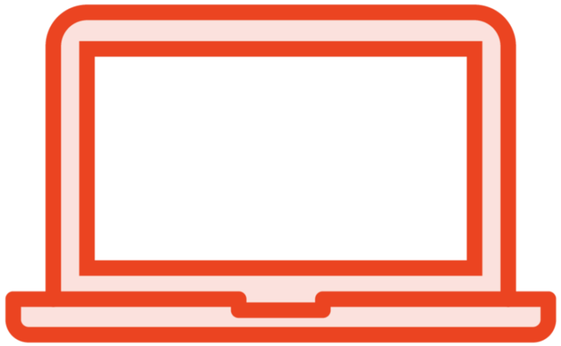
ACK + RST

PORT IS OPEN

Target

How a Full Scan Works

Attacker



SYN Packet + Port #

RST

PORT IS CLOSED

Target

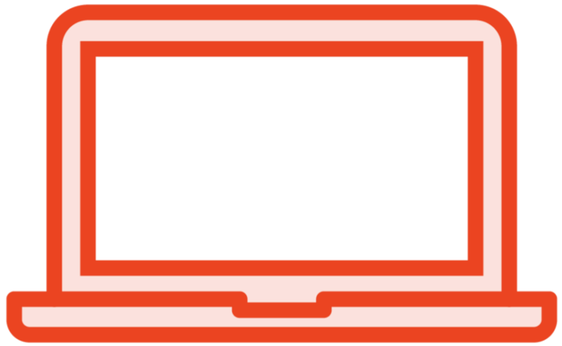
Demo

Let’s watch a Full Scan

Half-Open/Stealth Scans

How a Half-Open Scan Works

Attacker



SYN Packet + Port #

SYN / ACK

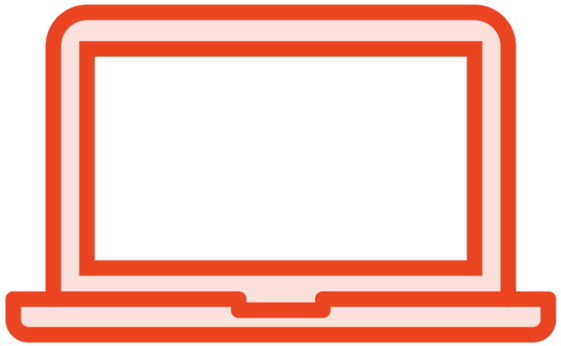
RST

Target

PORT IS OPEN

How a Half-Open Scan Works

Attacker



SYN Packet + Port #

RST

PORT IS CLOSED

Target

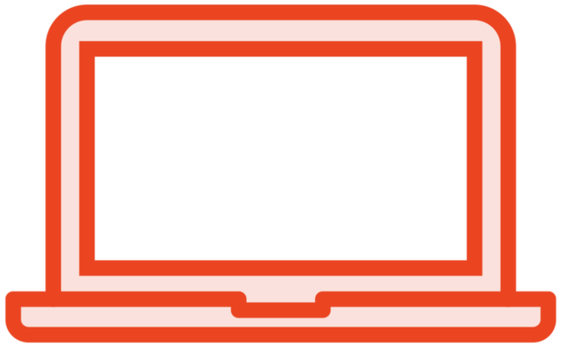
Demo

Let’s watch a Half-Open Scan

Xmas Scans

How a Xmas Scans Works

Attacker



FIN, URG, PUSH

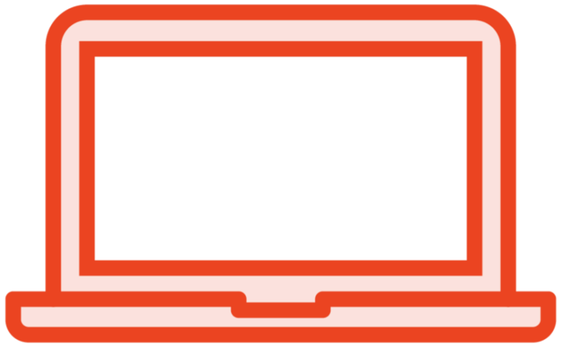
Nothing

Target

PORT IS OPEN

How a Xmas Scans Works

Attacker



FIN, URG, PUSH

RST

Target

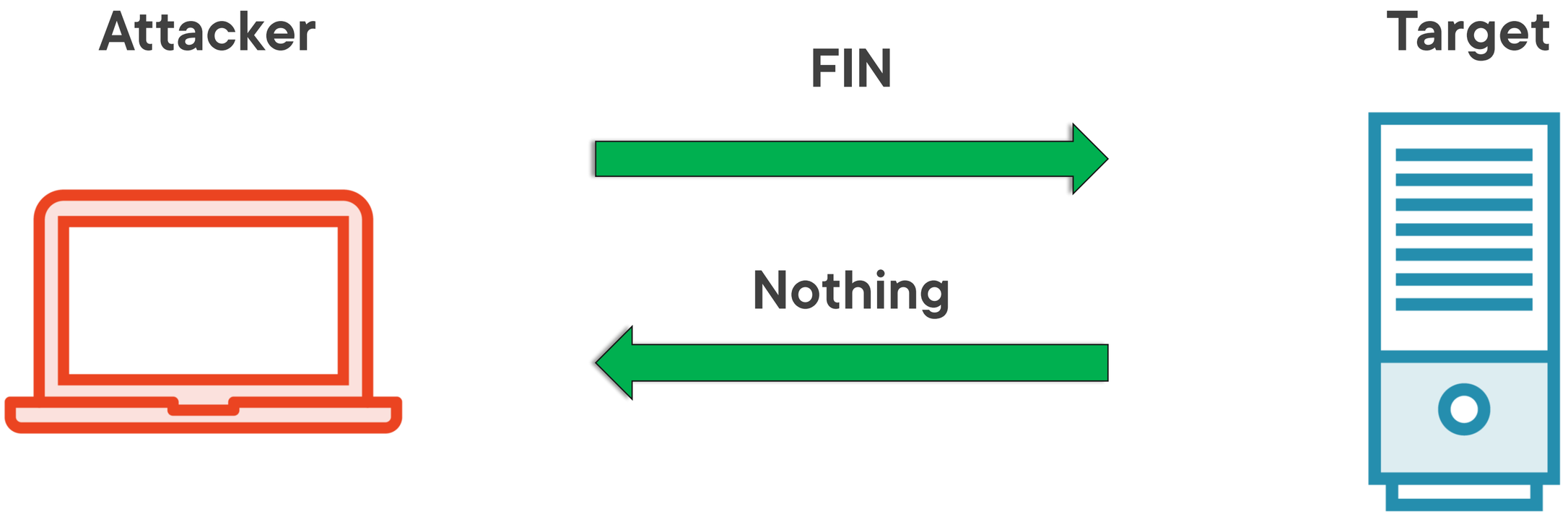
PORT IS CLOSED

Demo

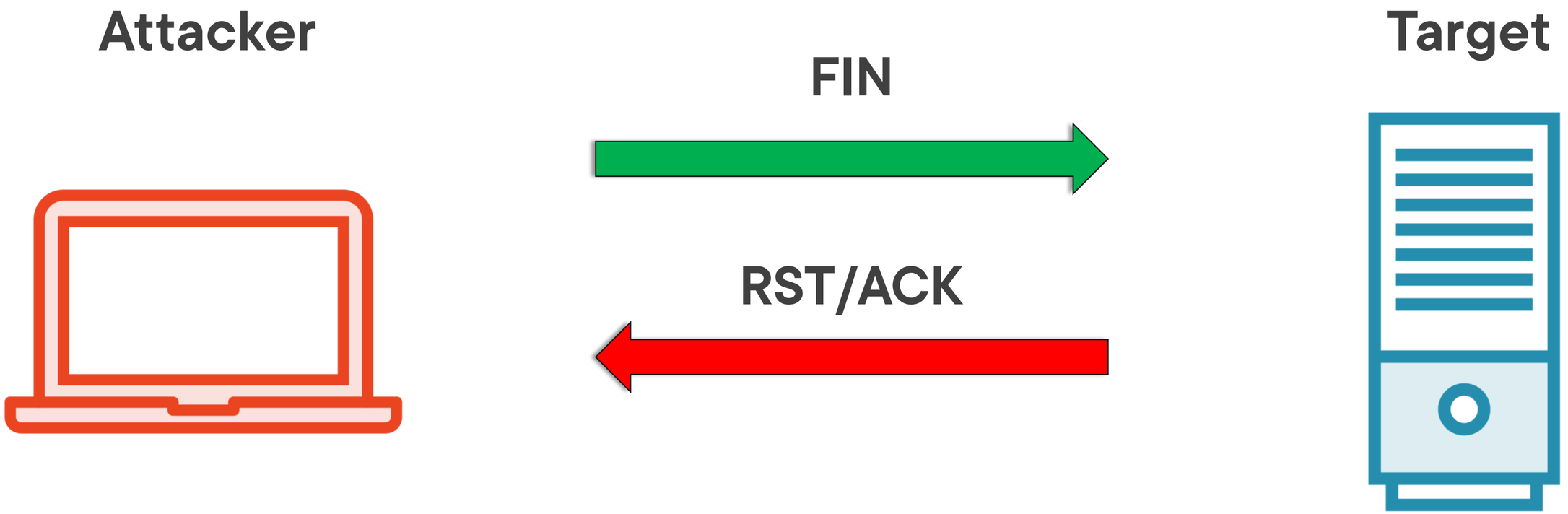
Let’s watch a Xmas Scan

FIN Scans

How a FIN Scans Works



How a FIN Scans Works



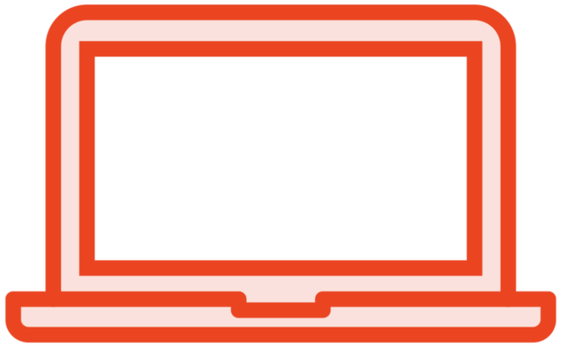
Demo

Let’s watch a FIN Scan

NULL Scans

How a NULL Scans Works

Attacker



TCP Packet / No Flag

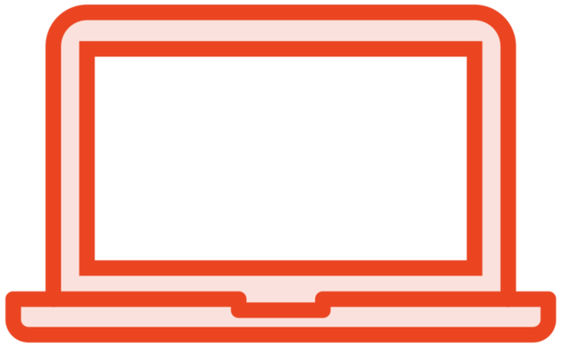
No Response

Target

PORT IS OPEN

How a NULL Scans Works

Attacker



TCP Packet / No Flag

RST/ACK

Target

PORT IS CLOSED

Demo

Let’s watch a NULL Scan

UDP Scans

Remember UDP?

No 3-way handshake!

Advantages

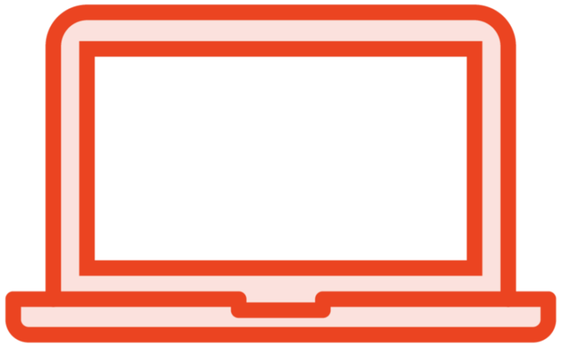
- **Harder to monitor**
- **No TCP overhead / # frames can be larger**
- **Very efficient against Windows targets**

Disadvantages

- **Port data only**

How a UDP Scans Works

Attacker



Is Port 31 Open?

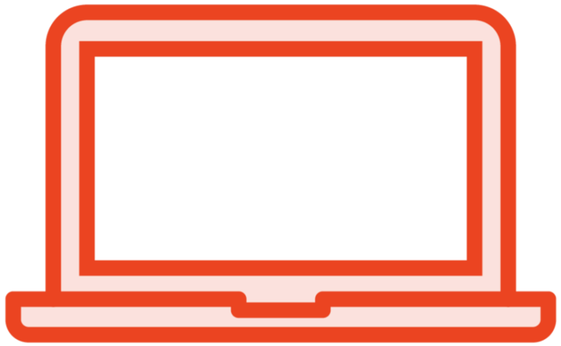
No Response

Target

PORT IS OPEN

How a UDP Scans Works

Attacker



Is Port 31 Open?

ICMP Port Unreachable

Target

PORT IS CLOSED

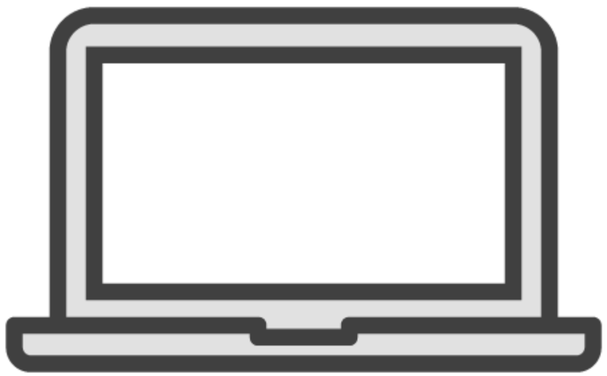
Demo

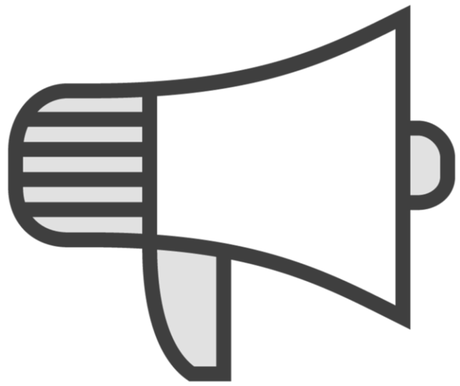
Let’s watch a UDP Scan

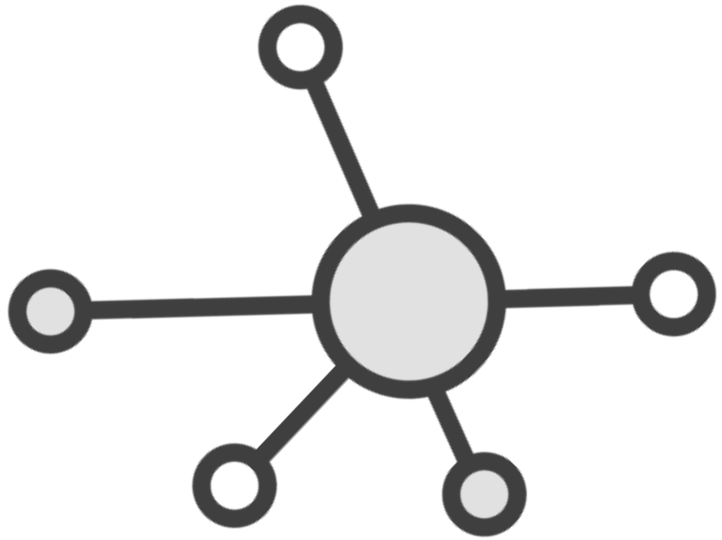
Listing and SSP Scans

Listing Scanning

SSDP Scanning





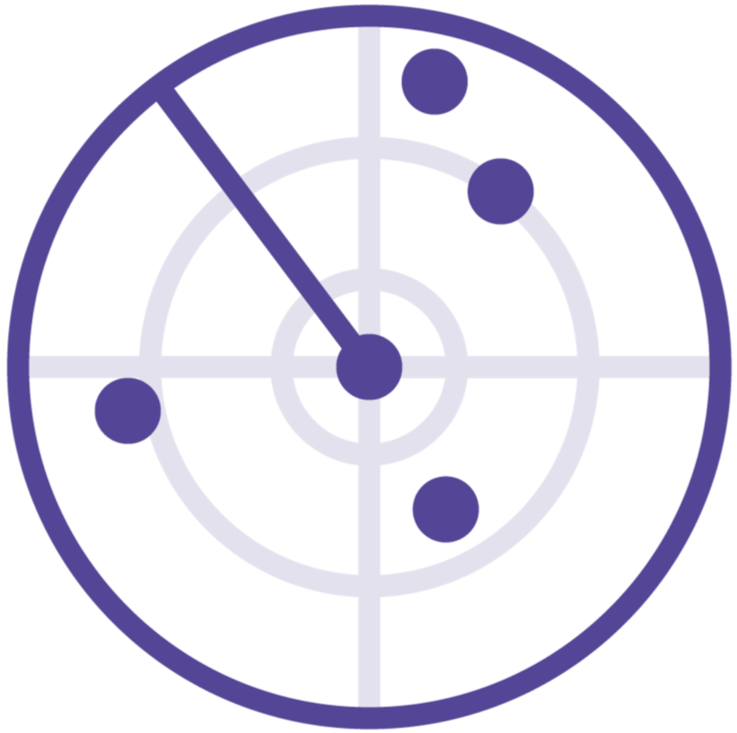


Demo

List Scan with Kali

IDS Evasion Methods

IDLE Scans



Uses TCP port scanning method BUT we spoof the “source address”

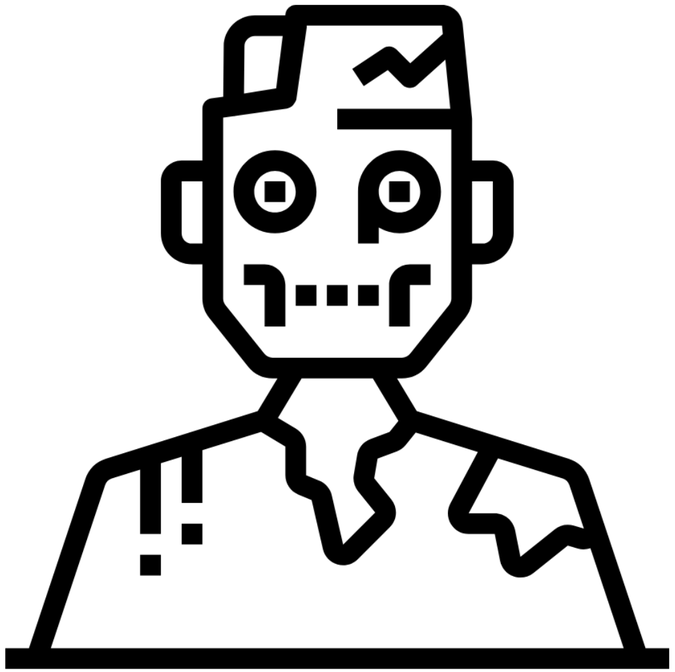
Advantages

- **Blame someone else ;-)**

Disadvantages

- **Requires a zombie**

First Step

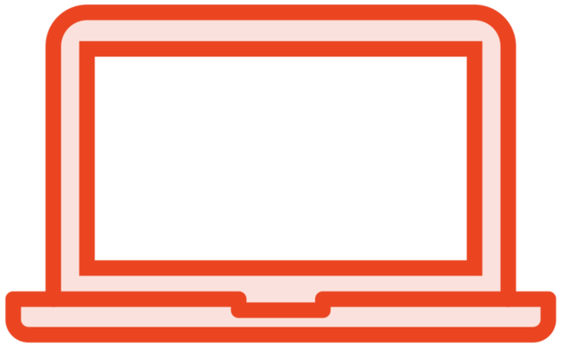


Find/use a zombie

Send a SYN/ACK watch for the IP ID *make a note of it

Step #1 IDLE Scan

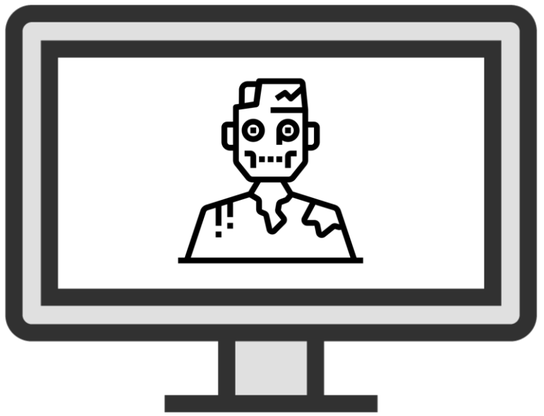
Attacker



SYN/ACK

RST / IPID=2001

Zombie



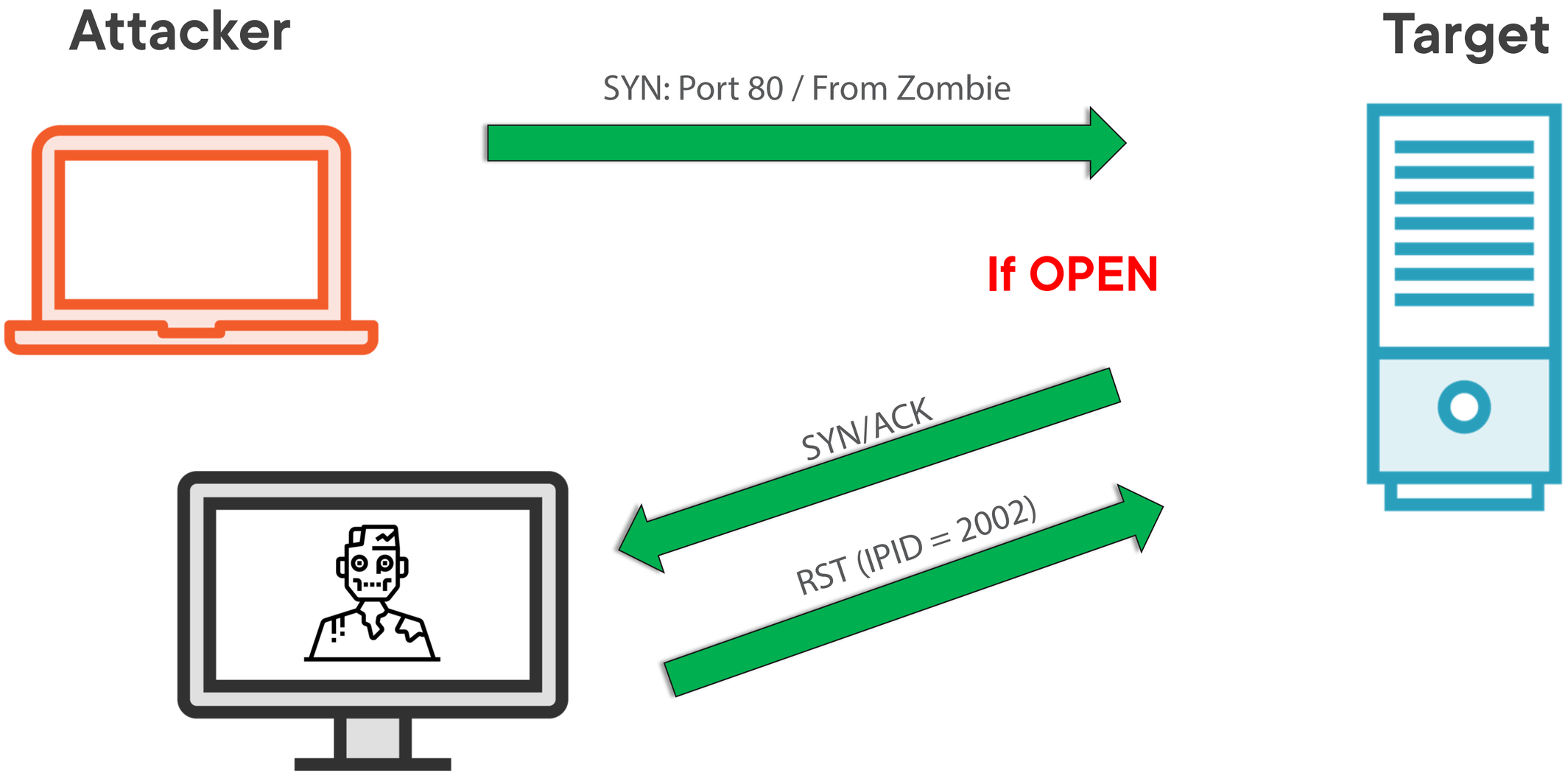
PORT IS OPEN

2nd Step

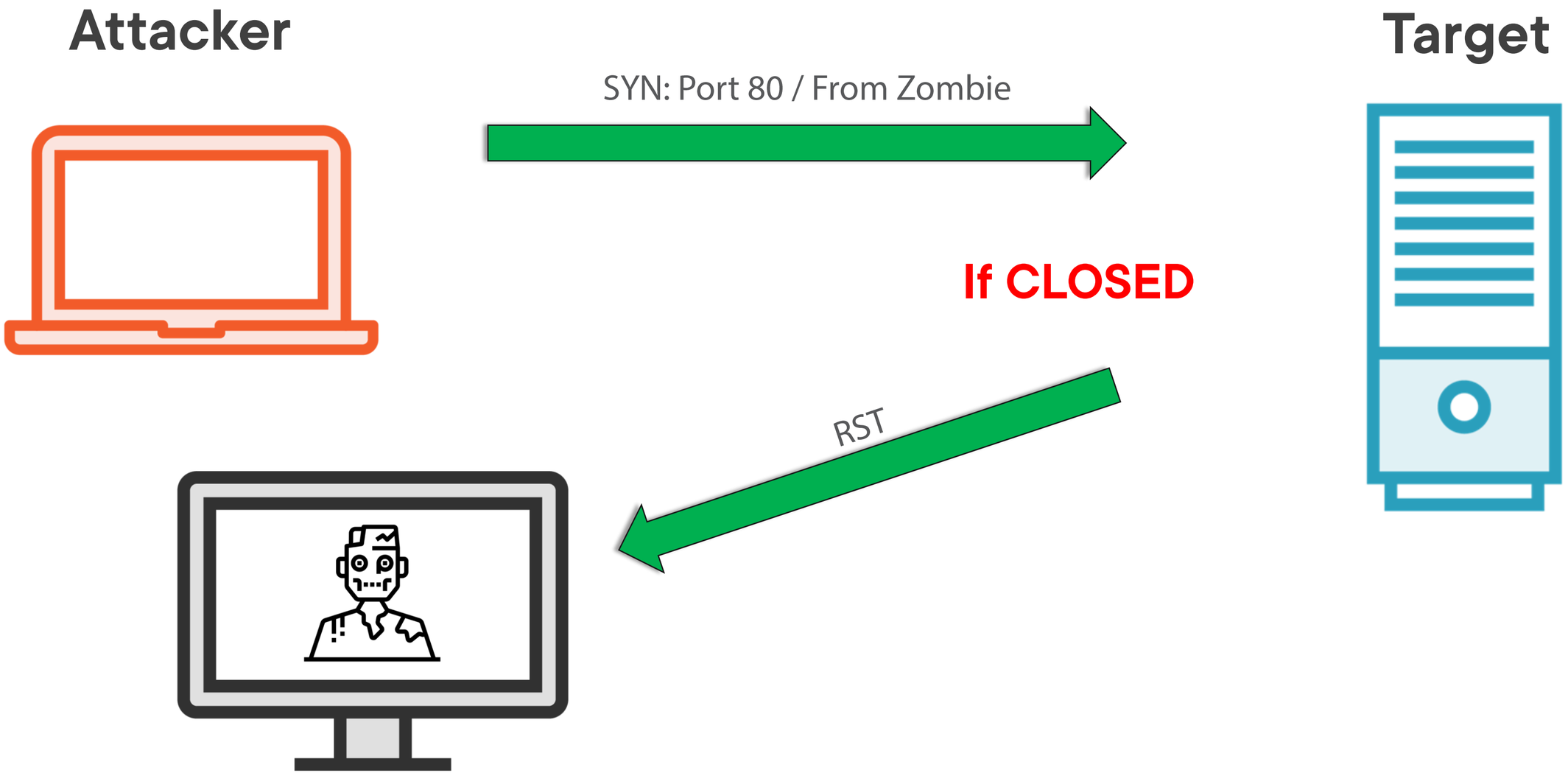
Send a SYN packet to the target

You'll list the "source IP" as the zombie's IP

Step #2 IDLE Scan



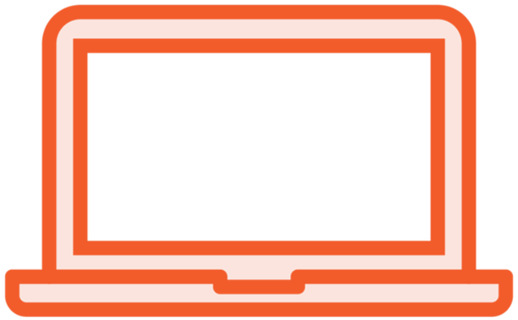
Step #2 IDLE Scan



Step #3 IDLE Scan

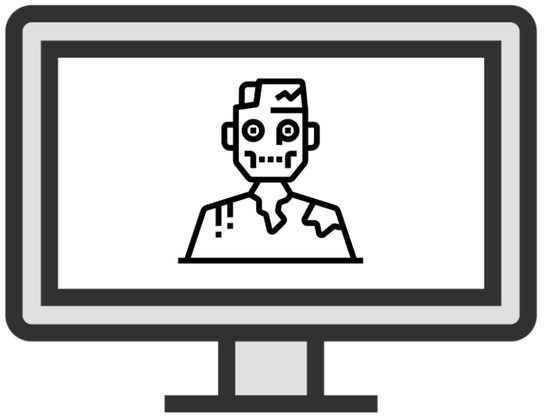
Attacker

Zombie



SYN/ACK

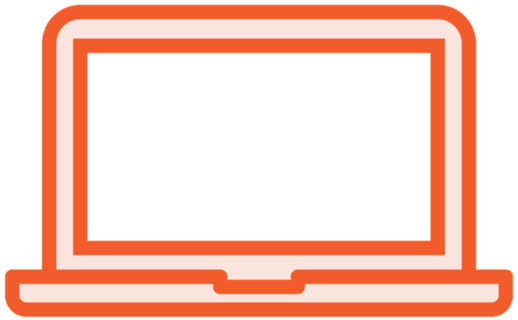
RST / IPID=2002



PORT IS CLOSED

Step #3 IDLE Scan

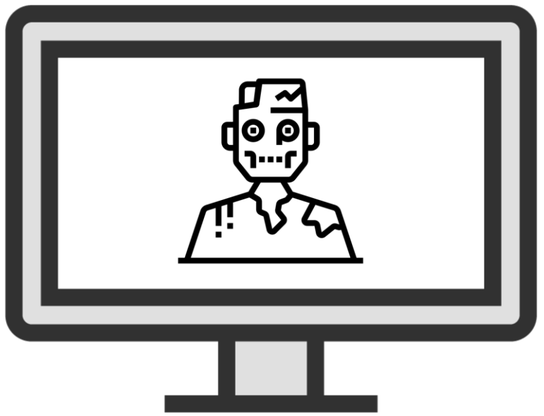
Attacker



SYN/ACK

RST / IPID=2003

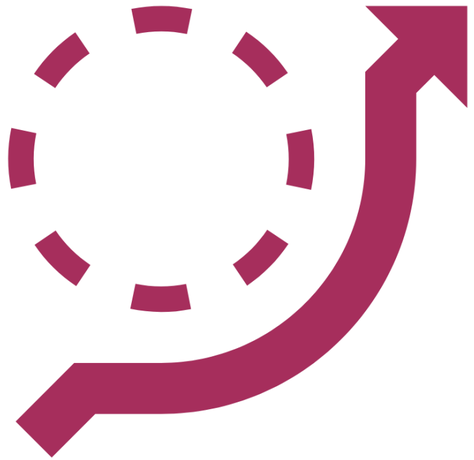
Zombie



PORT IS OPEN

More IDS Evasion Methods

There's Always a Way Around



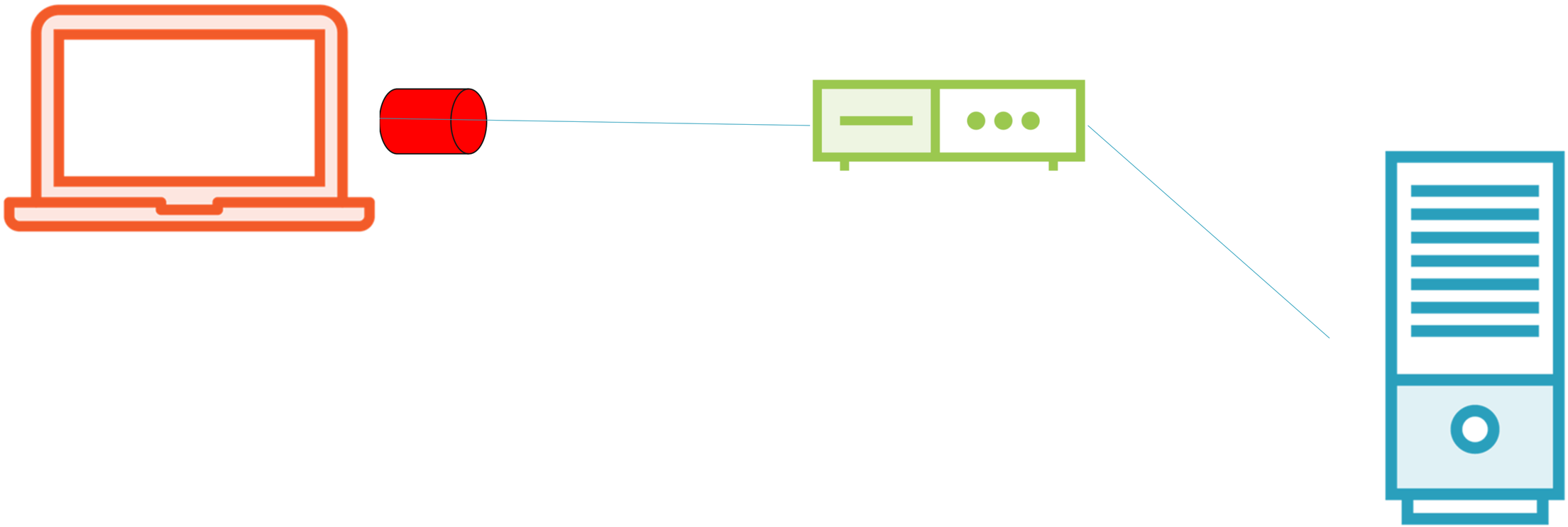
Spoof your IP and sniff the responses

Use a proxy or pwned machine

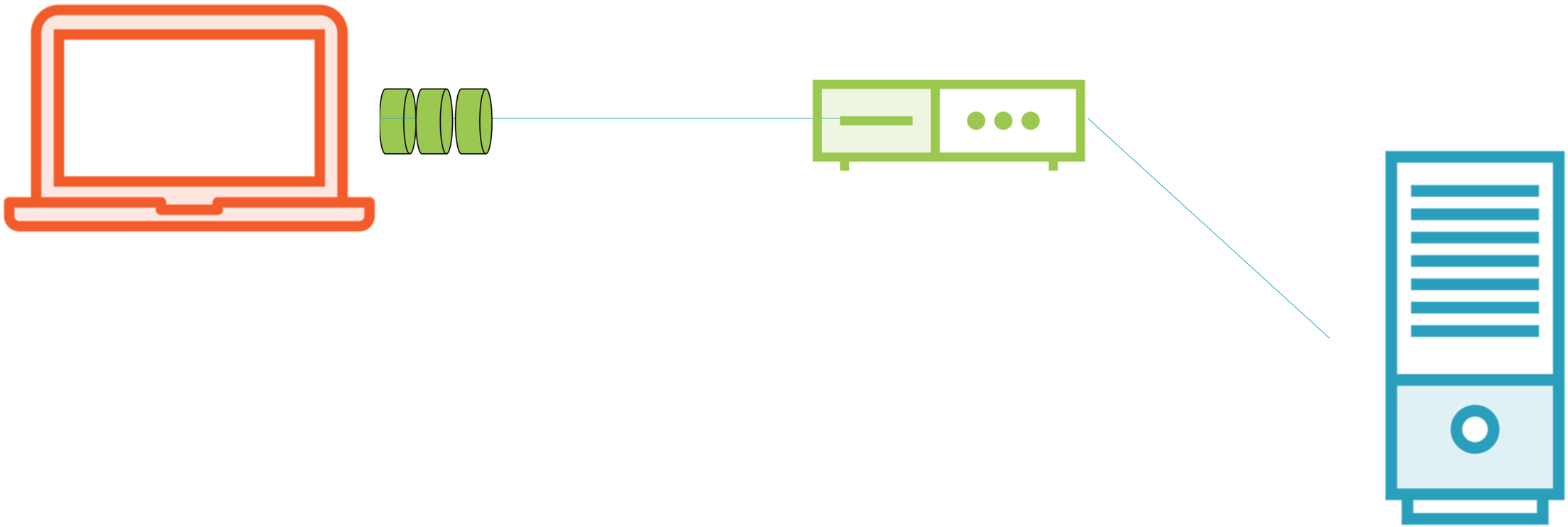
Fragment IP Packets

If you're able, use source routing

IP Fragments



IP Fragments



Demo

Nmap:

- **Idle scan**
- **IP Fragment**

Countermeasures

Countermeasures

Firewalls configured to look for SYN cans	**IDS should detect Nmap/Snort**	**Open only require ports**
Filter ICMP messages	**Test your own network**	**Keep firewalls / IDS updated/patched**

Next Up:
Understanding the 3-way Handshake