# Identifying Network Attacks

# Module Overview

Wireless

On-Path Attacks

ARP poisoning

Layer 2 attacks

DNS attacks

Malicious code / script execution

# Covered Topics

Wireless
- Evil twin
- Rogue access point
- Bluesnarfing
- Bluejacking
- Disassociation
- Jamming
- Radio frequency identifier (RFID)
- Near field communication (NFC)
- Initialization vector (IV)

On-Path Attacks
- Man in the Middle (MiTM)
- Man in the Browser (MiTB)

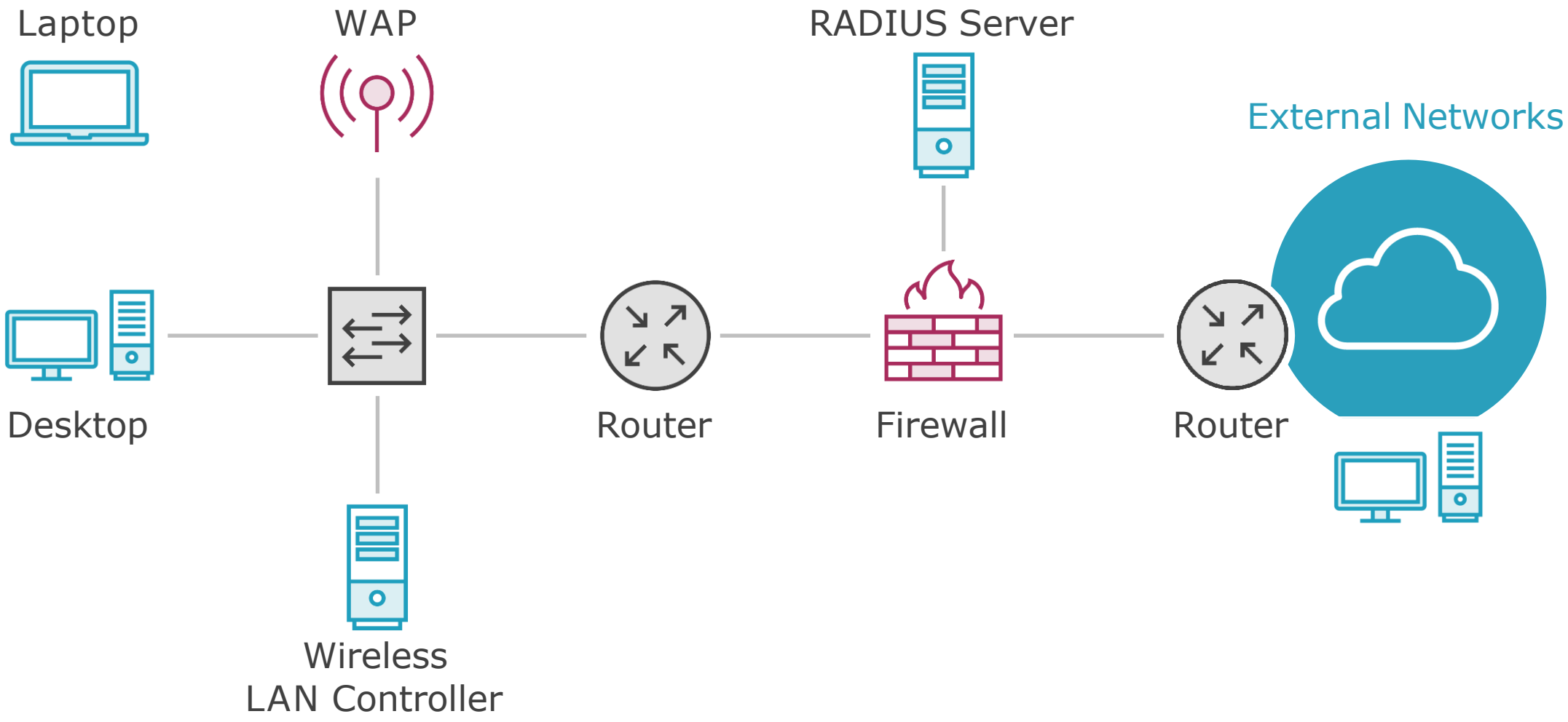
Layer 2 attacks
- Address resolution protocol (ARP) poisoning
- Media access control (MAC) flooding
- MAC cloning

Domain name system (DNS)
- Domain hijacking
- DNS poisoning
- Universal resource locator (URL) redirection
- Domain reputation

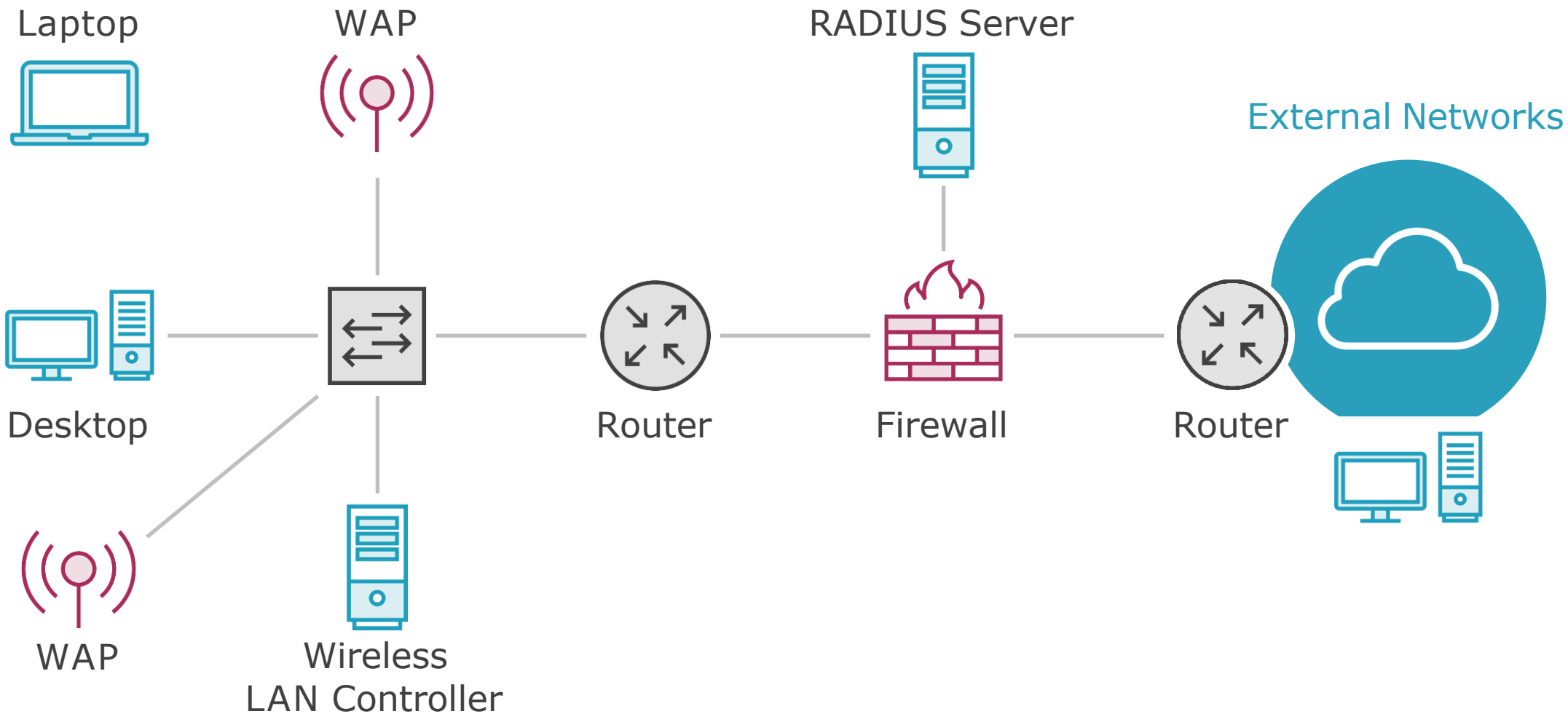
Distributed denial of service (DDoS)
- Network
- Application
- Operational technology (OT)

Malicious code or script execution
- PowerShell
- Python
- Bash
- Macros
- Virtual Basic for Applications (VBA)

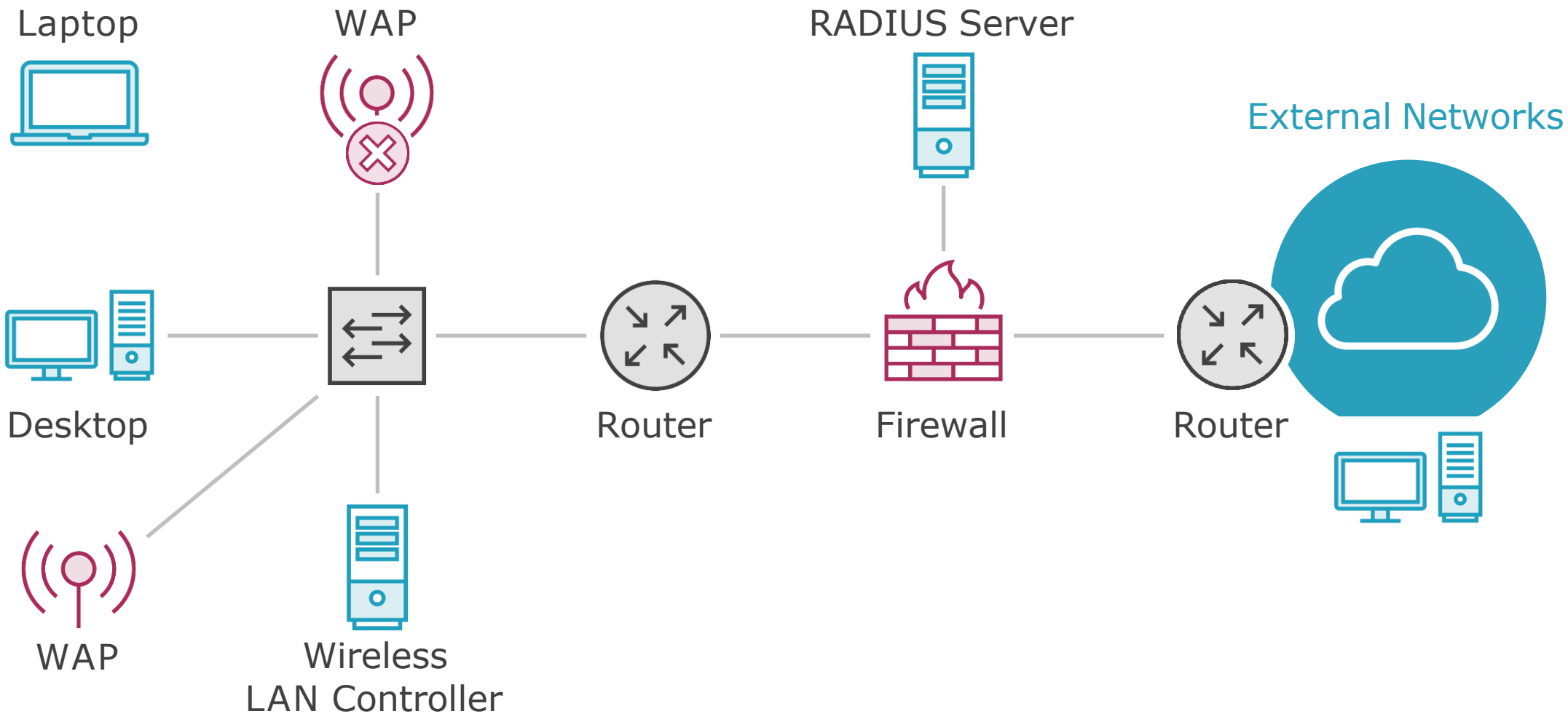
# Rogue Access Points



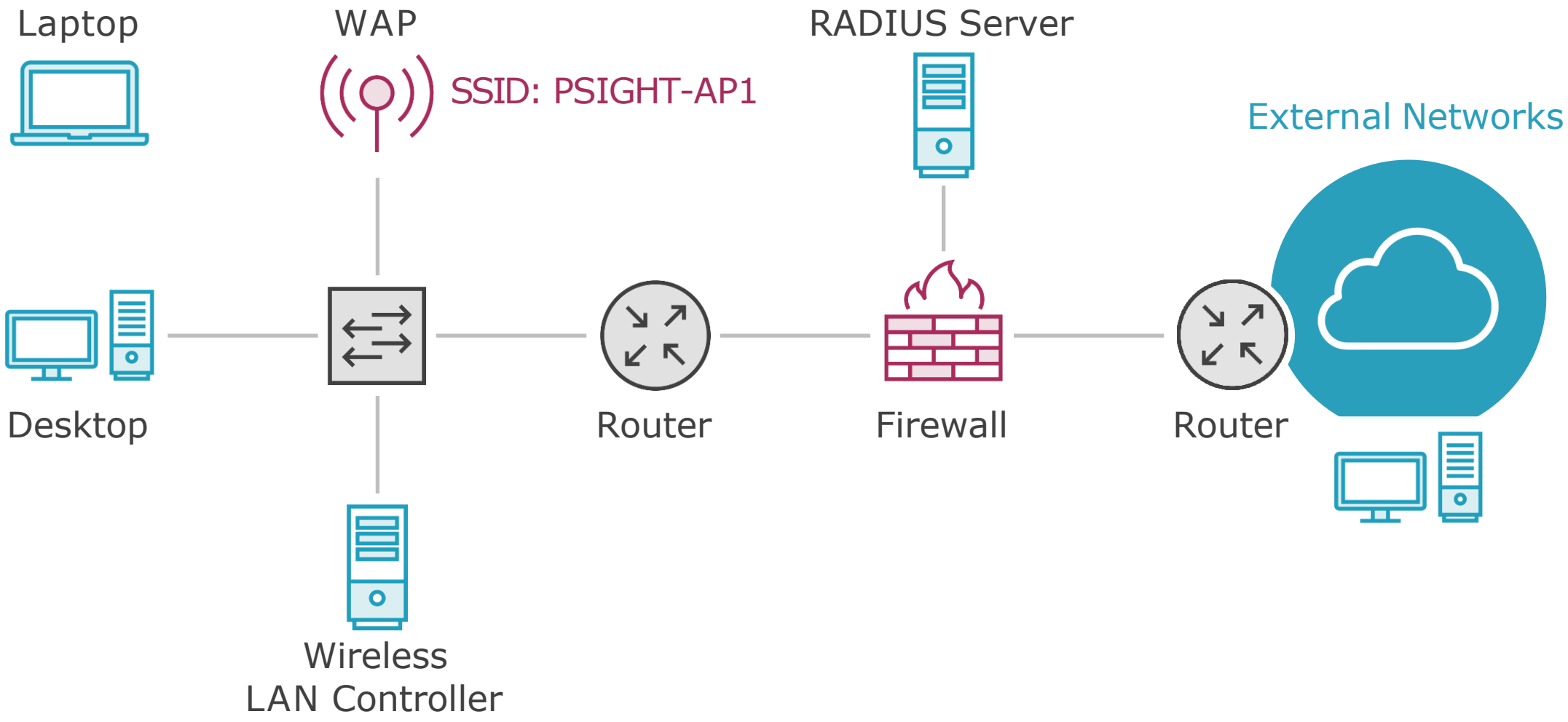
# Rogue Access Points



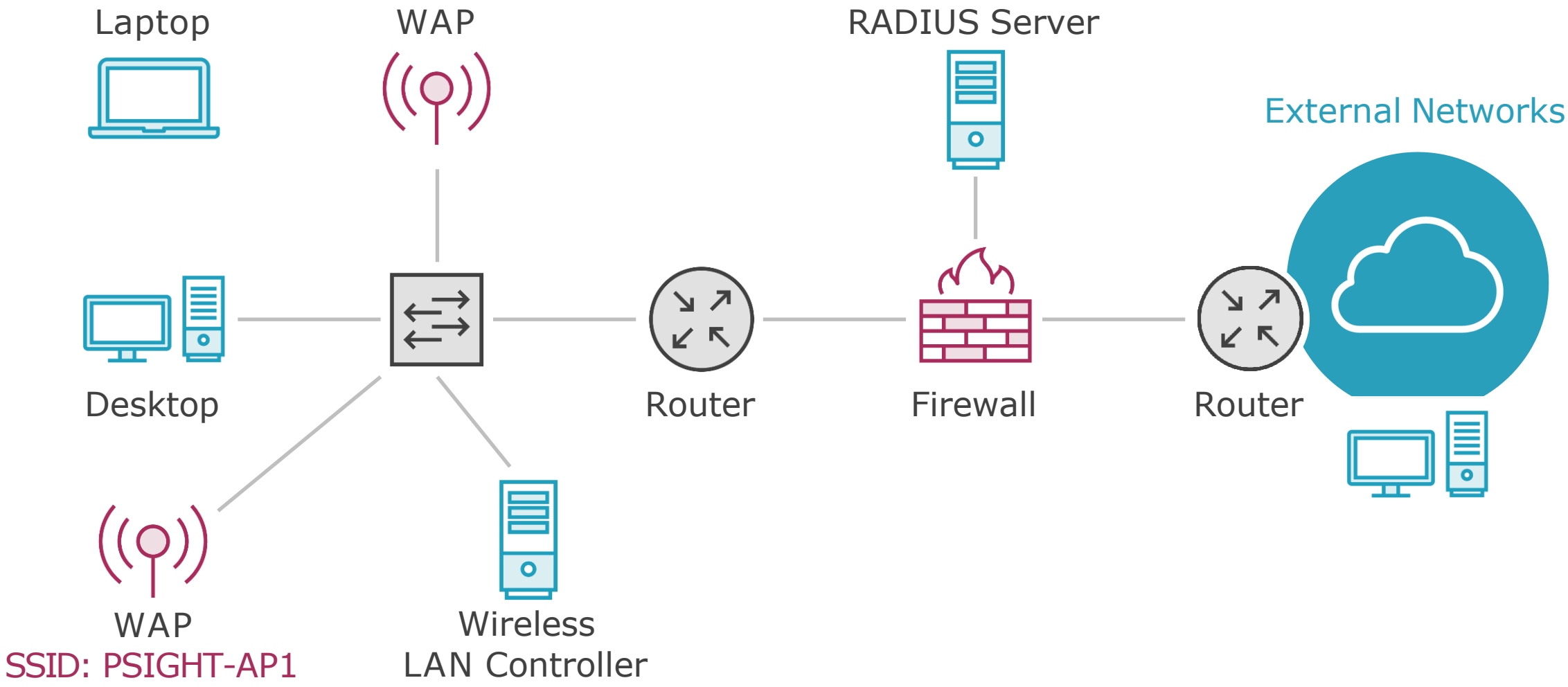
# Rogue Access Points



# Rogue Access Points



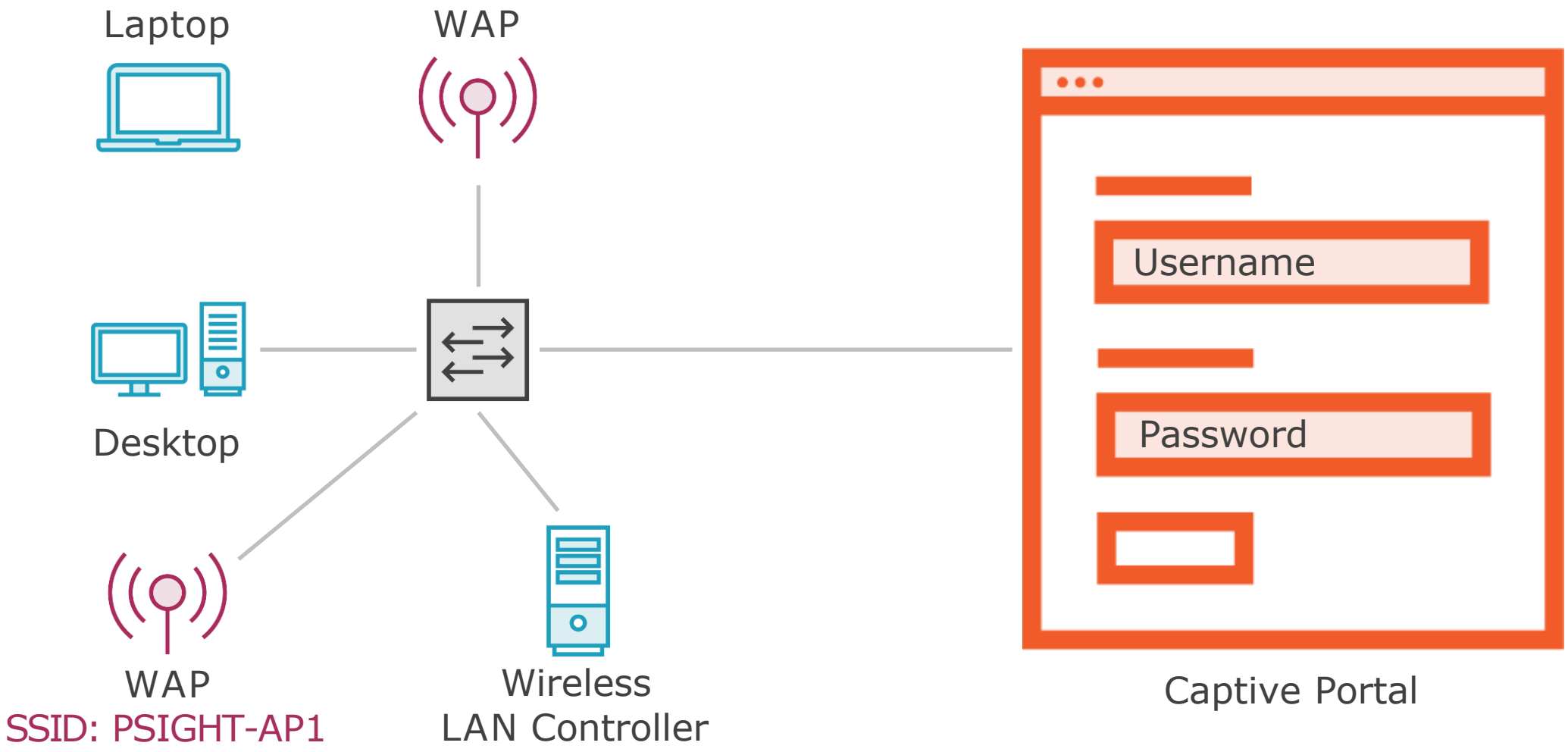
# Rogue Access Points



# Evil Twin

Rogue access point that is impersonating a legitimate access point – using the same SSID

# Rogue Access Points



# Bluejacking

Sending of unauthorized messages or data to a victim’s device via Bluetooth technology

# Bluesnarfing

Bluesnarfing is the opposite of bluejacking, in that data is pulled off the victim device

- Contact lists
- Pictures
- Messages

# Bluejacking

Typically sending a vCard which contains a message in the name field to another Bluetooth-enabled device via the OBEX (OBjectEXchange) protocol

# Dissociation

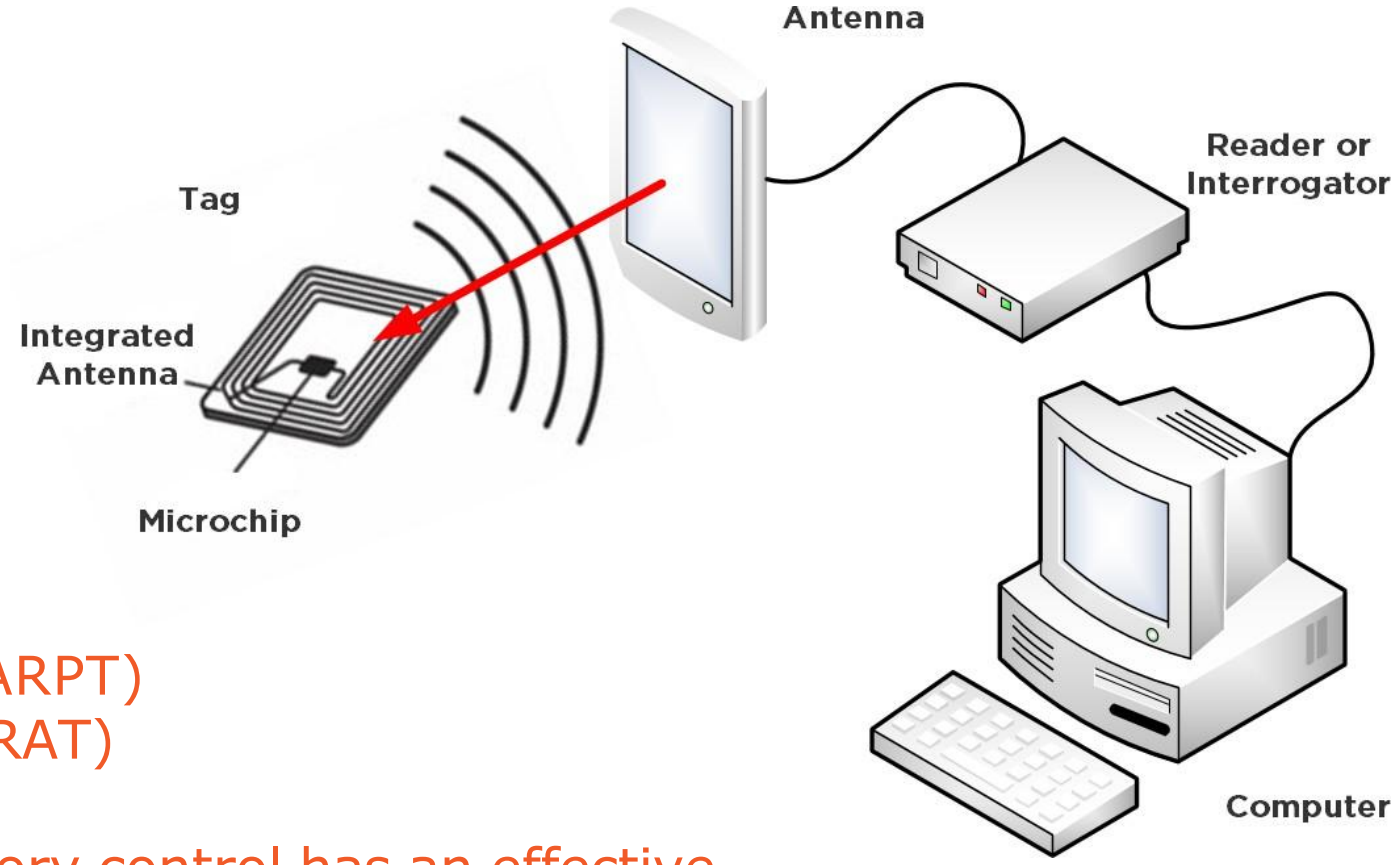
An attacker can create a DoS scenario on a wireless network by sending a spoofed disassociation frame

- Source MAC address is set to that of the Access Point (AP)

## Jamming

- Sending out excessive RF noise basically making Wi-Fi channels unusable
- Typically requires specialized equipment
- Illegal in most places

# Radio Frequency Identification (RFID)




Two types of RFID systems:

- Active Reader/Passive Tag (ARPT)
- Active Reader/Active Tag (ARAT)

Most commercial RFID for inventory control has an effective distance of ~3 ft.

# Near Field Communication (NFC)

Technology to allow communication between devices within close proximity to each other (usually 3-4”)

- Builds upon RFID (one-way) whereas NFC is two-way communication
- Can be used by a malicious attacker to steal data from a nearby device


# Near Field Communication (NFC)

Technology to allow communication between devices within close proximity to each other (usually 3-4”)

- Builds upon RFID (one-way) whereas NFC is two-way communication
- Can be used by a malicious attacker to steal data from a nearby device



# IV Attack

Initialization Vector Attack

- Weaker encryption had short IVs that would repeat fairly quickly
- Attacker could flood the network, sniff the packets and see the IVs being sent
  - As they eventually repeat, the attacker could derive the IV and then gain access

WEP uses a 24-bit IV

- Easily cracked
- Since been deprecated

# IV Attack

| Standard | Method | Security | Notes |
|---|---|---|---|
| WEP | RC4 Stream | 24-bit encryption | IV attack/Packet injection can crack WEP in several seconds |
| WPA | TKIP | 128-bit encryption | TKIP has been cracked as well |
| WPA2 | AES-CCMP | 128-bit encryption | 48-bit IV makes it much more secure |

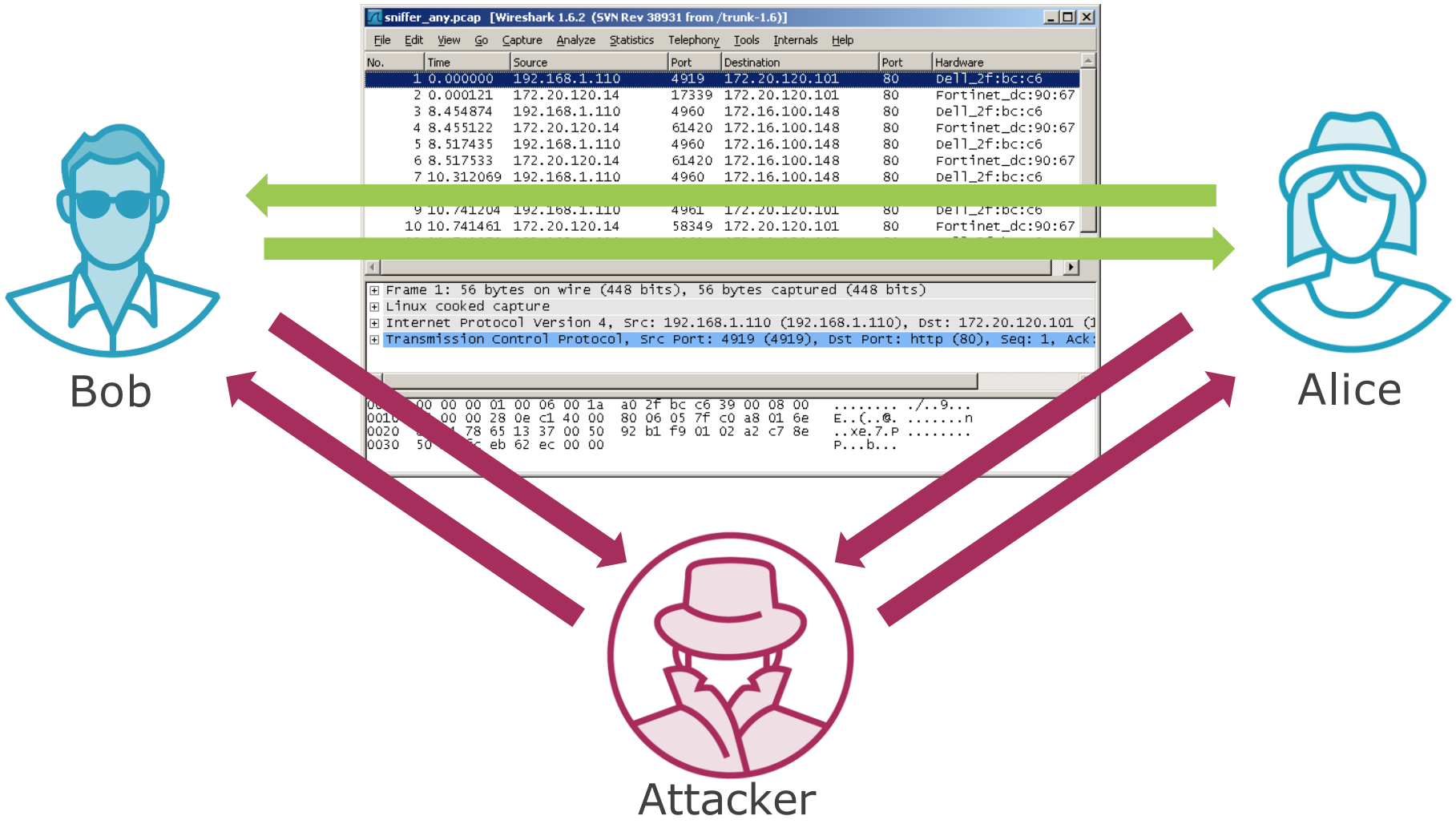
WEP Weakness

- Initialization Vector (IV) is only 24 bits long
- Sent in clear text
- IV is static and is reused
- IV is part of the RC4 encryption key

WEP should be avoided unless backward compatibility with older devices is needed

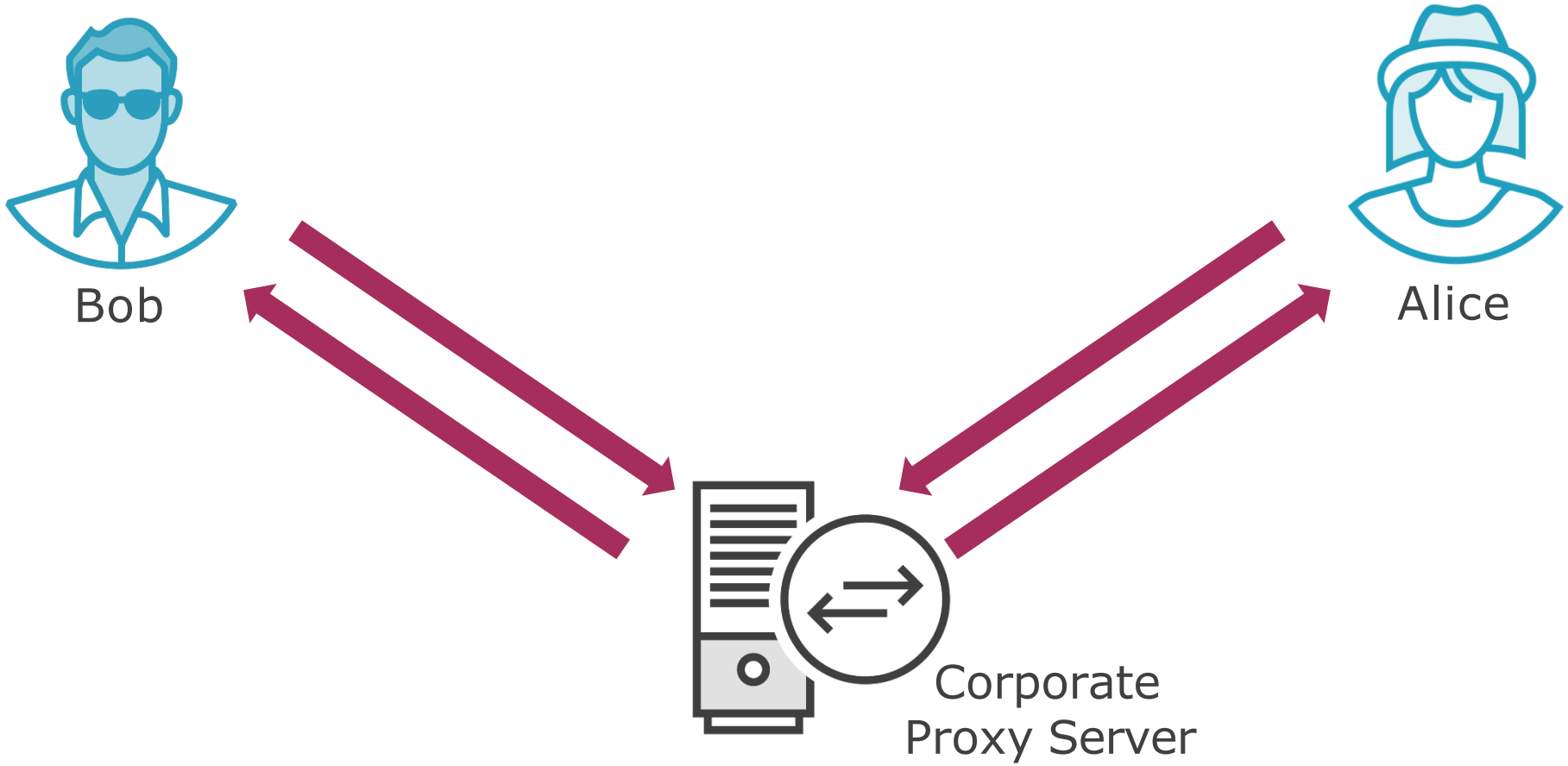
# On-Path Attack

## Previously known as “Man-in-the-Middle” attack (MiTM)



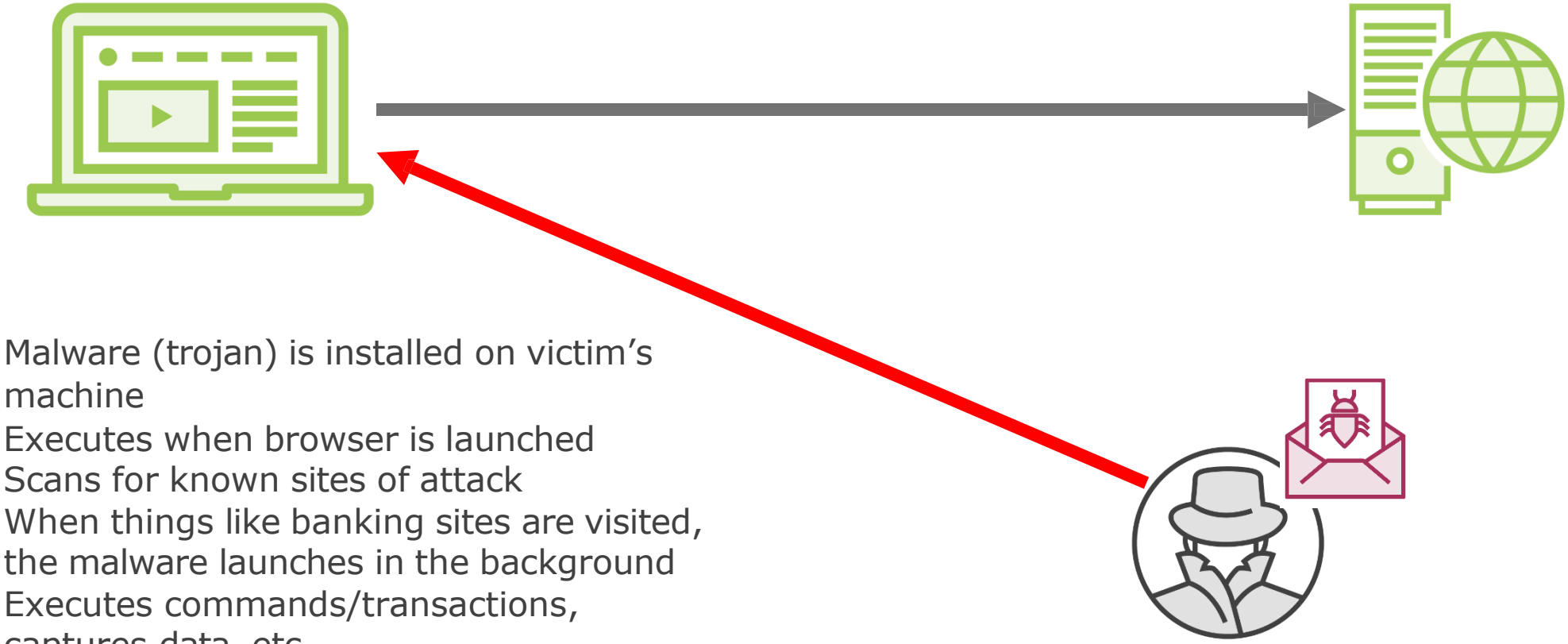
# On-Path Attack

Previously known as “Man-in-the-Middle” attack (MiTM)



# On-Path Attack

Previously known as “Man-in-the-Browser” attack (MiTB)



- Malware (trojan) is installed on victim’s machine
- Executes when browser is launched
- Scans for known sites of attack
- When things like banking sites are visited, the malware launches in the background
- Executes commands/transactions, captures data, etc.
- Returns expected results to victim, avoiding easy detection

# ARP Poisoning

Also known as ARP Cache Poisoning

- Attacker sends out spoofed ARP messages onto a LAN to associate their machine with another host IP (i.e. default gateway)
- Allows the attacker to intercept data intended for another recipient
- Can be used for DoS, MiTM or session hijacking

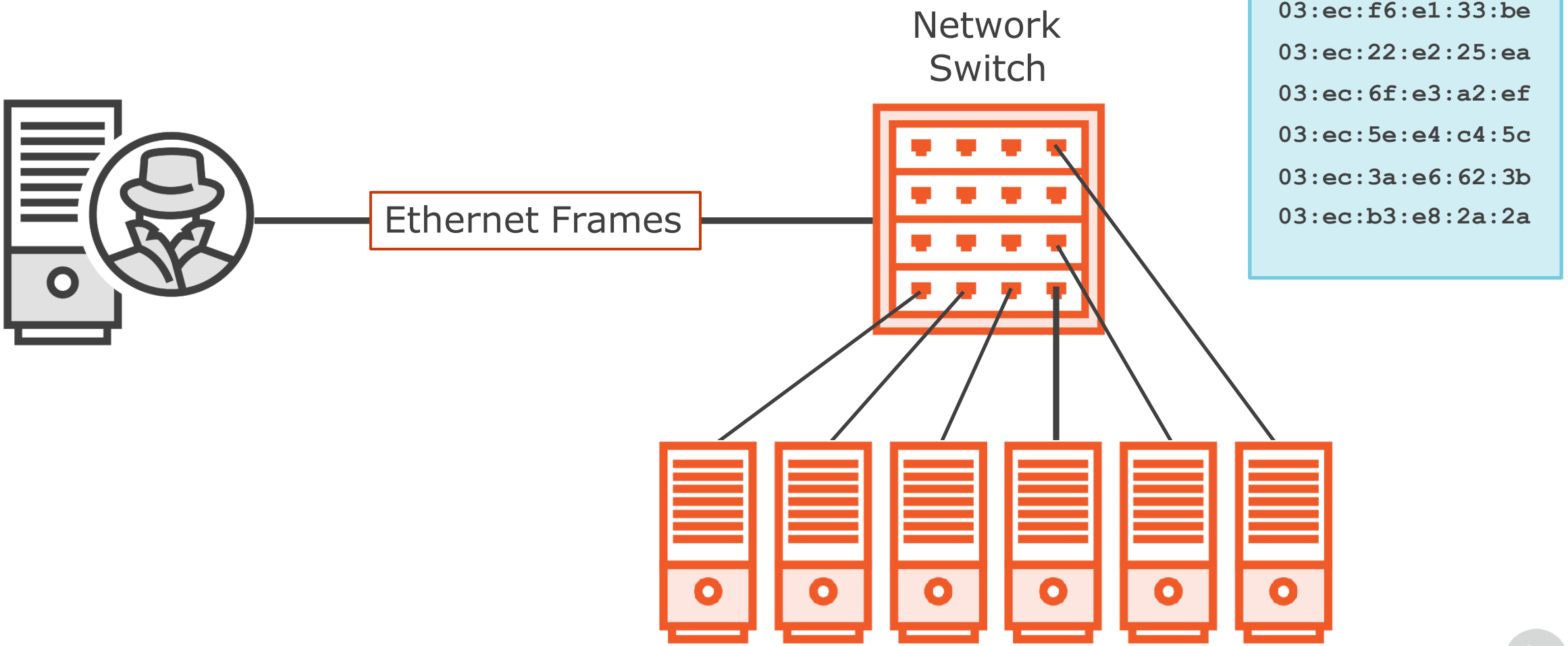
# IP/MAC Spoofing

Masquerading as another using their IP or MAC address

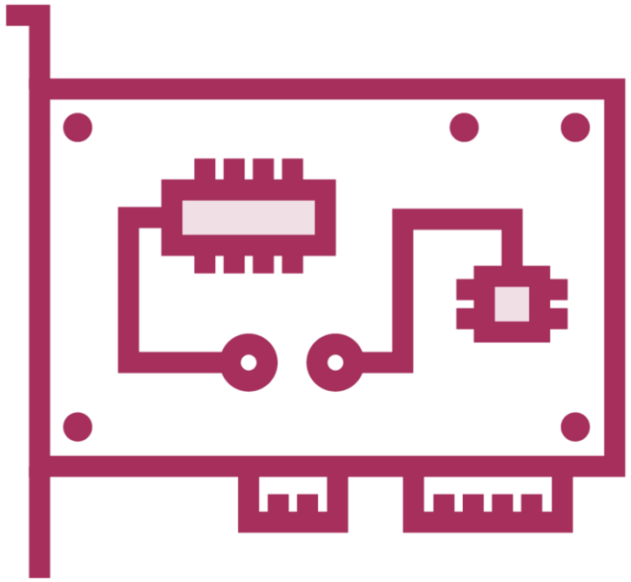
- IP Address spoofing
- Address Resolution Protocol (ARP) spoofing
  - ARP resolves an IP address to a MAC address

Can be used with MiTM middle attacks

# MAC Flooding



# MAC Cloning



- Also known as MAC spoofing
  - Change the MAC address of a network interface card
    - Burned in at the factory
    - 48-bit HEX address with first three octets identifying the manufacturer
    - 7C:67:A2:45:EB:2D (Intel NIC)
- MAC randomization is a feature to avoid tracking
  - iOS, Android, Windows and Linux

# DNS Poisoning


Also known as "DNS Cache Poisoning"

- Manipulating the data in a DNS server's cache to point to different IP addresses
- Attacker could redirect a site's traffic from the legitimate site to one they own

# Typo Squatting/URL Hijacking

Setting up domain names to capitalize on the fact that users make typos

- Facbook.com instead of Facebook.com
- Goggle, Googel, Googgle, etc

Fraudulent websites are set up to resemble the real ones

- Capture user credentials

Ad portals full of ads that might appeal to a user going to that website

- Hoping to create ad revenue by supplying complementary advertising

# DDoS

Large scale attack against a target

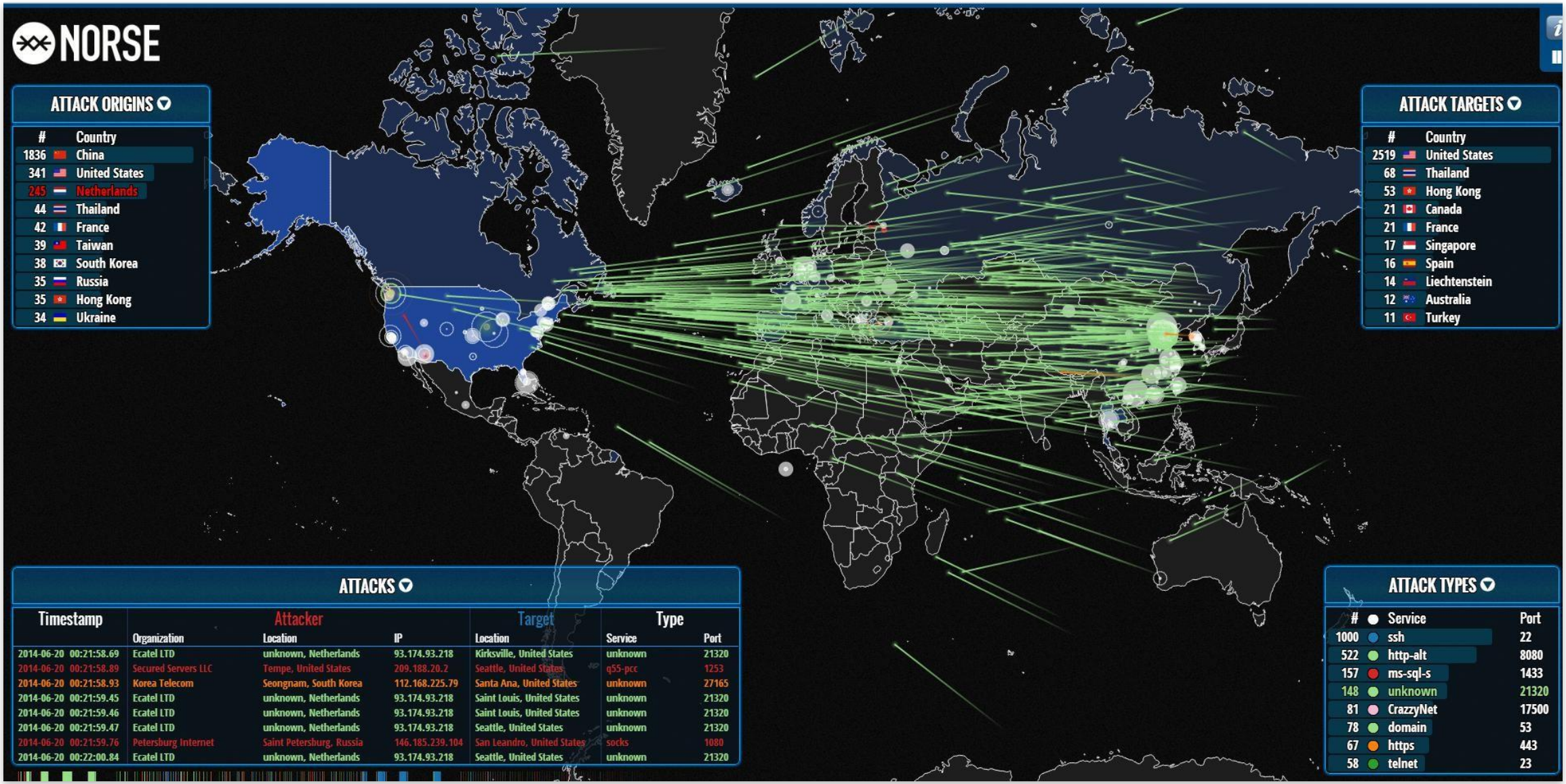
- Botnets
- Bot herders
- Command and Control (C&C) Center

C&C issues command(s) to botnet zombies to initiate attack against a target

- Could be hundreds, thousands or millions of zombies comprising a botnet army

DoS (Denial of Service)

- Similar type of attack but on much smaller scale




Distributed Denial of Service (DDoS) Attack From Points in China against the United States

# Smurf Attack (Amplification)

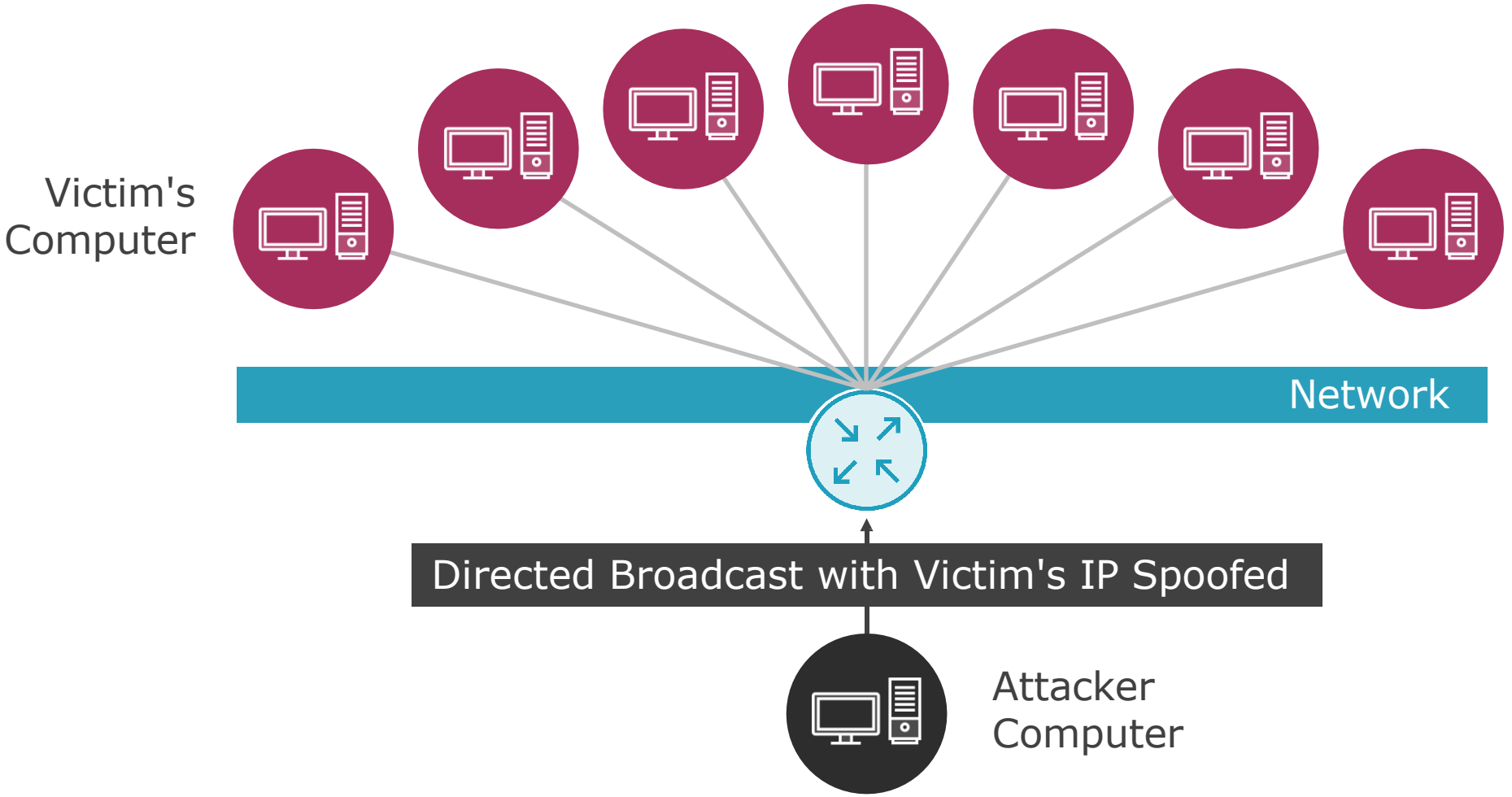
DDoS type of attack

- Victim's IP address is spoofed and ICMP messages are broadcast to a computer network
- Recipients will respond with reply to victim's IP address, flooding it with responses
- Goal being it will slow the target/victim PC to point of being unusable

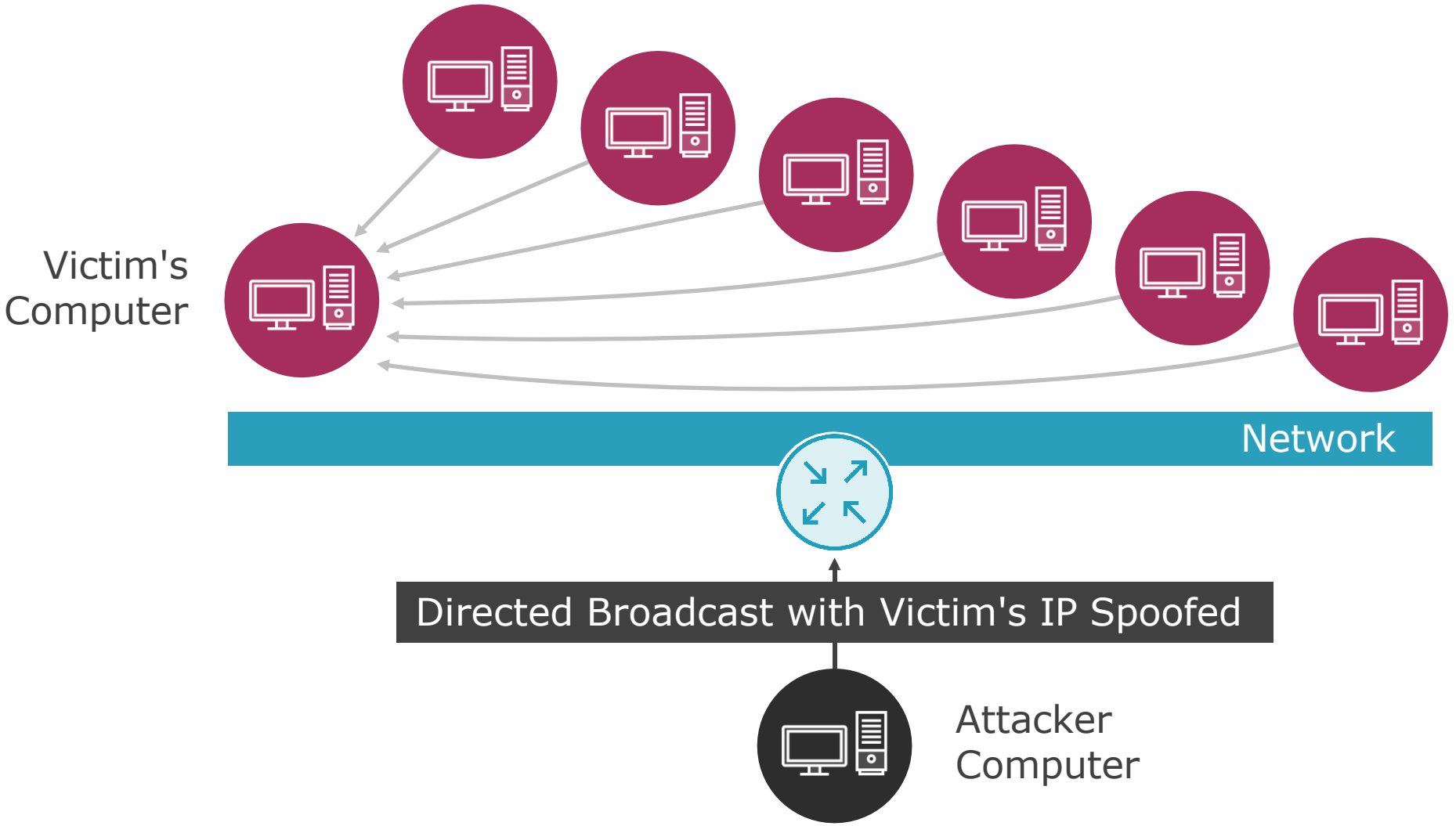
Mitigation

- Can be mitigated by network administrators setting policy to disallow computers from responding to ICMP requests or broadcasts
- Configure routers to not forward broadcasts (default on most routers)

# Smurf Attack



# Smurf Attack



# Distributed Denial of Service (DDoS)

DDoS type of attack

- Goal being to slow down the target server or network to point of being unusable

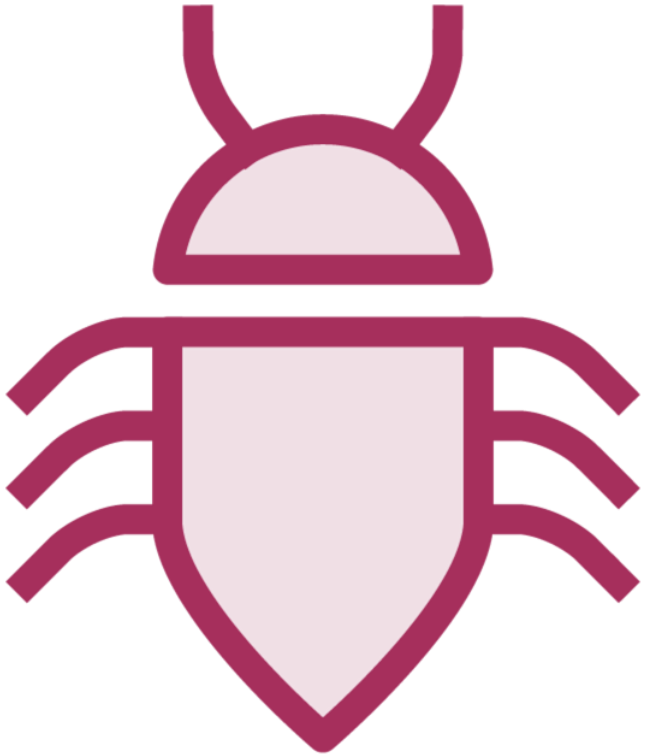
Attack vectors

- Network
  - DNS amplification (SMURF attack)
- Application
  - HTTP GET / POST attacks

Operational Technology (OT)

- Web Application Firewalls (WAF)
- IP reputation databases
- Challenge to requestor (i.e. CAPTCHA)

# Malicious Code Execution



Powershell

Python

Bash

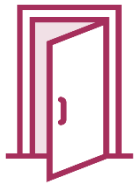
Macros

Virtual Basic for Applications

# Malicious Code Execution

Malware sent via email or malicious links
Malicious code can be installed and run to execute MiTM, MiTB and other data manipulation / exfiltration attacks

Infected USB sticks and other removable media
Scripts can be executed automatically upon access to install malicious code (malware, ransomware, backdoors)



Remote Access Trojans (RAT) / Backdoors
RAT programs can allow complete control over a target system including access to browser sessions, data, webcams, etc.

# Module Review

Wireless

On-Path Attacks (MiTM, MiTB)

ARP poisoning

Layer 2 attacks

DNS attacks

Malicious code / script execution