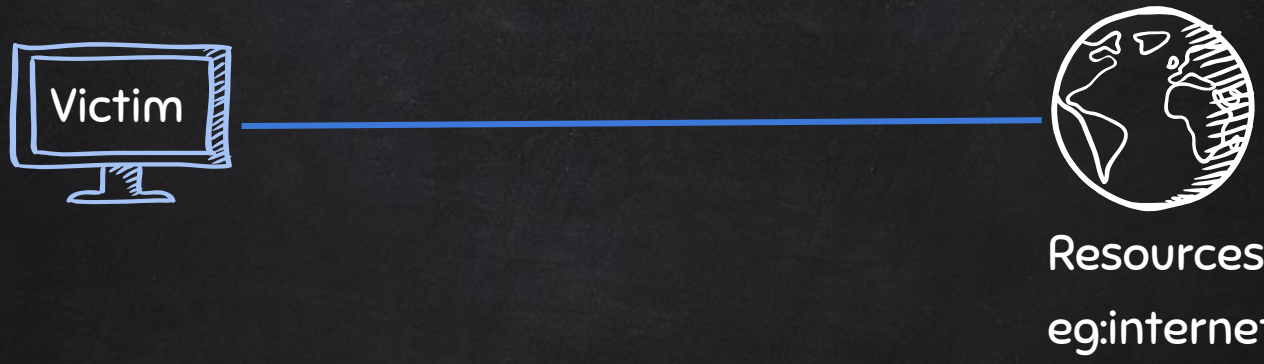
Network Mapping

Nmap / Zenmap

- HUGE security scanner.
- From an IP/IP range it can discover:
  - Open ports.
  - Running services.
  - Operating system.
  - Connected clients.
  - + more

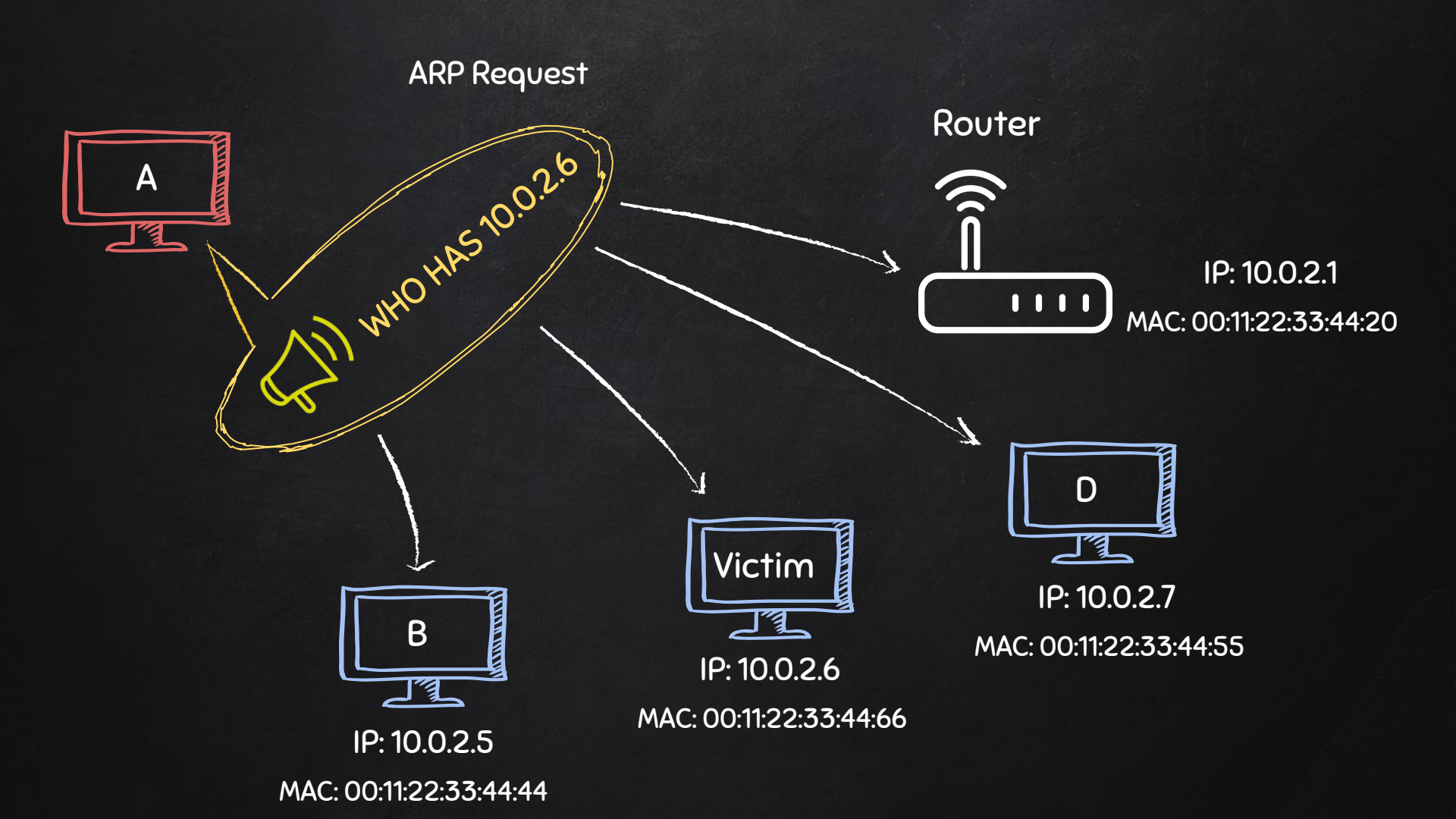
MITM Attacks

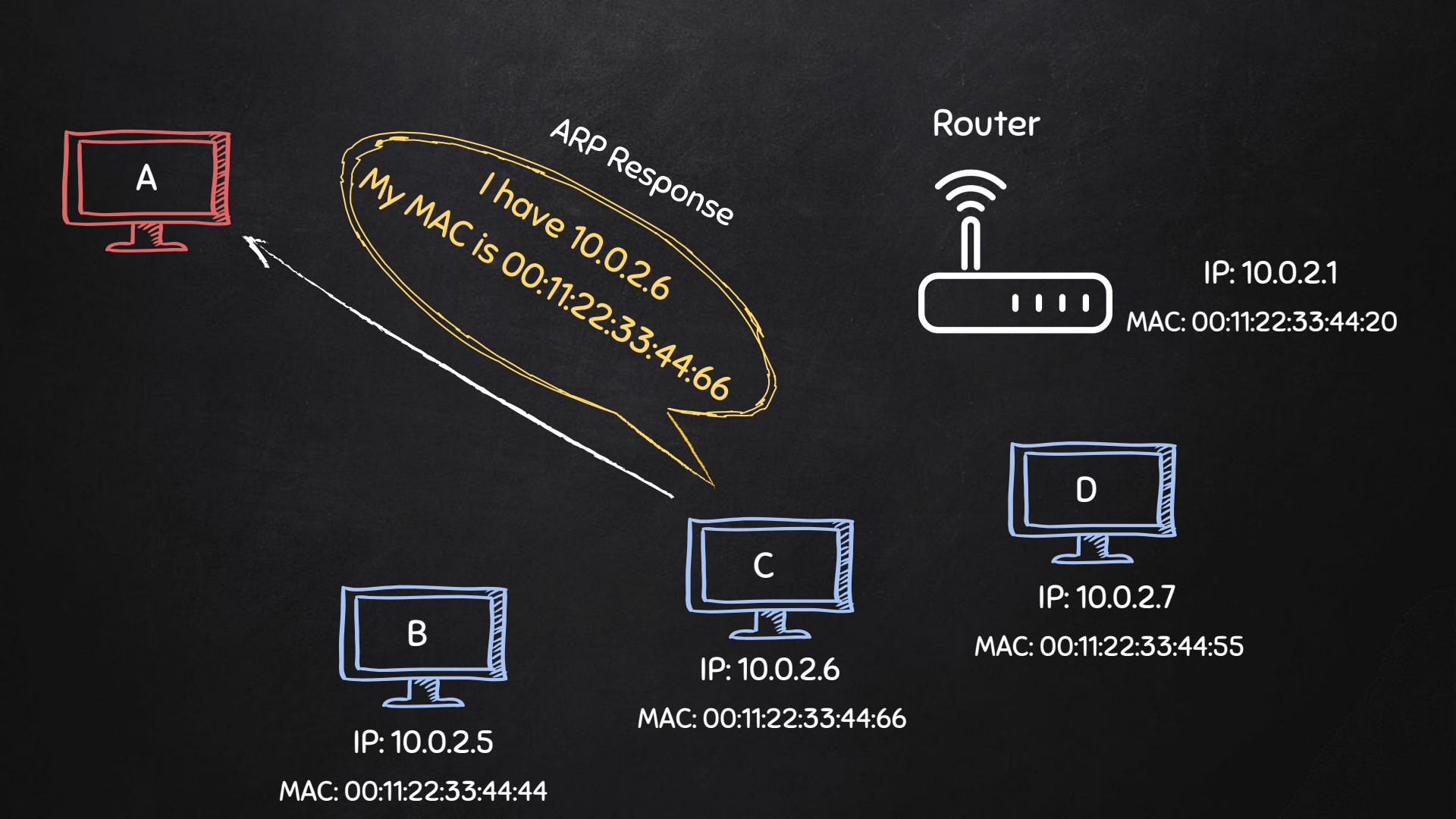


Address Resolution Protocol

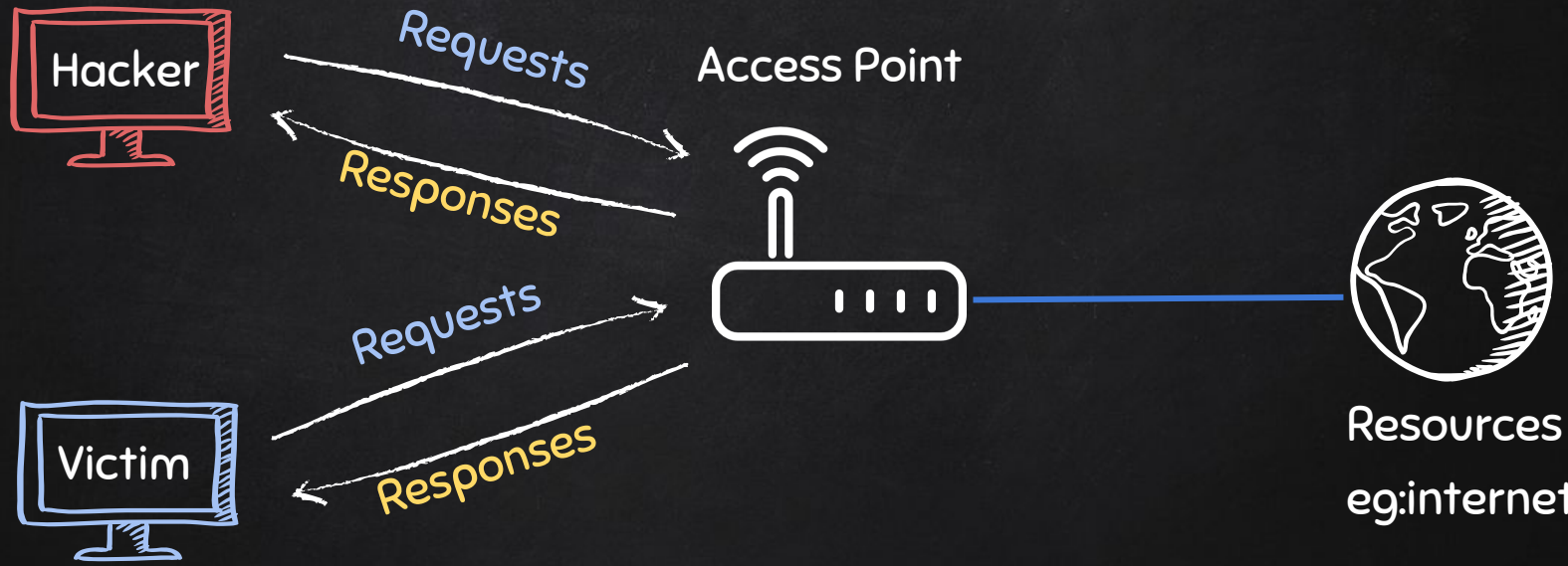
(ARP)

→ Simple protocol used to map IP Address of a machine to its MAC address.


ARP Request
A
WHO HAS 10.0.2.6
Router
IP: 10.0.2.1
MAC: 00:11:22:33:44:20
B
IP: 10.0.2.5
MAC: 00:11:22:33:44:44
Victim
IP: 10.0.2.6
MAC: 00:11:22:33:44:66
D
IP: 10.0.2.7
MAC: 00:11:22:33:44:55

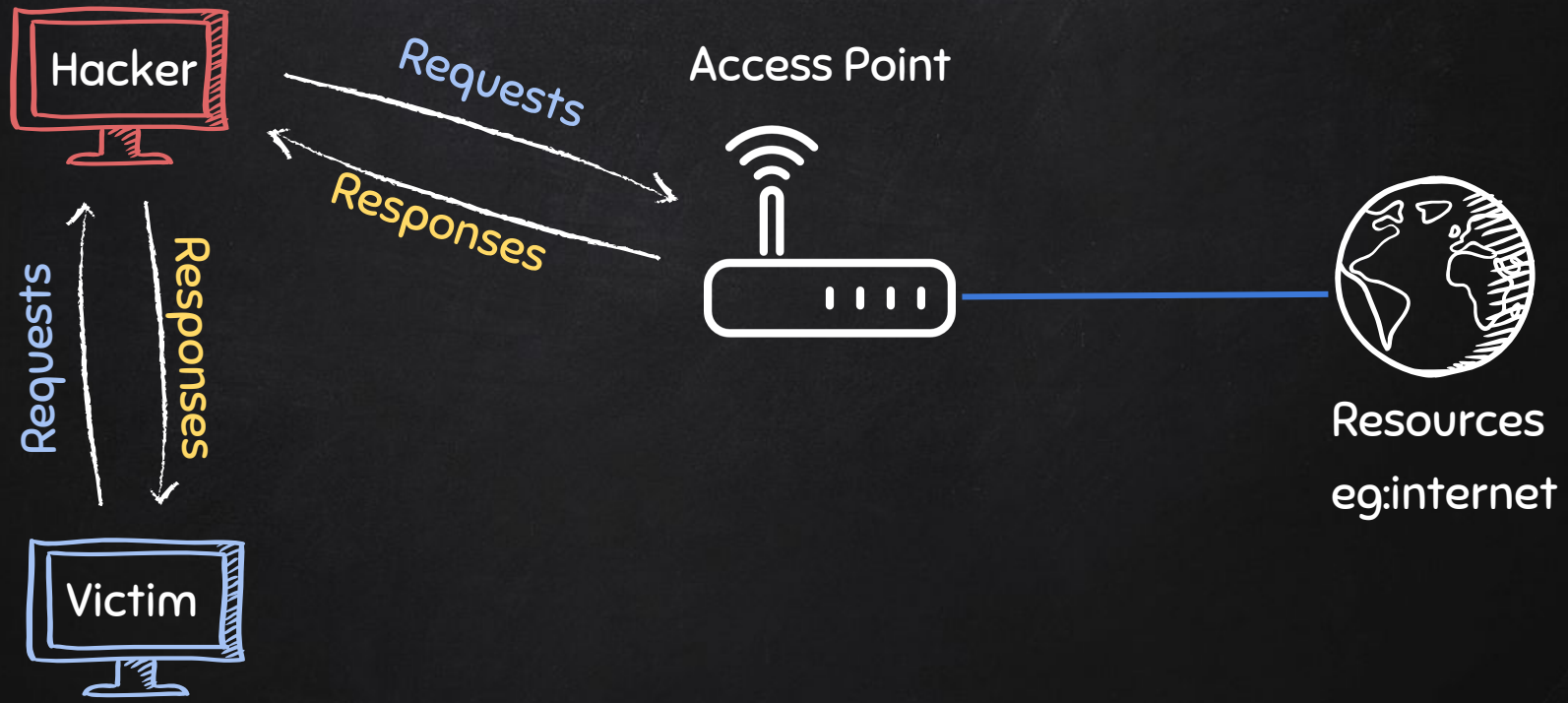

A
ARP Response
I have 10.0.2.6
My MAC is 00:11:22:33:44:66
Router
IP: 10.0.2.1
MAC: 00:11:22:33:44:20
D
IP: 10.0.2.7
MAC: 00:11:22:33:44:55
C
IP: 10.0.2.6
MAC: 00:11:22:33:44:66
B
IP: 10.0.2.5
MAC: 00:11:22:33:44:44

Typical Network

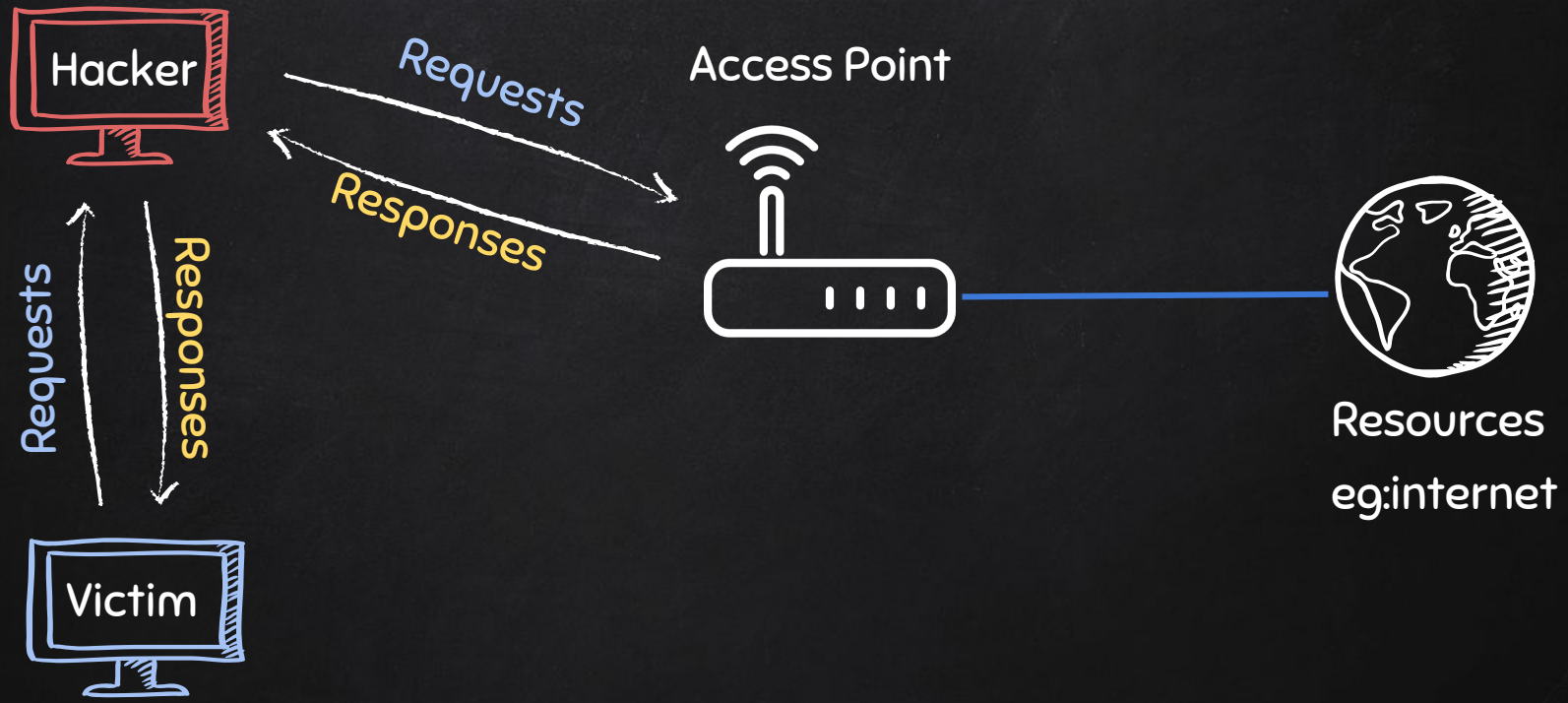


ARP Spoofing

ARP Spoofing



ARP Spoofing



ARP Spoofing

Using arpspoof

- arpspoof tool to run arp spoofing attacks.
- Simple and reliable.
- Ported to most operating systems including Android and iOS.
- Usage is always the same.

use:

```
arpspoof -i [interface] -t [clientIP] [gatewayIP]
arpspoof -i [interface] -t [gatewayIP] [clientIP]
```

ARP Spoofing
Using Bettercap

- Framework to run network attacks.
- Can be used to :
  - ARP Spoof targets (redirect the flow of packets)
  - Sniff data (urls, username passwords).
  - Bypass HTTPS.
  - Redirect domain requests (DNS Spoofing).
  - Inject code in loaded pages.
  - And more!

use:

```
bettercap -iface [interface]
```

HTTPS

Problem:

- Data in HTTP is sent as plain text.
- A MITM can read and edit requests and responses.

→ not secure

Solution:

- Use HTTPS.
- HTTPS is an adaptation of HTTP.
- Encrypt HTTP using TLS (Transport Layer Security) or SSL (Secure Sockets Layer).

Bypassing HTTPS

Problem:

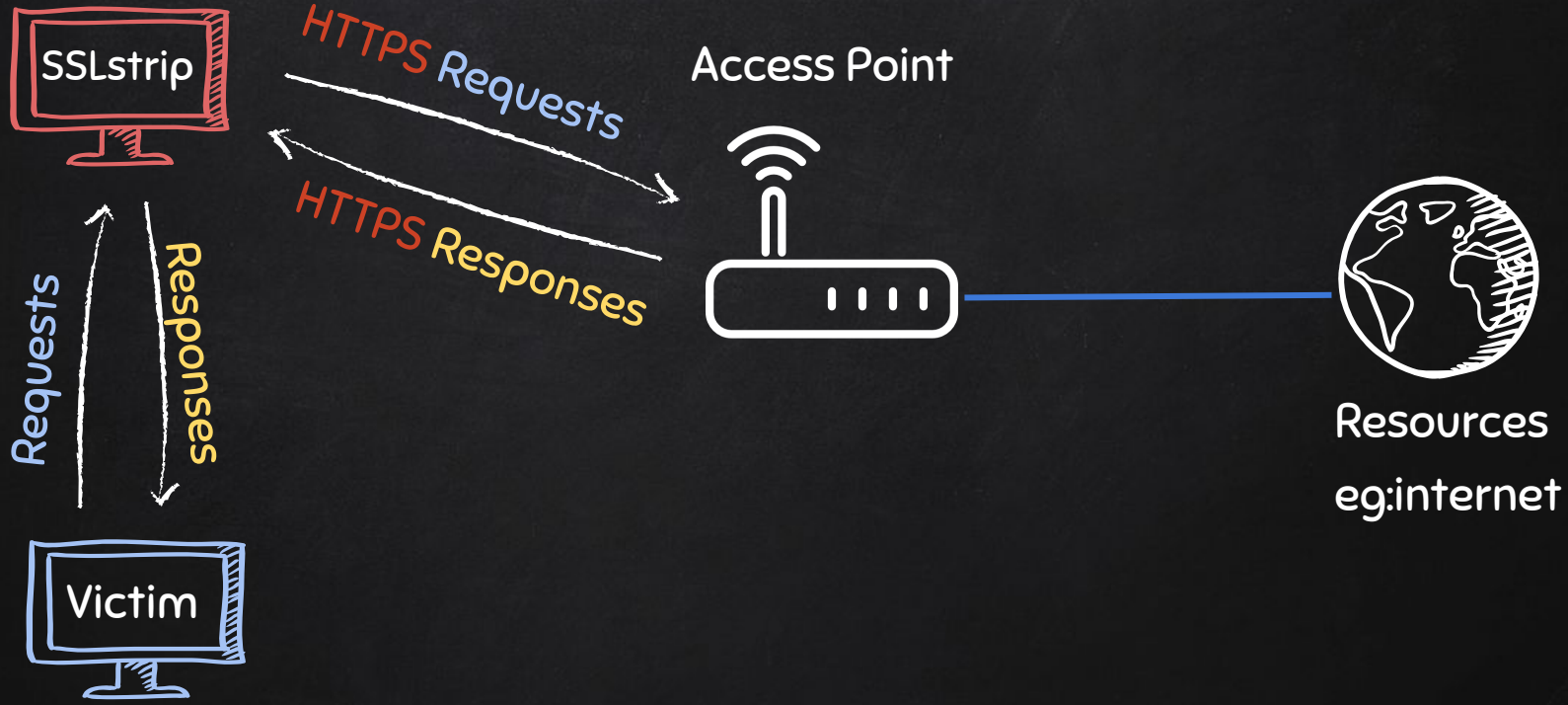
- Most websites use HTTPS

→ Sniffed data will be encrypted.

Solution:

- Downgrade HTTPS to HTTP.

SSL Stripping



HSTS

- HTTP **Strict** Transport Security.
- Used by Facebook, Twitter and few other famous websites.

Problem:

→ Modern browsers are **hard-coded** to only load a list of HSTS websites over https.

Solution:

- Trick the browser into loading a different website.

Bypassing HSTS

Problem:

→ Modern browsers are **hard-coded** to only load a list of HSTS websites over https.

Solution:

- Trick the browser into loading a different website.

→ Replace all links for HSTS websites with similar links

Ex:

facebook.com → facebook.corn

Twitter.com → twiter.com

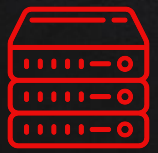
DNS Spoofing

- DNS → Domain Name System.
- Translates domain names to IP addresses.
- Eg: links www.google.com to the IP of Google's server.

bing.com	A	204.79.197.200
facebook.com	A	195.44.2.1
zsecurity.org	A	104.27.153.174
……..etc		

FACEBOOK.COM WEB SERVER
195.44.2.1

LIVE.COM WEB SERVER
204.79.197.200



HACKER WEB SERVER
10.0.2.16

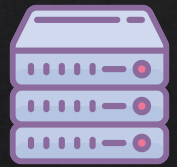
DNS SERVER

live.com

FACEBOOK.COM WEB SERVER
195.44.2.1

LIVE.COM WEB SERVER
204.79.197.200

HACKER WEB SERVER
10.0.2.16



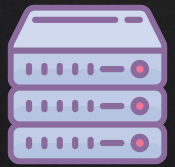
DNS SERVER

FACEBOOK.COM WEB SERVER
195.44.2.1

LIVE.COM WEB SERVER
204.79.197.200

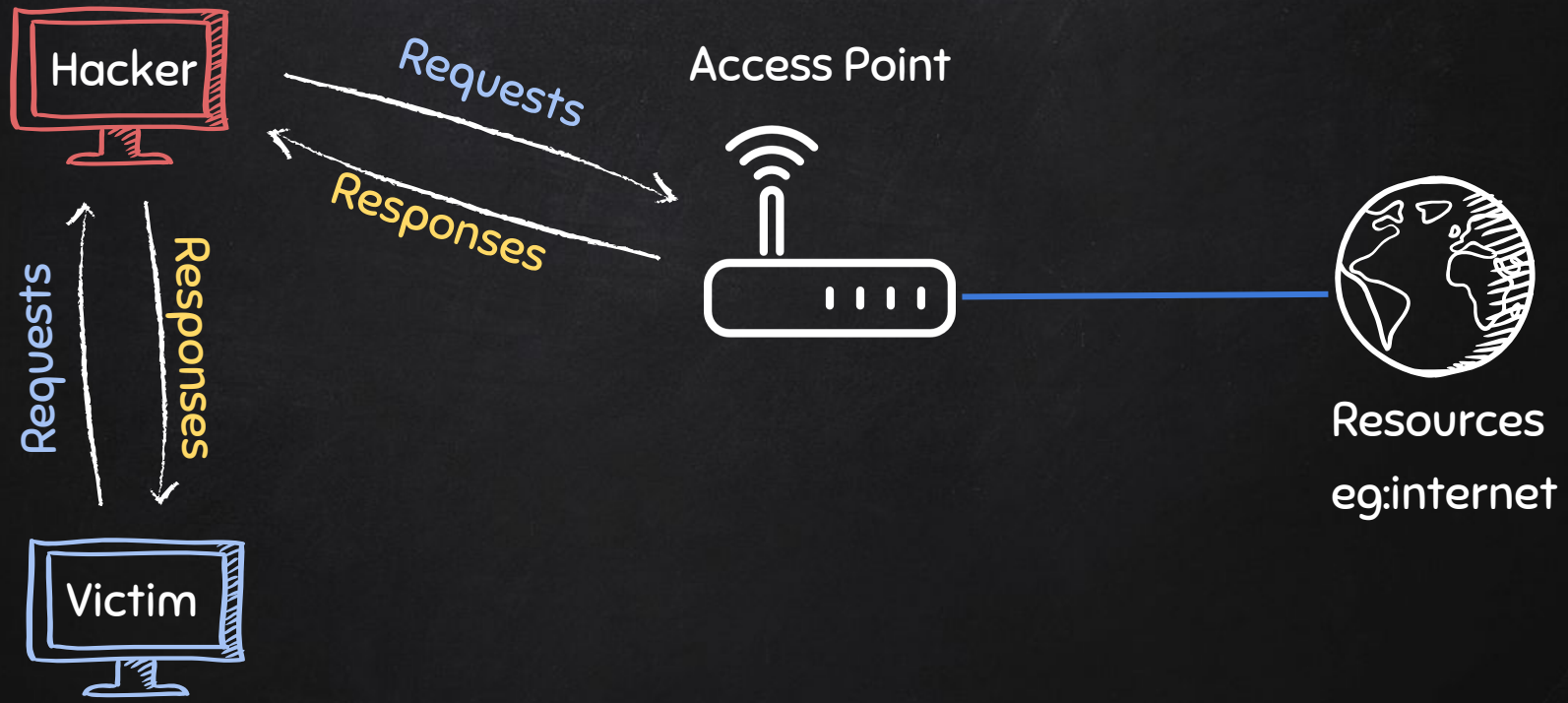
10.0.2.16

HACKER WEB SERVER
10.0.2.16



DNS SERVER

ARP Spoofing



Bettercap

Code Injection

- Inject Javascript code in loaded pages.
- Code gets executed by the target browser.
- This can be used to
  - Replace links.
  - Replace images.
  - Insert html elements.
  - Hook target browser to exploitation frameworks.
  - + more!

Bettercap

Web Interface

- Web interface:
  - More user-friendly.
  - Requires more resources.
  - And more modules.

Creating a Fake Access Point Using Mana-Toolkit

- Tools run rogue access point attacks.
- It can:
  - Automatically configure and create fake AP.
  - Automatically sniff data.
  - Automatically bypass https.
  - ....etc

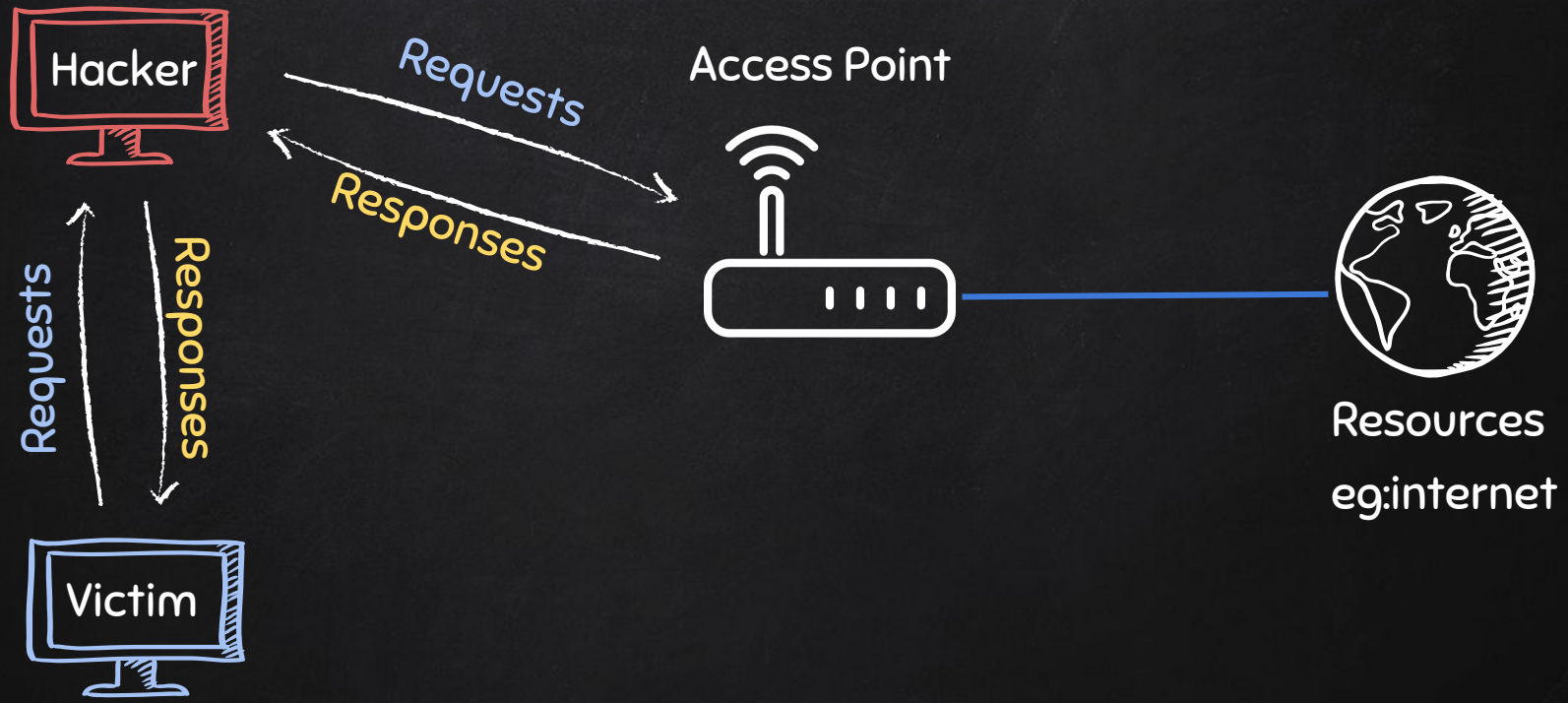
Creating a Fake Access Point Using Mana-Toolkit

- Tools run rogue access point attacks.
- It can:
  - Automatically configure and create fake AP.
  - Automatically sniff data.
  - Automatically bypass https.
  - ....etc

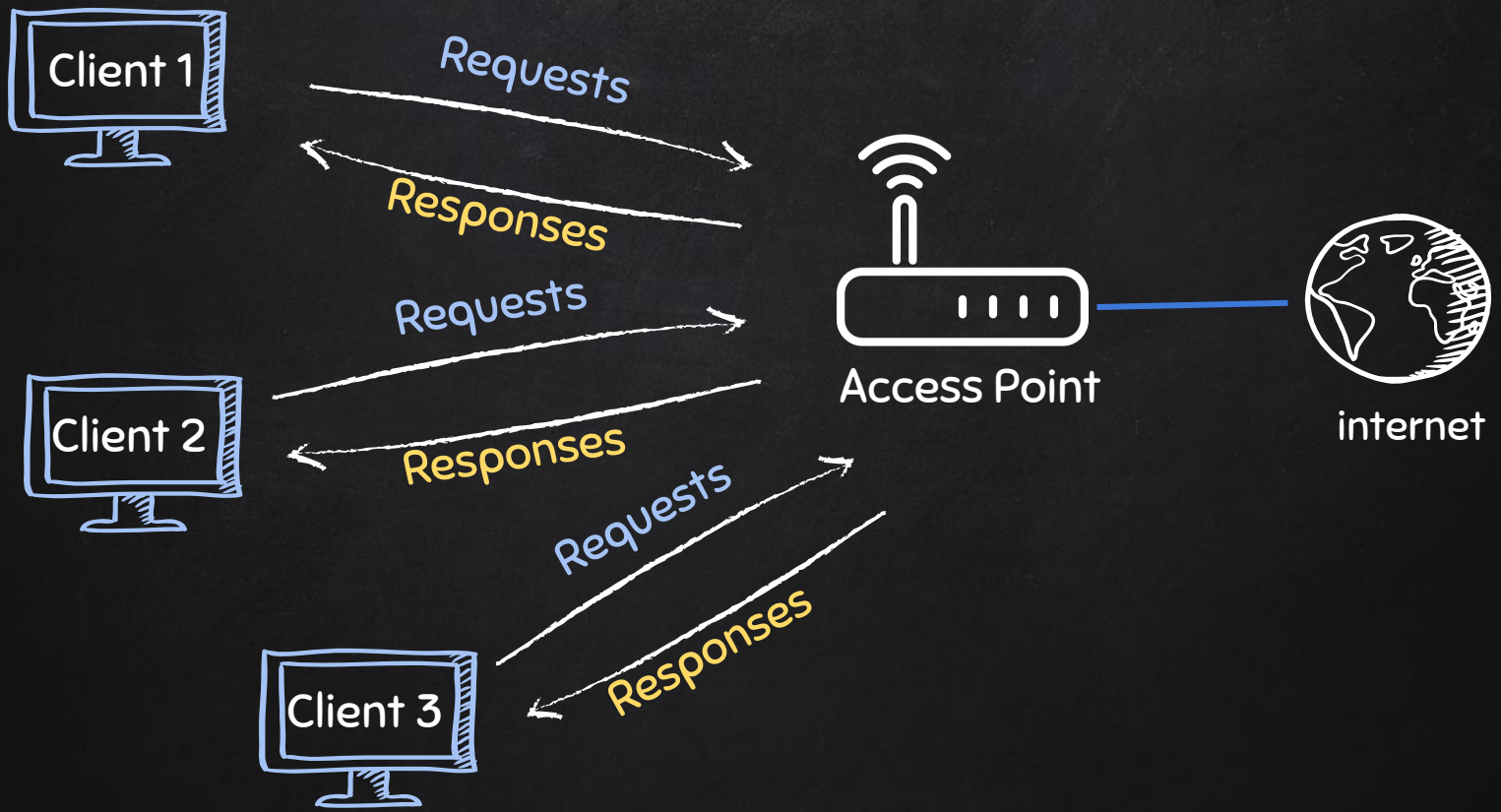
Mana has 3 main start scripts:

1. start-noupstream.sh – starts fake AP with no internet access.
2. start-nat-simple.sh – starts fake AP with internet access.
3. start-nat-full.sh – starts fake AP with internet access, and automatically starts sniffing data, bypass https.

ARP Spoofing

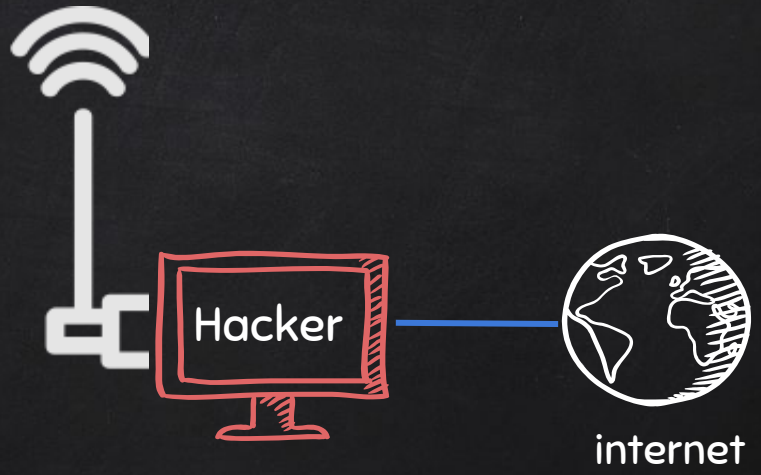


Typical Network

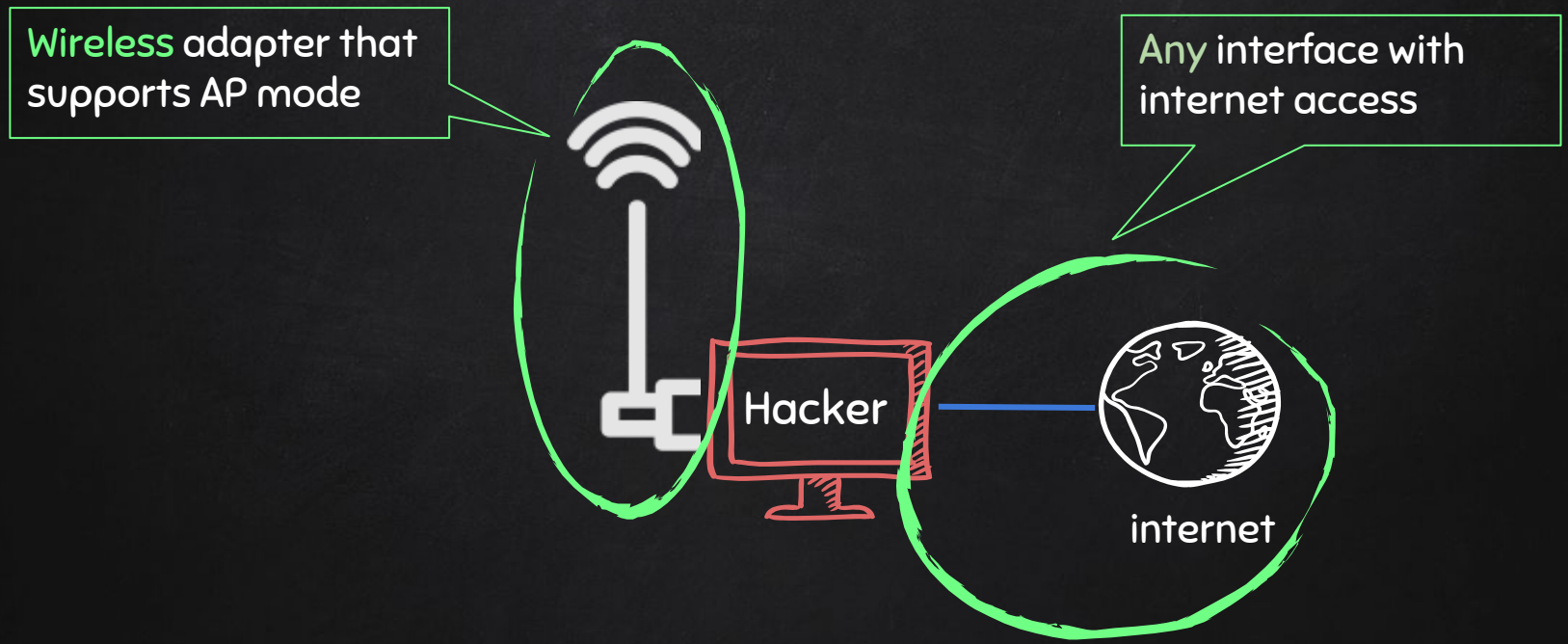


Creating a Fake Access Point

Creating a Fake Access Point



Creating a Fake Access Point



MITM Attacks

Detection & Prevention

Detection:

1. Analysing arp tables.
2. Using tools such as Xarp.
3. Using Wireshark.

MITM Attacks

Detection & Prevention

Detection:

1. Analysing arp tables.
2. Using tools such as Xarp.
3. Using Wireshark.

Problems:

1. Detection is not the same as prevention.
2. Only works for ARP Spoofing.

MITM Attacks

Detection & Prevention

Detection:

1. Analysing arp tables.
2. Using tools such as Xarp.
3. Using Wireshark.

Problems:

1. Detection is not the same as prevention.
2. Only works for ARP Spoofing.

Solution:

–> Encrypt traffic.

- HTTPS everywhere plugin.
- Using a VPN.

MITM Attacks

Prevention

	Pros	Cons
HTTPS Everywhere	Free	– Only works with HTTPS websites. – Visited domains still visible. – DNS spoofing still possible.

MITM Attacks

Prevention

	Pros	Cons
HTTPS Everywhere	Free	– Only works with HTTPS websites. – Visited domains still visible. – DNS spoofing still possible.
VPN	– Encrypts everything. – Protects from all MITM attacks.	– Not free. – VPN provider can see data.

MITM Attacks

Prevention

	Pros	Cons
HTTPS Everywhere	Free	– Only works with HTTPS websites. – Visited domains still visible. – DNS spoofing still possible.
VPN	– Encrypts everything. – Protects from all MITM attacks.	– Not free. – VPN provider can see data.
HTTPS Everywhere + VPN	– Encrypts everything. – Protects from all MITM attacks.	– Not free

MITM Attacks

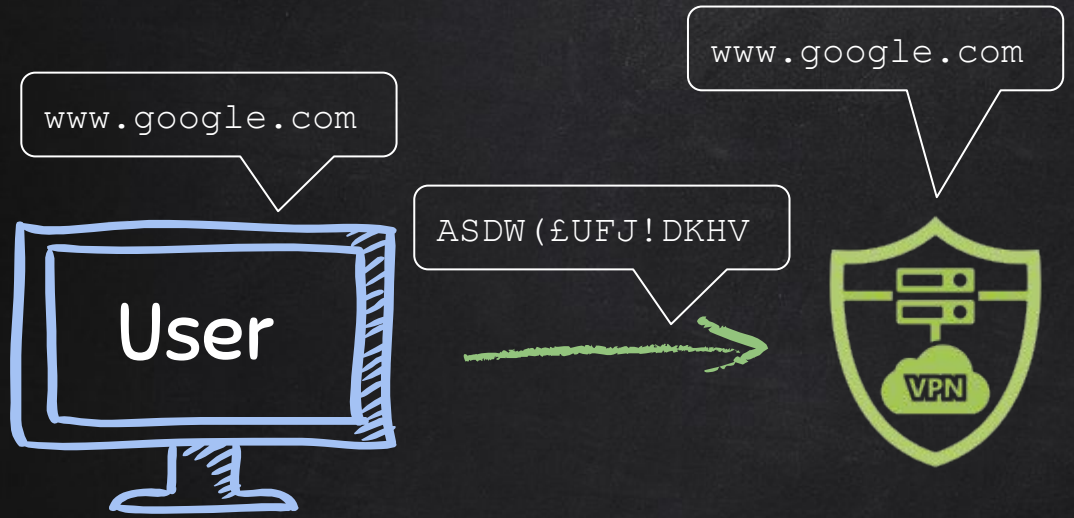
Prevention

VPN – Virtual Private Network


User
Google.com


User
VPN


www.google.com
User
www.google.com
VPN


www.google.com
User
ASDW(£UFJ!DKHV
www.google.com
VPN


www.google.com
User
ASDW(£UFJ!DKHV
www.google.com
VPN
Google.com

Benefits:

- Extra layer of encryption.
- More privacy & anonymity.
- Bypass censorship.
- Protection from hackers.

Benefits:

- Extra layer of encryption.
- More privacy & anonymity.
- Bypass censorship.
- Protection from hackers.

Notes:

- Use reputable VPN.

Notes:

- Use reputable VPN.
- Avoid free providers.

Notes:

- Use reputable VPN.
- Avoid free providers.
- Make sure they keep no logs.

Notes:

- Use reputable VPN.
- Avoid free providers.
- Make sure they keep no logs.
- Use HTTPS everywhere.

Notes:

- Use reputable VPN.
- Avoid free providers.
- Make sure they keep no logs.
- Use HTTPS everywhere.
- Optional – pay with crypto.