

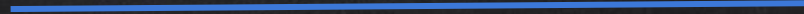
NETWORK MAPPING

NMAP / ZENMAP

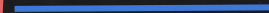
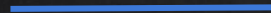


- HUGE security scanner.
- From an IP/IP range it can discover:
 - Open ports.
 - Running services.
 - Operating system.
 - Connected clients.
 - + more

MITM ATTACKS



Resources
eg:internet



Resources
eg:internet

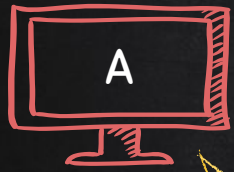
Man In The Middle

<https://t.me/learningnets>

ADDRESS RESOLUTION PROTOCOL (ARP)

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

ARP Request

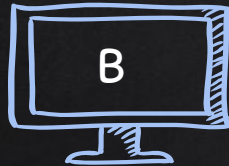


Router



IP: 10.0.2.1

MAC: 00:11:22:33:44:20



IP: 10.0.2.5

MAC: 00:11:22:33:44:44



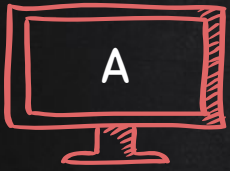
IP: 10.0.2.6

MAC: 00:11:22:33:44:66



IP: 10.0.2.7

MAC: 00:11:22:33:44:55



ARP Response
I have 10.0.2.6
My MAC is 00:11:22:33:44:66

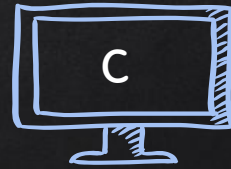
Router



IP: 10.0.2.1
MAC: 00:11:22:33:44:20



IP: 10.0.2.5
MAC: 00:11:22:33:44:44

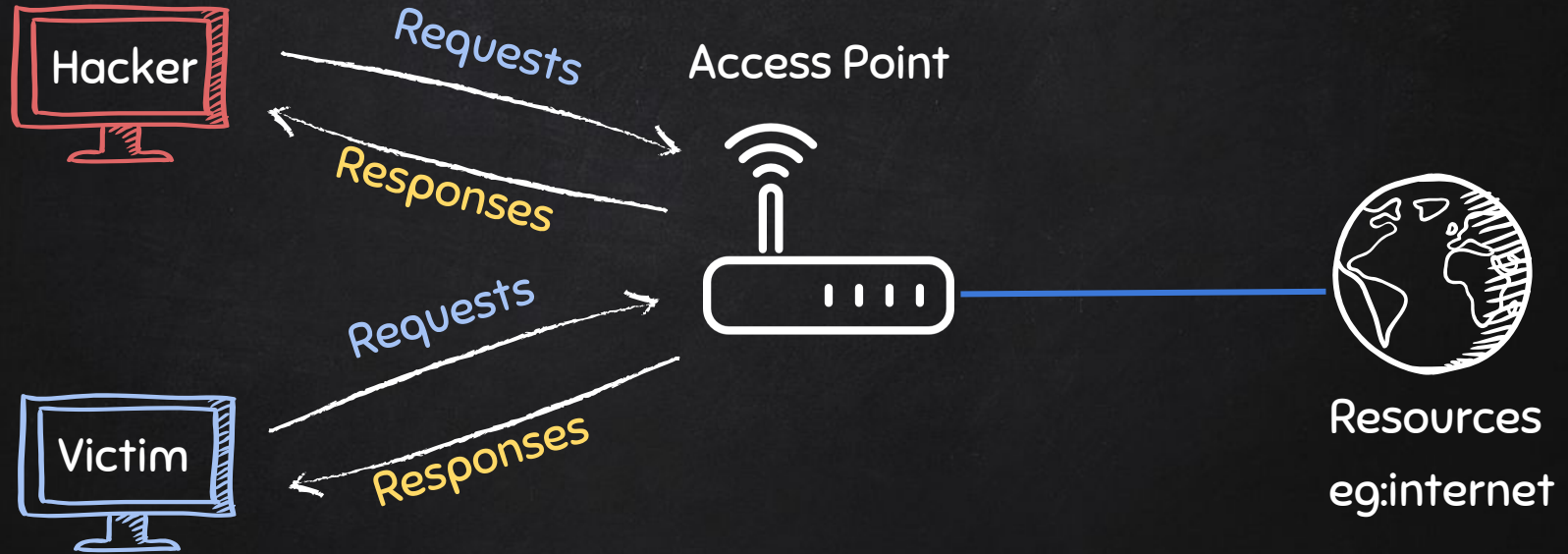


IP: 10.0.2.6
MAC: 00:11:22:33:44:66



IP: 10.0.2.7
MAC: 00:11:22:33:44:55

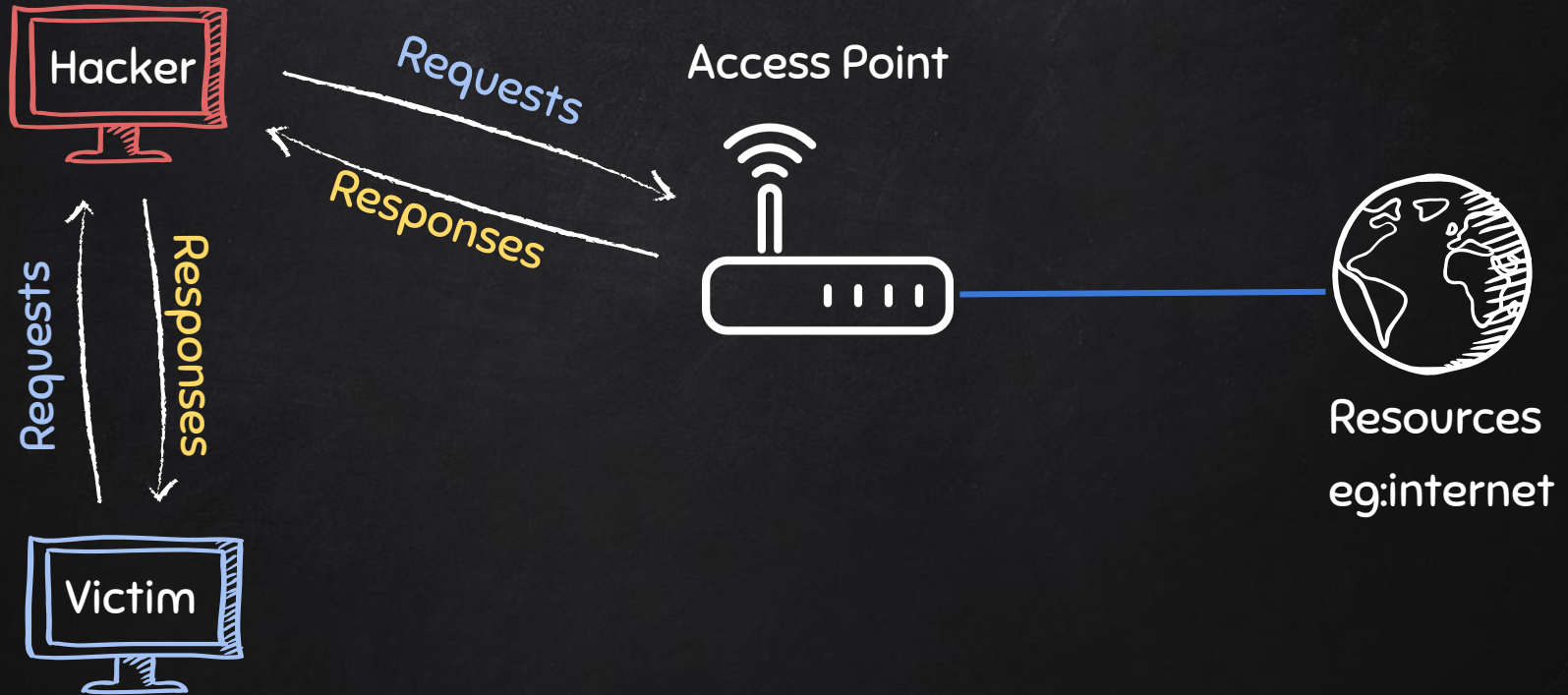
TYPICAL NETWORK



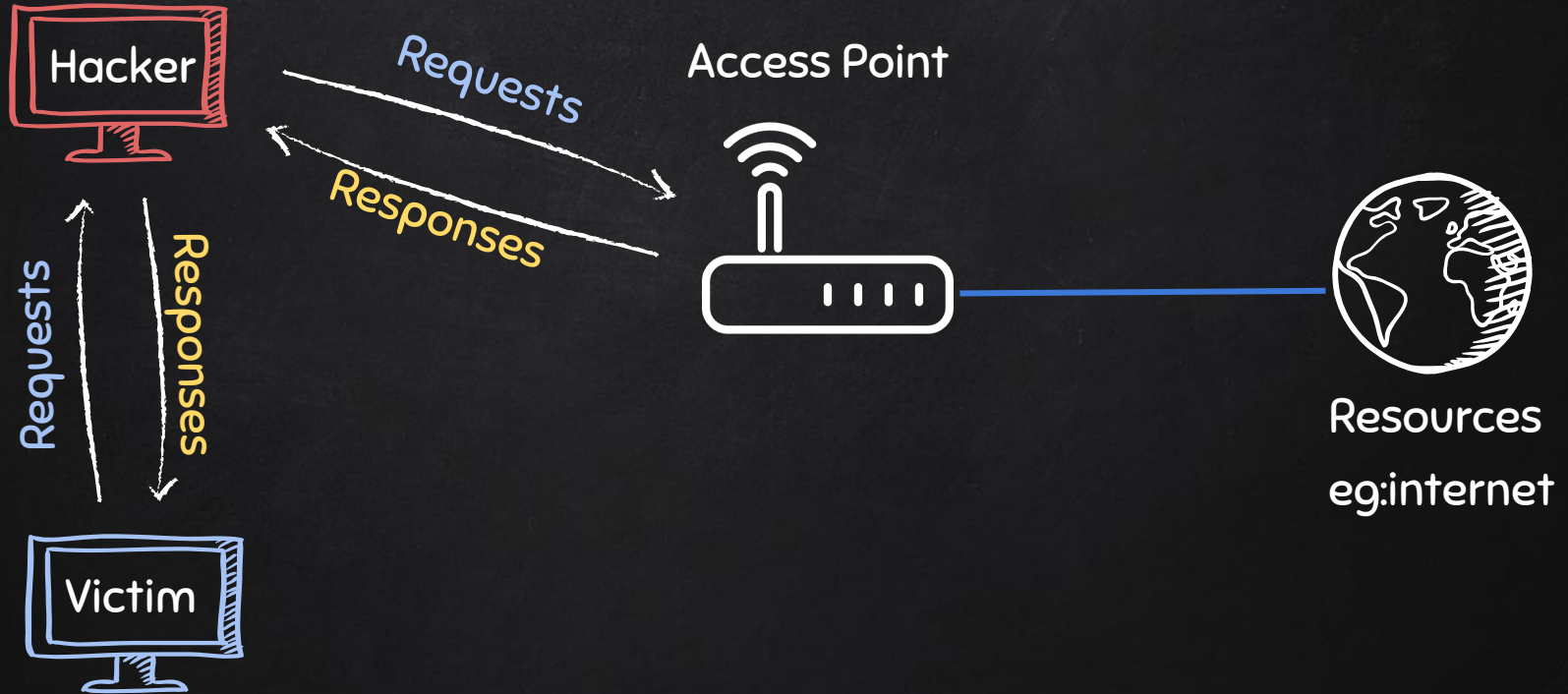
ARP SPOOFING



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://t.me/learningnets>

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



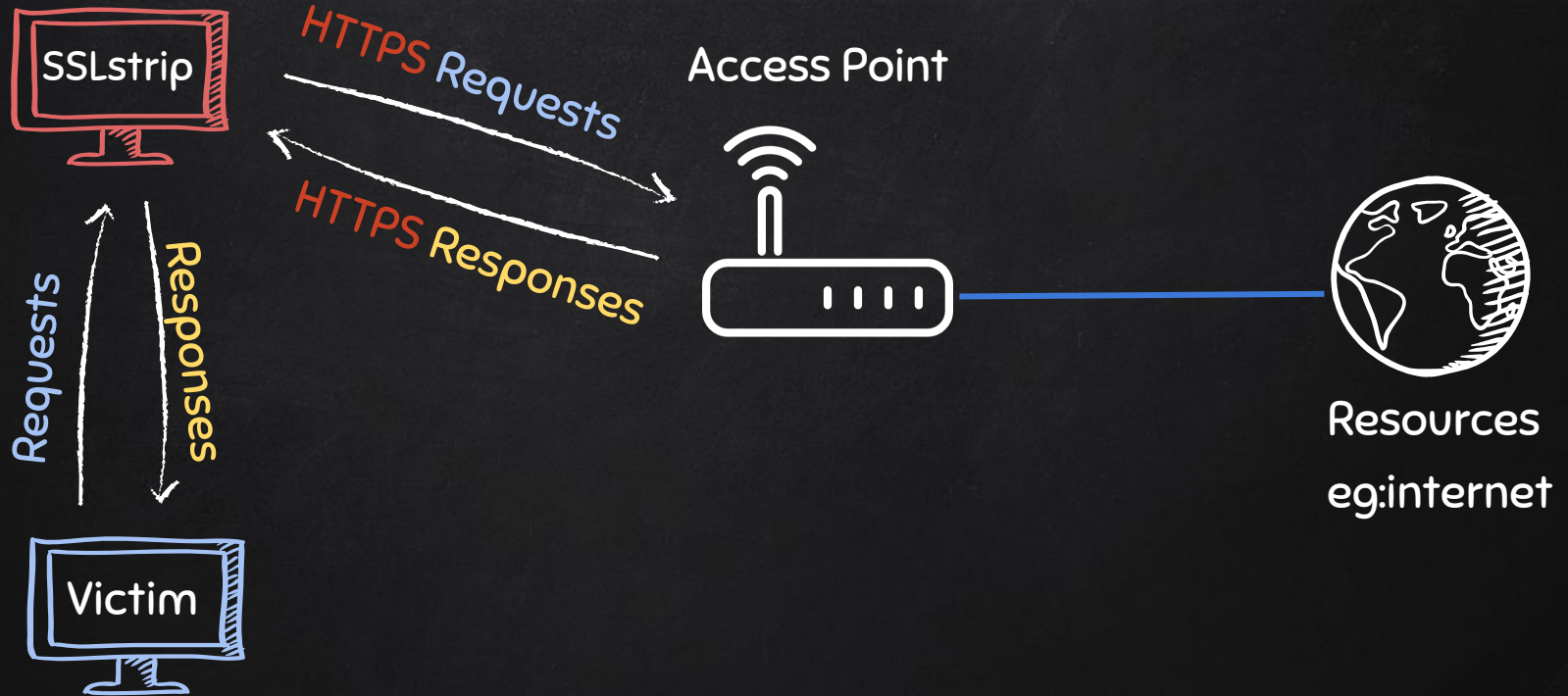
Problem:

- 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.

<https://t.me/learningnets>

BYPASSING HSTS



https://

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

<https://t.me/learningnets>

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



<https://t.me/learningnets>



FACEBOOK.COM WEB SERVER
195.44.2.1



LIVE.COM WEB SERVER
204.79.197.200



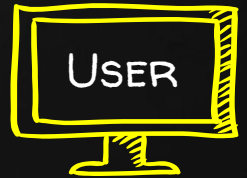
HACKER WEB SERVER
10.0.2.16



DNS SERVER

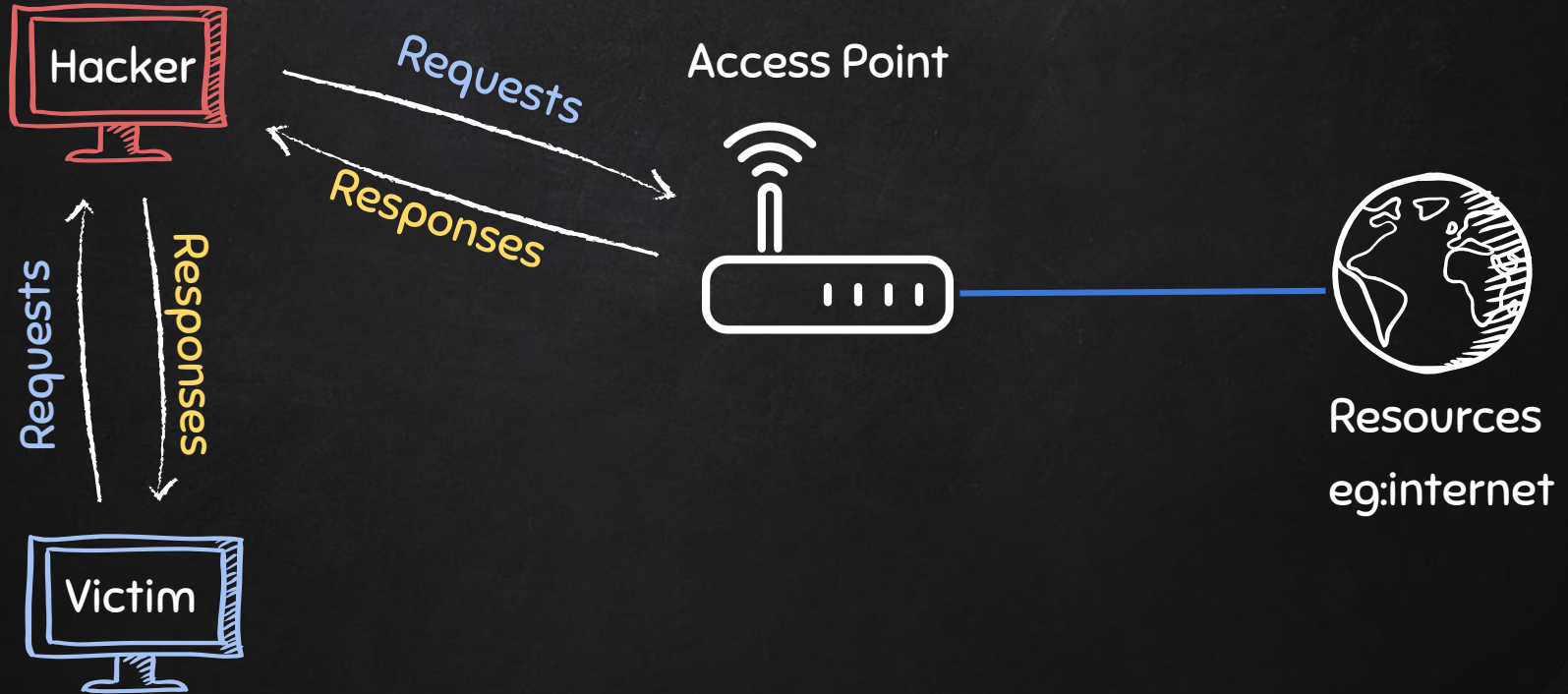


10.0.2.16



<https://t.me/learningnets>

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

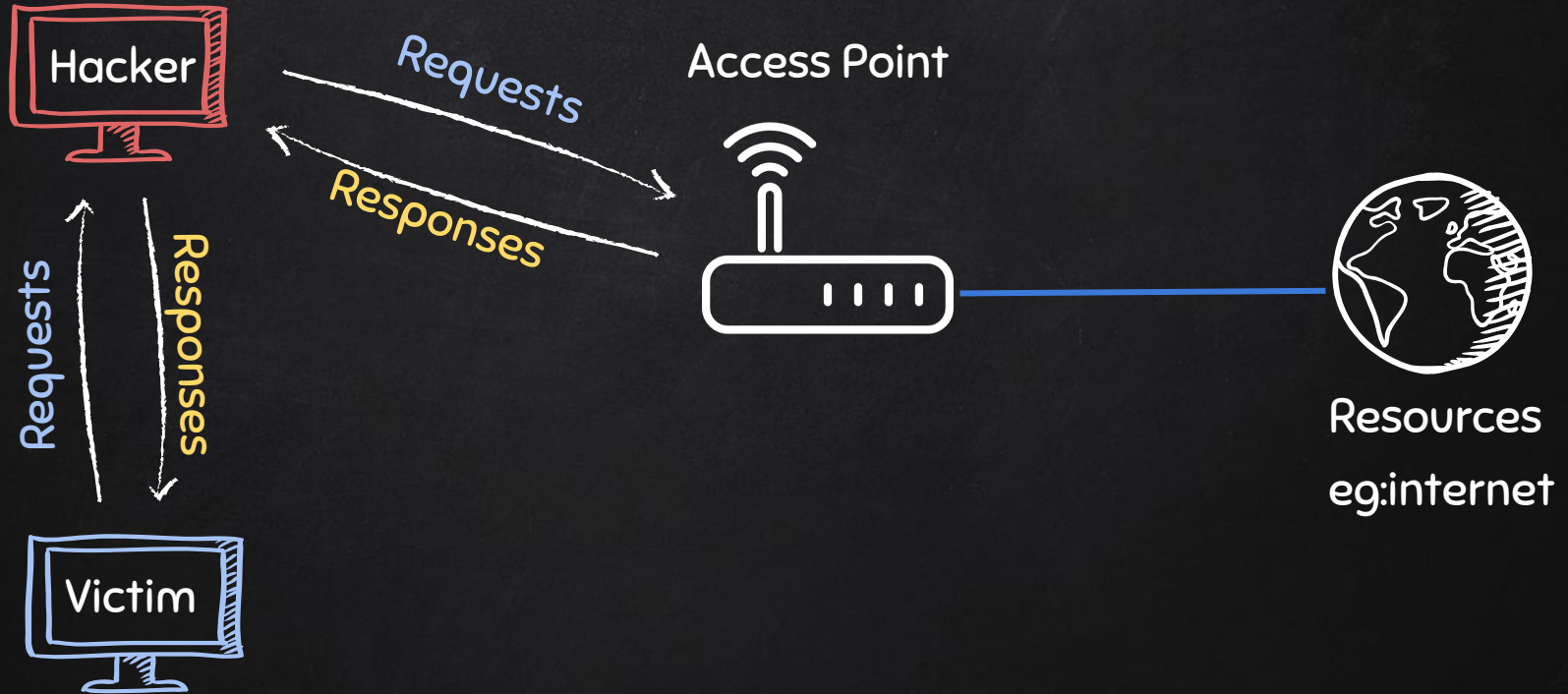
- Tools run rogue access point attacks.
- It can:
 - **Automatically** configure and create fake AP.
 - **Automatically** sniff data.
 - **Automatically** bypass https.
 - ...etc



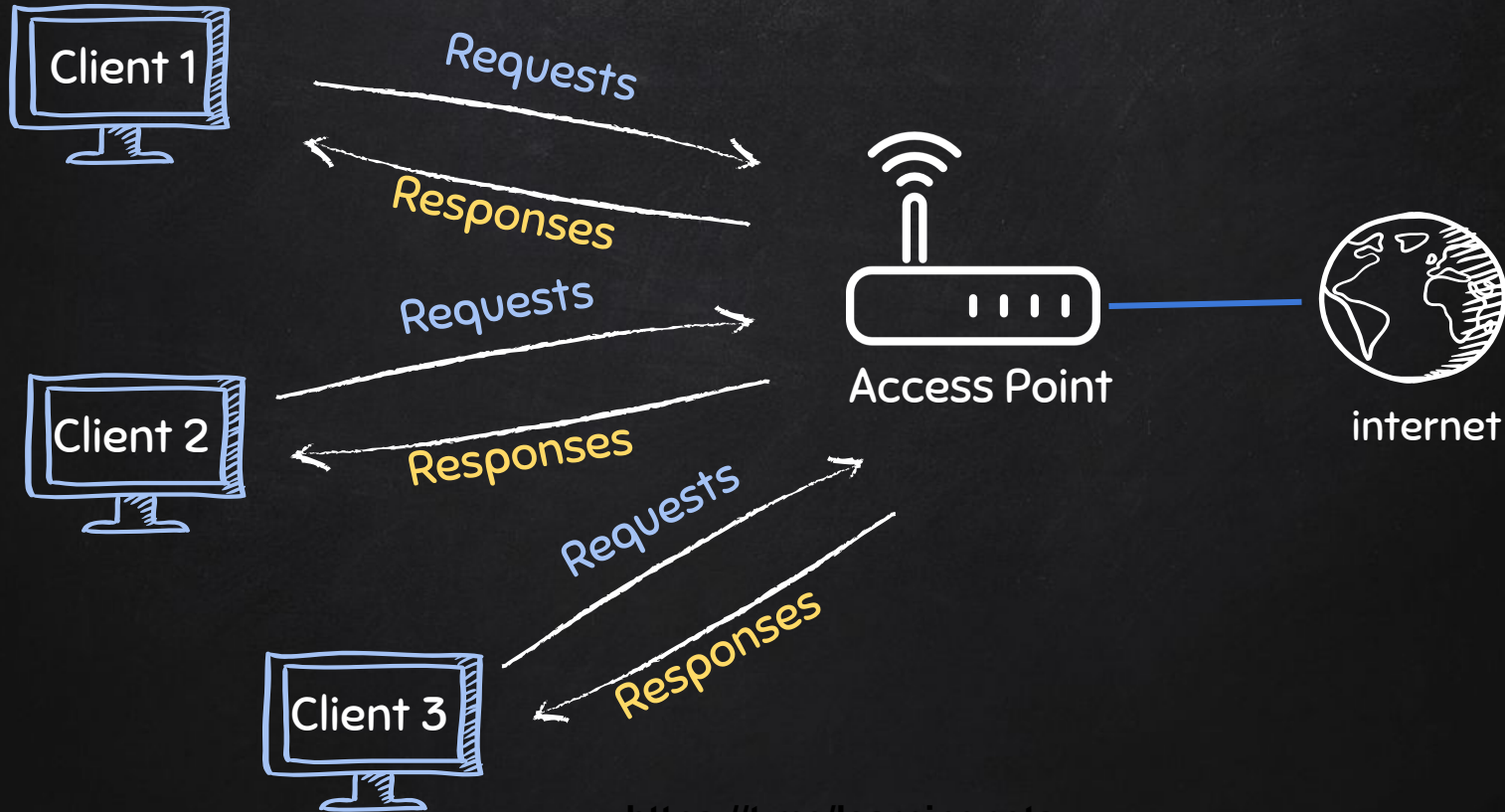
Mana has 3 main start scripts:

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

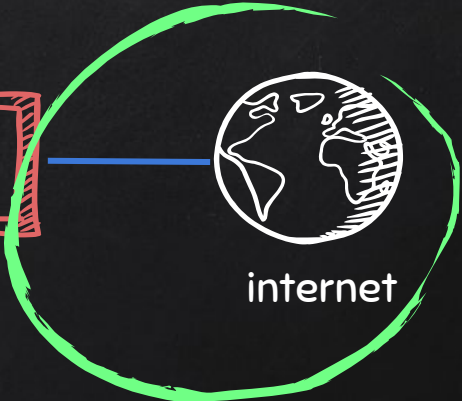


CREATING A FAKE ACCESS POINT

Wireless adapter that supports AP mode



Any interface with internet access



MITM ATTACKS

PREVENTION

	Pros	Cons
HTTPS Everywhere	Free	<ul style="list-style-type: none">- Only works with HTTPS websites.- Visited domains still visible.- DNS spoofing still possible.

MITM ATTACKS

PREVENTION

	Pros	Cons
HTTPS Everywhere	Free	<ul style="list-style-type: none">- Only works with HTTPS websites.- Visited domains still visible.- DNS spoofing still possible.
VPN	<ul style="list-style-type: none">- Encrypts everything.- Protects from all MITM attacks.	<ul style="list-style-type: none">- Not free.- VPN provider can see data.

MITM ATTACKS

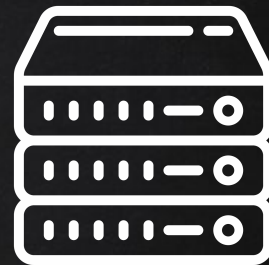
PREVENTION

	Pros	Cons
HTTPS Everywhere	Free	<ul style="list-style-type: none">- Only works with HTTPS websites.- Visited domains still visible.- DNS spoofing still possible.
VPN	<ul style="list-style-type: none">- Encrypts everything.- Protects from all MITM attacks.	<ul style="list-style-type: none">- Not free.- VPN provider can see data.
HTTPS Everywhere + VPN	<ul style="list-style-type: none">- Encrypts everything.- Protects from all MITM attacks.	<ul style="list-style-type: none">- Not free

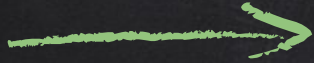
VPN - VIRTUAL PRIVATE NETWORK



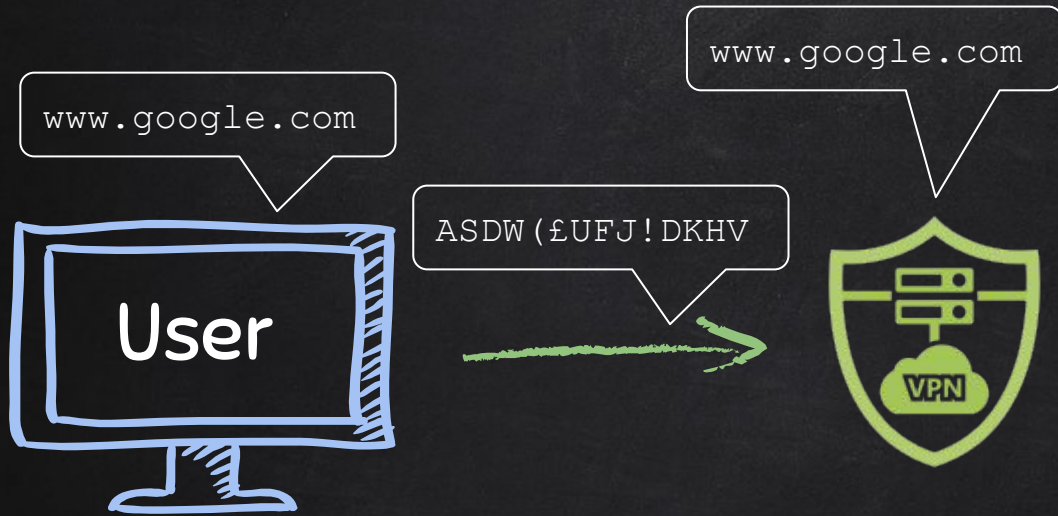
<https://t.me/learningnets>

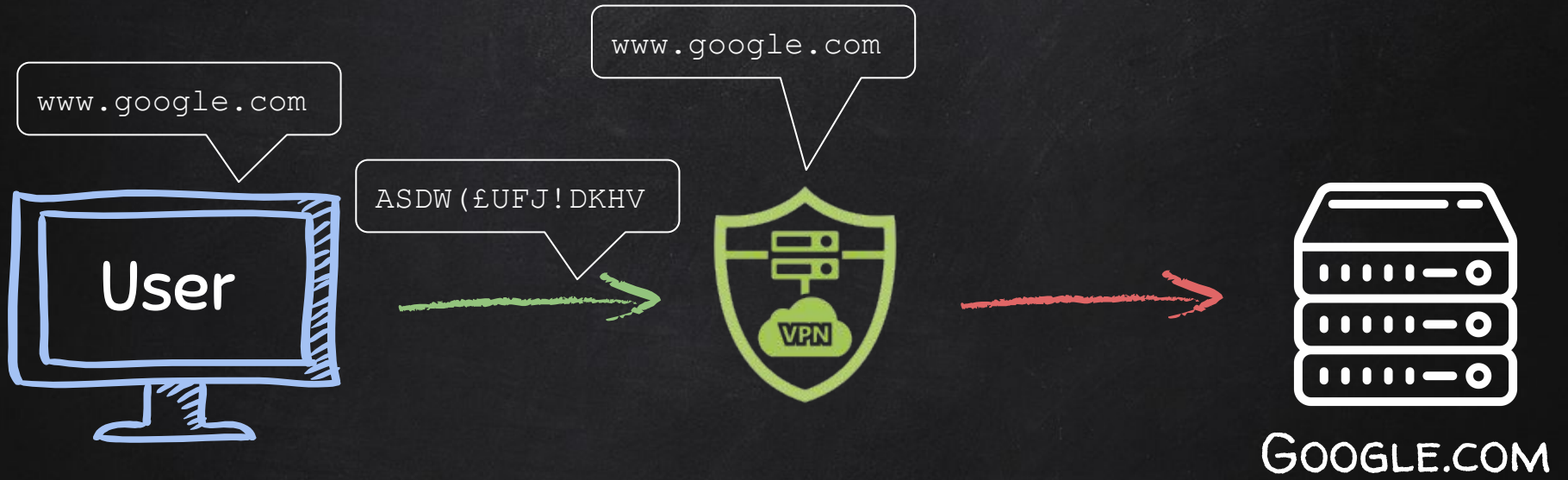


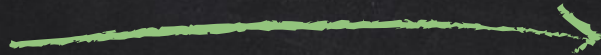
GOOGLE.COM











Internet

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.



Internet

Notes:

- Use reputable VPN.



Internet

Notes:

- Use reputable VPN.
- Avoid free providers.



Internet

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.