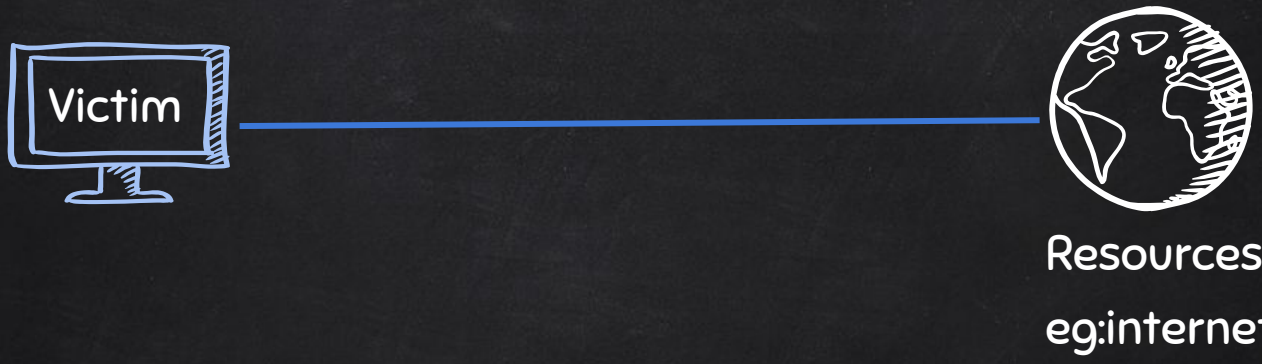
Network Mapping

Nmap / Zenmap

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

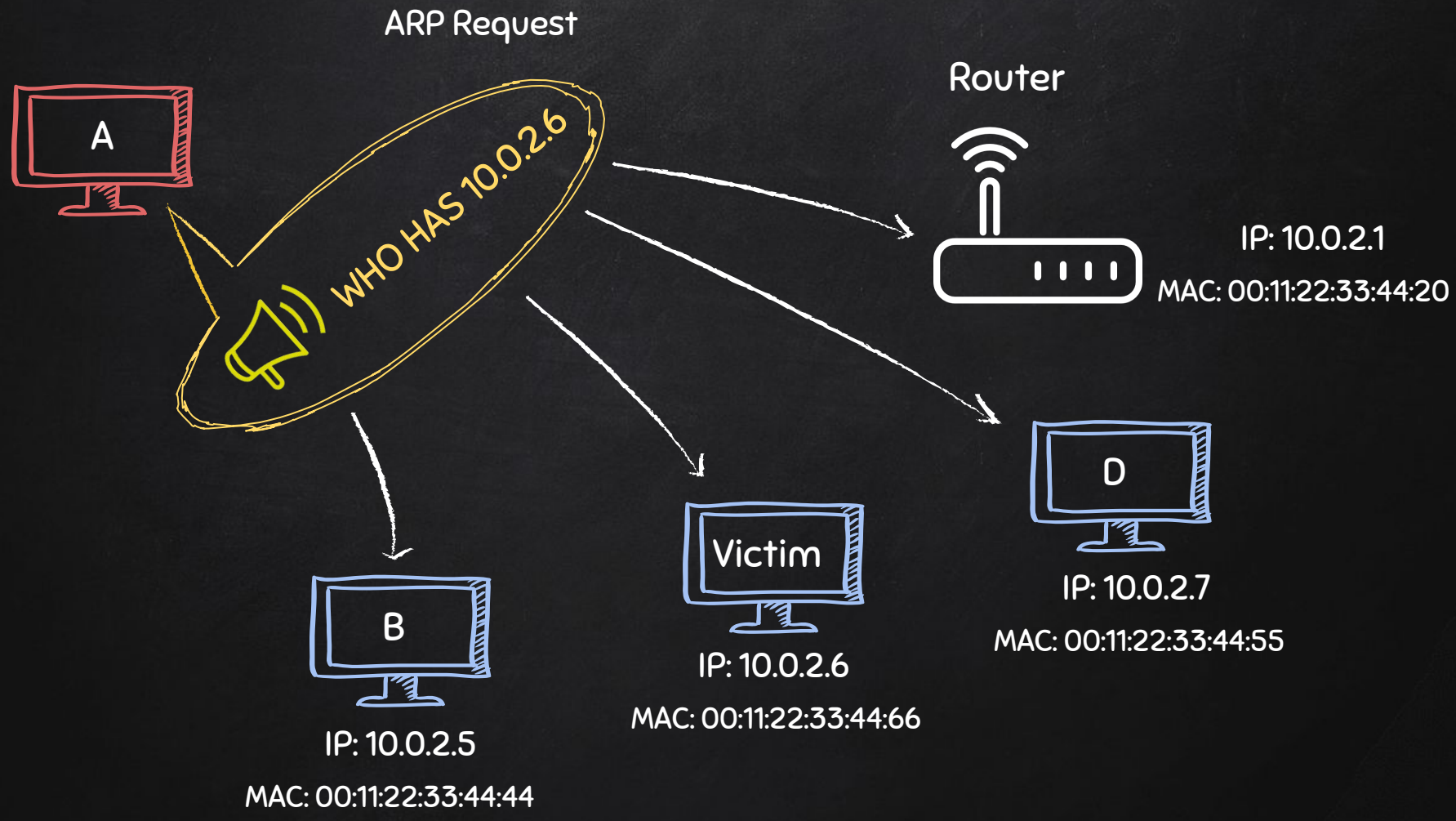
MITM Attacks

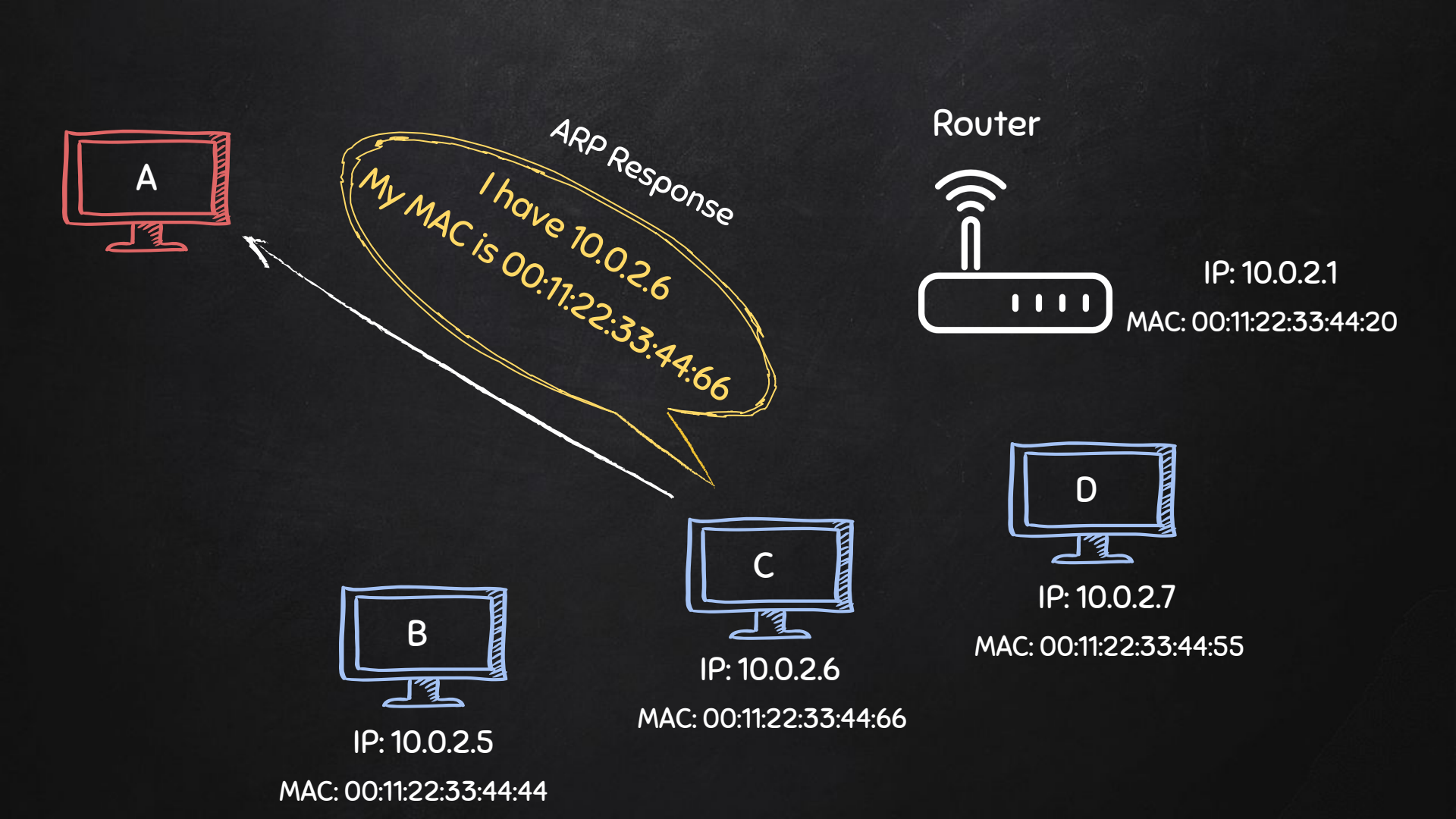


Address Resolution Protocol

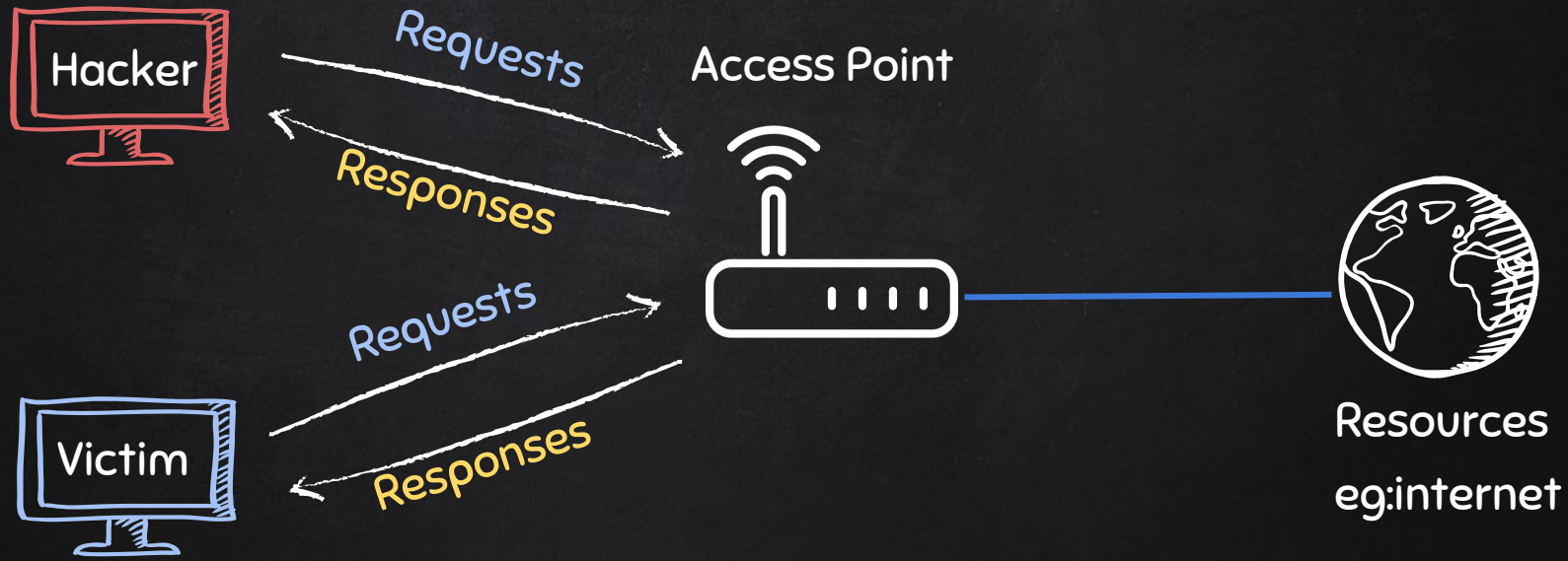
(ARP)

→ 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

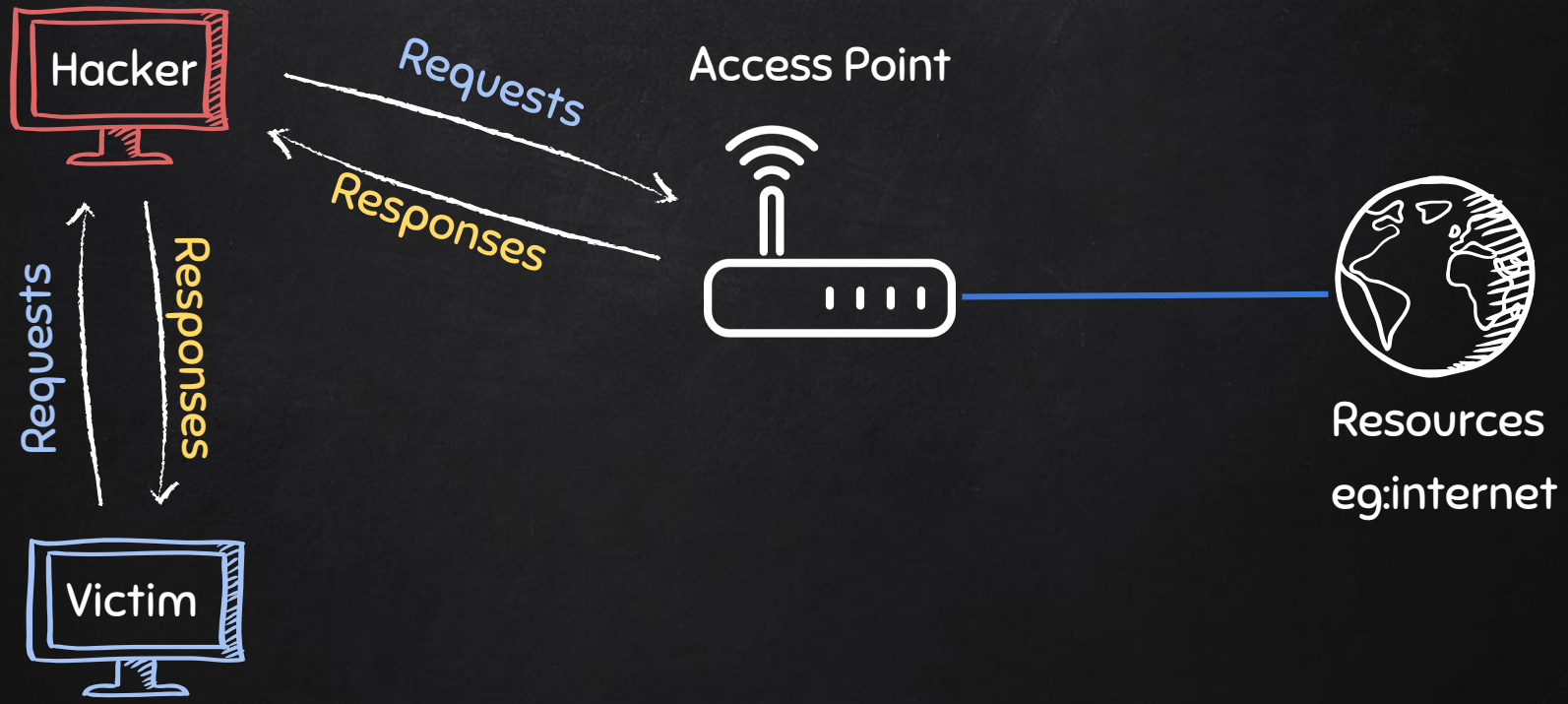

A
ARP Response
I have 10.0.2.6
My MAC is 00:11:22:33:44:66
Router
IP: 10.0.2.1
MAC: 00:11:22:33:44:20
D
IP: 10.0.2.7
MAC: 00:11:22:33:44:55
C
IP: 10.0.2.6
MAC: 00:11:22:33:44:66
B
IP: 10.0.2.5
MAC: 00:11:22:33:44:44

Typical Network

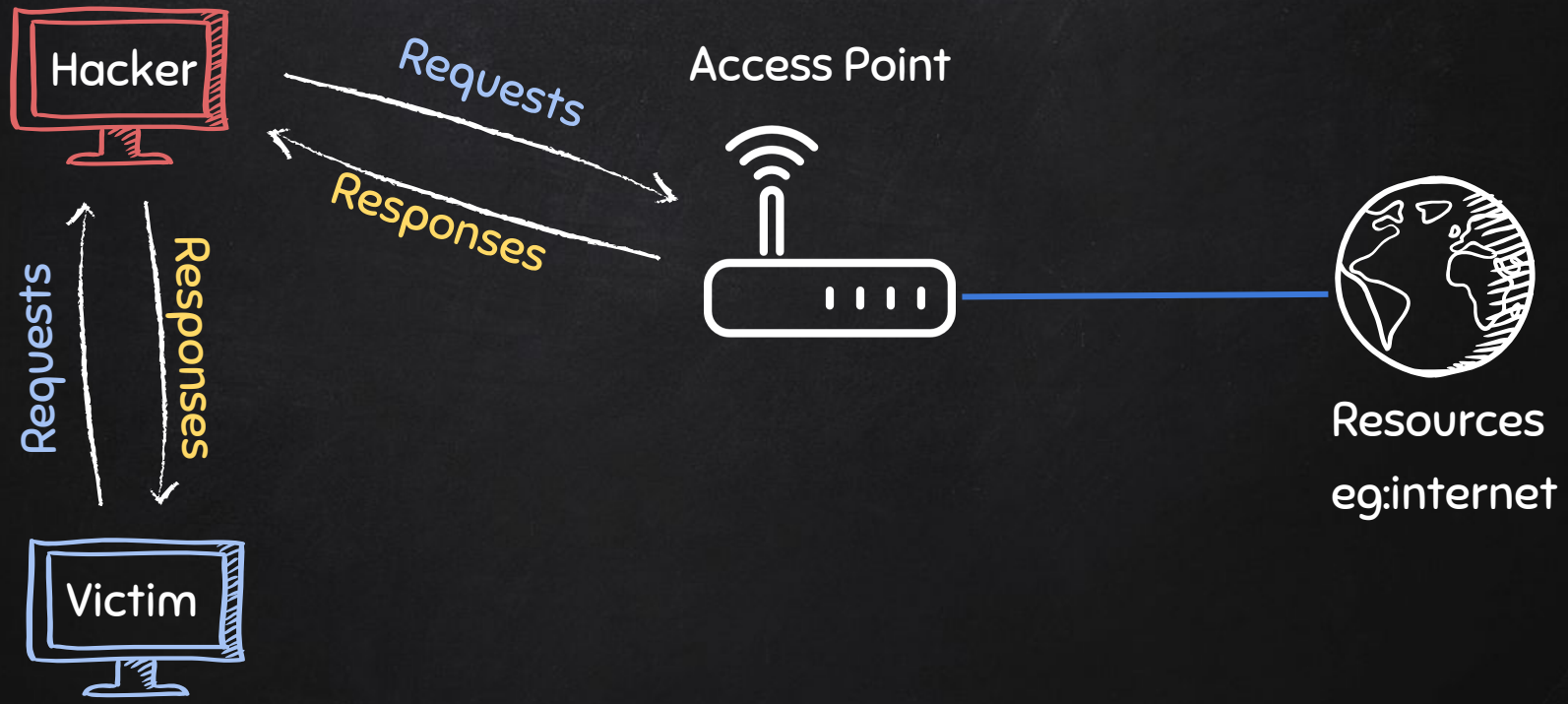


ARP Spoofing

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:

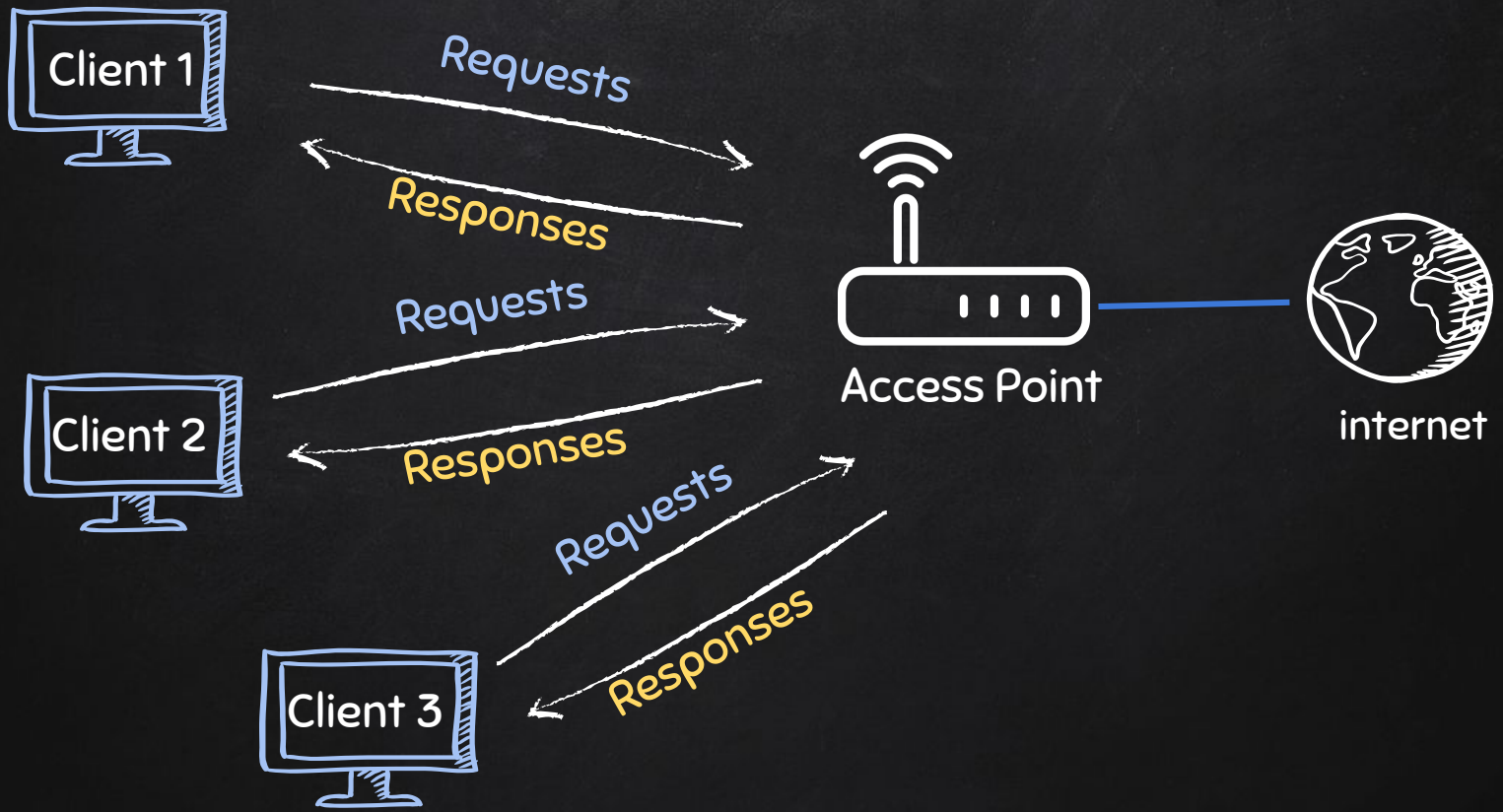
- Most websites use HTTPS

→ Sniffed data will be encrypted.

Solution:

- Downgrade HTTPS to HTTP.

Typical Network



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

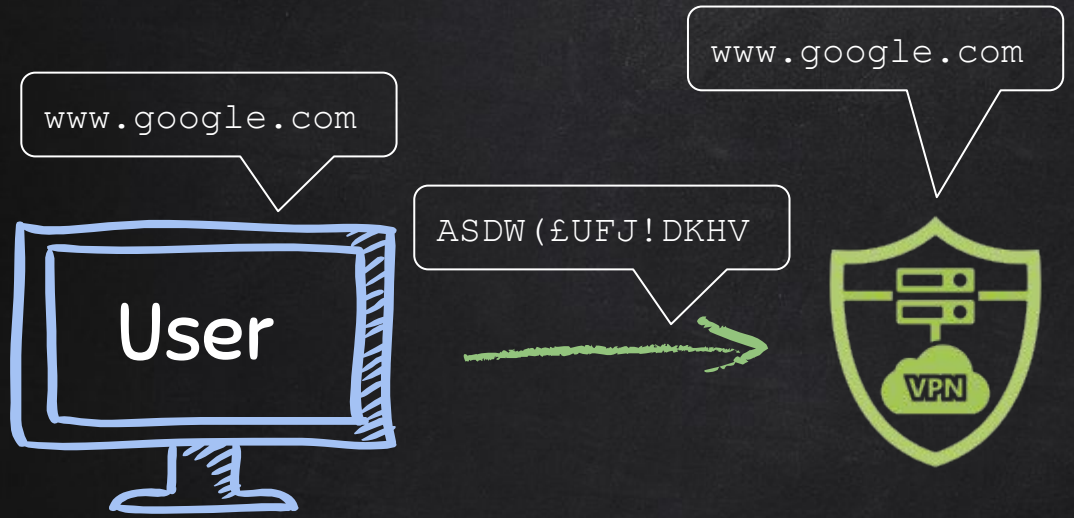
	Pros	Cons
HTTPS Everywhere	Free	– Only works with HTTPS websites. – Visited domains still visible. – DNS spoofing still possible.
VPN	– Encrypts everything. – Protects from all MITM attacks.	– Not free. – VPN provider can see data.
HTTPS Everywhere + VPN	– Encrypts everything. – Protects from all MITM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

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.