ARP Spoofing & Man-in-the-Middle Attacks

Team 7:

Juan Fernández García

Pablo Lolo Neira

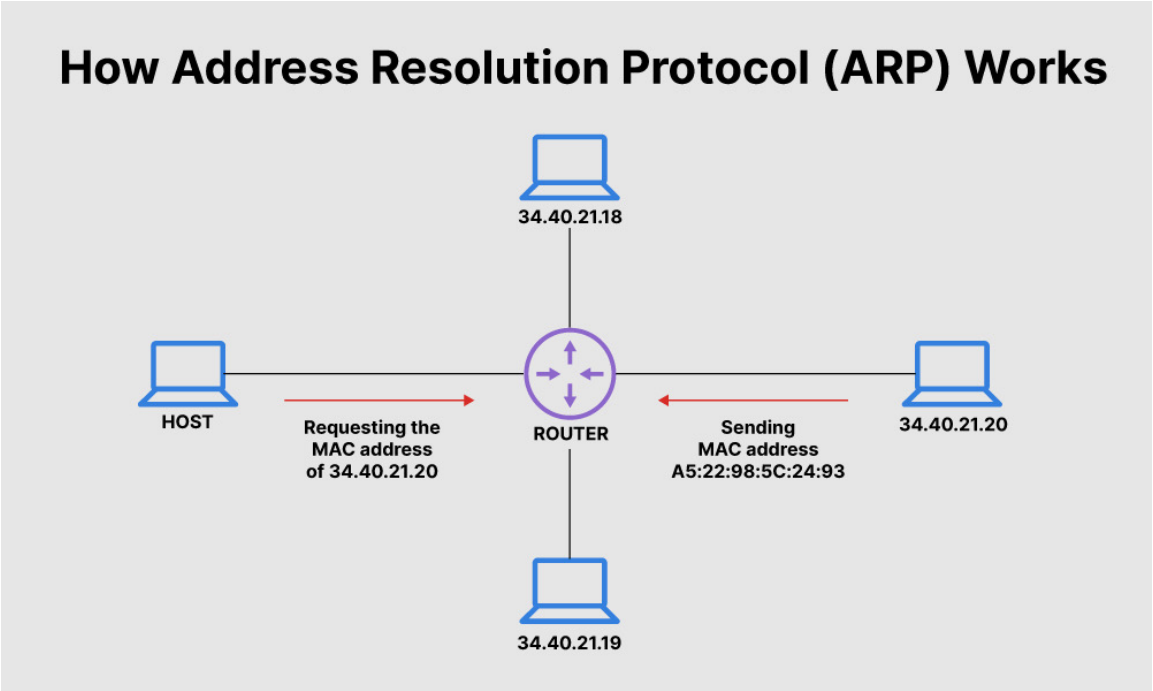
juan.fernandezgarci01@universitadipavia.it

pablo.loloneira01@universitadipavia.it

University of Pavia – Department of Electrical, Computer and Biomedical Engineering

What is ARP?

- Protocol mapping IP to MAC.
- ARP Request & ARP Reply.
- ARP Table.



Why ARP is Vulnerable

NO AUTHENTICATION.

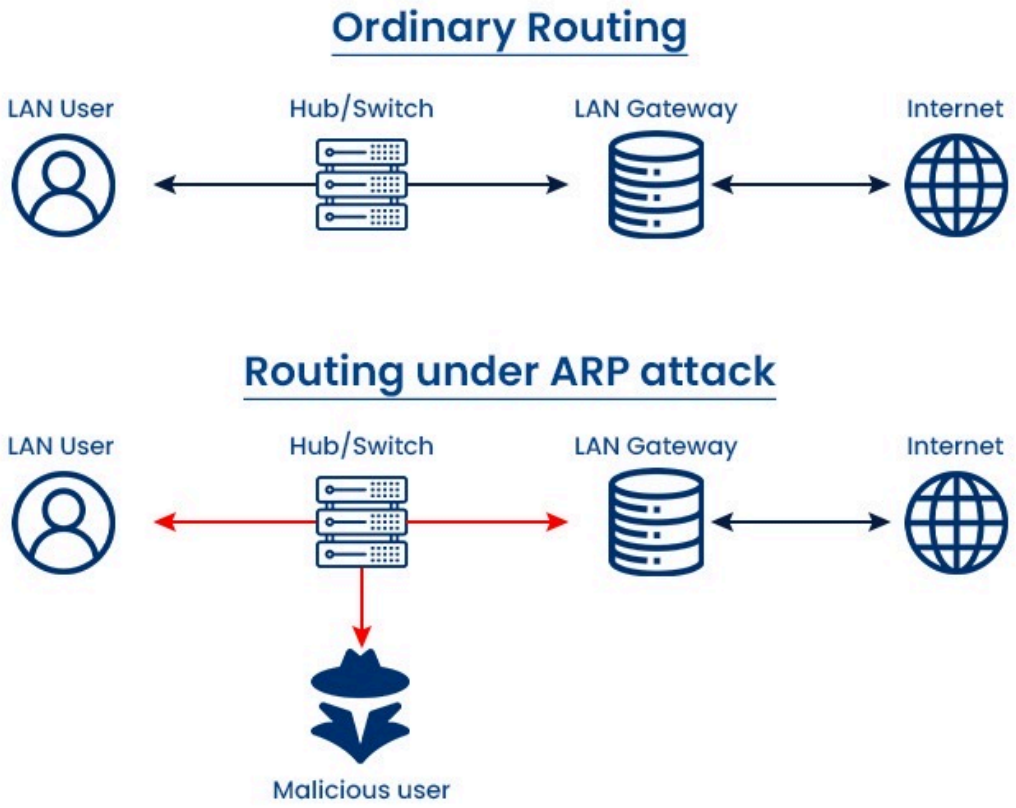
DEVICES TRUST ANY ARP REPLY.

What is ARP Spoofing?

- Sending fake ARP replies.
- Altering ARP tables.
- Used to initiate MITM.

Visual Example

- Attacker places itself between victim and router.

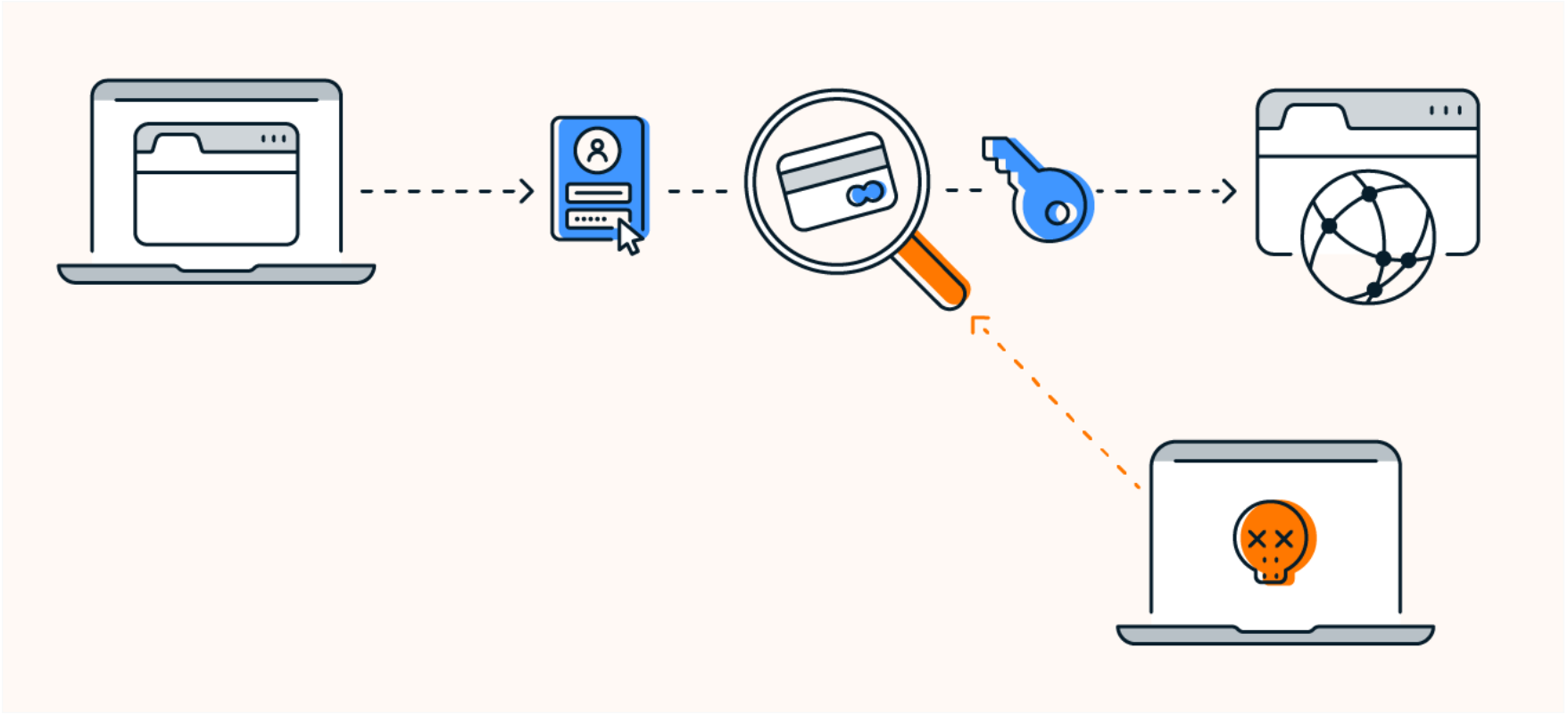


Conseceunces of ARP Spoofing

Paswords
Tracking our activity
Session hijacking
Modifications
Redirections.

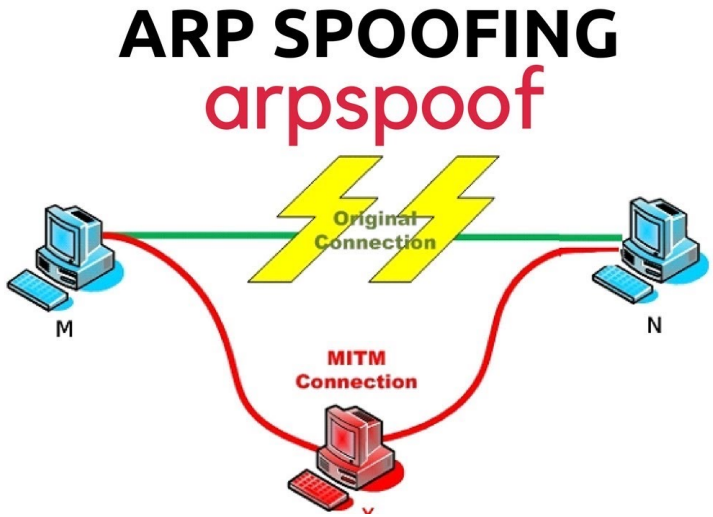
Sniffing

Wireshark/tcpdump capture credentials & sessions.



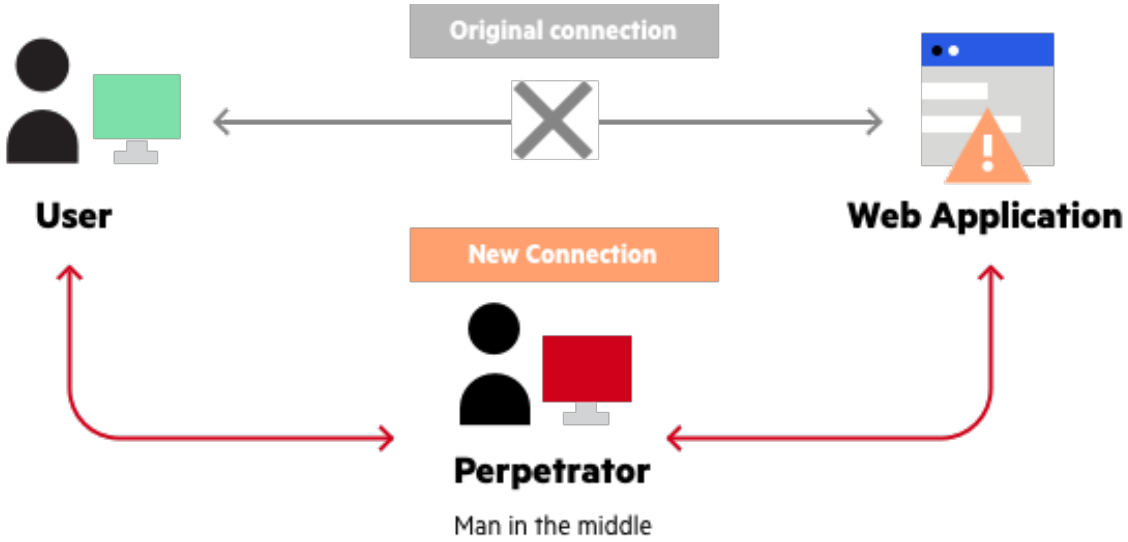
Tools

- Ettercap, ARPspoof, Wireshark,TCPdump.



What is a MITM Attack?

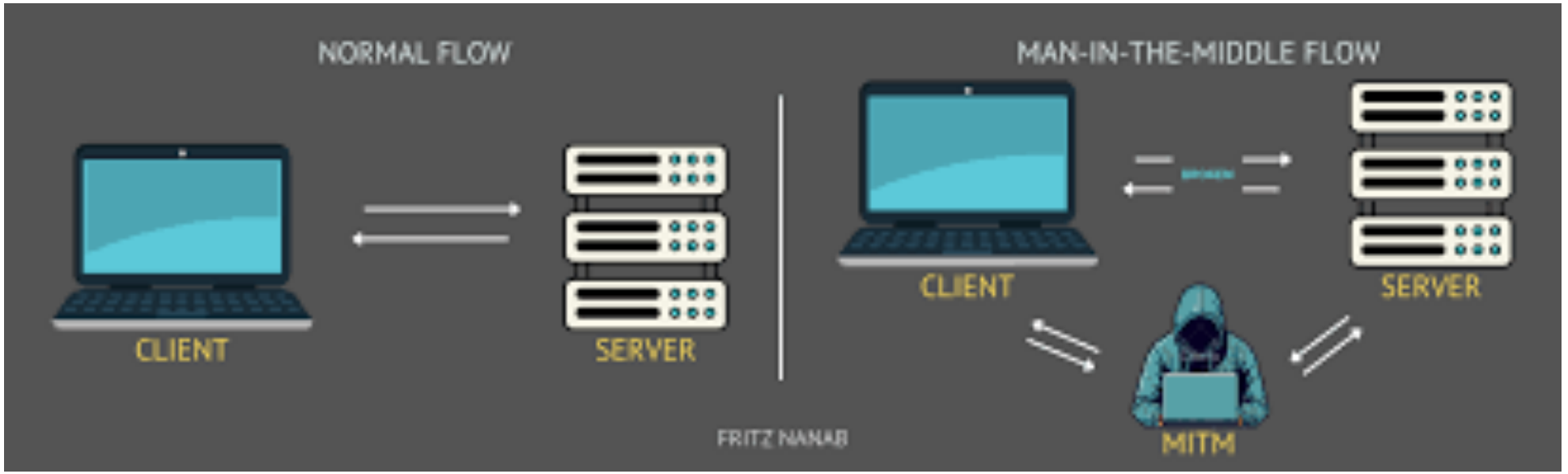
- Attacker intercepts communication between two parties.



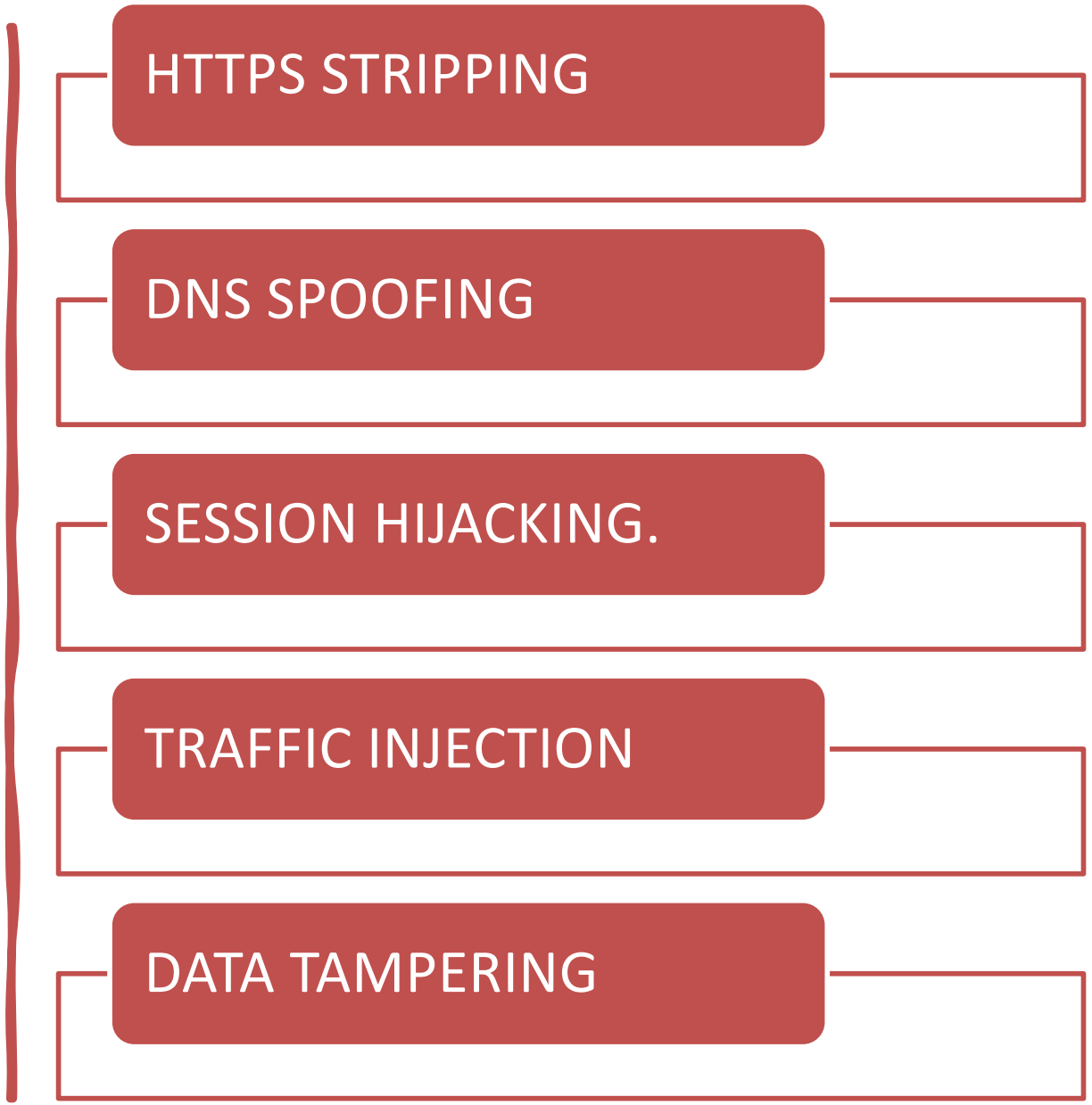
MITM Flow

Victim → Attacker → Router.

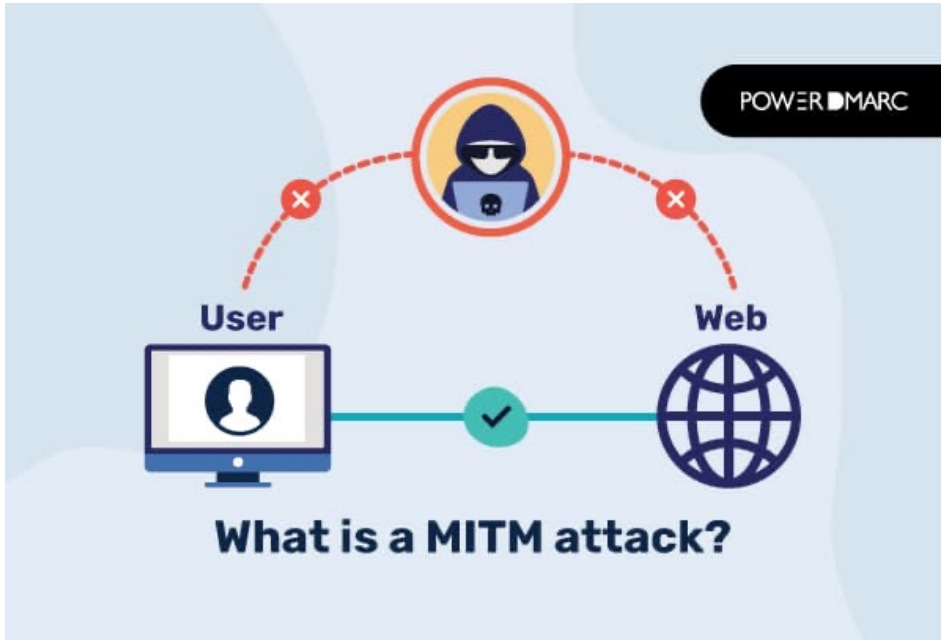
ROUTER→ Attacker → VICTIM.

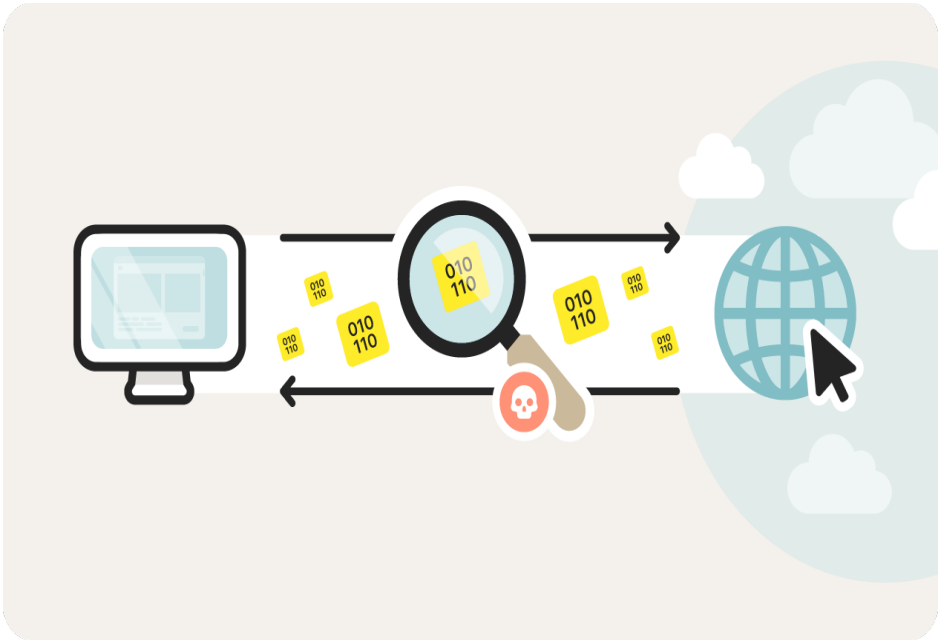


Techniques inside MITM



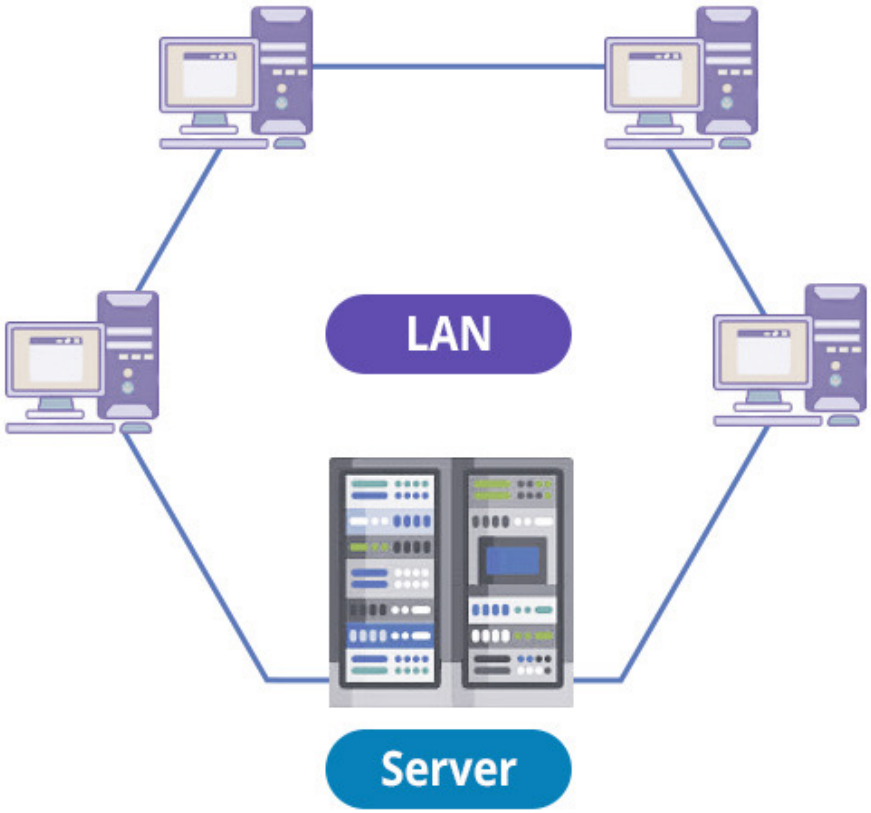
Sniffing during MITM





Limitations

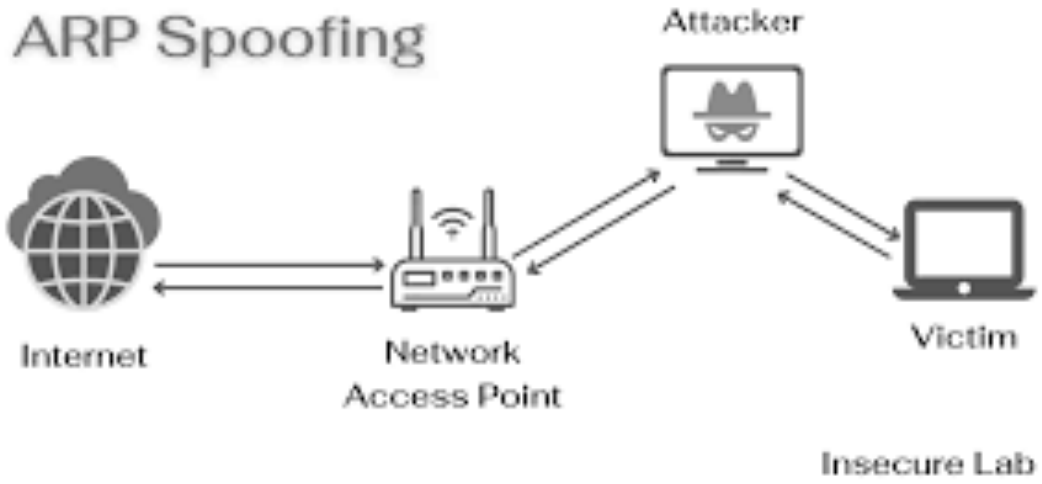
- Requires same LAN.
- Common in cafés, offices, universities.



DEFENSES MITM

- HTTPS
- HSTS
- SWITCH LEVEL PROTECTION
- ARP MONITORING TOOLS
- VPN
- segmentation.

Conclusion



- ARP Spoofing enables MITM.
- Simple but dangerous attack.

Sources

- https://www.cisco.com/c/en/us/about/security-center/arp-spoofing.html
- https://www.cloudflare.com/learning/ddos/glossary/arp-spoofing/
- https://www.kaspersky.com/resource-center/definitions/man-in-the-middle-attack
- https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNz3CAG
- https://www.fortinet.com/resources/cyberglossary/arp-spoofing