OWASP

Open Web Application Security Project

# MITM Attacks with Bettercap

OWASP Cuttack

# OWASP Cuttack

SPONSORED BY



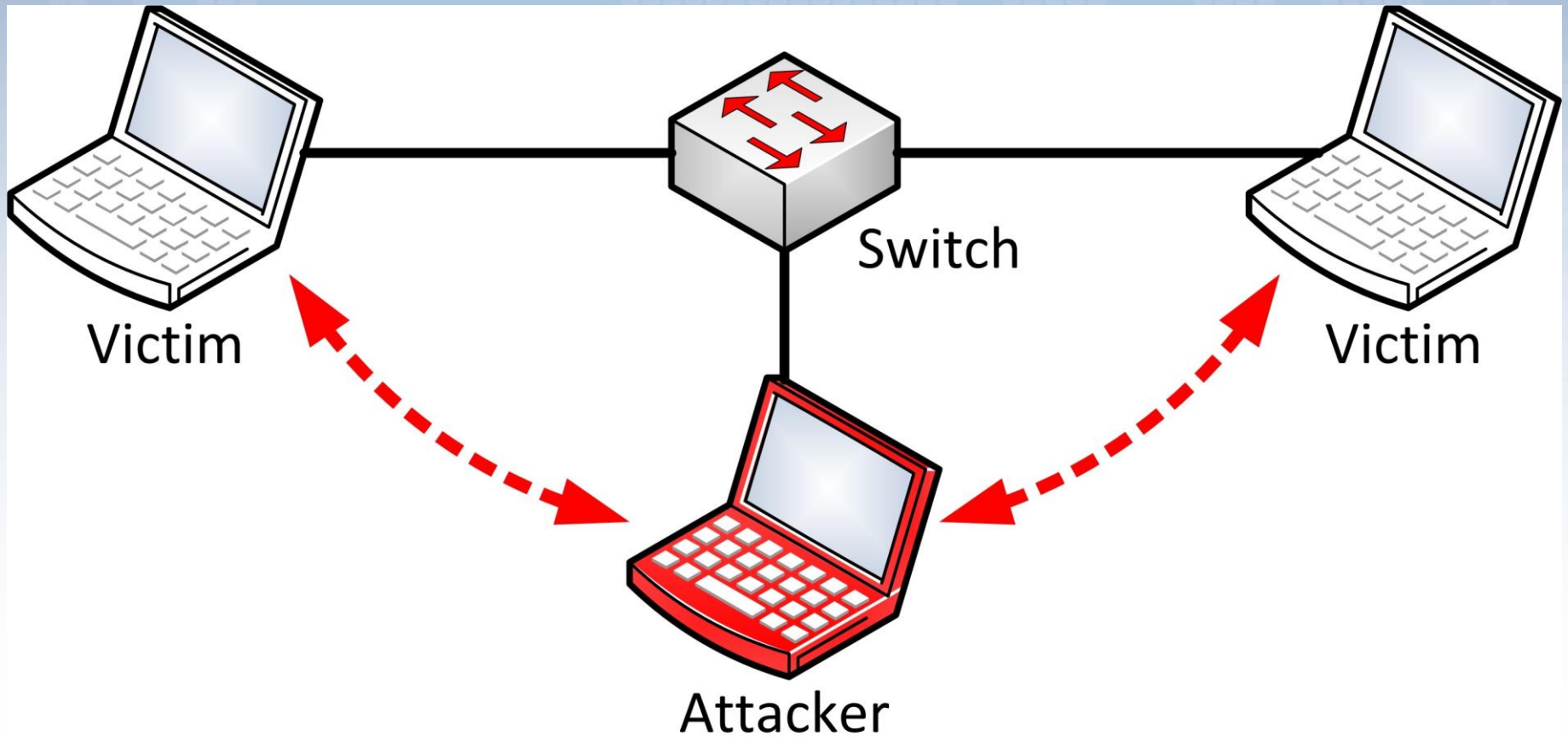
# What is OWASP ?????

- Open Web Application Security Project
- A Non Profit Organisation
- Spreading software security awareness
- Developing and maintaining various open source project on Software Security
- Defined Top 10 standard of Application security

# What is a MITM attack

- In the context of Information Security, a **Man-in-the-Middle(MITM)** attack is one where the attackers eavesdrop on the communication between two targets. The attack takes place in between two legitimately communicating hosts, allowing the attacker to “listen” to a conversation they should normally not be able to listen to, hence the name “man-in-the-middle.”

# What is a MITM attack



# Types of MITM Attacks

- **ARP Spoofing**
- **DNS Spoofing**
- **mDNS Spoofing**
- **Rogue Access Point**

# Types of MITM Attacks(contd…..)

**ARP Spoofing:**

**ARP (Address Resolution Protocol)** is used to resolve IP addresses to physical MAC (media access control) addresses in a LAN. When a host needs to talk to a host with a given IP address, it references the ARP cache to resolve the IP address to a MAC address. If the address is not known, a request is made asking for the MAC address of the device with the IP address.

***ARP Weakness:***

Clients accept responses even if they did not send a request.

Clients trust these responses without any form of verification.

**DNS Spoofing:**

**DNS (Domain Name Server)** resolves domain names to IP addresses. When using a DNS spoofing attack, the attacker attempts to introduce corrupt DNS cache information to a host in an attempt to access another host using their domain name, such as www.onlinebanking.com. This leads to the victim sending sensitive information to a malicious host, with the belief they are sending information to a trusted source. An attacker who has already spoofed an IP address could have a much easier time spoofing DNS simply by resolving the address of a DNS server to the attacker's address.

# Types of MITM Attacks(contd…..)

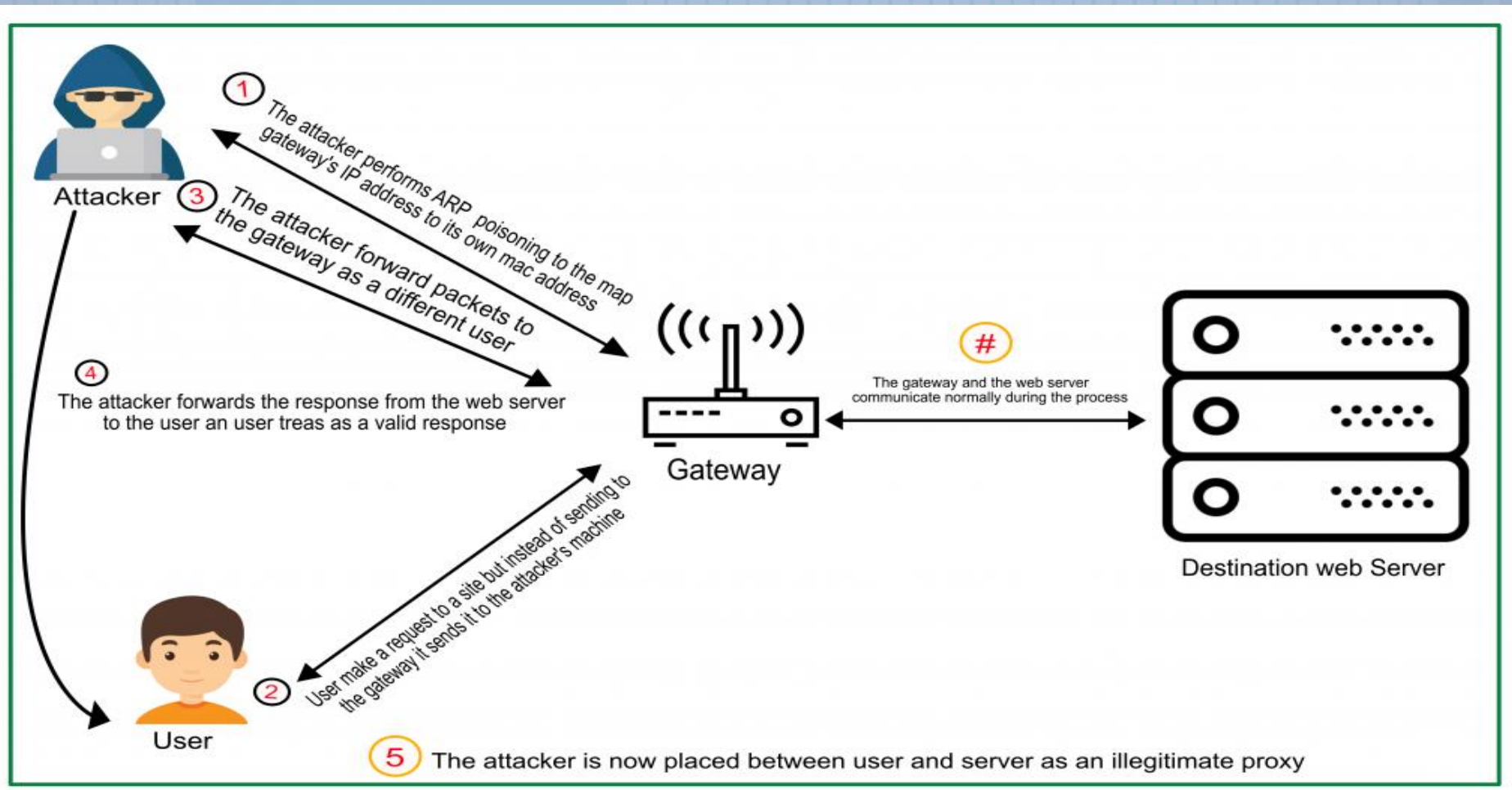
**mDNS Spoofing:**

**Multicast DNS** is similar to DNS, but it's done on a LAN using broadcast like ARP. This makes it a perfect target for spoofing attacks. The local name resolution system is supposed to make the configuration of network devices extremely simple. Users don't have to know exactly which addresses their devices should be communicating with; they let the system resolve it for them. Devices such as TVs, printers, and entertainment systems make use of this protocol since they are typically on trusted networks. When an app needs to know the address of a certain device, such as tv.local, an attacker can easily respond to that request with fake data, instructing it to resolve to an address it has control over. Since devices keep a local cache of addresses, the victim will now see the attacker's device as trusted for a duration of time.

**Rogue Access Point:**

Devices equipped with wireless cards will often try to auto connect to the access point that is emitting the strongest signal. Attackers can set up their own wireless access point and trick nearby devices to join its domain. All of the victim's network traffic can now be manipulated by the attacker. This is dangerous because the attacker does not even have to be on a trusted network to do this—the attacker simply needs a close enough physical proximity.

# Types of MITM Attacks



# MITM Attack Techniques

- **Sniffing**
- **SSL Stripping**
- **Packet Injection**
- **Session Hijacking**

# MITM Attack Techniques(contd…..)

**Sniffing**

Attackers use packet capture tools to inspect packets at a low level. Using specific wireless devices that are allowed to be put into monitoring or promiscuous mode can allow an attacker to see packets that are not intended for it to see, such as packets addressed to other hosts.

**SSL Stripping**

An attacker can also leverage their device's monitoring mode to inject malicious packets into data communication streams. The packets can blend in with valid data communication streams, appearing to be part of the communication, but malicious in nature. Packet injection usually involves first sniffing to determine how and when to craft and send packets.

**Packet Injection**

Most web applications use a login mechanism that generates a temporary session token to use for future requests to avoid requiring the user to type a password at every page. An attacker can sniff sensitive traffic to identify the session token for a user and use it to make requests as the user. The attacker does not need to spoof once he has a session token.

**Session Hijacking**

Since using HTTPS is a common safeguard against ARP or DNS spoofing, attackers use SSL stripping to intercept packets and alter their HTTPS-based address requests to go to their HTTP equivalent endpoint, forcing the host to make requests to the server unencrypted. Sensitive information can be leaked in plain text.

# What is BetterCap ?

BetterCAP is a powerful, flexible and portable tool created to perform various types of **MITM** attacks against a network, manipulate **HTTP**, **HTTPS** and **TCP** traffic in realtime, sniff for credentials and much more.

# Demo

# Counter Measures

- ARP Tables
- XArp
- Wireshark

# References


- https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/
- https://en.wikipedia.org/wiki/Address_Resolution_Protocol
- https://www.bettercap.org/legacy/
- http://www.xarp.net/


# Q & A

# Thank You