Network Security Lab Activity: Man in the Middle (MitM) attacks

Gabriele Gemmi
Lorenzo Brugnera

University of Trento

Wednesday, 18 April 2018

Outline

- How to mount a MitM attack
  - ARP Spoofing
  - DHCP (DHCPv6) poisoning
  - Evil Twin
- Attacks that can be mounted after the MitM
  - DNS Spoofing
  - HTTP Interception
  - SSL Stripping
  - HSTS Bypass

What is a MitM attack?

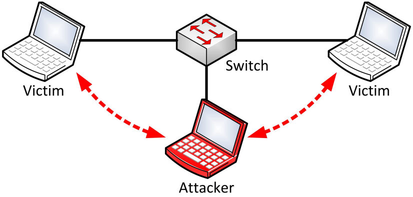


Diagram of a MitM attack

Requisites

- The attacker must be near the victim (in the same local network)

What is a MitM attack?

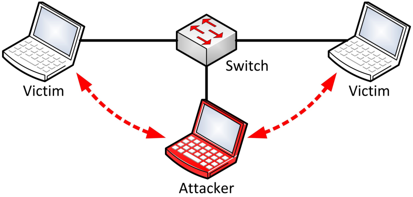


Diagram of a MitM attack

How to mount this attack

- The attacker must be physically connected between the victim and the rest of the network

or

- The attacker must hijack the traffic from the victim to himself

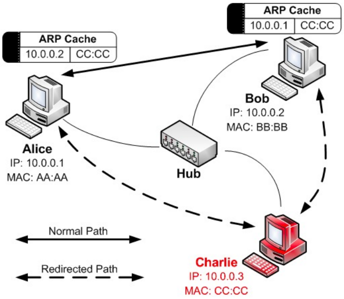
Network layer attacks

- ARP poisoning
- DHCP (DHCPv6) poisoning
- Evil Twin

ARP Poisoning

How it works

-
-



ARP Spoofing attack diagram

ARP Poisoning

How to prevent it?

ARP Poisoning

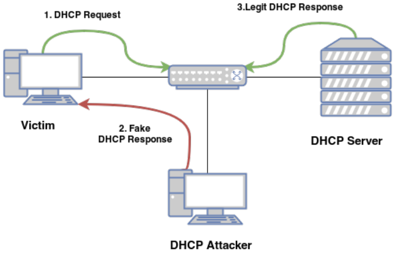
How to prevent it?

-
-

DHCP (DHCPv6) poisoning

How it works

- The attacker sets-up a rogue DHCP server
- Each time a victim sends a DHCP request the rogue server answers with a forged response
- The response contains a malicious default gateway to perform the MitM attack



DHCP poisoning attack diagram

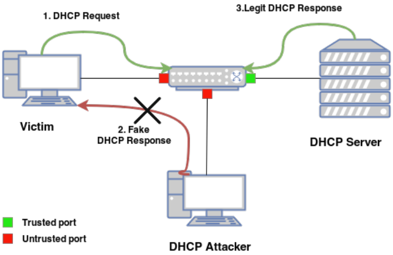
DHCP (DHCPv6) poisoning

How to prevent it?

DHCP (DHCPv6) poisoning

How to prevent it?

- A smart switch can be configured to allow DHCP response only on certain trusted ports

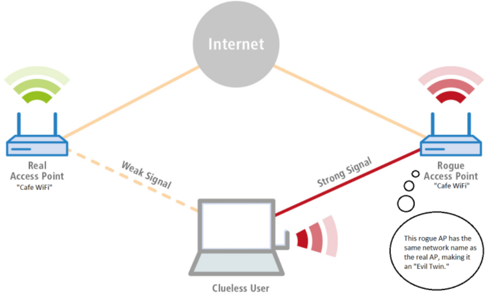


DHCP snooping diagram

Evil Twin

How it works

- The attacker sets-up a rogue Wi-Fi Access Point with the same ESSID as the target network.
- The victim must receive the rogue AP with a stronger signal than the legit one.



Evil Twin attack diagram

Evil Twin

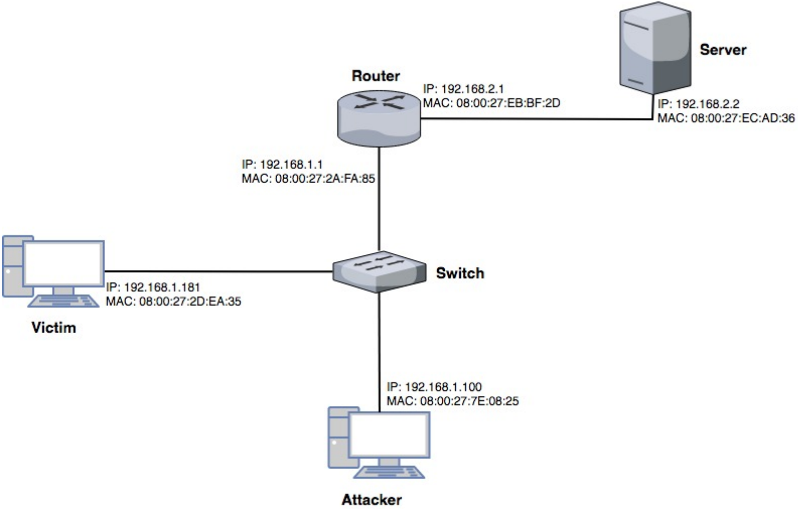
How to prevent it?

Evil Twin

How to prevent it?

- A simple authentication (WPA) doesn't ensure the client that the AP is legit. (The attacker just need to discover the key)
- The client must authenticate the AP (802.1x) and verify its legitimacy

Network Topology



Topology of the VMs network

Tools

This is a list of tools we will be using in this lab, in the next slides the usage and the purpose will be explained

- arpspoof
- wireshark
- dnsspoof
- sslstrip
- sslstrip2
- dns2proxy

Tips and Tricks

Useful infos

- Type `sudo` before every command, the password is “netsec”

To do after every exercise

- Flush the DNS cache: `systemd-resolve --flush-cache`
- Clean the iptables chains `iptables -t <chain name> -F`
- Clean the browser cache “CTRL+SHIFT+CANC“

MitM Network attack

- To mount the following attacks you can use any of the attacks we illustrated you
- Since you already know how to mount it and due to its simplicity, we wll be using ARP spoofing

- You can use either ettercap or this simple command line tool
```
arpspoof -t <victim ip> -r <router ip>
```

HTTP Interception

How it works

- Using wireshark it's possible to capture all the traffic that flows between the victim and the router
- Sensitive information can be sniffed by the attacker

HTTP Interception

Exercise

- Mount an MitM network attack
- Open a browser and navigate to “http://gugol.it”
- Sniff the HTTP traffic exchanged between the victim and the server

HTTP Interception

How to prevent?

HTTP Interception

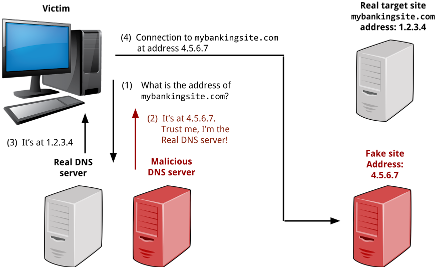
How to prevent?

- An encrypted channel can preserve the confidentiality
    - SSL/TLS
    - VPN

DNS Spoofing

How it works

- DNS messages are exchanged in clear using the UDP protocol on port 53
- An attacker who is *in the middle* can manipulate the DNS responses



Victim

(4) Connection to `mybankingsite.com` at address 4.5.6.7

(1) What is the address of `mybankingsite.com`?

(2) It's at 4.5.6.7. Trust me, I'm the Real DNS server!

(3) It's at 1.2.3.4

Real DNS server

Malicious DNS server

Real target site
`mybankingsite.com`
address: 1.2.3.4

Fake site
Address:
4.5.6.7

Diagram of the attack

DNS Spoofing

In practice

- dnsspoof forges replies to arbitrary DNS queries on the LAN

Usage

```
dnsspoof [-i interface] [-f hostsfile]
```

The hostfile contains the record associated with the A response for example:

```
www.google.it     192.168.1.1
www.facebook.com  192.168.1.1
```

DNS Spoofing

Exercise

- There's a malicious webserver running on the attcker VM
- Create a proper hostsfile to spoof requests for `www.gugol.it` pointing to the malicious webserver
- Mount a MitM attack
- Setup `dnsspoof` to answer to the DNS query of the victim
- Navigate to `www.gugol.it` to verify that the attacks has succeeded

DNS Spoofing

Exercise

- There's a malicious webserver running on the attcker VM
- Create a proper hostsfile to spoof requests for `www.gugol.it` pointing to the malicious webserver
- Mount a MitM attack
- Setup `dnsspoof` to answer to the DNS query of the victim
- Navigate to `www.gugol.it` to verify that the attacks has succeeded
- Block the DNS response from the legit server using `iptables`

DNS Spoofing

Exercise

- There's a malicious webserver running on the attcker VM
- Create a proper hostsfile to spoof requests for `www.gugol.it` pointing to the malicious webserver
- Mount a MitM attack
- Setup `dnsspoof` to answer to the DNS query of the victim
- Navigate to `www.gugol.it` to verify that the attacks has succeeded
- Block the DNS response from the legit server using `iptables`

```
iptables -A FORWARD -s <victim ip> -p udp --dport
<dns port> -j DROP
```

DNS Spoofing

How to prevent?

DNS Spoofing

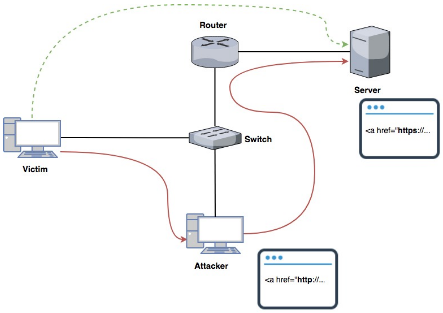
How to prevent?

- Cached responses cannot be spoofed
- DNSSec guarantees integrity of the records by using digital signature

SSL Stripping

How it works

- An attacker *in the middle* manipulates the HTTP responses
- Every `https://` url in the response gets downgraded to `http://`



SSL Stripping attack diagram

SSL Stripping

In practice

- sslstrip is an HTTP proxy that manipulates the messages to perform the attack
- The http traffic flowing through the attacker must be redirected to sslstrip

Usage

```
sslstrip -l <port>
```

SSL Stripping

Exercise

- There's a malicious webserver running on the attcker VM.
- Mount a MitM attack
- Setup `sslstrip` to manipulate the HTTP traffic
- Using `iptables` redirect the traffic from the port 80 to the port that sslstrip is using
- Navigate to `www.gugol.it` and click to the link.
- Verify that the connection with the website is unsecure

SSL Stripping

Exercise

- There's a malicious webserver running on the attcker VM.
- Mount a MitM attack
- Setup `sslstrip` to manipulate the HTTP traffic
- Using `iptables` redirect the traffic from the port 80 to the port that sslstrip is using
- Navigate to `www.gugol.it` and click to the link.
- Verify that the connection with the website is unsecure

```
iptables -t nat -A PREROUTING -p tcp
--destination-port <web server port> -J REDIRECT
--to-port <sslstrip port>
```

SSL Stripping

How to prevent?

HSTS Bypass

How it works

HSTS Bypass

In practice

HSTS Bypass

Exercise

HSTS Bypass

How to prevent?