# Security Testing and Cyber-Security: Use Case Simulated Man in The Middle Attack and Prevention

## Problem:

## Solution:

Tools are used in Man-In-The\_Middle Attack:

### 1. MAC Address Changer

Media Access Control (MAC Address) is a permanent physical and unique address assigned to network interfaces by the device manufacturer. Whether the target has a wireless card or an Ethernet card each one of these network cards comes with a specific address that is unique to this card. Therefore, there are no two devices within the target’s network(or in the world) that would have the same Mac address. This address will always be the same for this specific device even if the target unplugs it from one computer and connect it to another.

While the Mac address is used within the network to identify devices and transfer data between devices, the IP address is used on the Internet to identify computers and communicate between devices on the Internet. Therefore, each piece of data or packet that is sent within the network contains a source Mac and a destination Mac. This packet would flow from the source Mac to the destination Mac because this is how it identifies devices within its network.

Mac address is often used by filters to prevent or allow devices to connect to networks and do specific tasks on the network. Therefore, changing the target’s MAC address to another device's MAC address will allow hackers to impersonate this device and allow them to do things that they are not allowed to do. Also, they'll be able to bypass filters or connect to networks that only specific devices with specific Mac addresses can connect to, and hide their identity

Technology:

A basic MAC Address Changer can be created by Python and Linux commands. Depending on the hacking tools and interface that the hacker is going to use, the required packages are different. Since I am using Kali Linux and Python, the required Python packages are ” subprocess”, ”optparse”, and “re”.

### 2. Network Scanner

Information gathering is one of the most important steps when it comes to hacking or penetration testing. Hackers can't really gain access to a system if they don't have enough information about it. For our attack, the plan is to connect to the private network, and one or more of the devices connected to this network is our target. For us to hack into that target first we need to discover all the connected clients to this network, get their MAC addresses, and their IP addresses. Then from there try to gather more information or run some attacks to gain access to our target.

There are several programs (Net discover or Nmap) that do this job well. Moreover, Python also has a Nmap package that was rebuilt and can be used like the Nmap application. However, I decided to write my own network scanner to enable automation and more code-control. My Network Scanner is very similar to Net Discover (a scanner that comes with Kali Linux) and shows us all the connected devices connected to the same network plus their IP addresses and their Mac address.

As we have the returned data (IP addresses and Mac addresses), we can use it to gather information on the next attack. We also can measure the security level of each devices on the network to create suitable plan

### 3. ARP Spoofer (ARP Cache Poisoning)

### 4. Packet Sniffer

### 5. DNS Spoofer (DNS Cache Poisoning)

### 6. File Interceptor

### 1. Enviroment:

- Perform Man-In-The-Middle (MITM) attack on a virtual private network

- Etablished by using VM Ware

- Hardware:

- PC 64 bits, Intel Core i7 10th Gen, 36 GB of ram

- Software:

- Microsoft Window 10 (host)

- VM Ware Sphere (or free version)

- Kali Linux (free)

## Results:

## Conclusion/Future work

There are monitoring

## IV. Reference

- [IEEE: Advance Technology for Humanity](https://www.ieee.org/) [1]

- [ISO 9000-3: Quality management and quality assurance standards](https://www.iso.org/standard/26364.html) [2]

- [SWEBOK V3.0: Guide to the Software Engineering Body of Knowledge](https://ieeecs-media.computer.org/media/education/swebok/swebok-v3.pdf) [3]

- [Tutorial Point: STLC Tutorial](https://www.tutorialspoint.com/stlc/index.htm) [4]

- [Software Testing | Security Testing](https://www.geeksforgeeks.org/software-testing-security-testing/?ref=lbp) [5]

- [Security Testing: Types, Tools, and Best Practices](https://www.neuralegion.com/blog/security-testing/) [6]

- [API Security: The Complete Guide](https://www.neuralegion.com/blog/api-security/) [7]

- [STLC (Software Testing Life Cycle) Phases, Entry, Exit Criteria (guru99.com)](https://www.guru99.com/software-testing-life-cycle.html) [8]

- Fink, G. & Bishop, M. "Property-Based Testing: A New Approach to Testing for Assurance." ACM SIGSOFT Software Engineering Notes 22, 4 (July 1997): 74-80.[9]

- McGraw, Gary & Potter, Bruce. "Software Security Testing." IEEE Security and Privacy 2, 5 (Sept.-Oct. 2004): 81-85. [10a]

- McGraw, Gary. "Application Security Testing Tools: Worth the Money?" Network Magazine, November 1, 2004. (2004). [10b]

- [Kali Linux](https://www.kali.org/?msclkid=ccbd3c3faa2511ecbe541363c15a4582) [11]

- [Python Scapy Package](https://pypi.org/project/scapy/?msclkid=33343ba2aa2611eca8b9c3abfd8b35c1) [12]

- [Truc Huynh: Ethical Hacking Using Python](https://github.com/jackyhuynh/ethical-hacking-using-python) [13]

- [Udemy: Learn Python and Ethical Hacking from Scratch](https://www.udemy.com/course/learn-python-and-ethical-hacking-from-scratch/learn/lecture/10800892#overview) [14]