IRSTI 50.37.23

N. Abdinurova[1], D. Akmyrza[2], A. Mirash[3]
[1,2,3]Suleyman Demirel University, Kaskelen, Kazakhstan

# MITM. WHAT IS IT, HOW TO PROTECT YOURSELF AND IMPLEMENTATION FOR INSTRUCTIONAL USE

**Abstract.** This is an attack in which a cybercriminal intercepts data while it is being transmitted. Man-in-the-Middle attacks are a common type of cybersecurity attack that allows attackers to eavesdrop on communications between two targets. This article discusses how people can protect themselves, what they need to know, and how an attacker performs a MITM attack using the open-source tools bettercap and net-creds in kali Linux. Buttercup is a network attack and monitoring program that can perform ARP spoofing and sniffing. Net-creds is a sniffing tool available by cloning on Github. This article attempts to implement this attack for instructional use.

**Keywords:** Man-In-the-Middle (MITM), bettercap, net-creds, kali-Linux, ARP spoofing, sniffing.

***

Аңдатпа. Бұл киберқылмыскер деректерді беру кезінде ұстап алатын шабуыл. «Man-in-the-Middle» шабуылдары-киберқауіпсіздікке шабуыл жасаудың кең таралған түрі, бұл шабуылдаушыларға екі нысан арасындағы хабарламаларды тыңдауға мүмкіндік береді. Бұл мақалада адамдар өздерін қалай қорғауға болатындығы, нені білу керек және шабуылдаушы Kali-Linux-тағы bettercap және net-creds ашық бастапқы құралдарын қолдана отырып MITM шабуылын қалай жүзеге асыратыны қарастырылады. Buttercup-бұл ARP трафигін ауыстыру және анализатор жасай алатын желілік шабуыл және бақылау бағдарламасы. Net-creds-бұл GitHub-та клондау арқылы қол жетімді желілік трафикті ұстап алу және талдау құралы. Бұл мақалада осы шабуылды оқу мақсатында қолдануға әрекет жасалды.

**Түйін сөздер:** Man-in-the-Middle (MITM), ettercap, net-creds, kali-Linux, ARP ауыстыру, трафик Анализаторы.

***

**Аннотация.** Это атака, при которой киберпреступник перехватывает данные во время их передачи. Атаки «Man-in-the-Middle» - это распространенный тип атаки на кибербезопасность, который позволяет злоумышленникам прослушивать сообщения между двумя целями. В этой статье обсуждается, как люди могут защитить себя, что им нужно знать, и как злоумышленник выполняет атаку MITM с использованием

инструментов с открытым исходным кодом bettercap и net-creds в kali-Linux. Buttercup - это программа для сетевой атаки и мониторинга, которая может выполнять подмену и анализатор трафика ARP. Net-creds - это инструмент для перехвата и анализа сетевого трафика, доступный путем клонирования на Github. В этой статье предпринята попытка реализовать эту атаку для использования в учебных целях.

**Ключевые слова:** Man-in-the-Middle (MITM), bettercap, net-creds, kali-Linux, подмена ARP, Анализатор трафика.

*I. Introduction*

Cyber-attacks are now a major criminal offence, as well as a hotly debated subject. A man-in-the-middle attack is a form of cyberattack in which an unauthorized third party approaches an online conversation between two users and stays unnoticed by the two parties. Individual/classified information that was only discovered by the two users is often monitored and changed by the malware that is in the middle of the assault. An outsider within the machine is exposed to a man-in-the-middle assault, which allows the outsider to enter, read, and alter sensitive knowledge without leaving any traces of coercion. This is a serious problem, and most cryptographic schemes lacking adequate authentication protection are at risk of being compromised by the malware known as "men-in-the-middle". This paper focuses on interpreting the expression "men-inthe-middle attack", avoiding such attacks, and conducting a practical experiment using common methods to both deter and monitor for mitm. The aim of this paper is to assist readers in comprehending and familiarizing themselves with the subject of a "man-in-the-middle attack".

*II. Background materials*

Man in the Middle - a form of attack in which a hacker intercepts and replaces messages sent by correspondents while the latter are completely unaware of his presence in the channel. After connecting to the counterparties' channel, the attacker tampers with the transmitting protocol, removing or distorting data. During the attachment operation, the broker is embedded in the contact chain and simulates the second side of the communication, offering a plausible-looking certificate of trust. The broker must intercept all communications between the client and the server and encrypt and decrypt them with the right secrets in order to stay undetected.

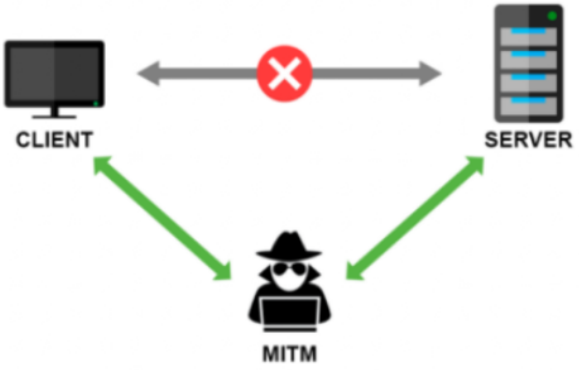



Fig. 1. An illustration of a MITM attack.

Attacks on networks that conduct financial transfers over the Internet are vulnerable to man-in-the-middle attacks. An attacker can obtain access to the user's account and perform various forms of financial fraud using this method. You must examine the server's IP address, DNS server, and server certificate to identify a man-in-the-middle threat (it should be signed by the certification authority, be revoked or recently changed, and other users on the Internet should receive the same certificate). One of the most common attacks when using the stable TLS protocol is this form of attack. The MITM attack is impossible for the client to detect, and the server almost never detects it.

ARP spoofing. ARP is a protocol that is used to communicate a device's IP address with its MAC address. In other words, it helps to determine the MAC address of a device by knowing its IP address. How ARP spoofing works. In order to get between the client and the router, thereby directing traffic through itself, the attacker needs to send false ARP responses to the client and the router. A false ARP response sent to the client will contain information that the router's IP address matches the attacker's MAC address. The false ARP response that will be sent to the router contains information that the client's IP address also matches the attacker's MAC address.

Thus, after sending false ARP responses, all traffic between the client and the router will pass through the attacker's laptop. Thus, all network user traffic will be routed through the attacker's laptop, including passwords, card numbers, and other critical information. Creating fake wifi hotspot. Most smartphones, laptops, and tablets automatically search for Wi-Fi networks and connect to them. First of all, such devices will search for networks with familiar names, such as FreeWifi or wireless. During the search, the devices send requests, the so-called probe request. An attacker can see them and create networks with registered names, or create a network with an arbitrary name, for example, with the name of the cafe where he is currently located. Moreover, an attacker can run special software that will automatically create open Wi-Fi

networks with the same names as at your home, at work, in your favorite cafes and shopping centers. A user who sees an open network with the name of a cafe will most likely connect to it, unaware that after connecting, an attacker will be able to control his connection. Running such software in a public place, the attacker will see a large number of clients connected to his fake access point in a few minutes. At the same time, most of the devices are connected automatically, without the user's knowledge.

*III. Literature review*

In IoT detection, an MITM attack is a routing protocol combined with an anomaly detection system that can identify traffic based on the probability of MITM manipulation. The presumption can be made that a delayed time gap between a source and destination implies a possible MITM by developing a protocol that provides consistent transmission time variability. In this article investigated by Hybrid Routing for Man-in-the-Middle in IoT Networks [1].

Encryption is one method of defending against MITM attacks. This will help protect users' messages from being read or altered by third parties [2].

A man-in-the-middle attack occurs when an attacker sends and potentially modifies correspondence between two parties who think they are communicating directly with each other [3].

This article uses an implementation of the MITM attack that was published in 2018 [5]. It was implemented using open source tools such as Ettercap. However, in 2021 it will not work properly as we expected, then we are going to implement it with other programs.

*IV. Methods and materials*

How personalities and companies can prevent from being attacked by mitm. As mentioned it is one of the popular attacks which needs to be handled so, it may affect individuals by getting personal information and other staff, in case of companies it may lead to remarkable problems as they can not secure information about their clients and staff. In this paragraph, it will be considered in terms of individuals and companies ways to defend themselves. Although we will give brief prevention methods which can be applied to both. Protecting "man in the middle" attacks may be a challengeable, but there are several ways to defend them from hackers. The most popular way to defend them for both parties is VPN (Virtual Private Network) which helps to ensure the secure connection and creates security for the sensitive information in the environment (local area network). It helps by usage of encryption which is called key-based to create subnet for secure connection. To make it simple it means that VPN creates a channel which is encrypted and secure for data that is transferred over the intermediate server from a device or a network. So even if hackers can see the network, it will be difficult for them to decrypt the traffic in VPN as they see only encrypted streams of traffic which is difficult for attackers to be able to find information. Despite the usage of VPN which has high network security, there are some shortcomings which can be solved by TOR. When using Tor over VPN,

you solve these drawbacks and have benefits. Tor over VPN gives better network encryption and privacy and anonymity. So, the Usage of different devices applications might involve important information about the user and by using virtual private networks or TOR, it helps to protect when connecting to public networks by adding an extra layer of protection from mitm attacks.

As mentioned above it is clear that hackers will not consider when someone uses VPN as everything is encrypted, but there might be the case when both categories have shared WiFi with some defects with encryption and other staff. From there we will consider wireless access points and different types of encryption, and making strong routers. The most common issues of each person and organisation is having a weak password in their wireless network. As weak encryption can permit hackers to brute-force into a network and can attack mitm. Thus strong encryption on wireless access points helps to defend from nearby unwanted users who are joining the network. Even if an attacker can intercept the data shared over the wireless network, it will be challengeable to decrypt. In addition, strong encryption, especially when backed up with a strong password of at least 12 characters, guarantee that users themselves connect to the network. Despite having encryption, it is also important to secure from malware as they can be used for gaining access. Currently, it is found that many attackers use malware in order to break or bypass encryption. To prevent this it is important for both company and person to install good anti-virus which can help to get rid of malware on the system. Also current anti-virus can be used to provide additional network security, which makes it even safer. So it is important for both of them to secure from malware and to not install it as malware applications might run automatically.

The second popular way to prevent mitm attacks for companies is keeping systems up-to-date and to have strong firewalls and protocols to prevent unauthorized access to their network. Using a firewall is also a secure way to protect browsing data. However, MiTM hackers have a popular way to gain access to servers which is through the use of outdated software and firmware on the system. By having a policy that regularly updates the system can prevent potential MiTM hotspots. The main reason making up-to-date is modern systems have all the current security measurements, which makes them challenging for hackers to access. For the company it should be better if routers, devices, and other hardware be up-to-date as single failure can put the entire network in danger.

For many companies and organizations, the best way to defend against MiTm attacks is to implement authentication certificates or Public Key Pair Based Authentication. There are huge differences between them and we will consider both of them. Either Certification authorities (CAs) and Public Key Pair Based Authentication can be used to prevent MitM attacks. The former can be used to authenticate users on the network. As stated by the certificate-based authentication system, any user who would like to work

on the network must have a concrete certificate to access it. It is more flexible as employees only need to install certificates for usage of the Internet. The letter one like RSA can be used in different layers to help assure that the user transferring data is actually the thing that is transferring with. Both of them can be used to prevent MITM attacks as both are considered to be used for the company as they will ensure that only in a separate internal network can only be used by employees as hackers will have difficulties in gaining access to the company server.

*V. Data and results*

Before launching a MITM attack, install the programs according to this instruction. Installations program for MITM [6].

The following commands should be entered in the terminal of the attacker machine.

1) *sudo bettercap -iface [interface].* Here we are starting the program and specifying the interface of the Wi-Fi adapter or Ethernet, if you are not on a Wi-Fi network, but on a wire.

2) *net.probe on* Enables the search for devices on the network.

3) *ticker on* Constantly update this list

4) *net.show* Shows a list of found devices

| Name | Vendor | Sent | Recvd | Seen |
|---|---|---|---|---|
| eth0 | PCS Computer Systems GmbH | 0 B | 0 B | 14:17:00 |
| | Huawei Technologies Co.,Ltd | 1.4 kB | 870 B | **14:17:22** |
| | Samsung Electronics Co.,Ltd | 240 B | 184 B | **14:17:22** |
| DESKTOP-OF7D08N | Intel Corporate | 68 kB | 3.5 MB | **14:17:21** |
| | | 70 B | 92 B | **14:17:16** |
| | | 120 B | 92 B | **14:17:16** |
| | Samsung Electronics Co.,Ltd | 0 B | 92 B | **14:17:17** |
| | | 1.3 kB | 92 B | **14:17:16** |

5) set arp.spoof.targets [ip] Sets the target of ARP spoofing.

If you don't know the IP of the device on the local network, you will need nmap to find the device you need.

6) arp.spoof on Enable ARP spoofing

7) set net.sniff.verbose false with this command there will be fewer messages in the console when sniffing.

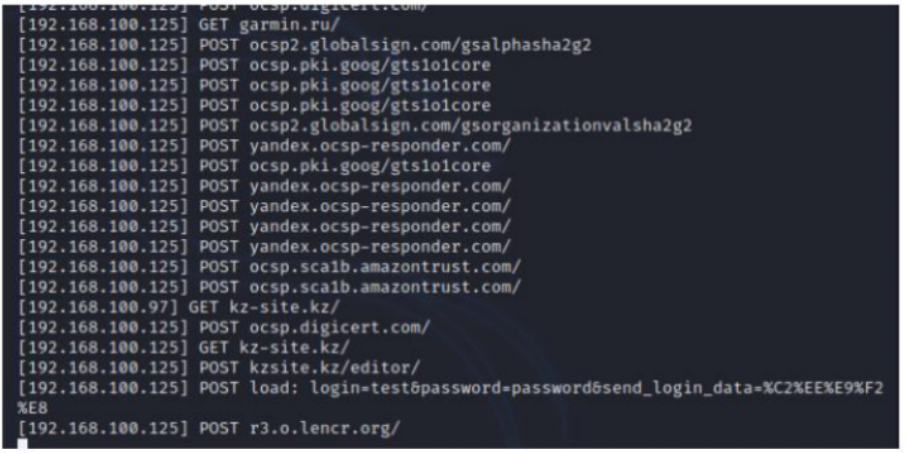
8) set http.proxy.sslstrip true enable SSLStrip

9) http.proxy on Enable proxy server for SSLStrip

10) net.sniff on Enable a sniffing

After running all of this command we should enter another terminal and go to net-creds directory which we have cloned [7].

And run the *net-creds.py* file only with second version of python. *sudo python2 net-creds.py.* After running net-creds this will display the sites visited by the person, as well as the usernames/passwords that were intercepted.




Above, you can see the username and password that we captured.

*VI. Conclusion*

Cybersecurity is becoming increasingly important. This is a requirement for every person to be aware of attacks and observe certain security measures while online. Privacy and data protection have become the needs of today. Sensitive data, such as the user name and password, can be easily sniffed if the user does not observe the principle of security when working on the Internet. Above, in practice it was shown that the user credentials are easily sniffed using the bettercap, netcred tools. Even if the user went to a web page with the https protocol, it was easily done. This is done because the site is poorly configured with HSTS (HTTP Strict Transport Security). These days, users should be aware of best practices to protect against popular cyber attacks.

## References

1 Hybrid Routing for Man-in-the-Middle (MITM) Attack Detection in IoT Networks https://www.researchgate.net/publication/340971393 Hybrid Routing for Man-in-the-Middle MITM Attack Detection in IoT Networks.

2 Man-in-the-middle-attack: understanding in simple words. URL: https://jurnal.ar-raniry.ac.id/index.php/cyberspace/article/view/3453/27.

3 Fact Sheet: Machine-in-the-Middle Attacks What are they, and how can we prevent them? URL: https://www.internetsociety.org/resources/doc/2020/fact-sheet-man-in-the-middle-attacks/.

4 EECDH to prevent MITM attack in cloud computing. URL: https://www.researchgate.net/publication/336793622_EECDH_to_prevent_MITM_attack_in_cloud_computing.

5 Real-World Man-in-the-Middle (MITM) Attack Implementation Using Open Source Tools for Instructional Use. URL:

https://ieeexplore.ieee.org/document/8500082.
6 Installation instructions. URL:
https://github.com/darkhanakmyrza/MITM/blob/master/prep.txt.
7 Open source tool net-creds.URL:
https://github.com/DanMcInerney/net-creds.git.