WJAETS

World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266

Cross Ref DOI: 10.30574/wjaets

Journal homepage: https://wjaets.com/

(Review Article)

Check for updates

Man-in-the-Middle (MitM) Attacks: Techniques and defenses

Bogdan Barchuk *

Independent researcher.

World Journal of Advanced Engineering Technology and Sciences, 2024, 13(02), 919-933

Publication history: Received on 17 November 2024; revised on 28 December 2024; accepted on 30 December 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.13.2.0650

Abstract

MitM attacks pose a significant risk when unauthorized third parties grab and control the exchanged communications between different parties unnoticed. It describes the main ways a MitM attack can take place, and why knowing about passive and active approaches are crucial. Through examining how successful Man-in-the-Middle attacks are carried out, including reviewing networks, guessing passwords, and exploiting network protocols, the study points to the many and complicated ways cyber-attacks can happen. To help understand the process of launching an attack, various tools, such as Wireshark, Aircrack-ng, Hashcat, and Airgeddon, are explained. The article continues with strategies that hackers use to intercept and analyze traffic as well as to grab passwords for these types of attacks. Techniques and ideas such as encryption, monitoring networks, and preventing social engineering are studied as part of the review. Above all, this article aims to explain MitM threats further and recommend ways that companies can defend their networks in the current digital age.

Keywords: Man-in-the-Middle; Wireless Security; Network Monitoring; Password Cracking; ARP Spoofing; Incident Response

1. Introduction

MitM attacks are now a major threat in cybersecurity, as they can steal and change information being passed between two parties without anyone noticing. Because of these attacks, the confidentiality and integrity of data on networks, especially SCADA systems, can be put at risk. As more devices are connected to the Internet and the IoT, attackers can now target a larger surface area with MitM attacks. A mitigation-in-the-middle attack in industrial control systems can lead to major issues and damage, making it necessary to have better security measures in place (Deb et al., 2020). More importantly, as attacks have evolved from listening in to attacking protocols, it proves that attackers are adjustable and tests the importance of continuous improvement in security and defense. Since wireless, cloud, and mobile services are used more often, attackers now exploit the vulnerabilities in identity verification and coding of data during transmission. These problems can be handled by understanding the attack methods, how they operate, and any weaknesses that help make a MitM scenario possible. By studying previous attacks and defenses, researchers and practitioners can design strategies ahead of time to prevent and address these threats, making sure networking in different environments stays strong (Sharma et al., 2022).

1.1. Overview

In a MitM attack, an assailant acts as an intermediary between two communicating parties, tricking them into following the attacker's instructions. Attackers can perform these actions by sniffing network packets, hijacking a session, or exploiting network protocols, all to break the security of communications (Mallik, 2019). There are attackers who aim to attack public Wi-Fi and those who are much more advanced, seeking important data or making it hard for operations to run as usual. The main targets in these attacks are usually to get someone's passwords, gain entry without permission,

[*] Corresponding author: Bogdan Barchuk

corrupt data, and keep an eye on activities. The networks most at risk from MitM attacks are wireless LANs, public hotspots, and systems with poor protection on their cables. They take advantage of weak connections, inadequate security, and personal careless moves to become part of conversations. To make good defense plans, it is necessary to identify the different attackers and what drives them to act. Also, understanding all kinds of impacted networks and attack techniques helps discover possible threats and improve the security of your network. The overview introduces the basics of MitM attacks and their surroundings so that later, we can cover the more complex aspects and methods to avoid them (Mallik et al., 2019).

1.2. Problem Statement

Catching and deflecting MitM attacks is consistently difficult in cybersecurity because of how invisible they tend to be. Typically, attackers hide in between parties having a conversation, so it is often hard to spot them unless you have the right monitoring equipment. Today's computer networks are so complicated and come in so many forms like wired, wireless, and hybrid, that defending them becomes more difficult. Although encryption and authentication add some level of defense, attackers manage to find flaws or find a way around them. Also, when we use unsecured Wi-Fi, it becomes very easy for an attacker to launch MitM attacks. It is important to use strong technology as well as educate users and change their habits to keep away these attacks. False signals from detection machineries or their failure to catch subtle traces might result in the problem not being noticed quickly. Similarly, using social engineering, changing network protocols, and malware together allows attacks to become more complex and tougher to detect. This clearly shows the importance of having all-round defense structures that can react instantly to protect against breaches in sensitive communications.

1.3. Objectives

The purpose of this research is to review the major methods used in Man-in-the-Middle (MitM) attacks to find out how attackers are able to break into and exploit network connections. I need to learn about the various tools and ways attackers can grab, change, or take data. It is also vital to map out the standard methods used by attackers to carry out a successful Man-in-the-Middle attack. Mapping these supply chains allows the study to discover the most important places to focus its security efforts. Also, the research aims to observe and assess modern precautions and detection methods to find out how they work in different network setups. Both technical methods such as encryption and analysis of traffic, as well as teaching users and watching the network, will be included. In the end, the purpose of the study is to suggest useful steps and strategies that can guide organizations and cyber experts in erecting solid security systems to guard against MitM threats on their networks.

1.4. Scope and Significance

This research mainly addresses MitM attacks happening in wireless and local area networks because such attacks are most likely to intercept and alter data traffic. Since wireless networks rely on broadcast communication, they have their own weaknesses that attackers can access from a distance without being there physically. Local networks are also vulnerable inside organizations, as problems from inside the organization or unsafe devices can result in attacks. The area of focus should be on how these attacks harm privacy, as private or company details could be exposed through interception. In addition, the study looks at how such security issues can negatively impact a company, such as by interrupting normal work, causing data leaks, and damaging public trust. The research singles out these types of networks to show where attacks through MitM are more successful in practice. It is significant because it makes people aware of them and helps defend against such attacks.

2. Literature review

2.1. Understanding the Key Concepts of Man-in-the-Middle Attacks

An attacker in a MitM attack can intercept and change messages that are transferred between two parties. To capture the right network packets, the attacker must ensure the correct network interface is used on their machine. You can see this process in Image 1, as the Wireshark Network Analyzer gives you access to Wi-Fi, Ethernet, and virtual adapters. Selecting the right interface, and one attached to the target network, is very important for monitoring and capturing packets.

Usually, after selecting the right interface, the attacker turns on promiscuous or monitoring mode to receive all packets, no matter if they are directed to them or not. This makes surveillance efficient, as the attacker can listen to all network communications openly without interacting. However, in more serious MitM cases, hackers can abuse the network's hardware or protocols to steer or change the flow of data.

Whether packet interception is possible depends a lot on the routers, switches, and hubs used in the network. Unlike switches, hubs broadcast each packet to all connected devices, making it easier for someone to see the data with a passive sniffer. Attackers may find and abuse security holes in routers, or use ARP spoofing to change flow of traffic, allowing them to intercept and modify it (Cherian and Varma, 2022).

It is key to tell apart passive from active Man in the Middle attacks. In passive attacks, confidential data is quietly captured, but in active attacks, information is either uploaded or changed, which might lead to disturbances or theft of data (Bloch, Chatterjee, and Dutta, 2023). Having a clear idea of these theories supports putting in place effective ways to catch and stop these types of attacks.

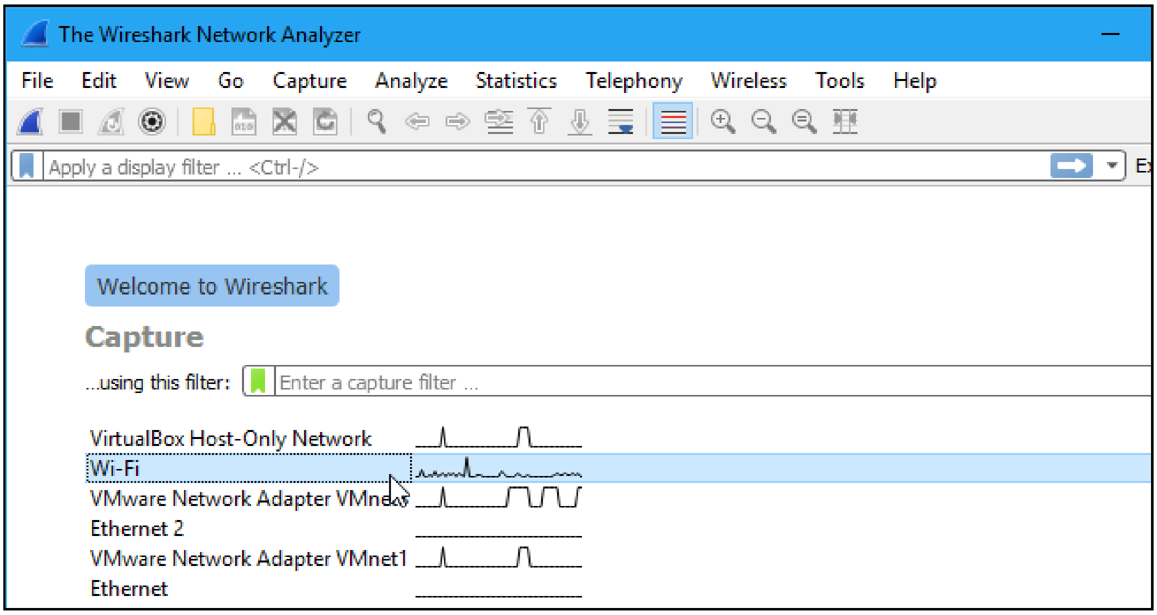

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
VirtualBox Host-Only Network
Wi-Fi
VMware Network Adapter VMnet8
Ethernet 2
VMware Network Adapter VMnet1
Ethernet

Figure 1 Wireshark Network Analyzer interface showing available network adapters for packet capture

2.2. Exploring Wireless Network Auditing and Different Entry Techniques

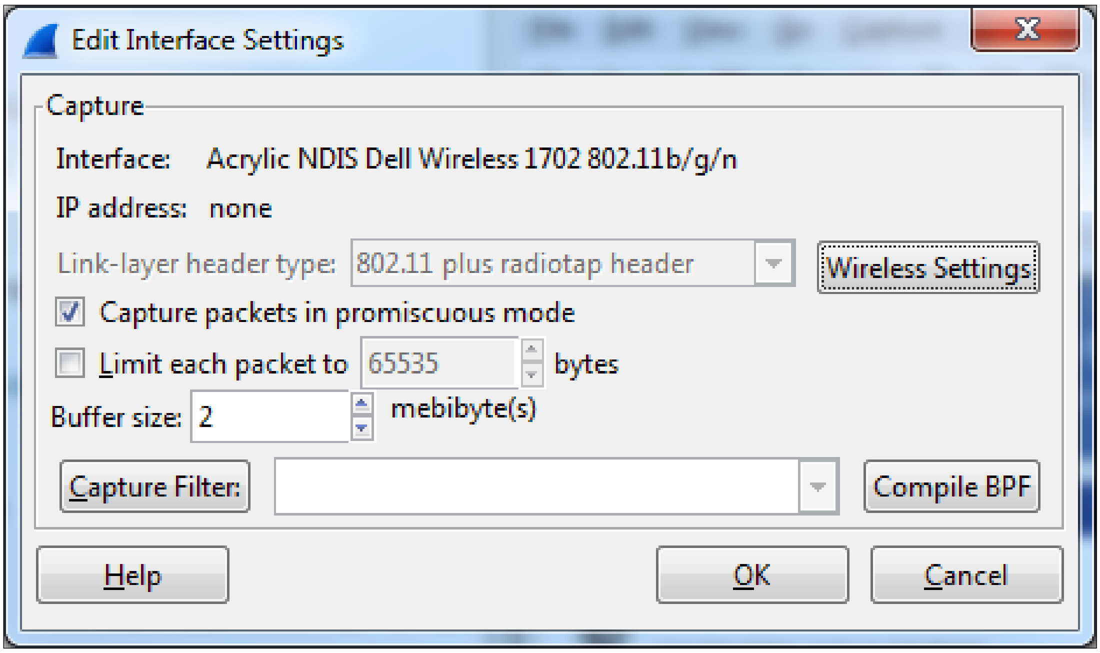
Proactive wireless network security is possible by using features which allow for intercepting and studying all traffic, which requires using monitoring or promiscuous settings for the wireless network interface. As you can see in Image 2, setting "Capture packets in promiscuous mode" on a wireless adapter means the device can pick up all nearby packets, no matter if they are meant for it. This helps gather handshake packets and different network data important for auditing wireless security and running penetration tests.

Social engineering, gaining physical access, and weaknesses in the protocol can all lead to wireless networks being attacked. Many cyberattacks involve social engineering, with attackers convincing victims to hand over their login details or link to unsafe internet sites. Hackers can gain access to the network by coming into contact with routing hardware or cables (Nazir et al., 2021).

It is common for brute force attacks on WPA/WPA2 handshakes, detected using monitoring mode in wireless networks, to use weak passwords or misconfigurations. The wireless interface on tools must work in promiscuous mode to fully make use of the data captured (Rajadurai and Gandhi, 2020).

The functions mentioned are generally brought together in wire release toolkits for easy handling of attacks including dictionary, capture of initial handshake, and WPS exploits. It is very important to configure the network adapter as shown in Image 2 for wireless auditing to be successful.

Remember, adopting promiscuous mode on your wireless adapter along with knowing the risks makes it easier to analyze and improve wireless network security (Nazir et al., 2021; Rajadurai and Gandhi, 2020).



Edit Interface Settings

Capture

Interface: Acrylic NDIS Dell Wireless 1702 802.11b/g/n

IP address: none

Link-layer header type: 802.11 plus radiotap header

☑ Capture packets in promiscuous mode

□ Limit each packet to 65535 bytes

Buffer size: 2 mebibyte(s)

Capture Filter:

Figure 2 Edit Interface Settings window demonstrating enabling promiscuous mode for comprehensive packet capture

2.3. Ways for Attacking Wireless Networks and Using Crack Methods

Attackers use different tools made for wireless networks to exploit the encryption systems used in WPA and WEP. Shown in Image 3, the Wifislax platform is an extensive and common toolkit on Linux for auditing and securing wireless networks. It brings together a large set of tools that make it easier to attack wireless networks, mainly by aiming at cracking message exchanges, guessing passwords, and using dictionary lists.

You can choose between several software on the Wifislax WPA tools menu like Airlin, Autohsgui, and BrutusHack, which all have their role in cracking WPA. One example is Chapcrack, which breaks the MS-CHAPv2 protocol in WPA, while Fluxion helps set up Evil Twin attacks. Tools such as Pyrit and Hashcat allow for much faster brute force attacks by using both CPU and GPU power.

The ability to use these tools together in one area gives hackers flexibility to try launching different attacks, including those based on rainbow tables, general password crackers, dictionaries, or social engineering tricks. It also comes with user-friendly scripts that perform complicated attack steps, opening up the field to new users and helping the experienced run attacks in an efficient manner.

If a wireless attack is to be effective, you need to grab the important handshake data and then try to crack the password on your computer using Wifislax. You can see from Image 3 that a wide range of attack methods is used, each fitting a different vulnerability seen in wireless security systems.

All in all, Wifislax is a useful all-in-one tool that gathers important cracking and attacking tools for the purpose of auditing, testing, and regrettably attacking vulnerable wireless networks

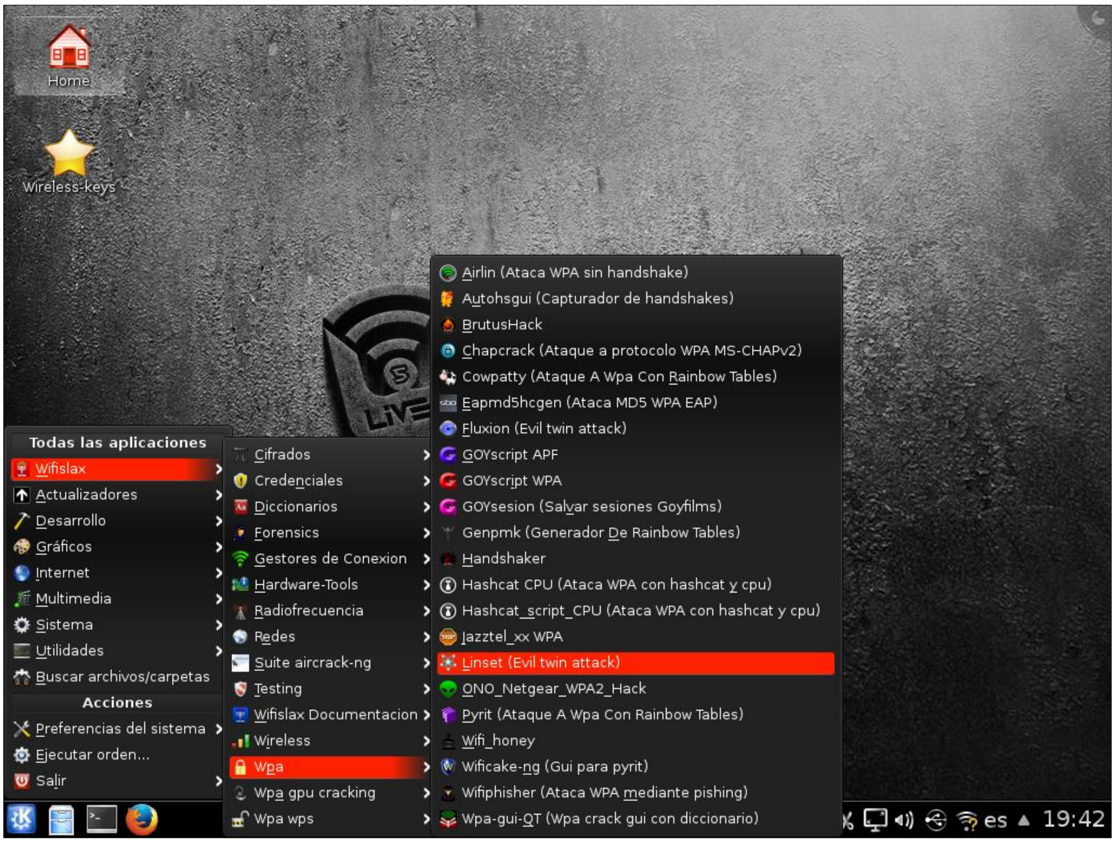

Home
Wireless-keys
Todas las aplicaciones
Wifislax
Actualizadores
Desarrollo
Gráficos
Internet
Multimedia
Sistema
Utilidades
Buscar archivos/carpetas
Acciones
Preferencias del sistema
Ejecutar orden...
Salir
Cifrados
Credenciales
Diccionarios
Forensics
Gestores de Conexion
Hardware-Tools
Radiofrecuencia
Redes
Suite aircrack-ng
Testing
Wifislax Documentacion
Wireless
Wpa
Wpa gpu cracking
Wpa wps
Airlin (Ataca WPA sin handshake)
Autohsgui (Capturador de handshakes)
BrutusHack
Chapcrack (Ataque a protocolo WPA MS-CHAPv2)
Cowpatty (Ataque A Wpa Con Rainbow Tables)
Eapmd5hcgen (Ataca MD5 WPA EAP)
Fluxion (Evil twin attack)
GOYscript APF
GOYscript WPA
GOYsesion (Salvar sesiones Goyfilms)
Genpmk (Generador De Rainbow Tables)
Handshaker
Hashcat CPU (Ataca WPA con hashcat y cpu)
Hashcat_script_CPU (Ataca WPA con hashcat y cpu)
Jazztel_xx WPA
Linset (Evil twin attack)
ONO_Netgear_WPA2_Hack
Pyrit (Ataque A Wpa Con Rainbow Tables)
Wifi_honey
Wificake-ng (Gui para pyrit)
Wifiphisher (Ataca WPA mediante pishing)
Wpa-gui-QT (Wpa crack gui con diccionario)
es
19:42

Figure 3 Wifislax WPA tools menu displaying a variety of wireless network auditing and attack utilities

2.4. Password Cracking and Hash Attacks

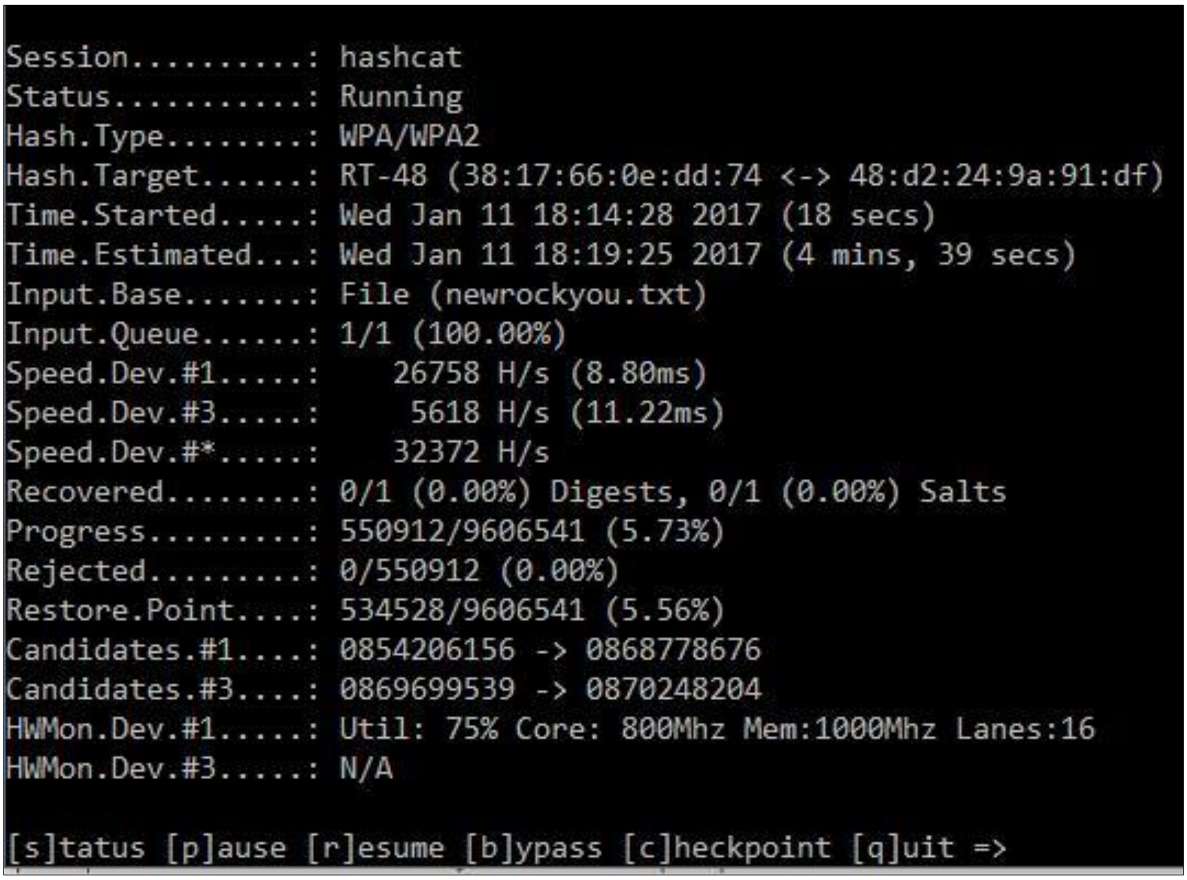
Cracking passwords helps make Man-in-the-Middle (MitM) attack chains more powerful, especially in breaking into wireless messages that are protected by encryption. Using brute force or a dictionary, Hashcat is a tool that allows users to attack and crack WPA/WPA2 handshakes quickly, leveraging the power of both the CPU and GPU.

The spyglass allows you to see valuable insights as the cracking is taking place. It reports the session name, status, and the type of hash known as WPA/WPA2, along with the MAC address of the attacked wireless access point. Users can watch the attack's progress by checking metrics, for example, seeing how fast device #1 is working (26,758 hashes per second) and how many percent of the work has been done overall (5.73%). The progress includes the number of passwords that have been tested from the input wordlist to show how complete brute force and dictionary methods can be.

Furthermore, it reports on the recovery progress, listing how many hashes have been cracked, how many were rejected, and the latest save point so that the attacker can start over from that point if necessary. This matter becomes crucial when we work with large sets, as it can take a long time to crack the keys.

By keeping track of everything your computer and GPU are doing, the Hashcat interface makes sure that your resources are managed well when you attack. These statistics permit users to adjust the cracking procedure so it runs both quickly and within the bounds of their hardware's abilities.

All in all, Hashcat's real-time progress and powerful features make it unavoidable for anyone aiming to crack the passwords found in WPA/WPA2 capture files. It is important to know about these tools to learn how MitM attackers steal passwords from wireless networks.



```
Session..........: hashcat
Status...........: Running
Hash.Type........: WPA/WPA2
Hash.Target......: RT-48 (38:17:66:0e:dd:74 <-> 48:d2:24:9a:91:df)
Time.Started.....: Wed Jan 11 18:14:28 2017 (18 secs)
Time.Estimated...: Wed Jan 11 18:19:25 2017 (4 mins, 39 secs)
Input.Base.......: File (newrockyou.txt)
Input.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:    26758 H/s (8.80ms)
Speed.Dev.#3.....:     5618 H/s (11.22ms)
Speed.Dev.#*.....:    32372 H/s
Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 550912/9606541 (5.73%)
Rejected.........: 0/550912 (0.00%)
Restore.Point....: 534528/9606541 (5.56%)
Candidates.#1....: 0854206156 -> 0868778676
Candidates.#3....: 0869699539 -> 0870248204
HWMon.Dev.#1.....: Util: 75% Core: 800Mhz Mem:1000Mhz Lanes:16
HWMon.Dev.#3.....: N/A

[s]tatus [p]ause [r]esume [b]ypass [c]heckpoint [q]uit =>
```

Figure 4 Hashcat terminal output monitoring real-time WPA handshake cracking progress and device utilization

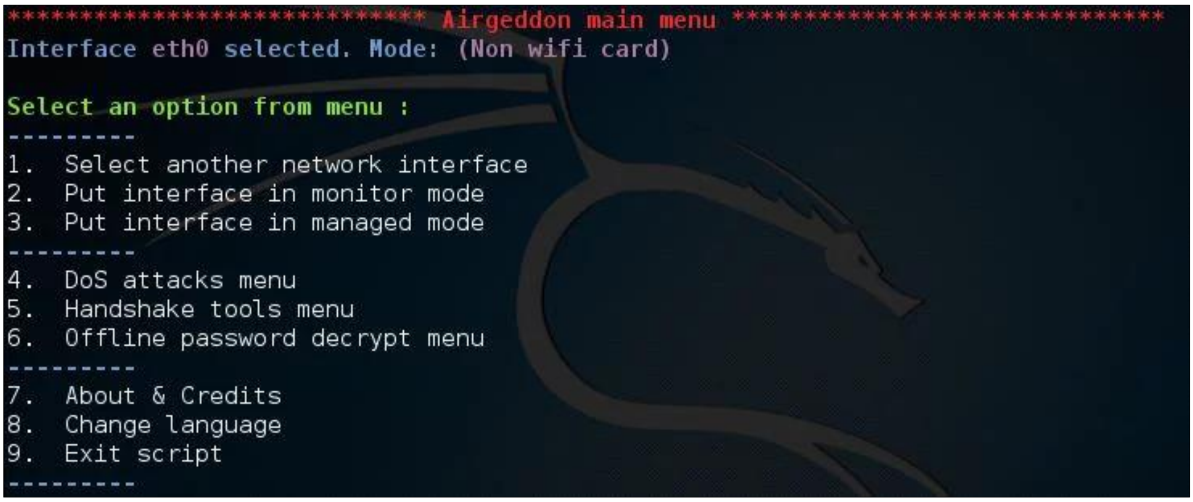
2.5. Automated Attack Frameworks and Network Interface Management

Man-in-the-Middle (MitM) and wireless network attacks have been transformed by having a collection of tools and techniques brought together into single, simple interfaces. A notable example is Airgeddon, a script that helps automate and make simple tasks such as launching attacks. Managing and selecting the needed test features is made easy in Image 6 through the Airgeddon main menu, helping penetration testers carry out effective network penetration testing.

The user interface on the menu includes several important options for managing the network, such as picking network cards and switching to either monitor or managed sysadmin mode. Capturing data packets and sending out these packets with traffic injections is not possible without changing to monitor mode, which is why this mode is essential for wireless auditing and attacks. A doctor's quick switch to various interface modes means less need for command-lines, allowing attackers and penetration testers to use Airgeddon's full potential more easily and quickly.

Alongside managing the user interface, Airgeddon supports different attack types, including DoS attacks, tools for capturing handshakes, and offline password decryption. With this suite, you can execute several MitM attacks, such as Evil Twin and handshake cracking, easily following a guided process. Automating tedious jobs in Airgeddon not only reduces mistakes but also speeds up attacks when time and closure are critical.

The module-based structure and intuitive menus improve how people use the tool and make it useful for people who want to use it for good or bad. It explains why defenders must realize that modern MitM attacks are now carried out using complex and fast processes, so they need to be aware of how to handle these attacks.



```
**************************** Airgeddon main menu ******************************
Interface eth0 selected. Mode: (Non wifi card)

Select an option from menu :
---------
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
---------
4.  DoS attacks menu
5.  Handshake tools menu
6.  Offline password decrypt menu
---------
7.  About & Credits
8.  Change language
9.  Exit script
---------
```

Figure 5 Airgeddon main menu offering automated attack options and network interface mode management

2.6. Traffic Capture and Analysis Techniques

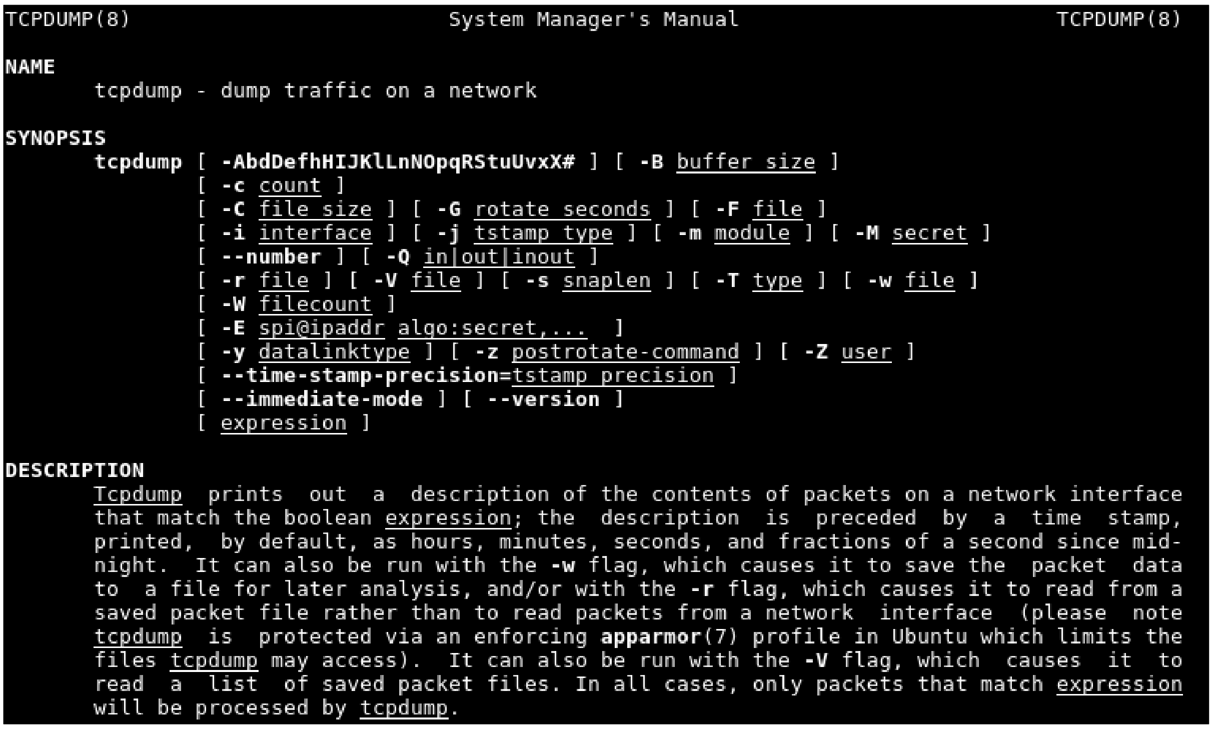
To understand and conduct a MitM attack, you must first observe and analyze the traffic going through the network. Image 7 points out that tcpdump is a popular command-line program for capturing and recording network traffic items coming in and out of various interfaces. The multiple filtering, capturing, and storage features allow for both wide-range and fine-tuned data assembly. Because tcpdump is so flexible, it is useful for both attackers and those defending a system.

You need to enter the network interface, along with desired capture filters and the output method, to run tcpdump. Users may change the buffer size (-B), specify the maximum number of packets per capture (-c), and the file size (-C) to control the running of tcpdump efficiently. By rotating files through intervals (-G), the logs will remain small and easy to manage during drawn-out surveillance. The '-f' argument with tcpdump makes sure only valuable and targeted traffic is displayed, cutting out unnecessary information.

You can use the -w flag to save captured packets in files and use -r to analyze them offline. The tool can precisely set the time window and apply rotations automatically on the processed images. By outputting information about packets in a format people can understand, tcpdump helps analysts spot differences in the usual network behavior.

When coming across MitM attacks, tcpdump allows for catching the crucial handshake, ARP, and unencrypted traffic needed for the attack or analysis. Since it lacks a graphical user interface like Wireshark, it can still easily run packet capture on systems with limited resources. Using advanced tcpdump commands and filters can give an attacker or security analyst the tools to easily view and discover possible network vulnerabilities.

All things considered, tcpdump is the backbone of network traffic capture and analysis, allowing for powerful and adaptable features useful in MitM reconnaissance and planning attacks.



```
TCPDUMP(8)                    System Manager's Manual                   TCPDUMP(8)

NAME
       tcpdump - dump traffic on a network

SYNOPSIS
       tcpdump [ -AbdDefhHIJKlLnNOpqRStuUvxX# ] [ -B buffer_size ]
               [ -c count ]
               [ -C file_size ] [ -G rotate_seconds ] [ -F file ]
               [ -i interface ] [ -j tstamp_type ] [ -m module ] [ -M secret ]
               [ --number ] [ -Q in|out|inout ]
               [ -r file ] [ -V file ] [ -s snaplen ] [ -T type ] [ -w file ]
               [ -W filecount ]
               [ -E spi@ipaddr algo:secret,...  ]
               [ -y datalinktype ] [ -z postrotate-command ] [ -Z user ]
               [ --time-stamp-precision=tstamp_precision ]
               [ --immediate-mode ] [ --version ]
               [ expression ]

DESCRIPTION
       Tcpdump  prints  out  a  description of the contents of packets on a network interface
       that match the boolean expression; the  description  is  preceded  by  a  time  stamp,
       printed,  by default, as hours, minutes, seconds, and fractions of a second since mid-
       night.  It can also be run with the -w flag, which causes it to save the  packet  data
       to  a file for later analysis, and/or with the -r flag, which causes it to read from a
       saved packet file rather than to read packets from a network  interface  (please  note
       tcpdump  is  protected via an enforcing apparmor(7) profile in Ubuntu which limits the
       files tcpdump may access).  It can also be run with the -V flag, which  causes  it  to
       read  a  list  of saved packet files. In all cases, only packets that match expression
       will be processed by tcpdump.
```

Figure 6 Tcpdump manual snippet outlining command-line options for network traffic capture and filtering

2.7. Deep Packet Inspection and Protocol Analysis

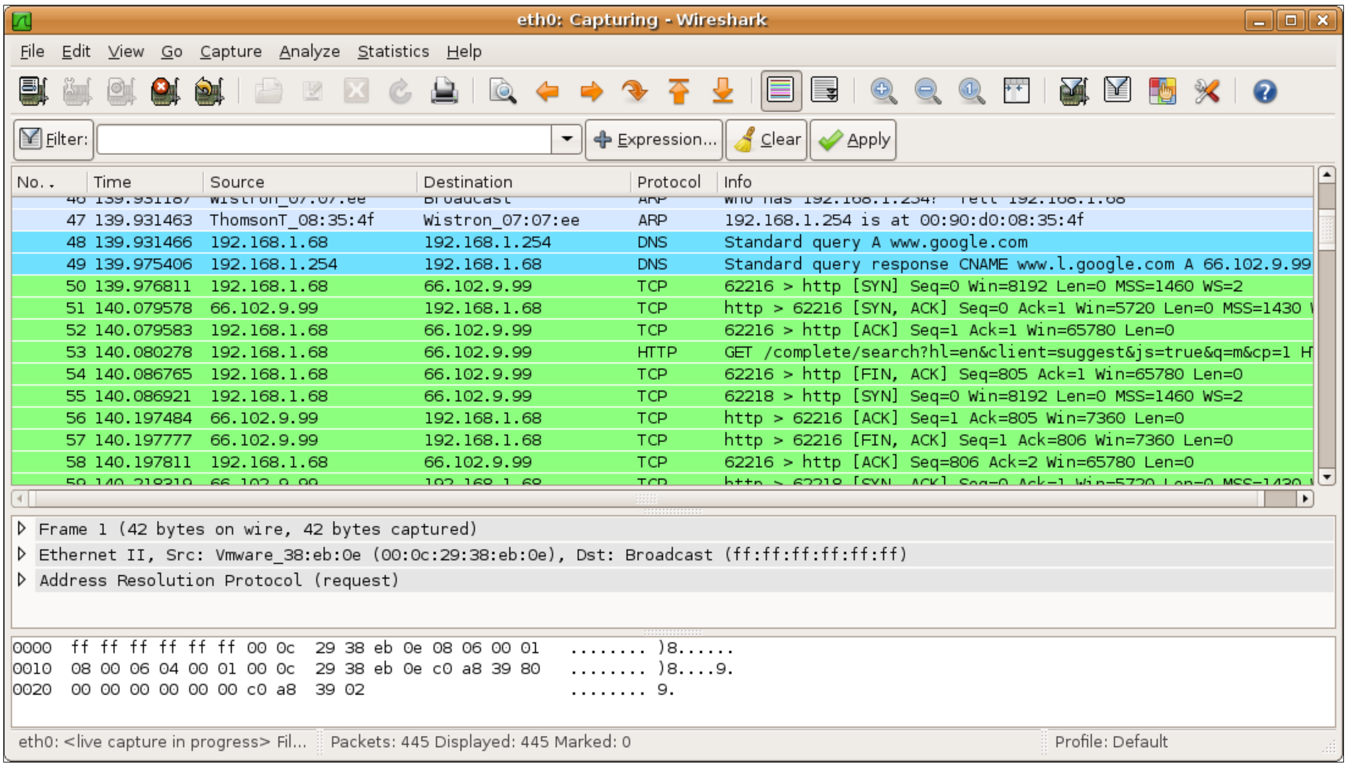
DPI and protocol analysis are important to MitM attacks, as they allow both attackers and experts to analyze packets and protocols in detail. The captured and dissected traffic in Wireshark that you can see in Image 8 highlights the specification's advantages.

With Wireshark, people can analyze network-related traffic by capturing live packets on a network and seeing how they are built and organized. On the interface, you will see information such as the source and destination IP addresses, the format of the packets, and their payload. Adding colors to packet lists makes them easier to read, especially for highlighting protocols such as DNS, TCP, HTTP, and ARP, which we see in the captured traffic of Image 8. The table makes it easier to see any unusual or suspicious activities in the flow of data.

Wireshark is powerful because it allows users to observe all the layers of a packet, from Ethernet to the application-specific kind. By inspecting the traffic at multiple points, analysts are able to see network activity, spot where attacks are injected, and identify areas that can be abused during MitM attacks. Looking at unencoded traffic or observing DNS queries can help develop ways to attack or locate suspicious behavior.

You can also use built-in features in Wireshark to examine specified types of traffic, IPs, or communication protocols. You need this feature when going through a lot of data to pick out the relevant traffic.

Overall, Wireshark enables detailed review of packets and an easy-to-use interface, which is useful for carrying out and preventing MitM attacks. Getting good at analyzing protocols is key to improving your network's behavior and security.


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply

No. .	Time	Source	Destination	Protocol	Info
46	139.931187	Wistron_07:07:ee	Broadcast	ARP	Who has 192.168.1.254? Tell 192.168.1.68
47	139.931463	ThomsonT_08:35:4f	Wistron_07:07:ee	ARP	192.168.1.254 is at 00:90:d0:08:35:4f
48	139.931466	192.168.1.68	192.168.1.254	DNS	Standard query A www.google.com
49	139.975406	192.168.1.254	192.168.1.68	DNS	Standard query response CNAME www.l.google.com A 66.102.9.99
50	139.976811	192.168.1.68	66.102.9.99	TCP	62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51	140.079578	66.102.9.99	192.168.1.68	TCP	http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52	140.079583	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
53	140.080278	192.168.1.68	66.102.9.99	HTTP	GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
54	140.086765	192.168.1.68	66.102.9.99	TCP	62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55	140.086921	192.168.1.68	66.102.9.99	TCP	62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56	140.197484	66.102.9.99	192.168.1.68	TCP	http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57	140.197777	66.102.9.99	192.168.1.68	TCP	http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58	140.197811	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
59	140.218319	66.102.9.99	192.168.1.68	TCP	http > 62218 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430

```
▷ Frame 1 (42 bytes on wire, 42 bytes captured)
▷ Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 0c  29 38 eb 0e 08 06 00 01   ........ )8......
0010  08 00 06 04 00 01 00 0c  29 38 eb 0e c0 a8 39 80   ........ )8....9.
0020  00 00 00 00 00 00 c0 a8  39 02                     ........ 9.
```

eth0: <live capture in progress> Fil... Packets: 445 Displayed: 445 Marked: 0 Profile: Default

Figure 7 Wireshark packet capture interface illustrating deep packet inspection and protocol analysis during live traffic capture

2.8. Wireless Network Attack Configuration and GUI Tools

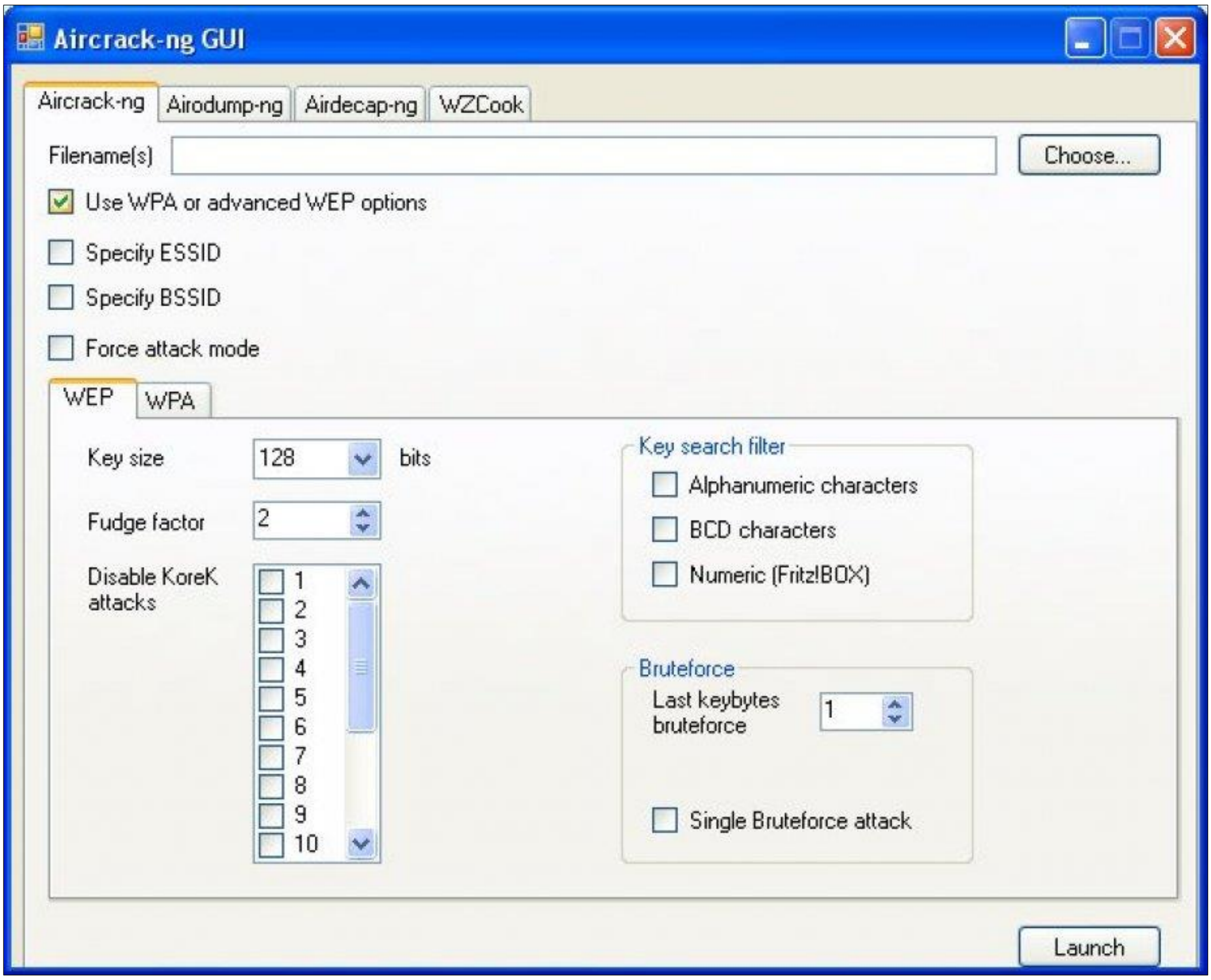
Graphical user interfaces (GUIs) make it much easier for people at every experience level to run wireless network attacks. Aircrack-ng GUI, as shown in Image 8, is a useful tool that helps you organize and use various attack options to assess WEP and WPA networks.

On the interface, users have access to important aspects like setting the key size for WEP attacks and also disabling the KoreK attack feature. Command of fudge factor through the GUI lets you adjust the level of tolerance for key verification, allowing for better control of the attack's accuracy. When setting up a WPA attack, users can decide how many key bytes they want to try and whether or not to use single brute force attacks.

With filters for alphanumeric, BCD, and numeric characters specific to routers like Fritz!BOX, the GUI of Aircrack-ng makes it much easier and more reliable to perform attacks. The real-time view during attack planning is important for attackers to make on-the-spot decisions that work well with their resources and attacks.

With GUI, several ways to attack are stacked in a single window to connect complicated commands and easier user interfaces. This makes it easier to work quickly when setting up and testing things in wireless auditing. Attackers can test several parameters after studying the handshake and progress made with trying passwords.

Such tools make it easier for users to perform wireless attacks, which helps them understand, audit, and protect against Man-in-the-Middle attacks in today's networks.



Filename(s)

☑ Use WPA or advanced WEP options

□ Specify ESSID

□ Specify BSSID

□ Force attack mode

Key size: 128 bits

Fudge factor: 2

Disable KoreK attacks: □ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10

□ Alphanumeric characters

□ BCD characters

□ Numeric (Fritz!BOX)

Last keybytes bruteforce: 1

□ Single Bruteforce attack

Figure 8 Aircrack-ng GUI providing a graphical interface for configuring WEP and WPA wireless network attacks

3. Methodology

3.1. Research Design

Instead of relying solely on real-life incidents, the research team has controlled setups and simulations to learn about MitM attacks and how to guard against them. They make use of real-world network types such as wireless and wired local networks to make the experiments useful. In attack simulations, experts use well-known MitM techniques such as ARP spoofing, DNS spoofing, and making fake access points. The aim of each simulation is to watch how the attack gets bigger, how it gains data during the process, and how effective the various defenses are. Several attack methods and tools are used to measure how quickly and effectively these threats can be used. The design supports the same set of testing conditions and makes it possible to experiment with different types of attacks and the responses to them. Traffic across the network, the start-up messages sent, and the authentication methods used are all examined to observe the results of the simulation. Doing so lets you see where the system is weak and what can be done to improve it across different networks, revealing much about the dynamics of MitM attacks.

3.2. Data Collection

Network traffic, handshake information, and logs are collected to help study details of the MitM attack attack. Packets captured from live networks by Wireshark and tcpdump during simulation attacks are saved in standard formats, making them easy to look at later. Handshake files, which are important for WPA/WPA2 cracking, are obtained during wireless attacks to find out any weaknesses in the encryption. Records from attack tools and frameworks include details about the attack's process and the outcomes. Network events are organized in such a way that it is easier to link them to different stages of an attack. The processes used for collecting packets are designed to ensure both they are complete and accurate, so relevant data can be reviewed and accessed during an evaluation. By storing datasets safely and making sure they are labeled, you support repeatability and future research, which can help in finding patterns, abnormalities, and possible safeguards against MitM attacks.

3.3. Case Studies/Examples

3.3.1. Case Study 1: Public Wi-Fi Rogue Access Point Attack

It is now very common to find Wi-Fi in hotels, airports, cafés, and other public areas. Secureness in these networks can sometimes be lacking, allowing Man-in-the-Middle attacks to occur. The author uses this case study to show how hackers managed to intercept the banking details and other important user information using a false Wi-Fi network in a café.

A rogue access point was placed that loudly advertised the correct network name (SSID) to trick people into connecting to it. Commonly referred to as an Evil Twin attack, this method purposefully deceives people into using the malicious network, making them feel it is safe. Since users often don't check if a public Wi-Fi is real, the rogue access point was able to attract many unwitting victims.

As soon as the users were connected, the attacker became the middleman for their internet activity. As a result, the attacker could silently grab data packets exchanged between the users and the internet. Due to the lack of effective encryption or weak protocols, information like your login, credit card, and email could easily be picked up by someone when using public networks.

The attackers watched for unsecure traffic and got hold of login information on websites that had errors with their SSL certificates. In addition, through session hijacking, an attacker could enter and use someone else's account, without first needing the password.

This attack showed that there was a major problem facing the industry. people using public Wi-Fi usually do not realize how risky it is. Many do not realize that they may not be entirely safe online when they are not using VPNs or looking for secure websites. This event made it clear that users should verify the network, not do sensitive tasks on unprotected networks, and use VPNs when they are connected to public Wi-Fi.

Technically, the event highlighted weaknesses in the ways Wi-Fi devices secure their connections and authentication. While WPA2 is commonly applied, quite a few public hotspots either do not protect their network at all or make it very easy for anyone to guess the password. The weak points were used by the attackers because clients did not authenticate their networks, so the rogue APs could imitate the real APs without making the users aware.

Applying stronger network access controls like WPA3 makes it more difficult for attackers to pretend they are part of a real network. Deploying intrusion detection systems is also a good way to pick up on suspicious APs using recognized SSIDs.

It was made clear in this case that end-to-end encryption should happen at all stages, not just for wireless communications. Strong security features such as HTTP Strict Transport Security (HSTS) and certificate pinning should make sure that services and websites block attackers, even if they succeed at reaching the network layer.

After the attack, many cafés and public hotspots ensured their networks were more secure and informed their customers about the issue. Due to these attacks, many users learned to avoid sensitive transactions in public and started using VPNs to hide what they did on the internet.

Therefore, it is clear from this example that rogue access points are used in public Wi-Fi to exploit unsecured wi-fi networks and carry out MitM attacks. This shows that using multiple security layers, like strong network defenses, encryption practices, training employees, and constant surveillance are important to stop interception of private data in open Wi-Fi areas.

3.3.2. Case Study 2: Corporate Network ARP Spoofing Breach

In a recent attack on a business network, intruders took advantage of ARP spoofing to intrude and modify important data traffic inside the network. This means the attacker uses ARP to falsely link their device's MAC address to these important IP addresses, allowing them to eavesdrop on and hijack data. By carrying out this type of attack, the attacker manages to intercept important data or disrupt both communication and business activities with a device.

In this case, a mid-sized organization had a network that wasn't divided well, making it easy for the breach to happen. After getting inside the network, attackers could easily perform ARP spoofing attacks on various devices. The attackers managed to connect themselves to the network, acting as middlemen, without getting spotted right away by inserting forged ARP entries into both client and server caches. They were able to grab unprotected data packets, including important emails, login information, and internal files.

Part of the main reasons this happened was because network segmentation and isolation were not in use. Without using VLANs or other means to logically divide a network, attackers could easily move sideways, making the harm of the attack significant. Devices which needed to be separate for security purposes were connected to the same broadcast domain, so ARP spoofing attacks became easier and caused more damage.

Lack of real-time network monitoring by the company allowed the attackers to exploit it. Legacy security methods mainly protected the periphery, allowing internal traffic to go without much security. As the network did not have ways to track ARP or suspicious MAC-IP links, the intruders were free to steal a lot of information without being noticed for a while. The lack of clarity in these attacks demonstrates the need to set up internal network monitoring systems with ARP spoofing security modules.

Additionally, the incident revealed that there were problems in the company's security rules and the way employees were trained. Because ARP was not secured and anti-spoofing wasn't enabled at the endpoints, it allowed attackers to get to the network. Employees did not have enough training to identify possible network breaches, which slowed down the response to the issue.

Therefore, the group took several steps to solve the issues. The network structure was changed using VLANs to limit access to critical parts and lessen the chances of an attack. The company set up improved monitoring tools to detect any ARP spoofing, allowing for quick response to incidents. Anti-spoofing methods were added to our endpoint security policies, and training was given to our team on how to detect inside threats.

The lesson here is that corporate environments should always follow a defense-in-depth strategy. Using perimeter security alone is not enough to stop ARP spoofing, which can get inside the network. The main way to protect from such internal threats is to properly segment a network, watch traffic, and enforce solid security policies.

All in all, the attack on corporate ARP proved that attackers can exploit protocol and design flaws to gain access to internal communications. It highlights the need for multiple layers of security, constant supervision, and ongoing education of staff to stop Man-in-the-Middle attacks from harming important company details.

3.4. Evaluation Metrics

Assessing the quality of MitM attack prevention methods and tools must rely on a wide range of performance indicators. The success rate refers to the percentage of times the tool can intercept, decrypt, or alter the planned traffic. A good track record in warfare suggests that a military is well-equipped, but it can also reveal possible risks to security. Being able to avoid network monitoring, intrusion detection, and endpoint defenses is also a key factor when judging a cybersecurity tool. Using tools that are not easy to see makes it easier for attackers to get positive results, increasing the level of risk.

How quickly the attacks can take place, such as handshake capture, has a strong impact on the security of both sides. Greater speed in tools and systems makes exploiting or responding to an attack easier, which changes the overall impact and effectiveness of defenses. It checks whether a tool will work as intended in various situations and networks. Employing tools that are highly reliable means there are fewer errors and less chance of a false positive outcome.

By using these measures, one can compare MitM tools and methods to defend against attacks, which helps in boosting network security.

4. Findings

4.1. Router Compromise and Gateway Control

If a router is compromised by an attacker, it can make it easy to manage and watch network traffic. Attackers who exploit loopholes in firmware, easily guess passwords, or bad system setups can regain control of networking traffic on networks. Thanks to controlling the gateway, hackers can manipulate, monitor, or split up traffic sent or received online.

With this kind of control, an agent can take sensitive data, place unwanted programs, or open a constant backdoor for continuous access. If a router is hacked, it affects all devices using the network and opens the door to a bigger attack. You can protect yourself from such issues by using secure and different passwords on your routers, routinely updating their firmware, and switching off the services you don't need. Segmenting the network and regularly looking for out-of-place gateway activity can help stop access to your network. Overall, safeguarding the gateway of the network makes it harder for MitM attacks and supports its integrity.

4.2. DNS Spoofing and Phishing Integration

In mitigation attack chains, DNS spoofing, or DNS cache poisoning, means attackers take control of the DNS to redirect people to harmful websites. Attackers can use DNS attacks to steer users towards fake websites set up to steal their credentials or spread malware. Phishing and DNS spoofing used together make it possible for attackers to steal valuable information from unwitting users. This approach makes use of the fact that users know and trust well-known domain names, as many networks' DNS is not properly secured. At the beginning, the attacker gets access to the victim's network by either blocking or poisoning the DNS requests. In order to tackle this problem, DNSSEC, enforcing HTTPS, and educating people about verifying URLs play a key role. Careful observation of DNS traffic helps many find abnormalities quickly. The connection between DNS spoofing and phishing demonstrates how MitM attacks today are complex and involve several techniques.

4.3. ARP Spoofing and Data Injection

In MitM attacks, hackers may use ARP spoofing to connect their MAC address to the IP address of another device with the help of ARP messages. Thanks to this trick, attackers are able to steal or alter the data traveling across the network for the victim. After being on the communication path, attackers might inject data to change packets or introduce harmful material and use this to exploit certain vulnerabilities or mislead users. In some cases, data injection might bring about session hijacking, delivering malicious software, or sharing false information. Such attacks mostly succeed on local networks with poor security, such as those that lack the necessary ARP inspection or separation into various segments. It is difficult to detect ARP spoofing because the attack covers the main workings of the protocol, so close watching is always needed. Methods to prevent ARP attacks are static ARP entries, separating networks, and using tools to detect unusual ARP activity. ARP spoofing in combination with data injection demonstrates how attackers can control and crack the confidentiality and safety of a network.

4.4. Exploitation of Network Services

During many mitigation of man attacks, the attackers exploit issues in protocols and network services, especially LDAP, SMB, RDP, and NetBIOS. Such services are usually responsible for keeping files private, allowing access from distant computers, and identification, so they appeal to attackers. After scanning for services that are either not protected or have errors in their configuration, the attackers use known attacks or brute-force the system to get access to unauthorized areas. Following breach, the perpetrator can remove sensitive information, deploy viruses, or move further inside the network. Most of the time, the attack involves taking advantage of the computer's standard credentials, passwords that are easy to guess, or weaknesses in systems like EternalBlue. You can prevent such attacks by frequently patching your systems, using tough login credentials, and always monitoring your network. This step underlines that securing internal services is crucial, since attackers often rely on them to further infiltrate the network and stay inside the target system.

5. Defense

5.1. Network Monitoring and Anomaly Detection

To prevent Man-in-the-Middle attacks, having strong monitoring and detection tools is very essential. As long as networks are watched carefully, businesses can notice any irregularities that may point to an ongoing cyber attack. Such systems go over metrics including volume, source and destination addresses, and protocols to notice any abnormalities. Such systems can find suspicious signs like sudden ARP broadcasts, strange DNS requests, or uncommon routing, which are commonly done during a MitM attack. Figuring out an attack quickly allows for a swift response that can minimize the problems caused by the attack. Adding IDS and IPS makes security stronger as they either block dangerous traffic or let the network administrators know if any is detected. A combination of network monitoring tools and logging and analysis platforms gives full insight and forensic support. Good monitoring involves adjustments to reduce false alarms and make sure notifications come at the right time. To prevent major harm, it is important to continuously watch over the network and respond to sneaky MitM attacks.

5.2. Strong Encryption and Certificate Validation

Using strong encryption and checking valid certificates is the basis for saving data privacy and its integrity while being sent. When using TLS (Transport Layer Security), the messages people send and receive are encoded, so stolen information is unreadable to anyone trying to eavesdrop. Still, using only encryption is not enough; it must be paired with checking certificates to be sure the endpoints joining in a communication session are trustworthy. Certificates can be exploited, allowing attackers to perform attacks that could comprise the security of protected communications. If you use strict rules and verify certificate revocation lists, as well as pin certificates, trust in secure connections is increased. TLS 1.3 protects users better by removing well-known vulnerabilities that are present in earlier encryption standards. In addition, extended use of HTTPS and application of HSTS make it challenging for attackers to get involved with web traffic. Both strong encryption and strict validation of certificates make it extremely hard for attackers to conduct Man-in-the-Middle attacks.

5.3. Secure Wireless Protocols and Configuration

It is very important to use safe wireless protocols and properly configure your networks to stop Man-in-the-Middle attacks on wireless networks. Basic security features in standards like WPA2 have been enhanced by standards like WPA3, which also include better safeguards against attacks. Arranging wireless networks with powerful, special passwords and disabling out-dated protocols such as WEP makes them much safer. It is important for network administrators to enable PMF to secure the network from spoofing and deauthentication attacks. Separating guest and corporate traffic helps protect your network by reducing the opportunities for an attacker to advance in it. Also, make sure to not use services that are not needed and regularly update firmware on your wireless access points to improve security. Applying strong protocols and careful setting of configurations will help organizations protect their wireless networks from MitM attacks.

5.4. Making sure employees are cautious about possible social engineering

Being aware of cyber threats is important because it can help defend against Man-in-the-Middle attacks that begin using social engineering. Educating employees to detect phishing emails, notice strange activities on the network, and not use unsecured Wi-Fi makes them less likely to fall victim to certain dangers. By verifying your network, refraining from sharing information without security, and using a VPN, you can keep yourself protected from possible exposure. Having regular security awareness training should help users stay aware of new risks and best practices online. Moreover, when employees are aware of security, they are more likely to notice things that seem off and act on it immediately. Educating people about social engineering methods is the best practice to stop MitM attacks since they rely on human errors.

5.5. Incident Response and Forensic Analysis

Dealing with and limiting the damage of MitM attacks relies on incident response and analysis. Having an effective incident response plan allows organizations to spot, stop, and remove threats before they do serious harm. You should detect systems that are compromised, remove them from the network, and implement fixes or changes to avoid another attack. Analysis of traffic, logs, and system artifacts helps establish how large the attack was, how it took place, and when. By performing in-depth forensic investigations, experts can discover attackers' tactics, how they entered the system, and how they transferred the data out, something that is useful for future defense planning. Having complete and undamaged logs is important for the correct analysis of events and for handling legal issues. While dealing with the effects of an incident, firms should learn from forensics reports, review and update their policies, and train staff. Acting quickly to deal with MitM attacks and carrying out a detailed analysis beforehand protects an organization's reputation and ability to cope with new attacks.

6. Conclusion

6.1. Summary of Key Points

In this article, we discussed how Man-in-the-Middle (MitM) attacks work, and we looked at different tactics hackers use to disrupt and alter communication on networks. Some methods used in attacks are compromising routers, spoofing DNS, ARP, and using services that are vulnerable. Discussion revealed some important tools like Wireshark, Aircrack-ng, Hashcat, as well as Airgeddon, which help carry out these attacks with ease. Often, defense strategies include network monitoring, great encryption, secure wireless protocols, and education for users to reduce risks. GUI-based tools make it easier for attackers to execute their attacks, pointing to their advancing skills. In addition, properly reacting to incidents and analyzing them is important for detecting and recovering from cyber attacks. All in all, being aware of both attack and defense techniques is necessary to protect today's networks from MitM threats, and this approach should always be closely and carefully maintained.

6.2. Future Directions

Battle strategies for MitM attacks will include the use of advanced technologies and detection tools. More and more, AI and machine learning are used to review network data in real time and detect the signs of MITM attacks. With proactive systems, problems can be detected and resolved automatically and in a shorter time. Also, using cutting-edge encryption and zero-trust designs will reduce the risk of data interception or manipulation by attackers. Benefits from research on this subject could improve long-term security for communication systems. Educating individuals and analyzing their actions will go hand in hand with other security techniques. For the most part, fighting MitM requires a comprehensive, evolving approach that considers advances in technology as well as human behavior to remain one step ahead of threats.

References

[1] Bloch, F., Chatterjee, K., and Dutta, B. (2023). Attack and interception in networks. Theoretical Economics, 18(4), 1511–1546. https://doi.org/10.3982/te5122

[2] Cherian, M. M., and Varma, S. L. (2022). Mitigation of DDOS and MiTM attacks using belief based secure correlation approach in SDN-based IoT networks. I. J. Computer Network and Information Security, 1, 52–68. https://doi.org/10.5815/ijcnis.2022.01.05

[3] Deb, D., Chakraborty, S. R., Lagineni, M., and Singh, K. (2020). Security Analysis of MITM Attack on SCADA Network. Communications in Computer and Information Science, 501–512. https://doi.org/10.1007/978-981-15-6318-8_41

[4] Mallik, A. (2019). MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS. Cyberspace: Jurnal Pendidikan Teknologi Informasi, 2(2), 109. https://doi.org/10.22373/cj.v2i2.3453

[5] Mallik, A., Ahsan, A., Shahadat, M. M. Z., and Tsou, J. C. (2019). Understanding Man-in-the-middle-attack through Survey of Literature. Indonesian Journal of Computing, Engineering and Design (IJoCED), 1(1), 44. https://doi.org/10.35806/ijoced.v1i1.36

[6] Nazir, R., Iaghari, A. A., Kumar, K., David, S., and Ali, M. (2021). Survey on Wireless Network Security. Archives of Computational Methods in Engineering. https://doi.org/10.1007/s11831-021-09631-5

[7] Rajadurai, H., and Gandhi, U. D. (2020). A stacked ensemble learning model for intrusion detection in wireless network. Neural Computing and Applications. https://doi.org/10.1007/s00521-020-04986-5

[8] Sharma, A., Tyagi, A., and Bhardwaj, M. (2022). Analysis of techniques and attacking pattern in cyber security approach: A survey. International Journal of Health Sciences, 6(S2), 13779–13798. https://doi.org/10.53730/ijhs.v6nS2.8625