KU LEUVEN

FACULTEIT INGENIEURSWETENSCHAPPEN

Problem Solving and Engineering Design part 3

ESAT2A2

Jarle Braeken (r0998124)
Arthur Cukier (r0976603)
Pieter Deferme (r0995734)
Robin Derikx (r0978208)
Willem Hendig (r0995944)
Giel Swenters (r1006315)

Crack the Wi-Fi

PRELIMINARY REPORT

Co-titular
Vincent Rijmen

Coach(es)
John Gaspoz
Dilara Toprakhisar

ACADEMIC YEAR 2024-2025

Declaration of originality

We hereby declare that this submitted draft is entirely our own, subject to feedback and support given us by the didactic team, and subject to lawful cooperation which was agreed with the same didactic team.
Regarding this draft, we also declare that:

1. *Note has been taken of the text on academic integrity (https://eng.kuleuven.be/studeren/masterproef-en-papers/documenten/20161221-academischeintegriteit-okt2016.pdf).*
2. *No plagiarism has been committed as described on https://eng.kuleuven.be/studeren/masterproef-en-papers/plagiaat.*
3. *All experiments, tests, measurements, …, have been performed as described in this draft, and no data or measurement results have been manipulated.*
4. *All sources employed in this draft – including internet sources – have been correctly referenced.*

Contents

0 Man-in-the-Middle (+ track changes)

The main target of this project is to intercept Locale Area Network (LAN) traffic packages and alternate them. In this way,~~This way~~ a man-in-the-middle (MitM) attack can be performed between the traffic forwarding (forwarding to the Wide Area Network (WAN)) router and the victim's device.

[rp 1] T1

To perform a MitM attack, the victim's device has to think that the attacker's device is the traffic forwarding router and vice versa the router has to think the attacker's device is the victim's device. See figure 2.

[1] Bij2

This manipulation is done by fooling the Address Resolution Protocol (ARP). "ARP is a commonly used protocol pertaining to computer communications." [Aayush Majumdar, 2021]~~ARP is a commonly used protocol pertaining to computer communications.~~ In a LAN, ARP messages are shared. With these messages, the router in the network knows which IP addresses belong to which computer in the network, through correlating IP addresses and corresponding physical addresses (MAC addresses). Network messages are sent within the LAN, this obligates the attacker to connect to the LAN for carrying out an ARP Poisoning or Spoofing attack.~~The boundary that the messages are sent within the LAN, obligates the attacker to connect to the LAN for carrying out an ARP Poisoning or Spoofing attack.~~ ~~[Aayush Majumdar, 2021]~~

[rp 2] R2

[rp 3] T3

For this project, the MitM will be demonstrated for two attacks. The first attack is through implementations of~~by changing the~~[rp] redirection links. Redirect links redirect a user that interacts with a webpage to another webpage, which wasn't the intented webpage of the original site.~~This way, a user who clicks on "sign in" can be redirected to a web page of the attacker's choice.~~ The second attack redirects a subscription payment for renting an account to another account.

[rm 1] R3

[rp 4] T1 & T3

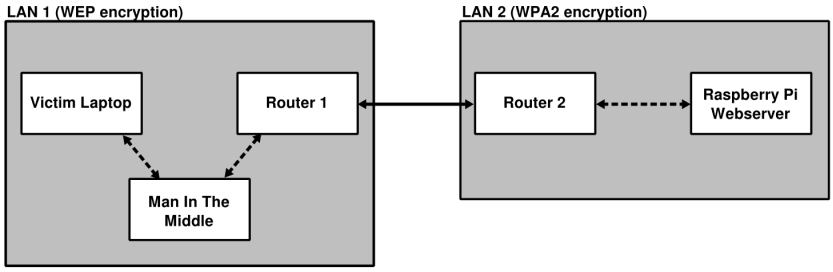

Figure 1: Network scheme

0.1 ARP poisoning

An ARP Poisoning attack is an attack in which spoofed ARP messages are sent to the default gateway on the locale network (LAN) with the intent of changing the ARP cache table. [Aayush Majumdar, 2021] The default gateway on a network is a node/gate with the purpose of connecting and so gaining access to another network. In the ARP cache table is information of the relation IP address $\longleftrightarrow$ MAC address stored. [Wikipedia, 2024]

Once the default gateway receives these ARP packets, the changes are broadcast to all devices connected to the network. Broadcasting makes it possible for devices to locate other devices within the network from which it needs to ask something.~~This way other devices can locate other devices, from whom it has to request something.~~ ~~Now~~[rm] After swapping the ARP cache table, all devices recognize the attacker's device as the victim's device. Afterwards, all requests are sent to the attacker.~~So all requests are first sent to the attacker.~~[rp] Depending on the kind of attack to use, the attacker has to forward the network packets to the victim and in reverse if the packets came from the victim. In this process, the data packages may change. ~~In this process data containing the packets can be changed.~~ This process of intercepting and alternating the data packets is the man-in-the-middle (MitM) attack. ~~[Aayush Majumdar, 2021]~~

[rp 5] T1 & T3 & Sp

[rp 6] Z

[rm 2] R3

0.2 Scapy

For ARP-spoofing and the MitM attack, Scapy is used in Python for setting up an ARP poisoning packet, sending it to the gateway and afterward restoring the network by reversing the ARP spoofing. The physical address (MAC address), the gateway and the victim's IP needed for this program are found by Aircrack [chapter **??**].

[2] Refer-ention to Aircrack chapter

To control if the ARP cache table has changed, the ARP table can be printed using the command:
>>> **ARP -a**

or using the package 'sniff' from Scapy in Python.

0.3 Live intervention

Once the ARP poisoning attack succeeds, the attacker can implement its goal. This project's goal of the MitM attack is first to implement redirect links and second to redirect a subscription payment. Detour links are of interest to the attacker. They redirect the user to other sites with different targets. Targets such as advertising but also malicious websites. The second concept lets the user pay for the attacker by diverting the user's account rent to the attacker's account.

~~After a certain time and amount of user interactions, the next interaction causes the redirect link to be activated. Another possible goal locks the user in an unwanted screen view.~~[rm]

1 Man-in-the-Middle

The main target of this project is to intercept Locale Area Network (LAN) traffic packages and alternate them. In this way, a man-in-the-middle (MitM) attack can be performed between the traffic forwarding (forwarding to the Wide Area Network (WAN)) router and the victim's device.

To perform a MitM attack, the victim's device has to think that the attacker's device is the traffic forwarding router and vice versa the router has to think the attacker's device is the victim's device. See figure 2.

This manipulation is done by fooling the Address Resolution Protocol (ARP). "ARP is a commonly used protocol pertaining to computer communications." [Aayush Majumdar, 2021] In a LAN, ARP messages are shared. With these messages, the router in the network knows which IP addresses belong to which computer in the network, through correlating IP addresses and corresponding physical addresses (MAC addresses). Network messages are sent within the LAN, this obligates the attacker to connect to the LAN for carrying out an ARP Poisoning or Spoofing attack.

For this project, the MitM will be demonstrated for two attacks.The first attack is through implementations of redirection links. Redirect links redirect a user that interacts with a webpage to another webpage, which wasn't the intented webpage of the original site. The second attack redirects a subscription payment for renting an account to another account.

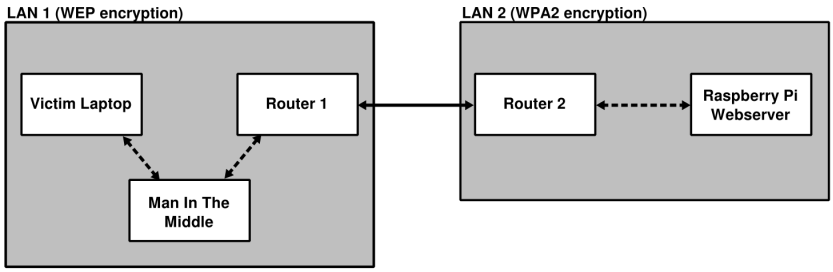

Figure 2: Network scheme

1.1 ARP poisoning

An ARP Poisoning attack is an attack in which spoofed ARP messages are sent to the default gateway on the locale network (LAN) with the intent of changing the ARP cache table. [Aayush Majumdar, 2021] The default gateway on a network is a node/gate with the purpose of connecting and so gaining access to another network. In the ARP cache table is information of the relation IP address $\longleftrightarrow$ MAC address stored. [Wikipedia, 2024]

Once the default gateway receives these ARP packets, the changes are broadcast to all devices connected to the network. Broadcasting makes it possible for devices to locate other devices within the network from which it needs to ask something. After swapping the ARP cache table, all devices recognize the attacker's device as the victim's device. Afterwards, all requests are sent to the attacker. Depending on the kind of attack to use, the attacker has to forward the network packets to the victim and in reverse if the packets came from the victim. In this process, the data packages may change. This process of intercepting and alternating the data packets is the man-in-the-middle (MitM) attack.

1.2 Scapy

For ARP-spoofing and the MitM attack, Scapy is used in Python for setting up an ARP poisoning packet, sending it to the gateway and afterward restoring the network by reversing the ARP spoofing. The physical address (MAC address), the gateway and the victim's IP needed for this program are found by Aircrack [chapter **??**].

To control if the ARP cache table has changed, the ARP table can be printed using the command:
>>> **ARP -a**

or using the package 'sniff' from Scapy in Python.

1.3 Live intervention

Once the ARP poisoning attack succeeds, the attacker can implement its goal. This project's goal of the MitM attack is first to implement redirect links and second to redirect a subscription payment. Detour links are of interest to the attacker. They redirect the user to other sites with different targets. Targets such as advertising but also malicious websites. The second concept lets the user pay for the attacker by diverting the user's account rent to the attacker's account.

2 What did I learn?

I learned to refer better and write some sentences more formally (This way → In this way). Then I changed the content sentence structure of my report to make it clearer.

References

[Aayush Majumdar, 2021] Aayush Majumdar, Shruti Raj, T. S. (2021). Arp poisoning detection and prevention using scapy. *Journal of Physics*.

[Wikipedia, 2024] Wikipedia (2024). Default gateway — Wikipedia, the free encyclopedia. [Online; accessed 14-October-2024].