The Dangers and Execution of a Man in the Middle Attack (MITM)

Donovan Roberts

St. Mary's University of Minnesota

The Dangers and Execution of a Man in the Middle Attack (MITM)

Abstract

This paper explores a multitude of published articles that report on what man in the middle attacks (MITM) are, how they are executed, and the dangers of them. The articles vary in uses regarding the discussion of MITM. The initial article, by Conti, Mauro, Nicola, Lesyk, and Viktor (2016) provide us with a foundational understand of what man in the middle attacks are and then the additional articles discuss the execution and dangers of man in the middle attacks.

The Dangers and Execution of a Man in the Middle Attack (MITM)

The Dangers and Execution of a Man in the Middle Attack (MITM)

The vulnerability I choose to hack is the "Man in the Middle Attack (HTTPS)". The Man in the Middle Attacks "targets the actual data that flows between endpoints, and the confidentiality and integrity of the data itself." (Conti, Mauro, Nicola, Lesyk, and Viktor, 2016). In the following sections I will discuss the dangers of MITM attacks, how I went about exploiting this vulnerability and lastly, what I observed.

MITM attacks can occur with a broad range of techniques and approaches that we will discuss later, all in hopes of targeting the data that flows between endpoints. As mentioned on fraud.com there are several dangers or risk that man in the middle attacks poise to individuals or organizations, the following are risked associated with MITM attacks: Loss of Sensitive Data, Data Manipulation, Compromised Authentication, Unauthorized Access to Systems, Denial of Service Attacks, and Malware Infections. Hackers can utilize data gained from MITM attacks "'for espionage or financial gain, or to just be disruptive,' says Turedi. 'The damage caused can range from small to huge, depending on the attacker's goals and ability to cause mischief.'" (Swinhoe, 2022) said Zeki Turedi a technology strategist EMEA at Crowdstrike. Now, we will move on to how I exploited this vulnerability.

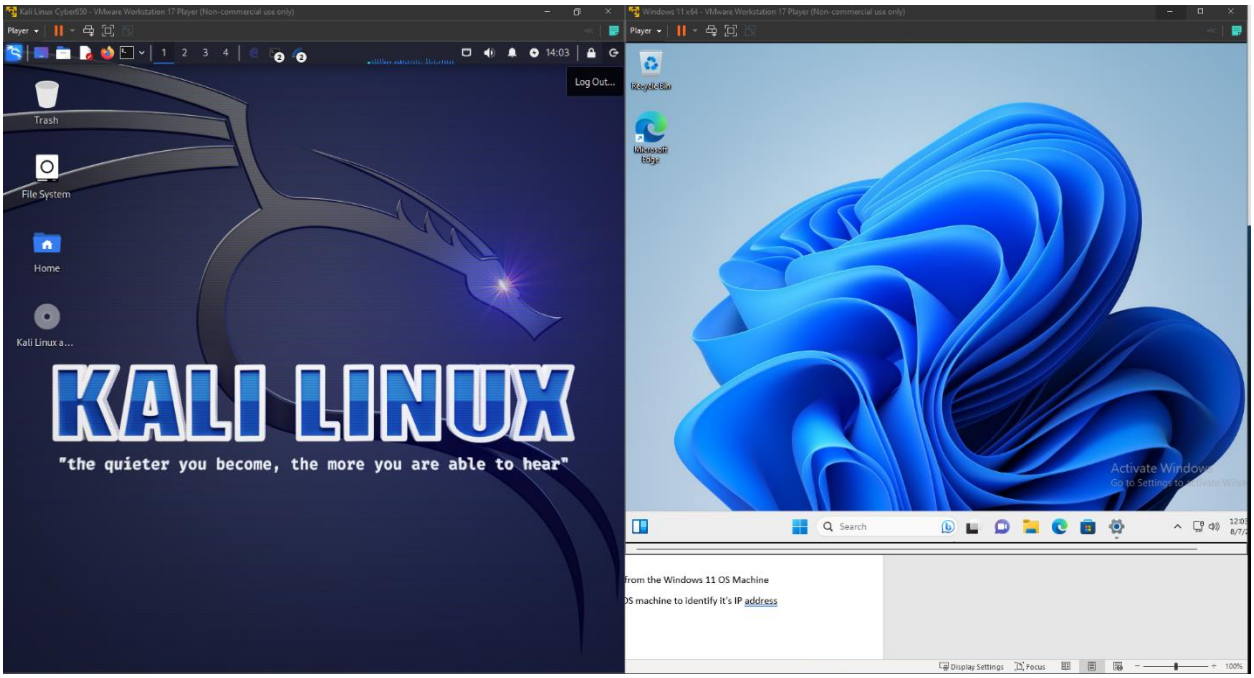
As mentioned previously MITM attacks have several ways that they can be executed. Mentioned in the article "Man-in-the-Middle-Attackk: Types and Examples" on fortinent.com MITM attacks can be executed through Email Hijacking, Wi-Fi Eavesdropping, DNS Spoofing, Session Hijacking, Secure Socket Layer (SSL) Hijacking, ARP Poisoning, IP Spoofing, and Stealing Browser Cookies. For this assignment I utilized ARP Poisoning, in ARP Poisoning "the victim's computer is tricked with false information from the cyber criminal into thinking that the

fraudster's computer is the network gateway. As such, the victim's computer, once connected to the network, essentially sends all of its network traffic to the malicious actor instead of through the real network gateway. The attacker then utilizes this diverted traffic to analyze and steal all the information they need, such as personally identifiable information (PII) stored in the browser." (Fortinet, n.d.). Below I will outline how I executed an ARP Poisoning:

1. The man in the middle attack utilized, two virtual machines.

    - Kali Linux OS Machine

    - Windows 11 OS Machine



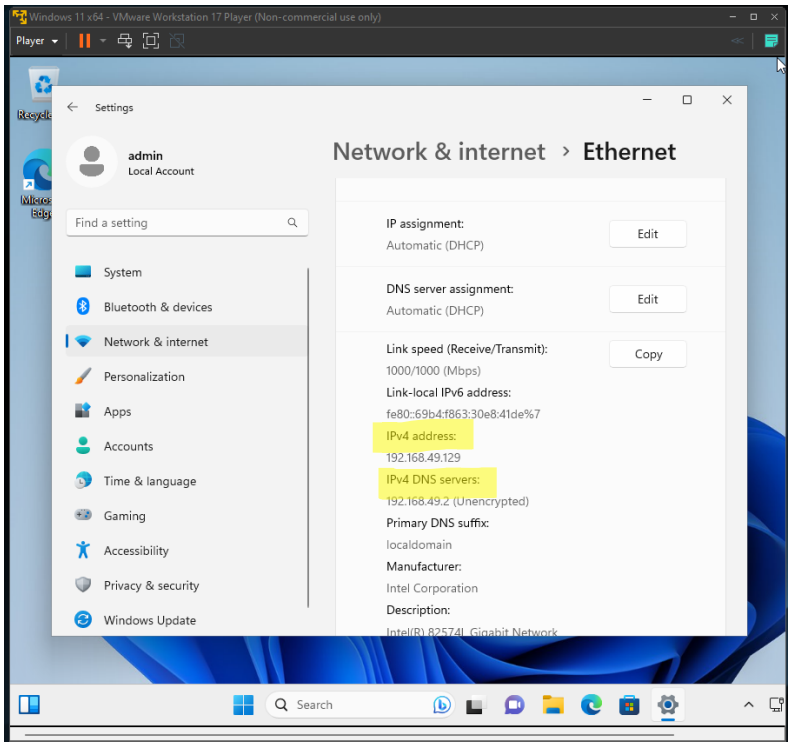
The Dangers and Execution of a Man in the Middle Attack (MITM)

2. On the Kali Linux machine, the following tools were utilized:

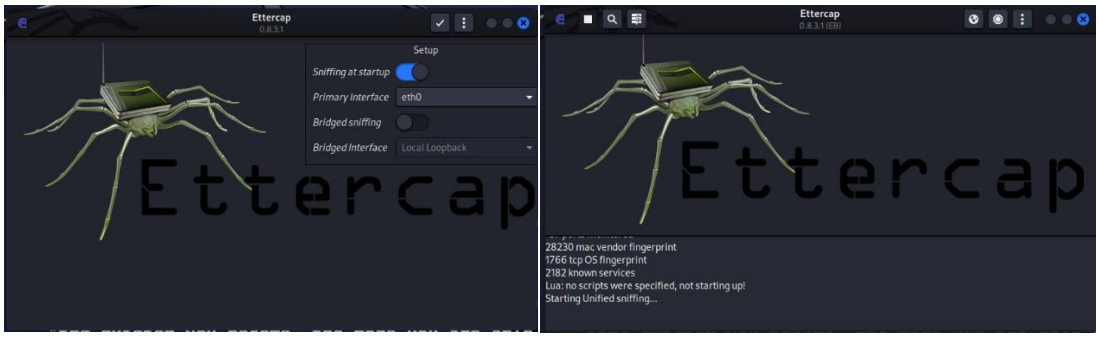
   - Wireshark

   - Ettercap

3. In the settings on the Windows VM the IP address of that system was confirmed.



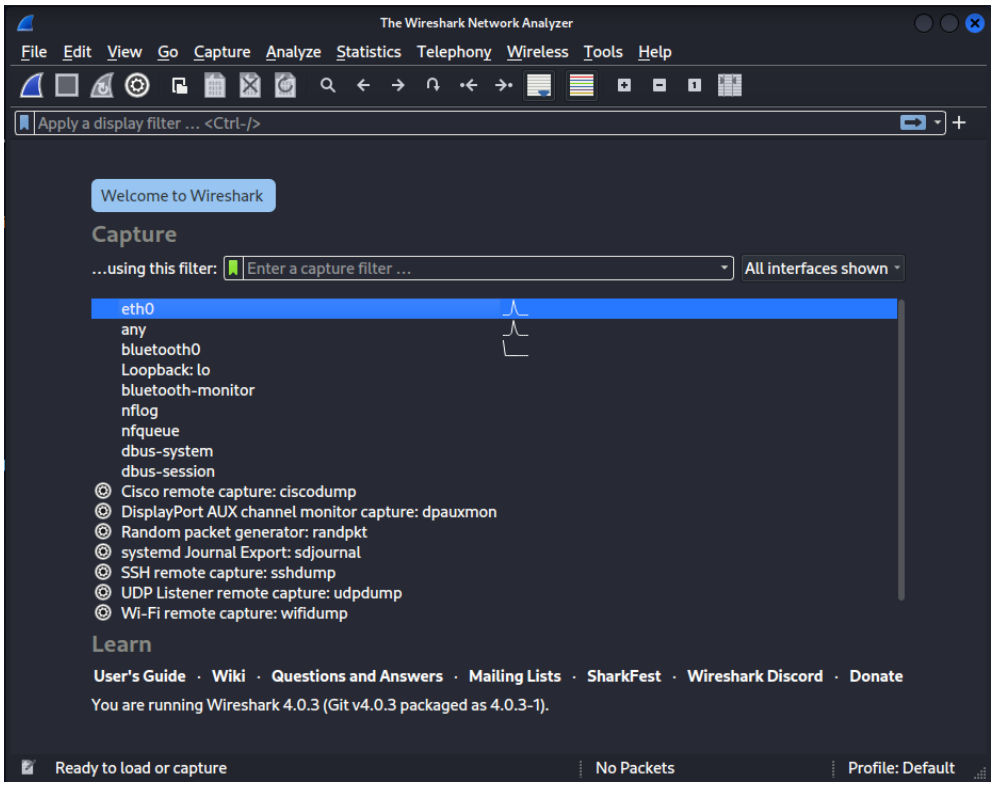
4. Now on the Kali Linux VM “Ettercap” tool was opened.



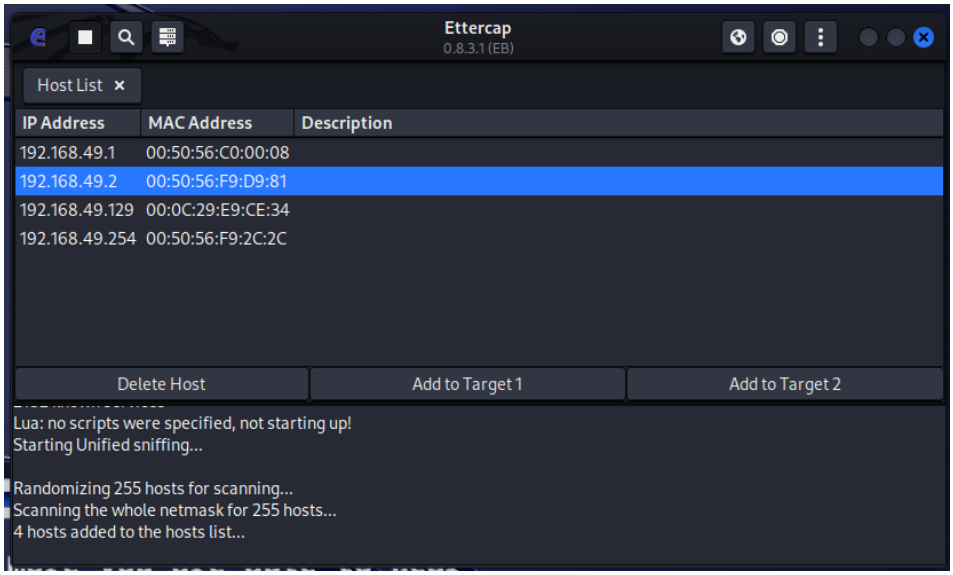
Left Picture: Tool Opening Page- Clicked check mark in upper right corner /

Right Picture: Once check mark is clicked, right image appeared.

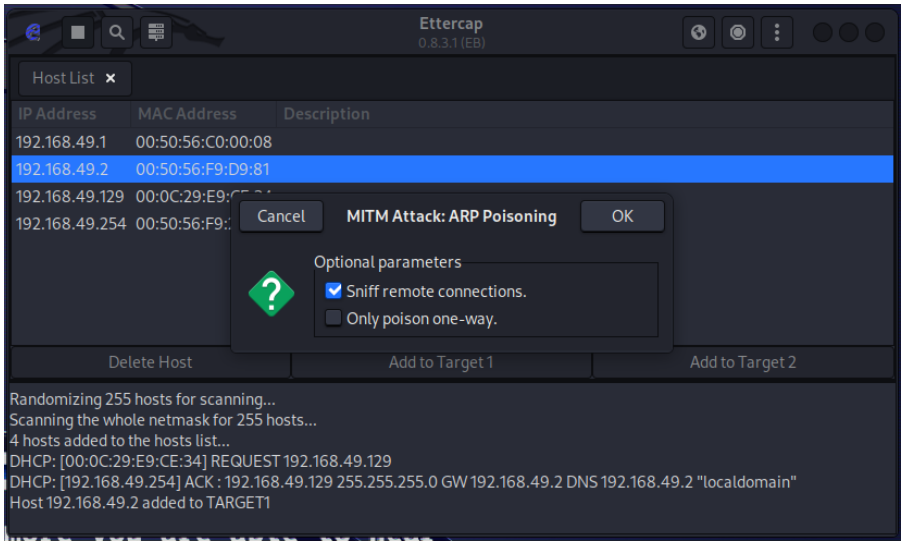
5. Now Wireshark was opened and the sniffing of eth0 is initiated.



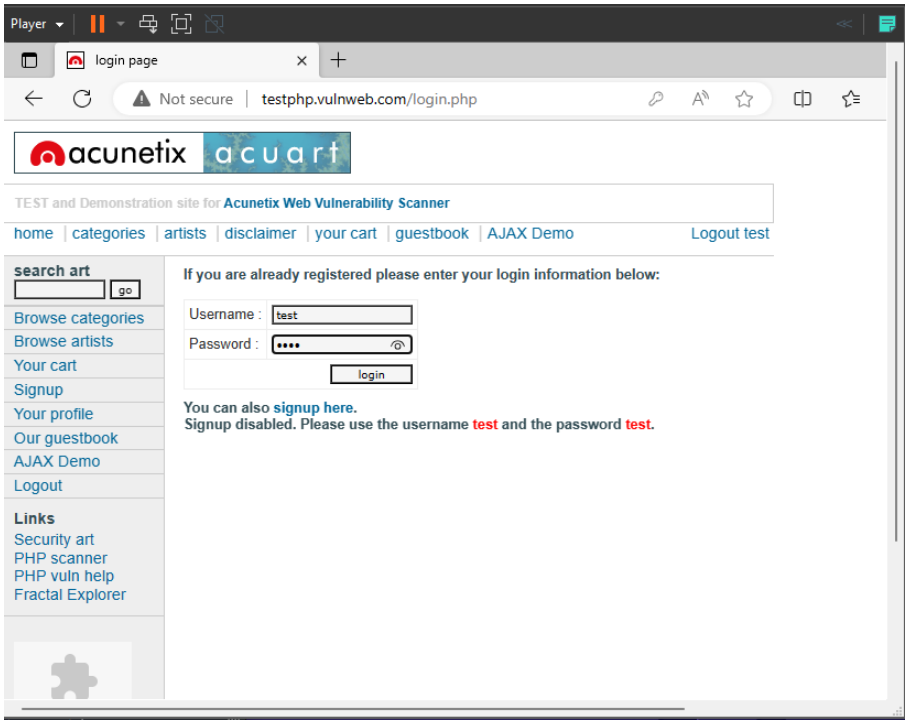
6. Switching back to Ettercap and it picked up the Windows VM mac address on the network which was added as a target by pressing the “Add to Target 1” (Note the IP Address is the same as the one from step 3)



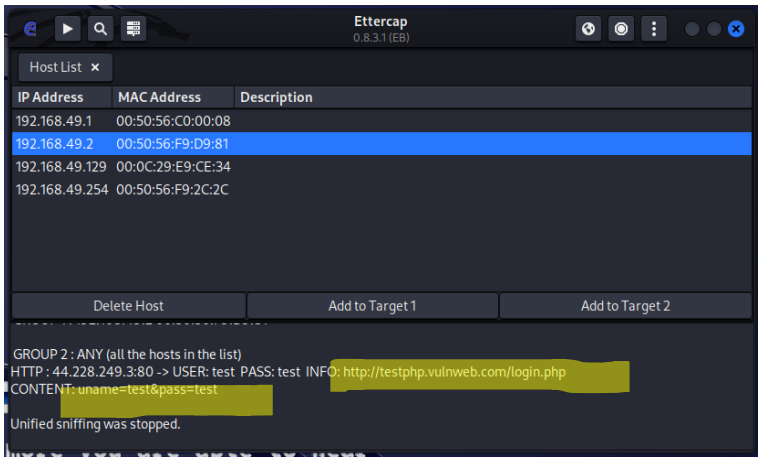
7. Once targeted, the ARP Poison attack initiated. (Now the Windows VM thinks the Kali Linux VM is the Router, and the Router now thinks the Kali Linux VM is the Windows VM)



8. To ensure that the ARP Poison Attack was working a “http” website with a sign-in option was visited on the Windows VM. The login credentials were username: ”test” & password: “test”



9. From there, both the Wireshark and the Ettercap were stopped, and it indeed intercepted the data. It collected the website URL as well as the username and password.



In conclusion, the Man in the Middle Attack was successful, and I see how dangerous it can be especially due to my limited experience and the ease of use of the tools provided. There is no question that MITM Attacks can lead to Loss of Sensitive Data, Data Manipulation, Compromised Authentication, Unauthorized Access to Systems, Denial of Service Attacks, and Malware Infections and the ARP Poisoning Demo showed conclusive evidence of that.

Resources

Conti, Mauro & Dragoni, Nicola & Lesyk, Viktor. (2016). A Survey of Man in the Middle Attacks. IEEE Communications Surveys & Tutorials. 18. 1-1. 10.1109/COMST.2016.2548426.

Man-in-the-Middle Attack: Types and Examples. (n.d). Fortinet https://www.fortinet.com/resources/cyberglossary/man-in-the-middle-attack

Man-in-the-Middle Attacks: Strategies for Prevention(n.d.) Fraud https://www.fraud.com/post/man-in-the-middle-attacks

Swinhoe, D. (2022, March 23) [Man-in-the-middle (MitM) attack definition and examples]. CSO Online. https://www.csoonline.com/article/566905/man-in-the-middle-attack-definition-and-examples.html

Chris, G. [Chris Greer]. (2021, December 9). How ARP Poisoning Works // Man-in-the-Middle [Video]. YouTube. https://www.youtube.com/watch?v=cVTUeEoJgEg&t=1s

[Ubuntu Maniac]. (2022, February 4) Man in the Middle Attack MITM Using Wireshark and Ettercap | Full Tutorial For Beginner 2022 [Video]. YouTube. https://www.youtube.com/watch?v=DElzWHWDG9Q