**Study on Eavesdropping and Session Hijacking Attacks**

Naga Venkata Sai Sudheer Bandaru, MS in Cybersecurity, University of North Texas

Dharma Teja Kollipara, MS in Cybersecurity, University of North Texas

Akhil Kalyanam, MS in Cybersecurity, University of North Texas

Sai Deekshith Mulakala, MS in Cybersecurity, University of North Texas

*Abstract*—Eavesdropping and session hijacking attacks are Wireless network attacks. These attacks can be both passive and active. This report describes how eavesdropping and session hijacking attacks are performed and prevention methods of these attacks.

Keywords—Eavesdropping, Session Hijacking, Packet capturing,

# introduction

Wireless attacks are categorized into two types of namely active attacks and passive attacks. Eavesdropping can be both active and passive. In active eavesdropping, the attacker acts a legitimate user or a gateway router and gain access to the user’s information. In passive Eavesdropping, attacker sniffs on the users traffics and can find passwords to the websites whose data is transferring in plain text.

Session Hijacking takes place when an attacker gets access to the user’s session and gain private or financial information of the user. There are different methods for performing a session hijacking attack. Downgrading HTTPS to HTTP is a famous attack and easy perform by the attacker. Downgrading attacks can be man-in-the middle(MITM) attack. Hence it is an active attack.

# Method

## Performing an eavesdropping attack

### The first thing to do when performing a eavesdropping attack is to enable packet forwarding. It can be enabled by using “echo 1 > /proc/sys/net/ipv4/ip\_forward”. Enabling packet forwarding helps in forwarding the victim network packets to the gateway router and from the gateway router to the victim. In this way attacker acts as a middle man.

### ARP Spoofing: Address Resolution Protocol which is short for ARP helps in finding the appropriate device to which an user is trying to communicate. Due to the nature of ARP protocol, when a user wants to connect with other user or to the internet, ARP requests are sent out to all the devices in the network. So the requested device will unicast it’s MAC address along with it’s IP address in the ARP reply. Attacker send the ARP replies as a ligitimate gateway router by spoofing the ARP request of a user. Then the user thinks as it is a legitimate devices and adds it to the ARP cache. This is known as ARP poisoning. From now victims traffic is routed through the attacker machine.

### After performing ARP poisoning victims traffic is seen in the attackers machine by using any packet analyzer. URLSnarf is a tool that captures the url’s which a victim is browsing from his machine. Sometimes attacker gains access to the user credentials, if a website is using http protocol to transfer data.

### In the same way attacker can view the images of the website which a user is surfing through. Driftnet is a tool which gets the images from the website viewing by the victim.

### To automate this attack, a tool named Eavesdropper is being written, which enables packet forwarding, ARP poisoning and captures the images and url’s visited by the victim.

Text

Description automatically generated

**Figure 2.1: Eavesdropper tool Script**

## **Performing a Session Hijacking attack:**

TTP’s are the most important aspects of offensive security. Tactics, Techniques, Procedures contained in TTP’s.

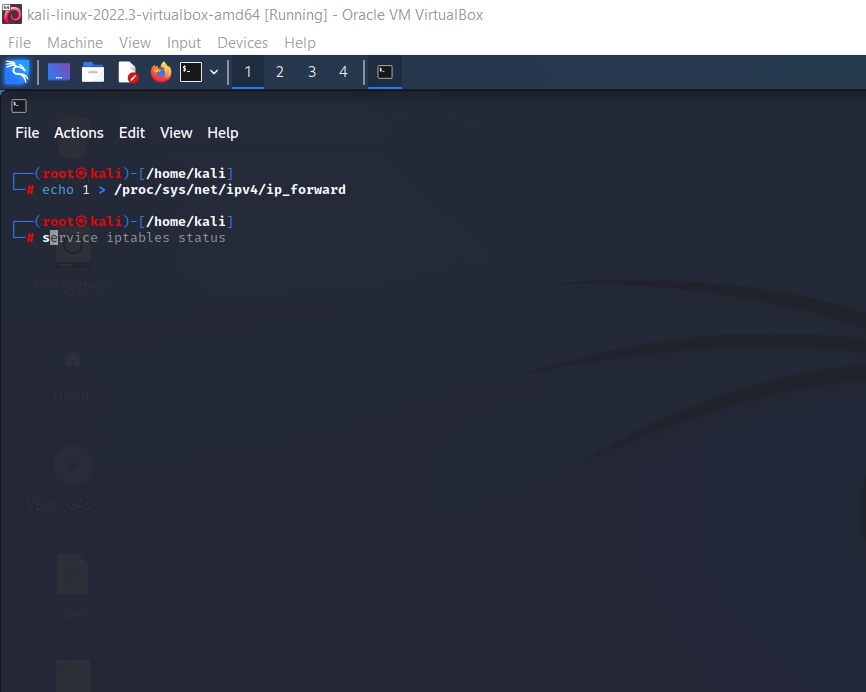
Today we are performing a session hijacking attack.

**Tactics** we are using today is Man in the middle and security downgrading of a website.

**Techniques** we are using are ARP Poisoning and SSL Stripping.

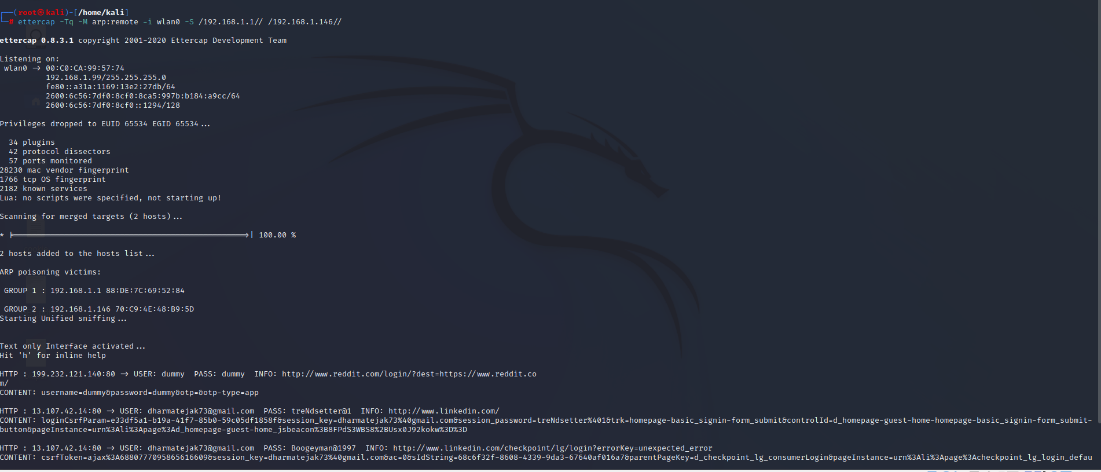
**Procedure**:

### 1) First, we enable the packet forwarding by “echo 1 > /proc/sys/net/ipv4/ip\_forward” command.



**Figure 2.2: IP packet Forwarding**

2) To do ARP poisoning we are using ettercap and this will display the stolen credentials.

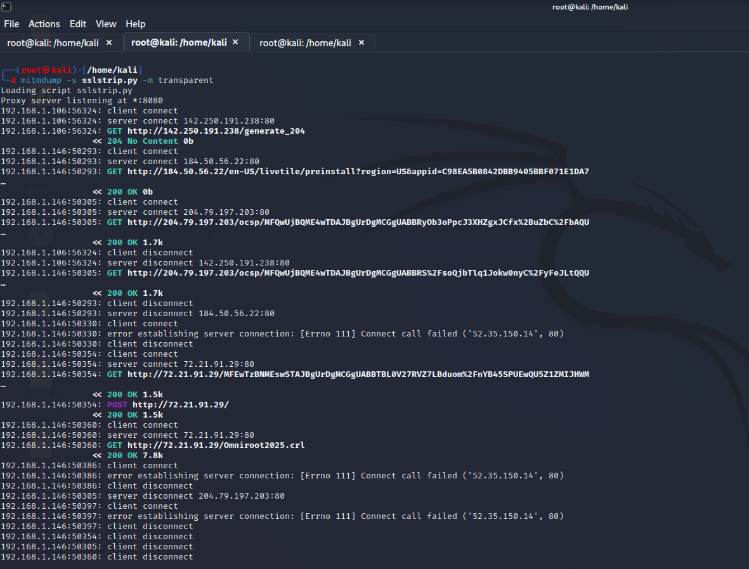


**Figure 2.3: ARP Poisoning using Ettercap**

3) To perform SSL Stripping we are using MITM dump tool and SSL stripping script.

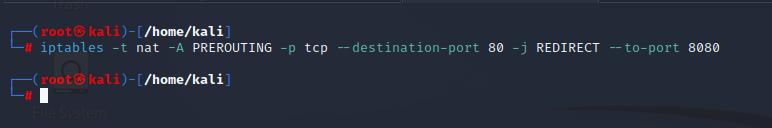
Mitmdump –s sslstripping.py -m transparent.

Here –s flag indicates next to it is script and –m flag indicates mode of transparent to not to change settings in victim machine. Mitmdump is the proxy for http and https.



**Figure 2.4: SSL Stripping**

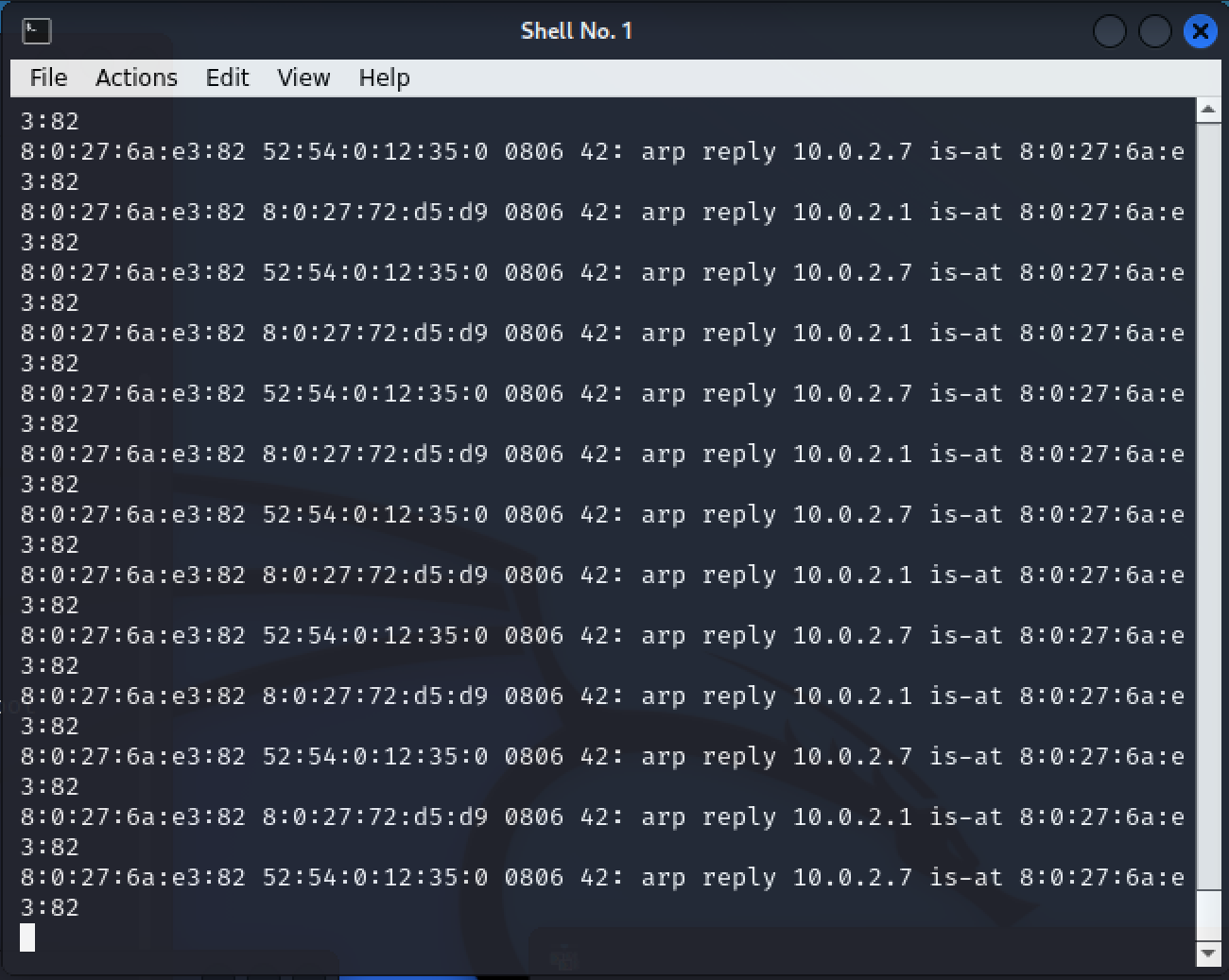
4) We used iptables to do traffic redirect from port 80 to port 8080.



**Figure 2.5: Configuring iptables**

# ATTACK Analysis

#### Eavesdropping Attack result analysis:

The Successful eavesdropping attack using eavesdropper gives the url’s and images of the visited websites. But if the website is securely built, the attacker cannot access the images. The below image shows the arp spoofed replies.

**Figure 3.1: ARP Poisoning**

A screenshot of a computer

Description automatically generated with medium confidenceThe ARP tables of the victim will change after ARP Spoofing by the attacker. Below figure shows the ARP tables before and after attack.

**A screenshot of a computer

Description automatically generated with medium confidenceFigure 3.2: ARP table of victim machine before attack**

**Figure 3.3: ARP table of victim machine after attack**

Text

Description automatically generatedThe below terminal window shows the urls along with the time when a user is accessing it. This lets the attacker know what victim is browsing through the internet and it is great for open-source intelligence on the victim.

**Figure 3.4: Captured urls by urlsnarf**

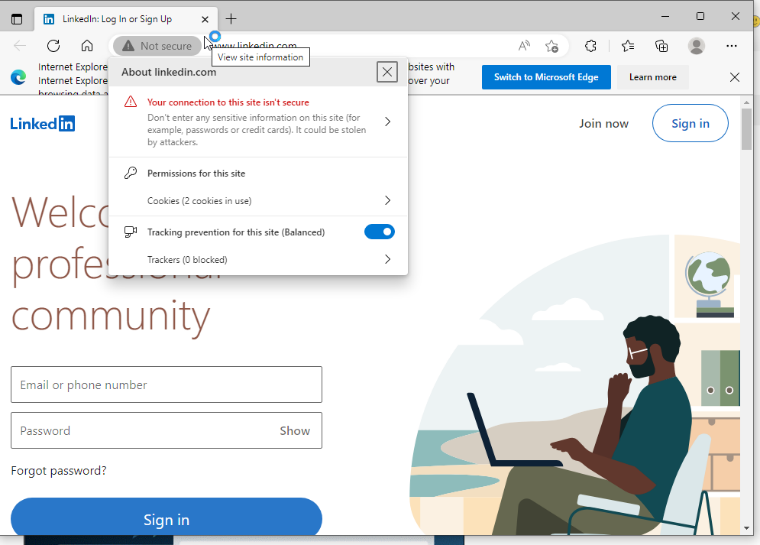
The below terminal window shows the images captured by driftnet. It has captured the logos and images.

Graphical user interface, website

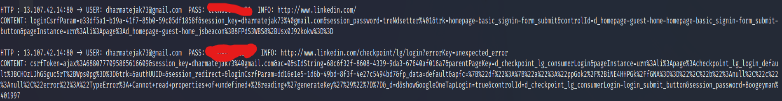
Description automatically generated

**Figure 3.5: images captured using driftnet**

1. Session Hijacking Attack result analysis:



**Figure 3.6: Browser showing website is not secure after ssl stripping**

By the above result we downgraded the result status of a website to https to http using ssl stripping.

**Figure 3.7: Captured credentials of LinkedIn**

# Discussion and conclusions

Due to the weakness in ARP protocol, it allows ARP spoofing. Even if the attacker be able to perform the ARP Poisoning, data should not be leaked. One can achieve this by using secured networks. Network segmentation will prevent from eavesdropping. Because of the restricted access to the network one can prevent eavesdropping.

Creating awareness and using best security practices can also prevent from data loss and data theft. By doing network log analysis and network monitoring there is a minute chance of detecting eavesdropping attacks.

Root cause analysis of session hijacking:

This attack is caused because of the ARP poisoning and poor or no configuration of HSTS (HTTP strict transport security).

##### References

1. N. Tripathi and B. M. Mehtre, "Analysis of various ARP poisoning mitigation techniques: A comparison," 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014, pp. 125-132, doi: 10.1109/ICCICCT.2014.6992942.
2. Corey Nachreiner, WatchGuard Network Security Analyst, “ Anatomy of ARP Poisoning Attack”, 2012 WatchGaurd.
3. X. Hou, Z. Jiang and X. Tian, "The detection and prevention for ARP Spoofing based on Snort," 2010 International Conference on Computer Application and System Modeling (ICCASM 2010), 2010, pp. V5-137-V5-139, doi: 10.1109/ICCASM.2010.5619113.
4. S. Y. Nam, D. Kim and J. Kim, "Enhanced ARP: preventing ARP poisoning-based man-in-the-middle attacks," in IEEE Communications Letters, vol. 14, no. 2, pp. 187-189, February 2010, doi: 10.1109/LCOMM.2010.02.092108.
5. Anuj Kumar Baitha, Prof. Smitha Vinod, “Session Hijacking and prevention techniques”, International Journal of Engineering & Technology, 2018.
6. J. Clark and P. C. van Oorschot, "SoK: SSL and HTTPS: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancements," 2013 IEEE Symposium on Security and Privacy, 2013, pp. 511-525, doi: 10.1109/SP.2013.41.
7. Qing Huang, University of California, Irvine; Deliang Chang, Tsinghua University; Zhou Li, “A Comprehensive Study of DNS-over-HTTPS Downgrade Attack”, University of California, Irvine.
8. Eman Salem Alashwali, Pawel Szalachowski, Andrew Martin, Exploring HTTPS security inconsistencies: A cross-regional perspective, Computers & Security, Volume 97, 2020, 101975, ISSN 0167-4048, <https://doi.org/10.1016/j.cose.2020.101975>.
9. Y. Zou, J. Zhu, X. Wang and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," in Proceedings of the IEEE, vol. 104, no. 9, pp. 1727-1765, Sept. 2016, doi: 10.1109/JPROC.2016.2558521.
10. S. Balakrishnan, P. Wang, A. Bhuyan and Z. Sun, "Modeling and Analysis of Eavesdropping Attack in 802.11ad mmWave Wireless Networks," in IEEE Access, vol. 7, pp. 70355-70370, 2019, doi: 10.1109/ACCESS.2019.2919674.

Github: <https://github.com/bandarusudheer/Eavesdropper> (all members are added in this repository)