**CSE3501 - Information Security Analysis and Audit**

**“Man in the middle attack implementation and prevention”**

Aayushi Jethani - 19BCE0101 Pratishta Gaur - 19BCE01014 K Arjun Rao - 19BCE2401

**School of Computer Science and Engineering, VIT University**

**Under the guidance of**

Prof. Chandra Mohan B.

****

**DECEMBER 2021**

**Table Of Contents**

#### 

### **1. ABSTRACT**

### 

### **2.** **INTRODUCTION**

**2.1. OBJECTIVE**

**2.2. MOTIVATION**

### **3.** **LITERATURE SURVEY**

### 

### **4.** **PROPOSED SYSTEM**

### 

### **5.** **ALGORITHM**

### 

### **6.** **DESIGN**

### 

### **7.** **RESULTS AND DISCUSSION**

### 

### **8.** **CONCLUSION**

**APPENDIX-A(CODE SNIPPET)**

1. **ABSTRACT**

Today with the rush of technology and everybody using the internet, opportunities for attackers have increased. Cybercrime has become a hotly debated issue. Cyberattacks violate individuals' privacy and the security of their data, particularly hacking, malware, identity theft, financial fraud, medical fraud, without individuals' consent. It is important to protect ourselves from such crimes, and use prevention measures to protect ourselves from cybercrime. We have to be aware of the crimes and the attacks in-depth to solve them. One will notice various kinds of attacks over the internet some being, SQL injection, DDoS attack, Cross-site scripting and Man in the middle(MITM) attack. Here we would try to understand MITM attacks by implementing a few of its kinds and thus trying to prevent them. The man-in-the-middle-attack is a kind of cyberattack where an unapproved outsider enters into an online correspondence between two users. MITM attack as a protocol is subjected to an outsider inside the system, which can access, read and change secret information without keeping any trace of manipulation. Hence, a MITM attack is one of the most dangerous and effective attacks that one can carry out in a network.

### **INTRODUCTION**

**2.1. OBJECTIVE**

MITM assault is an overall term for when a culprit positions himself in a discussion between a client and an application. Causing it to show up as though a typical trade of data is in progress. The objective of an assault is to take individual data, for example, login qualifications, account subtleties and Visa numbers.The initial step captures client traffic through the assailant's organization before it arrives at its expected destination.After block attempt, any two-way SSL traffic should be decoded without alarming the client or application. Different Man in the Middle assaults are completed by aggressors which include: The assailant introduces a parcel sniffer to investigate network traffic for uncertain interchanges. At the point when a client signs in to a site, the assailant recovers their client data and sidetracks them to a phony site that mirrors the genuine one. The aggressor's phony site accumulates information from the client, which the assailant would then be able to use on the genuine site to get to the objective's data. Sidejacking - An aggressor sniffs information parcels to take meeting threats from your gadget, permitting them to seize a client meeting assuming they find decoded login data. Malicious Twin - An aggressor copies a genuine Wi-Fi organization, empowering them to block information from clients who accept they are marking on the genuine organization.

**2.2 MOTIVATION**

We all have been victim to some type of online attacks so our motivation to implement 2 attacks and 1 prevention technique emerged from the common experience of getting our data stolen in some way or form. The attackers target the actual data flowing between the endpoints and compromise the integrity and confidentiality of the data.One of the advantages of the tool that is designed in this journal is that the tool does not require high fees for third party software and provides the users with flexibility in taking measures against MITM attacks using ARP spoofing technique. So our responsibility as good netizens is to understand the atack and also find a way of preventing the attack. Hence we are doing this.

### **LITERATURE SURVEY**

| Sr | Title | Description | Inference |
| --- | --- | --- | --- |
| 1 | Man in the middle attack in wireless and computer networking- a review (IEEE 2017) | * MITM attacks have been classified based on various parameters such as attacker location, impersonation techniques and nature of channel and the existing countermeasures are surveyed. * The paper categorizes MITM attacks into four categories namely spoofing based MITM, TLS/SSL MITM, BGP MITM and false base station based MITM attack. * Various MITM defence mechanisms such as Entropy increasing mechanisms, cryptographic solutions have also been presented. | The attackers target the actual data flowing  between the endpoints and compromise the integrity and confidentiality of the data. |
| 2 | The SSL MITM Attacks with DNS Spoofing (Trans Tech Publications, Switzerland 2013) | * SSL provides a transparent encryption transmission channel between user browser and website * server but has become the most effective way to implement SSL attack, as a result of security * leaks caused by certificate validation of browser, user negligence and the website server * architecture. In this paper, SSL MITM attack combined with DNS spoofing has been performed * to analyse the security about user account login. | * The results show that attention needs to be paid to the improvement of network security. * It emphasizes that network service providers should take measures to improve data security, such as safe hash calculation about user account and password information referring to data on web pages and data submitted by the user. * It highlights that safe DNS service needs to be used to prevent ID spoofing or the injection attack. |
| 3 | A study of Cookies and threats to Cookies (International Journal of Advanced Research  in Computer Science and Software Engineering 2016) | * One of the main threats to the network is session hijacking which can be carried out with the help of cookie exploitation. There are many websites which are vulnerable to cookie theft. In this paper, various methods to steal the cookies which are used by the attacker have been discussed. * It also explains the working of cookies to give a clear idea about Session hijacking which deals with cookies. | * Remedy for Sniffing Network Traffic for Cookies: Using a long number or string instead of a small number or string as the session key. So, an attacker is not able to brute force the session-id. * Remedy for Cross-Site Scripting Attack: Filtering i.e. passing external data through a filter which would remove the dangerous keywords. Also, escaping dangerous character with the help of escaping characters can serve as a solution. * Remedy for Cross-site request forgery (CSRF) Attack: Using a Synchronizer token pattern. |
| 4 | Man in the middle attacks detection tool design (International Journal of Engineering  Sciences and Research Technology 2018) | * In this study their aim was to create a MITM detection tool which detects ARP spoofing attacks on LANs. * This attack can induce a high level of threats on the targets and so it is crucial to be protected against this type of attack. * This study suggests a better perspective to the users, software developers and security administrators about the key features of the MITM detection tool that can be used as a solution. * Some of the ARP spoofing detection methods that are mentioned in this journal are:   + Using static ARP tables   + Secure ARP(S-ARP)   + Ticket based ARP(TARP) | * One of the advantages of the tool that is designed in this journal is that the tool does not require high fees for third party software and provides the users with flexibility in taking measures against MITM attacks using ARP spoofing technique. * Just like honeypot * The tool which the authors developed detected MITM attacks rather quickly and efficiently. |
| 5 | Mitigating ARP poisoning-based man-in-the-middle attack in wired or wireless LAN  (EURASIP journal on wireless communications and networking 2012) | * In this paper, an enhanced version of address resolution protocol (ARP) is proposed to prevent ARP poisoning-based man-in-the-middle (MITM) attacks in wired or wireless LAN environments. * The proposed scheme is based on two key concepts: long term IP/MAC mapping table and computational puzzle-based voting. * The ARP poisoning attack refers to the behaviour of registering a false (IP, MAC) address mapping in the ARP cache of another node for malicious purposes. * The proposed mechanism is based on the idea that when a node knows the correct MAC address for a given IP address, if it does not delete the mapping while the machine is alive | * In this paper, an enhanced version of address resolution protocol (ARP) is proposed to prevent ARP poisoning-based man-in-the-middle (MITM) attacks in wired or wireless LAN environments. * The proposed scheme is based on two key concepts: long term IP/MAC mapping table and computational puzzle-based voting. * The ARP poisoning attack refers to the behaviour of registering a false (IP, MAC) address mapping in the ARP cache of another node for malicious purposes. * The proposed mechanism is based on the idea that when a node knows the correct MAC address for a given IP address, if it does not delete the mapping while the machine is alive |

### 

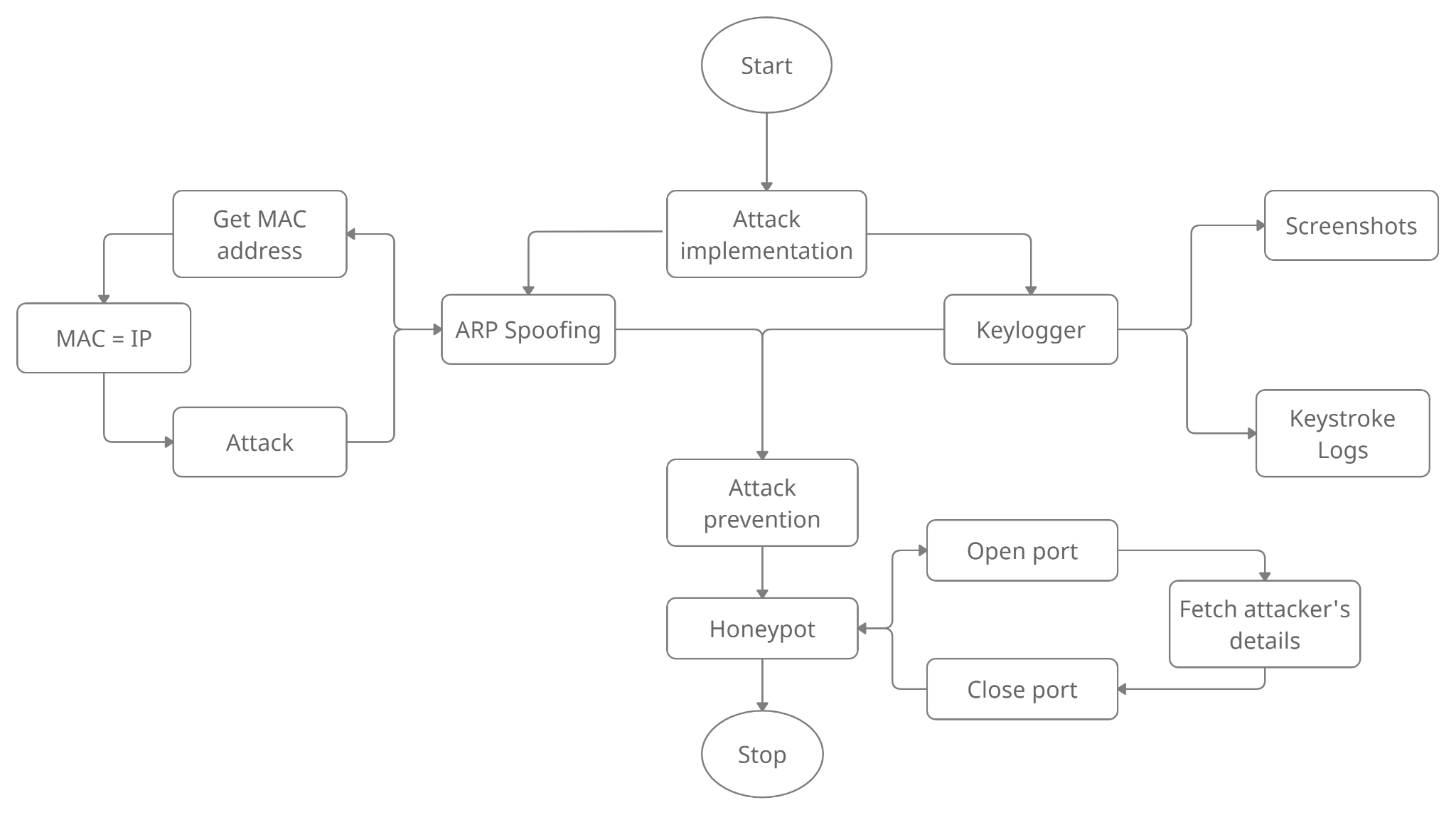
### **ALGORITHM/TECHNICAL SPECIFICATION**

### **Arp spoofing**

* + The attacker opens an ARP spoofing tool and sets the tool’s IP address to match the IP subnet of a target.
  + The attacker uses the ARP spoofing tool to scan for the IP and MAC addresses of hosts in the target’s subnet.
  + The attacker chooses its target and begins sending ARP packets across the LAN that contain the attacker’s MAC address and the target’s IP address.
  + As other hosts on the LAN cache the spoofed ARP packets, data that those hosts send to the victim will go to the attacker instead. From here, the attacker can steal data or launch a more sophisticated follow-up attack.
  + After stopping the attack all caches are restored.

1. **Keylogger**
   * Execute keylogger in somebody’s system either manually or through spam mail make them download self executable file
   * In the code define keylogger log format.
   * What all keys should write what in the logs.
   * Frequency with which to take screenshot
   * Define a location in server to where files must be stored
2. **Honeypot**
   * Define a computer you want to protect and trap the hacker using
   * Note its ip address
   * Open a port for attacker to attack
   * Build socket connection when hacker tries to access port.
   * Fetch attackers info and close port and connection.

### **DESIGN**



We basically plan to perform 3 operations. In honeypot, we open a port. And let any attacker form a connection. On connecting, it fetches attacker details and closes the connection and the port. In keylogger, we use python libraries to take screenshots of the attacked pc along with maintaining a log file recording all keystrokes. In arp spoofing we fetch IP and gateway addresses from discovering devices on the network. Perform spoofing command to resolve mac address to IP address then perform any attack one wants to. After spoofing user can use driftnet to get pictures of the host or sniff to fetch packets of the host and so on

**5.1 Tentative demo design**

Inputs:

* IP Address of host machine
* Gateway Address of host machine
* Both attacker and victim have to be on the same network

Outputs:

* In arp implementation mac address of the attacker was resolved as the gateway address
* In keylogger, a text document of everything a user writes after an attack along with a screenshot of everything a user does.
* Honeypot results in finding the IP address of the attacker and the system details of the attacker

### **PROPOSED SYSTEM**

### **6.1 ARP SPOOFING**

### The assailant (programmer) sends manufactured ARP Messages pretending to be a real client as it connects the aggressor machine's MAC Address to the authentic IP Address. In ARP Spoofing, the programmer essentially tricks the passageway and the casualty by imagining as the passage before the person in question and as the casualty before the passage Victim's solicitations presently go through the aggressor's machine rather than the real passage. This allows an opportunity for the aggressor to block, change, or stop the information.

### 

### The aggressor opens an ARP caricaturing instrument and sets the apparatus' IP address to match the IP subnet of an object. The aggressor utilizes the ARP caricaturing instrument to examine for the IP and MAC locations of hosts in the object's subnet. The aggressor picks its objective and starts sending ARP bundles across the LAN that contain the assailant's MAC address and the objective's IP address. As different hosts on the LAN store the ridiculed ARP parcels, information that those hosts ship off the casualty will go to the aggressor, all things considered. From here, the aggressor can take information or dispatch a more complex subsequent assault. Subsequent to halting the assault, all stores are reestablished.

### 

**5.2**  **KEYLOGGER**

A keylogger is a guileful type of spyware. You enter delicate information onto your console, accepting no one is watching. Indeed, keylogging programming is working diligently logging all that you type.Keyloggers are movement observing programming programs that give programmers admittance to your own information. The passwords and Visa numbers you type, the website pages you visit – all by logging your console strokes. The product is introduced on your PC, and records all that you type. Then, at that point, it sends this log record to a server, where cybercriminals hold on to utilize this delicate data.

Executing keylogger in someone's framework either physically or through spam mail cause them to download a self executable document In the code characterize keylogger log design. What keys compose what in the logs. Recurrence with which to take a screen capture. Characterize an area in server to where records should be put away

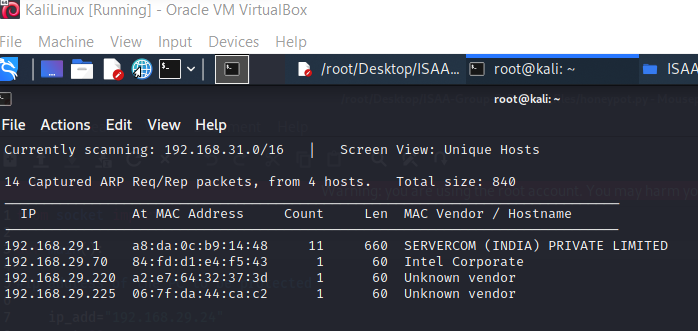
**5.3 HONEYPOT**

A security component that makes a virtual snare to draw aggressors. A deliberately compromised PC framework permits assailants to take advantage of weaknesses so you can concentrate on them to further develop your security approaches. You can apply a honeypot to any figuring asset from programming and organizations to document servers and switches. Characterize a PC you need to secure and trap the programmer utilizing Note its ip address Open a port for an aggressor to assault the Build attachment association when a programmer attempts to get to the port. Bring assailants' information and close ports and associations.

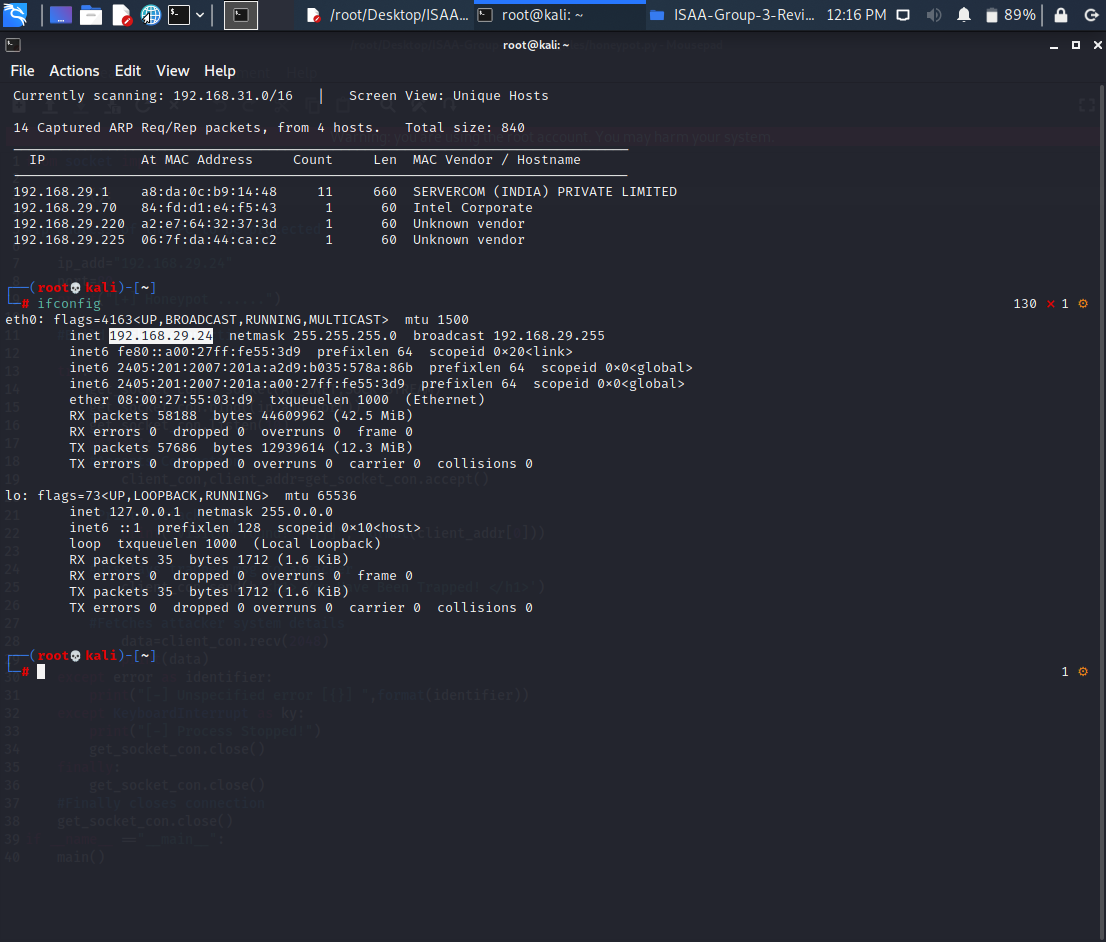
### **6.** **RESULTS AND DISCUSSION**

ARP Spoofing attack

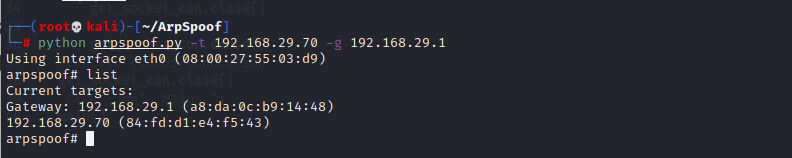
To perform ARP attack we first need to have the IP address and gateway address of the system, now since they are under same network connection gateway is the same but IP address needs to be found out. To gather IP addresses in same network we use a command called netdiscover and choose a IP to be attacked on.



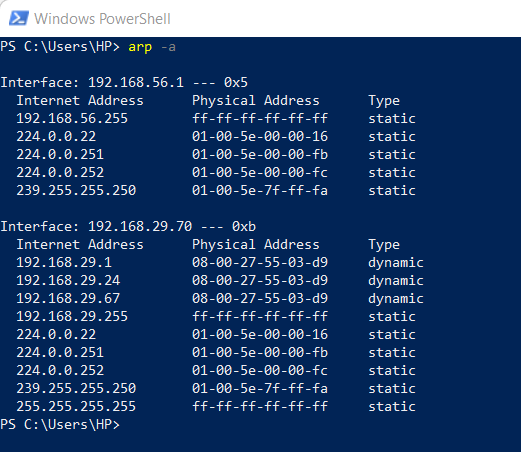
Now on performing ifconfig the gateway address of the network is stored



To run the arpspoof python code we give gateway and attacker ip as argument

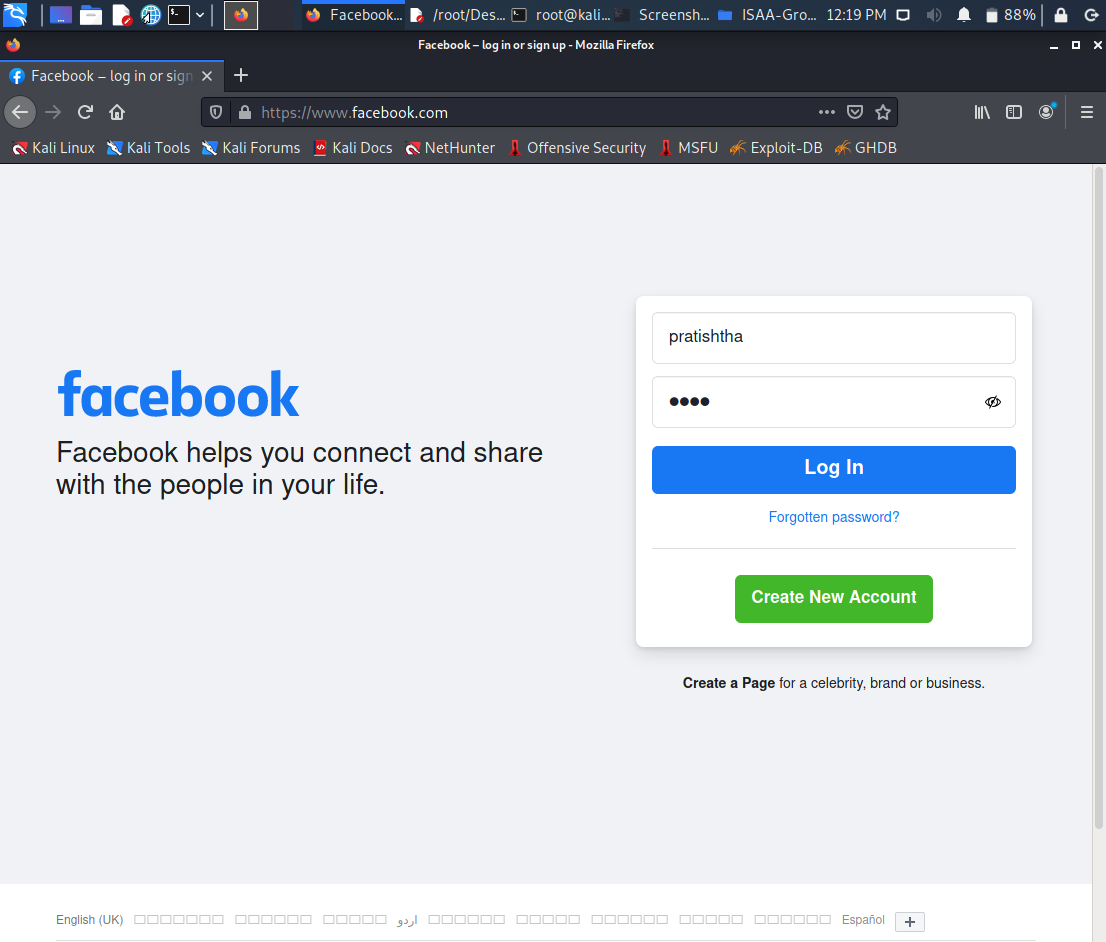


Now if we check the IP address of the System on will observe that the the IP address of attacker system is changed to the same as gateway address now all the packets will be routed to the attacker system along with the gateway.

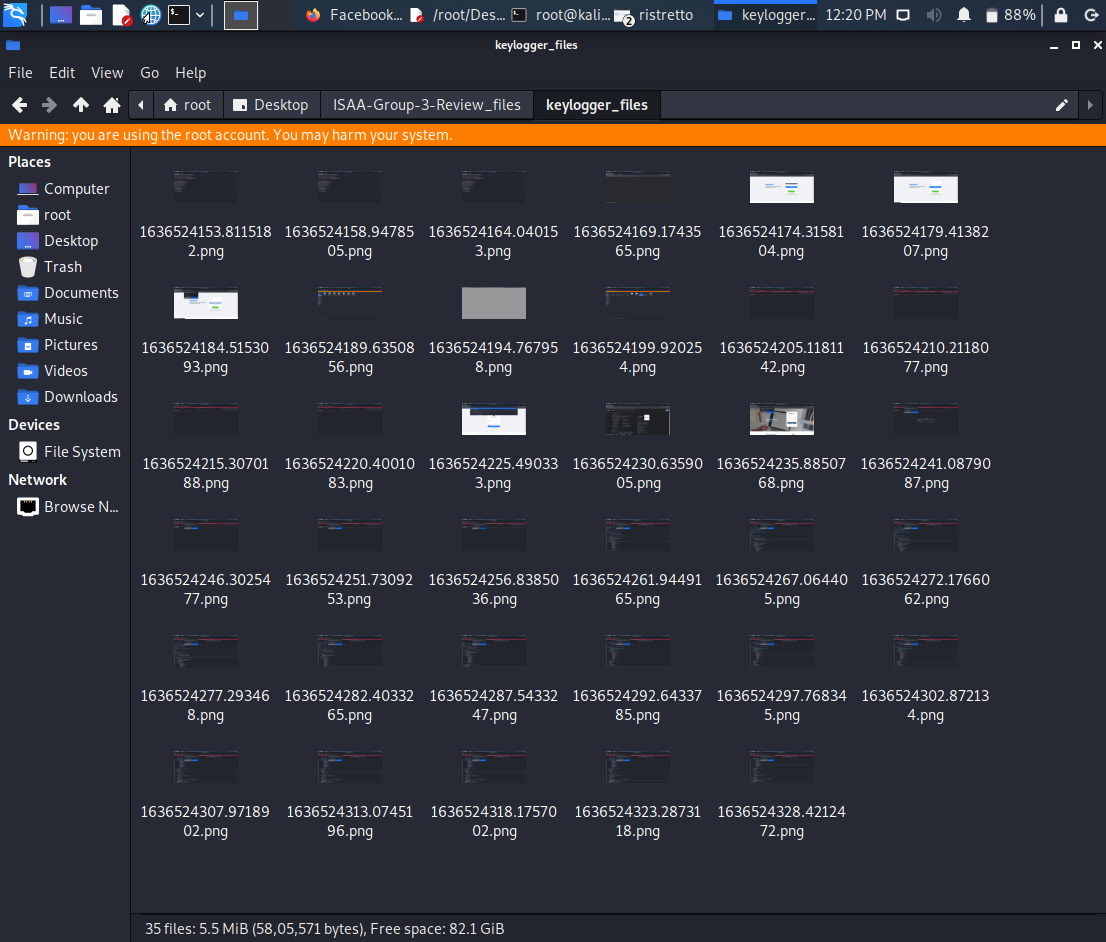


Keylogger attack

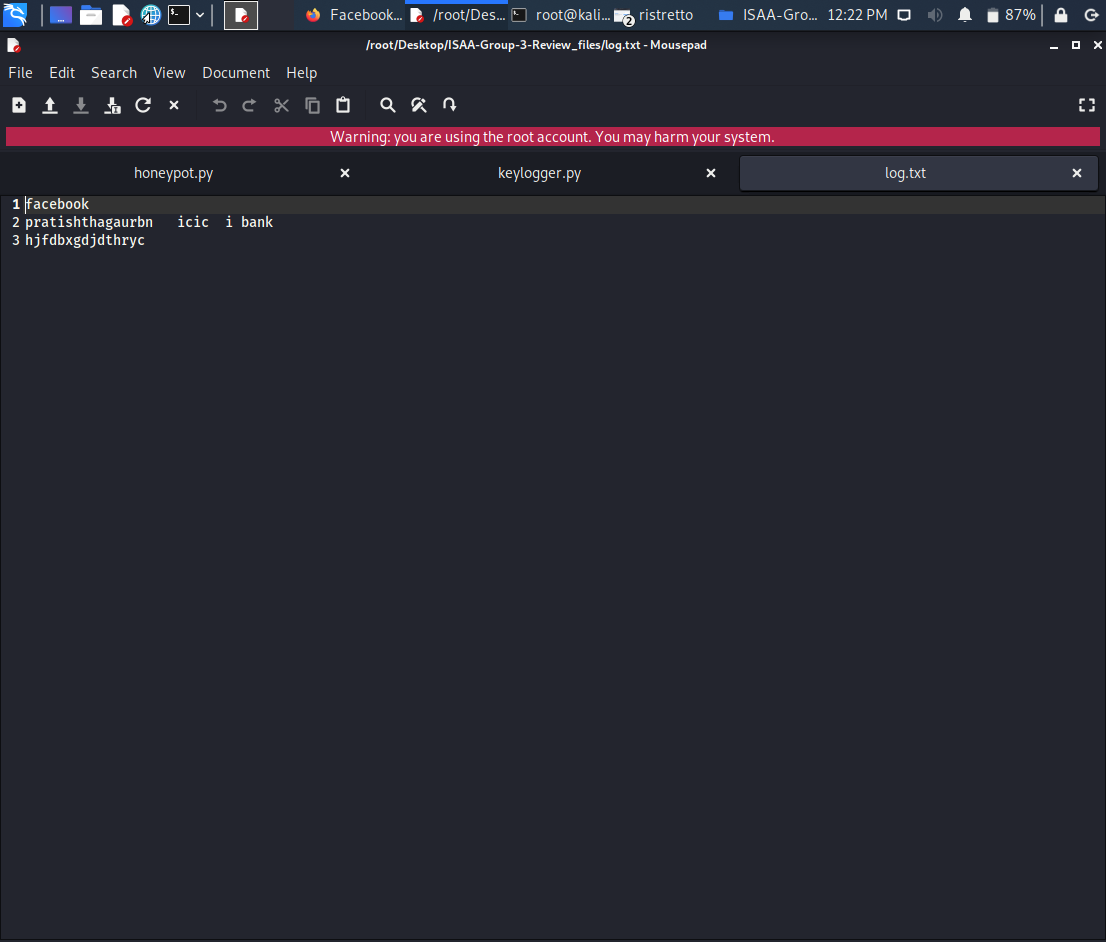
Keylogger attacker takes the screenshot of whatever user performs suppose for demonstrating we log in to the Facebook account then the result would be that the username of the user will be captured in the screenshot.



All the screenshots are saved as the timestamp to note the order of screenshot taken. All these can be stored in any place in the server.

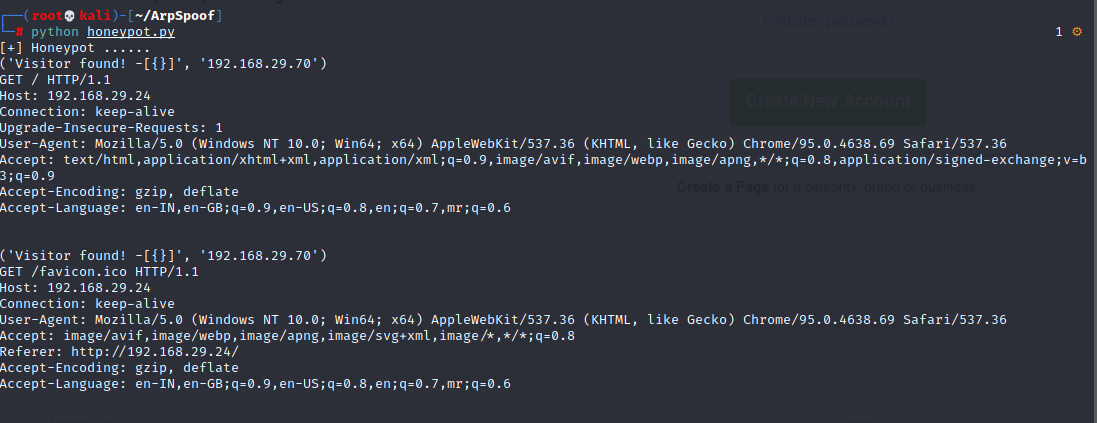


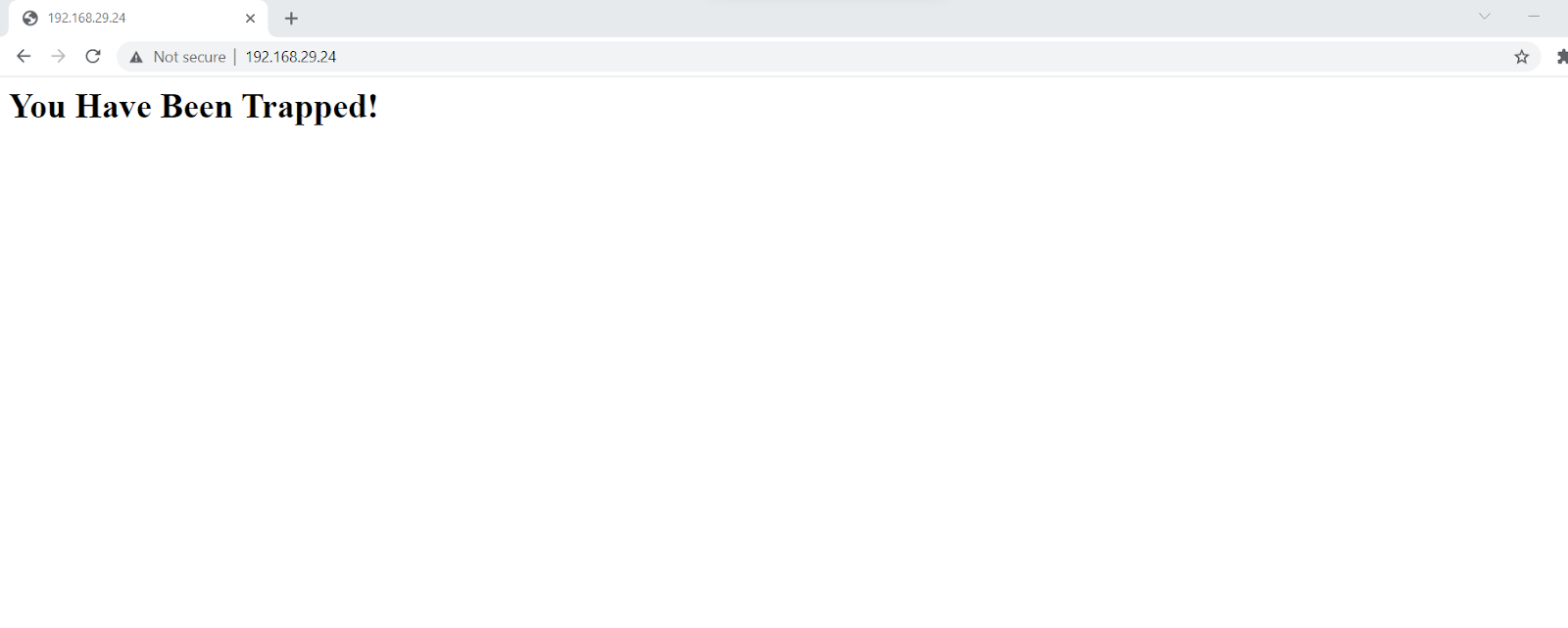
This is the log file that is saved, Now since we first searched the Facebook page Facebook word is recorded and then username and password as well.



Honeypot implementation

Honeypot implementation here results in capturing the details of the attacker, we can clearly see the IP address of the attacker and the connection and browser details.





Dependencies

A few dependencies that have to be implemented before executing the above codes are

* Make a virtual machine for Kali linux
* Connect it as a bridged network to connect through wifi
* Laptop connected with a wifi
* All mss, listener for keylogger to take screenshot
* All socket libraries for honeypot
* Code work in root mode

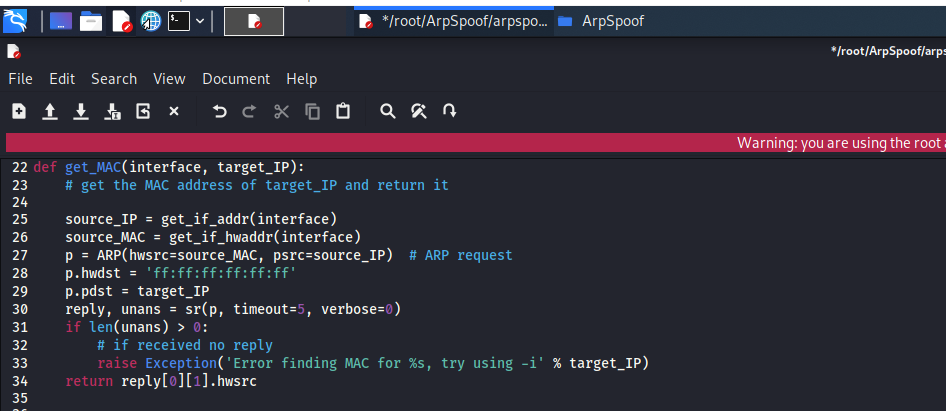
### 

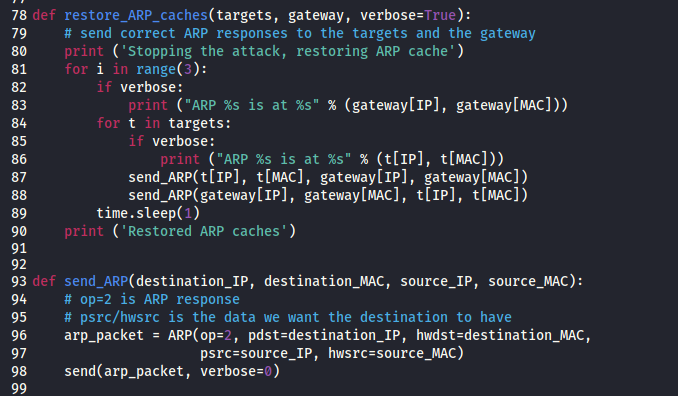
### **7.** **CONCLUSION**

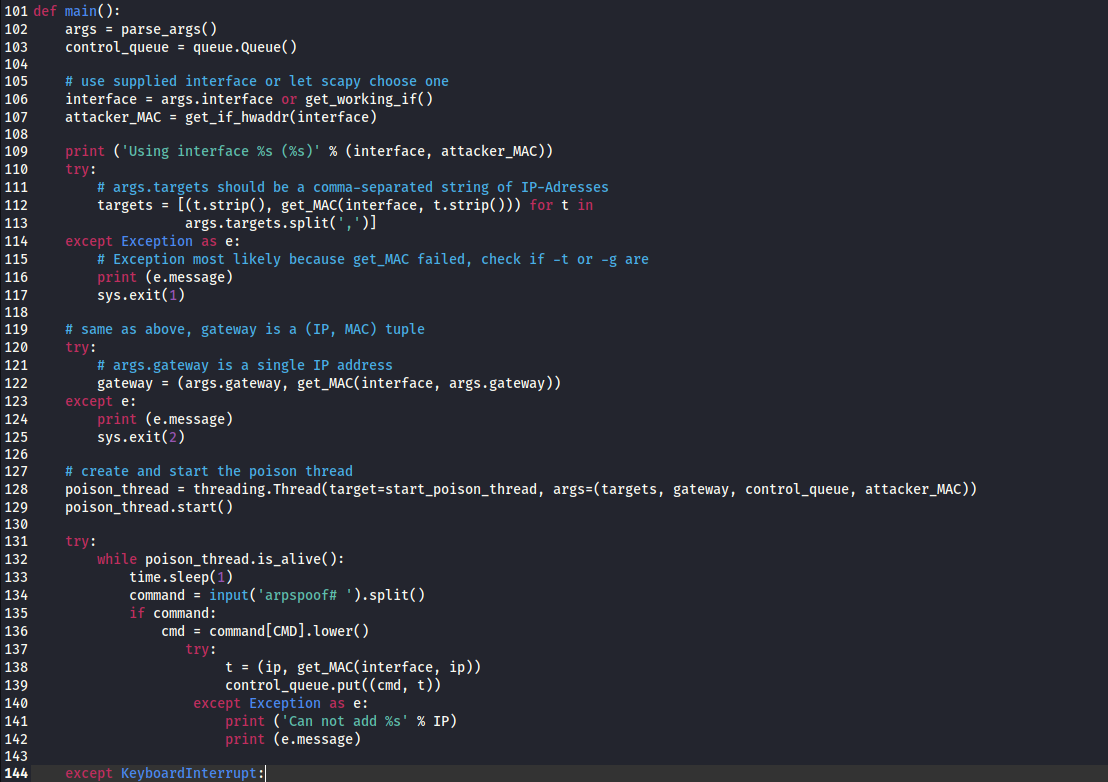
We thoroughly analyzed the various MITM attacks in real-time, successfully implemented MITM attacks with various tools, we also implemented an ARP spoofing attack with our Python code, and we were also able to detect MITM attacks on the target machines. We are implementing a honeypot to protect various websites from MITM attacks. In our Keylogger implementation, we focus on taking real-time system screenshots of the system and also storing the details of the user pressed by the user in a text file.

**APPENDIX-A(CODE SNIPPET)**

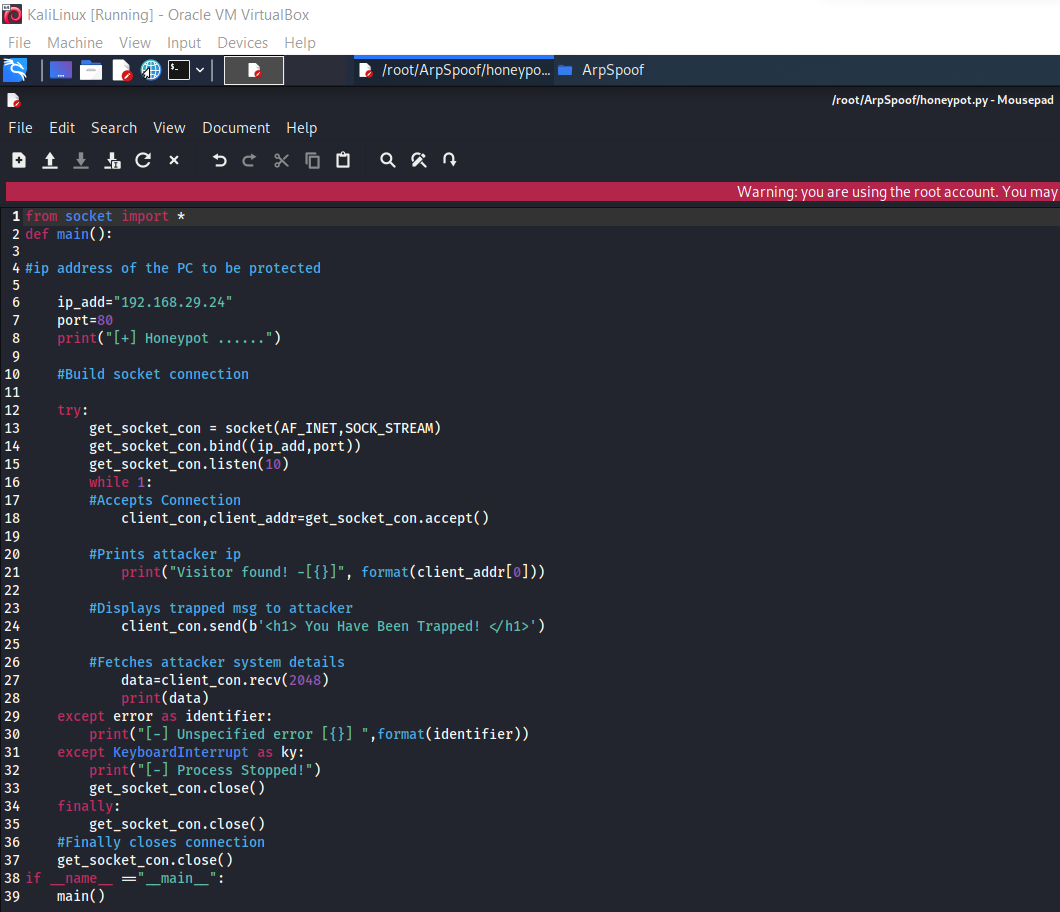
**ARPSpoof**

****

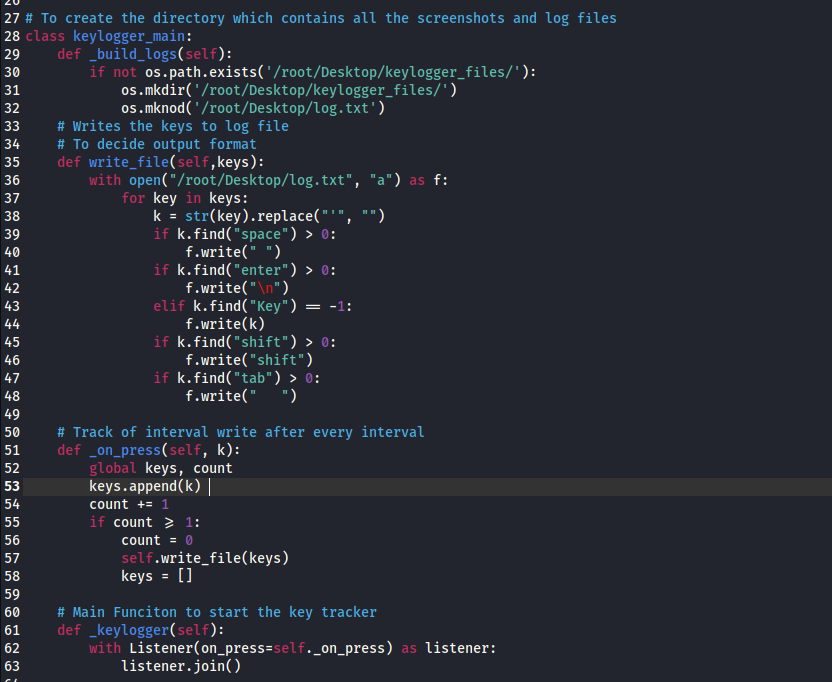
****

****

**Honeypot Implementation**

****

**Keylogger Implementation**

****

## **References**

## Bharat Bhushan, G Sahoo, Amit Kumar Rai (2017). Man-In-The-Middle Attack in Wireless and Computer Networking: A review. IEEE

## Zhang Yalan, Xia Guishu (2013). The SSL MIMT Attack with DNS Spoofing. Trans Tech Publications, Switzerland

## Rajinder Singh, Dr. Satish Kumar (2016). A Stusy of Cookies and Threats to Cookies. IJARCSSE

## Baris Celiktas et al (2018). Man in the Middle attack detection tool design. International Journal of Engineering Sciences and Research Technology

## Seung Yeob Nam et al (2018). Mitigating ARP poisoning-based man-in-the-middle attack in wired or wireless LAN. EURASIP Journal on wireless communications and networking

## Huan Ma et al (2016). Bayes-Based ARP Attack Detection Algorithm For Cloud Centres. Tsinghua Science and Technology ISSN

## Pushpendra Kumar et al (2012). Analysis on Man in the Middle- Attack on SSL. International Journal of Computer Applications

## Richard Ford et al (2009). Man-in-the-Middle Attack to the HTTPS protocol. IEEE Computer Society

## Gopi Nath Nayak et al (2010). Different Flavours of Man-In-The-Middle Attack, Consequences and Feasible solutions. IEEE

## Maderi Lavanya et al (2016). IP spoofing and its Detection Technique. International Journal of Advance Computing technique and Applications

## Ziv Rafalovich, Lior Arzi, Ron Karidi, Efim Hudis (2009). Personalized honeypot for detecting information leaks and security breaches.

## Abhishek Mairh, Debabrat Barik, Kanchan Verma, Debasish Jena (2011). Honeypot in Network Security: A Survey. International Conference on Communication, Computing & Security, ICCCS

## J. Briffaut, J.-F. Lalande, C. Toinard (2009). Security and Results of a Large-Scale HighInteraction Honeypot..Journal of Computers