Internal Security Monitoring of an Organization by Scapy & Kali Linux

Most. Mithyla Zaman
ID: 011141161
Badrun Nahar Bristy
ID: 011141163
Tasnim Morium Mukur
ID: 011131081

A project in the Department of Computer Science and Engineering presented
in partial fulfillment of the requirements for the Degree of
Bachelor/Master of Science in Computer Science and Engineering

United International University
Dhaka, Bangladesh
December 2018

Declaration

We, Most. Mithyla Zaman, Badrun Nahar Bristy, Tasnim Morium Mukur, declare that this project titled, **"Internal Security Monitoring of an Organization by Scapy & Kali Linux"** and the work presented in it are our own. We confirm that:

- This work was done wholly or mainly while in candidature for a BSc degree at United International University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at United International University or any other institution, this has been clearly stated.
- Where we have consulted the published work of others, this is always clearly attributed.
- Where we have quoted from the work of others, the source is always given. With the exception of such quotations, this project is entirely our own work.
- We have acknowledged all main sources of help.
- Where the project is based on work done by ourselves jointly with others, we have made clear exactly what was done by others and what we have contributed ourselves.

_____

Most. Mithyla Zaman, ID: 011141161 and Department of CSE

_____

Badrun Nahar Bristy, 011141163 and Department of CSE

_____

[Tasnim Morium Mukur, 011131081 and Department of CSE]

Certificate

I do hereby declare that the research works embodied in this project entitled **"Internal Security Monitoring of an Organization by Scapy & Kali Linux"** is the outcome of an original work carried out by Most. Mithyla Zaman, Badrun Nahar Bristy, Tasnim Morium Mukur under my supervision.

I further certify that the dissertation meets the requirements and the standard for the degree of BSc in Computer Science and Engineering.

_____

Mohammad Mamun Elahi

Department of CSE

United International University

Abstract

This project is based on Internal Monitoring System of an Organization using Scapy and Kali Linux. The goal of using Scapy is to decipher operations of an extensive amount of protocols, transmit them on the wire, adopt them, fit in requests and responses, and many more. This can effortlessly manage greater portion of highest duties like identifying, vestige routing, probing, unit tests, raids or network invention. It moreover executes very good at a heap of other inelastic duties that greater portion of other tools can't manage. And we use Kali Linux because Kali allows us to use similar tools and technics that an attacker would use to test the security of our network so we can find and correct these issues before a real attacker finds them. By using these tools the proposed project can enable to provide security mechanism for an organization that will enable them to track their employee's online activities easily.

Acknowledgements

In the name of ALLAH, the Most Gracious and the Most Merciful

First and foremost, we would like to pay our gratitude to Allah for giving us the will and strength to accomplish our final project. Thank you for giving us the guidance and courage in order to complete this project well.

Very special thanks to Mohammad Mamun Elahi sir who acted as our project supervisor and examiner respectively, for his ideas, patience, supports and guidelines to come up with this project. Indeed, his advice and continuous encouragement made the completion of this project possible.

We thank our parents for giving birth to us at the first place and supporting us spiritually throughout our life.

We also would like to extend the appreciation to all our friends who were willing to share their opinions and experiences together throughout the whole project completion. You guys are great and fantastic!

We are also grateful to our Vice Chancellor Prof. Dr. Chowdhury Mofizur Rahman sir & Head of Department Prof. Dr. Salekul Islam sir for giving us the opportunity to complete our undergraduate project.

Last but not least, to all people that I forgot to mention here, who have contributed towards the completion of this project either directly or indirectly. Your kindness and cooperation in completion of this final year project paper are very much appreciated. Thank you very much in advance and May Allah bless all of you.

Table of Contents

List of illustrations

Chapter 1

Introduction

Now a days everyone around us uses internet and there is so many way to communicate with each other via social media. Is this a very good thing? Yes, to communicate and share data and information with everyone it can do a vital role. But in some cases like in the middle of a meeting or time while working or even in the class room it will decrease productiveness or sometimes can spoil the whole purpose. So proposed system "*Internal Security Monitoring of an Organization by Scapy & Kali Linux*" can be a time saver and solution to these kind of problems.

1.1. Motivation

The motivation for doing this project was primarily an interest in undertaking a challenging project in an interesting area of network security. The opportunity to learn about a new area of network security not covered in lectures. Interest to use new tools motivated us the most.

1.2. Project Goals

The main goal of this project is to provide security mechanism for an organization that will enable them to track their employee's online activities easily and examine if employees are working properly or not. So that employees can be productive and efficient and for that purpose Preventing access to specific website for different groups of employees is important.

1.3. Possible Application Area

Though Internal Security Monitoring is important for so many areas of work, there are many different places or cases where the proposed system can be used.

1.3.1. For an organization

Employees of organizations sometimes browse internet for Facebook, YouTube or other sites at their workstation. And admin does not want this. But for some employees it is important to have access to those sites.

In figure: 1.1, we can see an organization where this project can be used. There is an admin who wants to monitor the employees. Employees will be divided into two or more groups as you can see in the figure “Group A” and “Group B”. Employees of Group A can access to the restricted sites initially but if admin wants then we can restrict them from those websites. And employees of Group B are initially blocked from those sites and admin can also open those sites for them if needed.

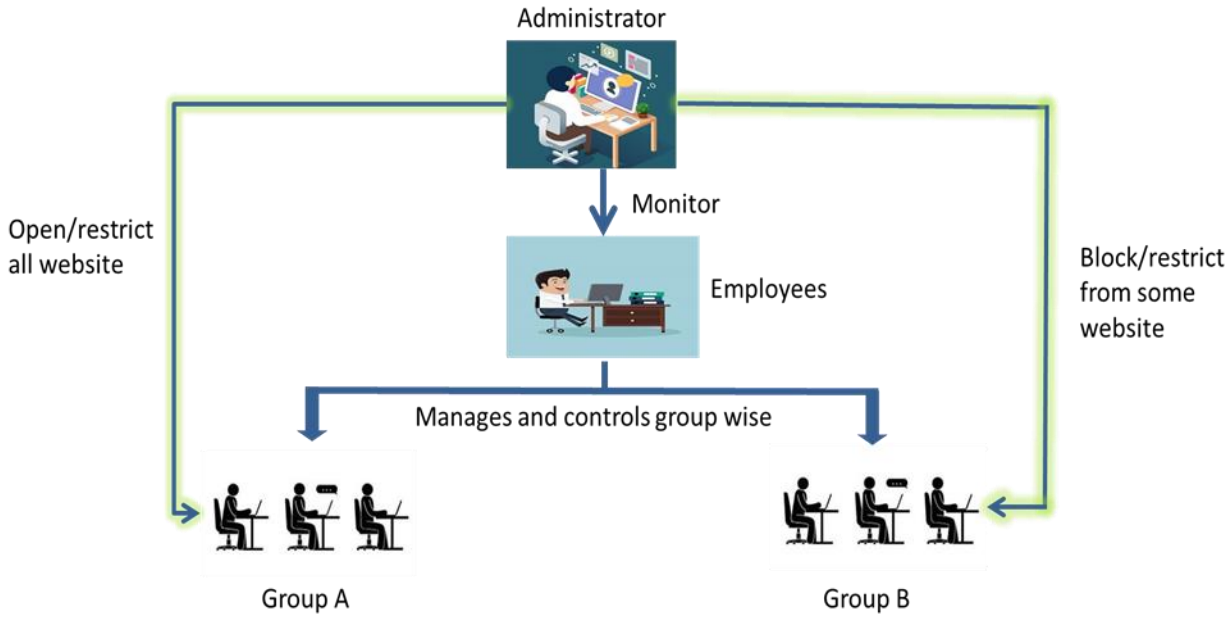

Fig: 1.1(organization’s work flow)

1.3.2. Educational Institution

Another example can be a university. Universities offer different types of courses examples. But mainly there are lab classes and theory classes. In figure: 1.2, we can see university administrator wants to monitor student's movement on the internet. There are two types of class's lab classes and theory classes. In the lab classes there is two type of situation (exam time and normal lab classes). During lab exam sometimes students need internet to download questions from elms or netacad.com or this type of sites. But sometimes some students violate the rules of examination and exchanges answers using Facebook, whatsapp, or other social networking sites. It can spoil the whole purpose of the examination. So proposed system will divide lab classes of the university into two groups and for exam time classes elms or netacad.com etc. sites will be opened and other sites will be closed. And for regular lab classes those sites will be accessible. And on the other hand for theory classes those students will be able to access those sites.

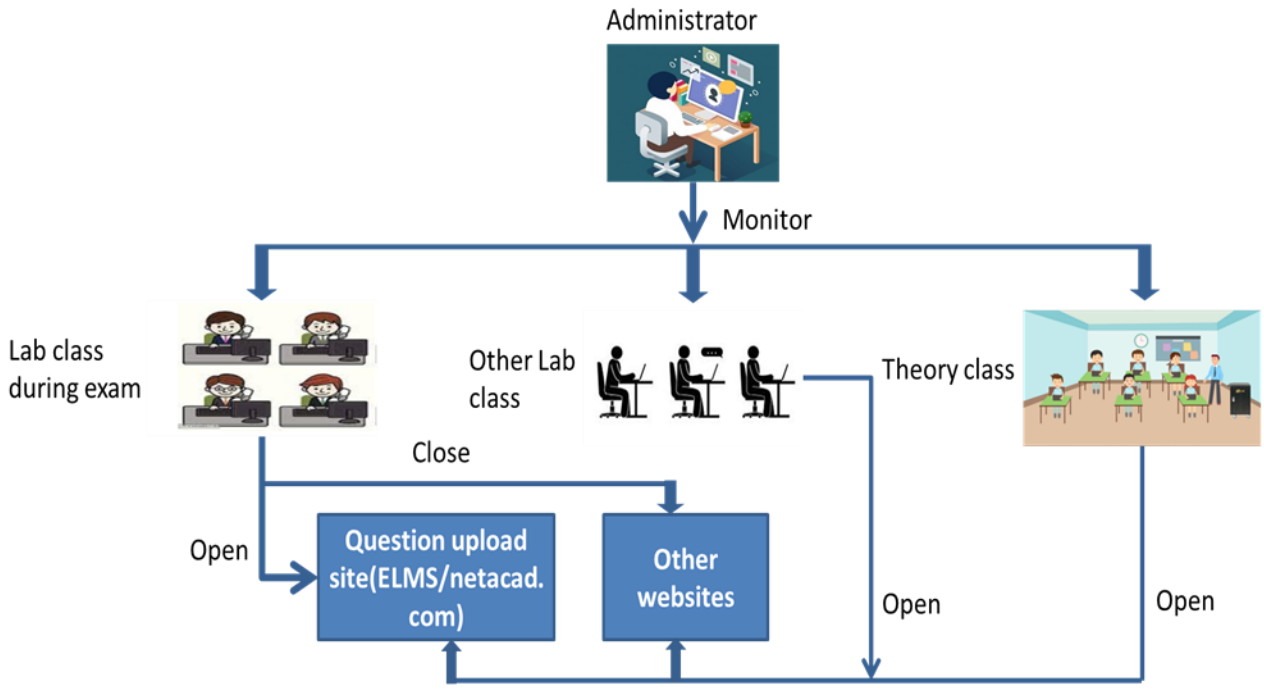

Fig: 1.2(Educational Institution's work flow)

1.4. Background Study

There are many related tools to work with for building network security related project.

Fig: 1.3 (studied tools)

Wireshark[1], TCPDUMP & libpcap [2], MITMPproxy[3], netsniff-ng[4] these are some packet analyzer tools that capture's packet and network traffics for packet sniffing.

1.5. Organization of the Report

Here you can get a short description about all the contents of each chapter.

In Chapter 2 you can get a clear concept on Network Security. And you can also know the concept on how can network security is used to monitor an organization.

In Chapter 3 you can learn about Scapy and Kali Linux. And also can get knowledge about python.

In Chapter 4 you can get an idea about the overall project. This chapter describes how the proposed project works. And the working policy of the project is described by necessary diagram.

In Chapter 5 There is a short description of the limitations of proposed project. And you can also find some future works here. Then you get the conclusion.

Chapter 2

Network Security & Monitoring

2.1 What is network security?

It is any action designed to immune the secrecy, purity and availability of your network and data. That takes in both hardware and software technologies [5]. It contains the strategies and applications adopted to restrain and observe disallowed entrance, misconduct, alteration, or refusal of computer network-accessible resources. This comprises the permission of entrance to data in a network, which gets controlled by the network ruler. It felicitates endpoint security, which focuses on individual devices; network security instead focuses on how those devices interact, and on the connectivity between them. Efficient network security manages entrance to the network. It fixes on a diversity of impendence and stops them from entering or to spread on your network.

2.2 Varieties of network security

One of the major kinds of safety you should have is Network security. Network security works by identifying and pick out impedance and then halt them from invading your network. It is like your own private protection wall.

There are many varieties of network security [6], such as:

2.2.1 Access control:

This procedure aids you to rule who can get entrance in network. Identify in every device and user is significant in order to keep out possible aggressor.

2.2.2 Antivirus and antimalware software:

This is applied for defending versus malware, which involves spyware, Trojans, worms, and viruses. These can be very hazardous that it can corrupt a network and remain hidden for days or weeks. It can handle this kind of impendence by searching for malware entry and tracks files afterward in order to find out violation, resolve malware, and fix it regularly.

2.2.3 Application security:

It is significant to have an app safety because no application is built faultlessly. Any app is able to form of susceptibility, or holes, that attackers use to enter your network. Application security thus encloses the software, hardware, and method you pick for ending those holes.

2.2.4 Behavioral analytics:

You must know what usual behavior looks like to detect unusual network attitude. Behavioral analytics instruments automatically fix performances that drift from the norm. Your safety team can then better recognize exhibitors of compromise that pose a possible problem and quickly remediate threats.

2.2.5 Data loss prevention:

Corporate institutions should give surety that their employee does not share critical info out the network. DLP, technologies can halt section of people from uploading, forwarding, or printing sensitive info in an unsecure way.

2.2.6 Email security:

For a security breach email gateways are deliberated to be the most important impedance. Social engineering techniques are used by the raider and personal info in order to make refined phishing attack to gag receiver and then redirect them to malware sites. An email security app is able to block incoming raid and control departing messages to halt the reduction of critical data.

2.2.7 Firewalls:

Firewalls raise an interruption in between your personal networks that you can rely on and external unreliable networks as the Internet. They applies a defined rules set to approve or impede traffic. Hardware, software, or both can be a firewall. Cisco offers established impendence management devices and impendence-focused next-generation firewalls.

2.2.8 Intrusion prevention systems:

An intrusion prevention system (IPS) searches for network traffic to immediately stop raids. Cisco Next-Generation IPS(NGIPS) appliances do this by making tally with a large number of global impedance knowledge to stop maleficent movement and trace the development of suspicious documents and malware over the network to restrain the expansion of appearances and reinfection.

2.2.9 Mobile device security:

Mobile gadgets and apps are getting aimed by the cybercriminals to an increasing extant. 90% of IT institutes might accept corporate apps on private mobile gadgets approximately in three years. You need to manage the gadgets which can enter to your network and also need to setup their connections to keep network traffic hidden.

2.2.10 Network segmentation:

Software-defined segmentation makes network traffic into various types of categorizations and makes imposing safety rules easy. Mainly, the categorizations are based on endpoint ID, not every IP addresses. You can give entrance based on role, location, and more so the fair portion of entrance is served to the genuine people and questionable gadgets are held and rectified.

2.2.11 Security information and event management:

SIEM actions haul together the info that your safety worker needs to recognize and react to impendence. Those actions are in several manners, inclusively physical and virtual usages and server software.

2.2.12 VPN:

A virtual private network encrypts the connection from an endpoint to a network, often over the Internet. Typically, a remote-access VPN uses IPsec or Secure Sockets Layer to authenticate the communication between device and network.

2.2.13 Web security:

A web security solution will control your staff's web use, block web-based threats, and deny access to malicious websites. It will protect your web gateway on site or in the cloud. "Web security" also refers to the steps you take to protect your own website.

2.2.14 Wireless security:

Wireless networks are not as secure as wired ones. Without stringent security measures, installing a wireless LAN can be like putting Ethernet ports everywhere, including the parking lot. To prevent an exploit from taking hold, you need products specifically designed to protect a wireless network.

2.3. Internal Security Monitoring

Organization monitoring is the use of several methods of work-area observation to gather information about the activities and internet browsing of staff members. Monitoring an organizations internal internet access and devices is an important issue. Employee monitoring is attracting more interest as companies seek to gather and use data to increase efficiency.

Why internal security monitoring?

Every organization wants their workers or stuffs to be productive and efficient. For these purpose spying or monitoring on the internet access and collect information about their online activities is necessary.

The main purpose of internal security monitoring is to track employee's online activities and restrain internal crib of an organization.

2.4. Appellation of ARP Spoofing

Address Resolution Protocol spoofing is an example of offensive in which a bitchy performer transmits misstate ARP information regarding a native surface network. It ends in the joining of a raider's MAC address with the IP address of a lawful device in the network. On time the raider's MAC address is joint to a true IP address, the raider will start taking a bit data this is meant for that IP address. ARP spoofing could qualify bitchy groups to aggressive, temper or even end information in transit mode. ARP spoofing raid can sole happen on native surface networks those utilize the ARP.

2.4.1. ARP Spoofing Raids

The impact of Address Resolution Protocol spoofing raids can have grave effects with regard to initiatives. Within their most fundamental petition, ARP spoofing raids are applied to snitch sensorial messages. Out of it, ARP spoofing raids are sometimes applied to simplify another raid for example:

- **Denial-of-service raids:** Denial of service raids sometimes leverage ARP spoofing to join abundant IP addresses with an individual aim's MAC address. Consequently, operation which is meant in the sake of multiple various IP addresses will be redirected to the aim's MAC address, overburdening the aim with operation.

- **Session hijacking:** Session hijacking raids can use ARP spoofing to snitch meeting IDs, deliver raiders entrance to unofficial systems or information.

- **Man in the middle raids:** Man in the middle raids can rely on ARP spoofing to be aggressive and tone down operation within preys.

2.4.2. An Example of MITM

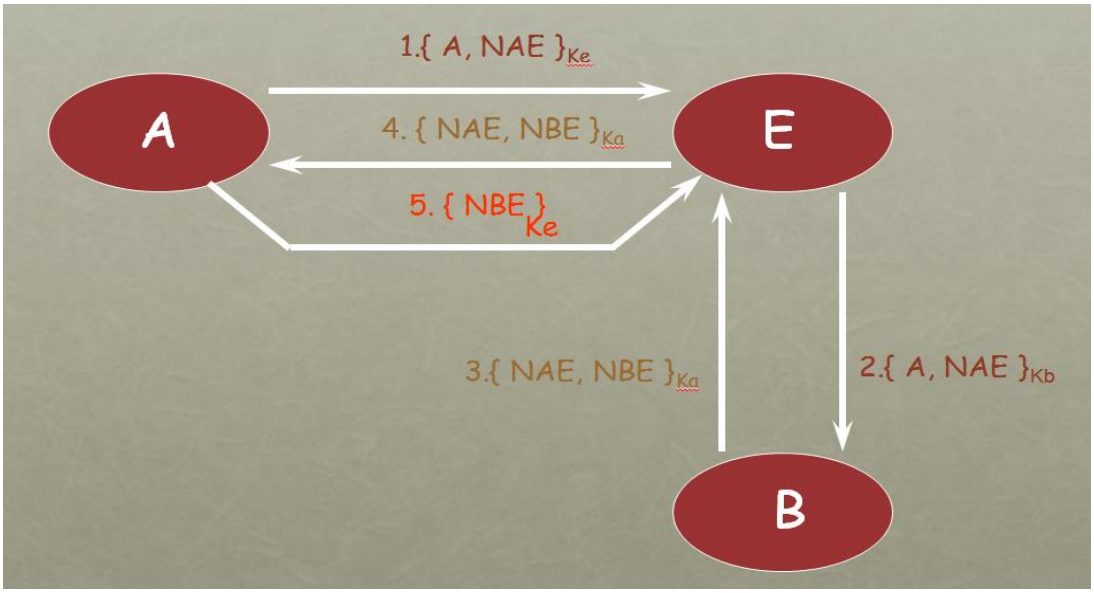

Fig: 2.1(Man in the Middle Attack)

In fig: 2.1 Evil agent E tricks honest A into revealing private key NB from B. Evil E can then fool B.

2.5. Appellation of Packet Sniffing

Internet functions are sent by diverse routers and shifts en route to their goal. These packets are capable to gathering and resolution at every of these dots by a method named packet sniffing.

2.5.1. Who can sniff packet?

Anybody who has entrance to a router can make packet recruitment and following resolution. As internet user usually don't have any concept how his stir is being routed, really it's not feasible to learn who perhaps watching this stir.

2.5.2. Set up a Packet Sniffer by the Following Ways

- **Impure** : All the packets have been taken
- **Pure** : Takes only that packet bearing inelastic data elements [7]

2.5.3. Outbreak and Danger Factors

By sniffer, it's feasible to taking nearly a bit knowledge— Such as, Those websites that a user approaches, which is observed on the location, the objects and goal of somewhat Gmail towards with trifles as regards somewhat downloaded documents. Companies use protocol analyzers sometimes to placement tug of network conduct by officiary and are moreover a portion of multiple honorable antivirus software bundles. Exterior-frontal sniffers identify incoming network operation for inelastic weather of bitchy article, aiding to confine PC virus transit and line the expansion of malware.

Its charge referring, nevertheless, those analyzers can moreover be used for bitchy aims. If the users are curtained to download malware-laden Gmail tainted files from a web location, it's feasible for a disallowed packet sniffer to be placed on a common network. At one time in space, the packet sniffer can warrant a bit information sent and transmitted it to a decree and rule server for therewithal analysis. It's then feasible for raiders to try bundle injection or man-in-the-middle raids, with atoning bit information that was not encrypted earlier on transmitted.

Right use of packet sniffers may help pure up network operation and line malware transit; to defend in opposition to bitchy use, nevertheless, knowledgeable security application is necessary.

2.6. Appellation of DNS Spoofing

DNS poisoning happens if a special DNS server's registers of changed resentfully to redirect operation to the raids**.** That redirection of operation permits the raider to expanse malware, snitch data. Such as, when a DNS record is poisoned, then the raider can handle to redirect all the operations those confide on the right DNS record to look over a mash website that a raider has built to likeness the true location or a several location fully.

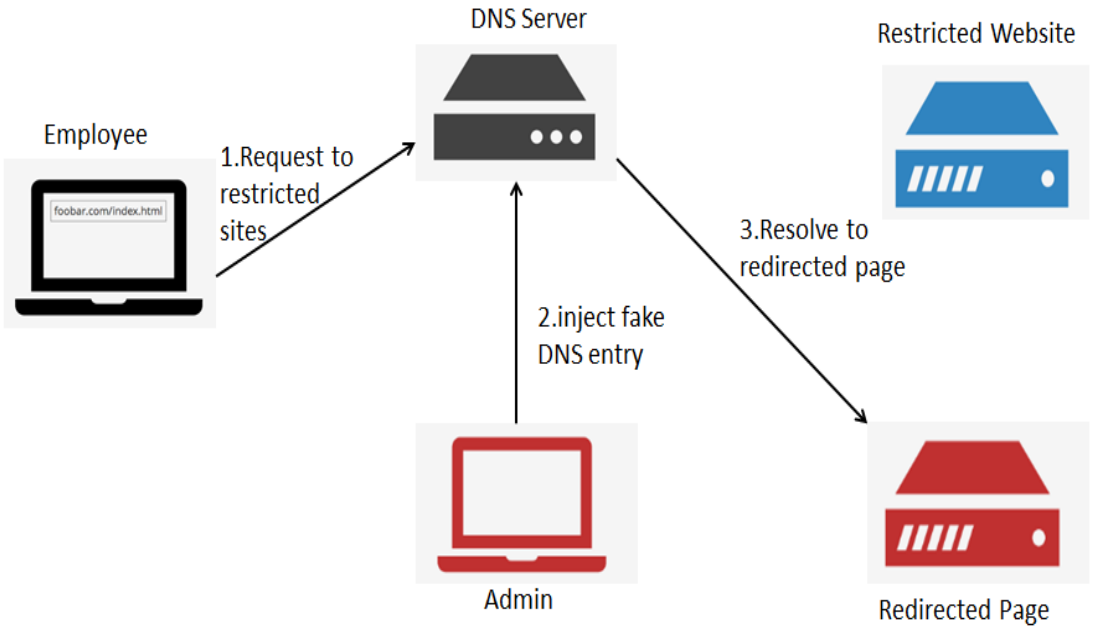

Fig: 2.2[8] (DNS spoofing)

2.7. Using Tools

In this proposed project we use Python for coding part. And use kali Linux and Scapy tools. Later in chapter 3 you can find the details about the tools.

Chapter 3

Tools & Language Used

3.1. Scapy

Scapy is a strong interactive packet skillful programming tool. It is capable to decipher operations of an extensive amount of protocols, transmit them on the wire, adopt them, fit in requests and responses, and many more. This can effortlessly manage greater portion of highest duties like identifying, vestige routing, probing, unit tests, raids or network invention. It moreover executes very good at a heap of other inelastic duties that greater portion of other tools can't manage.

Why we choose Scapy?

1st, by numerous different tools, we shall not make anything the author didn't imagine. Those tools are created because of a particular goal and cannot misguide numerous from this. Such as, an ARP spoof program will not approve we use duel 802.1q encapsulation. And attempt to find a program which can transmit, say, an ICMP packet with padding. Really, in each period we have a recent necessity; we have to make a recent tool.

2nd, usually decipher and explaining are destroyed by them. Devices are good at decipher and society may obtain favor by this. Meaning is conserved for society. Few programs attempt to make similar that function. Such as, they said this port was tile in place of I accepted a SYN-ACK. Often they are right. Often not right. It's easier for new comers, but when you the knowledge what you are performing, you impose attempting to conjecture what actually occurred from the program's explanation to make your personal, that is difficult since you ruined a large quantity of sense. And sometimes decipher and explanation are ended up by you using tcpdump -xX to what the tool given up.

3rd, alone deciphered program does not deliver you all the learning they taken. Their conferred network's prospect is the one their author idea was sufficient. But it is not ended, and you have a benefit. Such as, tools that responses do you have knowledge about the padding?

These puzzles are attempted to overcome by scapy. The operations that are correctly requisite by you it qualified you to make them. Even what if I imagine heaping a 802.1q tier on peak of TCP that has no knowledge, this can have few for someone else performing on few manufacture that is not known to me. Scapy has a flexible pattern which attempts to get off as these right streaks. You are loosely to set a bit charge you want in a bit area you want and load them as you want. You're a full-aged above all.

Really, it's propose creating a recent tool every period, but in space of task with a 100 series C program, you only write two lines of Scapy.

Since a identify Scapy evermore offers you the total decipher operation from the scan, earlier on a bit interpretation. That behalf that you can probe one time and explain much periods, inquire for a trace route and see at the padding for example.

3.2. Kali Linux

Kali is the advanced and highest version of the ever exoteric Discard Linux penetration testing format. The authors of the Discard series repose Kali on a format very resembling to Discard, so anybody intimate with the older Discard platform will feel right at home. Kali re-vamp from the ground up to be the best and most feature rich Ethical Attacking/Pen-testing distribution available. Kali also runs on more hardware devices greatly increasing our options for computer security penetration testing or "pen-testing" systems. If we are coming to Kali from a Discard background, after a short familiarization period you should find that everything is very similar and our convenient level should grow very quickly. If we are new to Kali, once we get used to it, we shall find an easy to use security testing platform that includes hundreds of useful and capable tools to test and help secure our network systems.

Why Use Kali?

Kali comprise over 300 security testing tools. Many unnecessary tools from Backtrack have been withdrawn and the tool interface streamlined. Now we can get the most used tools quickly as they be manifest in a top ten security tool menu. We also can find the same tools and an excess of others all fair classify in the menu system. Kali allows us to use similar tools and techniques that an attacker would use to test the security of our network so we can find and correct these issues before a real attacker finds them.

Tech Note: Attackers commonly execute an abbreviation of steps when targets a network and these steps are shortened below:

Recast – Checking out the target using different sources like sprite gathering.

Scrutinize – Mapping out and examining your network.

Occlusion – Attacking holes found during the scrutinize process.

Elevation of Privileges – Elevating a lower access account to Root, or System Level.

Controlling Access – Using ethnics like backdoors to keep access to your network.

Covering their Tracks – Erasing logs, and manipulating files to hide the intrusion [9].

An Ethical attacker or Penetration Tester imitator numerous of this techniques, with parameters and guidelines establish with collective administration, search out security problems. Then they responses to their discovering to administration also support to fixing the problems. We will not be turnover all the step in the procedure, but we will show you some of the techniques that are used, and how to defend versus them.

I would figure out the largest drive to exercise Kali on trade security resolutions is the value. Security trying tools can be highly expensive, Kali is gratis! Secondly, Kali covers loose origin portrayal of many trade security goods, so you could understandably replace expensive programs by merely trying Kali. All though Kali does cover various loosely rending of popular software programs that can be promoted to the complete structured given portrayal and tried straight by Kali. There genuinely are no main machine conducts varieties within discard and Kali. Kali is originally discard version six, or the newest portrayal of Discard. But this has been fully rearranged from the land up, creating software updates and collation more simple. In discard updating few programs indicated to interval others, in Kali, you modernize entire thing trying the Kali modernize commandment that remains system morality much excellent. Easily modernize Kali and it will trait down the newest editions of the covered instruments for you. Just a note of chariness, modernizing instruments severally could stave Kali, so moving the Kali modernize is constantly the right mood to find the newest packages for the OS. I must obey although, few instruments that I preferred in the real discard are absence in Kali. It is not too large of a transaction like other instruments in Kali most probably does the equivalent substance. And after that freshly you can install another program you prefer if wanted. In collation to remain singly and virtual machine premises of Kali, I also try Kali on a Raspberry Pi – a small credit card sized ARM founded computer. By Kali, you can do nearly all things on a Pi that you could do on a complete sized process. In my book I will shroud trying the PI as a security trying platform together with trying Wireless networks. Trying networks with a computer you could fitting in your purse, is not it cool? Though Kali can't probably hold all the feasible security instruments that all individual would like, it holds sufficient that Kali could be tried from starting to last. Always remember that Kali is not only a security instrument, but a full-grown Linux OS. So if your favorite instrument moves down Linux, but is not covered, most likely you can install and run it in Kali.

3.3. Python

Python is an illustrate high level programming language for potential uses. That is created by Guido van Rossum and freed in 1991. Code readability and notable using significant whitespace are two design philosophy that provides constructs enable clear programming on both small and large scales.

Dynamic type system and automatic memory management is a features of Python. It corroboration different programming exemplar, including object oriented, imperative, functional and procedural. Also it has a large and widespread standard library.

For many operating system python imitator are available. CPython is the reference implementation of Python. IT is an open source software and has a community based development model. It also do nearly all of Python's other implementations. Python and CPython are drive by the non-profit Python Software Foundation.

Why is Python used for network programming?

Python is a general purpose programming language; it has libraries that facilitate writing network-based applications. Hence it *can* be used for "network programming". So can Java, C#, Ruby etc.

The question you *might* be trying to ask is perhaps "Why use Python for network programming?"

If that is the case, these are valid reasons:

1. The network programmer might *prefer* Python over another language.
2. Python has some really good libraries that make network programming easier, e.g. Twisted, AsyncIO

If you're asking as to why are there so many internet sites that use Python. That is more of an ecosystem question. Many use Python to make sites because there are very good tools available for doing so. Frameworks like Flask and Django make things rather easy.

Chapter 4

Project Description & Implementation

4.1. Block diagram of working process:

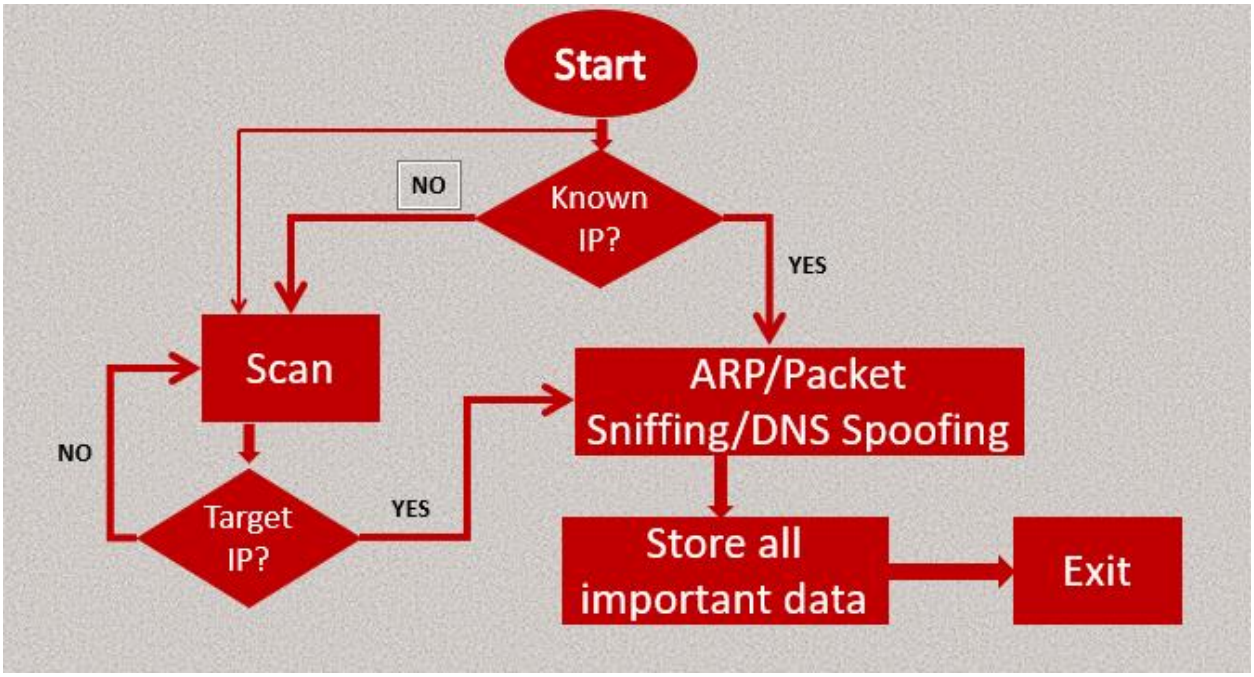

Fig: 4.1(project block diagram)

How does it work?

The fig: 4.1 belongs to how the projects work. If you carefully see the flowchart, you will understand the working process of the project. At the beginning admin (user of this project) have to need scan all the network address in a same router. Then admin target a particular network and generate ARP spoof. If admin can not find any target IP he needs to scan again. And admin already know his target IP, he can directly generate ARP spoof. After that admin can start packet sniffing. Now he will able to see all the incoming and outgoing request or the target IP. Now admin can also generate DNS spoof. BY DNS spoofing admin can prevent access to specific website for target IP or a group of target IP. And all the browsing time, date, important information will be saved in a selected folder.

4.2. Block diagram of ARP spoof:

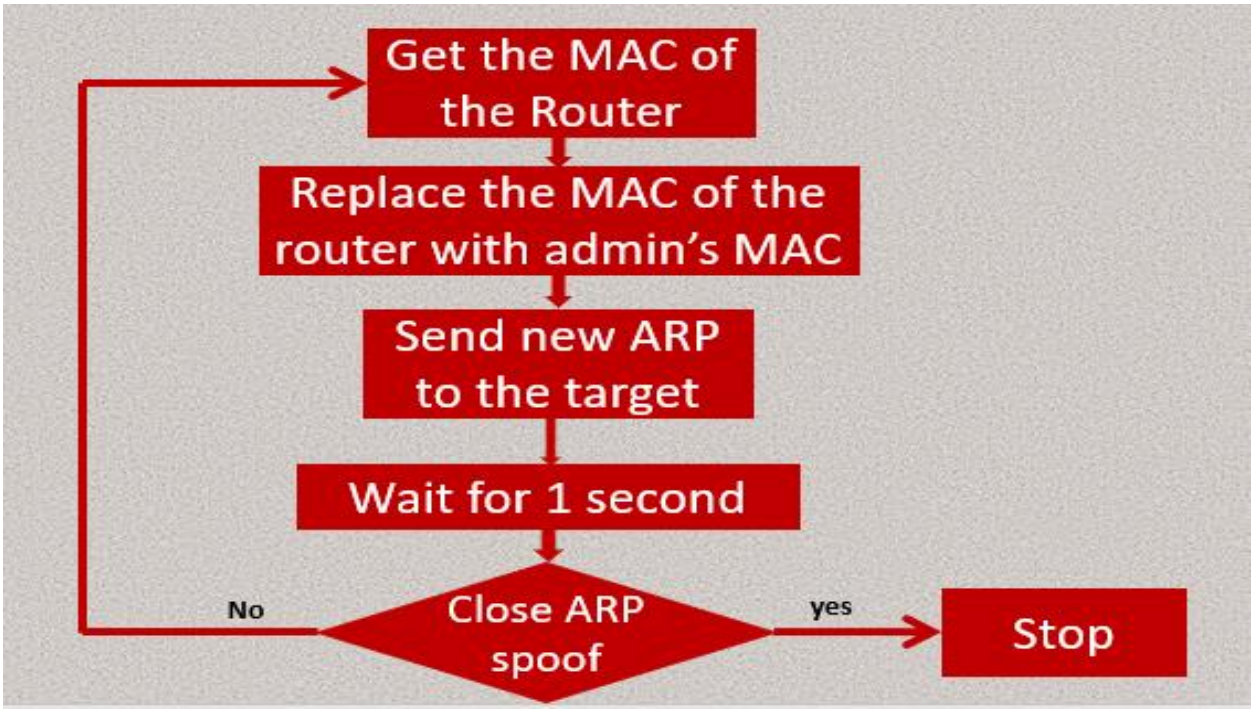

Fig: 4.2(working process of ARP spoof)

How does ARP spoof work?

The fig: 4.2 belongs to how ARP (Address Resolution Protocol) spoof work in this project. At first admin need to know the MAC address of the router. Then he replaces the MAC address of the router with his own device MAC address. And send new ARP table to the target. After that the process waits for one second and close the ARP spoof. If admin want to close the ARP spoof the process is stopped and don't want to close it will run again and again.

4.3. Block diagram of DNS spoof:

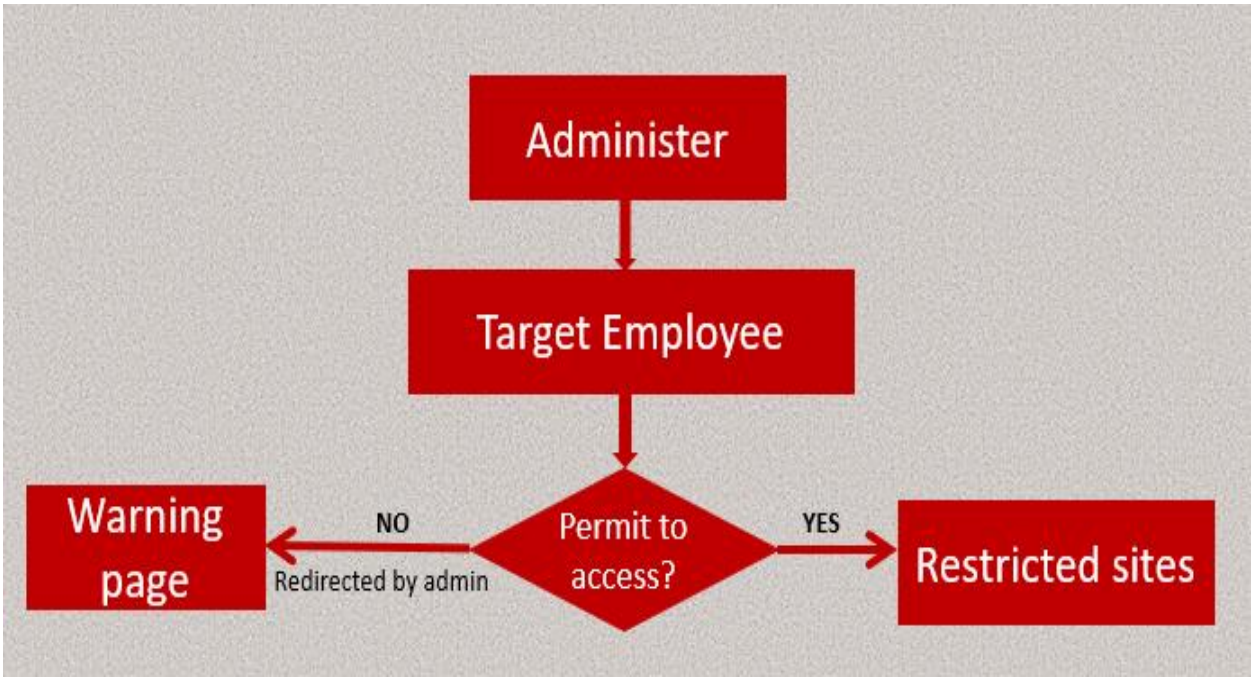

Fig: 4.3(working process of DNS spoof)

How does DNS spoof work?

In fig: 4.3 we can see that after ARP spoofing admin can generate DNS spoofing. In this flowchart we see how DNS spoof work in this project. Here we create a Warning page. If the target IP or target group restricted for some sites they will not able to browse those sites and will redirected from restricted sites to warning page. And if they permitted for restricted they will able to browse those sites.

4.4. Implementation

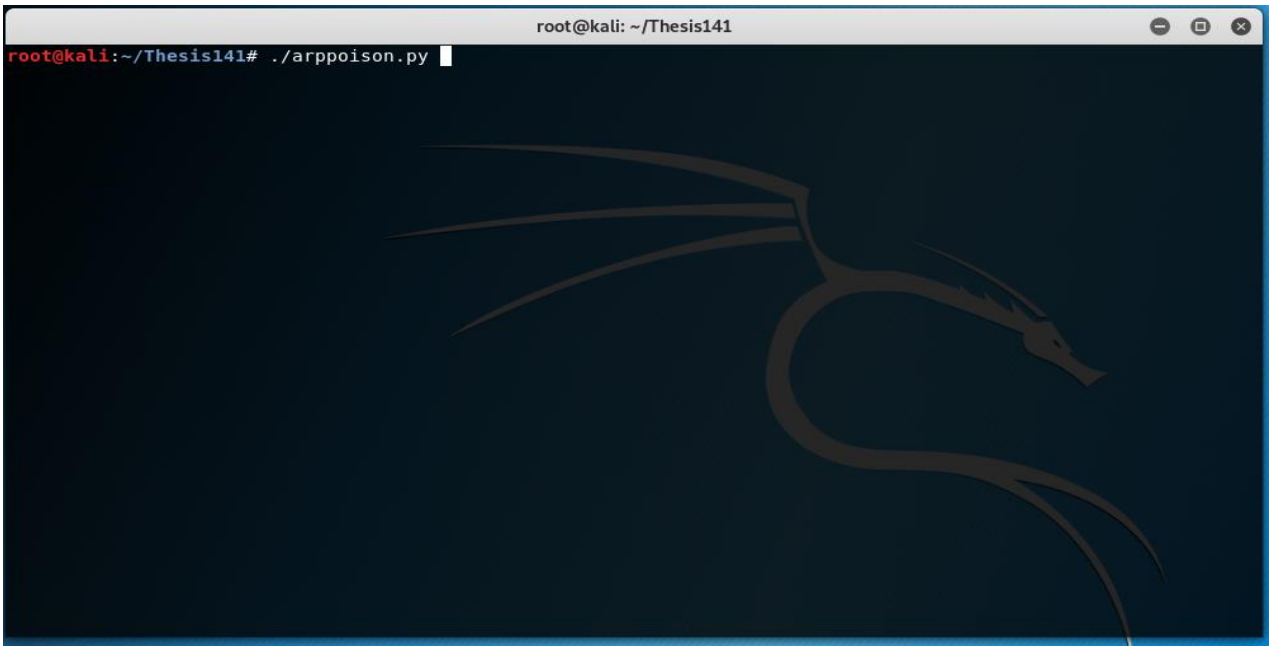

Fig: 4.4 (Running python code)

We can see in Fig: 4.4 that the user runs the python code which is about ARP poison.

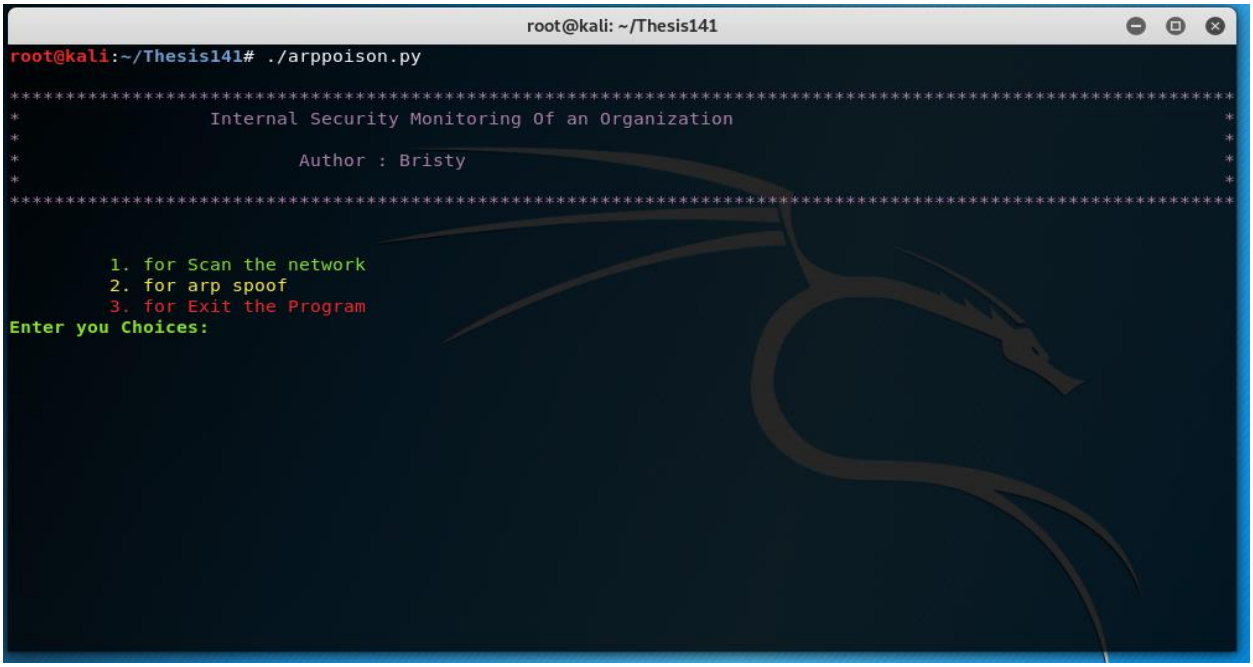

Fig: 4.5(Three options for user)

After running the code we see in Fig: 4.5 that there are three options for a user. Number 1 is for scan the network. Number 2 is for arp spoof. Number 3 is for Exit the program. The user can choose an option among this three options.

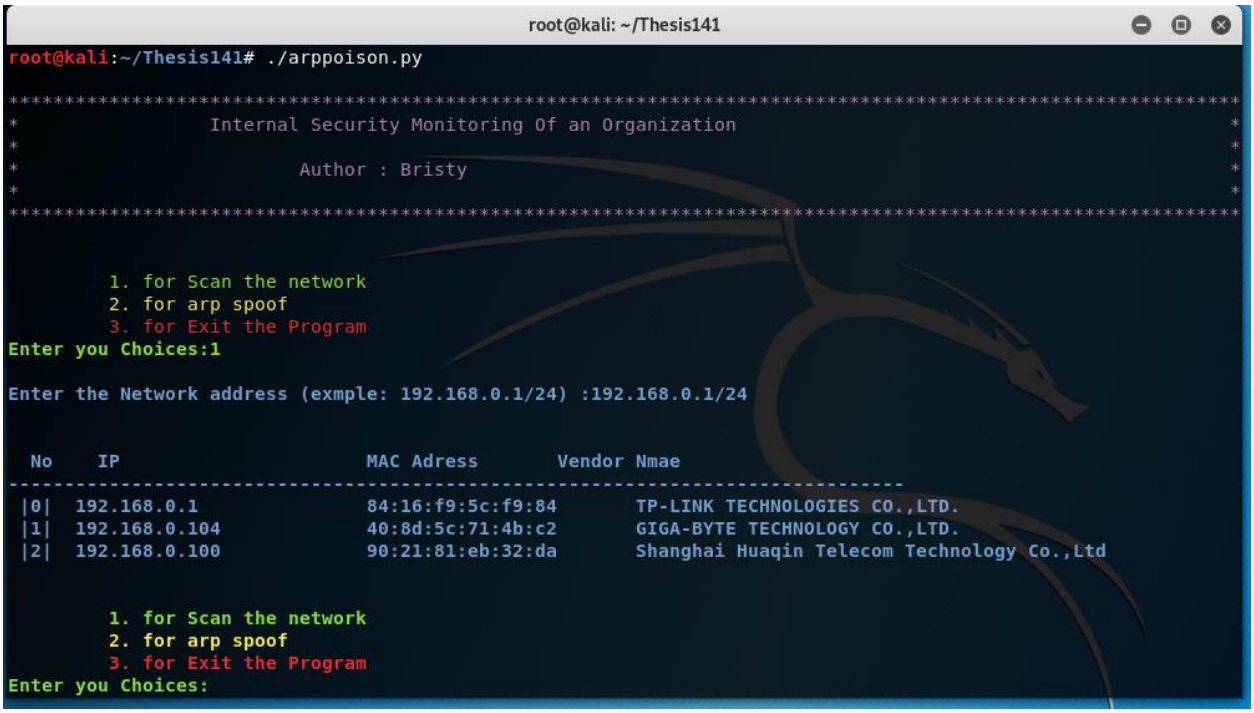

Fig: 4.6 (choose option 1)

In Fig: 4.6 the user choose option 1 and he/she can able to see all the network's IP address, MAC address, and vendor name .This all networks are must be under a same router.

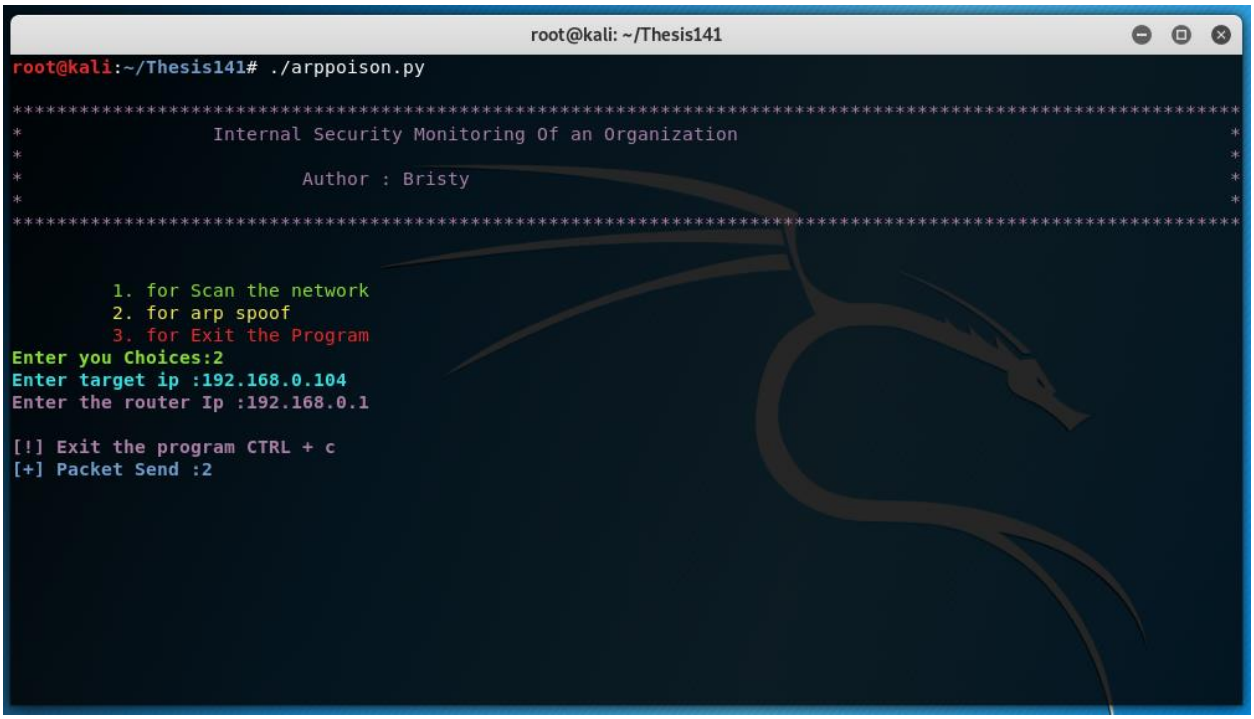

Fig: 4.7(Choosing option 2 and picking an IP)

In Fig: 4.7 the user chooses option 2 and picks a network. Now ARP spoof is started.

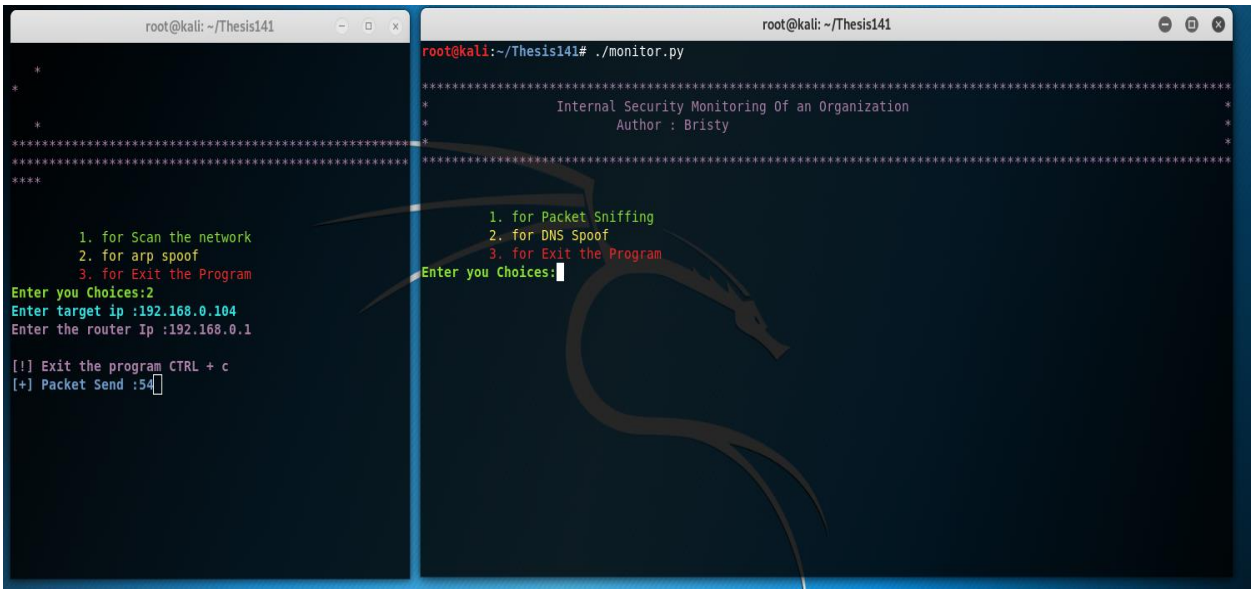

Fig: 4.8(opening new terminal)

Now in Fig: 4.8 the user can see three options again. Number 1 is for Packet sniffing. Number 2 is for DNS spoofing. And number 3 is for exiting the program.

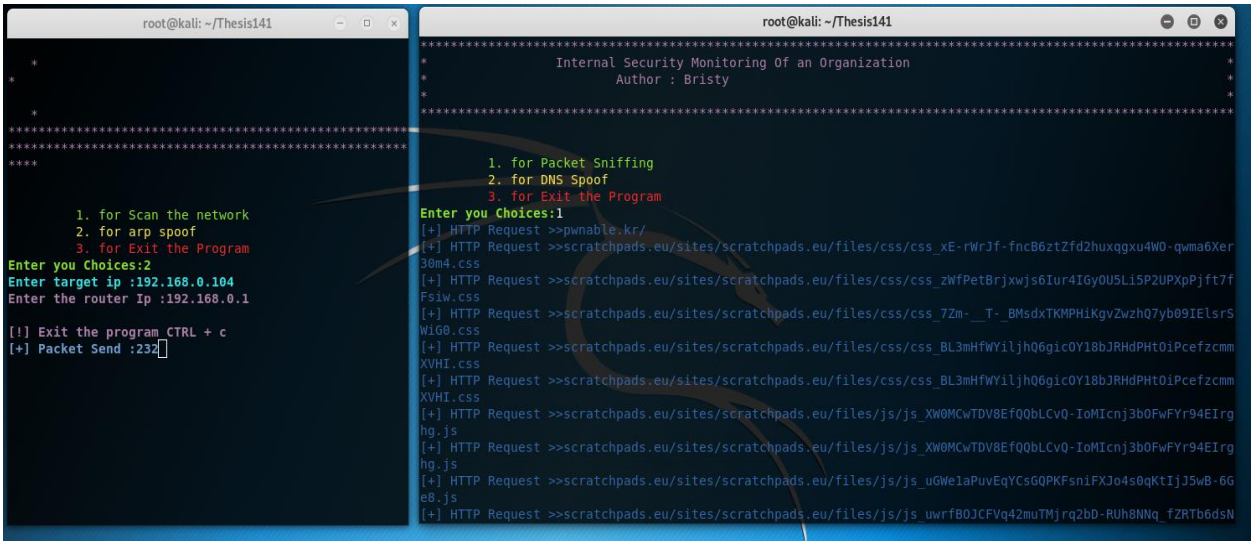

Fig: 4.9(Packet sniffing is started)

In Fig: 4.9 the user chooses option 1 and packet sniffing is started. Now the user can able to see all the incoming and outgoing requests of the target network.

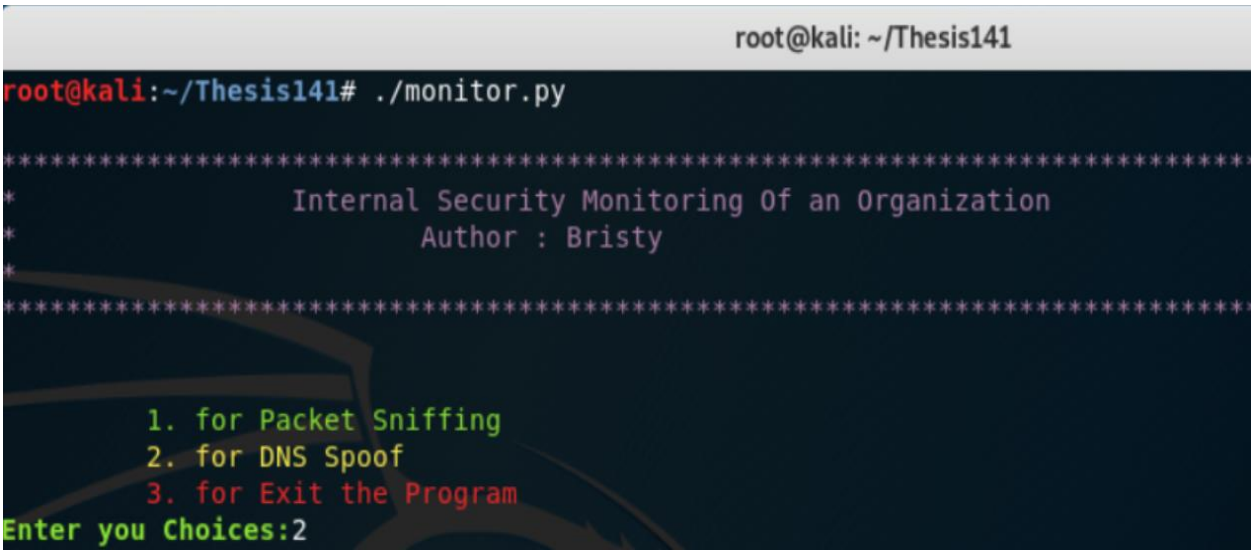

Fig: 4.10(choose option 2)

In Fig: 4.10 the user can also generate DNS spoof. For this he/she has to choose option 2. By DNS spoofing a user can redirect the target network from the restricted sites to another address.

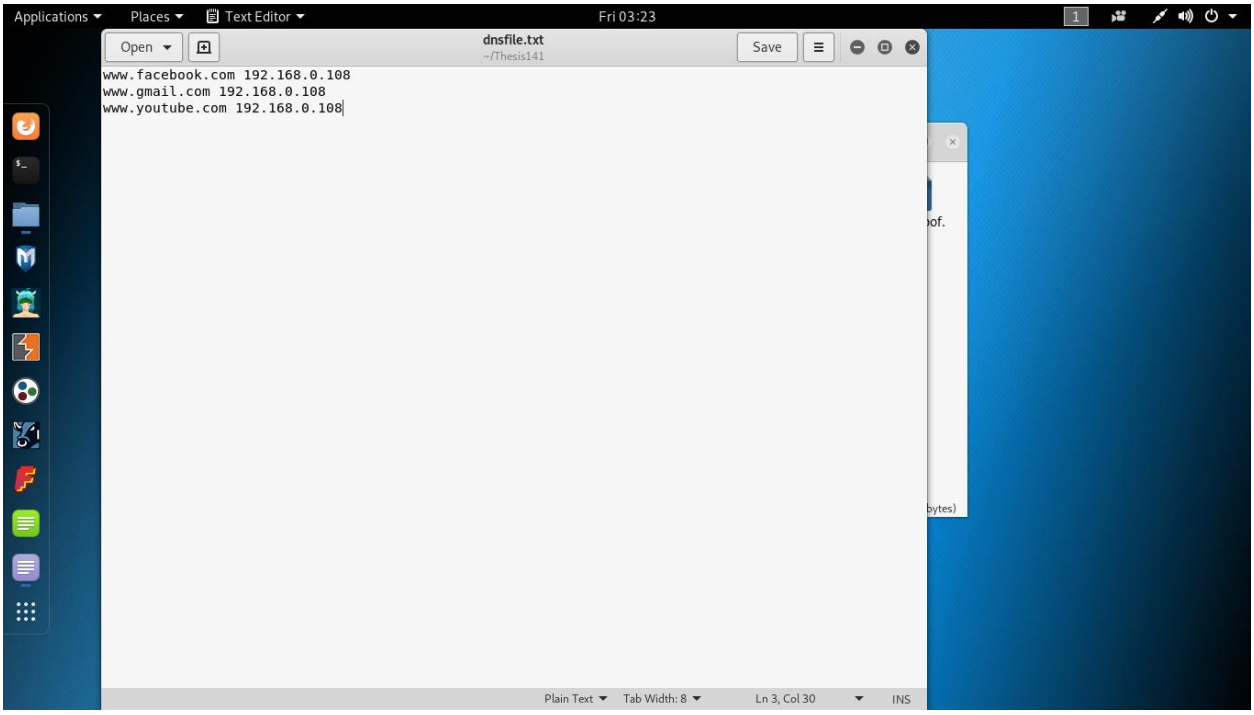

Fig: 4.11(saved websites addresses)

In Fig: 4.11 we can see that there is already a file where all the restricted site's addresses are saved.

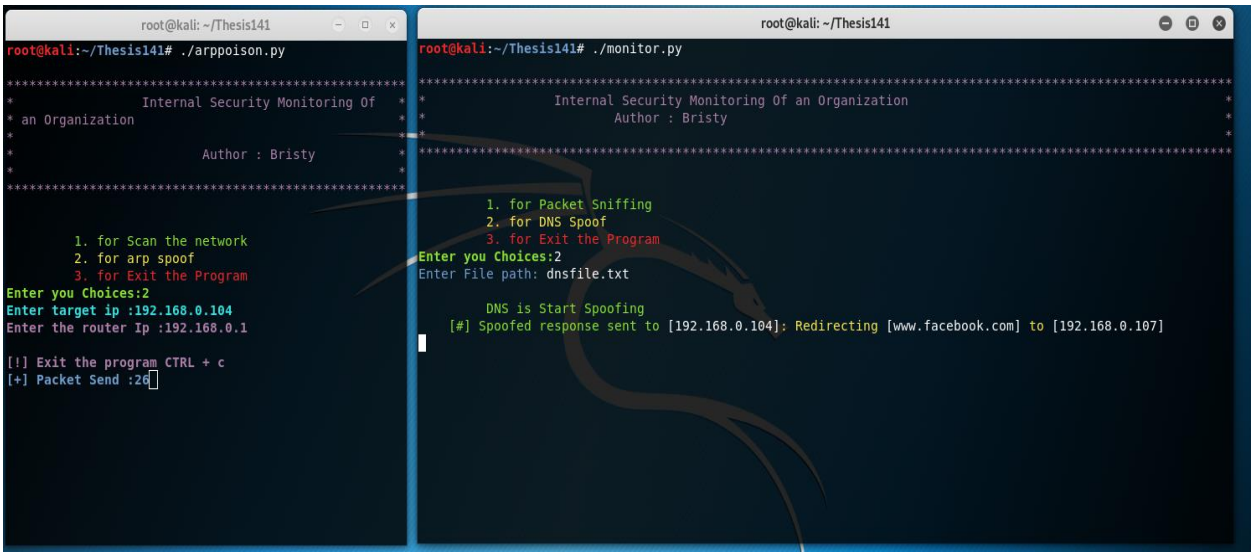

Fig: 4.12(DNS is start spoofing)

The user enters the file path and DNS is started spoofing. Here we can see that the target IP is redirected from Facebook to another page.

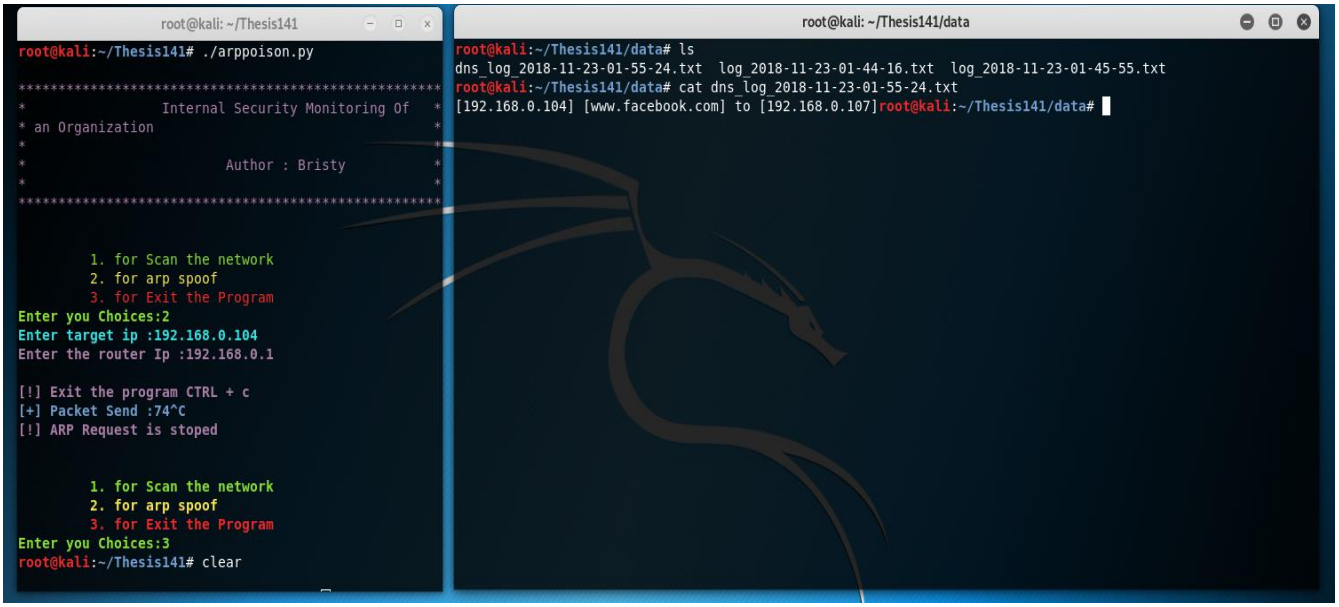

Fig: 4.13(browsing time and date)

In Fig: 4.13 admin can see the browsing time and date of the target network.

Chapter 5

Limitations & Conclusion Remarks

5.1. Limitation

The proposed project has some limitations. And one of the limitations is if there is a manual configuration between a router and a device then ARP spoofing is not possible. Because if a device is already known the IP address of the router then Man-in-the-middle attack is not possible.

Another limitation is if the router has high quality ARP table then Arp spoofing is not possible. For example, the routers of Google or the routers of CISKO academy which have a high quality ARP table and it is not possible to generate ARP spoofing with those routers. Because these type of routers have a good authenticity.

5.2. Future Plan

In This Proposed Project DNS spoof is used for redirecting the employees from the restricted websites to warning page. For many essential purposes the restricted sites are blocked for the employees. But there is no time limitation for it. An employee does not know that how much time he/she is blocked from the restricted websites. In future we want to put the time duration. By putting this time duration and admin can block an employee for a fixed time and for this an employee is not blocked for a long time.

5.3. Conclusion Remarks

Network security is a great area which is finding more and more care as the internet spreads. In our project we use network security as a guard for all employees of an organization. So we hope that by using this project an organization can get a better security system to monitor its employees.

References

[1] Techopedia.com. (2018). *What is Wireshark? - Definition from Techopedia*. [online] Available at: https://www.techopedia.com/definition/25325/wireshark [Accessed 4 Dec. 2018].

[2] Tcpdump.org. (2018). *TCPDUMP/LIBPCAP public repository*. [online] Available at: http://www.tcpdump.org/ [Accessed 4 Dec. 2018].

[3] Mitmproxy.org. (2018). *mitmproxy - an interactive HTTPS proxy*. [online] Available at: https://mitmproxy.org/ [Accessed 4 Dec. 2018].

[4] Netsniff-ng.org. (2018). *netsniff-ng toolkit*. [online] Available at: http://netsniff-ng.org/ [Accessed 4 Dec. 2018].

[5] P. Services, (2018). *What Is Network Security?*. [online] Cisco. Available at: https://www.cisco.com/c/en/us/products/security/what-is-network-security.html [Accessed 4 Dec. 2018].

[6] Garden, H., Security, C. and Security, C. (2018). *How Carnivore Worked*. [online] HowStuffWorks. Available at: https://computer.howstuffworks.com/carnivore2.htm [Accessed 4 Dec. 2018].

[7] Google.com. (2018). *dns spoof pic - Google Search*. [online] Available at: https://www.google.com/ [Accessed 4 Dec. 2018].

[8] Cybrary. (2018). *What Is Kali Linux and Why Do Hackers Use Kali Linux OS - Cybrary*. [online] Available at: https://www.cybrary.it/0p3n/kali-linux-hackers-use-kali-linux-os/ [Accessed 4 Dec. 2018].