Network Monitoring, Detection & Analysis

Ahadul Islam Tushar
Student Id: 011142090
Urbi Roy Choudhury
Student Id: 011142092
Sadeka Afrin Boby
Student Id: 011142093
Md. Rasheduzzaman Rajon
Student Id: 011142098

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



United International University
Dhaka, Bangladesh

January 2019

Declaration

We, Ahadul Islam Tushar, Urbi Roy Choudhury, Sadeka Afrin Boby, Md. Rasheduzzaman Rajon, declare that this project titled, **"Network Monitoring, Detection & Analysis"** 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 project 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 thesis is entirely my own work.
- We have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, we have made clear exactly what was done by others and what we have contributed myself.

_____

Ahadul Islam Tushar, ID: 011142090, Department of CSE

_____

Urbi Roy Choudhury, ID: 011142092, Department of CSE

_____

Sadeka Afrin Boby, ID: 011142093, Department of CSE

_____

Md. Rasheduzzaman Rajon, ID: 011142098, Department of CSE

Certificate

I do hereby declare that the research works embodied in this project entitled "**Network Monitoring, Detection & Analysis**" is the outcome of an original work carried out by Ahadul Islam Tushar, Urbi Roy Choudhury, Sadeka Afrin Boby and Md. Rasheduzzaman Rajon 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
Assistant Professor
Department of CSE, UIU

Abstract

As we know, the amount of connecting devices is increasing very fast. The rapid growth of computer network system brings many benefits of an organization. As well as there are many networking security issues also.

We need strong security system like firewall technology, antivirus technology, valid authentication system to protect our vulnerable networks. But it may not possible to eliminate all vulnerabilities of networks. Because secured networks can also be hacked, we need such as machines for our vulnerable networks which can monitor, detect and analyze malicious activities. In this project, we have implemented a security system, which can monitor, detect and analyze malicious activities of our network. Here we have used **Security Onion** as a security monitoring machine. It can detect malicious activities and we can analyze those activities by using its pre-installed tools.

Acknowledgement

First of all, we like to thank almighty for giving us enough bravery and knowledge to complete our BSc degree final project in time. We extend our sincere thanks to our honorable supervisor Assistant Prof. Mohammad Mamun Elahi for supervising us at every stage of our project. We are profoundly grateful towards the unmatched services rendered by him.

We would like to thank all the people including our classmates for their inspirations. Last but not the least, we would like to express our deep sense of gratitude and earnest thanks giving to our dear parents for their moral support.

Table of Contents

1. Introduction....1
1.1 Motivation....1
1.2 Problem Statement....3
1.3 Background and Methodology....4
1.4 Organization of the Report....5
2. Tools Used....6
2.1 Security Onion....6
2.2 Kali Linux....10
2.3 Metasploitable Framework....11
3. Implementation Details....13
3.1 Environment setup....13
3.2 Live Attack Generation....14
3.3 Analysis the Captured Events....24
3.4 Recorded File Analysis....30
4. Limitations, Challenges and Future Works....37
4.1 Limitations....37
4.2 Problems we faced....37
4.3 Future Extensions....38
5. Conclusion....39
6. References....40

Chapter1

Introduction

In this world, we all are now interconnected through network. Life is getting easier because of internet. We are using internet to make communication with our beloved, work purposes. People usually share their information, documents and data through internet. All these are sharing for personal reason or organizational motive. Day by day number of device is increasing. As a result vast number of people are getting connected. They are making life flexible but everything is not as smooth as it looks like. Because as the amount of connecting device is increasing rapidly, the amount of security threat is also increasing simultaneously. So today, it is a big challenge to protect our network system as well as our data.

1.1 Motivation

Nowadays, huge number of people are sharing their valuable data in internet, a portion are trying to get those information for their evil aim. Hacker is not an unknown word for internet user. Hacker attack is occurring continuously in every second. Since 2013 there are 3,809,448 records stolen from breaches every day. By 2020 there will be roughly 200 billion connected devices. The average cost of a data breach in 2020 will exceed $150 million.

Computer virus are one kind of computer program which enters computer and make own copy without user's permission. These viruses can affect one computer when an infected computer is taken to the normal one. A user can spread the virus by floppy disk, CD, USB drive or through Internet. When a virus attack a network system, the users are using same network system are become affected. An affected network system can affect all computers on that system. Now-a-days personal computer connected with local area network can spread harmful code. Moreover web, email, sharing files through worldwide can be affected by virus.

Some virus are discard program, important files, infect hard disk can get affected. Some viruses do not attack directly but creating a numerous number of copy which exposes their presence through video, audio or messages. These viruses usually take the memory space which is needed by important program. Infect there is a possibility to loss important information or system crush. Sometimes malware found in programs which is officially provide by companies. Sometimes they can hide in downloadable program. These seem to be useful but it can affect program system.

Different virus can affect Windows, Mac, Linux computers, even the data servers which are using by any companies or personal user. It can affect running Internet system. Over the years, there have been thousands and thousands of virus spread online and damage production, waste resources which caused billions dollars loss. Some of those virus are stand out, some speed quickly affect a lot of people or create a huge amount of damage. Some did all of the above. Malware is a short form of malicious software which is a harmful computer program. Which program is caused harm to computer that is called malware or malicious software. Malware is a computer virus, a common name of worms, ransomware, spyware, adware etc. Malicious programs.

Though virus and malware use to harm computer, but now-a-days those are used to steal credit card numbers and other sensitive information. We are facing 4 kinds where around 12 kinds of malware are exists. Malware attack in computer is not a new thing. It make your computer unable to access. Ruin your access power from your sensitive files. Malware is not only annoying or funny to computer user. Even spreading out malware to harm computer or to discard access power above important files is not the main aim of attackers.

The malware word was first used in 1990 by **Yisrael Radai**. Malicious software or malware is a computer virus. By attaching some part of software with executable file malware spread out. These parts can be machine code which can be affect a spy on computer users for an extended period of time without their knowledge. Or it may be designed to cause harm to computer, demand profit from users. Application, system program, even any important

code which is essential to start program. Intention of malware to steal information. It seems to be executable code, scripts. When we talk about a computer virus, we usually mean any kind of code that's designed to do harm and spread itself to more computers. Malicious programs are created by malicious programmers who might want to attack a computer. By stealing personal information they demand money. Sometimes they are simply check how far their virus can spread.

1.2 Problem Statement

Network security prevents unauthorized activity in network. It is a process of protection for network infrastructure from unauthorized access, modification. Network security ensures secure environment for computer users. Network security consists of:

- **Protection**: System should be configured as correctly as possible
- **Detection**: Can identify if any configuration change occurred or any network traffic problem happened
- **Reaction:** Provide quick response against problem and ensure security

Network security maintains some policies to prevent unauthorized activity. Physical assets are visible so when we lost them we can easily find out our need or we can keep duplicate of our needed things, as we can find them when we need. Information storing in computer can make our life easier. All type of data we usually store in our computer so that we can use them further. Communication Medias are now over internet so internet is also a large media which maintain our information. Accessing that information in internet or in our device by unauthorized person is not healthy for us.

So, our main task is to make sure all our information are safe. So the idea came to make devices secure as no one can access device with evil aim. Implementing security in device level is not enough. All secure devices are in threat in this growing up internets age. Attacker makes different high technical device and program to hack. We are not safe from them.

Implementing security in device is an option to make information or communication secure. Important part is maintained security by continuously monitoring them is more important. But only security implementation, monitoring will be useless if network experts do not take any action against attackers. As the following picture, the attacker can easily burn security devices, can get access of network and also can transfer valuable data without user's permission.

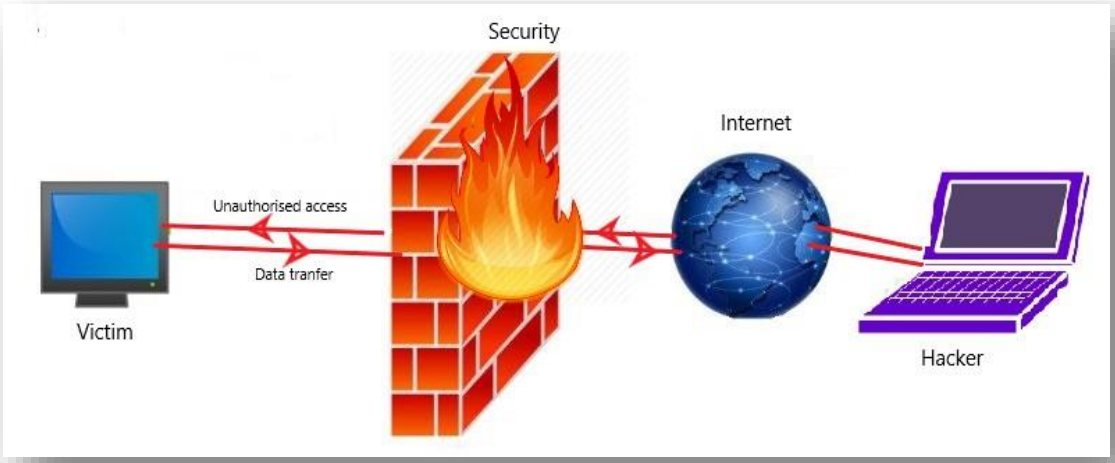


Figure: 1.2.1

1.3 Background and Methodology

IDS: Intrusion Detection System deal with getting the alert. Monitors network traffic and also gives alerts for doubtful event.

NSM: Network Security Monitoring. Monitoring network for security related events such as alerts, session data and full packet capture**.**

Network security implementation is not enough, so we are introducing tool which helps us in monitoring network, detect malicious activities, analysis malicious activities. Unauthorized activity can analyze to find out the way of attacker, their activity pattern and amount of loss we faced. Security onion helps to maintain all these need. Security Onion is an NSM image.

Our proposed system can maintain these following needs

- Network Monitoring
- Detect Malicious Activities
- Analysis Malicious Activities

1.4 Organization of the Report

We have distributed our project report into 6 chapters. In chapter 1, we have already discussed about introduction, problem statements and methodology.

In chapter 2, we discussed in details about all the tools which we have used to demonstrate our project. Here we have discussed also about some important security tools for analyzing malicious activities.

Chapter 3 is about the main two parts of our project. One part is about how we can setup environment to demonstrate our proposed security model, generate a live attack to check detection ability of that machine and analyze the detected malicious events. The second part is about how we can analyze previously recorded malicious activities!

Chapter 4 is about the limitations, challenges we have faced to complete this project and future work of this project.

Chapter 5 is conclusion of our project work and chapter 6 is about the references we have used to successfully complete our work.

Chapter 2

Tools Used

We have proposed a security system for monitoring, detecting malicious activities and analyzing malicious activities. For testing purpose, we have demonstrated this security system as the following picture

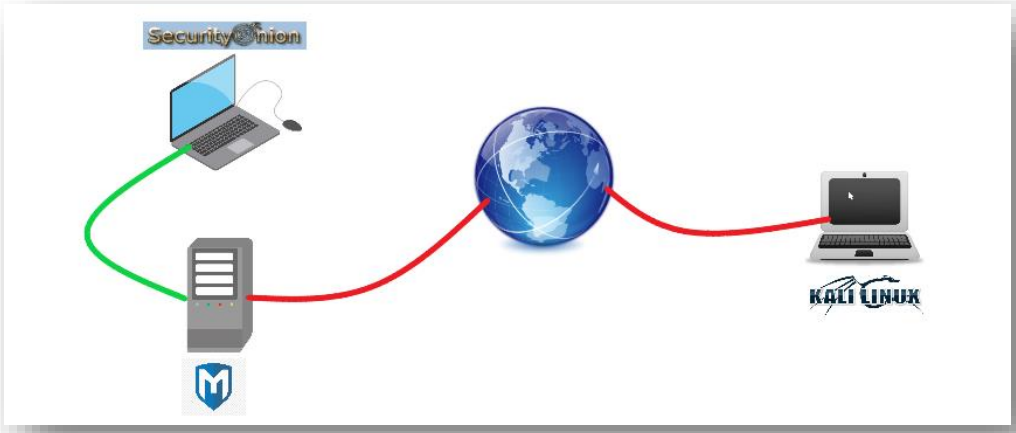


Figure 2.1

Here we have used ‘Kali Linux’ as an attacker, ‘Metasploitable Framework version 2.0’ as a victim server and ‘Security Onion’ as a NSM. The details of each machine has described below.

2.1 Security Onion

There are many Linux distributions. Security onion is one of them which is Distributed for the system of intrusion detection. Used as a monitoring the system of network security. Also works as a system of log management. IDS mean intrusion detection system. There is contaminated work that is harmful to a software application and also some other devices in that case software application can be harmful. An intrusion detection system is one kind of network that monitors this kind of situations. Network security systems are usually used to monitor all networks that require security. This is a system that works by utilizing its

intelligence. It is a network of weaknesses through its monitoring. Log management basically collects all kinds of log procedure, activities of software, different kinds of user events and as well as the analysis of network traffic etc. Security Onion is normally one kind of Ubuntu based and it comprises different kinds of tools like as Kibana, CapME, CyberChef, Snort, Suricata, Bro, Sguil, Squert, Snorby, ELSA, Xplico, Network Miner and many other security tools. Security Onion is one kind of position that Permission for that monitoring the safety of the network. For the use of safety onions, we need virtual environments, which include virtual box and VMware in that case we use any of these we use the security onion. Basically three core functions of Security onion like as –

- The capture of Full Packet
- Not only Network but also Host-based intrusion detection systems and as well as the analysis of powerful tools
- Provide log and watchful data to find out activity and events.

Full packet capture is usually a function that works by video cameras inside our network. As we look at this video camera through everything in our network. We do not know if everything is right or not. If anybody comes inside the leader, if we have received any files, then we find this video camera. Security Onion is usually done as a multiple of IDS. Networks, as well as host-based entry detection systems, usually have a network host or traffic system, which they do in parasites and carefully provide important information for the activity.

Security Onion Layers

- Ubuntu based OS.
- Snort, Suricata
- Snorby
- Bro
- Sguil
- Squert
- ELSA
- Network Miner
- PADS

- Kibana
- CyberChef etc.

Snort

Snort is basically an open source system where networks work as intrusion detection and there is also a resistance mechanism. It usually works as an intrusion detection system/intrusion prevention system. It is a simple one that has the ability to analyze real-time traffic. Besides, there are many other things that include any type of prototype parasite, and any search by which it is discovered, and one with another. Along with a firewall, this should be another fundamental part of our network security. IDS and IPS both of them are combined in one device. They are not separate. IDS basically identified dangerous traffic analysis on the other hand IPS takes action. Snort basically running in three different modes like as-

- Running like as packet capture mode
- Running like as logging mode
- Running like as intrusion detection mode etc.

Snort watches our internal network which is very important because many of the problems of security are coming inside our network and in that case, we are chance our network correctly.

Suricata

Suricata is a lofty performance Network not only intrusion system but also intrusion prevention system and Monitoring the system of network security. IDS and IPS both of them are combined in one device. They are not separate. IDS basically identified dangerous traffic analysis on the other hand IPS takes action.

Suricata is a network that works very fast with a robust network. This network acts as a threat to the detection engine.

There is not much difference between snort and Suricata. Some differences include here like as snort basically works as a single thread, on the other hand, Suricata works as multiple threads. Another one is Suricata package is not available on the other hand snort package are required and also it’s available.

Snorby

Snorby means monitoring the system of network security's which is based on web fronted. Snorby is available for in security onion. When we click the icon of Snorby then go to open any type of browser. After that email and password given we are looking for a dashboard in Snorby. In the dashboard, we are looking some alerts like as High Severity, Medium Severity, and Low Severity etc. We can also see about sensor, protocols, severities, signatures, sources, destinations etc. We can see interesting statics about sources. Then we can go to the events option. This is the main option for that which is also an actual network based ideas alert. Then we can one event option click we can see about full details for that event like as Source IP, Destination IP, Source port, Destination Port, the file will be HTTP or not also see about full information etc. we can also see about packet capture option.

- Ramification
- Complete Packet
- Determined intentionally etc.

Squert

Squert is a web application interface. It is used for a search. Through this, we can see the event data that the data is stored in the Sguil Databases.

Squert is a visual tool. It attempts to provide which is additional context to events through the use of metadata, time series representations.

Squert is available for in security onion. We click the icon of Squert. Giving we access to this sguil database from any type of browser. After that log in username and password which is specified in set up. Squert is not only access to network-based ideas alert but also host-based ideas alert. Here https log coming from bro as well. Event data are coming from a different database. Once we any source id or destination id for any type of event and put on this here we see about details for this event in Squert. We already know about Squert also use capME to capture full packet. We need to write Src IP and DST IP then click to submit Button after that we know full information about ip address or

port etc. After click the submit button we know about Sensor Name, Timestamp, Src IP or Src port and also dst IP or Dst port. Also we can see the full details about data when data will be sent. Sometimes we can see that no data has been sent that's why we don't know about the full information of the data.

Bro

Bro is generally a strong network. This is a network that we can analyze this network on the framework. It works as a top-level application. In addition, the Bro is Semantic Analysis. When we open Sguil to launch any event, we can go to the Bro option and see the contents of the event, and we know that this is the HTML File or PHP file. Apart from this, we can also know about timestamps. As a matter of fact, its Sguil site is scheduled. The events that we initiate through Sguil, act as many powerful. We see the event's content through Sguil.

Sguil

Sguil is an analysis tool. It provides an SQL database backend. Sguil usually works as a GUI interface. When we take a file, we work in the program through the TCP-reply in the terminal and act as the Sguil interface for viewing events. Generally, when the username and password are entered by the Sguil interface that is given in the setup, it is inserted into the Sguil which usually acts as real time conjunction. We can also analysis Wireshark, Network Miner inside sguil etc.There are lots of data types in Sguil like as NIDS, HITS, session data, asset data, HTTP etc. Sguil is normally is not browser based but works as a powerful. In Sguil we see the event details as well as we also see about different event message. In Sguil we can select one event option then we can move and see different kinds of option for that option.

Elsa

Elsa is a powerful application. This application is basically works for centralized processing system logs, which is used for MySQL and Syslog NG. Elsa is basically works as a query. User can configure email alerts and perform tasks on a schedule. It is also possible to create some reports in the form of graphs. Elsa basically provides a user interface that can be used for some analysis and also filtering of it by IP, port and others. Using Elsa, we can also generate some statistical data. After that we can overview this statistical performance of the network being monitored.

2.2 Kali Linux

Kali Linux is an operating system. Usually this system is used for hacking. When we use the Windows system, there are some tools that we do not need to download. They are inside Windows. Among them are calculators that we use in our calculations. In the same way, kali Linux is also something that we use for hacking. This means that kali Linux has some great tools that we use in such things. In addition, there are some tools in it, such as if there is a mistake on the website or if the website is hacked, then it is also used as a job to alert the website administrator. Compared to kali Linux, there are other versions of Linux such as Ubuntu which we can use to hack the website. But the problem is that if we want to hack the website using this version we will have to write many code for it. Hacking something by writing this code is a lot of hard work that cannot be used for a long time, so we do not use these versions for hacking purposes. Kali Linux is one of the best versions of hacking websites. Besides, no other version was created based on the base. . For this, we need to write the complete code when using those versions. So we do not have to type the complete code as well so that any website can be hacked, we use kali Linux. The Kali Linux code does not have to be written because the Kali Linux is based on the base. Our job is to code based on the bases. This way we can generally hack websites. Kali Linux is an open source system. So we can download Kali Linux from anywhere, and then we can use it too.

2.3 Metasploitable Framework

Metasploitable is a framework. Additionally, this framework is usually an open-source infringement tool that is used for the development and execution of exploited code, rather than for the remote target machine. The Metasploitable framework is known as the world's largest database. This framework is usually published independently. Apart from this, there are various types of programming languages. This framework works as a limited platform for a specific platform. Moreover, this framework does not have a clear document, no code style due to which it is working well for a long time. It is not properly seen or understood. Other than this, there is another word that can be used to collect equipment that we can use for our software testing work or for any telescope we ever have on the web site or we can also use it or test it for the sake of our network security. This means that the Metasploitable framework is being used for security testing purposes. When a new website has been created, we really face different types of problems. Then we have to overcome those

problems, and for this we have to use this framework. We have to keep an eye on any bugs that do not exist. Whenever a website is created for the network only, then no permission is needed to access it. Since Metasploitable framework works as a type of equipment collection, it targets those tools, scans those processes. Metasploitable framework is also used inside kali Linux etc. To install this kali Linux and Metasploitable framework we first installed the virtual machine. Then inside the virtual machine we install kali Linux and metasploitable framework and then using it by running.

Chapter 3

Implementation Details

3.1 Environment setup

- First of all, we have to download and install virtual machine.
- After that we have to download and install security onion and as well as settings the network adapter.
- Then we have to download and install Kali Linux and as well as settings the network adapter.
- Finally we have to download and install Metasploitable framework and settings the network adapter.

We are usually using internal network adapter. This adapter is commonly used to connect from VM to another VM. Suppose, Kali Linux, Metasploitable, Security Onion are these three different VM. To bring three different VMs to a network, we are using the internal network adapter in three.

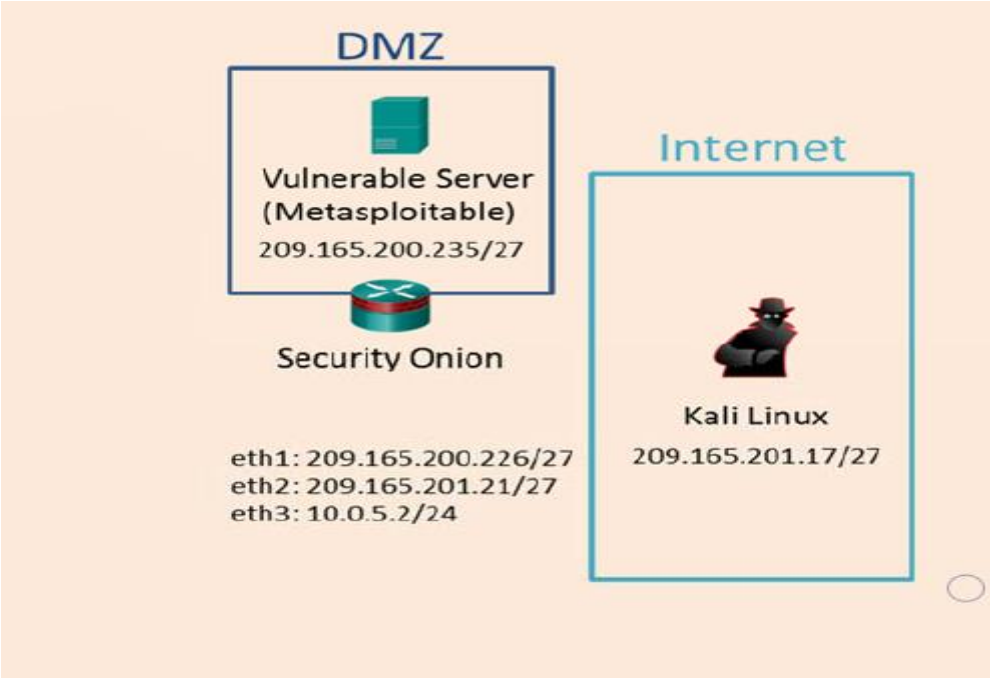


Figure: 3.1

After setting the internal network adapter it must be given a name. We have used the "internet" in kali Linux. We have used "DMZ" at metasploitable frameworks. An internal network adapter is usually used on a metasploitable framework which is used for any other purpose. This internal network adapter is not used in our work. Now we have two things used in kali Linux and metasploitable, we will use the same name as security onion. After using the same name as security onion, then the internal network adapter should be selected. The name given after the internal network adapter is selected. One name is "internet" and the other name is "DMZ". The same name is given because these two names will work as a gateway to kali Linux and metasploitable. Security onion has four adapters. We already know about two adapters. Now we know about two other adapters where a name is "inside" and other name is "Nat". An internal network adapter which name is "inside" is usually used for other purposes. This internal network adapter is not used in our work. An internal network adapter which name is "Nat" is usually used to browse the internet.

3.2 Live Attack Generation

- Here is the terminal for metasploitable Framework (Fig: 3.2.1). In this terminal when we write to Command ifconfig then we see IP address, subnet mask and other some basic information etc.

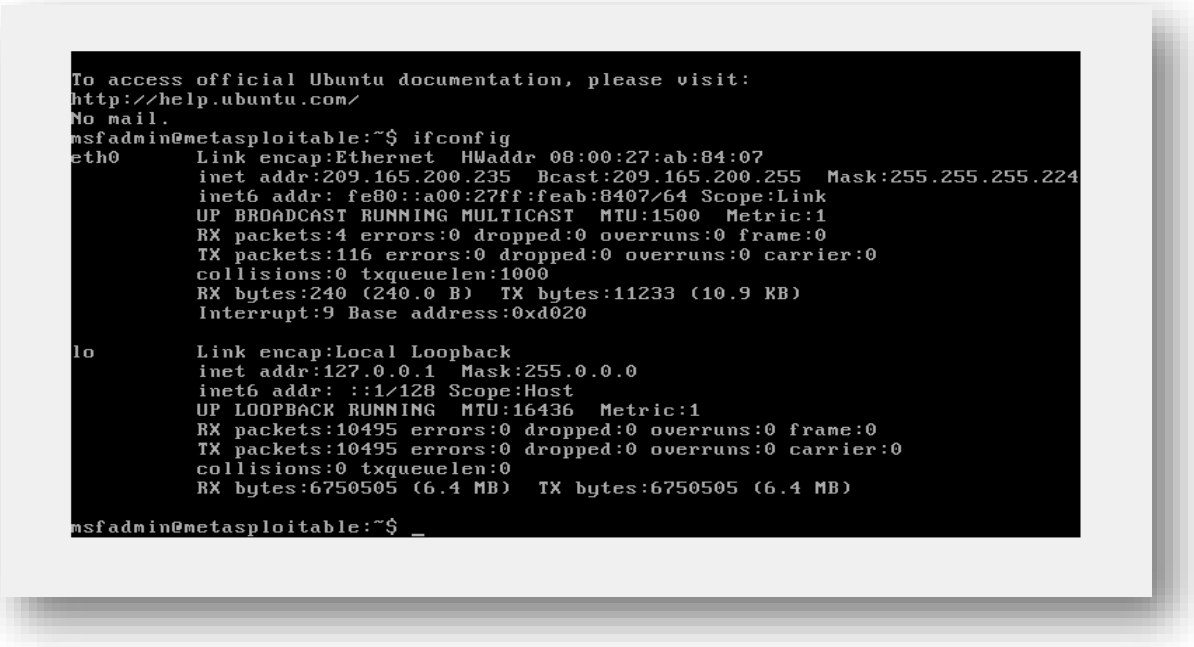


Figure: 3.2.1

- In this terminal we have to create a directory and a text file(Fig: 3.2.2).



Figure: 3.2.2

- Here is the metasploitable terminal (Fig: 3.2.3). In this terminal If we see what files are present inside another files that is test.txt then we have to use sudo command like as sudo nano test.txt. Then we have to know what kind of files are here or not. Here we see in this test.txt file (Fig: 3.2.3), there are one line and that is Hello, I am from metasploitable framework!



Figure: 3.2.3

Nmap

Nmap means a type of network map. A hacker does not know what I'm doing, but if he does not know my IP address, then he has scanned it with Nmap, and then the hacker goes after everything, usually I am working or what kind of work I am doing. I n addition to whether a port is open now or a port is now closed or any kind of service is running. Nmap is advanced network mapping and scanner equipment. These tools are used in kali Linux as a data collection tool. With these tools, we use network IP address, domain, firewall, router and other hurdles, for various types of scan scans such as TCP, UDP, OS detection, service detection, version detection etc. Apart from this, we also know about information about ports, identification, network analysis, etc. Nmap is also used for graphical user interfaces. Then we also know about the same as the basic information in this IP address.

- Here is the terminal for kali Linux (Fig: 3.2.4), in this terminal when we write to command ifconfig then we see IP address, subnet mask and other some basic information etc.
-

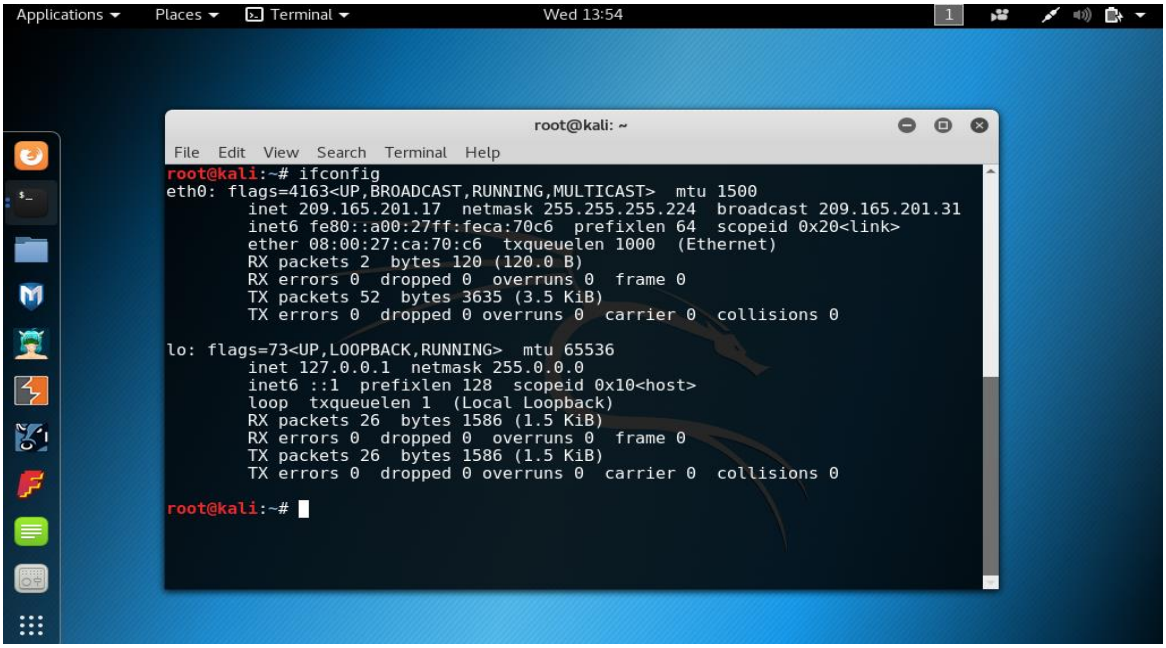


Figure: 3.2.4

Here the interface of metasploitable framework inside kali Linux (Fig: 3.2.5). Service Postgresql start that is the start database for exploit. Then we write the mfsconsole and that is the command line metasploitable framework. The msfconsole is basically the most useful interface to the Metasploitable Framework (MSF).

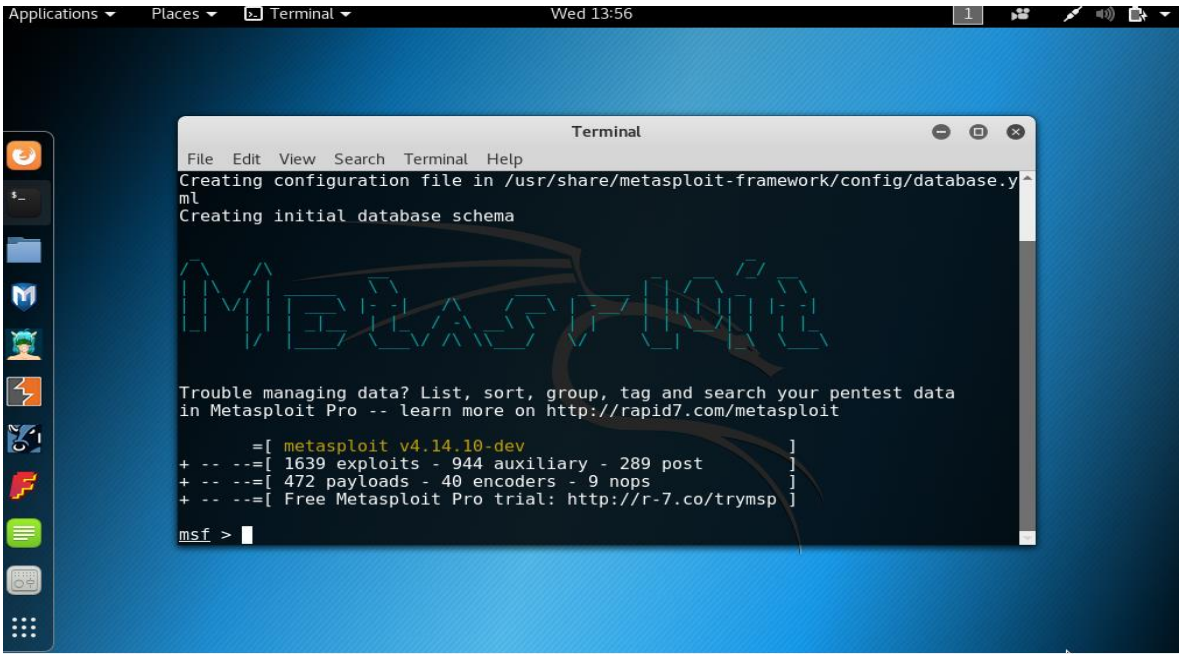


Figure: 3.2.5

The process of backdoor attack:

- Open metasploit
- Command : db_nmap -O -sV 209.165.200.235
- Take the ftp version name (vsftpd 2.3.4)
- Command : search vsftpd 2.3.4
- Take exploit_path
- Command : Use exploit path
- Command : Set RHOST 209.165.200.235
- Run exploit that means Command : exploit

- We have already known about details nmap. In the (Fig: 3.2.6), we know about the basic information about IP address by using nmap.

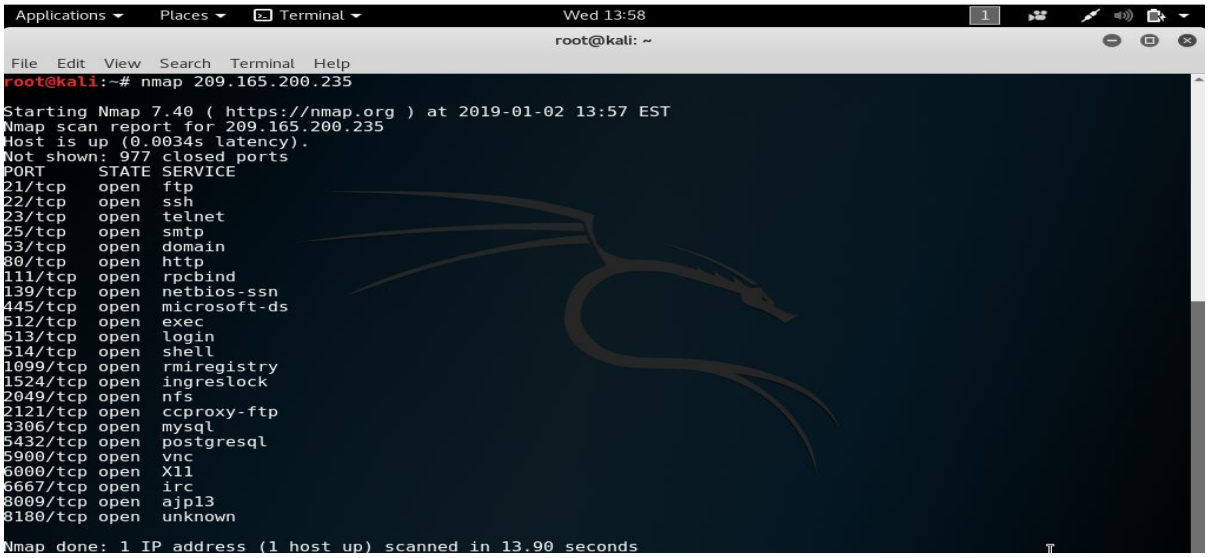


Figure: 3.2.6

- In this (Fig: 3.2.7), we are scanning victims port 21 using nmap. We are trying to service version detection using nmap and the command is - nmap –sV p IP address. P is the port number. Suppose p-21 that means port number 21, which port we want to scan for the version. We are going to scan 21 number port .21 TCP port and then next its ftp port .then press the enter we know about the basic information of IP address.

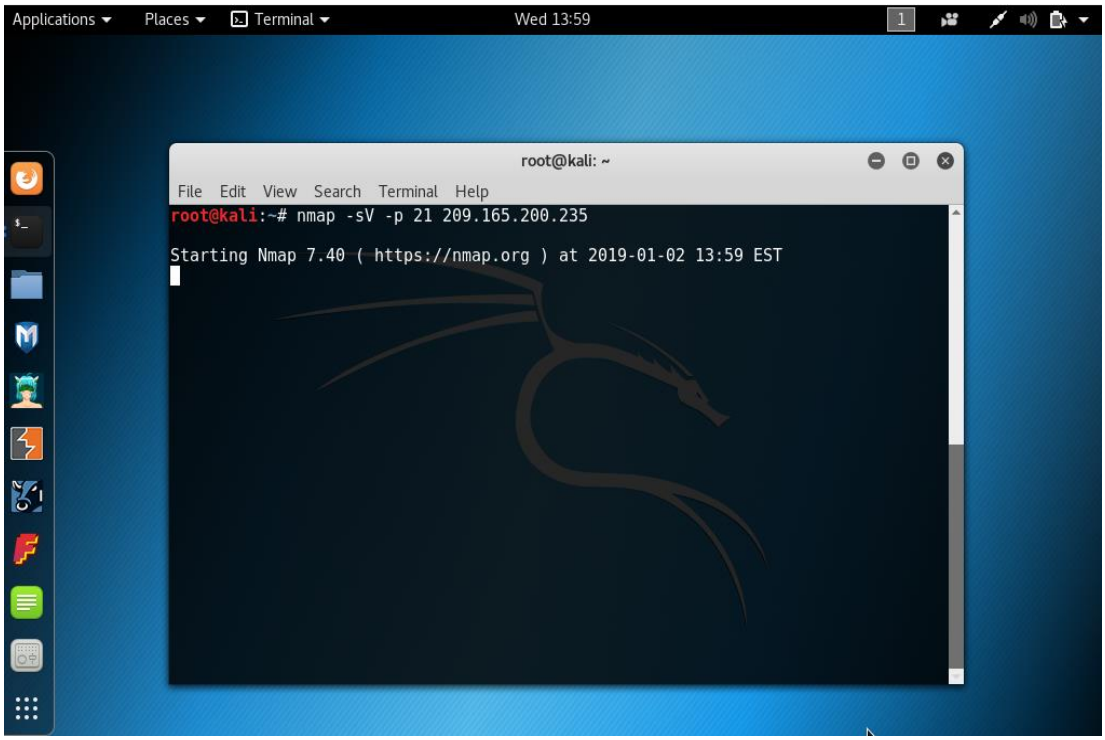


Figure: 3.2.7

- With this command we can determine the version of the service running on the port (Fig: 3.2.8). From this, we know about the **vsftpd 2.3.4.** It's about ftp version name.

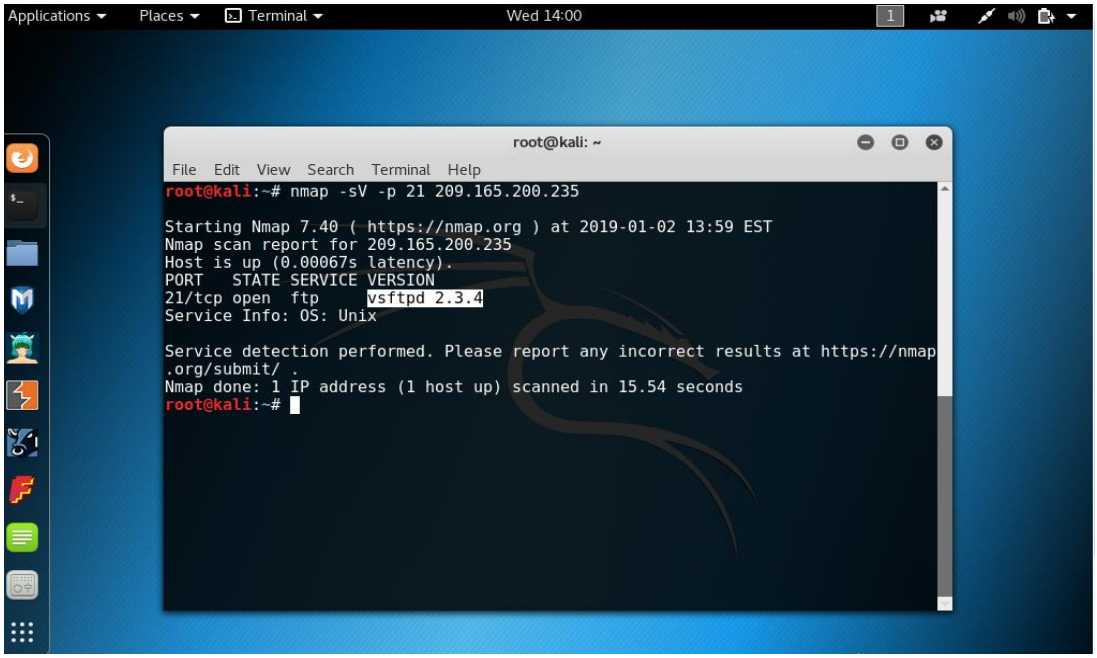


Figure: 3.2.8

- Here we write this command (Fig: 3.2.9) that is search vsftpd and then we see the exploit path name.

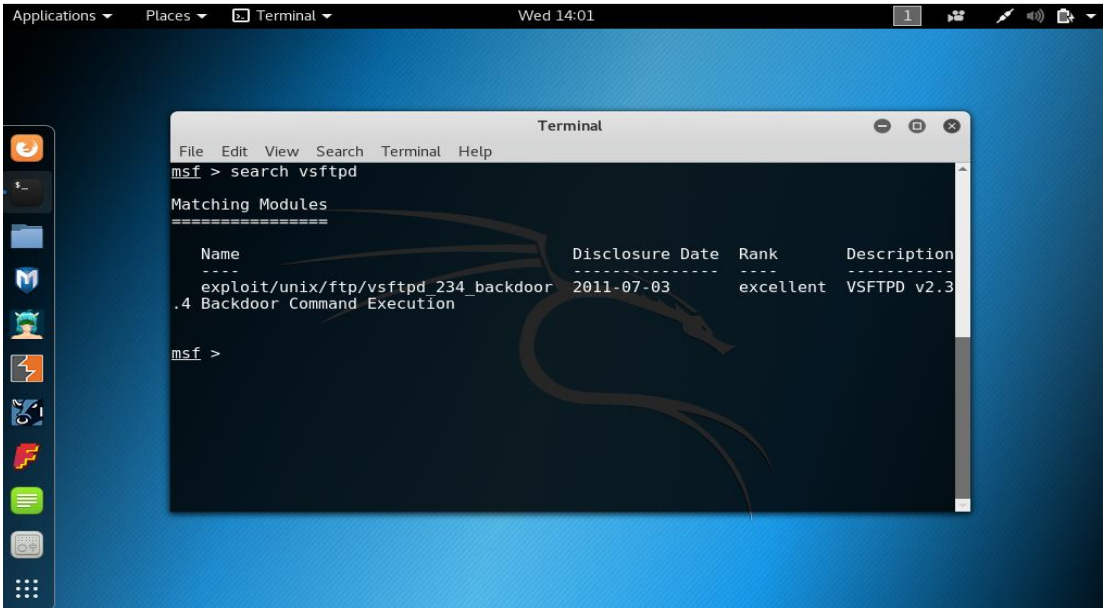


Figure: 3.2.9

- After that we use exploit path (Fig: 3.2.10) .when we enter the press button then we are basically going to inside backdoor attack. Path will be a most important and when we are know the path then exploit the path. Then set RHOST and run exploit.

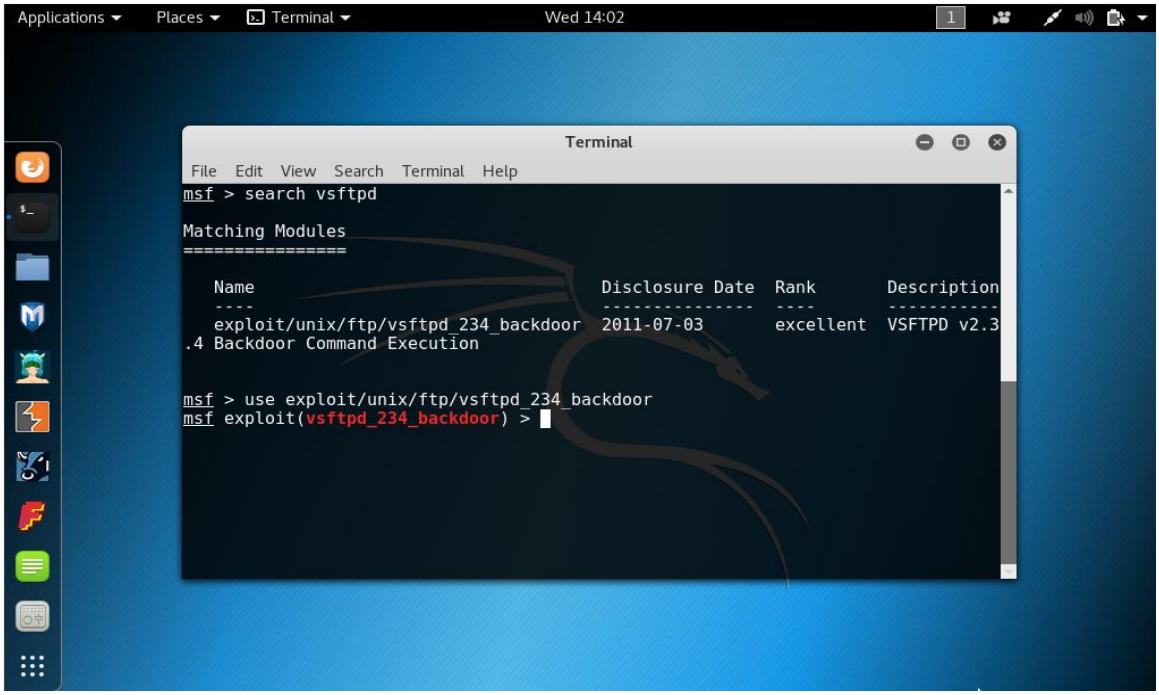


Figure: 3.2.10

- Whenever we use exploit we must use show option command (Fig: 3.2.11). So that this command gives us information that we needs to be. After show option command we see information missing that is current setting about for the target address. We have to know the target address to backdoor attack that is metasploit IP address on the other hand kali Linux that is control the target machine. After that the set of IP address and write the target address than we know about the information which is missing (fig: 3.2.12) that is we see all the information which we need. The command

Set RHOST target IP address (209.165.200.235)

After this command then all the information are properly done then finally run the exploit.

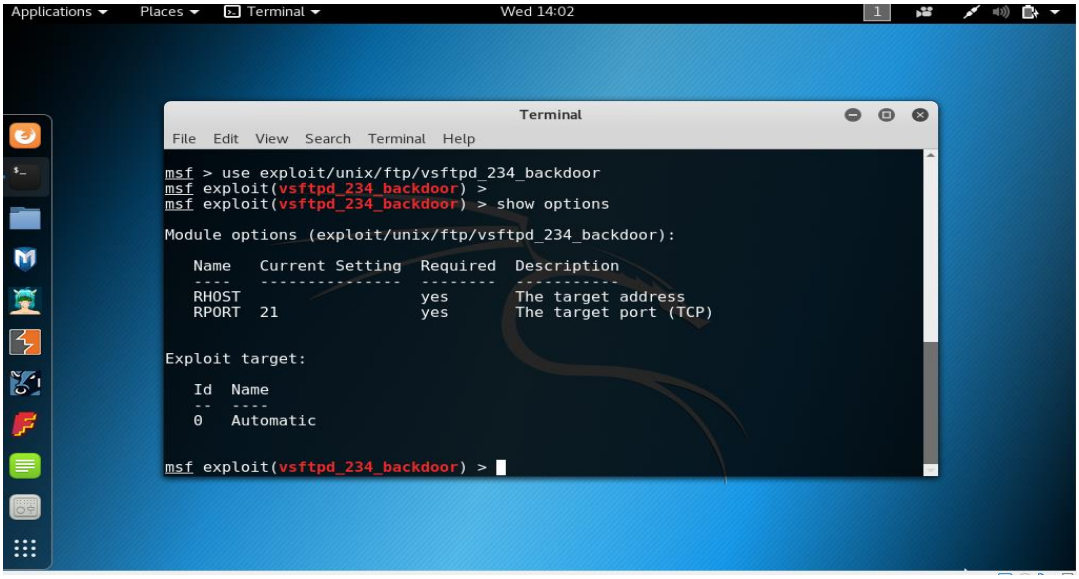


Figure: 3.2.11

- In this terminal(Fig: 3.2.12), we can see when we write to command like as Set RHOST target IP address (209.165.200.235) then all the information are properly done then finally run the exploit. After that successfully run the exploit then we see the terminals which is actually terminal towards target machine. So check this whoami-root. Now it's not for kali-Linux machine this is actually in other machine or server which is metasploit. After successfully run the exploit then we see in command shell. In this command shell we write or see everything. We see all the files like as ls or other things all of this are other server files. That is successfully backdoor attack into another remote system.

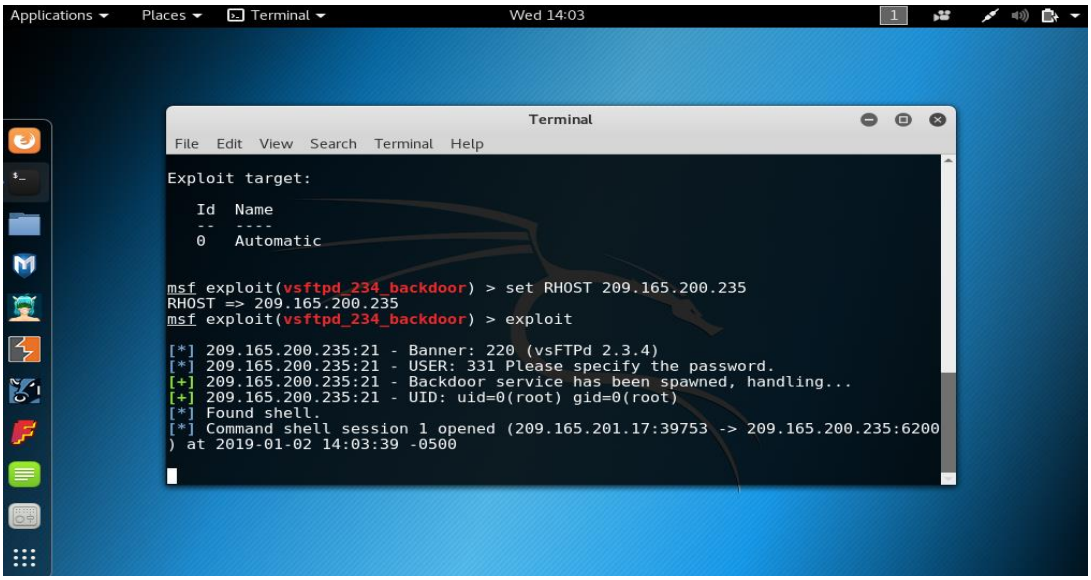


Figure: 3.2.12

- After successfully run the exploit then we see in command shell. In this command shell we write or see everything. We see all the files like as ls or other things all of this are other server files. That is successfully backdoor attack into another remote system. Here we see also some files which is already present in the metasploit server and check the kali-Linux that is exactly the same files so we have successfully done the backdoor attack (Fig: 3.2.13).

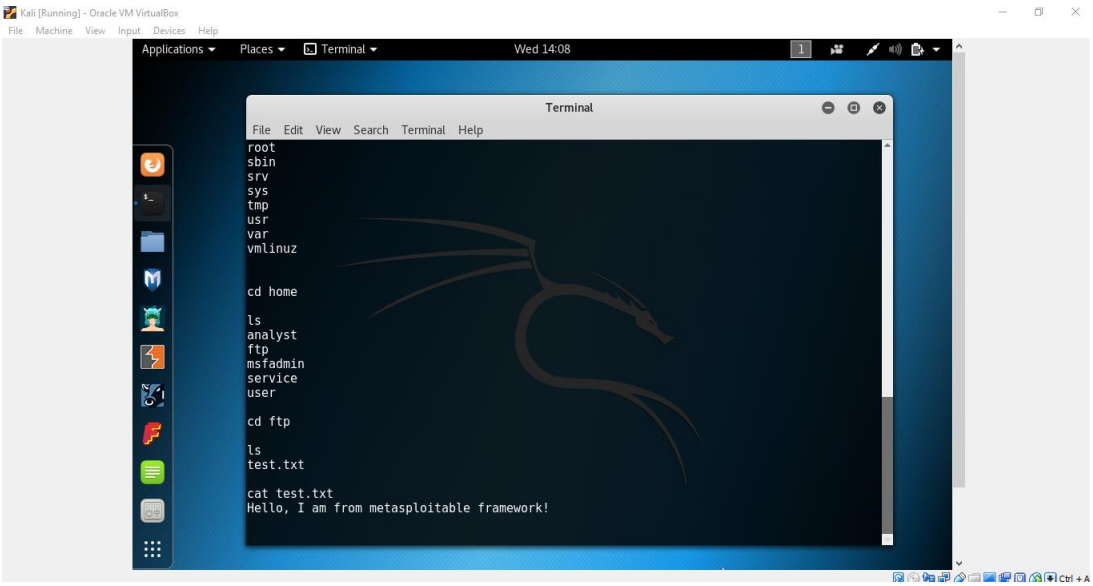


Figure: 3.2.13

- In the (Fig: 3.2.14), we know about the interface of sguil. Generally, when the username and password are entered by the Sguil interface which is given in the set up then sguil is open.

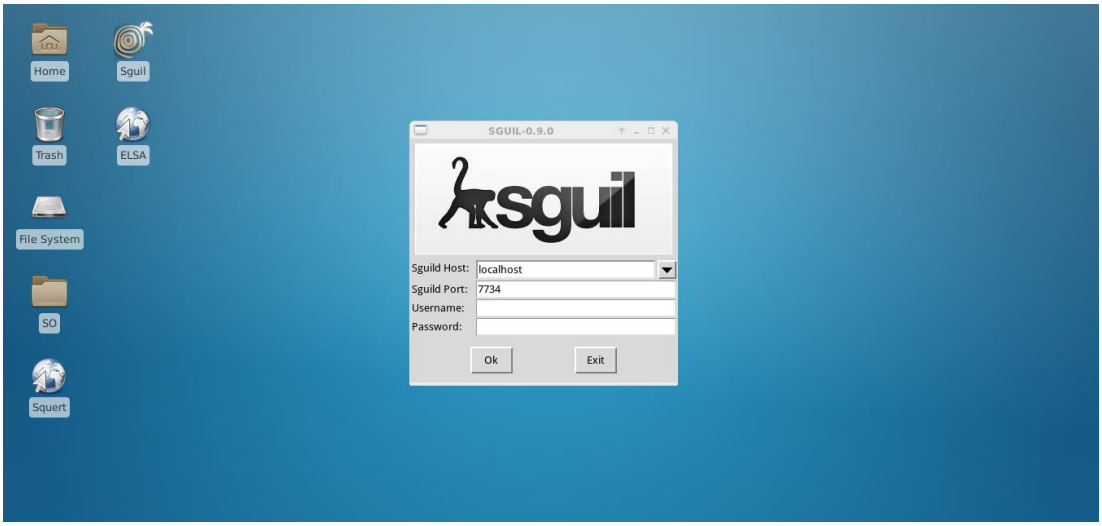


Figure: 3.2.14

- Initially sguil dashboard is empty (Fig: 3.2.15).

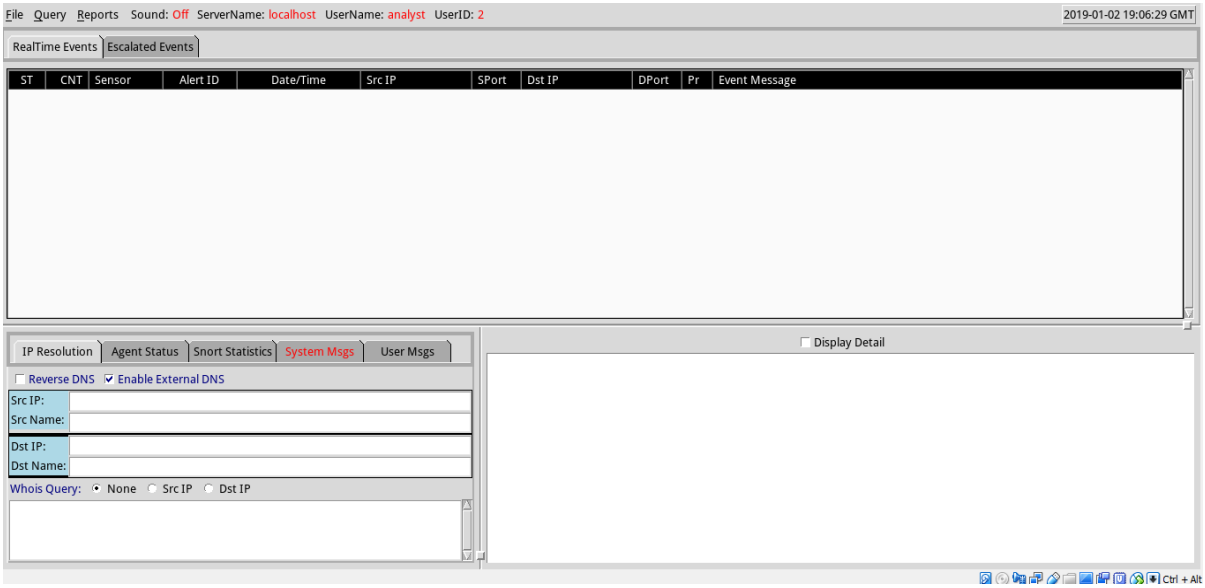


Figure: 3.2.15

- After exploiting, we can see Sguil (Fig: 3.2.16) capture many events for the unauthorized access which we have gained by exploiting. We see in each events source port, destination Port, source IP, destination IP etc. In events, we see ST in different colors. Some colors are red which events are really attacking for a virus.

When mouse pointer point on Alert Id of an event, there will be many options for analysis a malware like a transcript, Bro, Network Miner.

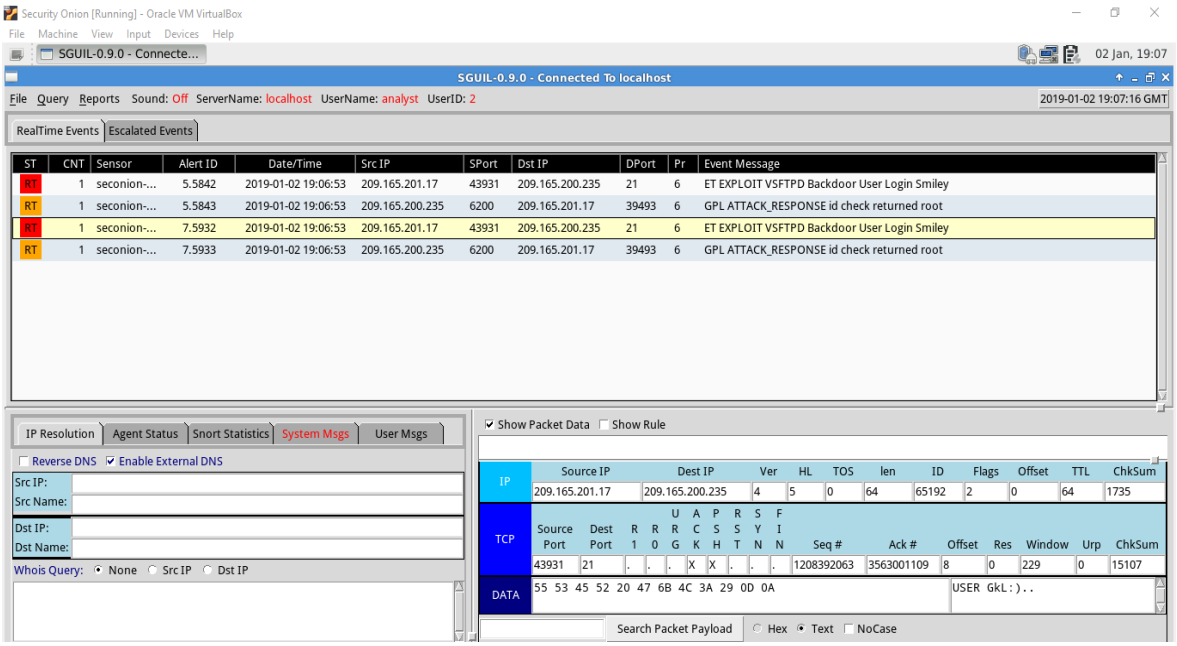


Figure: 3.2.16

3.3 Analysis the Captured Events

- Squert provides Network based IDS, Host based IDS alerts, PRADS data, HTTP logs. This tool helps to view event in sguil database. First we login Squert by providing the username and password of Sguil (Fig: 3.3.1).

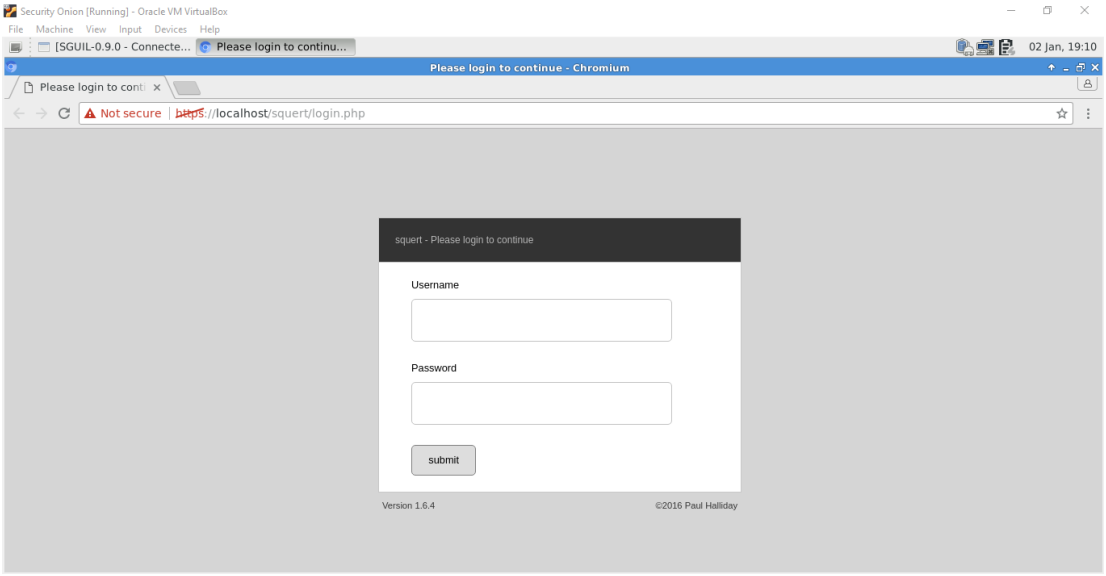


Figure: 3.3.1

- After login we can see Squert dashboard (fig: 3.3.2) where there are options for events, IP address locations, summary. Here some sort of term as SC, DC, Last event, ID is remained. Also same type of event can be grouped if needed. Squert also use capME to capture full packet.

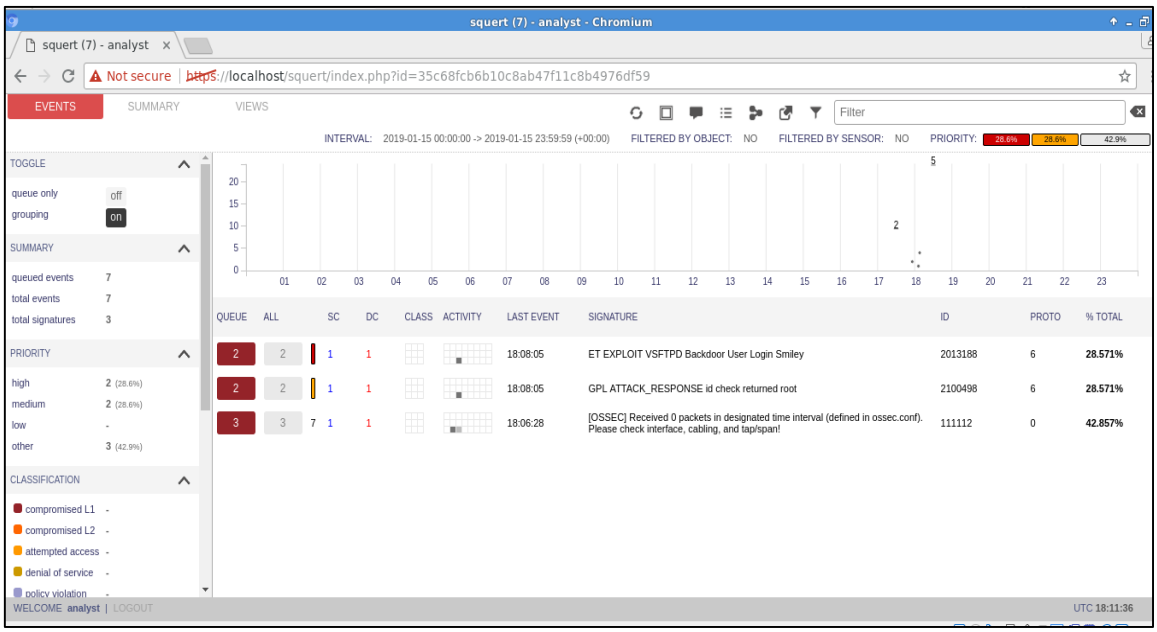


Figure: 3.3.2

- In this dashboard (Fig: 3.3.3), where we can see view some ip, source country, Destination country and their information etc. In this dashboard, the main part is the view of ip location.

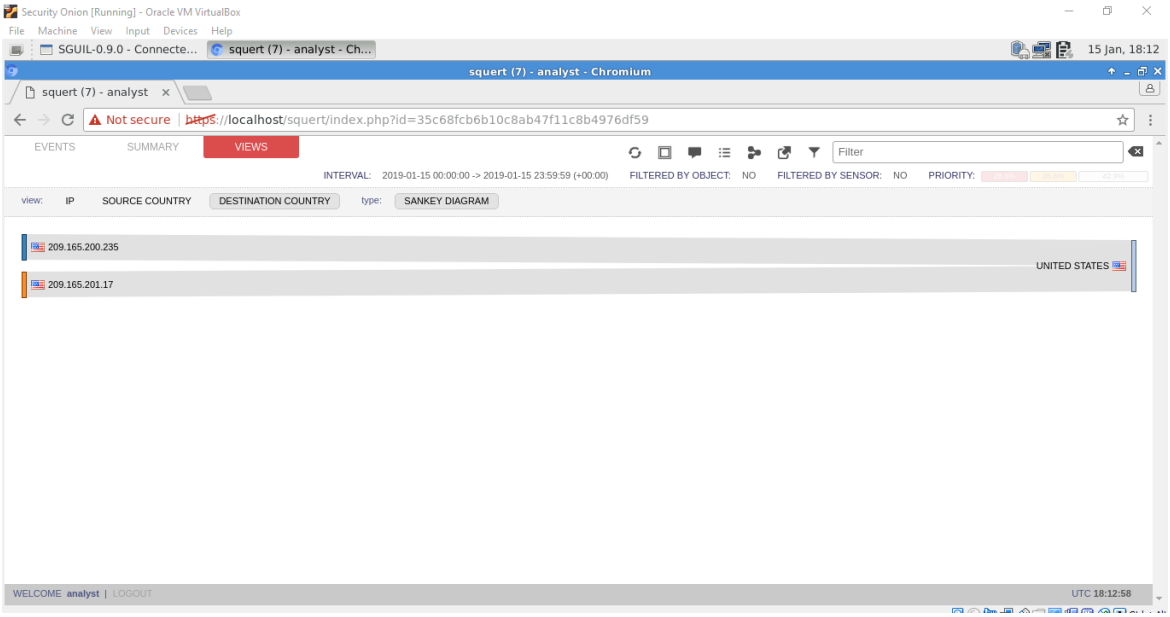


Figure: 3.3.3

- In this dashboard (Fig: 3.3.4), when we click one of this IP of countries then we can see the details or full information about these countries. Here we can see the top signatures, top source IPS and top destination IPS, top source countries and top destination countries etc.

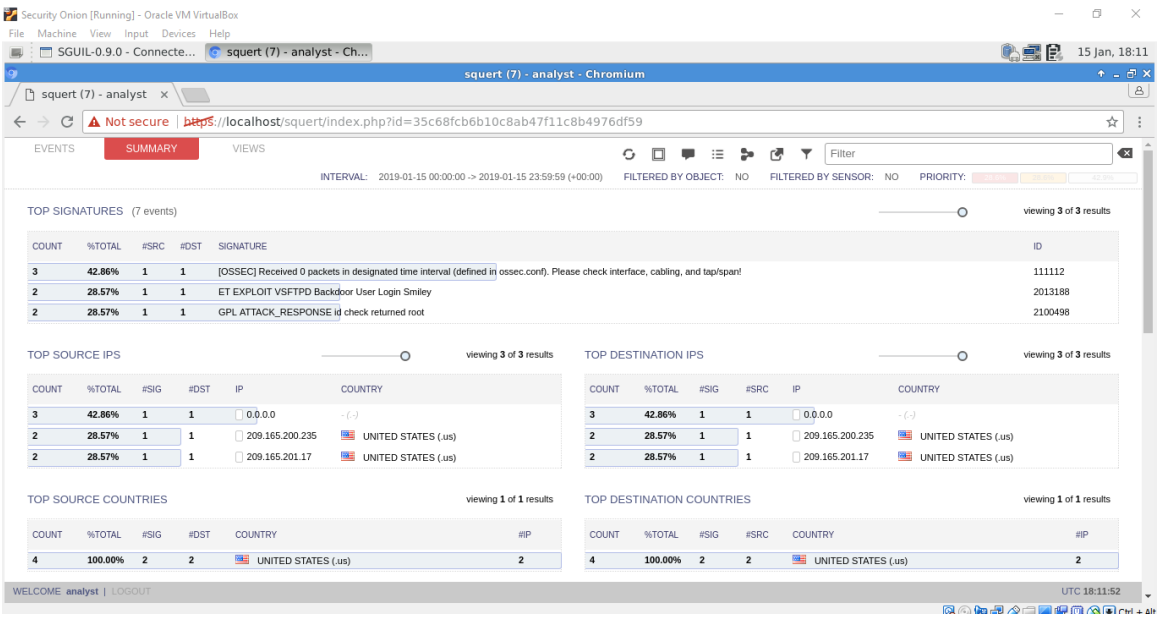


Figure: 3.3.4

- In this dashboard (Fig: 3.3.5), we can see about the port that is top source ports and top destination port etc. In top ports we can see the results about SIG, SRC and DST etc. Similarly in destination port we can see the results about SIG, SRC and DST etc.

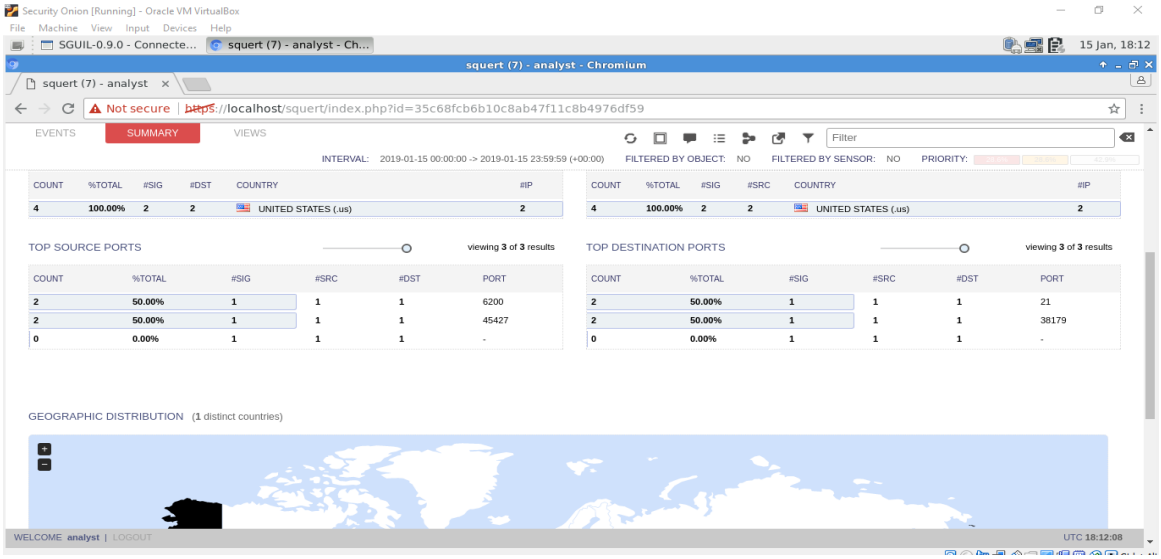


Figure: 3.3.5

- In case of an attack, from the Region, it is a view to measure it. As a result, we can easily see the map from where it comes from (fig: 3.3.6)

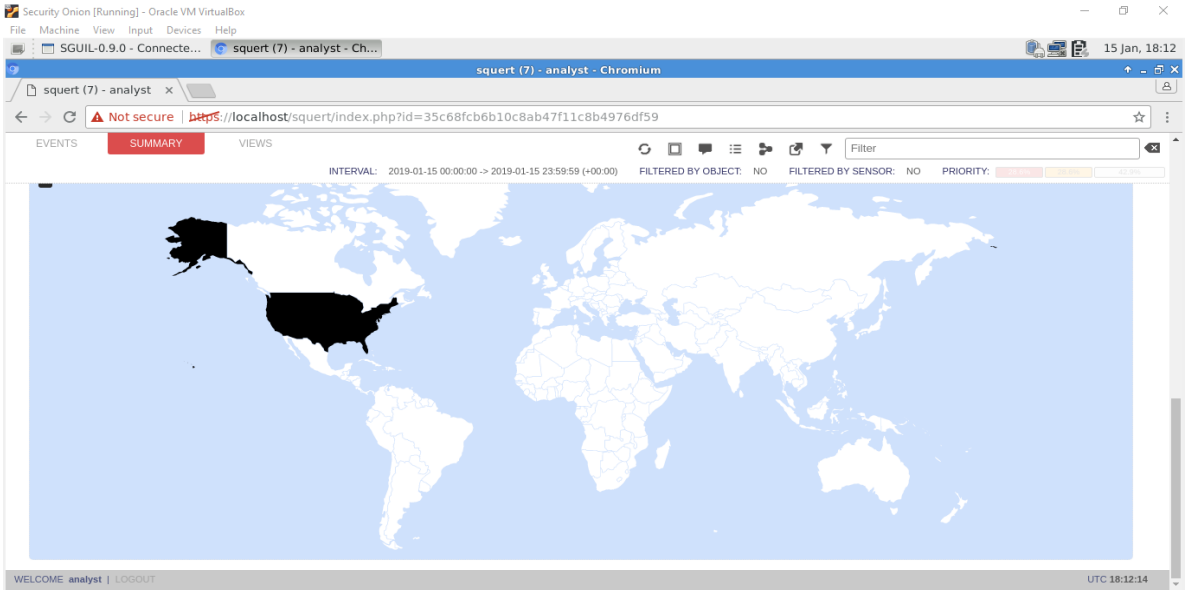


Figure: 3.3.6

- Here is the interface of Elsa (Fig: 3.3.7). First we login Elsa by providing the username and password of Sguil.

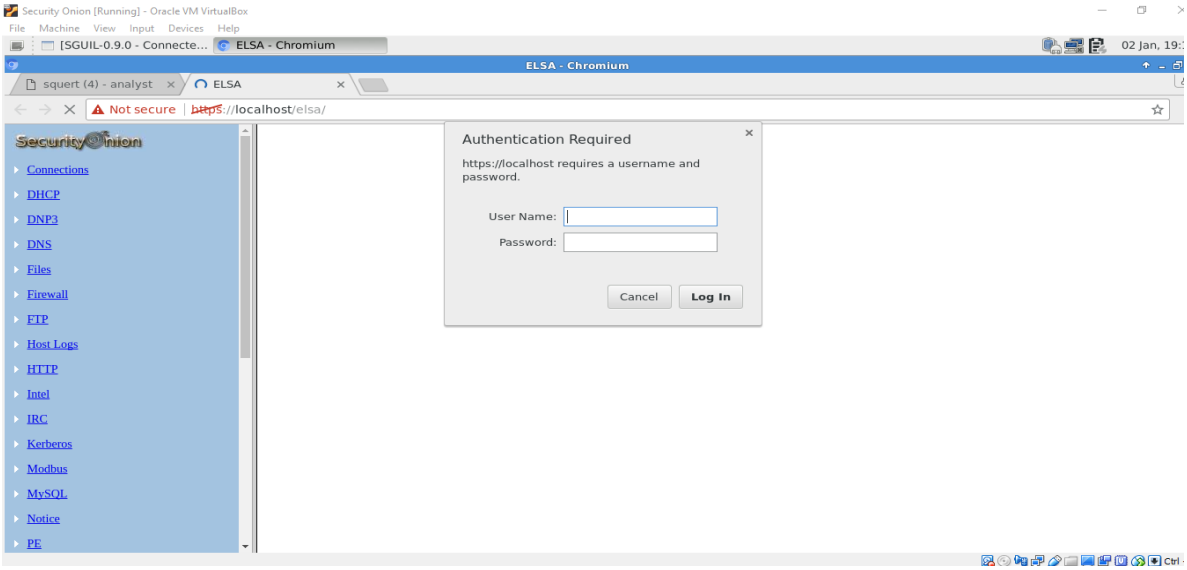


Figure: 3.3.7

- Elsa basically works as a query (Fig: 3.3.8).When we write down the IP address then we can see lot of files. We can also see about files name, hostname, class etc. we are basically working with bro. in this dashboard we can see an option like as info. When we click info option then we can see more files.

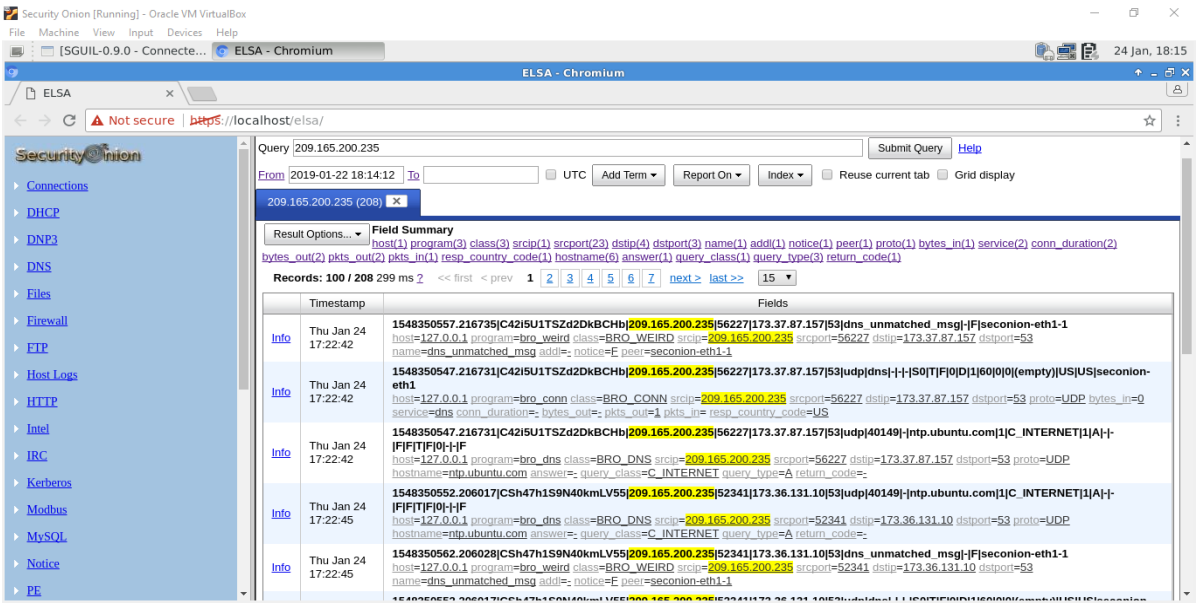


Figure: 3.3.8

- When we click file option then we can see a statistics about bro (fig: 3.3.9). Here we can see count as well as their value like as bro_com, bro_dns etc.

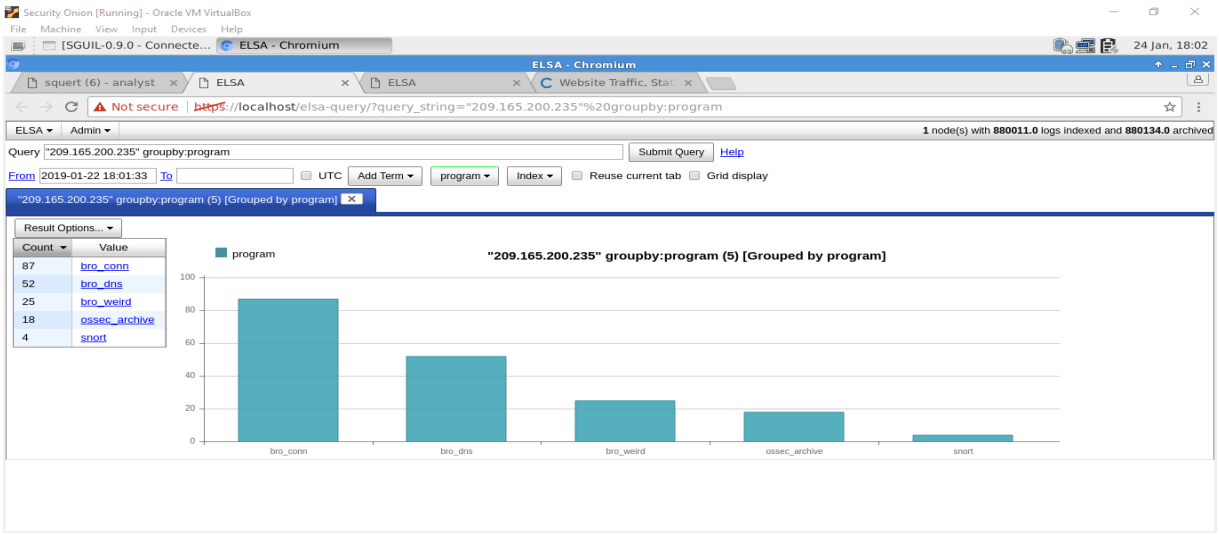


Figure: 3.3.9

- We already know about Squert also use capME to capture full packet. Here is the capME interface (Fig: 3.3.10). In this interface, we need to write Src IP and Dst IP then click to submit

Button after that we know full information about ip address or port etc.

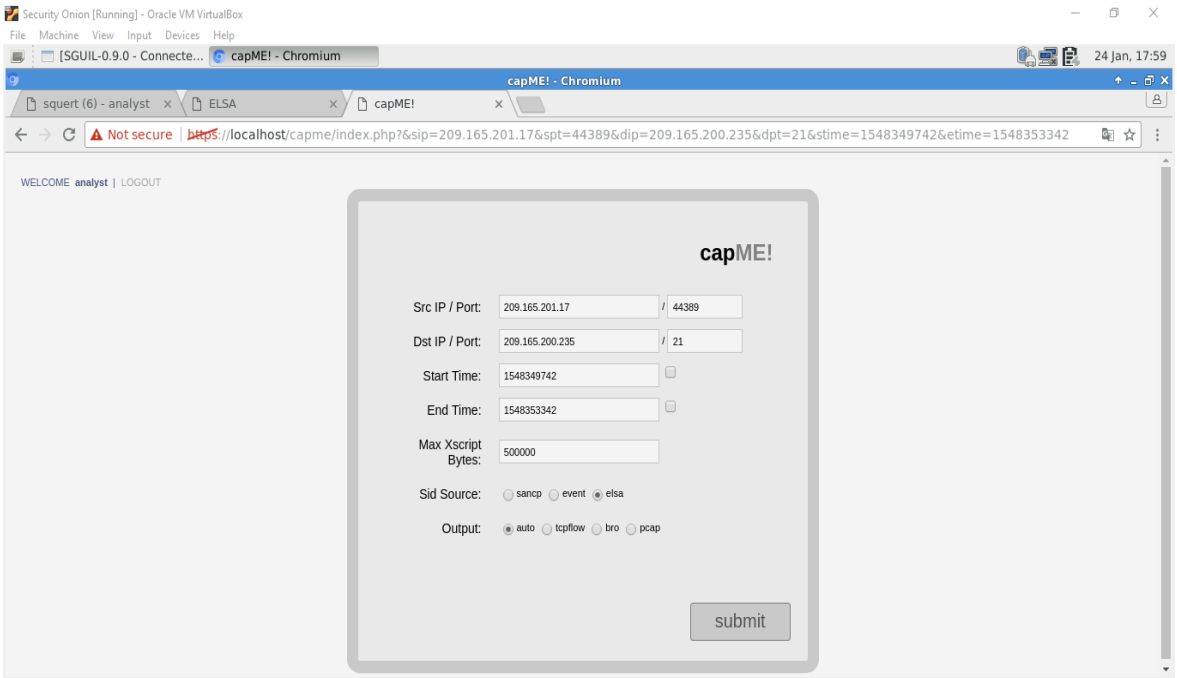


Figure: 3.3.10

- After click the submit button we know about Sensor Name, Timestamp, Src IP or Src port and also dst IP or Dst port. Also we can see the full details about data when data will be sent. In this (Fig: 3.3.11), we can see that no data has been sent that's why we don't know about the full information of the data.

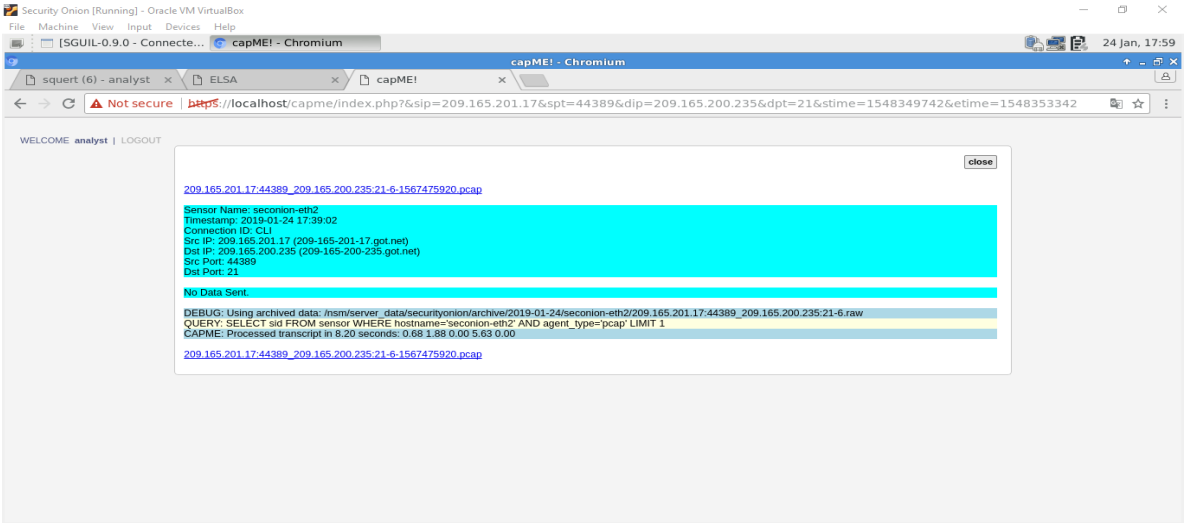


Figure: 3.3.11

3.4 Recorded File Analysis

- To analyze a malware first we have to download a malware pcap file.
- We used www.malware-traffic-analysis.net sit to download malware pcap file (Fig: 3.4.1).

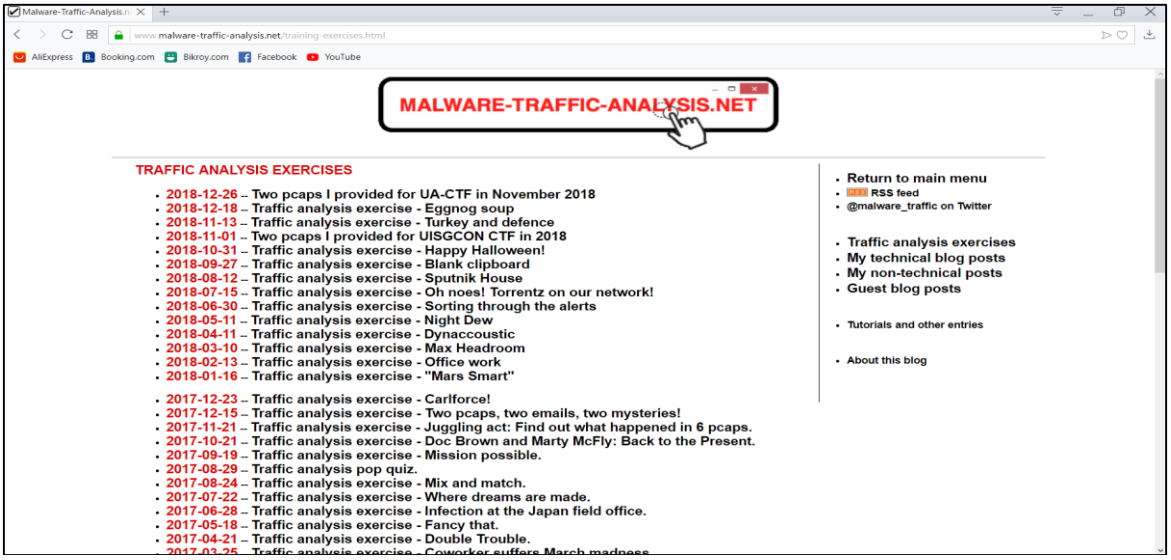


Figure: 3.4.1

- Generally, when the username and password are entered by the Sguil interface which is given in the set up then Sguil is open now to trace events(Fig: 3.4.2).

Basically, Sguil is a GUI interface. Then we are going to open the terminal to write the command and see how Sguil traces the events.

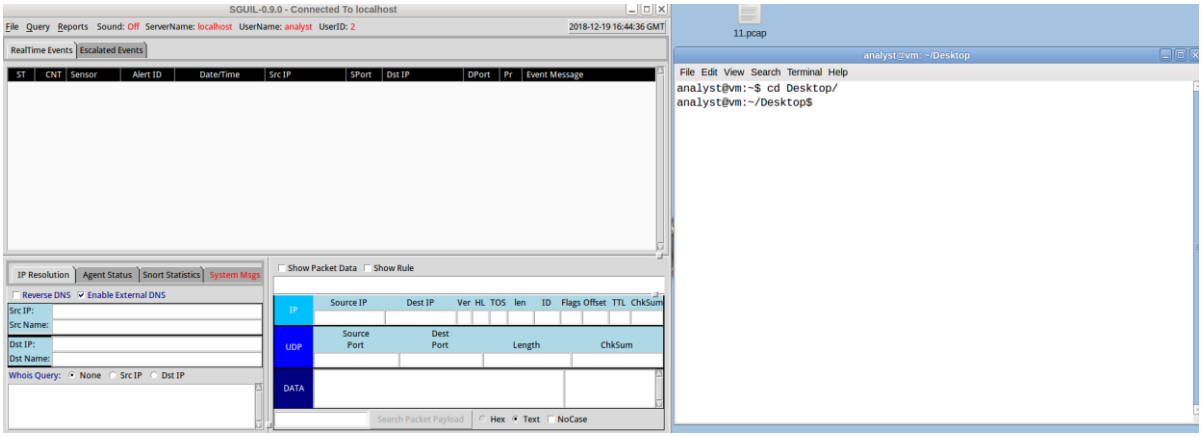


Figure: 3.4.2

- To analyze a malware first we have to download a malware pcap file. We used www.malware-traffic- analysis.net sit to download malware pcap file. Then we open in terminal and go to desktop option. In the terminal, we have to run a command for malware pcap file (Fig: 3.4.3) sudo tcpreplay -i eth0 -M10 11.pcap. After that, Sguil is showing, many events and we see this event and also this event in a virus or not.

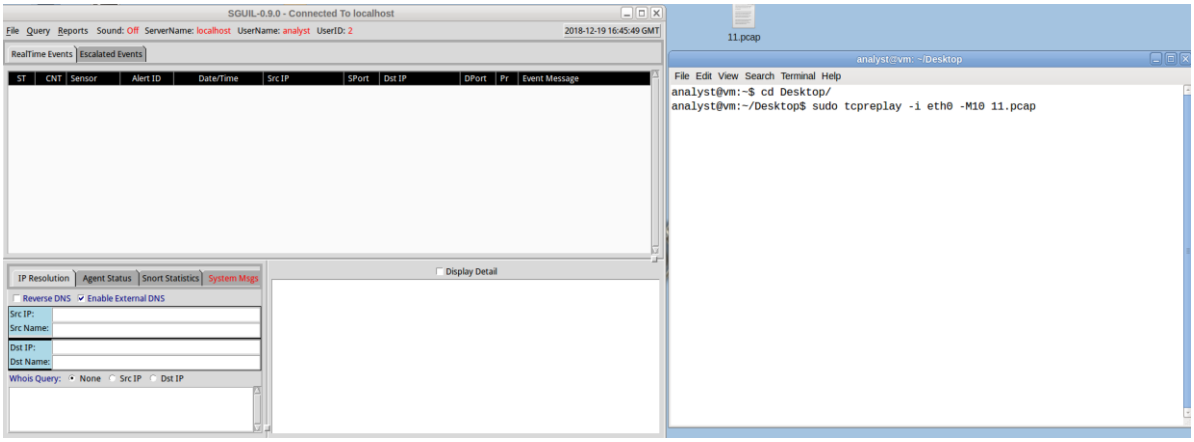


Figure: 3.4.3

- After running this command, Sguil shows many events for the pcap file. Also, we see in the terminal, how many packets are successful, how many packets are failed, how many packets are attempted etc. we see in each events source port, destination port, source IP, destination IP etc. In events, we see ST in different colors. Some colors are red which events are really attacking for a virus (Fig: 3.4.4) that means

normally danger of the events indicated with different colures. When mouse pointer point on Alert Id of an event, there will be many options for analysis a malware like a transcript, Bro, Network Miner.

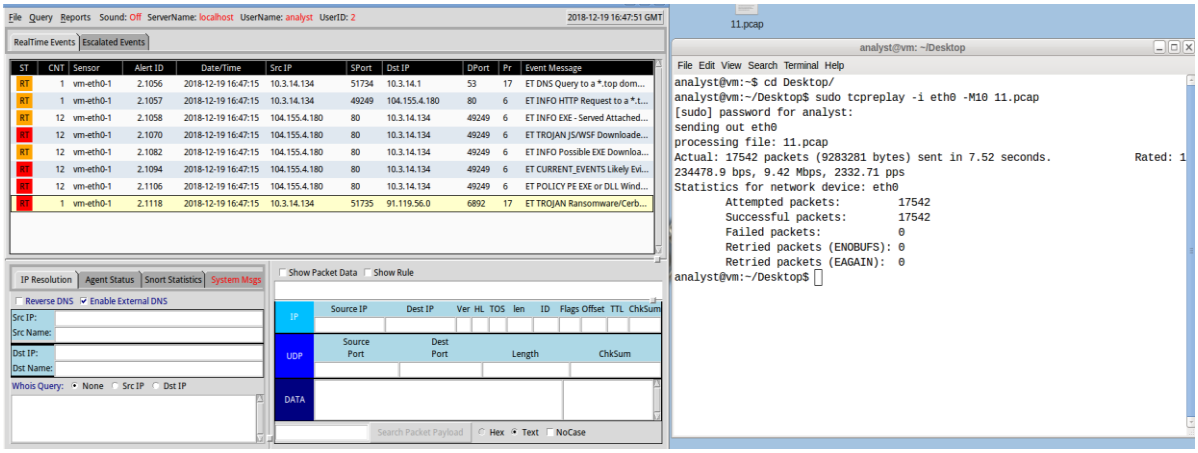


Figure: 3.4.4

- In this (Fig: 3.4.5), we see show packet data and show rule that has been used for a particular event. In network miner, we can get those files for which this event/virus is generated (Fig: 3.4.5). Network Miner can extract files, emails and certificates transferred over the network by parsing a PCAP file or by sniffing traffic directly from the network. We also get the host, server details.

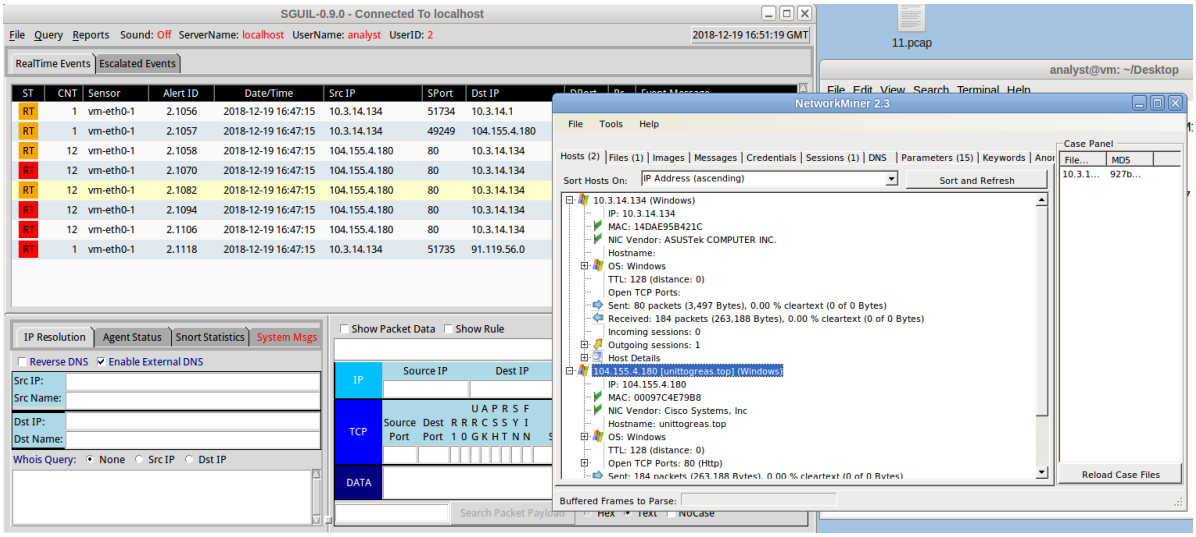


Figure: 3.4.5

- When we click on the file option, there will be some options (Fig: 3.4.6). But the major option is Calculate hash. Using this, we can calculate the hash of the selected file. Hash number will help to identify that is the file really corrupted or not.

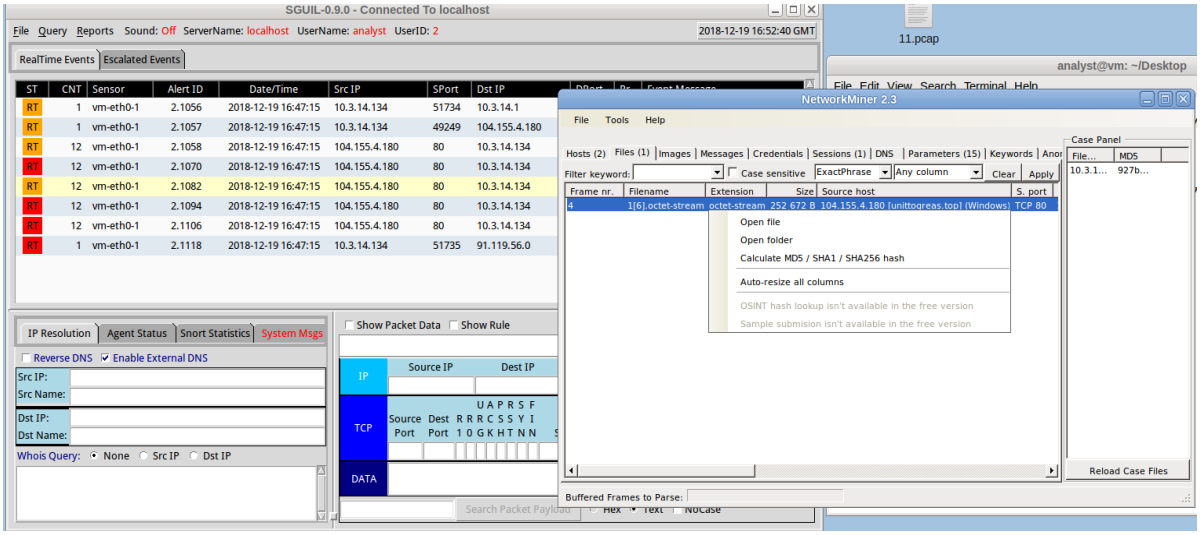


Figure: 3.4.6

- After click on the Calculate Hash option (Fig: 3.4.7), we get a new window with some information. Then using the hash number we will get the exact information of this file.

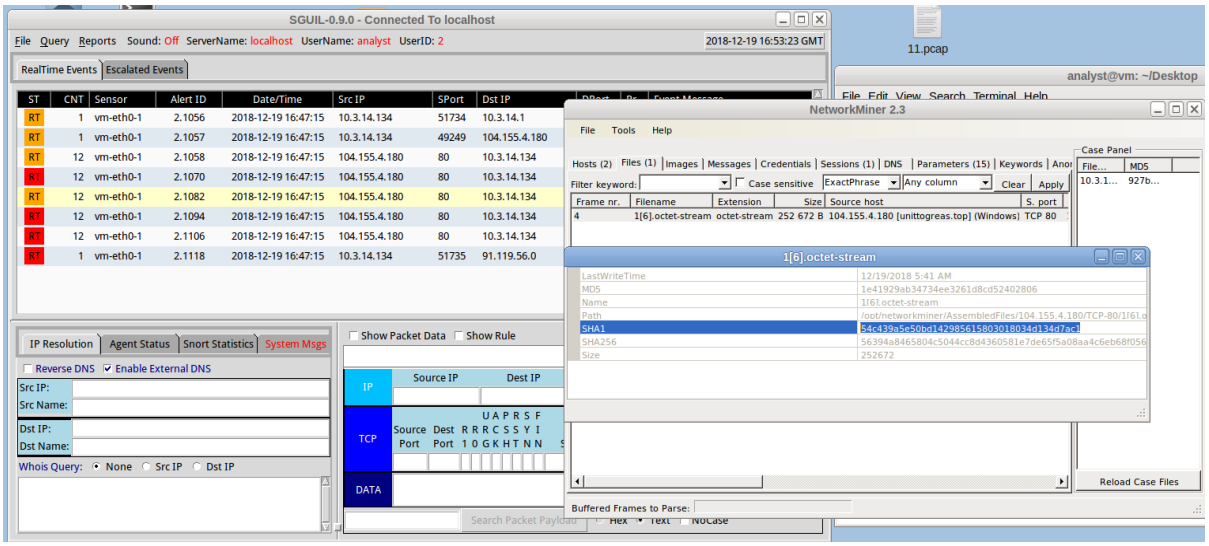


Figure: 3.4.7

- This is the virus total website (Fig: 3.4.8). Here we can search the hash file or SID for each event and see the file is a virus or not. If the review of this file is red color, and from this details, we can say that this file generates a virus, on the other hand, the review of this file is green, and from this details, we can say that this file does not generate a virus.

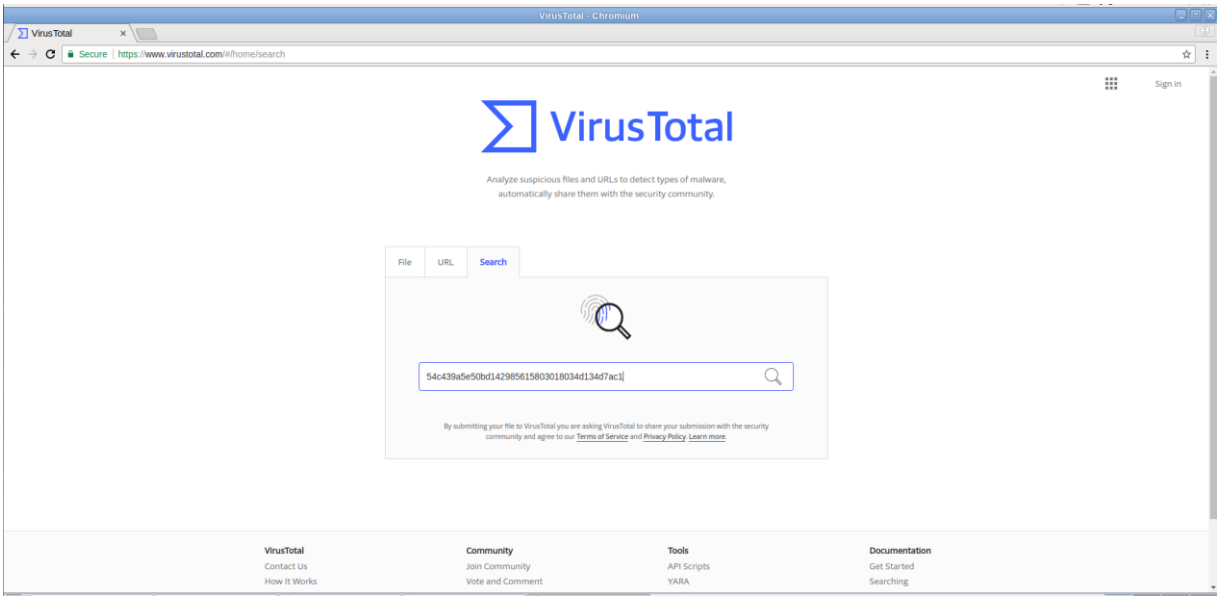


Figure: 3.4.8

- Here we see that Most of the review of this file is red color, and from these details, we can say that this file generates a virus (Fig: 3.4.9).

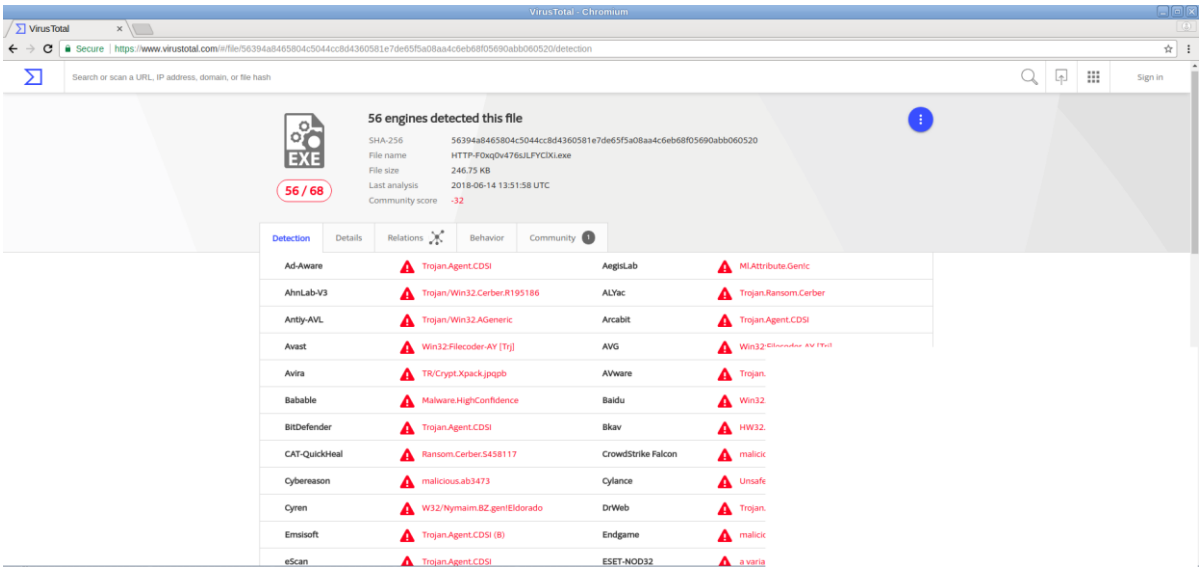


Figure: 3.4.9

- Here we see that Most of the review of this file is red color, and from these details, we can say that this file is generating a virus but some file is green color but this is not helpful for this file. (Fig: 3.4.10).

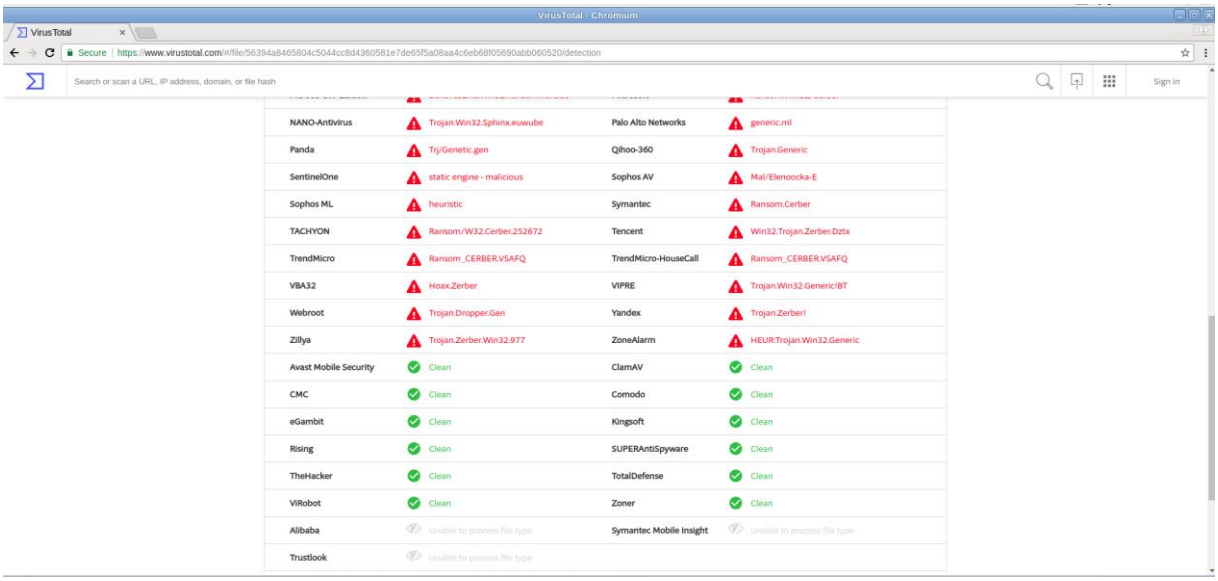


Figure: 3.4.10

- User can see the entire event by clicking the mouse button and choosing the option needed that is transcript or bro. This function is provided by transcript (Fig: 3.4.11).

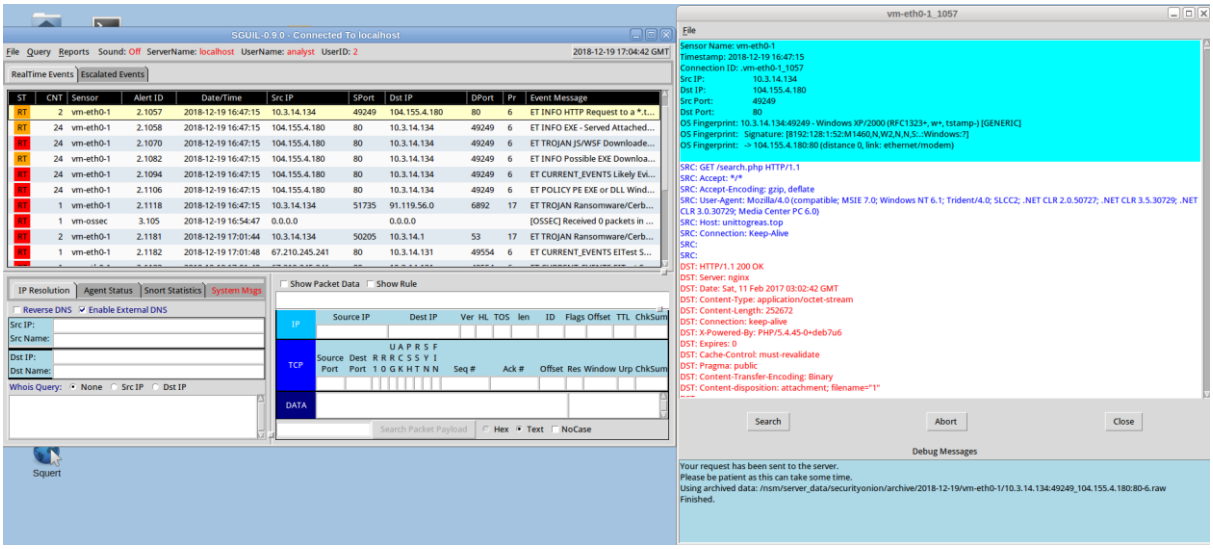


Figure: 3.4.11

- User can see the entire event by clicking the mouse button and choosing the option needed that is transcript or bro. This function is provided by Bro (Fig: 3.4.12). When we open Sguil to launch any event, we can go to the Bro option and see the contents of the event, and we know that this is the HTML File or PHP file. Apart from this, we can also know about timestamps. Bro is generally a strong network. This is a network that we can analyze this network on the framework. It works as a top-level application.

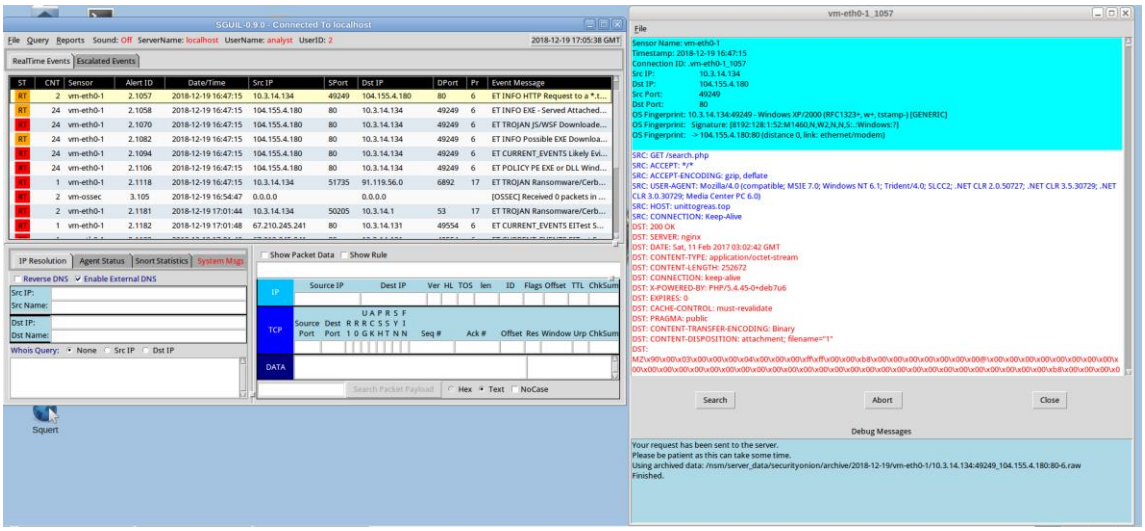

SGUIL-0.9.0 - Connected To localhost
vm-eth0-1_1057
Squert
Search
Abort
Close
Debug Messages

Figure: 3.4.12

Chapter 4

Limitations, Challenges and Future Works

4.1 Limitations

Our main goal was preparing a model for securing vulnerable networks from unauthorized access and detecting data damages. We tried our best but there are some limitations of our work. For now, we can identify the unauthorized access events and analyze those. It will work for any network if configured the network properly.

In this project, we have used Elsa for analyzing the captured malicious events. But this tool is not available for all version of Security Onion. This tool is available only for lite version. Instead of this tool, we can use Kibana. This is updated version of Elsa and compatible for all version.

4.2 Problems we faced

Our topic is security monitor, detection and analysis. We faced many problem to prepare this issue. First of all, we did not get any kind of clear information or resource, by which we can get the prepare knowledge. We read many paper about security issues, monitor issues, but there was not enough ideas.

Second, we faced a major problem, which is tools version problem. We used three versions of security onion but each and every version there was some limitations. In analyses process we saw that, Elsa did not work properly, sometimes Kibana and Squert did not give accurate summery of an event. So basically security onion tools are depend on which version we are using.

Third, as far we know day by day software getting updated so, when we tried to setup an environment using Kali Linux, Metasploitable and Security Onion we faced space problem in our device and also version problems.

In backdoor attack process sometimes exploit did not work successfully because, we did not get accurate exploit port version, exploit path.

When we used malware pcap file to analyses events on security onion sometimes events also not captured in sguil. From captured events we did not get enough necessary data by which we can declare that it was a virus or not.

4.3 Future Extensions

The work we did now is a primary label work. In the future, we want to do a lot about it. Those things are:

- We are now using many tools. But in the future we will use the advance tools like as Kibana. We know Kibana is a powerful tool. We will use advance tools to detect and analysis malicious events. Here is the Kibana interface

- We've already analyzed our record Pcap files. But in the future we will try to further analyze our record Pcap files.

- We will use advance analysis using CapMe Plugin. If big Pcap files are here then we can see huge information about this Pcap files by using CapMe Plugin

- Try to exploit secure devices like windows. But the most important part is data damage analysis. We see every day that the data is going hacked. Suppose when the hacker access our machine, then they will take some data or complete data from there or put some malware input in our machine. In that case the data becomes unreliable. As a result how many data will be lose or some range all of these are we will work in future.

Chapter 5

Conclusion

We know that number of device increasing day by day. Secure device is important but not enough. Secure device is also hack able. We need three things to overcome this problem like as monitoring, detection and analysis. We have using some security onion tools in our analysis part like as Elsa, Squart etc. Try to overcome this situation we also need experienced people to take this challenge.

We see that only 38% of global organizations claim they are prepared to handle a sophisticated cyber-attack which is very poor number. That's way we hope that this rate will be increase in future. We also hope that we will be combining our analysis part for any organization in future.

References

[1] Ecpi Blog. (2018). *Importance of Network Security: Safety in the Digital World* [Online]. Last accessed on 2019, January 23. Available: https://www.ecpi.edu/blog/importance-of-network-security-safety-in-the-digital-world

[2] CSO. Josh Fruhlinger. (2018, Jul 03). *What is Network Security?* [Online]. Last accessed on 2019, January 23. Available: https://www.csoonline.com/article/3285651/network-security/what-is-network-security-definition-methods-jobs-and-salaries.html

[3] CSO. Steve Regan. (2017, Sep 13). *Penetration Testing Tools and the Pros Use* [Online]. Last accessed on 2019, January 24. Available: https://www.csoonline.com/article/2943524/network-security/17-penetration-testing-tools-the-pros-use.html

[4] Github. Weslambert. (2018, Sep 12). *Introduction to Security Onion* [Online]. Last accessed on 2019, January 24. Available: https://github.com/security-onion-solutions/security-onion/wiki/IntroductionToSecurityOnion

[5] Shahmeer Amir. (2017, Sep 16). *Penetration Testing of an FTP Server* [Online]. Last accessed on 2019, January 24. Available: https://shahmeeramir.com/penetration-testing-of-an-ftp-server-19afe538be4b

[6] Rapid7. (2018). *Metasploitable 2 Exploitability Guide* [Online]. Last accessed on 2019, January 24. Available: https://metasploit.help.rapid7.com/docs/metasploitable-2-exploitability-guide