A Survey on Network Security Tools for Open Source

Nabanita Mandal
Computer Engineering Dept.
Thadomal Shahani Engineering College
Mumbai, India
nmandal88@gmail.com

Sonali Jadhav
Computer Engineering Dept.
Thadomal Shahani Engineering College
Mumbai, India
sonalighadge14@gmail.com

***Abstract* - Providing security to the network in an open source has become a major challenge nowadays. Data transmitted through the network is not considered to be safe. Various threats like sniffing, spoofing, phishing exist. This paper presents an overview of various network threats and attacks to the network. There are many tools in the open source which are developed as a counter measure to these attacks. Tools like nmap, tcpdump, firewall, wireshark has been discussed in this paper.**

Keywords- Vulnerability; Reconnaissance; Spoofing; Sniffing; Firewall

I. INTRODUCTION

Network security consists of the policies adopted to prevent and monitor denial of a computer network, authorized access, modification & misuse of computer. It is the process of taking software and physical preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers. The aim of network security is to provide authorization in order to access data in a network. Network security starts with authentication, which it provides using a username and a password. Another way to provide security is using firewall. Firewall enforces access policies like what services are allowed to be accessed by network administrator.

II. NETWORK VULNERABILITY

Vulnerability can be defined as a weakness that is present in every network. Threats are from the people who are interested in taking advantage of this vulnerability. The attacks are launched using various tools. Not only the TCP/IP protocol stack but also the network equipments [1] are vulnerable to attacks.

To attack a particular machine, the first step is Reconnaissance. The term Reconnaissance means gathering information about the victim. Reconnaissance can be active or passive. In active reconnaissance there is a direct interaction with the client. The tools are mainly dig, whois, traceroute and nslookup. Fig. 1. shows the dig command which is used for reconnaissance.

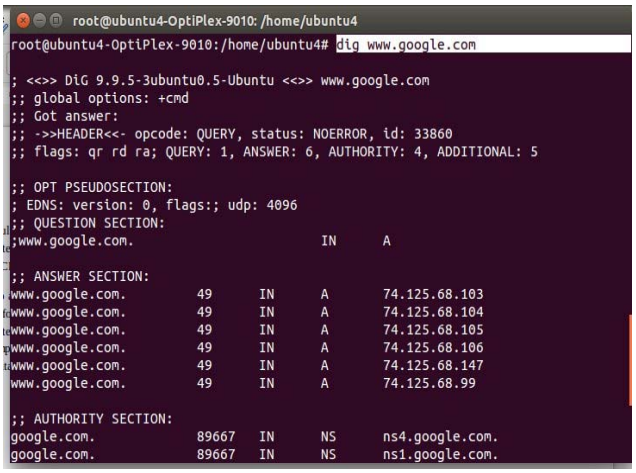

Fig. 1. Dig Command

The passive reconnaissance can be implemented using Netcraft which is a UK based company. It tracks virtually every website and offers data which is extremely valuable to the hacker.

Fig. 2. shows the whois command which a protocol for getting the response of a query from the whois database.

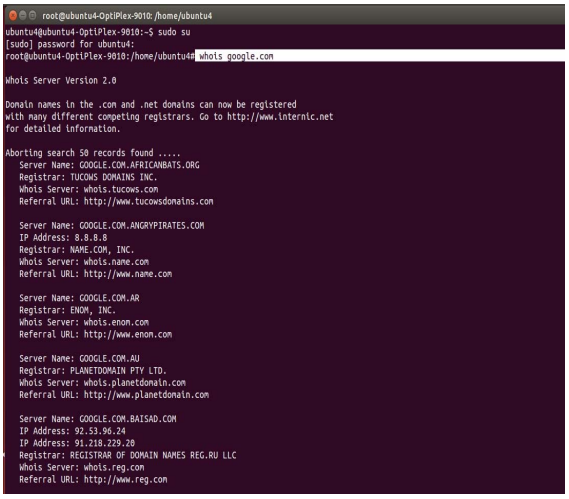

Fig. 2. Whois Command

978-1-5090-1936-6/16/$31.00 ©2016 IEEE

Fig. 3. shows the traceroute command. Traceroute is used to find out ip addresses of routers and firewalls that protect victim hosts.

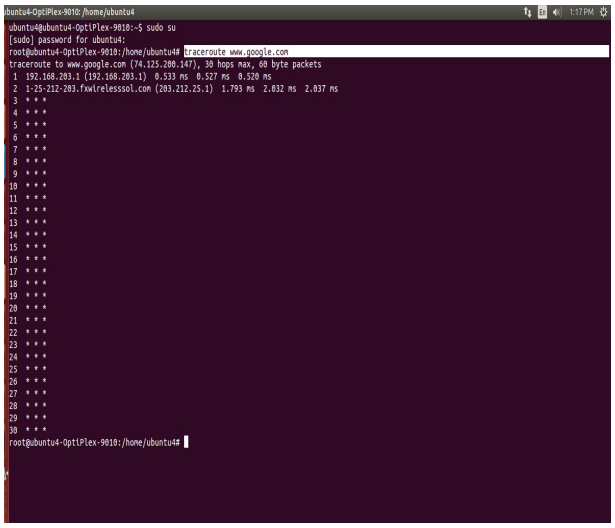

Fig. 3. Traceroute Command

The nslookup command shown in Fig. 4. is used to query internet name servers interactively for information.

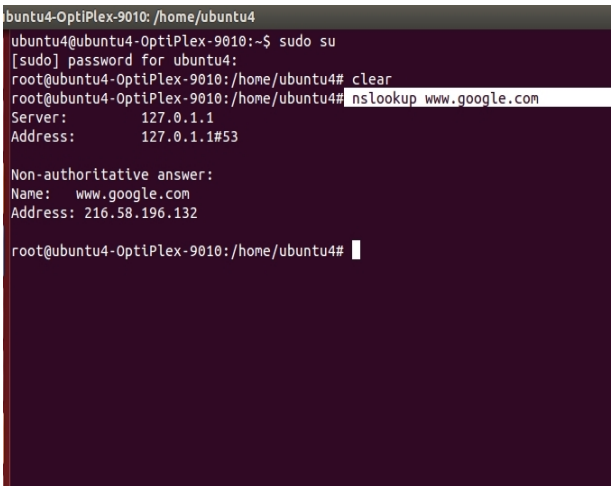

Fig. 4. nslookup Command

To prevent active reconnaissance, a firewall along with Intrusion detection system is used. This combination helps in detecting active reconnaissance attack. Passive reconnaissance there is no direct interaction with the client. Information can be gathered without the knowledge of the client.

III. SCANNING THE NETWORK

Network vulnerability scans are the scans used to find the vulnerabilities present in a network. a scan helps to protect the network from an outside attack. Hackers may use a scan to find vulnerabilities which helps them to launch an attack. Scanning of a port is defined as a process in which the client sends requests to different servers and finds an active port on a host.. Hackers use this technique is to probe the services of the target machine.

Nmap (network mapper) [2] is a security scanner. in a network, it discovers services and hosts and thus a "map" of the network is created. in nmap specially crafted packets are sent to the target host and then the responses to those packets are analyzed. the different features of nmap are: host discovery, port scanning, version detection, and os detection. nmap is installed using the command:

$ sudo apt-get install nmap

Fig. 5. shows the port scan of a target machine. In this command only selected ports like 21,22,23,25 and 80 are scanned to see its state and service. Port scanning is of different types: - TCP connect scan, SYN scan, XMAS scan, NULL scan, FIN scan, UDP port scan [3].

Fig. 5. nmap port scan

In TCP connect scan there is an attempt to perform three-way handshaking with every tcp port. In SYN scan the port scanner generates raw IP packets whose responses are monitored by itself. The other name of this type of scan is "half-open scanning", because a full tcp connection is never opened. In a FIN scan closed ports reply to a FIN packet with a RST packet but open ports simply ignores this packet. In NULL scan if any TCP packet is sent without the RST flag set to a closed port then it should receive an RST response. If the port is open (or listening) then it should receive no response. For each RST packet received, a closed port is reported and when no response is received a remote open TCP port is assumed. The XMAS scan [4] is identical to the NULL and FIN scans except that all flags are set on each outbound TCP packet. Only closed ports respond with a RST packet. In UDP

port scan a UDP packet is sent to each port on a target. Any open UDP port will accept the packet, sending no reply, any closed port will respond with an ICMP unreachable packet.

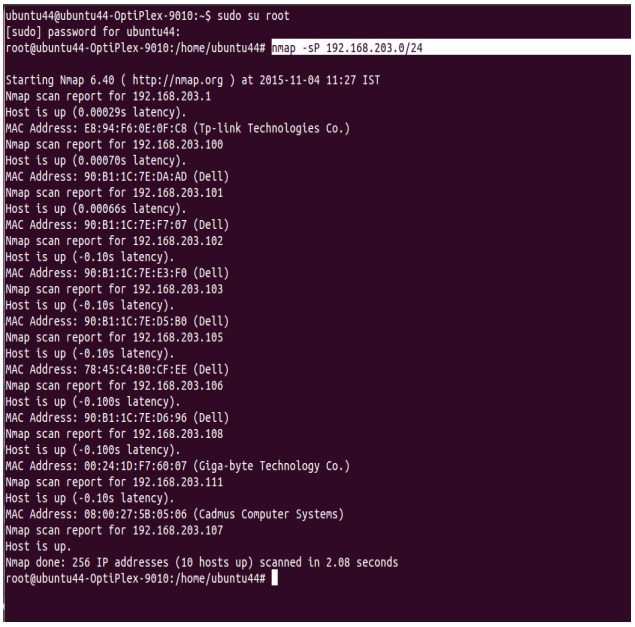

Fig. 6. Ping scan

This scan is effective in finding unknown open UDP ports. Fig. 6. shows Ping scan command. Ping scan also known as Ping sweep is a basic network scanning technique which is used to determine which of a range of IP addresses map to live hosts.

IV. ATTACK ON NETWORK

In a network there can be passive and active attack. Passive attack means monitoring the network traffic to obtain passwords and sensitive information which is not encrypted. It results in disclosure of information without the knowledge of the user. In an active attack the attacker tries to compromise the secured system. It results in disclosure or modification of data or denial of service (DoS). Sniffing and spoofing are types of passive and active attacks respectively. In Sniffing, a system which is not the destination reads the data. Financial information, e-mails, passwords, confidential information, low level protocol information like ip address, hardware address, routing information can be obtained through sniffing. In Spoofing, one system present in the network masquerades as another system. IP spoofing, MAC spoofing, ARP spoofing are some of the examples.

In open source there are certain sniffing and spoofing tools available. For sniffing, TCPDUMP and WIRESHARK can be used. Tcpdump is a network debugging tool that can be used for displaying and intercepting packets on a network. It is a filter that allows displaying of only the limited packets which the user wants to see using a specific port number. Wireshark on the other hand is a modified form of tcpdump. It also captures a packet from the network and analyses it in detail. Wireshark is considered to be the best packet analyzer which provides the open source GUI. Wireshark is used by administrators and network security engineers to troubleshoot network related problems and examine security problems respectively. Users use it to learn network protocol internals. Developers use it to debug protocol implementations.

Wireshark can be started from the ubuntu terminal using the following command:-

$ sudo wireshark

Fig. 7. shows the capturing of packets by wireshark.

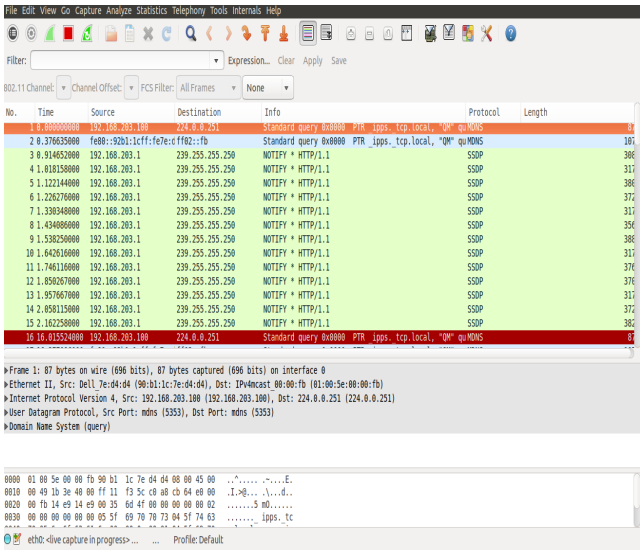

Fig. 7. Wireshark-Capturing packets

Wireshark GUI has a filter option which helps in identifying what type of packet is captured. It can capture all tcp, udp, icmp packets. Fig. 8. shows the capturing of tcp packets by wireshark.

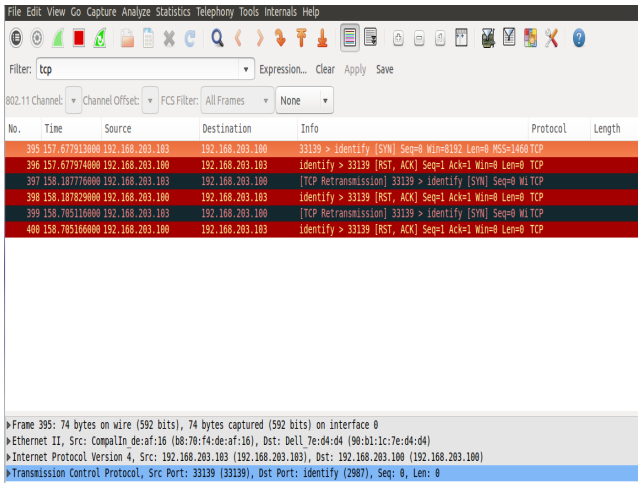

Fig. 8. Wireshark-Capturing tcp packets

The captured packet can be studied in detail. The packet consists of Frame number, source and destination address, header length, flag, time to live, offset, checksum etc. All these details are shown in Fig. 9.

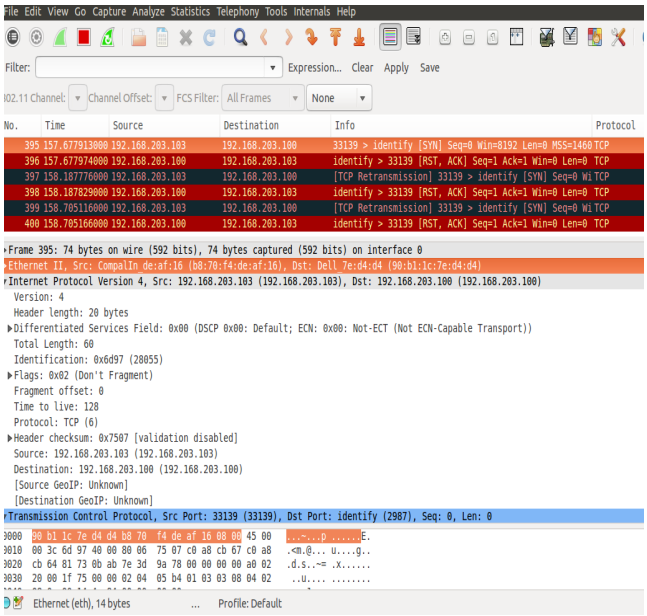

Fig. 9. Packet Details

After a tcp packet is captured, it can be analysed further. All the flag fileds are shown in Fig. 10.

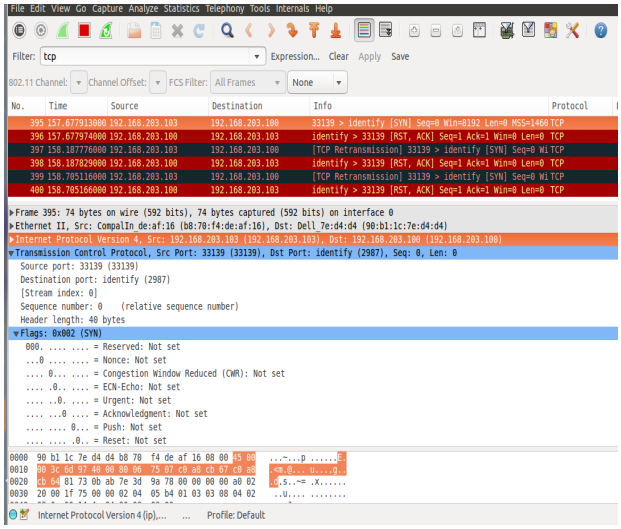

Fig. 10. TCP flags

For ARP spoofing, ETTERCAP [5] is used. It is a tool which can be used to perform Man in the Middle (Mitm) attack. Ettercap can be started from the ubuntu terminal using the following command:-

$ sudo ettercap –G

Ettercap[5,8] requires the network interface to be selected which acts as an input. Fig. 11. shows the selected interface.

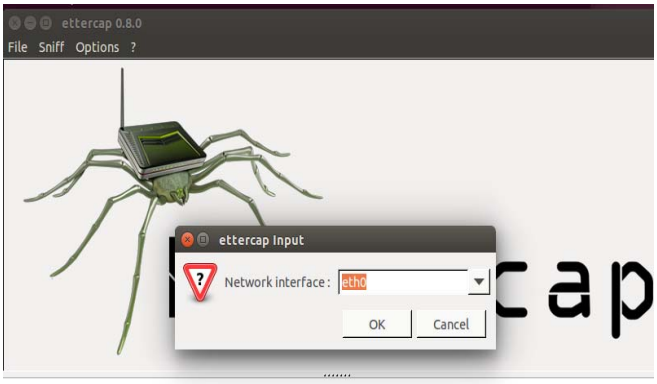

Fig. 11. Ettercap GUI

After the interface is selected, the network is scanned for hosts and a host list is obtained. Fig. 12. shows the scanning of network for hosts.

From the host lists, targets are selected. Two hosts are added as target1 and target2. This is shown in Fig. 13.

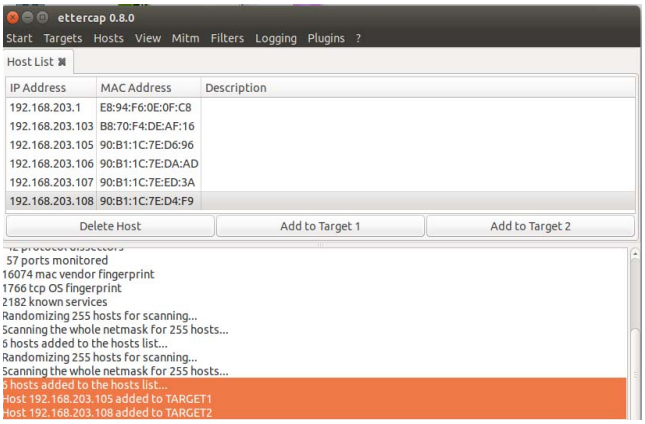

Fig. 13. Hosts added as target1 and target2

ARP Poisoning is done by selecting the Mitm option. It is shown in Fig. 14.

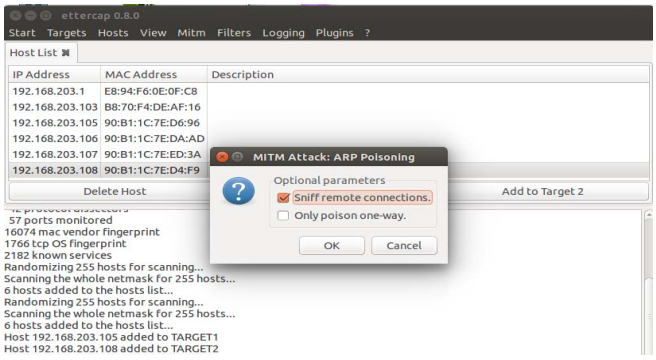

Fig. 14. ARP Poisoning

ARP poisoning victims are shown in Fig. 15.

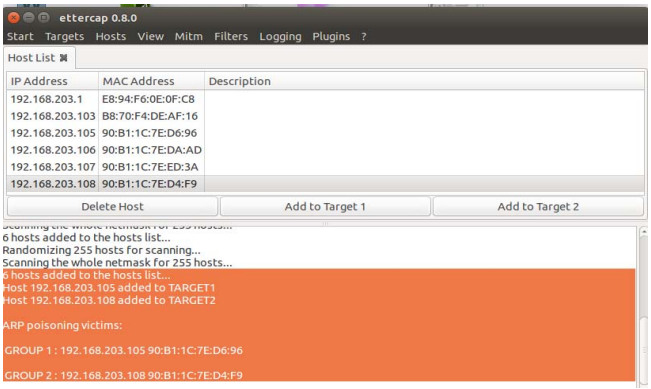

Fig. 15. Victims of ARP Poisoning

The arp cache of the victim can be seen using the following command:-

$ arp -e

The arp cache table shown in Fig. 16. shows that two different ip address are having the same hardware address. It shows that arp poisoning has taken place.

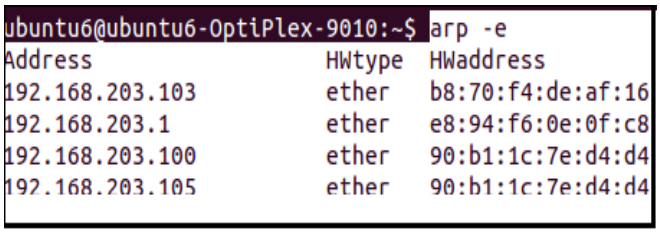

Fig. 16. ARP cache of victim

To protect against these attacks, FIREWALLS or Intrusion Detection System (IDS) must be used. Open Source provides tools for implementing both. Firewalls are implemented using iptables. SNORT [6] is an IDS that is widely used in open source.

V. FIREWALL

A firewall is a network security system designed to control incoming and outgoing traffic based on a set of rules. Firewalls when installed in the computer prevent outsiders to gain access of our computer. Firewalls can be implemented in both hardware and software, or a combination of both [7]. Hardware firewalls are present in modems which uses packet filtering.

In Linux, Software firewall is implemented using iptables. Iptables works on the concept of rules. If a packet satisfies the rule then it is allowed by the firewall else it is rejected. There are three type of chains known as input, output and forward. Input chain is used to control the behavior of incoming packets. Forward chain is used for transmitting the packets incoming in a router. Output chain is used for outgoing connections. Three common responses in iptables are:- a)Accept– which means to accepting the connection b)Drop- which means to discontinue the connection & act like it never happened. c) Reject which means to discard the connection with an error message. Fig. 17. shows the –L –n command which lists out the iptables rules.

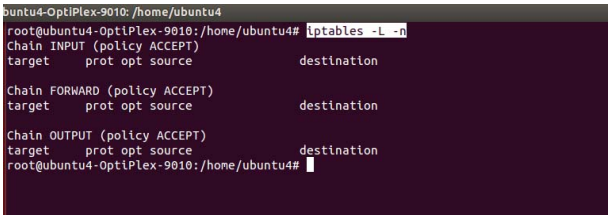

Fig. 17. Listing of rules

Rules for output chain are shown in Fig. 18.

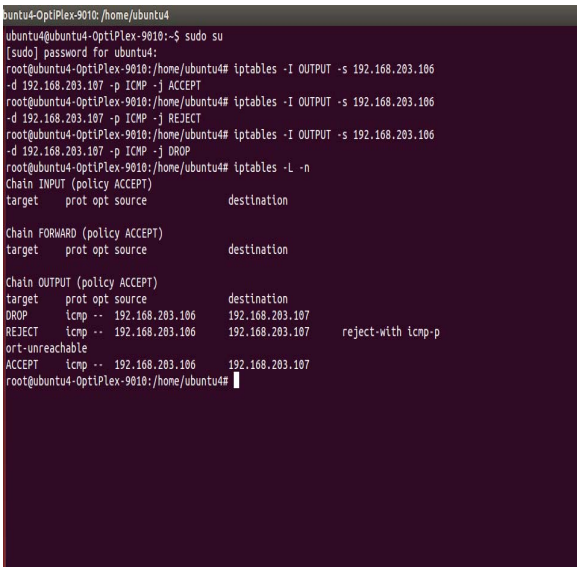

Fig. 18. Output chain rules

Rules for ACCEPT, REJECT and Drop are written. Packets from the given ip address will be accepted first then it will be rejected. After that it will be dropped. To delete all rules, Flush command is used. Whatever rules are written till now can be deleted using this command. It is shown in Fig. 19.

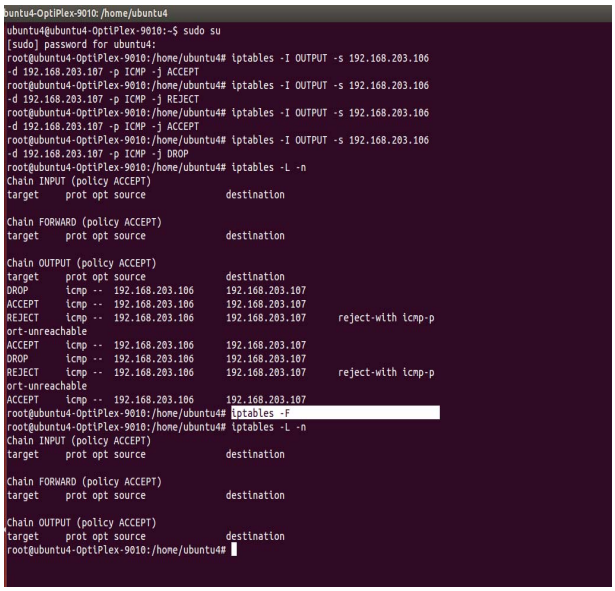

Fig. 19. Deleting rules

VI. COMPARISON

The Table I. shows the tools with respect to their purpose that are used in this paper.

It can be observed from the table that all the commands like dig, whois, traceroute and nslookup acts as information gathering tools. Commands like nmap and ping scan are used to scan the ports. Tools like wireshark and ettercap works as packet sniffing tool and arp poisoning tool respectively. To prevent from any kind of attack, firewall is implemented using iptables.

TABLE I. SECURITY TOOLS AND THEIR PURPOSE

Command/Tool	Purpose
dig	Reconnaissance
whois	Reconnaissance
traceroute	Reconnaissance
nslookup	Reconnaissance
nmap	Port scan
Ping scan	Port scan
Wireshark	Packet Sniffing
Ettercap	ARP Poisoning
iptables	Firewall

.

VII. CONCLUSION

Securing the network is the major concern these days. Although the open source is considered to be secure but still data transmitted over the network is not safe. Some reconnaissance tools, scanning tools, packet sniffing tools and firewall rules are presented in this paper to understand the threats, attacks and vulnerabilities of the network.

REFERENCES

[1] S. Mishra, L. Jena, and A. Pradhan," Networking Devices and Topologies: A succinct study", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No.11, pp. 347-357, November 2012.

[2] Nmap.org, 'Obtaining, Compiling, Installing, and Removing Nmap ', 2014. [Online]. Available: https://nmap.org/book/inst-linux.html#inst-rpm. [Accessed: 14- Oct.- 2015].

[3] ee.ryerson.ca,'Attacks and Defense', [Online]. Available: http://www.ee.ryerson.ca/~courses/ee8213/Lecture81.pdf. [Accessed: 15- Oct.-2015].

[4] Giac.org, 'Network Reconnaissance – Detection and Prevention', 2003. [Online]. Available: https://www.giac.org/paper/gsec/2473/network-reconnaissance-detection-prevention/104296. [Accessed: 14- Oct.-2015].

[5] Ettercap.github.io, 'Ettercap', [Online]. Available: https://ettercap.github.io/ettercap/index.html. [Accessed 10- Oct.-2015].

[6] S. Rani, V. Singh, "SNORT: An Open Source Network Security Tool for Intrusion Detection in Campus Network Environment", International Journal of Computer Technology and Electronics Engineering, Vol.2, No. 1.

[7] Thewindowsclub.com, 'Difference between hardware and software firewall' [Online]. Available: http://www.thewindowsclub.com/hardware-software-firewall-difference. [Accessed: 13- Oct. - 2015].

[8] Openmainak.com, 'Ettercap-The easy tutorial-ARP Poisoning' [Online]. Available: http://openmaniak.com/ettercap_arp.php. [Accessed: 15-Oct. - 2015].