© 2015 IJSRSET | Volume 1 | Issue 3 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Detection of Malicious Traffic and Checksum Error in Network using Wireshark

Gajendra Singh, Sandeep Baliya
Sri Satya Sai University of Technology & Medical Sciences, Madhya Pradesh, India

ABSTRACT

To secure the systems and information, each association or affiliation should lead a self-hacking-survey, dismember the perils and slaughter it before getting any issue. A firewall is a system or social occasion of systems that executes a passage control approach between two or more frameworks. In this proposition work noteworthy complement is on setup and headway of filtering standards to deny/grant the framework movement. These rules are created using the announcement, which support distinctive highlights like the relationship taking after highlight of IP Tables is an especially significant thing. It can be used to turn away most TCP hijackings for non- IP Masqueraded clients that experience the evil impacts of poor TCP game plan number randomization. Correspondingly, it can be used to deflect UDP bundle.

Keywords: IDS/IPS, Intrusion Detection and Response Systems, DoS Attack, TELNET, FTP, SMTP, Sniffing, DNS Spoofing, Data Sniffing and Spoofing, IP Spoofing, ARP Spoofing

I. INTRODUCTION

Computer networks by their very nature are designed to allow the flow of information. Network technology is such that, today, you can sit at a workstation in Delhi, and have a process connected to a system in London, with files mounted from a system in California, and be able to do work just as if all of the systems were in the same room. Impeding the free flow of data is contrary to the basic functionality of the network, but the free flow of information is contrary to the rules by which companies and governments need to conduct business. Information and sensitive data must be kept insulated from unauthorized access yet security must have a minimal impact on the overall usage of the network.

The purpose of a firewall is to provide a point of defense and a controlled and audited access to services, both from within and to an organizations private network. This requires a mechanism for selectively permitting or blocking traffic between the Internet and the network being protected. Routers can control traffic at an IP level, by selectively permitting or denying traffic based on source/destination address or port. Hosts can control traffic at an application level, forcing traffic to move out of the protocol layer for more detailed examination. To implement a firewall that relies on routing and screening, one must permit at least a degree of direct IP-level traffic between the Internet and the protected network.

Network Security

Network Security is a branch of Information Security which deals with systems that operate primarily at the network level. This includes the management of network devices such as Firewalls, VPNs, Proxies, NAC solutions, IDS/IPS, as well as the management and protection of the network infrastructure.

Network Security approaches

Security approaches are basically of following two types:

Proactive

Proactive approaches are measures that are taken to prevent computer or network from various types of attack. Every modern organization realizes the value of dedicating some resources to the prevention of expensive damages that will likely to occur if such preventive measures are not taken. Banks use thick steel and concrete vaults with advanced electronic systems to prevent and detect break-ins. Some organizations have

started using Intrusion Detection and Response Systems (IDRSes) to try to detect computer intrusions and then activate defensive measures when an attack is detected.

Reactive

Reactive approaches are those procedures that organizations use once they discover that some of their systems have been compromised by an intruder or attack program. Reactive methods include Disaster Recovery Plans, use of private investigation services and loss recovery specialists, reinstallation of operating systems and applications on compromised systems, or switching to alternate systems in other locations [7].

II. METHODS AND MATERIAL

Related Work

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service oobstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Website Defacement

Website defacement is an attack on a website that changes the visual appearance of the site. These are typically the work of system crackers, who break into a web server and replace the hosted website with one of their own. Website Defacement increasing tremendously experts no longer keep record of defaced sites. Attacker probes web services through normal Internet connection and modifies HTML or JAVA code, which changes website.

Website defacement is the unauthorized substitution of a web page or a part of it by a system cracker. This is a very common form of attack that seriously damages the trust and the reputation of a website. Detecting web page defacements is one of the main services for the security monitoring system.

Viruses and Worms

Viruses and Worms are computer programs that make computer systems not to work properly. There is a subtle difference between Virus and Worm; both can replicate itself, but when traveling on the network. Virus can't travel on its own on the network, whereas Worms can travel on its own without anything. It doesn't actually need any infected file to stick in. Viruses and Worms are really annoying problem for all systems. The ultimate aim of these Viruses and Worms are making a good working system to malfunction and sometimes worms can sniff in and steal private information to send it to its creator. Earlier days, Viruses were spreading through floppy diskettes. Nowadays, it spreads through Internet, which is a broad gateway for these malicious programs. It can spread quickly and affect all systems in an organization within a minute and can create millions of dollar loss for the organization in a minute.

Data Sniffing and Spoofing

Data Sniffing and Spoofing attack are those in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

Sniffing

It means seeing all packets passed through wires or sometimes through air for wireless networks. Initially, this technique was being used for fixing network problems. Because it can watch network packets, it is now being used by hacker for scanning login_ids and passwords over the wires. TCPdump and Wireshark are better examples for sniffing tools. The better way to avoid sniffing attack is encryption. If sensitive information is encrypted before sending to wires, hackers can’t really understand what it is. They need the key to decrypt the information. This way, the information sent over network could always be safe with

encryption. Typical services that are sniffed are: TELNET, FTP, SMTP (E-mail) packets if unencrypted.

Spoofing

The exact meaning of spoofing is deceiving others. It is actually fooling other computer users to think that the source of their information is coming from a legitimate user. There are several methods of spoofing. Some of them are as follows:

IP Spoofing

It changes the source-address of an IP packet to show that it is from a legitimate source, but really it might be coming from a hacker. Thus, the hacker attacks the system and at the same time hides his IP address from the eyes of firewalls. The targeted systems for IP Spoofing are UNIX systems and RPC services.

DNS Spoofing

This will direct the users to incorrect location. In other words, directing the users to a different website and collecting personal information through web forms illegally. DNS Spoofing is actually very dangerous threat, because DNS is the one that manages domain names and creates equivalent IP addresses. Suppose, if the domain name is www.dell.com <http://www.dell.com/> and DNS calculates an IP address that is related to a hacker's site, the users will be directed to the hacker's website. If the hacker maintains his website similar to dell, then the users may think that the hacker's website is the real dell- website and may provide all bank or credit card information when trying to purchase something. Now, the hacker can get that information easily without any difficulties.

ARP Spoofing

ARP is actually maintaining a table of MAC addresses of all computers connected in a network. Any information that comes to ARP is delivered to respective computer based on the mappings available on the ARP's tables. Suppose, if ARP couldn't find MAC address for a message, it broadcasts a message to all systems to get a reply from the exact destination-machine with its MAC address; when it gets the destination- machine's MAC address, it updates it on MAC table. This is the stage where ARP spoofing can happen. ARP Spoofing actually happens when a hacker (hacker's machine) sends a reply to the ARP's broadcasted message saying that the hacker's machine is the legitimate one. Then, ARP gets hacker's MAC address and adds it to its table. As a result, hacker will gain a legitimate connection to the network illegally. Once hacker is connected to the network, he can do all sorts of things.

III. RESULTS AND DISCUSSION

Wireshark and offline analyzing of these network data packets and after that on the basis of analyzing the packets writing of script to block/allow the network traffic using IPtables and after blocking traffic further capturing and analyzing of live traffic using Wireshark.

Implementation Setup

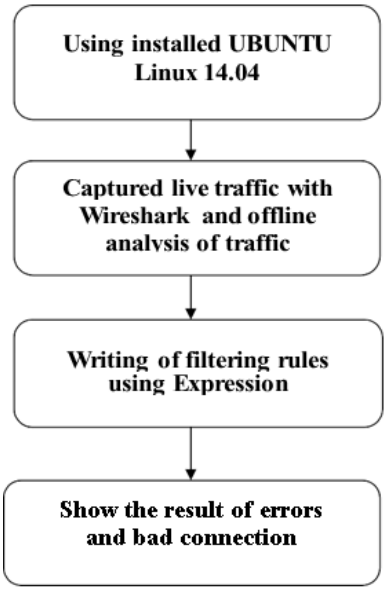

Figure 1: Implementation setup Diagram When capturing packets from a network interface, wireshark captures all of the packets coming and going

Over the network. Wireshark provides capture and display filters which allow you to capture only the packets you are interested and display allows you to specify which packets are shown in GUI. We use port numbers also that can be used to capture packets that are destined for certain applications. Like UDP had port no 53. HTTP has 80 and so on [4]. For analysis we use a term Protocol dissector.

Protocols coming under capturing of live network are

1. TCP/IP
2. HTTP
3. ARP
4. ICMP

HTTP request and transmission from one source to destination starting with sequence no. 0 in packet 974 in Figure 3. and GET message in packet 980.But this is not found by particular destination so it send HTTP/1.0

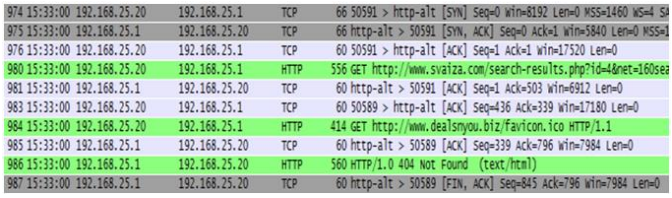

Figure 2: HTTP Protocol showing conversation between two end points

Not found message to source and end this conversation with FIN/ACK message in packet 987.

We can also draw graphs of packets captured in capture file. Click on Statistics menu and then TCP Stream Graph and then choose any graph type out of five graphs shown in option but first select packet for which you want to draw graph. I select one of the packets and for this Time Sequence graph (tcp-trace) graph displayed is as shown in Figure 2.

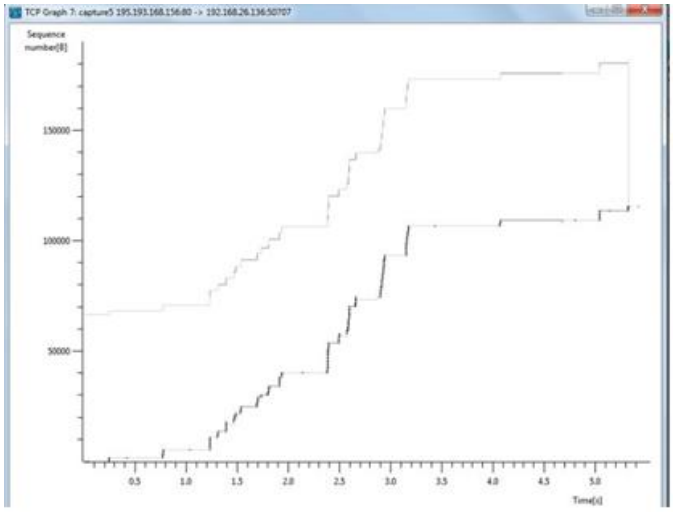

Figure 3. Time-Sequence Graph

IV. CONCLUSION

In this paper, work has been done on capturing the live traffic using the network protocol analyzer Wireshark and on the basics of analyzed data packets further explored and designed the script using IPtables to allow/deny the network traffic on the basics of the IP address of the computer sending the packets, the IP address of the computer receiving the packets, the type of packet (TCP, UDP, etc.), The port number, and URL's etc. This enables us to protect our system from a wide variety of hazards, including service attacks and hack attempts.

V. REFERENCES

[1] J. Alpert and N. Hajaj. We knew the web was big... Available online at http://googleblog.blogspot.com/2008/07/we-knew-web-was-big.html, Jul 2008.

[2] P. R. Clearinghouse. A chronology of data breaches. Technical report, Privacy Rights Clearinghouse, July 2009.

[3] C. Criscione, F. Maggi, G. Salvaneschi, and S. Zanero. Integrated detection of attacks against browsers, web applications and databases. In European Conference on Computer Network Defence - EC2ND 2009,2009.

[4] Facebook. Statistics. Available online at http://www.facebook.com/press/ info.php?statistics, 2009.

[5] A. Frossi, F. Maggi, G. L. Rizzo, and S. Zanero. Selecting and Improving System Call Models for Anomaly Detection. In U. Flegel and M. Meier, editors, DIMVA, Lecture Notes in Computer Science. Springer, 2009.

[6] T. Holz. A short visit to the bot zoo. IEEE Security & Privacy, 3(3):76–79, 2005.

[7] Gunter Schafer, "Network Security Tutorial", May 2003, Anchorage, Alaska.