© 2015 IJSRSET | Volume 1 | Issue 5 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Mitigation of Intruders and TCP bad Connection Detection in WAN Environment using Wireshark

Mahendra Kumar Rai, Gyanendra Haldkar
Shri Ram Institute of Technology, Jabalpur Madhya Pradesh, India

ABSTRACT

A couple of people achieve certifiable work over the Internet, and some must secure tricky or restrictive data. Ordinarily, a firewall's inspiration is to keep the intruders out of the framework while letting to do the occupation. In this proposition work critical highlight is on setup and progression of filtering standards to deny/grant the framework action. These rules are created using the announcement, which support distinctive highlights like the relationship taking after highlight of IP Tables is an incredibly profitable thing. It can be used to deflect most TCP hijackings for non- IP Masqueraded clients that experience the evil impacts of poor TCP plan number randomization. Correspondingly, it can be used to turn away UDP bundle.

Keywords: TCP, UDP, IP, Wireshark, WAN, ICMP, SMTP, ICMP, DN, Spoofing, DDoS Attack

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 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, Wiresharks, Proxies, Wireshark solutions, Wireshark, as well as the management and protection of the network infrastructure.

Commerce has become one of the vital parts of the modern life. Online payment is the supportive application for the payment of money for the products we buy. For the past years online security breach created a major problem and lots of money had been stolen. The proposed document deals by securing the payment through iris recognition [1]. This method also adds the method of using visual cryptography for securing the user credentials. This visual cryptography method was formerly invented by Moni Naor and Adi Shamir in 1994[6].

II. METHODS AND MATERIAL

A. Related Work

Without security measures and controls in place, data might be subjected to an attack. Some attacks are passive, meaning information is monitored others are active, meaning the information is altered with intent to corrupt or destroy the data or the network itself. Networks and data are vulnerable to any of the following types of attacks if do not have a security plan in place.

2.1 Wireshark : 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.

2.2 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.

2.3 Viruses and Worms: viruses 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.

2.4 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 Wireshark

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.

B. Proposed Work

Proposed system will used the concept of classification to check abnormality in the network and host both. Classification will be based on the normal and abnormal profile of the network

1. Wireshark network data after capturing in real time our anomaly classifier checks the following-
   - Check the anomaly in TCP packet and behavior during making connection.
   - DNS activities for the intrusion of flooding
   - UDP for UDP flood attack.
   - And ARP/RARP for LAN (second layering

attack).

a. Sniff real time traffic from wireshark
b. Extract TCP protocol traffic and UDP
c. Apply IDS detection scheme

```
{
 Calculate the length and Control bits of the TCP protocol
   Len[TCP]
   Len [TCP]
  COUNTER (UDP)
  COUNTER(DNS_ERRPR per minute)
 void   TCP_cntr ()
 {
  If ( S-F > 23)
    FLAG = "Alert- traffic suspicious"
 Else
  FLAG = OK
 }
}
```

Following Key point has been set and planned while implementing the proposed work:

Threshold:

The value of threshold for anomaly based IDS for the Flow matrices:

S-F >23

AND

S-F >17

III. RESULTS AND DISCUSSION

RESULTS I/O Graph

Most important facility provided by Wireshark is to draw I/O graph of the captured packets. At a time we can draw graph of five protocols of different colours with different tick interval and pixels per tick on X-axis and units and scale on Y-axis. Styles can also be changed instead of lines shown you can select impulse, Fbar, dot from the drop down and you get a different look of the graph. A line graph of TCP, HTTP, and ARP protocol is shown to you in Figure 1

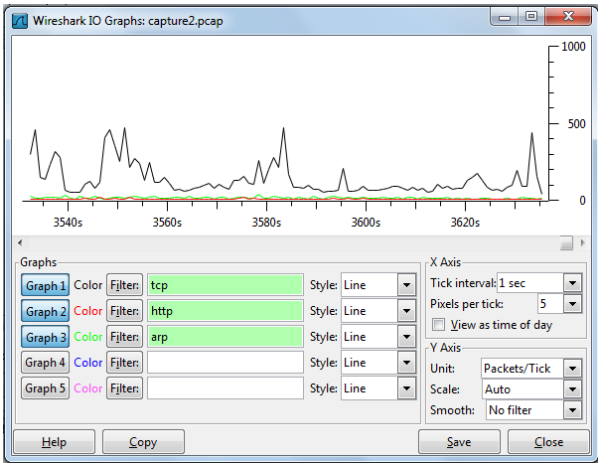

Figure 1. I/O Graph of Captured Trace

Network traffic from a live network is shown by taking various traces and monitoring and analysis is done on that captured files and then statistics is built. Detailed analysis and summary as well as conversations between two end points are shown. One interesting option which Wireshark give is objects which we captured or say user who are on the network using whatever sites can be listed in this object list. Graphs of captured files are shown and other attractive features are shown which make Wireshark a great tool for network analysis. The Output graphs generated through captured packets provide details of network dynamics and insight into the problems that lead to network slowness, network performance etc.

The main objective to concrete on developing a novel approach to finding out unknown types of attack using the anomaly (or profile based) approach, with producing low false rate integrating the automatic response mechanism against intrusive activity.

ICMP Protocol: - Internet Control Message Protocol. It is a part of IP protocol and seen by Type 8 echo (ping) request in the window pane. Computer send echo request, it should receive echo reply in response as shown in Figure 2. Next Packet is transmitted back from remote computer and is marked as

```
34228 15:26:08 192.168.26.136  192.168.25.1    ICMP  74 Echo (ping) request  id=0x0001, seq=5/1280, ttl=128
34229 15:26:08 192.168.25.1    192.168.26.136  ICMP  74 Echo (ping) reply    id=0x0001, seq=5/1280, ttl=64
34365 15:26:09 192.168.26.136  192.168.25.1    ICMP  74 Echo (ping) request  id=0x0001, seq=6/1536, ttl=128
34366 15:26:09 192.168.25.1    192.168.26.136  ICMP  74 Echo (ping) reply    id=0x0001, seq=6/1536, ttl=64
34732 15:26:10 192.168.26.136  192.168.25.1    ICMP  74 Echo (ping) request  id=0x0001, seq=7/1792, ttl=128
34745 15:26:10 192.168.25.1    192.168.26.136  ICMP  74 Echo (ping) reply    id=0x0001, seq=7/1792, ttl=64
```

Figure 2. ICMP Protocol showing request /reply response

HTTP request: 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 Not found message to source and end this conversation with Wiresharkmessage in packet 987.

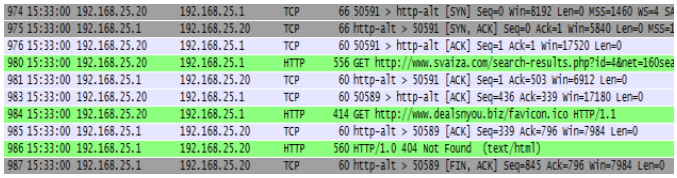

Figure 3. HTTP Protocol showing conversation between two end points

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. The script discussed here can be used for the purpose of network Security. Web traffic sent on HTTP can be analyzed. Denying of ICMP, SMTP data packets. Configuring of host based packet filtering firewall to deny various type of attacks like spoofing, Stop bad packets, Stop Xmas Tree type scanning, null scanning, syn flood and, ping flood attack etc. Deny P2P file sharing traffic.

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, Jul2008.

[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.

[8] Network Security policy and objectives, URL:http://publib.boulder.ibm.com/infocenter/iseri es/securitypolco.htm

[9] Deep Inspection,URL: http://www.ranum.com /security /computer_security/editorals/deepinspects /index.html

[10] Need of Network Security,URL: http://www.indiastudychannel.com/resources/1057 77-Network-Security-Attackers-Hackers.aspx

[11] Packet filtering process, URL: http://www.ibm.com/ developerworks/linux/library/s-netip/

[12] Packet filtering using IPtables, URL: http://netfilter.org/documentation/HOWTO/packet-filtering-HOWTO-7.html 13eSoft, "Modern Network Security: The Migration to Deep Packet Inspection", White Paper, 2006.

[13] John Peter Jesan, "Major threats to information security", Graduate School of Computer Information Sciences Nova Southeastern University, 2005.