Providing the Secure Data Transmission in the Network Using Open Source Packet Analyzer

[1]Hasina A. Razzak A. Karim, [2]S S Handa, [3]M V Ramana Murthy

[*]*Research Scholor, Dept. Computer Science &Engg., ManavRachna University, Faridabad, India.*
[**]*Professor in Dept. of Computer Science &Engg., ManavRachna University, Faridabad, India.*
[***]*Head Dept. of Mathematics & Computer Science, Osmania UniverSity, Hyderabad, India.*

Abstract—*Intrusion Detection System (IDS) is process of detecting intrusion in database, network or any other devicefor providing secure data transmission. In this paper, our purpose of IDS is to detect intrusion in network to provide safe and intrusion free network by using Open Source Packet Analyzer. Open Source Packet Analyzer is used to analyze network data and then that data is classified into normal data and abnormal data.*

Keywords—*Intrusion Detection System, Data Mining Techniques, TCP/UDP protocol, DOS attack*

INTRODUCTION

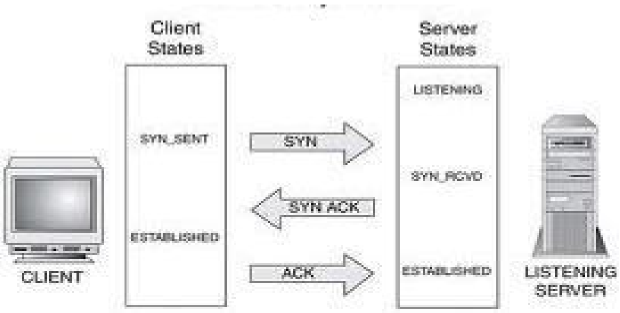
Intrusion detection system(IDS) is a device or software application that monitors network and system activities for malicious activities or policy violations and produces report to a management station.
Types of IDS:

Host-Based Intrusion Detection System(HIDS) is a system in which host observes the different activities such as filelogging and many other application of relevant field and protect from other field is called host based IDS.

Network Intrusion Detection System (NIDS) is an independent system that monitors the network traffic and analyzes themif they are free from attack or not. Network Intrusion Detection System (NIDS) is an intrusion detection system that attempts to discover unauthorized access to a computer network by analyzing traffic on the network for malicious activity. Traffic on the network may consist of any connection, Connectionless or connection-oriented. Connectionless use UDP protocol and connection-oriented use TCP protocol.

Transmission Control Protocol (TCP) connection is established using three steps:

1) SYN bit from host A(client) to host B(server)
2) SYN+ACK bit from host B(server) to host A(client)
3) ACK bit from host A(client) to host B(server), which is shown in Fig 1.



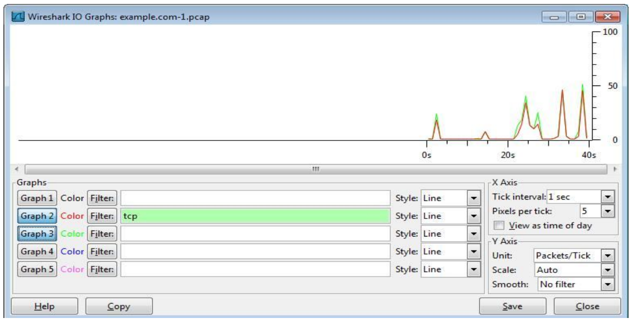
If any of the steps in connection establishment doesn't occur, means that connection is not established between client and server and there is some type of intrusion in network.

User Datagram Protocol (UDP) connection follows only request and response query from sender and receiver respectively.

COMPARING ALL TRAFFIC WITH TCP TRAFFIC

In the network which consists of number of communication using different protocols but maximum number of communication uses TCP protocol. Here, in our example we take captured data and show the comparison between total number of communications and TCP protocol communication.

In Fig 2 green graph shows total traffic and red graph shows TCP Traffic which indicates that much of the traffic in network uses TCP protocol in comparison to other protocol.



Wireshark IO Graphs: example.com-1.pcap

Graphs

Graph 1	Color	Filter:		Style:	Line
Graph 2	Color	Filter:	tcp	Style:	Line
Graph 3	Color	Filter:		Style:	Line
Graph 4	Color	Filter:		Style:	Line
Graph 5	Color	Filter:		Style:	Line

X Axis
Tick interval: 1 sec
Pixels per tick: 5
□ View as time of day

Y Axis
Unit: Packets/Tick
Scale: Auto
Smooth: No filter

INTRUSION DETECTION USING

Intrusion Can Be Detected Using Open Source Packet Analyzer ->Expert Info's

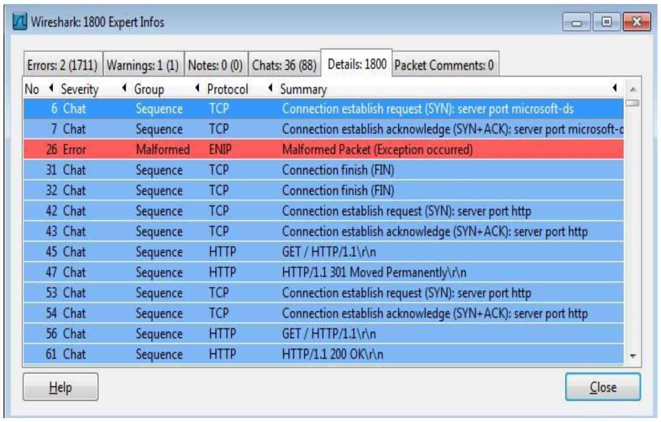
The expert info's is a kind of log of the anomalies found by Open Source Packet Analyzer in a capture file. Each expert info will contain the following things

severity:
Chat (grey): information about usual workflow
e.g. a TCP packet with the SYN flag set

Note (cyan): notable things
e.g. an application returned a "usual" error code like HTTP 404

Warn (yellow): warning
e.g. application returned an "unusual" error code like a connection problem

Error (red): serious problem



Wireshark: 1800 Expert Infos

Errors: 2 (1711) | Warnings: 1 (1) | Notes: 0 (0) | Chats: 36 (88) | Details: 1800 | Packet Comments: 0

No	Severity	Group	Protocol	Summary
6	Chat	Sequence	TCP	Connection establish request (SYN): server port microsoft-ds
7	Chat	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port microsoft-c
26	Error	Malformed	ENIP	Malformed Packet (Exception occurred)
31	Chat	Sequence	TCP	Connection finish (FIN)
32	Chat	Sequence	TCP	Connection finish (FIN)
42	Chat	Sequence	TCP	Connection establish request (SYN): server port http
43	Chat	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port http
45	Chat	Sequence	HTTP	GET / HTTP/1.1\r\n
47	Chat	Sequence	HTTP	HTTP/1.1 301 Moved Permanently\r\n
53	Chat	Sequence	TCP	Connection establish request (SYN): server port http
54	Chat	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port http
56	Chat	Sequence	HTTP	GET / HTTP/1.1\r\n
61	Chat	Sequence	HTTP	HTTP/1.1 200 OK\r\n

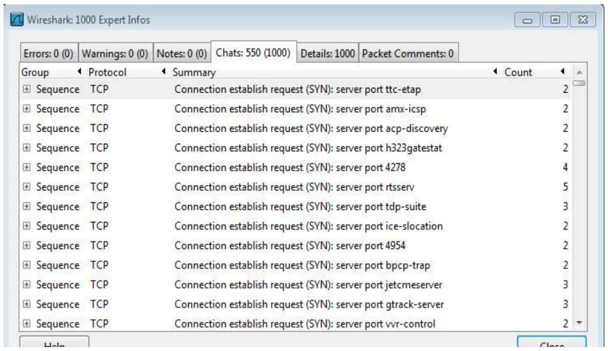
Network Intrusion Detection system (NIDS) – performs an analysis for a passing traffic on the entire subnet. Works in a promiscuous mode, and matches the traffic that is passed on the subnets to the library of knows attacks. Once the attack is identified, or abnormal behavior is sensed, the alert can be send to the administrator. Example of the NIDS would be installing it on the subnet where you firewalls are located in order to see if someone is trying to break into your firewall. Network Node Intrusion detection system (NNIDS) – performs the analysis of the traffic thatis passed from the network to a specific host.

The difference between NIDS andNNIDS is that the traffic is monitored on the single host only and not for the entire subnet. The example of the NNIDS would be, installing it on a VPN device, to examine the traffic once it was decrypted. This way you can see if someone is trying to break into your VPN device, Host Intrusion Detection System (HIDS) – takes a snap shot of your existing system files and matches it to the previous snap shot. If the critical system files were modified or deleted, the alert is sent to the administrator to investigate. The example of the HIDS can be seen on the mission critical machines, that are not expected to change their configuration.

Fig 3 shows the expert info about the communication on the network. Red packet shows that a serious problem occurred like malformed packet.

Intrusion Can Be Detected Using Open Source Packet Analyzer ->Chats

Chats for the TCP connection should contain sequence of SYN, SYN+ACK and ACK messages.



Wireshark: 1000 Expert Infos

Errors: 0 (0) | Warnings: 0 (0) | Notes: 0 (0) | Chats: 550 (1000) | Details: 1000 | Packet Comments: 0

Group	Protocol	Summary	Count
⊞ Sequence	TCP	Connection establish request (SYN): server port ttc-etap	2
⊞ Sequence	TCP	Connection establish request (SYN): server port amx-icsp	2
⊞ Sequence	TCP	Connection establish request (SYN): server port acp-discovery	2
⊞ Sequence	TCP	Connection establish request (SYN): server port h323gatestat	2
⊞ Sequence	TCP	Connection establish request (SYN): server port 4278	4
⊞ Sequence	TCP	Connection establish request (SYN): server port rtsserv	5
⊞ Sequence	TCP	Connection establish request (SYN): server port tdp-suite	3
⊞ Sequence	TCP	Connection establish request (SYN): server port ice-slocation	2
⊞ Sequence	TCP	Connection establish request (SYN): server port 4954	2
⊞ Sequence	TCP	Connection establish request (SYN): server port bpcp-trap	2
⊞ Sequence	TCP	Connection establish request (SYN): server port jetcmeserver	3
⊞ Sequence	TCP	Connection establish request (SYN): server port gtrack-server	3
⊞ Sequence	TCP	Connection establish request (SYN): server port vvr-control	2

Fig 4 shows the chat info. Here only SYN request indicates that there is no connection establishedbecause connection establishment requires three steps: SYN bit from host A to host B, ACK+SYN bit from host B to host A, ACK bit from host A to host B) So, DOS attack is detected.

Using these conversations as shown in Figure, we update this table by adding a column named conclusion which contain either normal or abnormal.

Firstly value of that column is set to abnormal and then based on the condition of normal behavior conclusion column is updated. We here used the condition that if packet sent from port A to port B and from port B to port A is not equal to zero, which means connection is established and data is transferring which shows normal behavior.

Update `example1`
Set example1.conclusion='normal'
WHERE example1.PacketsA2B<>0 AND
example1.PacketsB2A<>0

Where example1 is the name of the table, packetsA2B and packetsB2A are the packets sent from port A to port B and the packets sent from port B to port A respectively.

After updating the table, we can apply any data mining technique such as association rule, classification, clustering etc to find the rules using either Weka or Rapid Miner Tool. Here, we have first applied classification using J48 algorithm which time i.e. 0.13sec. So, J48 algorithm takes less time than random forest algorithm.

Data Security Issues are becoming increasingly important as civilization moves toward a global information age. The migration away from paperwork- oriented ways Of doing things requires the development of digital equivalents for traditional processes such as sealing envelopes, signing letters, and acknowledging receipt of items. The development of systems with such capabilities is one of the most complex and challenging tasks facing today's engineers. At the same time, the rewards to be reaped from breaking such systems acts as an attractive lure for modern criminals. One study estimates that the average traditionalbank robber nets $20,000 with a 90% chance of prosecution; the average electronic funds transfer nets $500,000 with a 15% chance of prosecution.

Conclusion

This paper detects intrusion in network for TCP protocol and detects DOS attack. In the future,protocol and different types of attacks in those protocols in the network.

takes 0.09sec. It is classified based on the number of packet sent, packet received and port number.

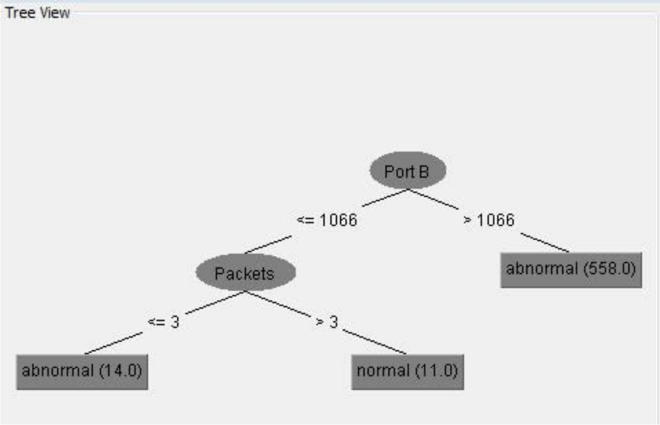


Fig 5 shows that if the port number is less than 1066 and packet sent is greater than 3,then only data sent is normal otherwise abnormal. When the classification is made using random forest algorithm it takes more

References

[1]Usha Banerjee , AshutoshVashishtha and MukulSaxena, Evaluation of the capabilities of wireshark as a tool for intrusion detection

[2]Jeff Markey, Using Decision Tree Analysis for Intrusion Detection Russ McRee, Security Analysis withWireshark.

[3][BOOK] Data mining: concepts and techniques J Han, M Kamber - 2006

[4] Qadeer, M.A. Zahid, M. ;Iqbal, A. ; Siddiqui, M.R. Network Traffic Analysis and Intrusion Detection Using PacketSniffer

[5]Shaoqiang Wang, DongShengXu, ShiLiang Yan, Analysis and Application of Wireshark in TCP/IP Protocol.

[6]Luo, H., Henry, P.: A common password method for protection of multipleaccounts. 14th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Vol. 3 (2003) 2749 – 2754

[7] Pinkas, B., Sander, T.: Securing passwords against dictionary attacks Proceedings of the 9th ACM conference on Computer and communications security Washington, DC, USA (2002) 161-170

[8] Gouda, M.G., Liu, A.X., Leung, L.M., Alam, M.A.: Single Password, Multiple Accounts. Proceedings of 3rd Applied Cryptography and Network Security Conference (industry track), New York City, New York (2005)