Volume 2, Issue 11, November 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Intrusion Detection System Using Wireshark

Shilpi Gupta
Software Engineering
I T M University
Sector 23-A, Gurgaon
India

Roopal Mamtora
Astt. Prof. Dept. of CSE
I T M University
Sector 23-A, Gurgaon
India

Abstract— ***Intrusion Detection System (IDS) is process of detecting intrusion in database, network or any other device for 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 Wireshark. Wireshark 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***

I. 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 file logging 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 them if 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.

II. TCP/UDP CONNECTION ESTABLISHMENT

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.

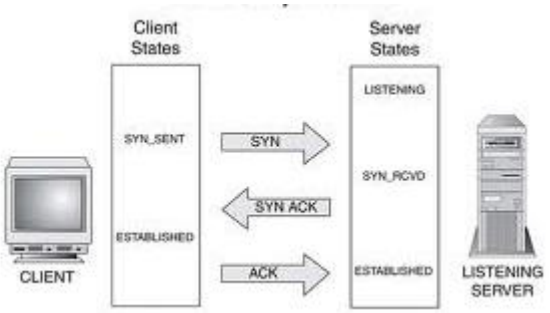


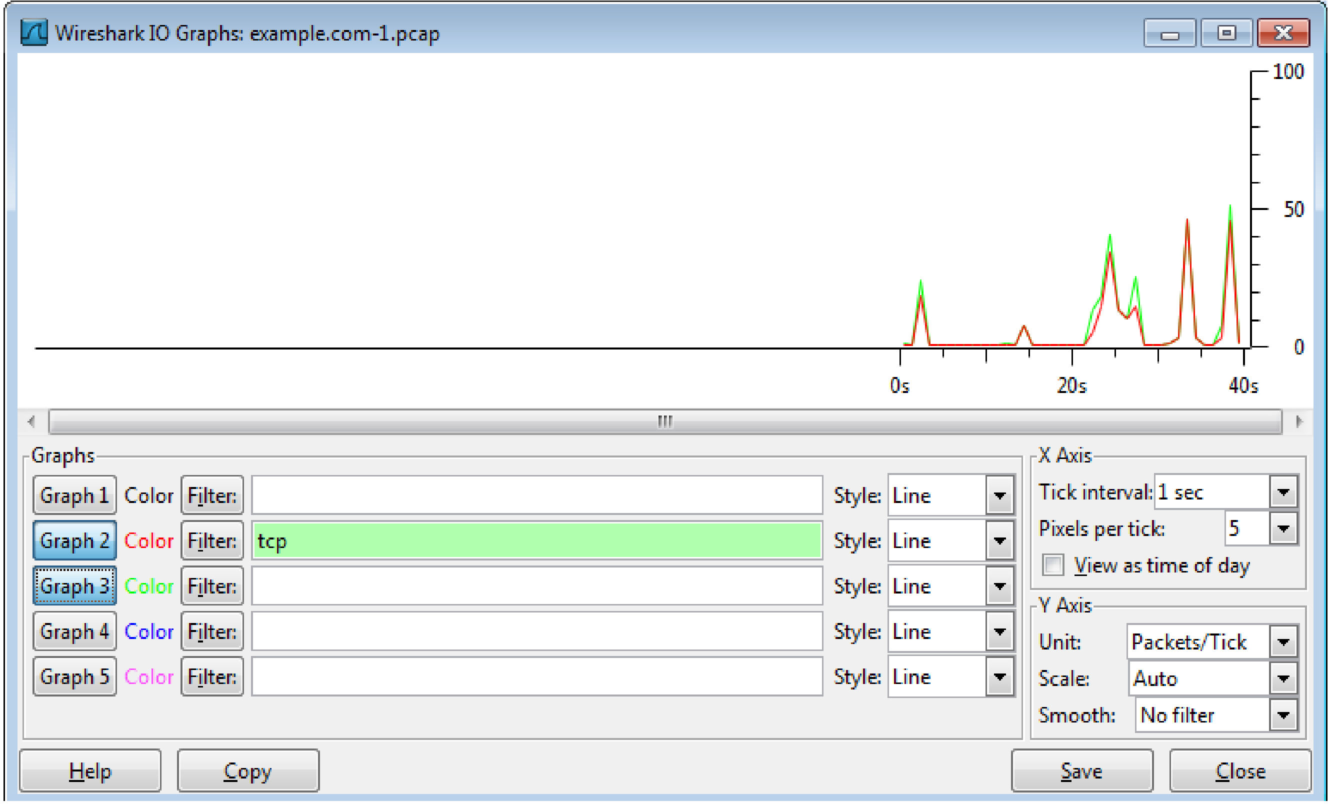
Fig 1 TCP connection establishment

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.

III. 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.



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

Fig 2 IO graph

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.

IV. INTRUSION DETECTION USING WIRESHARK

A. Intrusion Can Be Detected Using Wireshark ->Expert Info's

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

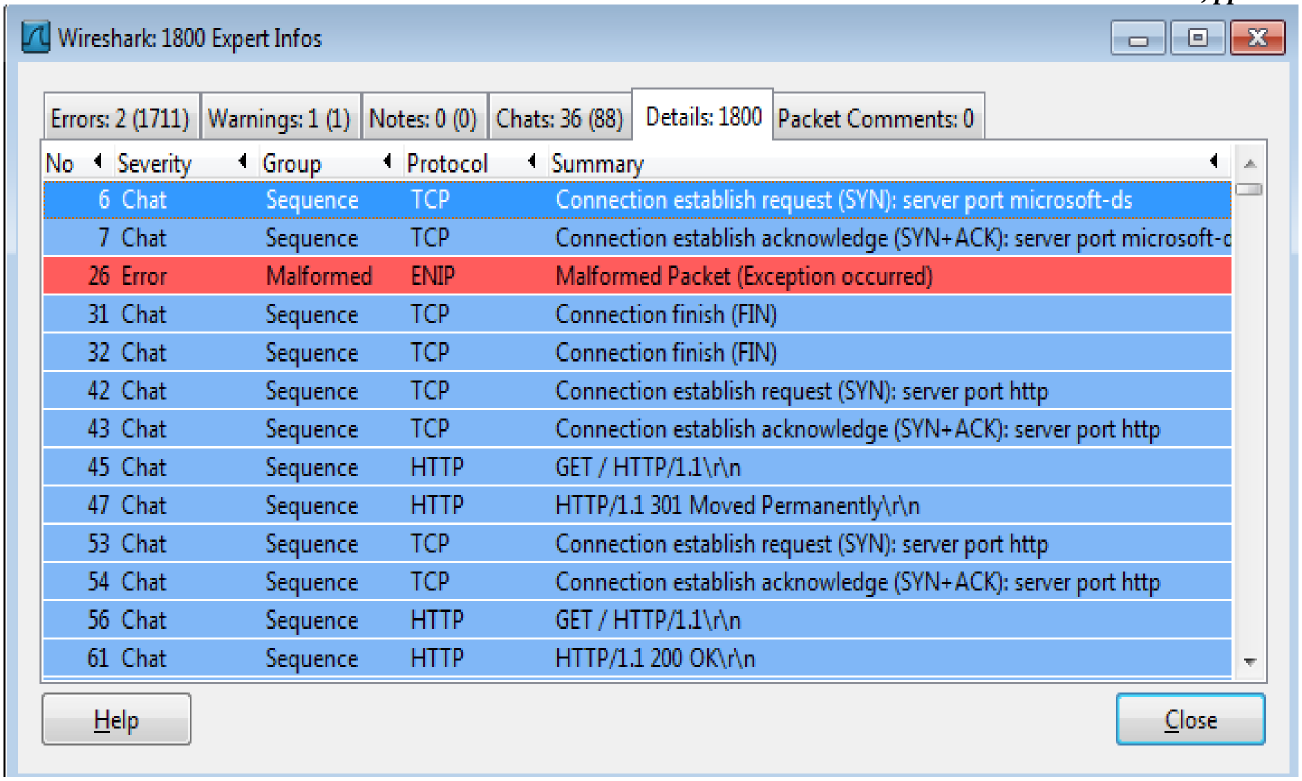
severity:

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
e.g. [Malformed Packet]



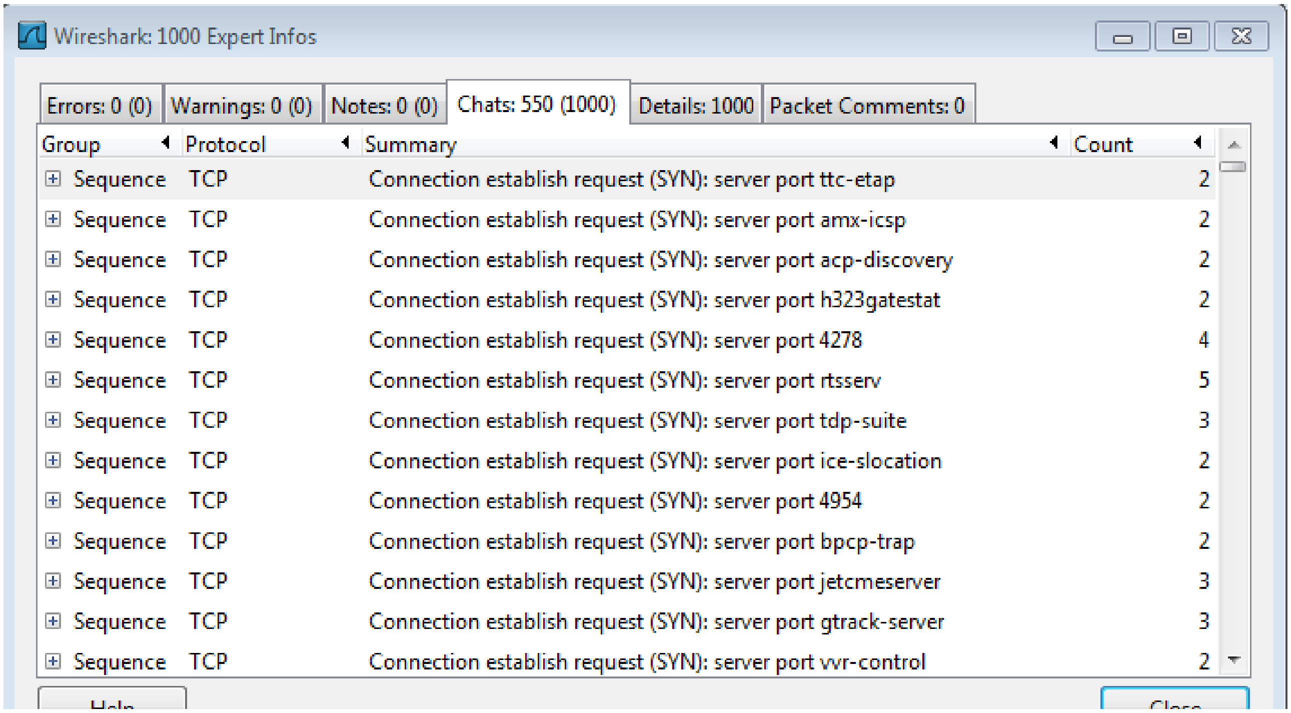
No	Severity	Group	Protocol	Summary
6	Chat	Sequence	TCP	Connection establish request (SYN): server port microsoft-ds
7	Chat	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port microsoft-d
26	Error	Malformed	ENIP	Malformed Packet (Exception occurred)
31	Chat	Sequence	TCP	Connection finish (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

Fig 3 expert infos

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

B. Intrusion Can Be Detected Using Wireshark ->Chats

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



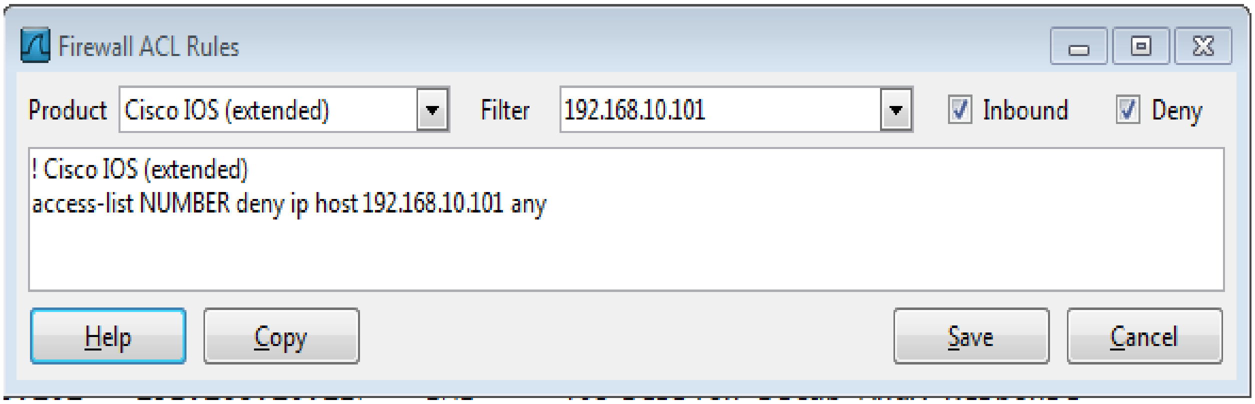
Group	Protocol	Summary	Count
⊞ Sequence	TCP	Connection establish request (SYN): server port ttc-etap	2
⊞ Sequence	TCP	Connection establish request (SYN): server port amx-icsp	2
⊞ Sequence	TCP	Connection establish request (SYN): server port acp-discovery	2
⊞ Sequence	TCP	Connection establish request (SYN): 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 chats

Fig 4 shows the chat info. Here only SYN request indicates that there is no connection established (because 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.

C. Firewall Can Be Applied Using Wireshark->Firewall ACL Rules

Using wireshark firewall can be applied for any of the IP address to deny/allow packet from that particular IP.



Product: Cisco IOS (extended) Filter: 192.168.10.101 ☑ Inbound ☑ Deny

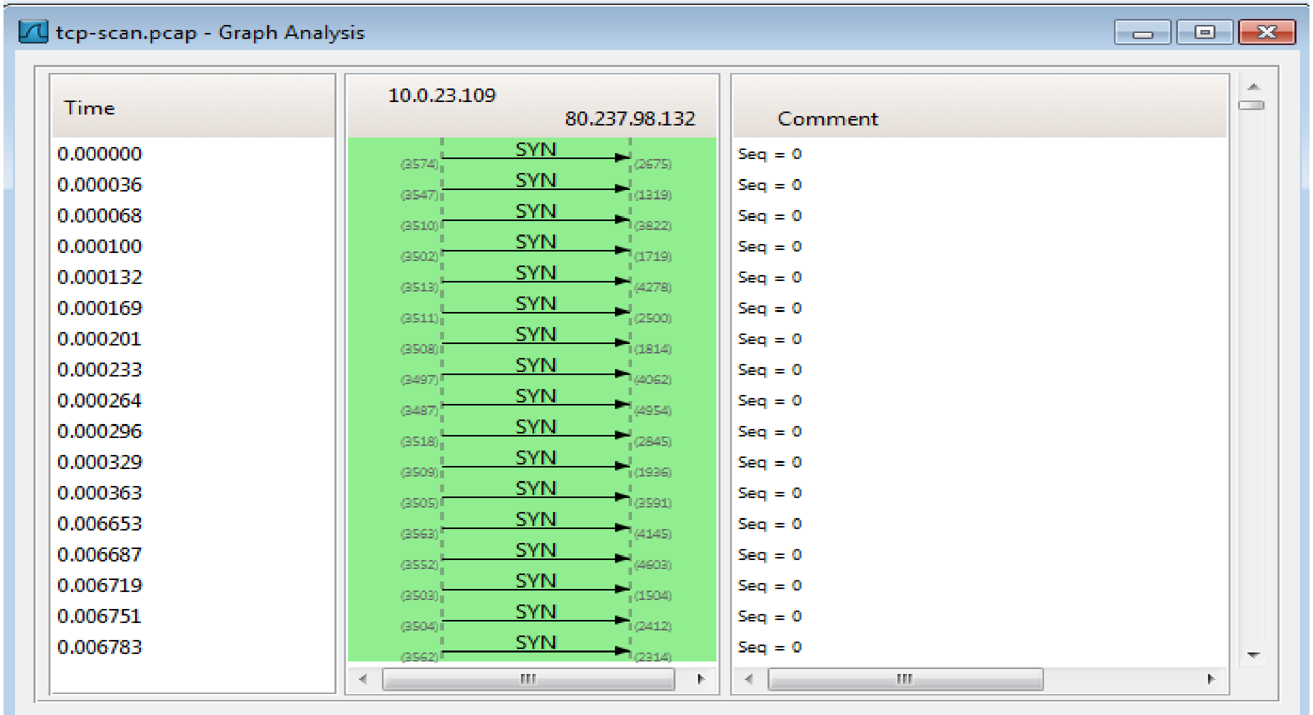
```
! Cisco IOS (extended)
access-list NUMBER deny ip host 192.168.10.101 any
```

Fig 5 firewall ACL rules

Fig 5 shows the Firewall ACL (Access Control List) rules using which we can access/deny any product IPfilter, NetFilter, Packet Filter, IPFirewall, Windows Firewall for Filter.

D. Intrusion Can Be Detected Using Wireshark->Flow Graph

Flow graph shows the communication between two or more different IP's.



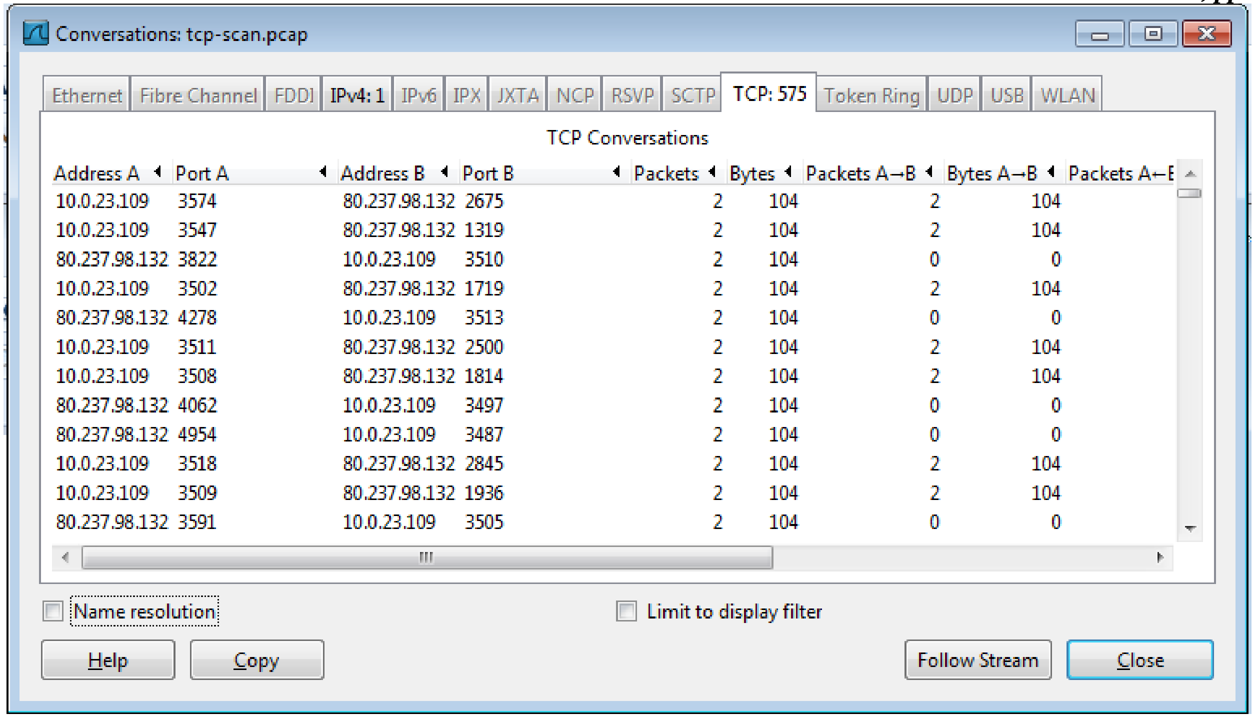
Time	10.0.23.109		80.237.98.132	Comment
0.000000	(3574)	SYN	(2675)	Seq = 0
0.000036	(3547)	SYN	(1319)	Seq = 0
0.000068	(3510)	SYN	(3822)	Seq = 0
0.000100	(3502)	SYN	(1719)	Seq = 0
0.000132	(3513)	SYN	(4278)	Seq = 0
0.000169	(3511)	SYN	(2500)	Seq = 0
0.000201	(3508)	SYN	(1814)	Seq = 0
0.000233	(3497)	SYN	(4062)	Seq = 0
0.000264	(3487)	SYN	(4954)	Seq = 0
0.000296	(3518)	SYN	(2845)	Seq = 0
0.000329	(3509)	SYN	(1936)	Seq = 0
0.000363	(3505)	SYN	(3591)	Seq = 0
0.006653	(3563)	SYN	(4145)	Seq = 0
0.006687	(3552)	SYN	(4603)	Seq = 0
0.006719	(3503)	SYN	(1504)	Seq = 0
0.006751	(3504)	SYN	(2412)	Seq = 0
0.006783	(3562)	SYN	(2314)	Seq = 0

Fig 6 flow graph

Fig 6 shows TCP flow graph in which only SYN message is transmitted from client to server using different different port number and no other message (SYN+ACK and ACK) is transmitted between the two IP so, connection is not established and DOS attack detected.

E. Intrusion Can Be Detected Using Wireshark->Conversations

A network conversation is the traffic between two specific endpoints. For example, an IP conversation is all the traffic between two IP addresses.



TCP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←E
10.0.23.109	3574	80.237.98.132	2675	2	104	2	104	
10.0.23.109	3547	80.237.98.132	1319	2	104	2	104	
80.237.98.132	3822	10.0.23.109	3510	2	104	0	0	
10.0.23.109	3502	80.237.98.132	1719	2	104	2	104	
80.237.98.132	4278	10.0.23.109	3513	2	104	0	0	
10.0.23.109	3511	80.237.98.132	2500	2	104	2	104	
10.0.23.109	3508	80.237.98.132	1814	2	104	2	104	
80.237.98.132	4062	10.0.23.109	3497	2	104	0	0	
80.237.98.132	4954	10.0.23.109	3487	2	104	0	0	
10.0.23.109	3518	80.237.98.132	2845	2	104	2	104	
10.0.23.109	3509	80.237.98.132	1936	2	104	2	104	
80.237.98.132	3591	10.0.23.109	3505	2	104	0	0	

□ Name resolution

□ Limit to display filter

Fig 7 TCP conversations

Using these conversations as shown in Fig 7, 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. Query used for this purpose is:

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

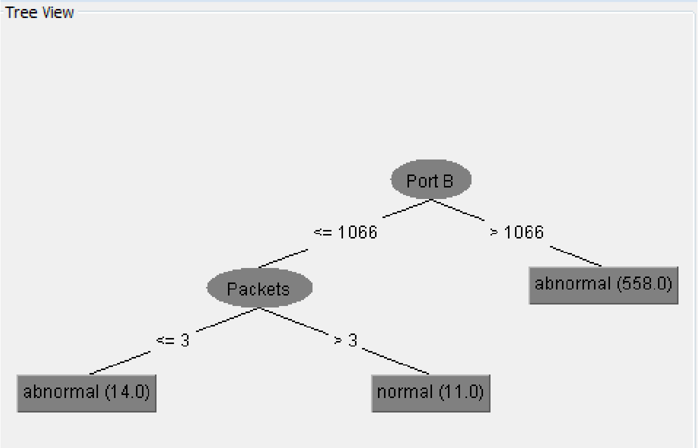


Fig 8 classification tree

Fig 8 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 time i.e. 0.13sec. So, J48 algorithm takes less time than random forest algorithm.

V. Conclusion

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

Acknowledgment

I would like to give my sincere gratitude to my guide Ms. Roopal Mamtora who guided me to pursue this topic and helped me to complete this topic. I would also like to thank her for providing me remarkable suggestions and constant encouragement. I deem it my privilege to have carried out my research work under her guidance.

References

[1]Usha Banerjee , Ashutosh Vashishtha and Mukul Saxena, 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 with Wireshark

[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 Packet Sniffer

[5]Shaoqiang Wang, DongSheng Xu, ShiLiang Yan, Analysis and Application of Wireshark in TCP/IP Protocol Teaching

[6]http://wiki.wireshark.org/

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

[8] 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

[9] 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)