

CHALMERS



Testing and Analysis of Personal Firewalls

Master of Science Thesis in Computer Science and Engineering

RASHID REHMAN
OBAID UR RAHMAN, SHEIKH

Chalmers University of Technology
University of Gothenburg
Department of Computer Science and Engineering
Göteborg, Sweden, October 2010

The Author grants to Chalmers University of Technology and University of Gothenburg the non-exclusive right to publish the Work electronically and in a non-commercial purpose make it accessible on the Internet.

The Author warrants that he/she is the author to the Work, and warrants that the Work does not contain text, pictures or other material that violates copyright law.

The Author shall, when transferring the rights of the Work to a third party (for example a publisher or a company), acknowledge the third party about this agreement. If the Author has signed a copyright agreement with a third party regarding the Work, the Author warrants hereby that he/she has obtained any necessary permission from this third party to let Chalmers University of Technology and University of Gothenburg store the Work electronically and make it accessible on the Internet.

Testing and Analysis of Personal Firewalls

Rashid Rehman
Sheikh Obaid Ur Rahman

© Rashid Rehman, October 2010.
© Obaid Ur Rahman, Sheikh, October 2010.

Examiner: Arne Dahlberg

Chalmers University of Technology
University of Gothenburg
Department of Computer Science and Engineering
SE-412 96 Göteborg
Sweden
Telephone + 46 (0)31-772 1000

Department of Computer Science and Engineering
Göteborg, Sweden October 20100

Abstract

The rapid growth of internet has directed a collinear increase of internet users. The majority of people using internet have limited understanding and knowledge of computer systems. The majority of users rely on the security software's that are provided by different firewall vendors to ensure the secure communication. These security software's design and developed by very highly qualified professionals to ensure threat detection against viruses, malware and spywares. The basic purpose of our thesis is to test and analyze the security firewalls against TCP ACK, TCP SYN, TCP FIN, TCP Connect, Echo Ping, UDP and Denial of Service attacks (Ping of Death, Teardrop, and Land Attack) to check security issues. We also have discussed the similarities and differences between them.

Preface

Finally, we have reached to another milestone of our lives i.e., completion of ours MSc thesis. We thank God who gave us lot of courage during our studies and in every sphere of our lifes. First of all, we want to thank our dear supervisor and examiner Arne Dahlberg for giving us the opportunity. We have learned a lot from your practical expertise and invaluable writing skills. Your kindness and patience is worth appreciation. We will continue to build our careers on these bases. Then, we want to extend our gratitude to our father who always supported us in our studies and made our dream true to come abroad to follow advance course in Computer Networks and Distributed Systems. Our brothers and sisters contribution is always very crucial to our career. Their support is a great asset for us. We assure you all to continue our quest to gain knowledge and expertise to achieve excellence.

Table of Contents

1.0	Introduction	2
1.1	<i>Tools Used For Testing and Analyzing Firewalls</i>	3
1.2	<i>Introduction of Firewalls</i>	4
1.2	Types of Filtering Techniques	5
1.3	<i>Port Scanning</i>	6
1.3.1	UDP Port Scanning	6
1.3.2	FIN Scan.....	6
1.3.3	TCP ACK.....	6
1.3.4	TCP Connect Scan.....	7
1.3.5	TCP SYN Flooding	7
1.4	Types of Attacks	8
1.4.1	Land Attack	8
1.4.2	Ping of Death.....	8
1.4.3	<i>Teardrop Attack</i>	8
1.5	Port States.....	9
	Open.....	9
	Closed.....	9
	Filtered	9
	Unfiltered	9
	Open/Filtered.....	9
	Closed/Filtered.....	9
2.0	Testing And Analysis of Firewalls	10
2.1	ZoneAlarm.....	10

2.1.1	TCP ACK Scanning at Full security	10
2.1.2	TCP ACK at Medium Security	10
2.1.3	Echo Ping at Full Security	11
2.1.4	Echo Ping at Medium Security	11
2.1.5	TCP FIN at Full Security	12
2.1.6	TCP FIN at Medium Security	12
2.1.7	TCP SYN Scan at Full Security	12
2.1.8	TCP SYN at Medium Security.....	13
2.1.9	TCP Connect at Full Security	14
2.1.10	TCP Connect at Medium Security.....	14
2.1.11	UDP Scan at Full Security	15
2.1.12	UDP Scan at Medium Security	15
2.1.13	Teardrop Attack at High and Medium Security	16
2.1.14	Land Attack at Full and Medium Security	16
2.1.15	Ping of Death at High and Medium Security	17
2.2	Comodo Firewall	18
2.3	Kaspersky Firewall.....	20
2.4	McAfee Firewall	22
2.5	Win7 Firewall	25
2.6	Comparison	27
Conclusion		29
References		30

1.0 Introduction

The rapid growth of internet has directed a collinear increase of internet users and a lot of activities involved in internet world. Internet has become the important part of human lives. It brings ease and comfort in lives by means of E-commerce, online banking, online gaming, IP telephony, video conferencing and social websites. The number of user's over the internet increases with a rapid rate. Most of the users have only the basic knowledge of computer system and internet so there interaction with the internet should be secure. The user's at home could not prevent their systems from Viruses, malwares, spywares, Worms, Denial of Service Attacks and Eavesdropping without the help of personal firewalls. In organization there are highly qualified professional to handle the security issues but users at home rely on security software's like personal firewalls. There are number of vendors that claims their product provide the best security solutions.

The internet is interconnection of small and big networks' and forms a big network of computers. This is very easy for intruders to spread the viruses, Trojans, Denial of services attacks within an organization if it finds any vulnerability. If anyone's computer is connected with internet there is risk of intrusions. To prevent computer system from intrusions security software (firewall) should be installed that will provide a maximum level of security against malicious activities.

The main focus of our thesis is testing the selected personal firewalls because firewalls are very critical point from security point of view.

- The purpose of our thesis is testing and analyzes how different firewalls work to protect the system against TCP SYN Flooding, TCP Connect, TCP SYN/ACK, TCP FIN, TCP/UDP port scanning and Denial of Services attacks like Teardrop, Ping of Death and Land Attack.
- As the firewall vendors claim that personal firewalls are best against malicious activities. We have attacked these firewalls to find out any weaknesses or flaw in them.
- We have tried to analyze and compare the results of different firewalls, how different firewalls address issues related to attacks and intrusions.
- How user-friendly these firewalls are? How they communicate with the user? Are the warning messages easy to understand?
- We analyze and evaluate similarities and differences between different types of host based (personal) firewalls.

1.1 *Tools Used For Testing and Analyzing Firewalls*

The tools that we have used to implement the different kinds of attacks are:

- ❖ NMAP
- ❖ Wireshark
- ❖ Nessus
- ❖ Engage packet builder

Wireshark

This is a tool for capturing and analyzing network traffic. It captures the packet which is then analyzed.

NMAP

This is the tool that can discover host, operating system and scan ports. Typically it is used to identify open ports on target computer, network inventory and network mapping.

Nessus

It is also a port scanning tool. It is a tool that we used for ping of death and teardrop attack. It contains hundreds of scripts, used for scanning and controlling a network for any vulnerability.

Engage Packet builder

This is a tool used for attacking. It has the ability to attack by SYN flooding.

We have selected the following attacks to test the security issues against the personal firewalls by using the above mentioned attacking tools.

- ❖ Land Attack
- ❖ TCP SYN Flooding
- ❖ TearDrop Attack
- ❖ TCP Connect
- ❖ TCP ACK
- ❖ TCP FIN
- ❖ TCP/UDP Port scanning
- ❖ Ping of Death
- ❖ ICMP Echo ping.

We have selected some well known firewalls for testing and analysis of security threats. Following are the personals firewalls

- ❖ Macfee Firewalls
- ❖ Window 7 Firewall

- ❖ Comodo Firewall Pro freeware
- ❖ Kaspersky Internet Security
- ❖ ZoneAlarm Pro 2010

1.2 *Introduction of Firewalls*

Types of Firewalls

- 1- Hardware Firewalls
- 2- Personal Firewalls

Hardware Based Firewalls

A hardware based firewall is a separate physical device that is used to protect a network. A hardware firewall is placed at the point from where the traffic goes out and comes in. One can place firewall with in the network but it all depends upon the network policy of the organization up to what level security is required. In hardware firewalls' filtering of traffic is done on the base of different kinds of filtering techniques like packet filtering, application filtering and NAT. Security policy is implemented by defining the set of rules. On the basis of that defined rules firewall inspect the incoming and outgoing traffic. This inspection of packet is possible on the base of one or more characteristics of packet like source IP, destination IP, source port, destination port, protocol type and by maintaining the state of connection. It is very important set of rules are configured properly otherwise attacker exploits these vulnerabilities and breach the security policy of organization. [1]

Personal Firewalls

A host based or personal firewall is a software program that protects a personal computer from the spyware, viruses, worms and other security threats. Whenever a PC or laptop is connected with the internet, it must have suitable security software for protection from malicious attacks. There are many host base firewall vendor's exists like McAfee, Norton, Comodo, ZoneAlaram, Kaspersky and many others. [1]

1.2 Types of Filtering Techniques

Stateless Filtering

It examines only the selected fields of the IP, TCP, ICMP, and TCP header and doesn't examine the data of application message. It examines the individual packet isolation of the context. It means that filtering rules apply only to the contents present in the packet and rest of the fields like connection state between the client and server are ignored. It could not differentiate at the arrival of packets either it is part of ongoing communication or not. That will provide an easy way to attacker. [2]

Stateful Filtration

Dynamic or Stateful packet filters keep record of the communication between client and server in a state table. When a host wants to establish a TCP connection with the external host they perform three way handshaking process to establish connection. Stateful firewall maintains the state of each packet in the state table. So on arrival of each packet it will check in the state table either it is the part of ongoing communication or not. But in case of Stateful firewall it does not check. [2]

Application Inspection

A Stateful and stateless inspection does not inspect the application contents. On the other hand application inspection filters the packet on the base of contents of message containing in TCP and UDP data field. Application inspection examines packets by using a program called proxy. Proxy acts as a middle man between client and server. When proxy receives a request from the client for the server, proxy forwards it to the server after examining the message contents of requested packet according to the defined filter policy. After receiving reply form server the proxy filter contents of the packet and finally send reply to the requested host. [2]

Network Address Translation

There is risk involved when an intruder places a sniffer program outside the firewall and start sniffing the packets. From those packets the intruder will get the IP address of internal host that exists in the network and might be able to get more details about the network. So by using NAT, you can spoof the internal host IP address. In this way intruder will get the IP address but a spoofed one not the internal host. [2]

1.3 *Port Scanning*

Port scanning is a technique to find out the open ports, discover the services on them and try to break into it. All computers connected to internet either use well known ports or not so well non ports. The foremost requirement before breaching the security of any computer system is to be aware of the ports that are open. The open ports are then used to attack the system.

Some of the well known ports are:

Port 20/UDP – FTP (File Transfer Protocol)

Port 21/TCP - File Transfer

Port 22/TCP - SSH remote login protocol

Port 23/TCP - Telnet

Port 80/TCP - World Wide Web HTTP

Ports from 0 to 1023 are quite well known. Ports from 1024 to 49151 are all registered ports. All the ports above 49151 are either Dynamic ports or Private ports. [3]

1.3.1 **UDP Port Scanning**

UDP port scanning is done to find out which UDP ports are open on the target machine. It is quite different from scanning TCP ports as TCP ports are connection oriented and gives good information to the attacker. In UDP scanning empty UDP datagram's are sent to the target. In case of closed ports 'ICMP Port Unreachable' message is sent back by the Operating system to the attacker. In this way it can be found out which port is open and which is close. But there is no guarantee that ICMP error messages will surely arrive for the close ports. UDP scanning is considered to be slow as in some systems ICMP error message rate is limited. [4]

1.3.2 **FIN Scan**

It is a technique in which erroneous packets are sent at the target hoping that the listening ports will reply back with RST segment. A FIN is actually used to close an open connection. RST is sent by the closed ports in reply to FIN packets. Normally FIN packets are ignored by the open ports. In case of non listening ports (close ports) operating system generates an error message while in case of listening ports (open ports) operating system silently drops the packet. So no reply indicates that ports are open. This is what the attacker is looking for. Once attacker is aware of the open ports it can use it for attacks. Although FIN Scan is not as effective as other scans because packets can be blocked by firewalls. [4]

1.3.3 **TCP ACK**

This scanning technique is different from others as this does not determine whether port is open or open/filtered. Thus it just provides information about firewall to check whether it's stateful or stateless. In TCP ACK scanning only ACK flag is set. In this case open and close ports both respond by resetting the connection. Nmap usually labels these ports as unfiltered but does not state clearly whether they are open or close. Those ports that don't respond are labeled as filtered. [3]

1.3.4 TCP Connect Scan

This scan is used when SYN scan is not an option. When there are no raw packet privileges with the user then TCP connect scan is used. The operating system establishes a connection with the target machine by sending 'connect' system call. This connection is established on high level as other application like web browsers, P2P do. As scanning is done usually by Nmap, it does not have good control over high level connections. It is not possible to establish half-open reset in high level connection which is not the case in SYN scanning. As TCP connect establishes a connection it may be logged by the target computer. [3]

1.3.5 TCP SYN Flooding

The one of the well known denial of service attack is SYN flooding. In this kind of attack the victim host is made so busy that it cannot reply back to legitimate users or the victim host crashes, this happens because it runs out of resources. SYN Flooding attack the attacker sends thousands of SYN TCP packets to the target host. Every time the victim receive TCP SYN packet it reserves some space and complete some other preparatory work required. Then victim send back SYN/ACK which shows that it wants to open the connection. When the attacker sends a lot of SYN packets the victim host runs out of resources and it will take more time to respond to other requests. [2]

1.4 Types of Attacks

1.4.1 Land Attack

Land Attack is a denial of service attack in which packet is sent with forged header. Normally the header contains same Source and Destination IP address. Even the same ports are also used. Land attack is also known as IP spoofing. It causes the computer to crash, but if the good firewall is installed, it detects the attack and drops the packet. [5]

1.4.2 Ping of Death

Ping of Death is an attack which sends malformed or malicious packets to the target computer. The size of ping is normally 56 byte and 84bytes including IP header. The maximum size of IP packet size can only be 65,535 bytes. In this attack the packet is send which exceeds the maximum allowed size of packet. This causes the target machine to crash. Although it's not possible to send packet larger than 65,536 bytes, but it is possible if packet is fragmented, when these fragmented packets are reassembled at the target computer, buffer overflow occurs which may cause system to crash. [6]

1.4.3 Teardrop Attack

Teardrop Attack is a denial of service attack that exploits the fragmentation issues in TCP/IP. As large packets are fragmented into small packets, each packet is given a sequence number and a common identification number so the system receiving it could easily reassemble the packets. But in teardrop attack false information is inserted into fragmentation packets. As a result there are empty and overlapping fragments when packets are reassembled and my cause the system to crash. [7]

1.5 Port States

Following are the main port states

Open

An application is animatedly taking UDP packets, TCP connections, on this port. It is obvious each open port is just open a door for attacker to exploits these open ports. It is a hole in the secure network. It is the responsibility of the network administrator taking measures by closing or protects these ports by using firewalls without affecting the legitimate users.

Closed

These are reachable ports but there is no application listening on it. Network administrator, by using firewall blocked such ports. After that these ports will appear as filtered state if any one scans the ports.

Filtered

In filtered port state it is not sure that port is open or not might be due to the firewalls filtering that restricts from reaching the port. This will not provide enough information to the attacker. Sometimes they reply with ICMP error message but most of the times drop without reply.

Unfiltered

It means that port is > reachable but it is difficult to say that either it is open or close. To confirm that port is open or close sending packet with ACK give information about a port either it unfiltered.

Open/Filtered

In this state it is difficult to judge either the port is open or filtered. This happens when open port sends no response.

Closed/Filtered

In this state it is difficult to know about a port either is closed or filtered. [3]

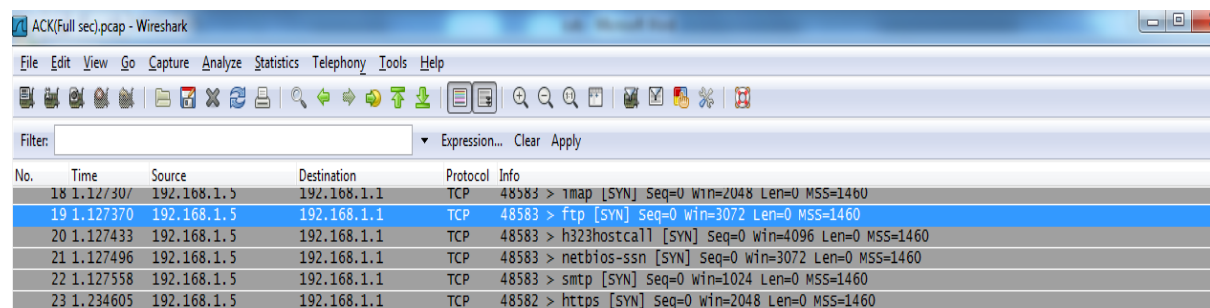
2.0 Testing And Analysis of Firewalls

2.1 ZoneAlarm

ZoneAlarm have different security levels i.e. Medium and Full security. At different security levels (Medium and Full security) it shows different results. We have performed many scan methods and denial of service attacks against ZoneAlarm.

2.1.1 TCP ACK Scanning at Full security

Nmap was used to carry out TCP ACK scanning. The purpose of this scan is to get the information of open ports which are then used to penetrate into the victim's computer. It is clear from figure2-0 that there is no reply from the victim computer. This means that the victim computer firewall drops the packets.



The image shows a Wireshark capture of network traffic. The packet list pane displays several TCP SYN packets sent from 192.168.1.5 to 192.168.1.1. The packets are for various ports: 48583, ftp (3072), h323hostcall (4096), netbios-ssn (3072), smtp (1024), and https (2048). All these packets are filtered out, indicating that the firewall at the destination is blocking them.

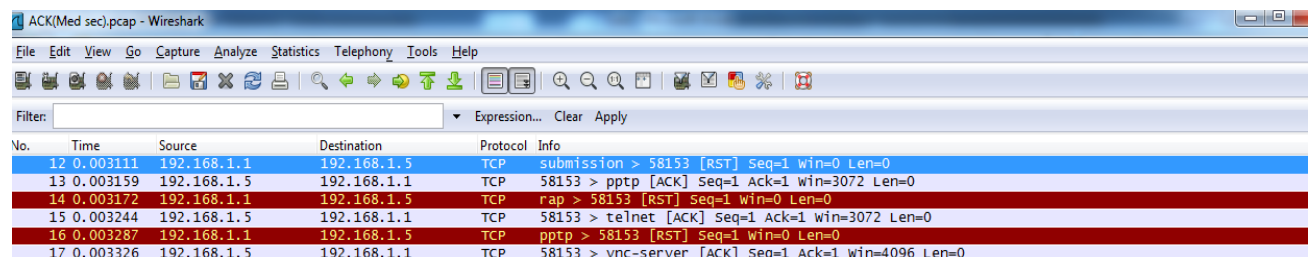
No.	Time	Source	Destination	Protocol	Info
18	1.12/30/	192.168.1.5	192.168.1.1	TCP	48583 > nmap [SYN] Seq=0 win=2048 Len=0 MSS=1460
19	1.127370	192.168.1.5	192.168.1.1	TCP	48583 > ftp [SYN] Seq=0 win=3072 Len=0 MSS=1460
20	1.127433	192.168.1.5	192.168.1.1	TCP	48583 > h323hostcall [SYN] Seq=0 win=4096 Len=0 MSS=1460
21	1.127496	192.168.1.5	192.168.1.1	TCP	48583 > netbios-ssn [SYN] Seq=0 win=3072 Len=0 MSS=1460
22	1.127558	192.168.1.5	192.168.1.1	TCP	48583 > smtp [SYN] Seq=0 win=1024 Len=0 MSS=1460
23	1.234605	192.168.1.5	192.168.1.1	TCP	48582 > https [SYN] Seq=0 win=2048 Len=0 MSS=1460

Figure 2-0 TCP ACK scanning packet captured by wireshark at full security level

The Nmap command used for TCP Ack Scan is `"nmap -sA 192.168.1.1"`. The Nmap scan result shows that all the 1000 ports scanned are filtered at the full security level of firewall.

2.1.2 TCP ACK at Medium Security

When attacker send TCP ACK and firewall set at medium security level it is clear from figure 2-1 that there is reply 'RST' reset the connection from the victim computer. This information is sufficient for attacker to gather the open port information to carry out malicious activities like Viruses, Trojans, Eavesdropping, and Denial of Service Attacks.



The image shows a Wireshark capture of network traffic. The packet list pane displays several TCP packets. Packets 12, 14, and 16 are highlighted in red, indicating they are RST (Reset) packets sent from 192.168.1.1 to 192.168.1.5. These RST packets are responses to the attacker's SYN packets. Packets 13, 15, and 17 are highlighted in blue, indicating they are ACK packets sent from 192.168.1.5 to 192.168.1.1. These ACK packets are responses to the victim's RST packets.

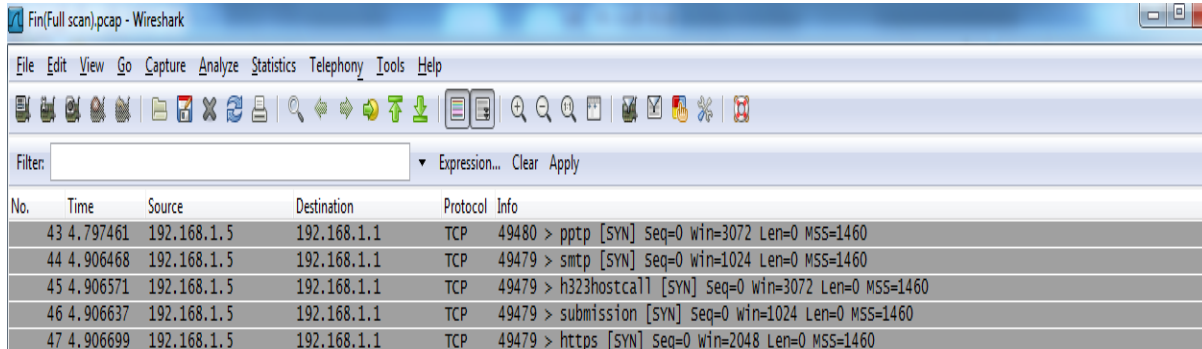
No.	Time	Source	Destination	Protocol	Info
12	0.003111	192.168.1.1	192.168.1.5	TCP	submission > 58153 [RST] Seq=1 win=0 Len=0
13	0.003159	192.168.1.5	192.168.1.1	TCP	58153 > pptp [ACK] Seq=1 Ack=1 win=3072 Len=0
14	0.003172	192.168.1.1	192.168.1.5	TCP	rap > 58153 [RST] Seq=1 win=0 Len=0
15	0.003244	192.168.1.5	192.168.1.1	TCP	58153 > telnet [ACK] Seq=1 Ack=1 win=3072 Len=0
16	0.003287	192.168.1.1	192.168.1.5	TCP	pptp > 58153 [RST] Seq=1 win=0 Len=0
17	0.003326	192.168.1.5	192.168.1.1	TCP	58153 > vnc-server [ACK] Seq=1 Ack=1 win=4096 Len=0

Figure 2-1 TCP ACK scanning packet captured by Wireshark at medium security level.

The Nmap command used for Ack Scanning is `"nmap -sA 192.168.1.1"`. The Nmap scan results shows that all the 1000 ports scanned are unfiltered.

2.1.5 TCP FIN at Full Security

When FIN scan is carried out in Full security mode there is no reply from victim computer. The figure 2-4 indicates that firewall at the victim computer drops the Fin packets.



The image shows a Wireshark capture window titled 'Fin(Full scan).pcap - Wireshark'. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Help), a toolbar with various icons, and a filter field. Below the filter is a table of captured packets. The table has columns for No., Time, Source, Destination, Protocol, and Info. Five packets are listed, all of which are TCP SYN packets from 192.168.1.5 to 192.168.1.1. The protocols are ppp, smtp, h323hostcall, submission, and https.

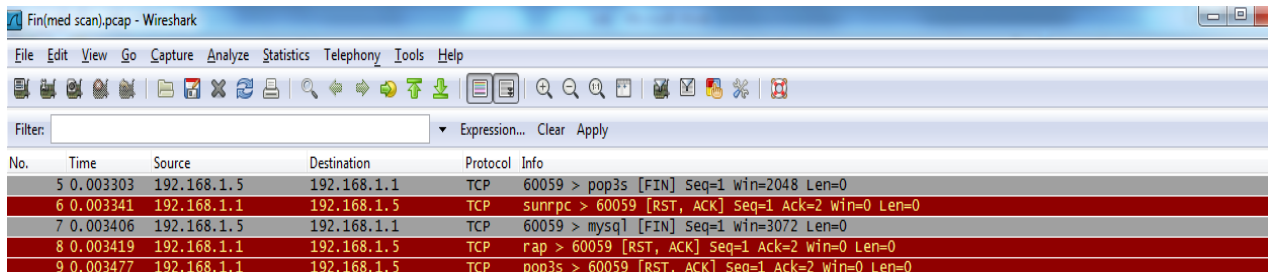
No.	Time	Source	Destination	Protocol	Info
43	4.797461	192.168.1.5	192.168.1.1	TCP	49480 > ppp [SYN] Seq=0 win=3072 Len=0 MSS=1460
44	4.906468	192.168.1.5	192.168.1.1	TCP	49479 > smtp [SYN] Seq=0 win=1024 Len=0 MSS=1460
45	4.906571	192.168.1.5	192.168.1.1	TCP	49479 > h323hostcall [SYN] Seq=0 win=3072 Len=0 MSS=1460
46	4.906637	192.168.1.5	192.168.1.1	TCP	49479 > submission [SYN] Seq=0 win=1024 Len=0 MSS=1460
47	4.906699	192.168.1.5	192.168.1.1	TCP	49479 > https [SYN] Seq=0 win=2048 Len=0 MSS=1460

Figure 2-4 shows the TCP FIN scan results when ZoneAlarm set at Full security level

The Nmap command used for FIN scanning is “*nmap -sF 192.168.1.1*”. Nmap results show that 1000 ports were scanned and all of them were filtered.

2.1.6 TCP FIN at Medium Security

When the firewall is set at Medium Security there is always a RST/ACK reply from the victim. Although victim computer firewall is resetting the connection but the attacker gets enough information that some firewall is blocking the ports. So the ports can be further exploited and used for malicious attacks as shown in the figure 2-5.



The image shows a Wireshark capture window titled 'Fin(med scan).pcap - Wireshark'. The interface is similar to Figure 2-4. The table of captured packets shows five entries. The first is a TCP FIN packet from 192.168.1.5 to 192.168.1.1. The subsequent four entries are TCP RST, ACK packets from 192.168.1.1 to 192.168.1.5, indicating that the victim's firewall is resetting the connection.

No.	Time	Source	Destination	Protocol	Info
5	0.003303	192.168.1.5	192.168.1.1	TCP	60059 > pop3s [FIN] Seq=1 win=2048 Len=0
6	0.003341	192.168.1.1	192.168.1.5	TCP	sunrpc > 60059 [RST, ACK] Seq=1 Ack=2 win=0 Len=0
7	0.003406	192.168.1.5	192.168.1.1	TCP	60059 > mysql [FIN] Seq=1 win=3072 Len=0
8	0.003419	192.168.1.1	192.168.1.5	TCP	rap > 60059 [RST, ACK] Seq=1 Ack=2 win=0 Len=0
9	0.003477	192.168.1.1	192.168.1.5	TCP	pop3s > 60059 [RST, ACK] Seq=1 Ack=2 win=0 Len=0

Figure 2-5 Packet captured through Wireshark during TCP FIN scanning

The ‘Nmap’ command used for FIN scanning is “*nmap -sF 192.168.1.1*”. According to Nmap 1000 ports were scanned and all of them were closed. This is because there is always connection reset reply from the victim.

2.1.7 TCP SYN Scan at Full Security

It is a nice method to learn the open and listening ports. To perform this method SYN packets are sent to the victim host to gather information of opening and listening ports. When the firewall is set to full security level, it drops the packets coming from intruder’s computer. Figure 2-6 clearly shows that there is no reply from victim’s host.

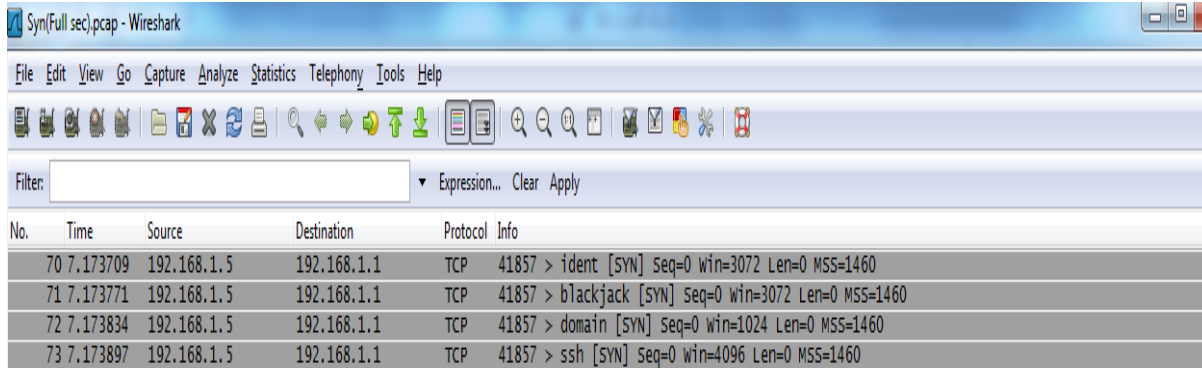


Figure 2-6 packet captured information of TCP SYN captured by Wireshark

The ‘Nmap’ command used for SYN scanning is “*nmap -sS 192.168.1.1*”. The Nmap scan result shows that all the 1000 ports scanned are filtered

2.1.8 TCP SYN at Medium Security

In this case the ports that are open send back SYN/ACK and the ports that are closed send back RST/ACK segment to the attacker which shows that ports are closed. The ports from which received no reply means that filtered as shown in figure 2-7.

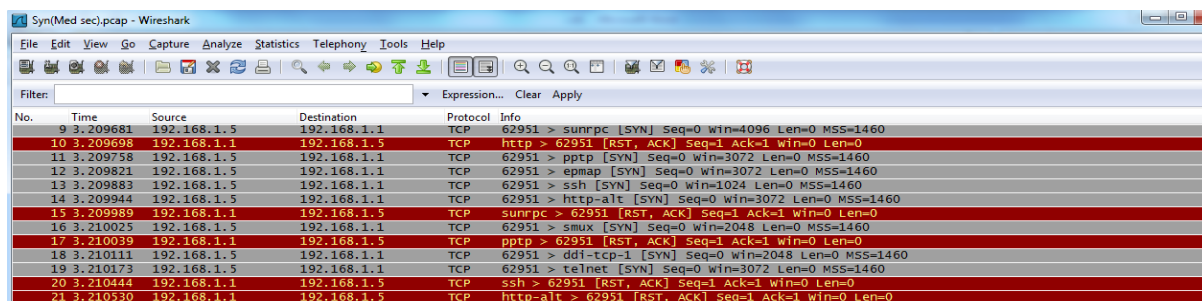


Figure 2-7 packet captured by Wireshark at the Attacker PC during TCP SYN scan

The Nmap command used for SYN scanning is “*nmap -sS 192.168.1.1*”. It is clear from the results shown by Nmap Table 2, 990 ports are closed, 1 port is filtered and 9 ports are in listening state.

Port	State	Service	Reason
135	tcp	msrpc	syn-ack
139	tcp	netbios-ssn	syn-ack
445	tcp	microsoft-ds	syn-ack
12000	tcp	cce4x	syn-ack
49152	tcp	unknown	no-response
49153	tcp	unknown	syn-ack
49154	tcp	unknown	syn-ack
49155	tcp	unknown	syn-ack
49156	tcp	unknown	syn-ack
49157	tcp	unknown	syn-ack

Table 2, shows information regarding the open ports during the TCP SYN scan

2.1.9 TCP Connect at Full Security

In full security mode the firewall at the victim host drops all the packets. It doesn't send any reset request or any other thing. So at full security the host is more secured against attacks. In the below figure there is no reply from victim host which is a clear indication that packets are being dropped by the firewall as shown in figure 2-8.

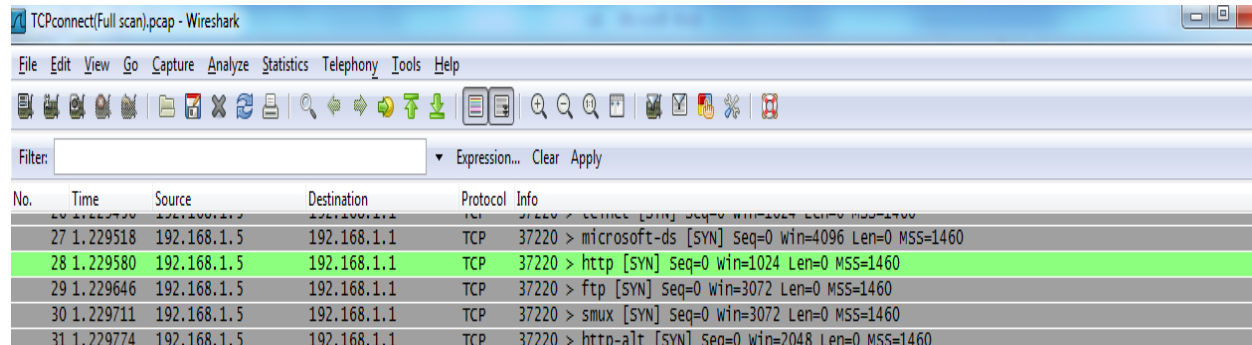


Figure 2-8 shows packets captured by Wireshark at the Attacker PC during TCP Connect

The Nmap command used for TCP connect is “*nmap -sT 192.168.1.1*”. NMAP scanned 1000 ports. All of them were filtered

2.1.10 TCP Connect at Medium Security

TCP connect is used to initiate a TCP connection with a remote device. In this case NMAP uses operating system normal method to initiate connection. In this case firewall blocks majority of the ports but still some ports are shown as open in figure 2-9.

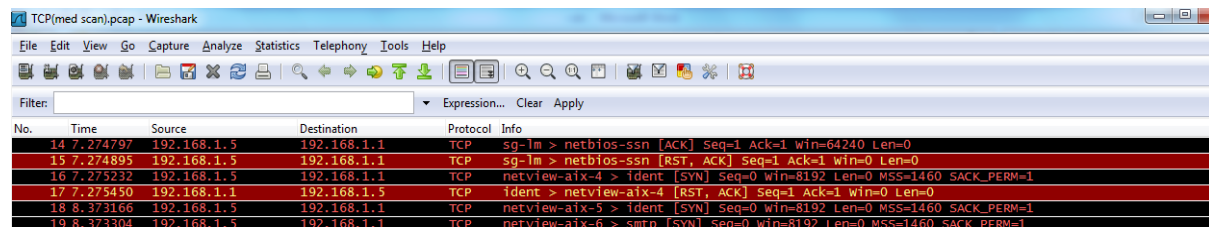


Figure 2-9 packets captured by Wireshark at the Attacker PC at medium security

The Nmap command used for TCP connect is “*nmap -sT 192.168.1.1*”. Nmap results shows that 991 ports are filtered and 9 ports were open as shown in Table 3.

Port	State	Service	Reason
135	tcp	msrpc	syn-ack
139	tcp	netbios-ssn	syn-ack
445	tcp	microsoft-ds	syn-ack
12000	tcp	cce4x	syn-ack
49153	tcp	unknown	syn-ack
49154	tcp	unknown	syn-ack
49155	tcp	unknown	syn-ack
49156	tcp	unknown	syn-ack
49157	tcp	unknown	syn-ack

Table 3, shows ports open by Nmap during TCP Connect

2.1.11 UDP Scan at Full Security

UDP scans are used to identify UDP open ports. In our case as the figure suggests there is no reply, this means the firewall is dropping the packets as shown in figure 2-10 there is no reply from the victim host.

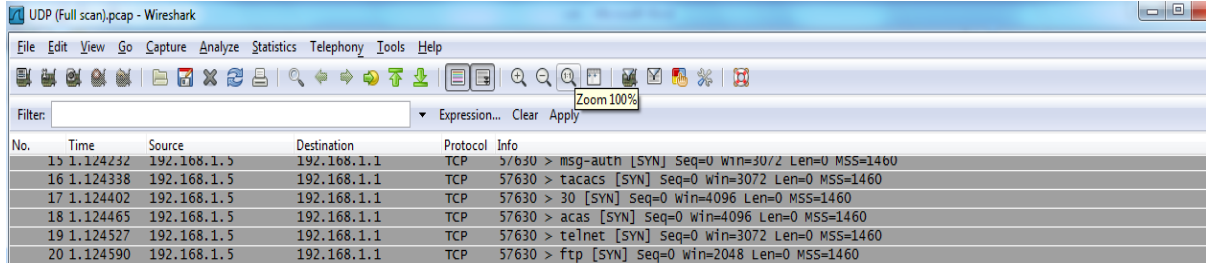


Figure 2-10 shows UDP scan packets captured by Wireshark

The Nmap command used for UDP port scanning is “*nmap -sU 192.168.1.1 -p 1-100*”. In this case 100 ports were scanned and all were found to be filtered.

2.1.12 UDP Scan at Medium Security

In UDP Scan we send UDP segment to check the open UDP ports on a system. If there is any response from the victim host it is open if victim reply with ICMP unreachable it means that port is closed as shown in the Table 4, 995 ports are closed, and from 2 ports received response and rest are open/filtered.

Port	State	Service	Reason
69	udp open	tftp	udp-response
123	udp open filtered	ntp	no-response
137	udp open	netbios-ns	udp-response
138	udp open filtered	netbios-dgm	no-response
500	udp open filtered	isakmp	no-response

Table 4, Nmap shows the UDP ports open during UDP scan

2.1.13 Teardrop Attack at High and Medium Security

We used Nessus to perform Teardrop attack. In teardrop attack Nessus fragments the packet whom sizes and offsets values were not consistent. This can cause receiving computer to crash due to the empty and overlapping fragementes when packets are reassambled. ZoneAlarm firewall drop all these packets as shown in the Table 5, which is the log file of ZoneAlarm firewall. It act in similar way on both high as well at medium security levels.

Rating	Date / Time	Type	Protocol	Program	Source IP	Destination IP	Direction	Action T...	Count	Source DNS	Destination DNS
Medium	2010-07-28 16:19:20+2:00	Firewall	TCP (flags:S)		129.16.20.205:49453	129.16.21.130...	Outgoing	Blocked	1	CSE-2562	CHIOS.ce.chalmer...
Medium	2010-07-28 16:19:00+2:00	Firewall	TCP (flags:S)		129.16.20.205:49452	129.16.21.130...	Outgoing	Blocked	1	CSE-2562	CHIOS.ce.chalmer...
Medium	2010-07-28 16:18:38+2:00	Firewall	TCP (flags:S)		129.16.20.205:49449	129.16.21.130...	Outgoing	Blocked	1	CSE-2562	CHIOS.ce.chalmer...
Medium	2010-07-28 16:18:18+2:00	Firewall	TCP (flags:S)		129.16.20.205:49448	129.16.21.130...	Outgoing	Blocked	1	CSE-2562	CHIOS.ce.chalmer...
Medium	2010-07-28 16:17:56+2:00	Firewall	TCP (flags:S)		129.16.20.205:49447	129.16.21.130...	Outgoing	Blocked	1	CSE-2562	CHIOS.ce.chalmer...
Medium	2010-07-28 16:17:06+2:00	Firewall	TCP (flags:S)		129.16.20.205:49442	129.16.21.130...	Outgoing	Blocked	1	CSE-2562	CHIOS.ce.chalmer...
Medium	2010-07-28 16:16:44+2:00	Firewall	TCP (flags:S)		129.16.20.205:49441	129.16.21.130...	Outgoing	Blocked	1	CSE-2562	CHIOS.ce.chalmer...
Medium	2010-07-28 16:16:24+2:00	Firewall	TCP (flags:S)		129.16.20.205:49440	129.16.21.130...	Outgoing	Blocked	1	CSE-2562	CHIOS.ce.chalmer...
Medium	2010-07-28 16:16:02+2:00	Firewall	TCP (flags:S)		129.16.20.205:49435	129.16.21.130...	Outgoing	Blocked	1	CSE-2562	CHIOS.ce.chalmer...
Medium	2010-07-28 16:15:42+2:00	Firewall	TCP (flags:S)		129.16.20.205:49434	129.16.21.130...	Outgoing	Blocked	1	CSE-2562	CHIOS.ce.chalmer...
Medium	2010-07-28 16:15:20+2:00	Firewall	TCP (flags:S)		129.16.20.205:49426	129.16.21.130...	Outgoing	Blocked	1	CSE-2562	CHIOS.ce.chalmer...
Medium	2010-07-28 16:15:00+2:00	Firewall	TCP (flags:S)		129.16.20.205:49424	129.16.21.130...	Outgoing	Blocked	1	CSE-2562	CHIOS.ce.chalmer...
Medium	2010-07-28 16:14:38+2:00	Firewall	TCP (flags:S)		129.16.20.205:49423	129.16.21.130...	Outgoing	Blocked	1	CSE-2562	CHIOS.ce.chalmer...
Medium	2010-07-28 16:12:32+2:00	Firewall	TCP (flags:S)		192.168.1.5:3940	192.168.1.1:631	Incoming	Blocked	1		CSE-2562
Medium	2010-07-28 16:12:32+2:00	Firewall	TCP (flags:S)		192.168.1.5:3939	192.168.1.1:280	Incoming	Blocked	1		CSE-2562
High	2010-07-28 16:12:32+2:00	Firewall	TCP (flags:S)		192.168.1.5:3938	192.168.1.1:80	Incoming	Blocked	1		CSE-2562
Medium	2010-07-28 16:12:32+2:00	Firewall	TCP (flags:S)		192.168.1.5:3937	192.168.1.1:79	Incoming	Blocked	1		CSE-2562
Medium	2010-07-28 16:12:32+2:00	Firewall	TCP (flags:S)		192.168.1.5:3936	192.168.1.1:9...	Incoming	Blocked	1		CSE-2562
Medium	2010-07-28 16:12:32+2:00	Firewall	TCP (flags:S)		192.168.1.5:3935	192.168.1.1:2...	Incoming	Blocked	1		CSE-2562
High	2010-07-28 16:12:32+2:00	Firewall	TCP (flags:S)		192.168.1.5:3934	192.168.1.1:23	Incoming	Blocked	1		CSE-2562
High	2010-07-28 16:12:32+2:00	Firewall	TCP (flags:S)		192.168.1.5:3933	192.168.1.1:21	Incoming	Blocked	1		CSE-2562
Medium	2010-07-28 16:12:26+2:00	Firewall	UDP		192.168.1.5:59784	192.168.1.1:9...	Incoming	Blocked	1		CSE-2562
Medium	2010-07-28 16:12:26+2:00	Firewall	TCP (flags:S)		192.168.1.5:3932	192.168.1.1:81	Incoming	Blocked	1		CSE-2562

Table 5, ZoneAlarm firewall’s log file that is blocking the packets.

2.1.14 Land Attack at Full and Medium Security

Land attack is based on spoofed IP address. We have performed this attack by using Engage Packet Builder. We used Two PC’s to carry out Land attack. From one PC we sent a malicious packet to the victim host with the same source IP address and destination IP address which is 192.168.1.1. The source port number and destination port number are also same which is 145. When the victim host received this malicious packet the ZoneAlarm firewall drops all these packets and shows an alert message. ZoneAlarm also save information of this packet its log file as shown in Table 6. Thousands of UNIX servers, Windows server, printers, switches and router got effected by this kind of attack when it first appeared in 1997 [2]. In land attack you can’t identify the identity of attacker because of the spoofed IP address. Modern operating systems are not vulnerable to such kind of attacks. As shown in figure 2-11 captured by the Wireshark the source IP, Destination IP, source port, destination ports are same.

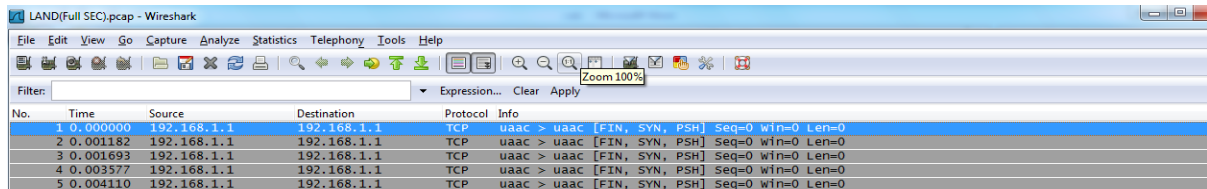


Figure 2-11 show the IP packets with the same source and destination IP address by wireshark during Land Attack

The Table 6 shows ZoneAlarm log file that clearly indicates the attack packet have been blocked by the firewall. It is also worth mentioning that after first packet is blocked ZoneAlarm blocks all communication with the attacking computer and doesn’t show anything in the log file for few

minutes. Even when the firewall is set at different security levels like at ‘Medium Security’ the results are same.

ZONEALARM Internet Security Suite											
Medium	2010-07-28 15:54:00+2:00	Firewall	TCP (flags:P...	192.168.1.1:145	192.168.1.1:145	Outgoing	Blocked	1	CSE-2562	CSE-2562	

Table 6, ZoneAlarm log file, it is blocking the IP packet with same source and destination IP address as well as source and destination ports number are also same

2.1.15 Ping of Death at High and Medium Security

To perform the Ping of Death attack we used Nessus. The normal size of IP packet is 65535 bytes. Nessus sends an IP segment greater than 65535. This attack doesn't damages the system but prevents the legitimate users to share resources. It may also cause the system to shutdown or reboot.

The ZoneAlarm firewall block all these malicious packets received from attacker as shown in the Table 7 which is the log file of ZoneAlarm.

Rating	Date / Time //	Type	Protocol	Program	Source IP	Destination IP	Direction	Action T...	Count
Medium	2010-07-28 16:34:10+2:00	Firewall	TCP (flags:S)		192.168.1.5:4301	192.168.1.1:7...	Routed	Blocked	1
Medium	2010-07-28 16:34:10+2:00	Firewall	TCP (flags:S)		192.168.1.5:4300	192.168.1.1:631	Routed	Blocked	1
Medium	2010-07-28 16:34:10+2:00	Firewall	TCP (flags:S)		192.168.1.5:4299	192.168.1.1:280	Routed	Blocked	1
Medium	2010-07-28 16:34:10+2:00	Firewall	TCP (flags:S)		192.168.1.5:4298	192.168.1.1:80	Routed	Blocked	1
Medium	2010-07-28 16:34:10+2:00	Firewall	TCP (flags:S)		192.168.1.5:4297	192.168.1.1:79	Routed	Blocked	1
Medium	2010-07-28 16:34:10+2:00	Firewall	TCP (flags:S)		192.168.1.5:4296	192.168.1.1:9...	Routed	Blocked	1
Medium	2010-07-28 16:34:10+2:00	Firewall	TCP (flags:S)		192.168.1.5:4295	192.168.1.1:2...	Routed	Blocked	1
Medium	2010-07-28 16:34:10+2:00	Firewall	TCP (flags:S)		192.168.1.5:4294	192.168.1.1:23	Routed	Blocked	1
Medium	2010-07-28 16:34:10+2:00	Firewall	TCP (flags:S)		192.168.1.5:4293	192.168.1.1:21	Routed	Blocked	1
Medium	2010-07-28 16:34:08+2:00	Firewall	TCP (flags:S)		192.168.1.5:4288	192.168.1.1:81	Routed	Blocked	1
Medium	2010-07-28 16:34:06+2:00	Firewall	UDP		192.168.1.5:55850	192.168.1.1:9...	Routed	Blocked	1

Table 7, Shows the log file of ZoneAlarm firewall which blocked all the malicious packets

2.2 Comodo Firewall

Comodo firewall showed almost the same results like other firewalls when we carried out different kinds of scanning tests like TCP ACK, Echo Ping, TCP FIN, TCP SYN, TCP Connect, UDP Scan and Denial of Service Attacks. During these scanning tests it showed many open ports. Ports 135, 139 and 445 which are very critical from security point of view were also shown open.

TCP port 445 is used for microsoft-ds service. The use of port 445 is resource sharing without the of NetBios layer. Port 445 should not be open if it is open it'll leave your system vulnerable against Trojans, Worms some of these are W32.Deloder, Iraqiworm, W32.HLLW.Moega, W32.Sasser.Worm, W32.Korgo.AB, Backdoor.Rtkit.B, Trojan.Netdepix.B and Windows Null Session Exploit. [8]

TCP Port 135 used for RPC services. This port should not be exposed or open when a host is connected to the internet if it is open it will cause your system vulnerable against Trojans, threats and Worms some of these are W32.Blaster.Worm, MSKB 330904, Secefa, W32.Kiman, Femot and W32.Cissi. [9]

Port 139 used for service Netbios Session Service. If file and print sharing is on than anyone can access them over the internet. Any PC with NetBios on and not configured properly than the PC is at risk. It'll leave your system vulnerable against Trojans some of these are Chode, Fire Hacker, Msinit, Nimda, Opaserv, Qaz, Nimda, SMB Relay, Sadmin and a Worm Netlogand God Message. [10]

<i>Scanning Method Performed</i>	<i>Port States</i>	<i>Explanation</i>
TCP ACK	Filtered	1000 ports are scanned and all the ports are filtered shown by Nmap.
Echo Ping	Filtered Ports 998 Open Ports 2	1000 ports are scanner and 998 ports are filtered and 139 and 445 ports are open shown by Nmap scanning results.
TCP FIN	Open/filtered	1000 ports are scanned and 1000 ports are open/filtered shown by Nmap TCP FIN scan.
TCP SYN	Filtered 996 Open Ports 135, 139, 445, 12000	1000 ports are scanned. Nmap scan shows that 996 ports are filtered and 135, 139, 445 and 12000 ports are opened.
TCP Connect	Filtered	1000 ports are scanned and all are filtered shown by Nmap.
UDP SCAN	Open/filtered	1000 ports are scanned and all are Open/filtered sate shown by Nmap.

Table 8, Nmap shows the ports states during performing the different kinds of scanning tests on Comodo Firewall

<i>Name Of Attack</i>	<i>Firewall Reaction</i>
Teardrop Attack	There is no effect of these attacks on Comodo firewall. In Wireshark we see the packets coming from the attacking computer but there is no effect on the victim. Even Comodo doesn't log anything regarding these attacks. It looks that Win7 automatically block these attacks.
Land Attack	
Ping Of Death Attack	

Table 9, shows the results while performing Denial of Service attacks on Comodo Firewall

2.3 Kaspersky Firewall

Kaspersky firewall has given the almost same results while performing the scan tests and Denial of Service Attacks. During the scanning tests it shows many open ports like 135, 137,139, 445, 1110, 12000, 19780, 49152, 49153, 49154, 49155 and 49156.

UDP Port 137 used for service Netbios Name Service. If file and print sharing is on than anyone can access files over the internet. Any PC with NetBios on and not configured properly is at risk. It'll leave your system vulnerable against Threats Bugbear, Msinit, Opaserv, Qaz and Femot [11]. The ports 135, 139 and 445 are very critical from security point of view as discussed in section 2.2. The remaining open ports Win7 used for its internal use.

Following are the results that we have obtained from Nmap during ports scanning as shown in Table 10.

<i>Scanning Method Performed</i>	<i>Port States</i>	<i>Explanation</i>
TCP ACK	Unfiltered	1000 ports are scanned and all the ports are unfiltered shown by Nmap.
Echo Ping	Close Ports 989 Open Ports 11	1000 ports are scanner and 989 ports are closed and ports 135, 139, 445, 1110, 12000, 19780, 49152, 49153, 49154, 49155, 49156 are open shown by Nmap scanning results.
TCP FIN	Closed Ports	1000 ports are scanned and 1000 ports are closed shown by Nmap TCP FIN scan.
TCP SYN	Closed Ports 989 Open Ports 11	1000 ports are scanner and 989 ports are closed and ports 135, 139, 445, 1110, 12000, 19780, 49152, 49153, 49154, 49155, 49156 are open shown by Nmap scanning results.
TCP Connect	Closed Ports 989 Open Ports 11	1000 ports are scanner and 989 ports are closed and ports 135, 139, 445, 1110, 12000, 19780, 49152, 49153, 49154, 49155, 49156 are open shown by Nmap scanning results.
UDP SCAN	Closed Ports 93 Open Ports 1 Open/Filtered 6	1000 ports are scanned and 993 ports are closed, 137 is open port and ports 138, 500, 1900, 4500, 5353, and 5355 are in Open/filtered sate.

Table 10, Nmap shows the ports states while performing the scan test on Kaspersky Firewall.

<i>Name Of Attack</i>	<i>Firewall Reaction</i>
Teardrop Attack	There is no effect of these attacks on Kaspersky firewall. In Wireshark we see the packets coming from the attacking computer but there is no effect on the victim. Even Kaspersky doesn't log anything regarding these attacks. It looks that Win7 automatically block these attacks.
Land Attack	
Ping Of Death Attack	

Table 11 shows the firewall results while performing Denial of Service attacks on Kaspersky Firewall

2.4 McAfee Firewall

McAfee firewall provides adequate protection against intrusions at different levels of security. The different security levels are Full Access, Monitored Access and Stealth Access. It is easy to use and there is a little interaction with the user. But a user has to have some knowledge to change the setting of firewall.

McAfee firewall has given the different results during the implementation of different kinds of scanning tests. During these scanning tests at different security levels it shows three open ports 137,139, 445. The importance of these open ports is discussed in sections 2.2 and 2.3.

Following are the results that we have obtained from Nmap during ports scanning as shown in tables 12, 13, 14 at different security levels.

<i>Full Access</i>		
<i>Scanning Method Performed</i>	<i>Port States</i>	<i>Explanation</i>
TCP ACK	Filtered	1000 ports are scanned and all the ports are filtered shown by Nmap.
Echo Ping	Filtered	1000 ports are scanner and all ports are filtered shown by Nmap scanning results.
TCP FIN	Open/filtered	1000 ports are scanned and 1000 ports are open/filtered shown by Nmap TCP FIN scan.
TCP SYN	Filtered 994 Open Ports 6646, 49152, 49153, 49154, 49155, 49156	1000 ports are scanned. Nmap scan shows that 994 ports are filtered and 6646, 49152, 49153, 49154, 49155, and 49156 are open due to received syn/ack from target.
TCP Connect	Filtered Ports 998 Open Ports 2	1000 ports are scanned oualt of which 998 l are filtered and 139 ,445 ports are open shown by Nmap.
UDP SCAN	Open/filtered Ports 999 Open Ports 1	1000 ports are scanned and 999 are Open/filtered sate and port 137 in open state shown by Nmap.

Table 12, Nmap shows the ports states while performing the scan tests on McAfee at Full Access security level.

<i>Monitored Access</i>		
<i>Scanning Method Performed</i>	<i>Port States</i>	<i>Explanation</i>
TCP ACK	Filtered	1000 ports are scanned and all the ports are filtered shown by Nmap.
Echo Ping	Filtered Ports 998 Open Ports 2	1000 ports are scanner out of which 998 ports are filtered and 139, 445 ports are open shown by Nmap scanning results.
TCP FIN	Open/filtered	1000 ports are scanned and 1000 ports are open/filtered shown by Nmap TCP FIN scan.
TCP SYN	Filtered 994 Open Ports 6646, 49152, 49153, 49154, 49155, 49156	1000 ports are scanned. Nmap scan shows that 998 ports are filtered and 139, 445 ports are open.
TCP Connect	Filtered Ports 998 Open Ports 2	1000 ports are scanned and 998 ports are filtered. The ports 139, 445 are open shown by Nmap.
UDP SCAN	Open/filtered Ports 999 Open Ports 1	1000 ports are scanned and 999 are Open/filtered sate and port 137 in open state shown by Nmap.

Table 13, Nmap shows the ports states during performing the scan tests on McAfee at Monitored Access security level.

<i>Stealth Access</i>		
<i>Scanning Method Performed</i>	<i>Port States</i>	<i>Explanation</i>
TCP ACK	Filtered	1000 ports are scanned and all the ports are filtered shown by Nmap.
Echo Ping	Filtered Ports 998 Open Ports 2	1000 ports are scanner out of which 998 ports are filtered and ports 139, 445 are open shown by Nmap scanning results.
TCP FIN	Open/filtered	1000 ports are scanned and all ports are open/filtered shown by Nmap TCP FIN scan.
TCP SYN	Filtered Ports 998 Open Ports 2	1000 ports are scanned. Nmap scan result shows that 998 ports are filtered and 139, 445 are open.
TCP Connect	Filtered Ports 998 Open Ports 2	1000 ports are scanned out of which 998 ports are filtered and 139, 445 ports are open shown by Nmap.
UDP SCAN	Open/filtered Ports 999 Open Ports 1	1000 ports are scanned and 999 are Open/filtered state and port 137 in open state shown by Nmap.

Table 14, Nmap shows the ports states while performing scan test at Stealth Access security level on McAfee.

<i>Name Of Attack</i>	<i>Firewall Reaction at All Levels of Security</i>
Teardrop Attack	There is no effect of these attacks on McAfee firewall. In Wireshark we see the packets coming from the attacking computer but there is no effect on the victim. Even McAfee doesn't log anything regarding these attacks. It looks that Win7 automatically block these attacks.
Land Attack	
Ping Of Death Attack	

Table 15, shows the firewall results while performing Denial of Service attacks on McAfee at Stealth Access.

2.5 Win7 Firewall

Win7 built in firewall gives adequate results while performing the scan tests like TCP ACK, Echo Ping, TCP FIN, TCP SYN, TCP Connect, UDP Scan and Denial of Service Attacks. The TCP ports 49152 to 49160 are used by Win7 for its internal use. Win7 firewall shows the same ports which are important from security point of view like TCP ports 445, 135, 139 and UDP ports 137 which are discussed in sections 2.2 and 2.3. Almost same ports are shown by the Comodo, Kaspersky, McAfee and ZoneAlarm firewalls at different scan test at different security levels of firewalls.

Following are the results that we have obtained from Nmap during ports scanning as shown in Tables 15 and 16.

<i>Scanning Method Performed</i>	<i>Port States</i>	<i>Explanation</i>
TCP ACK	Filtered	1000 ports are scanned and all the ports are filtered shown by Nmap.
Echo Ping	Filtered Ports 990 Open Ports 10	1000 ports are scanner, 990 ports are in filtered state and 135, 139, 445, 6646, 49152, 49153, 49154, 49155, 49159, 49160 are in open state.
TCP FIN	Open/filtered	1000 ports are scanned and 1000 ports are open/filtered shown by Nmap TCP FIN scan.
TCP SYN	Filtered Ports 990 Open Ports 10	1000 ports are scanner, 990 ports are in filtered state and 135, 139, 445, 6646, 49152, 49153, 49154, 49155, 49159, 49160 are in open state.
TCP Connect	Filtered Ports 996 Open Ports 4	1000 ports are scanned out of which 996 ports are filtered and 135, 139, 445, 12000 ports are open shown by Nmap.
UDP SCAN	Open/filtered Ports 999 Open Ports 1	1000 ports are scanned and 999 are Open/filtered sate and port 137 is in open state shown by Nmap.

Table 15, Nmap shows the port states of Win7 while performing scan test

<i>Name of Attack</i>	<i>Firewall Reaction</i>
Teardrop Attack	There is no effect of these attacks on Win7. Even Win7 log doesn't show any information in its log file and didn't show any kind of alert message. Win7 discard all these malicious packets.
Land Attack	
Ping Of Death Attack	

Table 16, shows the Win7 firewall results during different kinds of Denial of Service attacks.

2.6 Comparison

For TCP ACK Scan ZoneAlarm at Full Security, Comodo, McAfee at Full and Monitored Access levels shows the same results as all 1000 ports are filtered. Win7 also shows the same results as all 1000 ports filtered but Kaspersky and ZoneAlarm at Medium Security level gives all 1000 ports unfiltered.

For Echo Ping Scan ZoneAlarm at Full Security level and MacAfee at Full Access level shows the all 1000 ports are filtered but Comodo, Kaspersky and Win7 didn't show the same results and gives two or three common open ports 135, 139 and 445 which are very critical from the security point of view as discussed in section 2.2. The other open ports are not so important.

For TCP FIN Scan ZoneAlarm at Full Security level shows all 1000 ports are filtered, ZoneAlarm at Medium Security level as well as Kaspersky shows all 1000 ports are closed and Comodo, McAfee at Full, Monitored, Stealth Access levels and Win7 give all 1000 ports are Open/filtered.

For TCP SYN Scan ZoneAlarm at Full Security level show all 1000 ports are filtered, Comodo show 996 ports filtered, McAfee at Stealth Access level shows 998 ports filtered, at Full and Monitored access McAfee show 994 ports as filtered, win7 show 994 ports are filtered, Kaspersky show 989 ports and ZoneAlarm at medium security level show 989 ports are closed. The remaining ports are open ports as shown in Table 17 out of which three open ports 135, 139 and 445 are critical for security point of view which should be closed.

For TCP Connect Comodo, ZoneAlarm at Full and Medium Security level show all 1000 ports as filtered but Kaspersky show 989 ports as filtered, McAfee show 998 ports as filtered at all security levels and Win7 show 996 filtered ports. The remaining are open ports as shown in table 17. The ports 135, 139, 445 are important and should be closed as discussed in section 2.2.

For UDP Scan ZoneAlarm at Full Security level shows all 1000 ports are filtered and for Medium Security it shows 995 ports as closed, 3 ports as Open/filtered and 2 ports as open. Comodo firewall show 1000 ports as open filtered. McAfee at all security levels and Win7 show 999 ports as Open/filtered and one port as open. Kaspersky show 995 ports as closed, 1 port as open and 3 ports as open filtered. The open ports are 137 which are very important for security reasons.

Table 17 shows the comparison between different firewall while performing scan tests.

Scan Method	ZoneAlarm		Comodo	Kaspersky	McAfee			Win7
	Full Security	Medium Security			Full Access	Monitored Access	Stealth Access	
TCP ACK	1000 Ports Filtered	1000 ports Unfiltered	1000 ports filtered	1000 ports Unfiltered	1000 ports Filtered			1000 ports Filtered
Echo Ping	1000 Ports Filtered	990 ports Closed Open ports 135,139,445,12000,49152,49153,49154,49155,49156,49157	998 ports Filtered Open ports 139,445	989 Closed Ports Open Ports 139,135,445,1110,12000,19780,49152,49153,49154,49155,49156	1000 ports Filtered	998 ports Filtered Open Ports 139,445		990 ports Filtered Open ports 135,139,445,6646,49152,49153,49154,49155,49159,49160
TCP FIN	1000 Ports Filtered	1000 ports closed	1000 ports Open/Filtered	1000 Ports Closed	1000 ports Open/Filtered			1000 ports Open/Filtered
TCP SYN	1000 Ports Filtered	990 ports closed 1 filtered Open ports 135,139,445,12000,49152,49153,49154,49155,49156,49157	996 ports Filtered Open ports 135,139,445,12000	989 Closed Ports Open Ports 139,135,445,1110,12000,19780,49152,49153,49154,49155,49156	994 ports Filtered Open Ports 6646,49152,49153,49154,49155,49156		998 ports Filtered, Open Ports 139,445	990 ports Filtered Open ports 135,139,445,6646,49152,49153,49154,49155,49159,49160
TCP Connect	1000 Ports Filtered	1000 Ports Filtered	1000 Ports Filtered	989 Closed Ports Open Ports 139,135,445,1110,12000,19780,49152,49153,49154,49155,49156	998 Ports Filtered Open Ports 139,445		998 ports Filtered, Open Ports 139,445	996 ports Filtered, Open Ports 135,139,445,12000
UDP Scan	1000 Ports Filtered	995 ports closed Open filtered UDP Ports 123,138,500 Open ports 69,137	1000 Ports Open/Filtered	993 Closed Ports Open Port 137 Open/Filtered Ports 138,500,1900,4500,5353,5355,	999 Ports Open/Filtered Open Port 137			999 Ports Open/Filtered Open Port 137

Table 17 shows comparison of ZoneAlaram, Comdo, Kaspersky, McAfee and Win7 firewalls while performing Scan like TCP ACK, Echo Ping, TCP FIN, TCP SYN, TCP Connect, UDP Scan.

Conclusion

From the results it is clear that ZoneAlarm provide the best security results against all attacks and scanning methods. The reason is that it shows all ports are filtered at full security. It also gives warning alert against denial of service attacks and blocks the infected packets, while other firewalls didn't show the same results. In some cases ports were shown as filtered, Open/filtered, or closed. Some of the ports like 135, 137, 138, 139 and 445 were shown open. These open ports were not same for all the firewall as shown in Table 17. Most of the hackers or intruders exploit these ports to attack the victim hosts. McAfee, Kaspersky, Win7 and Comodo also provide good level of security.

In order for a firewall to be properly configured the user interface should be simple and attractive. It was easy to configure ZoneAlarm and Comodo firewalls. The interface was very user friendly. While the configuration of other firewalls (McAfee, Kaspersky, Win7) are somewhat tricky. The user needs to have at least some knowledge to configure them.

References

- [1] <http://accuwebhosting.com/articles>
- [2] Corporate Computer and Network Security, by Raymond R.Panko
- [3] <http://nmap.org/book/man-port-scanning-techniques.html>
- [4] <http://www.auditmypc.com/port-scanning.asp>
- [5] http://www.pcmag.com/encyclopedia_term/0,2542,t=land+attack&i=45907,00.asp
- [6] <http://insecure.org/sploits/ping-o-death.html>
- [7] <http://en.kioskea.net/contents/attaques/attaque-teardrop.php3>
- [8] www.speedguide.net/port.php?port=445
- [9] www.speedguide.net/port.php?port=135
- [10] www.speedguide.net/port.php?port=139
- [11] www.speedguide.net/port.php?port=137