Using Access Control List against Denial of service attacks

Hadya S. Hawedi[*]
Omran Ali Bentaher[**]
Kaled E. I. Abodhir[***]
Yousef abuadlla[****]

Abstract

The network security is very important in our daily life as people using the internet everywhere such as e-commerce, e-government, e-learning…..etc. One of the major threat on the network is denial of service attacks DoS. This paper studied DoS attacks, by launching them in a networked scenario and then demonstrated their effects. The objective of the study is to use Access control list ACL to stop these attacks. Wireshark had been used to monitor and analyze the flow of the packets. The administrator can decide whether there is DoS attacks or not based on server's resources (CPU usage, memory used) which are very high refer to unusual flood of packets. ACL has been used to stop the unusual flood. Cisco packet tracer had been used to demonstrate the DoS attacks and applied the ACL. This paper showed that the DoS attacks can be applied easily by the attackers and can be stopped easily using ACL by the administrator. The DoS attacks could

[*]- Faculty of information technology Al Asmarya university, hadia2008@yahoo.com
[**]- Higher institute of technology and science, omalbeta@yahoo.com
[***]- Faculty of economic Al Asmarya university, kdhir76@yahoo.com.
[****]- Faculty of electrical engineering Al Jafara university, ,aboadlla@gmail.com

be launched any way just the administrator has to stop it in early stage. This paper recommended that the administrators has to keep monitoring the network behaviors changes to stop the flooding.

Keywords: Denial-of-Service attacks, Access control list, Cisco packet tracer, Attacks, TCP/IP.

I. INTRODUCTION

The computer networks use for everything from banking, investing, shopping and communicating with others through email or chat programs [1]. When computer application developed to handle financial and personal data and you may not consider strangers reading your email, using your computer to attack other systems or sending forged email from your computer the real need for security was felt like never before. Network security is very important issue in our ear[2], however, one of the most important skills a network administrator needs is mastery of ACL [3]. The administrators use ACL to stop specified traffic while permit all other traffic on their networks. Network administrator uses ACL to protects the networks against flooding such as DoS attacks[4]. DoS attacks is one category of internet problems that can cause significant loss of time and revenue. DoS attacks are about sending large quantities of useless packets to overwhelm the victim. DoS attacks can be launch in a variety of ways due to a lot of vulnerabilities that exist in TCP/IP protocol. DoS is any type of attack on a networking structure to disable a server from servicing its clients such as (smurf , SYN flooding, land attacks). Attackers sending millions of requests using spoofed IP address to a victim(server) in an attempt to slow it down.

II. Types of DoS attacks.

1. Transmission control protocols synchronization |(TCP SYN) flooding: When a client attempts to establish a TCP connection to a server, the client first sends a SYN message to the server. The server then acknowledges(ACK) by sending a SYN-ACK message to the client. The client completes the establishment by responding with an ACK message. The connection between the client and the server is then opened, and the service-specific data can be exchanged between them. The abuse arises at the half-open state when the server is waiting for the client’s ACK message after sending the SYN-ACK message to the client. The server needs to allocate memory for storing the information of the half-open connection. The memory will not be released until either the server receives the final ACK message or the half-open connection expires(time out). Attacking hosts can easily create half-open

connections via spoofing source IPs in SYN messages or ignoring SYN-ACKs[5]. The consequence is that the final ACK message will never be sent to the victim, because the victim normally only allocates a limited size of space in its process table, too many half-open connections will soon fill the space. Even though the half-open connections will eventually expire due to the timeout, zombies can aggressively send spoofed TCP SYN packets requesting connections at a much higher rate than the expiration rate. Finally, the victim will be unable to accept any new incoming connection and thus cannot provide services. [6].

2. Internet control message protocol (ICMP) Smurf Flooding. ICMP is often used to determine if a computer in the internet is responding, to achieve this task, an ICMP echo request packet is sent to a computer, if the computer receives the request packet it will return an ICMP echo reply packet, attacking hosts forge ICMP echo requests having the victim's address as the source address and the broadcast address of these remote networks as the destination address, all the host in the subnets would reply to the victim. The victim would be affected and went down. [7] [8] [9].

3. Land Attack. Land attack occurs when an attacker sends spoofed SYN packets containing the IP address of the victim as

both the destination and the source IP address. The victim responds by sending the SYN-ACK packet to itself, creating an empty connection that lasts until the idle timeout value is reached. Flooding a system with such empty connections can overwhelm the system, causing a denial of service (DoS)[10].

III. Monitoring

It is difficult to mitigate an attacks without good information about their characteristics. Monitoring a network is essential step to know DoS attacks behavior. Wireshark was using to monitor the network. Wireshark is a very useful tool in monitoring traffic patterns and DoS attacks. Wireshark is a versatile and flexible network protocol analyzer that can be extended using plugins and dissectors. Since it is open-source and freely available, it can be adapted to the needs of specific applications. Wireshark can be attached to local network interfaces, thereby overhearing incoming packets that are subsequently analyzed and presented to the user. It allows to save packets into files for later analysis and to filter the displayed data. A flow TCP packets are defined as having the following unique attributes for example: Source and destination IP address. Source and destination port. After analyzing the packets the ACL rules can be defined.

IV. Access control list.

An ACL is a sequential list of permit or deny statements that apply to addresses or upper-layer protocols[11]. ACLs provide a powerful way to control traffic into and out of the network. You can configure ACLs for all routed network protocols. The most important reason to configure ACLs is to provide security for a network. There are two types of ACLs which are standard and extended as part of a security solution.Standard ACL's are used to control network access by specific hosts or networks. These ACL's control access based on the source address of the IP packets. Standard ACL's commonly use identification numbers from 1 to 99, but they can also use names. The basic syntax for a standard access control list is:

access-list <1 to 99> <permit or deny> <source IP address> <wildmask>. While Extended ACL's are used to filter specific types of traffic from specific locations. These ACL's control traffic by protocol, source address, and destination address of the IP packets. Extended ACL's use identification numbers from 101 to 199. Like Standard ACL's, Extended ACL's can also use names instead of numbers. The basic syntax for an extended access control list is:

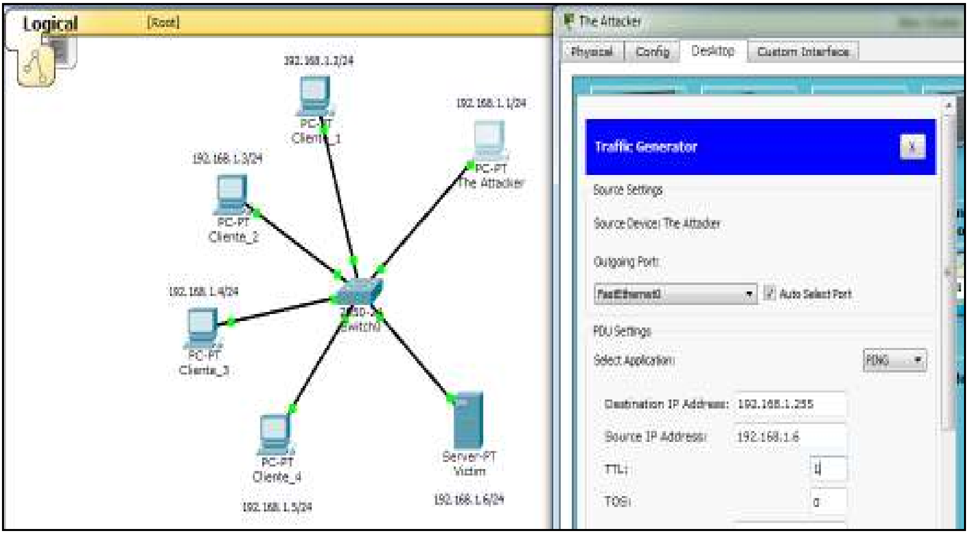
access-list <101 to 199> <permit or deny> <protocol> <source IP address> <wildmask> <destination IP address> <wildmask>[12].

V. Implementation and results

This paper explained how the ACL can be used to stop flooding the victim. Cisco packet tracer simulation tool had been used to implement flooding the victim in different scenarios such as smurf and TCP syn attacks. Different scenarios had been implemented to see the impacts of the DoS attacks on victim's resources (memory ,CPU usage) and how to stop noticed flood via wireshark using ACL.

Scenario 1:

We design the next topology which has 5 clients and one server. The attacker wanted to flood the server by launching smurf attack with spoofing it's IP address using the victim's IP (192.168.1.6) to ping the broadcast IP (192.168.1.255) as shown in fig (1)



Traffic Generator

Source Settings

Source Device: The Attacker

Outgoing Port:

FastEthernet0 ☑ Auto Select Port

PDU Settings

Select Application: PING

Destination IP Address: 192.168.1.255

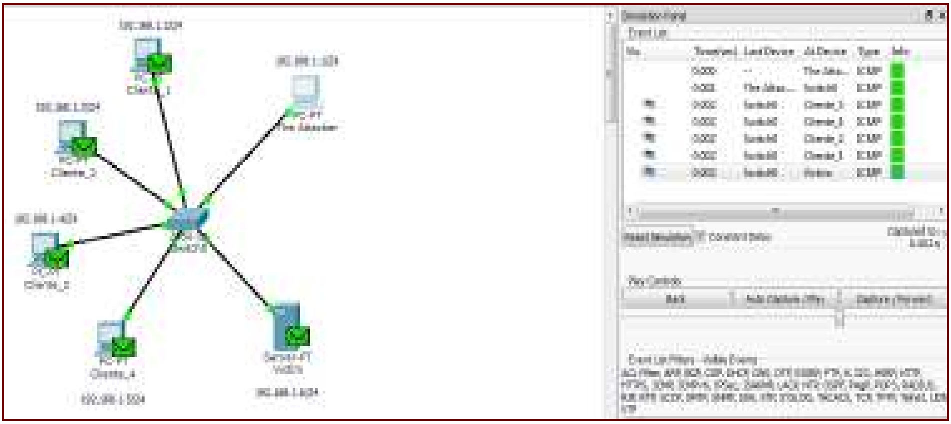
Source IP Address: 192.168.1.6

TTL: 1

TOS: 0

Figure (1) Traffic generator

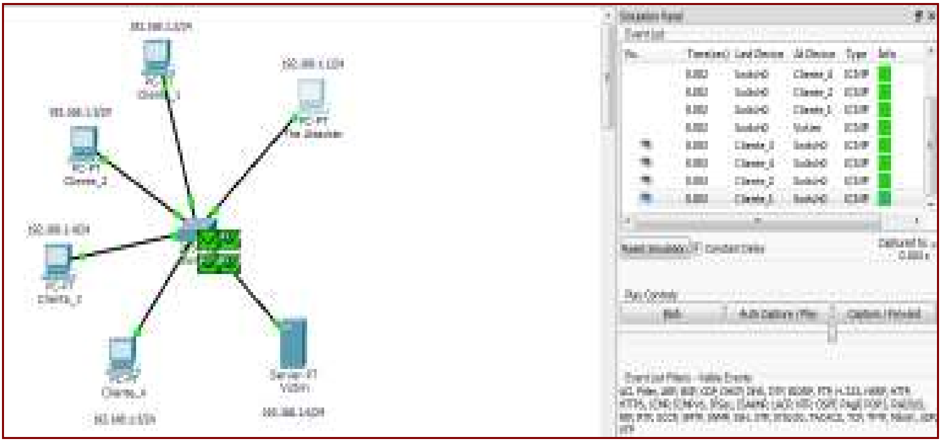
As you can see in fig (2,3) the attacker sent packets to all the clients via switch. All clients replied to the victim which is representing the server in this scenario as shown in fig (4). Imagine if there are thousands of clients in the net responding to the victim so it will not be available to the legitimate clients any more as its resources overwhelmed and that is what the attacker looking for.



Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	The Atta...	ICMP	🟩
	0.001	The Atta...	Switch0	ICMP	🟩
👁	0.002	Switch0	Clients_1	ICMP	🟩
👁	0.002	Switch0	Clients_3	ICMP	🟩
👁	0.002	Switch0	Clients_2	ICMP	🟩
👁	0.002	Switch0	Clients_1	ICMP	🟩
👁	0.002	Switch0	Victim	ICMP	🟩

Event List Filters - Visible Events
ACL Filter, ARP, BGP, CDP, DHCP, DNS, DTP, EIGRP, FTP, H.323, HSRP, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NTP, OSPF, PagP, POP3, RADIUS, RIP, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP

Figure (2) The attacker sends broadcast



Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.002	Switch0	Clients_4	ICMP	🟩
	0.002	Switch0	Clients_2	ICMP	🟩
	0.002	Switch0	Clients_1	ICMP	🟩
	0.002	Switch0	Victim	ICMP	🟩
👁	0.003	Clients_3	Switch0	ICMP	🟩
👁	0.003	Clients_4	Switch0	ICMP	🟩
👁	0.003	Clients_2	Switch0	ICMP	🟩
👁	0.003	Clients_1	Switch0	ICMP	🟩

Event List Filters - Visible Events
ACL Filter, ARP, BGP, CDP, DHCP, DNS, DTP, EIGRP, FTP, H.323, HSRP, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NTP, OSPF, PagP, POP3, RADIUS, RIP, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP

Figure (3) The clients reply to the victim

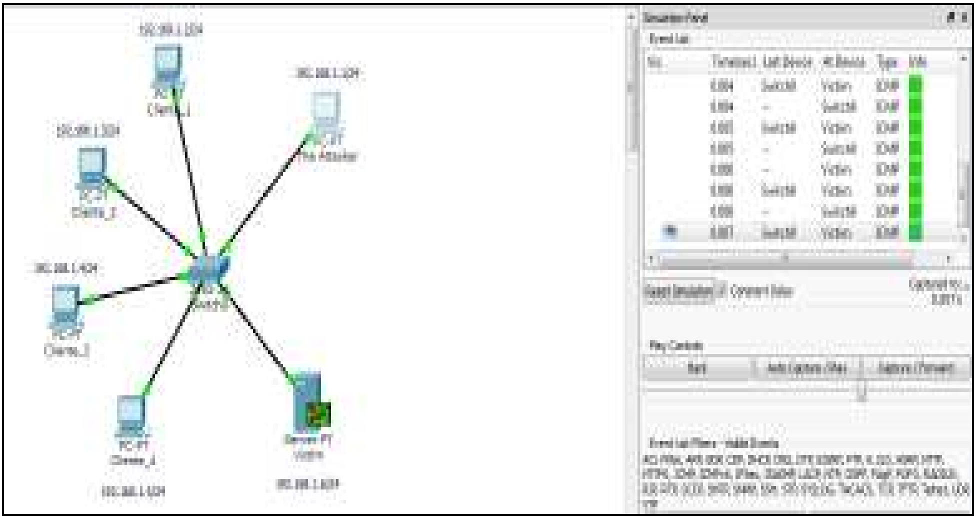


Figure (4) The victim is flooded

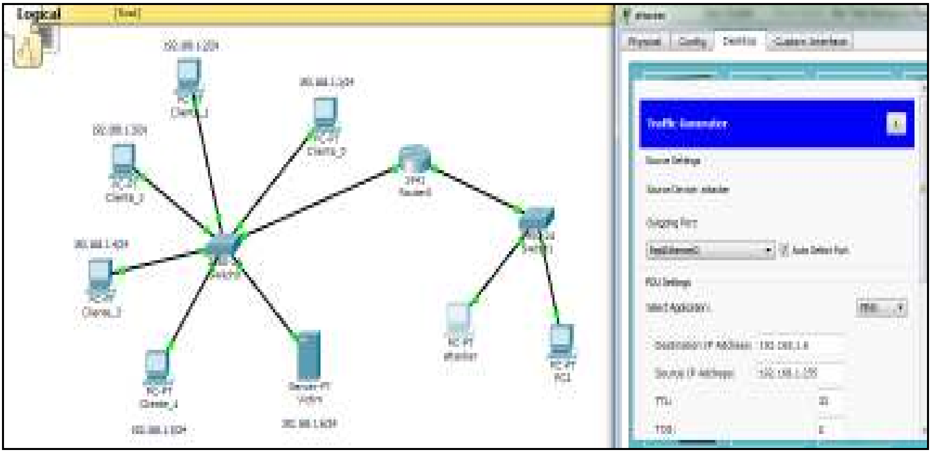
After monitoring, analyzing and noticing the flooding, the administrator activate the ACL to stop the smurf attack as shown before by applying the next rules.

- Access-list 100 deny icmp 192.168.1.1 0.0.0.0 192.168.1.6 0.0.0.0
- Access-list 100 permit ip any any

The first rule stoped the attacker (192.168.1.1) to launch the smurf attack against the victim used the ping command (ICMP). In the second rule permit other hosts to connect the same network. If the flooding launching by other clients, the administrator updates the ACL rules.

Scenario 2:

In this scenario we launched TCP SYN flood which explained earlier in section II. We designed the next topology in fig(5,6) which has an attacker wanted to established a connection with the server(victim) using it's IP address as a destination IP(192.168.1.6) and the broadcast IP address of the network where the victim reside (192.168.1.255) as source IP to create a lot of half open connection to overwhelm the server.



Traffic Generator

Source Settings

Source Device: attacker

Outgoing Port:

FastEthernet0 ☑ Auto Select Port

PDU Settings

Select Application: PING

Destination IP Address: 192.168.1.6

Source IP Address: 192.168.1.255

TTL: 32

TOS: 0

Figure (5) Generating TCP SYN flood

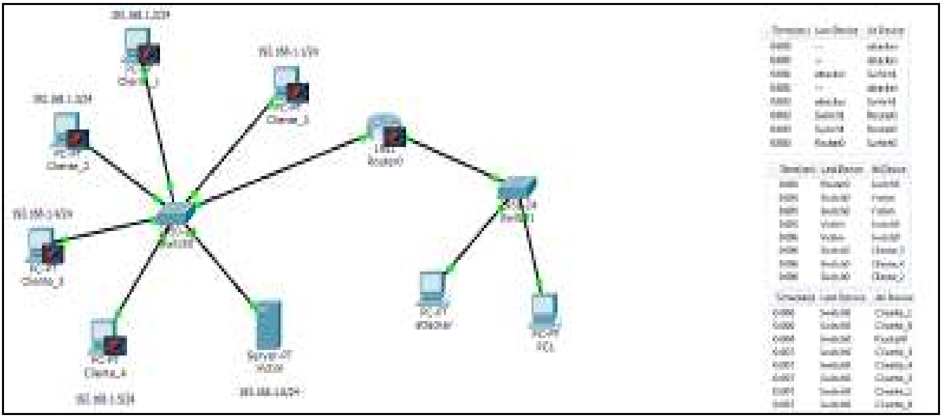


Figure (6) Clients omit the SYN ACK to the victim

As shown in figure(6) the server received the packets carrying broadcast IP(192.168.1.255) as source IP address and the victim IP address as destination IP(192.168.1.6).The victim reply to all clients to open the connection using three way hand shack then the clients would not complete the connection because they have not send the syn request. A lot of half open connection created to engage the server and will not be available to the legitimate clients any more, and that is attackers purposes. Immediately the administrator activate the ACL to stop the flooding by using the following rules:

- Access-list 88 ip deny 192.168.255 0.0.0.0
- Access-list 88 ip any

In the first rule stop any packet carrying broadcast IP address as source IP. In the second rule permit other packets.

VI. Conclusion

In this paper, we overviewed existing DoS attacks and their impacts in the networks. We have learned about how we can protect our networks using an ACL from DoS attacks. Monitoring the network behavior helped to indicate whether there is flood or not. ACL Permitted only allowed packets and denied all others based on predefined rules. The ACL which had been implemented in the scenarios worked properly to stop these attacks. ACL in place at the ingress and egress points of a network were a key part of the first line of defense. All the implementations done were consists of very simple and light loaded DoS attacks and simple ACL rules to satisfied the needs. Finally we conclude that DoS attacks can be launched easily but the idea in our work is to stop it in early stage by applying very simple ACL's rules.

VII. References

1 - R.K.C. Chang, “Defending against Flooding-Based Distributed denial-of-Service Attack: A
Tutorial,” IEEE Communication Magazine, October 2002, 42-51.

2- Ashima Jain ,Network Security-The Biggest Challenge in Communication, Advance in Electronic and Electric Engineering. Research India Publications,2013.

3- Routing Protocols Companion Guide. Cisco Networking Academy - Computers - 2014.

4- Dennis Eck, Access Control Lists to Protect a Network from Worm/DoS Attacks, CCNA, 2003.

5- Sílvia Farraposo, Network Security and DoS Attacks, 2005.

6- Ali kadhum m.Al-qurabat, Security Attacks, 2007.

7- C. Joshi, and Manoj Misra, Distributed Denial of Service Prevention Techniques B. B. Gupta, IEEE,2010.

8- Kavita Choudhary,Smurf Attacks: Attacks using ICMP, University, Gurgaon, Haryana, India 2011.

9- Harshita, Detection and Prevention of ICMP Flood DDOS Attack, 2017.

10- Marwan Darwish, Cloud-based DDoS Attacks and Defenses, Department of Electrical and Computer Engineering University of Western Ontario London, Canada ,2014.

11- Eng.Alaa Arabiyat, Access Control Lists (ACLs),Advance Networks Laboratory , University of Jordan.

12- Nancy Navato, Easy Steps to Cisco Extended Access List GSEC,2001.