Enhancing network security by implementing preventive mechanism using GNS3

[1]Dhanalakshmi.R, [2]Elakkiya.P, [3]Elavarasi.M, [4]Fareedha.A and [5]Rajesh kumar.K
[1,2,3,4]UG Scholar,Department of ECE,Adhiyamaan College of Engineering,Hosur,TN,India
[5]Assistant Professor,Department of ECE,Adhiyamaan College of Engineering,Hosur,TN,India
[1]dhanasenthil00750@gmail.com, [2]elakkiyamano22@gmail.com, [3]vijayaelavarasi@gmail.com,
[4]fareedhakhan53@gmail.com, [5]Rajeshmadesh@gmail.com

Abstract

Due to rapid need of computer's in business and other organizations many networks has been established. In today scenario attacks on computer networks has increased to a great extend. Networks are very much needed but they are very prone to attacks because of security breaches & vulnerabilities in traditional establishments. There are many types of attacks which can be penetrated in our networks or edge devices; one of the most prone attacks is the ICMP flood attack leading to denial of service. Further we describe the need of establishment of secure computer networks by using proper policies, rules on edge network devices. We also have tested them in Lab using GNS3 simulator. By implementing enhanced policies internal network's can be secured from attacks like ICMP flood.

Keywords--- **ICMP, GNS3**

1. Introduction

With rapid increase in the usage of computer networks for storing & sharing data, security breaches & attacks on computer networks has also increased at an alarming rate. Even attacks from outside has increased in the past few years. It also has been revealed by UK government, annual survey on cyber security not only the large organization but even the small business has been badly targeted by approximate 63% see figure **1.** Also it has been reported that attacks has also been increased upto 41 % a year ago.

Due to IPv4 network suffering more and more problems, especially the lack of address space as well as the network security flaws, the next generation IPv6 network research caught to be focused. The IPv6 has solved IP address crisis, which expands IP address from 32-bit to 128-bit. There is limitation of compatability between IPv6 and IPv4, therefore, transition mechanism from IPv4 to IPv6 is studied widely, mainly focuses on dual stack mechanism and the tunnel mechanism. This paper describes the principles of transition mechanism, makes a comparison of analysis by testing the performance of IPv6 based on commonly used transition mechanism.

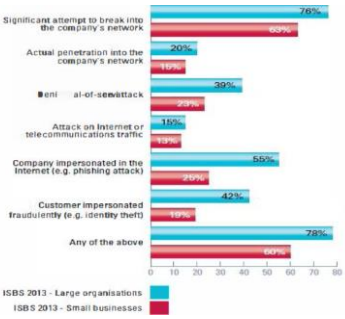

Figure 1:Attacks on small and large organizations

Figure 1, clearly shows that both small and large organizations are being repeatedly targeted.

2. Types of Network Attacks

There are many types of networks based attacks. Some major network attack can be classified as follows:

Distributed Attacks: In this type of attack malicious code is introduced by the attacker in the victim's system or network components , in order to gain unauthorized access to the network resources. By this valuable confidential information is lost. DDoS is an example of distributed type of attacks.

Active Attacks: In this Active Attacks type of attack, attacker gains access to the system by exploiting or changing resources or devices of the system. Once the system is compromised, the attacker can transmit, modify ordelete the data leading to the lost integrity of the network information. DoS are one of type of active attacks and in recent years there has been increase in the DoS attacks.

Close in attacks: One type of close in attacks is social engineering attacks where the attacker uses details of the other persons & tries to exploit them by sending email or phones & tries to obtain confidential information about their bank accounts etc. In close-in-attacks the attacker tries to gain information from physical entities or network components by getting physically close.

DOS attacks: Denial of service attack is one of the most dangerous attacks and a major threat to small & large organizations networks, systems, users etc. By increased usages of internet there is high increase in denial of service. (DOS) attacks. The main aim of this attack is the denial of services by attempting to bound access to a service or machine. DOS attack is an attack that uses much memory on the target system or devices that it cannot provide services to its users, or it may be able to reboot, system crash or denying services to legitimate users. Just about one or other server or host may experience DOS attacks at any time.

3. Types of DOS attacks

The first DOS attack occurred on November 2, 1988. This attack was self propagating & self replicating and as a result 15% of systems connected to network was stopped running and were infected. There are several kinds of DOS attacks, the popular are as follows:

- ICMP flood attack
- Teardrop attacks
- SYN-flood attacks
- Land attacks
- Surf attacks

These above have been used by many attackers at times to affect the target systems. One of the most dangerous attacks is the ICMP flood attacks. Here we would discuss this attack in particular the ping command makes use of the ICMP echo request and echo reply message and is used commonly to determine whether the remote host is alive.

ICMP Flood Attack: In this type of attack ping causes the remote system to hang, reboot or crash. To do so, the attacker exploits the internet control message protocol (ICMP) , which enables users to send an echo packet to a remote host to check whether it's alive. During a DOS ICMP Flood Attack, attacker sends a large volume of ICMP_ECHO_REPLY packets by using ping to victim. These packets request reply from the victim and this results in saturation of the bandwidth of the victim network connection.

4. Protection mechanism

There are many mechanisms available to counter Network Security breaches few of them are discussed briefly below:

Firewall: Firewall is a type of security mechanism system that controls the intrusion or say virus packet by analyzing incoming and outgoing packet at network.

Reactive Mechanisms: These mechanisms reduce the impact of attack on the victim. These mechanisms are also called as early working systems which respond to an attack immediately when the attack is detected.

There are many other mechanism available to enforce security in a network or edge devices, still they are not enough as newer networks are being established day by day and also the technologies are changing rapidly. In this paper our approach is to apply some policy on network edge devices like router to counter ICMP flood attack. We also would test these policies by simulating them using GNS3 network simulator.

5. Main contributions Simulation and Experimentation

- Analyzing current state of computer network security.
- Studying different types of DOS attacks.
- Analyzing the need of Policy to enhance network security on edge devices. Testing the policy using GNS3 network simulator to protect our network from
- ICMP flood attacks.

6. Simulation and Experimentation

In our work, Attackers flood the target system with connection requests from spoofed source. Here in the figure 2, below we have an internal network which contains few systems, connected to a switch connected to a web server. The internal network is connected by Cisco 3725, router's hypervisor run on 127.0.0.1:7200, console is on port 2101, aux is on 2501, Fast Ethernet 010 is connected to attacker.
Fast Ethernet is connected to switch sw1 port 1. The switch is further connected to systems in the Lan. We assume that the attacker attacks from outside the

internal network and tries to flood the target system by flood of ICMP messages. Large number and different large size ICMP packets are being send to the victim. This all is being tested and simulated using GNS3 which provides graphical user interface to simulate complex networks while being as close as possible from the way real network and devices perform.

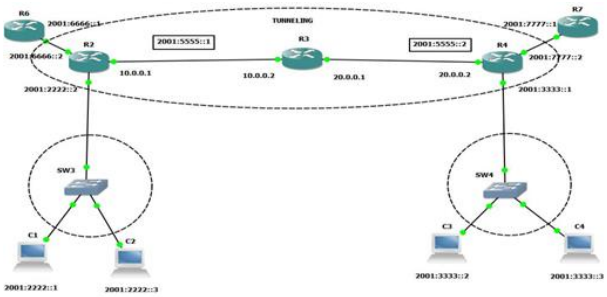

Figure 2. Network diagram

ICMP flood attack attempts to crash the system of the target system by sending many ICMP echo request packets, so that the victim gets flooded with packets reducing the data sending capacity for normal traffic. So as to protect our internal network from this attack we apply a policy on edge device. This policy can protect our internal network from following:

- Preventing the target system from device crash
- Network slowness
- Network outage

7. Policy

Open Shortest Path First (OSPF) is a commonly used IGP (Interior Gateway Protocol) routing protocol within Autonomous Systems which helps to improve inter-network performance by assigning weights to the links between routers. Cost factors can be applied to each link based on numerous metrics. These include distance to a router, maximum possible throughput of the link between routers, and the availability of a link. Using these metrics, a single unit-less number known as a weight is assigned to that link.

In order to calculate the shortest path, the network is considered as a graph, with each router being a node and the links between them being edges. A method based on Dijkstra's algorithm, a shortest-path-first algorithm, is then run to find the shortest path through the network, with the link weights being used in place of the edge distance that the algorithm requires.

These weights are then applied to each link between hardware, with a low weight corresponding to a desirable path, and a high weight signifying an undesirable path. By default, upon start-up before OSPF has initialised, each path will be assigned a value of 10.

For ipv4 configuration and ospf configuring

R1(config)#interface eth1/1
R1(config-if)#ip address 10.0.0.1 255.0.0.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router ospf 100
R1(config)#network 10.0.0 0.255.255.255 area 0
R1(config)#network 192.168.155.1 0.255.255.255 area 0

For ipv6 configuration and OSPF configuration

R1#Configure terminal
R1(Config)#ipv6 unicast-routing
R1(Config)#interface ethernet1/1
R1(Config)#ipv6 enable
R1(Config)#ipv6 address 2001:1111::1/56
R1(Config)#no shutdown
R1(config)#exit
R1#Configure terminal
R1(Config)#ipv6 unicast-routing
R1(Config)#ipv6 router ospf 100
R1(Config)#router-id 1.1.1.1
R1(Config)#exit
R1(Config)#interface eth1/1
R1(config)#ipv6 ospf 100 area 0
R1(config)#exit

Configure routing protocol in router ports

we have to send the ipv6 packets through ipv4 service network is enable by using tunneling method
R2#config t
R2(config t)#int tunnel 1
R2(config t)#ip address (tunnel address)
R2(config t)#tunnel source f0/1(To know where the artificial tunnel starts)
R2(config t)#tunnel destination(To know where the tunnel destination ends)
R2(config t)#tunnel made ipv6ip
R2(config t)#exit

The screen shots below (figure 3) shows that before applying the policy success rate of attack is very high, with different size and time intervals the attack is genetrate and is successful up to 100%. We tried to send packets of different sizes from the attacker and we see almost all packets reach to host

network. Just in the first case only one packet was dropped. Thus it clearly indicates the success percentage up to 99%.

Screen shot

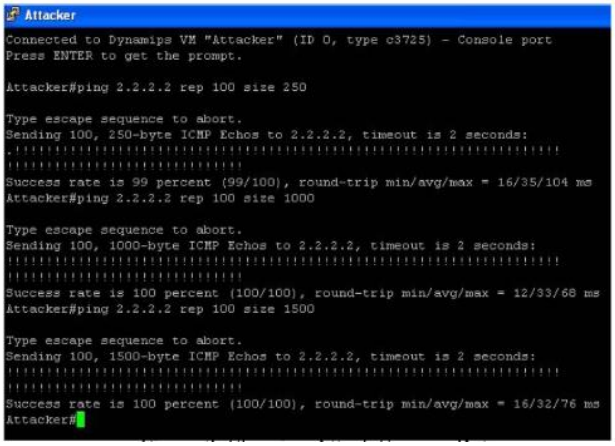

Figure 3: Showing attacks success rate

Below is the applied policy with other instructions which is applied on the edge device to protect internal network from ICMP flood attack.

7.1 Enabling security method

We have to enable the security to unauthorized user

R3#config t
R3(config t)#interface fastethernet0/0
R3(config t)#ipv6 ospf authentication ipsec spi 3000 md5 0123456789012345678 9ac
R3#config terminal
R3(config t)# interface fastethernet0/0
R3(config-if)# ipv6 ospf authentication ipsec spi 4000 md5 0123456789012345678 9bc

7.2 Ping test

We have to use the ping command to check whether the routing path is accessable for transferring the data packets from source to destination

eg: ping command
ping 10.0.0.1

7.3 Check for unauthorized userComparative Analysis

After giving the security to the authorized router the unauthorized routers cannot access our system

Eg:
ping 2001:7777::1

output: time out.

Before transferring the packets first the system has to assigned with some ip address in VPCS tool in GNS3 simulator

Screenshot

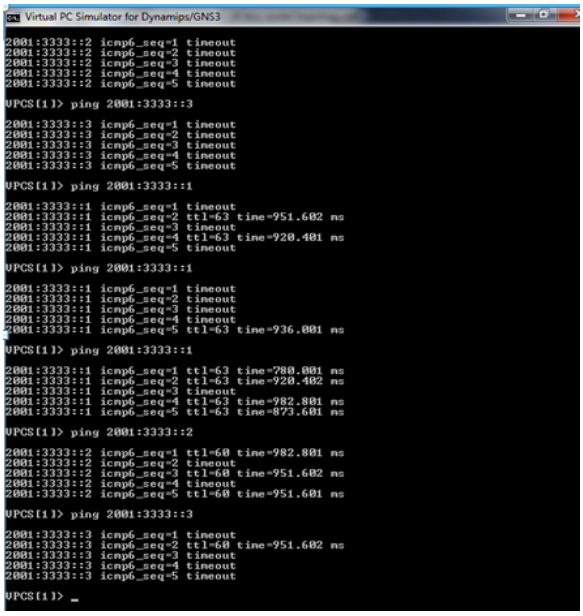

Figure: Output of the project

The IPV6 data is sent from any of the four system to another through tunneling path which is a IPV4 medium.The unauthorized routers [R6 and R7] cannot access the data from the host system.

8. Related work

There are many researchers who had done lots of work on network security maybe just even after the establishment of first Network, few more papers related to our work are:

Ioannidis and S. Bellovin, in 2002, implemented mechanism on router based on pushback concept for defense against flooding attacks.

In 2011, Mitko Bogdanoski, Aleksandar Risteski, By sending bogus ICMP redirect packets, a malicious user can either disrupt or intercept communication from a wireless access point. In their paper, they present an approach to simulate the ICMP Ping Flood Attack, and to analyze the effects of this attack on wireless networks using OPNET Modeler.

9. Comparative Analysis

In the paper by Katerina Argyraki and David R. Cheriton, in 2009 present Active Internet Traffic Filtering (AITF) [12], a network-layer defense mechanism against Internet Bandwidth- Flooding Attacks. They have showed that: (1) AITF allows a receiver to preserve on average 80% of its tail circuit in the face of a SYN-flooding attack that has ten times the rate of its capacity. (2) Each participating ISP needs a few thousand filters and a few megabytes of DRAM per client; the per-client cost is not expected to increase, unless botnet-size growth outpaces Moore's law. (3) The first two AITF-enabled networks can maintain their communication in the face of flooding attacks, as long as the path between them is not compromised.

10. Conclusion and Future Work

With rapid usage of computers attacks on networks is increasing day by day. While advanced techniques have been continuously developing for several years, it is very important to protect our office and business networks from new evolved attacks. Recent surveys have clearly revealed that attacks on smaller organizations also has increased to a great extend. Attacks like DOS attacks are also increasing thus there is a great need of more awareness among users and the development of advanced security policies, rules, devices to protect networks form security breaches. In this paper few categories of attacks are discussed, there are many mechanisms available to counter these types of attacks but for small organizations or small networks it is very hard to implement, configure or purchase mechanisms. Internal networks of small organizations can be well protected by applying improvised policies on edge devices like routers, web servers, firewalls etc. Our simulation result shows that policy inspection success rate becomes very high and the packets were dropped and even reached to maximum level. Further work is needed to investigate high level of monitoring is required for knowing attack categories their signatures and there is a great need to develop more efficient rules or policies which can be implemented on edge devices to counter maximum types of attacks with higher success rate and efficiency.

11. References

- Gu-Hsin Lai,"**A Light-weight Penetration Test Tool for IPv6 Threats** ",10th International Conference on Intelligent information Hiding and Multimedia Signal Processing, taiwan,2014

- Satwinder Singh, Abhinav Bhandri, "**Review of PPM, a Trceback Technique for Defending Against DDoS Attacks**", International Journal of Engineering Trends and Technology (IJETT)- volume 4 June 2013

- Harshita, N. Ramesh, "**A Survey of different types of Security threats and its counter measures**", International Conference on Electrical, Electronics and Computer Engineering, Mysore. May 2013.

- Frederic Beck, Olivier Festor, Isabelle Chrisment , Ralph Droms, "**Automated and secure IPv6 Configuration in Enterprise Networks**",CNSM,2010.

- Cynthia E. Martin , "**Internet Protocol Version 6(IPv6) Protocol Security Assessment**", IEEE ,2007

- Source: Computer weekly.com