Simulation of DOS, DDOS attacks & Design Test its Countermeasures

Aditi Srivastava
IET, Alwar (M.Tech, CSE Student)
ads.softech11@gmail.com

Deepak Chaudhary
IET, Alwar (Astt Professor)
deepak.se17@gmail.com

Abstract— Nowadays every organization uses an information system to maintain data and a web based network to make it available to its departments and outside customers. Various techniques have been developed to secure these systems and networks. Amongst various online attacks obstruct IT security, Denial of Service (DoS) has the most disastrous effects. It has also put immense pressure over the security experts lately, in bringing out productive defense solutions. These attacks could be implemented with diverse number of code and type. DDoS attacks are one of the crest security problems which is heavily affecting networks and damaging services to legitimate users. The indispensable step in dealing with DDOS attack is the network's ability to find out such attacks.

A network can be secured only if we know that in how many ways it can be attacked. This is done by network administrator as well as attacker for their prospective concern to keep track of the security vulnerabilities of the network. The aim of this paper is to check vulnerabilities status of a network and after knowing that apply DOS, DDOS attack, Verify these attacks and then apply countermeasures to prevent them.

Keywords- Vulnerebility,Denial of service attack,Distributed Denial of service attack, Network Design, VM Ware

1. Introduction

Information gathering is done to check whether the network is safe or not, is it being used by a system or network administrator and also by the attacker to analyze the server or a host.

A **port scanner** is application software designed to analyze a server or various host for finding open ports. This is generally used by network administrators to examine and verify security policies of their networks and also by the attackers to determine various running services on a host or server to compromise. A **port scan** is needed because it is an attack which sends client requests to a target server port addresses on a host, its aim is to find an active port and exploiting a known vulnerability of that service. Port scanning is done for passive attack to collect all possible information about the alive hosts.

Once information gathering, discovery and enumeration have been completed next step is to investigate the vulnerabilities that may exist in the target system. This could compromise the security of target and violate the confidentiality and integrity of a system.

Vulnerability comes into picture when there is any flaw in the logic, design or implementation of the system. It causes an unexpected and undesirable event which can execute damaging instructions to the system

We have designed a network using virtualization on VM ware Server. The environment of this network is a web host environment in that a router/firewall is used to connect internal network by using internal switch. A public switch is used for outer environment through which outside user will connect. We have taken various open source information gathering tools to scan this network which is designed with high security policy. We have taken various tools of both O.S. Environment Linux as well as windows. Backtrack is the best suitable platform for penetration testing by which a network administrator will easily test the network.
This Work is divided into five parts. The first part is enclosed with Introduction of work. In the second part background of DOS, DDOS and vulnerability Scanner tools has given. The third part includes creation of Web hosting network scenario using virtualization. In the fourth part scanning result of vulnerability tools is shown. In the fifth part denial of service attack, distributed denial of service attack has launched, verification is done and at last for prevention of these attack countermeasures has been given.

2. Background of Denial of service, Distributed denial of service and Vulnerability scanner tools

2.1 Denial of service

DoS attack is most affected attack among various attacks. It requires very less effort in implementation. It is also very tough to make a system which will be fully free from DoS attack. As they pose significant damage to the system, DoS attacks always capture special attention of security personals. In this attack, attacker overburdens the system lots of requests so prevent authorized people from accessing the server. Figure 2.1 demonstrates it very well.

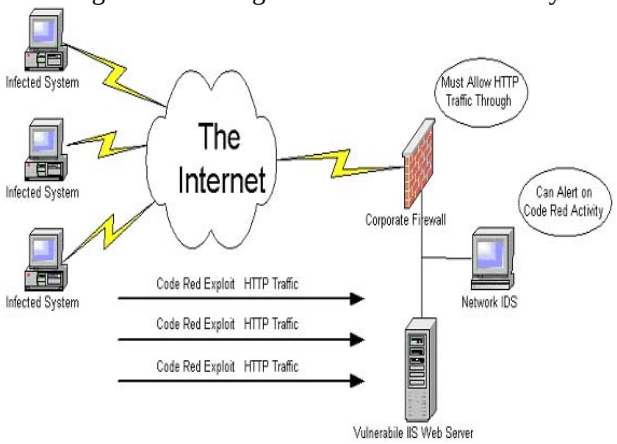


Figure 2.1 Denial of Service scenarios

2.2 Distributed denial of service

Now a day's every system and local network is having the information distributed over internet and that's why they are more prone to Distributed Denial of Service (DDoS) attacks.
A Distributed Denial of Service (DDoS) attack starts from exploiting the vulnerability of one system which becomes botmaster then it is used for affecting other systems further. Attacker overburdens the service by using all the bandwidth of the network and in some cases by making bogus application calls. Sending bogus requests continuously causes denial of service. It seems that only one system is getting affected by this but in reality many systems would be getting affected which are controlled by the botmaster.

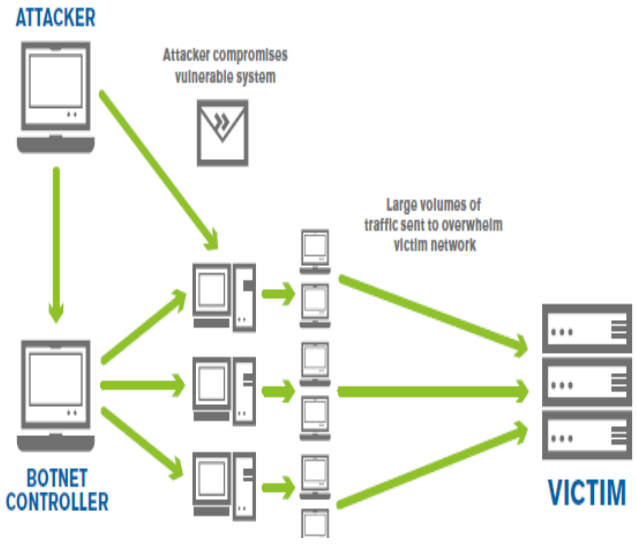


Figure 2.2 Typical DDOS Attack Environment

2.3 Nikto: -

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for diverse items, including over 6500 potentially hazardous files/CGIs, checks for feudal versions of over 1250 servers, and version distinct problems on over 270 servers. It also audit for server configuration items such as the presence of multiple index files, HTTP server options, and will pursuit to identify installed web servers and software. Scan items and plug-in are frequently updated and can be automatically updated.

2.4 Nessus: -

The Nessus vulnerability scanner provides patch, configuration, and compliance auditing; mobile, botnet discovery; malware, and sensitive data identification.
Nessus is a great tool. It is designed to automate the testing and discovery of known security problems. Generally by a hacker group, a security company, or a research scholar who wants to discover a specific way to breach the security of a software product. The discovery may be fortuitous or through directed research; the vulnerability, in numerous levels of detail, is then released to the security community. Nessus is designed to help, determine and solve these known problems, before any intruder takes advantage of them. Nessus is a tool with lots of capabilities.
One of the very powerful features of Nessus is its client server technology. Servers can be placed at distinct strategic points on a network allowing tests to be conducted from various points of view. An essential client or multiple distributed clients can control all the servers.

2.5 LanGuard:-

GFI LanGuard gives us the power to identify and correct any threats before any hackers can exploit them. GFI LanGuard scans devices, identifies and categorizes security vulnerabilities, and also recommends a course of action, gives us the tools to solve the problem.
It comes with a graphic threat level indicator – a perspective, weighted judgment of the vulnerability status of a scanned device or group of devices. Wherever achievable, a web link or more information on a particular security issue is provided such as a BugTrak ID or a Microsoft Knowledge Base article ID.
This is continually kept up-to-date with information about newly released Microsoft security updates as well as new vulnerability checks issued by using GFI and other community-based information repositories like OVAL database.

3. Webhost network scenario:-

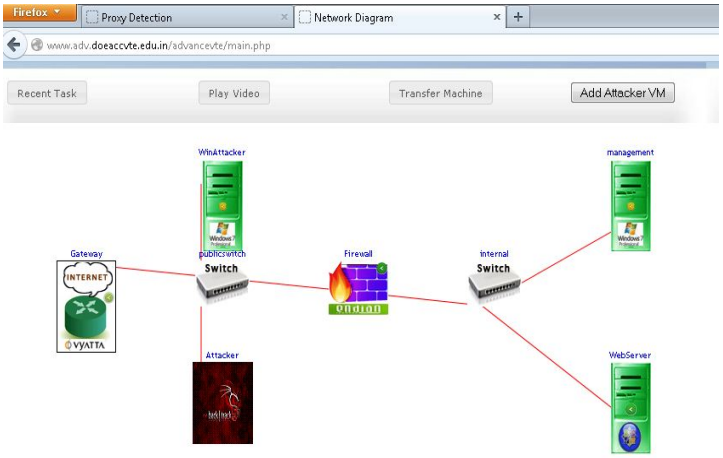


Figure 3.1 Web host Network

This is the network created similar to any webhosting network through virtualization on VMWARE server. A router/Firewall is used to connect any organization to outside network or internet. Endian firewall is taken for this network. Two switches has been used, one as a public switch and another as a internal switch. Organization server and management server is connected to this switch. A public switch is taken for the connection of other users. Gateway works as an ISP in Scenario; this provides Internet connection to organization and users. This scenario is created by using Advance VTE Lab.

Virtual Training Environment (VTE) is one way of amplifying the security training and best practices that have been developed and delivering the same through classroom training. The Virtual Training Environment (VTE) is a Web-based knowledge library for Information Assurance, computer forensics and incident response, and other IT-related topics.

4. Scanning result Snapshot of Vulnerability tools:-

4.1 Nikto

From the attacker machine attacker is trying to check the level of vulnerability by using nikto .For doing this open the console of attacker machine and type. **/nikto -h 10.0.1.1** Here 10.0.1.1 is the ip address of target.

The scan result is shown below

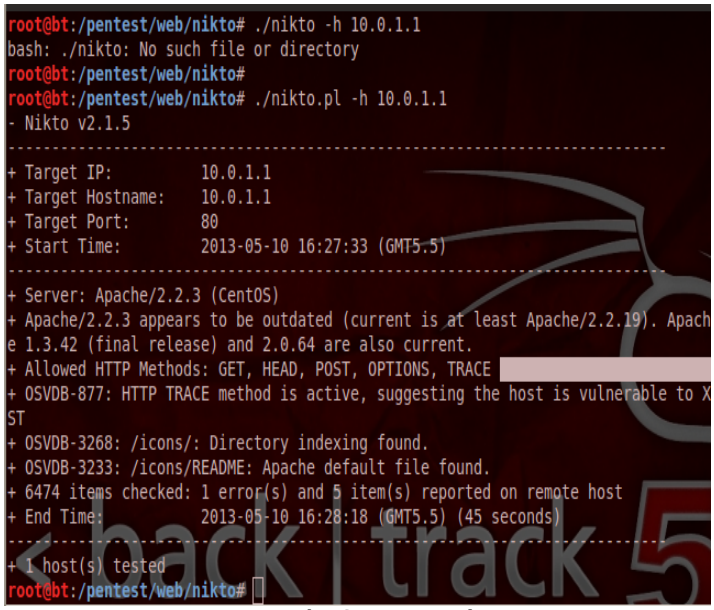


Figure 4.1Nikto Scanning Result

4.2 Nessus:- Another vulnerability scanner is used to discover more information about the vulnerability level of the server.

Nessus Scanning Process is illustrated below:-

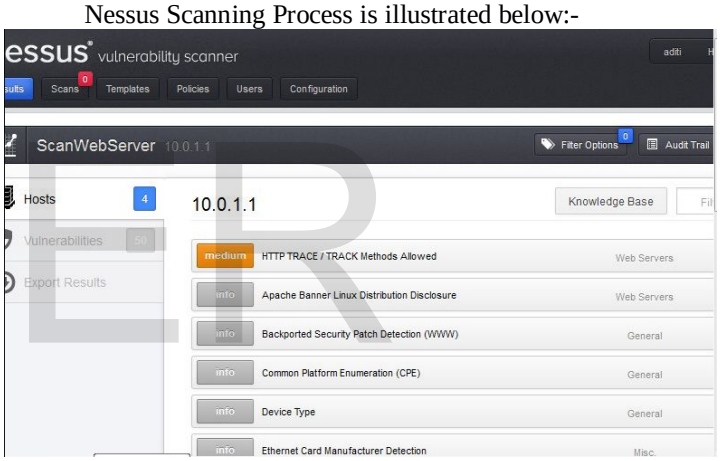


Figure 4.2(a) Nessus Scanning Result

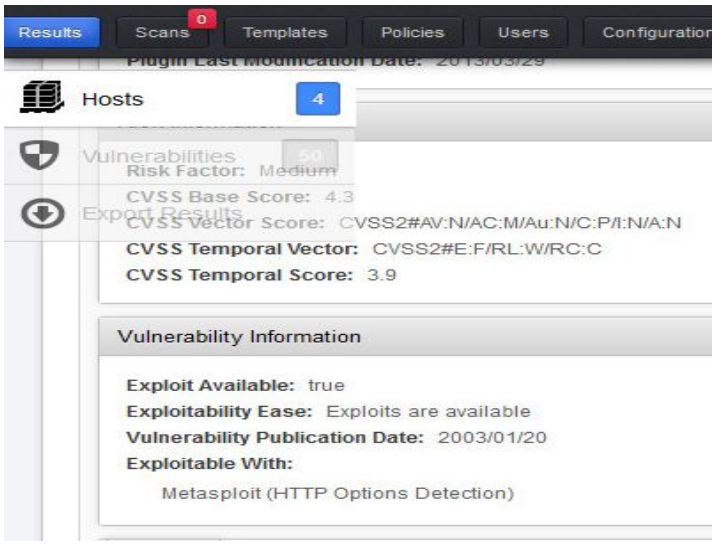


Figure 4.2(b)Nessus Scanning Result

4.3 LanGuard: - This software is also used for assessment of vulnerability level. From the win attacker machine

it can be launched because it only supports window environment.

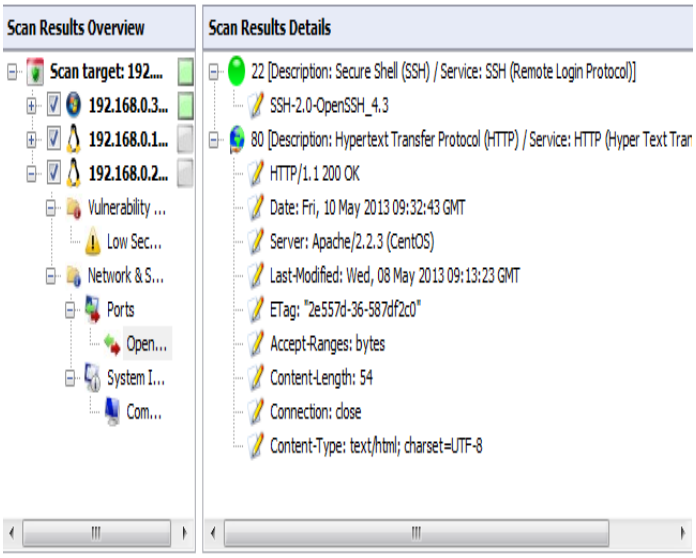


Figure 4.3(a)LanGaurd Scanning Result

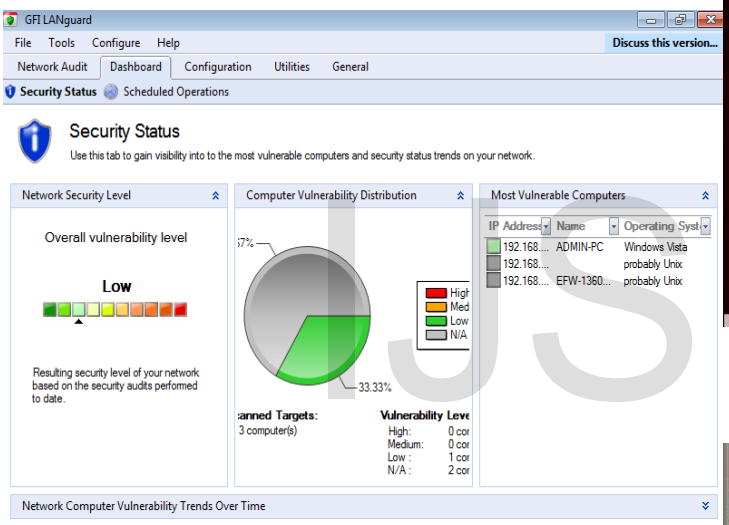


Figure 4.3(b)LanGaurd Scanning Result

5. DOS & DDOS ATTACK AND DETECTION

Step1:- Before launching the DOS attack on the particular site we confirm that site opening smoothly. Open Internet Explorer and type the URL of the website i.e. http://10.0.1.1/
The website is simply open like this.

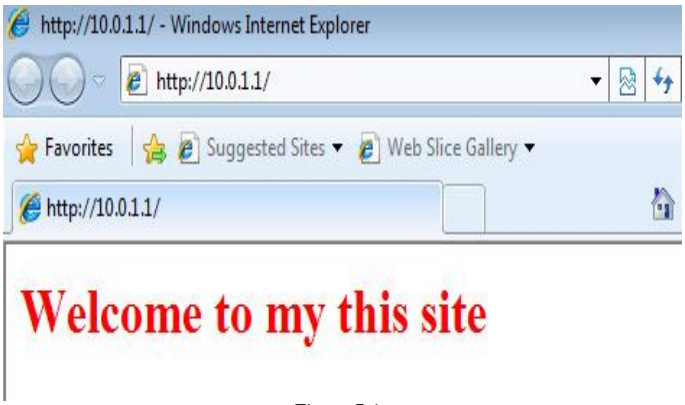


Figure 5.1

Step 2:- Now we can launch the attack by using sloloris.pl script. For this open the console of attacker machine and type **. / sloloris.pl - dns 10.0.1.1**

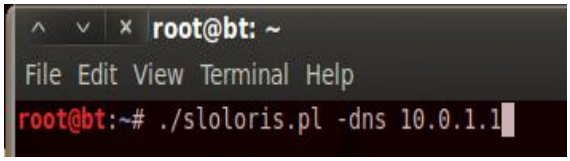


Figure 5.2

After pressing enter on this DOS attack has launched in this manner

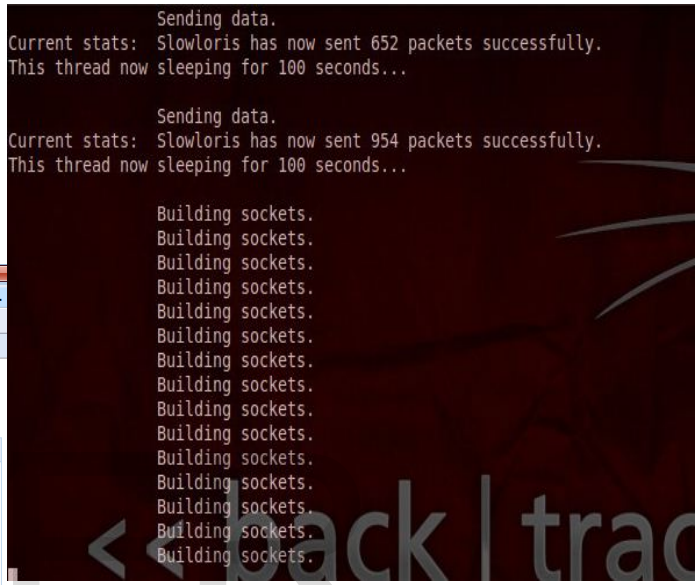


Figure 5.3(a)Slowloris Attack

Figure 5.3(b)Slowloris Attack

From the above screenshot we can see that within few seconds it has send thousands of packets to the target machine.

To check whether it effects or not again opens Internet Explorer and type the URL of the target.

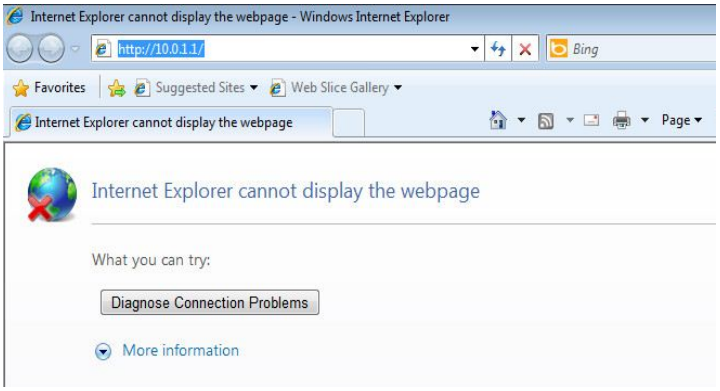


Figure 5.4 Varification of DOS Attack

We can see from the above Website is unable to open. So DOS Attack is working.

5.1 **Verification of DOS Attack:-**

5.1.1 **Verification from server terminal:-**

Attack detection part is done at administrator side on server machine whether it is a DOS attack or due to some other problem website is unable to open.

Go to the Web Server open the terminal and type the following command

```
[root@localhost ~]# netstat -ntap
```

This command works as follow:-

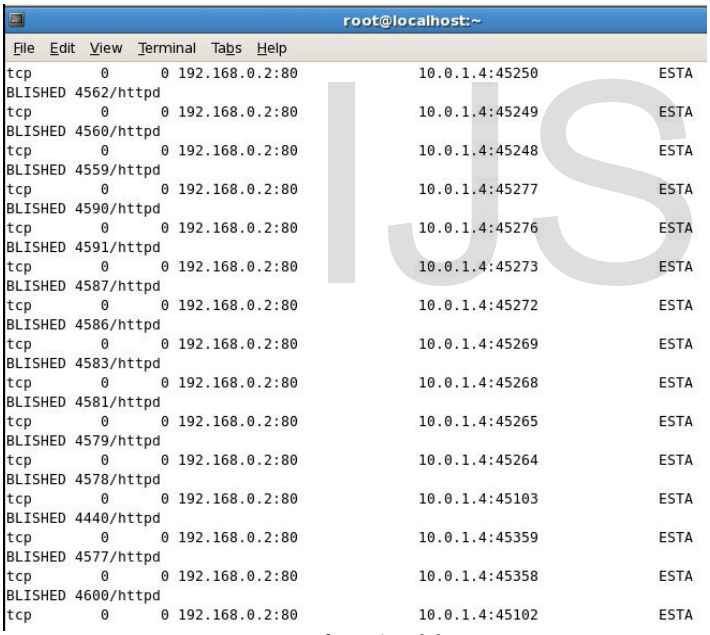


Figure 5.5 Detection of Dos Attack by server

From the above screenshot we saw that lot of connection opened by the single source ip and shown in the ESTABLISH Status.

5.1.2 **Detection from firewall:-**

Open the console goes to status and then connection, click on connection

Figure 6.6 Detection of Dos Attack by Firewall

We can easily detect that from only one ip address the connection has established. So from here we can verify Dos attack has launched on the website.

5.1.3 Design and Test Countermeasure for DOS attack:-

The administrator has to Harden the web server security policy weakness to prevent this attack. For doing this we are adding **Packet Filter rule** to limit the connection against the Web Server on port 80. Because this port is used for http request.

This rule is written for the website where we have limited the connection limit above 5. If more than 5 requests has encountered to the website it will drop the request by using the following command.

Open the console of server machine and type **iptables –I INPUT –p tcp --dport 80 -m connlimit -above 5 - - connlimit – mask 32 -j DROP**

```
[root@localhost ~]# iptables -I INPUT -p tcp --dport 80 -m connlimit --connlimit
-above 5 --connlimit-mask 32 -j DROP
```

After apply this rule website will be available

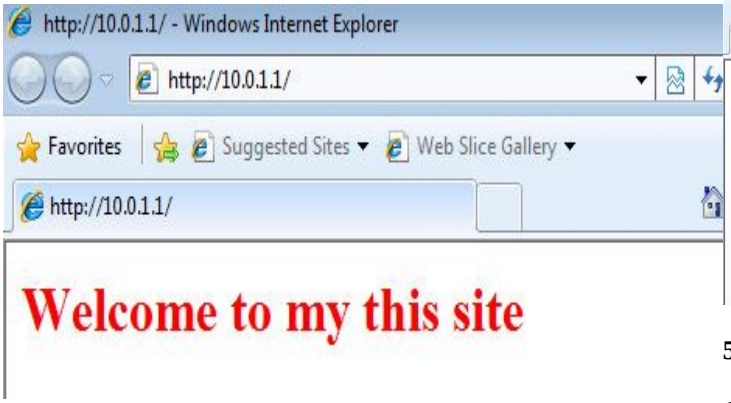


Figure 5.7

6.2 Launching DDOS attack:-

Before launching the DDOS first check whether the website is properly working or not.
For this open internet Explorer type the URL http://10.0.1.1/

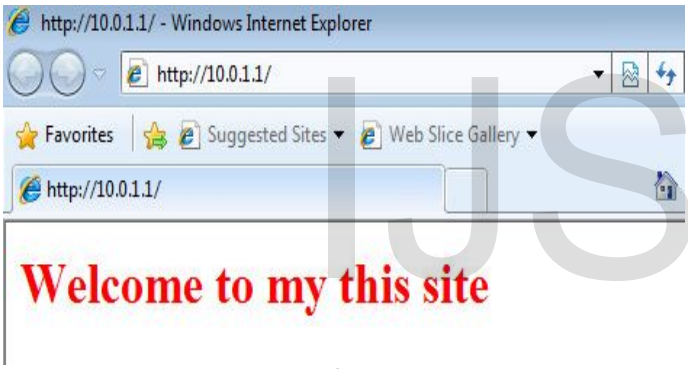


Figure 5.8

DDOS attack is launched by using hping command. Open the terminal and type

hping3 - - flood - - rand – source - s 1234 -k -s -p 80 10.0.1.1

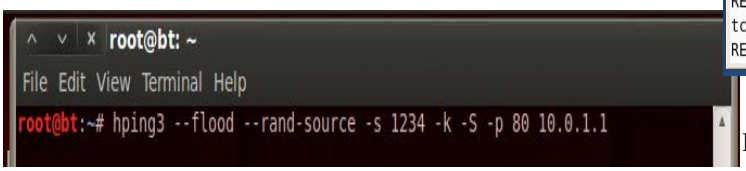


Figure 5.8(a) Launching DDOS by hping Command

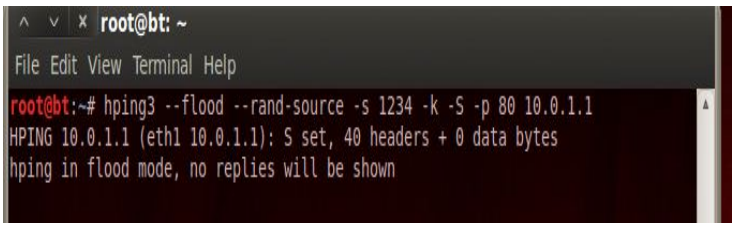
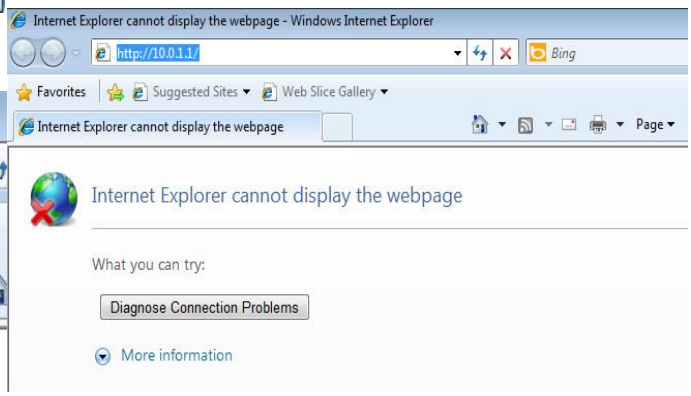


Figure 6.8(b) Launching DDOS by hping Command

To check whether it effects or not again opens Internet Explorer and type the URL of the target.



5.2.1Detection of DDOS Attack:-

Go to the Web Server open the terminal and type the following command

```
[root@localhost ~]# netstat
```

After entering this command this screen will appear.

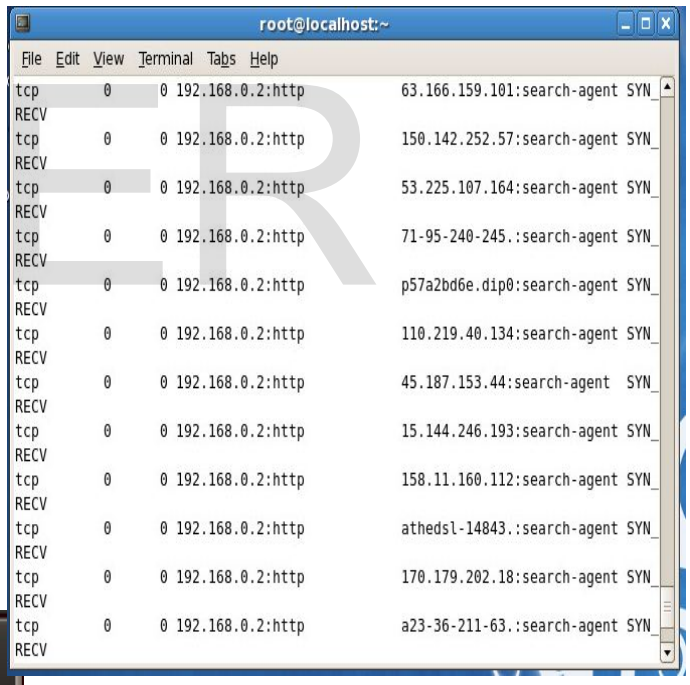


Figure 5.9 Detection phase of DDOS Attack

From the above figure we can see that from one ip address SYN packet is generated so this is the condition for DDOS attack.

5.2.2 Countermeasure for DDOS attack

Distributed attack tools influence bandwidth from multiple systems on multiple networks to produce very robust denial of service attacks. To a victim, an attack may appear to come from many distant source addresses, whether or not IP source address spoofing is employed by the attacker. According to CERT some basic recommendation they have made regarding distributed denial of service attacks:

- **Prevention to install distributed attack tools on the systems**

  Remain current with security-related patches to operating systems and applications software. We have to follow security best-practices when administrating the network and systems.

- **Monitor the network for signatures of distributed attack tools**

  Many Sites using intrusion detection systems (IDS) may wish to establish patterns to look for that might indicate trinoo or TFN activity based on the communications between master and daemon portions of the tools. Those sites who use pro-active network scanning may wish to include tests for installed daemons and/or masters when scanning systems on any network.

- **If we find a distributed attack tool on the systems**

  It is important to determine the role of the tools installed on the system. The piece we find may provide information that is useful in locating and disabling other parts of distributed attack networks.

6. Conclusion: - Denial of service attack and distributed denial of service attack are most disastrous and heavily found attack in any one's life. This work is done as a network administrator to know which kind of attack has launched on the network. Detection of denial of service attack has been tested by server as well as firewall both. After detection of any attack we can't secure our network. For doing that some prevention is required either manually or automatically. So to prevent denial of service attack **ip packet filter rule** has applied. For DDOS attack some manually prevention has been taken to prevent from these attacks.

No any exact solution available to prevent the DDOS but we consult to our ISP to decrease this type of activity to minimize the effect of DDOS in network, and about slowloris require to well hardening of APACHE web server to reduce and prevent this attacks

7. Acknowledgment:- This work is supported in part by the NIELIT Gorakhpur centre.

8. References

1. Advanced DDoS Attacks Traffic Simulation with a Test Center Platform By Jie Wang, Raphael C.-W. Phan, John N. Whitley and David J. Parish, High Speed Networks Research Group

2. Mitigation and traceback countermeasures for DDoS attacks by Basheer Nayef Al-Duwairi.

3. Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures By Stephen M. Specht, Ruby B. Lee Princeton University.

4. Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis by Subramani rao Sridhar rao , SANS Institute InfoSec Reading Room

5. "A Chronology of CERT Coordination Center Involvement with Distributed Denial-of-Service Tools,"

6. Steve Gibson, "Distributed Reflection Denial of Service Description and Analysis of a Potent, Increasingly Prevalent, and Worrisome Internet Attack," February 2002.

7. E. Cole. *Hackers Beware*. Indianapolis, In: New Riders,,2002.

8. A. Ma. Using Spirent Test enter to Generate Real-WorldTraffic. White paper, Spirent Communications Ltd. Jan 2008.

9. Alok Tripathi, Abhinav Mishra 'workshop on Information Security in Virtual Training Environment' IT Division,DOEACC Society, Gorakhpur Centre Gorakhpur, India.

10. Carl, C., Kesidis, G., Brooks, R.R., and Suresh Rai. (2006, January). Denial-of-Service Attack-Detection Techniques. IEEE Internet Computing, 10(1), 82-89.

11. Cotroneo, D., Peluso, L., Romano, S.P. and Ventre, G. An active security protocol against DoSattacks.Computers and Communications, 2002. Proceedings. ISCC 2002. Seventh International Symposium on Computers and Communications, vol., no., pp. 496-501, 2002

12. Haggerty, J., Shi, Q. and Merabti, M. (2002). Beyond the Perimeter: the Need for Early Detection of Denial of Service Attacks. In Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC '02). IEEE Computer Society, Washington, DC, USA, 413-423.

IJSER