International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2014): 3.05

Use of Honeypot and IP Tracing Mechanism for Prevention of DDOS Attack

Shantanu Shukla[1], Sonal Sinha[2]

[1]Pranveer Singh Institute of Technology, Kanpur, Uttar Pradesh, India

[2]Assistant Professor, Pranveer Singh Institute of Technology, Kanpur, Uttar Pradesh, India

Abstract: ***A DDoS attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet. Everybody has been hacked one way or another when dealing with computers. DDoS attackers hijack secondary victim systems using them to wage a coordinated large-scale attack against primary victim systems. These attacks are not easily detected. One of the main difficulties in the detection and prevention of Distributed Denial of Service (DDoS) attacks is that the incoming packets cannot be traced back to the source of the attack, because (typically) they contain invalid or spoofed source IP address. For that reason, a victim system cannot determine whether an incoming packet is part of a DDoS attack or belongs to a legitimate user. Various methods have been proposed to solve the problem of IP traceback for large packet flows. As new approach is developed to prevent DDoS attacks, attackers are constantly developing new methods to attack the system. In this paper we describe prevention mechanism of HoneyBOT software to find the intruder IP and trace the IP. Those IP we have prevent via advanced firewall rules in duration of attacking. These approaches illustrate similarities and patterns in different DDoS prevention mechanism, to assist in the development of more generalized solutions to DDoS solution.***

Keyword: DoS, DDoS, IP Tracing, Honeypot, HoneyBOT, Firewall

1. Introduction:

1.1 Denial of service (DoS)

As organizations continue to incorporate the Internet as a key component of their operations, the global cyber-threat level is increasing. One of the most common types of cyber-threats to these environments is known as a Denial of Service (DoS) attack – an attack preventing users from accessing a system for a period of time. [1]. An interruption is an unauthorized user's access to a computer network, typically one caused with malicious intent. The loss of service is the inability of a particular network service. Such as Email to be available of the temporary loss of all network connectivity and services. A denial of Service attack can also destroy programming and files in affected computer system.

1.2 Distributed denial of service(DDoS)

Distributed denial-of-service (DDoS) is a rapidly growing problem. The multitude and variety of both the attacks and the defense approaches is overwhelming. Distributed Denial of Service (DDoS), is a relatively simple, yet very powerful technique to attack Internet resources.[2]

In a DDoS attack, because the aggregation of the attacking traffic can be tremendous compared to the victim's resource, the attack can force the victim to significantly downgrade its service performance or even stop delivering any service. Compared with conventional DoS attacks that could be addressed by better securing service systems or prohibiting unauthorized remote or local access, DDoS attacks are more complex and harder to prevent. Since many unwitting hosts are involved in DDoS attacks, it is challenging to distinguish the attacking hosts and take reaction against them.

A DDoS attack is an attempt to make an online service unavailable by overwhelming from multiple sources. DDoS is a type of DoS attack where multiple compromised systems which are usually infected with a Trojan are used to target a single causing a DoS attack. In a DDoS attack, the incoming traffic flooding the victim originates from many different sources potentially hundreds of thousand or more.

2. DDoS Attack Architectures:

Two types of DDoS attack networks have emerged: [3]
1. Agent-Handler model
2. Internet Relay Chat (IRC)-based model.

Agent handler model

The agent handler is often used for unleashing DDoS attack . It consists of client's handlers and agent. The attacker of client's platform to communicate with other DDoS attack networks. The handlers are software packages that the attacker uses for the purpose of communicating indirectly with the agents. An agent needed only a small number of resources Therefore there is a minute effect on a compromise system performance. The process on communication between attackers and handlers and between handler and agent can be through TCP, UDP, and ICMP. While describing the DDoS tools, the terms master and daemon are often needed for handler and agent respectively.[4]

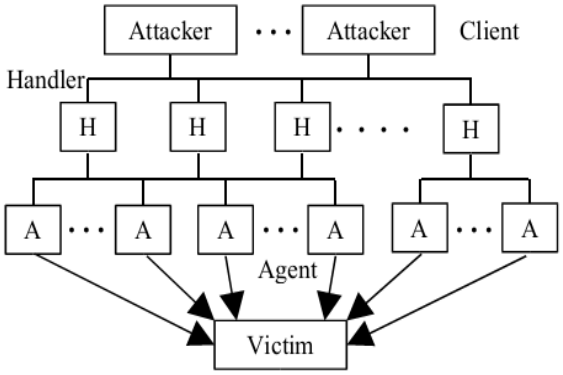

Figure 1: DDoS Agent Handler Model

Internet relay chart based model

IRC(Internet Relay chat) is a multiuser online chatting system consisting of a network of servers located throughout the Internet. The channel in this network architecture makes communication across the internet possible. Users can create public, private and secret channel. Public channels enable chat and share files and messages. An IRC based DDoS attack network is just like the agent handler DDoS attack model. The difference is that it is installed on a network server instead of using handler program. It makes use of IRC communication channel to connect the attacker to the agent. [4]

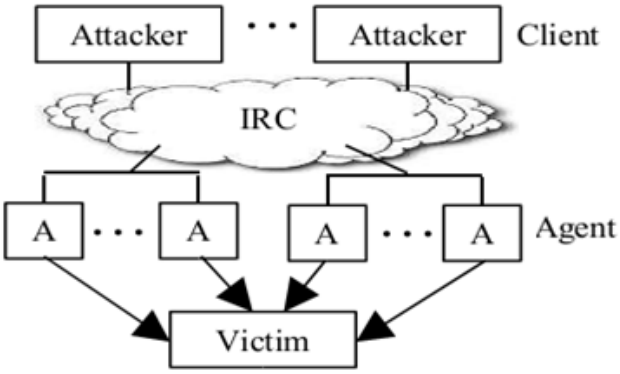

Figure 2: DDoS IRC based model

3. Problem Statement

We have read many prevention mechanisms. A honeypot is a faked vulnerable system used for the purpose of being attacked, probed, exploited and compromised. But difficulty is that how to create honeypot? How can trace the IP of incoming packet and prevention mechanism from them? And what are honeyBOT related with firewall and how can prevent the DDoS attack? That's problem statement to clarify and provide optimize solution in this paper.

4. Proposed solution

We have prevent the DDoS attack in many Technique. Honeypot is one of them. A **honeypot** is a trap set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of a computer, data, or a network site that appears to be part of a network, but it is actually isolated and monitored, and which seems to contain information or a resource of value to attackers. These are different defense mechanism as shown in Figure. We have chosen the intrusion prevention technique like honeypot. In honeypot we have trace the primary victim IP of incoming packet. .So we have provide the solution throw honeypot like HoneyBOT solution and IP tracing .HoneyBOT is the type of honeypot. In IP tracing to trace the IP packets where is it come from. If any packet with contain the same IP then we have block the malicious IP address through firewall and use advanced security firewall.

4.1 Honeypot

A honeypot is an "an information system resource whose value lies in unauthorized or illicit use of that resources"[5]. A more practical, but more limiting, definition is given by pcmag.com: "A server that is configured to detect an intruder by mirroring a real production system." A honeypot is a security resource, whose value lies in being probed, Attacked, or compromised. There are two general types of honeypots: Production honeypots are easy to use, capture only limited information, and are used primarily by companies or corporations; and Research honeypots are complex to deploy and maintain, capture extensive information, and are used primarily by research, military, or government organizations.[6]. Honeypot is a device placed on a computer network specifically designed to capture malicious network traffic. The logging capability of a honeypot is far greater than any other network security tool and captures raw packet level data even including the keystrokes and mistakes made by hackers. The captured information is highly valuable as it contains only malicious traffic with little to no false positives. Honeypots are becoming one of the leading security tools used to monitor the latest tricks and exploits of hackers by recording their every move so that the security community can more quickly respond to new exploits.

DDoS Defense Technique

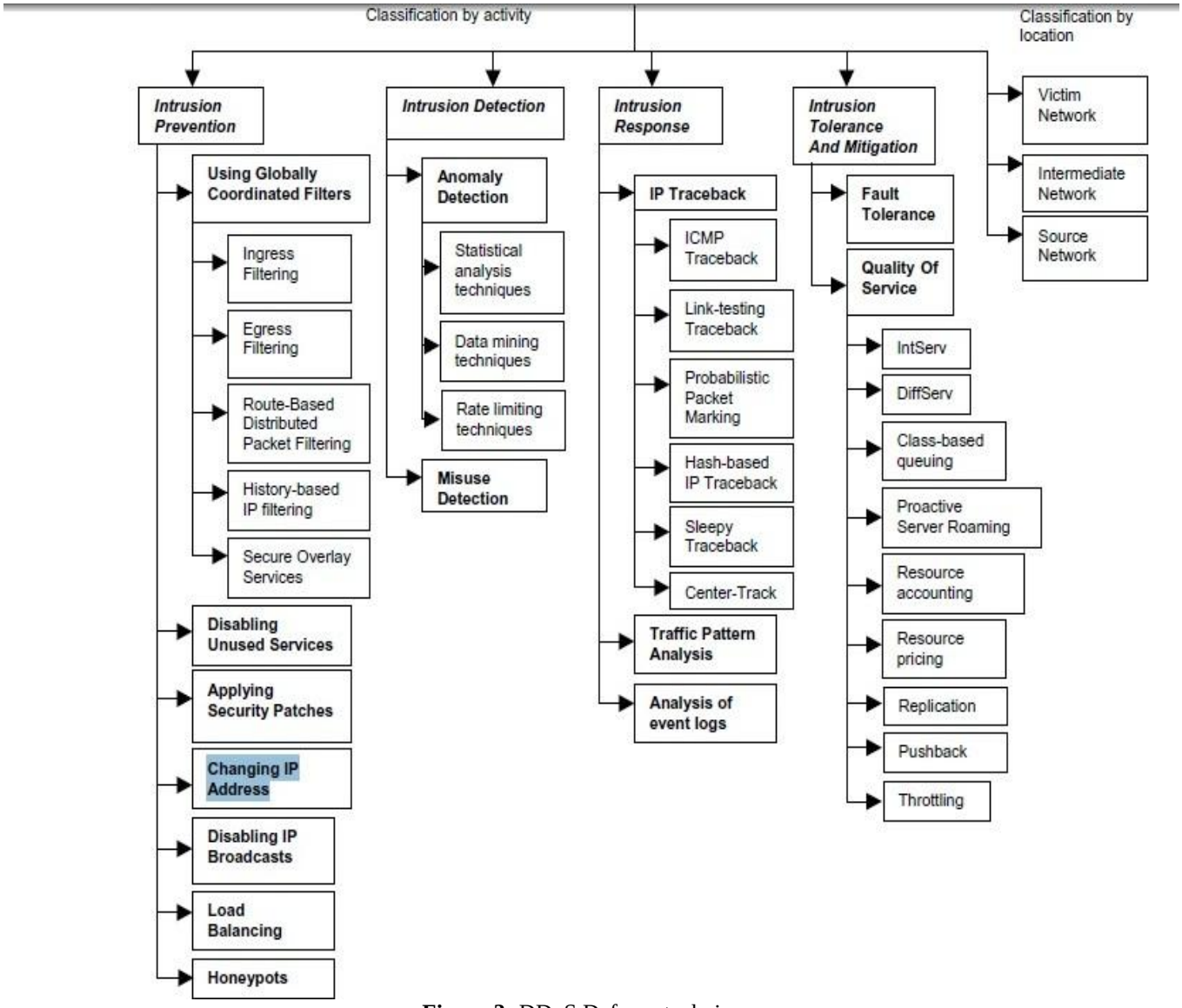

Figure 3: DDoS Defense technique

4.2 Existing Honeypot Products: [8]

In this section, we provide a very brief survey of the Honeyd, HoneyBOT, and Specter Honeypots.

.

Honeyd: Honeyd is a honeypot for Linux/Unix developed by security researcher Niels Provos. Honeyd was ground-breaking in that it could create multiple virtual hosts on the network (as opposed to just using a single physical host). The honeypot can emulate various operating systems (which differ in how they respond to certain messages) and services. Since Honeyd emulates operating systems at the TCP/IP stack level, it can fool even sophistic network analysis tools such as nmap.

HoneyBOT: HoneyBOT is a Windows medium-interaction honeypot .It originally began as an attempt to detect by the Code Red and Nimda worms in 2001 and has been released for free public use since 2005. HoneyBOT allows attackers to upload files to a quarantined area in order to detect trojans and rootkits.

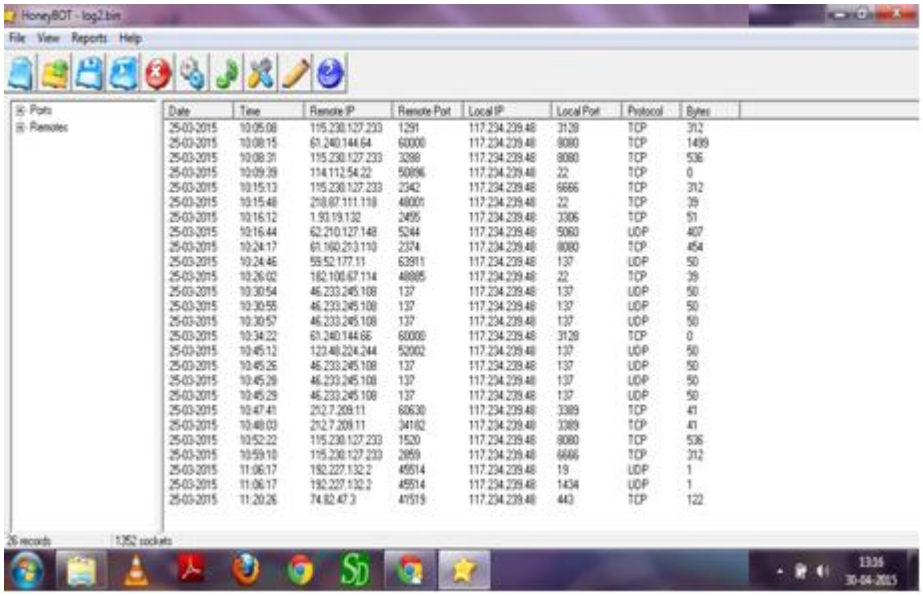

Figure 4: Snapshot of HoneyBOT User Interface

Specter : Specter's authors describes Specter as a "honeypot-based intrusion detection system". However, the product is primarily a honeypot designed to lure attackers away from production systems and collect evidence against the attackers. Specter actively attempts to collect information about each attacker. Here we discuss only HoneyBOT software to provide the IP of intruder and malicious attacker.

4.3 IP Tracing

IP traceback is a name given to any method for reliably determining the origin of a packet on the Internet. [5] IP tracing methods can be classified into two categories preventive and reactive. Precautionary steps can be taken by the preventive method for DoS and DDoS attack prevention. The goal of the reactive methods is to identify the source of attacks, for that these method provides the wide range of solutions. The reactive methods are more efficient to identify the source even the attacker spoofs their addresses. [7].

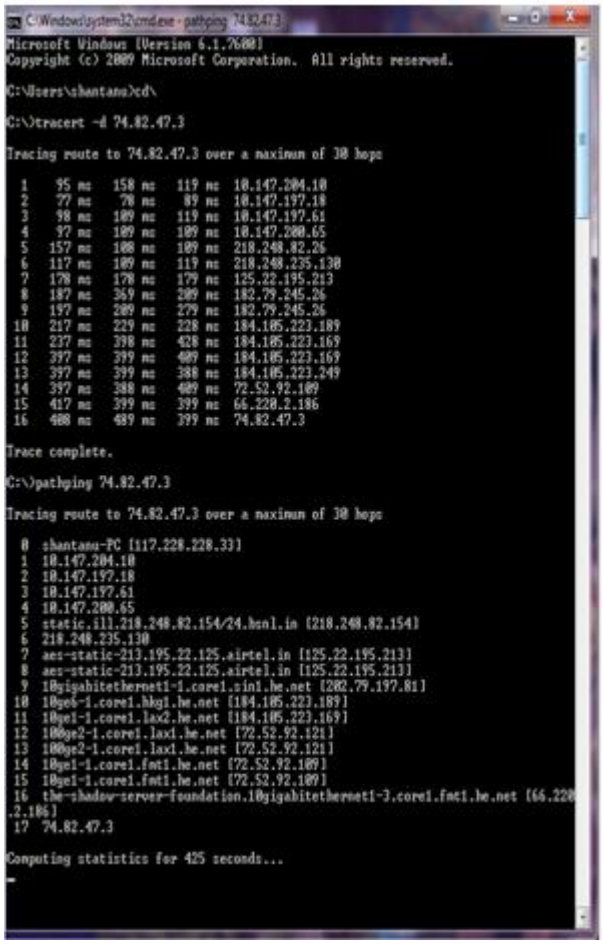

Figure 5: IP tracing detect via command prompt tool

To trace the IP we can use the online tools or IP tracer software. We have also used command prompt for tracing the ip and origin of packet. In that scenario we used command "pathping" and "tracert". If you want tracert command to resolve and display the names of all routers in the path use the –d parameter. This expedites the display of the path. For ex. Tracert –d www.facebook.com.

4.4 Firewall

In computing, a firewall is a network security system that controls the incoming and outgoing network traffic based on an applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is assumed not to be secure and trusted[9]. Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions[10]

Types of firewall

1. Network layer or packet filtering
2. Application layer
3. Proxies
4. Network address translation

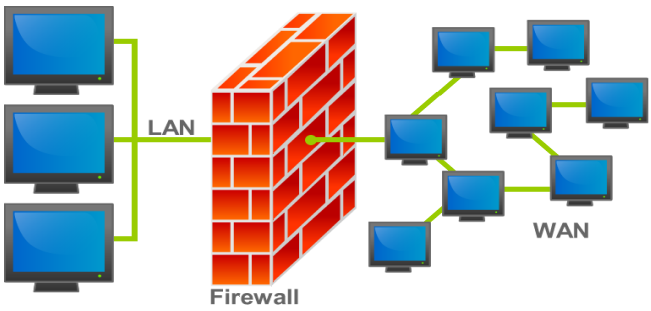

Figure 6: Diagram of Firewall

What Firewalls Do

Firewalls can protect your computer and your personal information from:

1. Hackers breaking into your system
2. Viruses and worms that spread across the Internet
3. Outgoing traffic from your computer created by a virus infection

To protect unauthorised access and malware we use Firewall. After using the IP tracing and honeybot we find some illegal IP to attack our server. Then we have use the firewall to prevent from them. To stopping these illegal activities we have provide more secure firewall such as proxy firewall. To provide the solution we have 8 basic steps to more secure the firewall.[11]

1. Enable Auto Updates for the Firewall.
2. Keeping setting consistent across network.
3. Tweaking the setting to your usage.
4. Add multiple layers to your pc and security system.
5. Use strong password.
6. A 128-bit encryption on your wireless network.
7. We use the proxy firewall
8. Change the setting as own specification

Sometimes we have blocked the IP which are repeated to attack my system. Then we provide some more secure option and establish advanced security. We establish advanced security firewall and create a new rules provide by the windows operating system like inbound and outbound rules. To create a Strong Firewall Security policy some specific points in our mind.

1. Using the firewall Rule Base.
2. Creating a Secure Firewall Rule Base
3. Defining Security Zones
4. Preventing IP Spoofing
5. Analyzing the rule base hit count.

5. Conclusion

In this paper, we tried to achieve a clear view of the DDoS prevent technique and the defense solutions that have been proposed. HoneyBOT is medium interaction open source software that provides those IP which have attack to my system .And after attacking we try to known the behaviour of those IP and tracking them to find the location. To prevent our system we have use the some specific technique and advanced technology of windows firewall system.

Reference

[1] Darshan lal meena, Dr. R.S. Jordan IJARCS Journal 2014 volume 2 issue 4 in “Distributed Denial of Service Attacks and Their Suggested Defense Remedial Approaches”
[2] Christos Douligeris , Aikaterini Mitrokotsa (October 2003) www.elsevier.com in topic DDoS attacks and defense mechanisms: classification and state-of-the- art.
[3] Sonal Sinha ,Madhulika Sharma IJETTCS journal 2014 in “ Simulation and analysis of DDoS attack by simulator using virtualization”
[4] Ethical Hacking and Countermeasures: Threats and Defense Mechanisms
[5] By EC-Council.
[6] PC- MAG honeypot Definition - PC Magazine. pcmag.com. 24 March 2009.http://www.pcmag.com/encyclopedia_term/0,2542,t=honeypot&i=44335,00.asp PC Magazine's encyclopaedia entry for honeypot.
[7] Ralph Edward Sutton DTEC 6783 Section 1 in paper “Build and use the honeypot”
[8] A johan, T.sivakumar “DDoS:Servey of Traceback Methods” International Journal of Recent Trends in engineering, Vol .1, No.2 May 2009.
[9] http://www.cse.wustl.edu/~jain/cse571-09/ftp/honey/index.html
[10] “A Practical Guide to Honeypots”
[11] Oppliger, Rolf (May 1997). "Internet Security: FIREWALLS and BEYOND". *Communications of the ACM* **40** (5): 94. doi:10.1145/253769.253802
[12] Definition of Firewall, Check Point Resources, "What is Firewall?" Retrieved 2015-02-12.
[13] http://www.itsecurity.com/features/more-secure-firewall-012207