

Honeypots: Approach and Implementation

Kumar Shridhar¹, Mayank Jain²

¹Department of Computer Science and Engineering, Bhagwan Parshuram Institute of Technology, Rohini, Delhi, India

²Department of Computer Science and Engineering, Bhagwan Parshuram Institute of Technology, Rohini, Delhi, India

Abstract: *Global communication is getting more important every day. At the same time, computer crimes are increasing. Countermeasures are developed to detect or prevent attacks - most of these measures are based on known facts, known attack patterns. By knowing attack strategies countermeasures can be improved and vulnerabilities can be fixed. Honeypot comes into play for such purposes. It is a resource, which is intended to be attacked and computerized to gain more information about the attacker, and used tools. Honeypots are closely monitored decoys that are employed in a network to study the trail of hackers and to alert network administrators of a possible intrusion. In this paper we present an overview of honeypots and provide a starting point for persons who are interested in this technology.*

Keywords: Honeypots, Network attack, N-Map, DMZ, Network Security

1. Introduction

Web applications are broadly deployed. More traditional services are extended to Internet. E-commerce and e-government has quickened up the process. At the same time, attacks and intrusions to the web application system become more popular. Hackers exploit more tricky and obscure methods. The traditional approach to security has been largely defensive so far, but interest is increasingly being paid to more aggressive forms of defense. One of these forms is decoy-based intrusion protection through the use of honeypots and/or honeynets.

It's necessary to put high priority to system security, minimize vulnerabilities and secure the computer system against intrusion. Today's standard of security is using specifically configured firewall in combination with the intrusion detection system (IDS). But using only IDS is not sufficient. We need to find out how attacker attacks actually so we will provide a security hole in system and will provide unimportant data in it. Attacker will attack in system, so that we can record all activities done by attacker that will help us to prevent actual data from these type of attackers, this technology is called as Honeypot. [1]

Since its introduction at the end of the 90's, honeypots have evolved in diverse directions to cope with various new security threats against not only security defenders but also novice users in the Internet today. The recent changes, including those in hardware, software and even user demography, have been rapid enough to require a new survey especially on the recent challenges to and evolutions in honeypots.

"HoneyNet" is a term that is frequently used where honeypots are concerned. A honeynet is simply a network that contains one or more honeypots. More precisely, it is a high-interaction honeypot that is designed to capture extensive information on threats and provides real systems, applications, and services for attackers to interact with [2].

This paper introduces honeypot and honeypot related technologies from the viewpoint of security management for

network. Basic concepts, types and its implementation technique are explained in further sections.

2. Related Work

Research in this area has resulted in a number of papers discussing specific topics concerning honeypots and how honeypots can be created and deployed [3]. It is difficult to find information from a single source that provides an overall picture of honeypots including their benefits, the concepts behind honeypots, the approach to using honeypots, and the challenges involved when implementing honeypots.

Several papers and projects have explored the technique of honeynets as an educational tool for IT students and academic institutions [4]. This research indicates that honeynets can be an effective tool in security education. A significant amount of work is available that details the benefits of honeypots.

Other papers go into some detail about prototype computer security lab and design of network security projects using Honeypots [5]. There are also papers that describe the strategy and tactics of how honeypots are used against insider threats [6]

A large amount of helpful information exists on the HoneyNet Project at [2]. This website documents lessons learned about security threats through the use of honeypots. While there is many research done on honeypot and its significance on modern day world there are few a papers focusing on algorithms for identifying intrusion detection by using Support Vector Machine(SVM).[1]

The purpose of this paper is to do a study of honeypots, and provide a reasonable understanding of its implementation for persons who are interested in this technology.

3. What is Honeypot?

In computer terminology, 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 is actually isolated and monitored, and which seems to contain information or a resource of value to attackers. This is similar to the police baiting a criminal and then conducting undercover surveillance [7].

Its primary purpose is not to be an ambush for the black hat community to catch them in action and to press charges against them. The focus lies on a silent collection of as much information as possible about their attack patterns, used programs, and the black hat community itself. All this information is used to learn more about the black hat proceedings and motives, as well as their technical knowledge and abilities. This is just a primary purpose of a honeypot. There are a lot other possibilities for a honeypot- divert hackers from productive systems or seize a hacker while conducting an attack are just two possible examples.

Honeypots can be classified based on their deployment and based on their level of involvement. Based on deployment, honeypots may be classified as:

Production honeypots are easy to use, capture only limited information, and are used primarily by companies or corporations. Production honeypots are placed inside the production network with other production servers by an organization to improve their overall state of security. Normally, production honeypots are low-interaction honeypots, which are easier to deploy. They give less information about the attacks or attackers than research honeypots do. Production honeypots tend to mirror the production network of the company (or specific services), inviting attackers to interact with them in order to expose current vulnerabilities of the network. Uncovering these vulnerabilities and alerting administrators of attacks can provide early warning of attacks and help reduce the risk of intrusion. The data provided by the honeypot can be used to build better defenses and counter measures against future threats [7] [8].

Research honeypots are run to gather information about the motives and tactics of the Blackhat community targeting different networks. These honeypots do not add direct value to a specific organization; instead, they are used to research the threats that organizations face and to learn how to better protect against those threats. Research honeypots are complex to deploy and maintain, capture extensive information, and are used primarily by research, military, or government organizations. Very little is contributed by a research honeypot to the direct security of an organization, although the lessons learned from one can be applied to improve attack prevention, detection, or response. They are typically used by organizations such as universities, governments, the military or large corporations interested in learning more about threats research[7][8].

4. Level of Interaction

A. Low Interaction Honeypots

On the basis of interaction low interaction honeypots doesn't provide Operating system access to the intruder .It provides

only services such as ftp ,http ,ssh etc. these low interaction honeypots plays the role of passive IDS where the network traffic is not modified. The well-known example of low interaction honeypot is Honeyd. Honeyd is a daemon and it is used to simulate large network on a single host. It provides a framework to create several virtual hosts using unused IP addresses of the network with help of ARP daemon For instance, several virtual number of operating systems, server, switches, routers, can be configured on a single host. Furthermore, emulated services include FTP service listening on port 21 (Telnet), login to FTP server etc. Other low interaction honeypot is specter and kFsensor. Specter can monitor total of 14 Tcp ports. Out of these fourteen ports seven ports are called traps and seven are called services. Traps act as a listener of ports i.e. when attacker makes connection with these ports the attempt is terminated and then logged. Services are more advanced wherever there is interaction between attacker and emulating services [9].

B. High Interaction Honeypots

These are the most sophisticated honeypots .These are difficult to design and implementation. These honeypots are very time consuming to develop and have highest risks involved with this as they involve actual OS with them .In high Interaction Honeypots nothing is simulated or restricted. Some example of High interaction honeypots are Sebek, Argos. As these honeypots involves real operating system the level of risk is increased by many extents, but to capture large amount of information by allowing an attacker to interact with the real operating system, it is a kind of trade off. This helps in capturing and logging of attacker's behavior that can be analyzed in later stage. [9]

5. Proposed Framework

Honeypots are closely monitored decoys that are employed in a network to study the trail of hackers and to alert network administrators of a possible intrusion. [10]

A more practical definition is given by pcmag.com:

"A server that is configured to detect an intruder by mirroring a real production system. It appears as an ordinary server doing work, but all the data and transactions are phony. Located either in or outside the firewall, the honeypot is used to learn about an intruder's techniques as well as determine vulnerabilities in the real system"[11]

5.1 How do we use honeypots?

Honeypots are used to know the system users or attackers better. A typical web server may get millions of hits every day. So it gets quite difficult to identify the attackers from the users. So we put honeypots in our same network system. Honeypots are just used to lure the attackers. If we get hits on our honeypots we can distinguish the attacker from the users.

As honeypots have no legitimate uses we trace back the attacker and improve our network security.

5.2 Where to put honeypots?

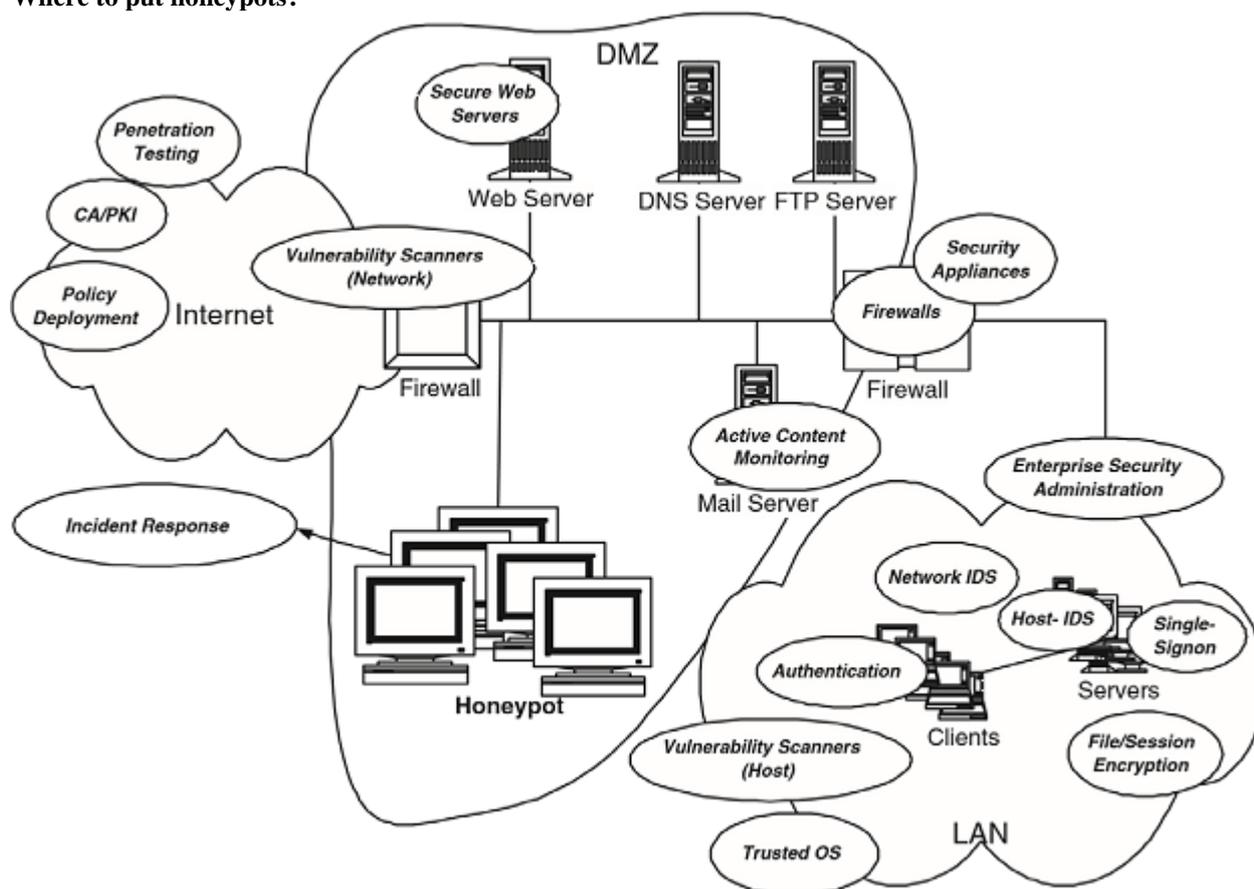


Figure 1: Implementation of Honeypots

In the above figure we create a Data Management Zone (DMZ) where we put our Data Servers, DNS servers and FTP Servers and we don't want the attacker to attack our some of the most important system files. Instead we create a bunch of honeypots or honeynets which lures the attacker to attack that network. The ports must be left open accordingly so as to make attackers believe it not to be a trap.

A genuine user can be distinguished from an attacker depending whether he access the data or the honeypot. Firewalls are employed in the whole network to increase its security.

Web server, mail server, client etc. are forwarded to the legitimate destination and honeypot fulfil the task of luring the attacker. Standard mechanisms are used for protection of web and mail servers. Services such as web, mail, ftp services and DNS that should be accessible from the out- side are situated in a demilitarized zone (DMZ).[12]

6. Implementation

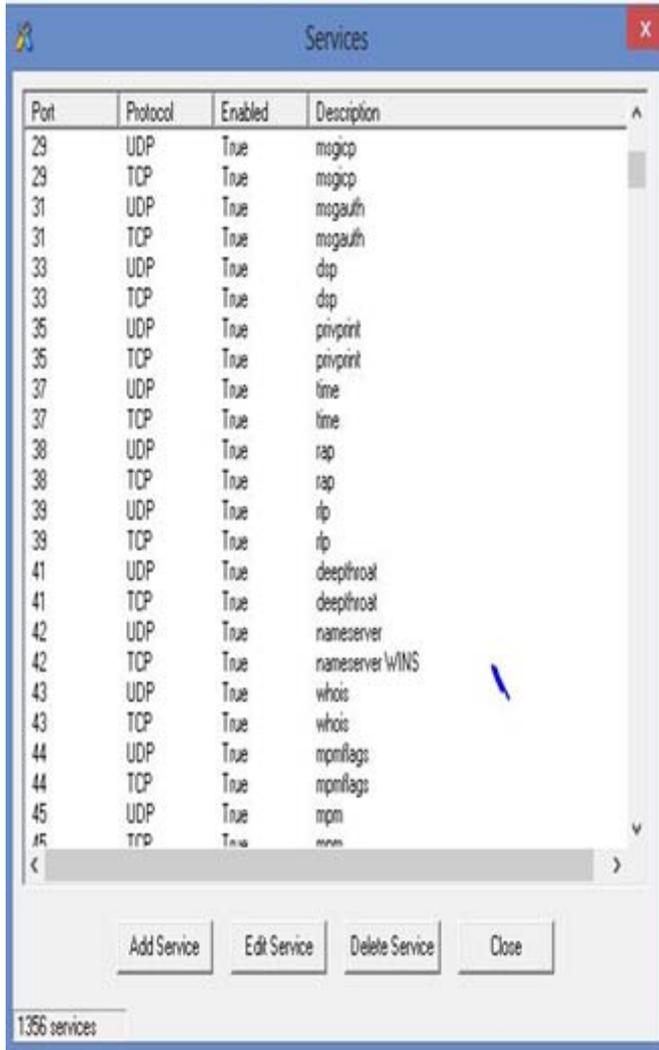
Honeypots are used to simulate a vulnerable host. In DMZ we store our valuable assets like Web server, DNS server and we place honeypots there which look vulnerable.

A DMZ is a secure server that adds an additional layer of security to a network and acts as a buffer between a local area network (LAN) and a less secure network which is the

Internet. A DMZ server is known as a Data Management Zone and provides secure services to local area network users for email, Web applications, ftp, and other applications that require access to the Internet. DMZ in networking gets its name from the demilitarized zones, which is land that the military would use as a barrier against the enemy.

One purpose of this is to study what the hackers are doing and from which address they are attacking. Honeypots are generally useless and it does not matter whether they attack or hack the honeypots. While they are busy doing it, we can see what kind of methods they use to hack the network as we will be snorting the network traffic all the time and we can locate the source of the attack.

It is also useful to distract attackers from the real target. We can also use honeynets which are entire network of honeypots and attacker might go after that thinking that as a whole bunch of machines there which makes the attacker more convinced to go after it.



Port	Protocol	Enabled	Description
29	UDP	True	magicp
29	TCP	True	magicp
31	UDP	True	magauth
31	TCP	True	magauth
33	UDP	True	dsp
33	TCP	True	dsp
35	UDP	True	privprint
35	TCP	True	privprint
37	UDP	True	time
37	TCP	True	time
38	UDP	True	rap
38	TCP	True	rap
39	UDP	True	rip
39	TCP	True	rip
41	UDP	True	depthroat
41	TCP	True	depthroat
42	UDP	True	nameserver
42	TCP	True	nameserver WINS
43	UDP	True	whois
43	TCP	True	whois
44	UDP	True	rpmiflags
44	TCP	True	rpmiflags
45	UDP	True	rpm
45	TCP	True	rpm

1356 services

Figure 2: Open ports in network

These are all the ports that seem to be left open. Although it is way too obvious that nobody leaves such a number of port open. It has got SMTP, UDP, FTP all sort of files open. So we need to make a wise and judicious decision to leave a few port open which will make the hacker believe it is not a honeypot but some real ports are open.

Now we will run an Nmap scan of the computer which will have the honeypot running.

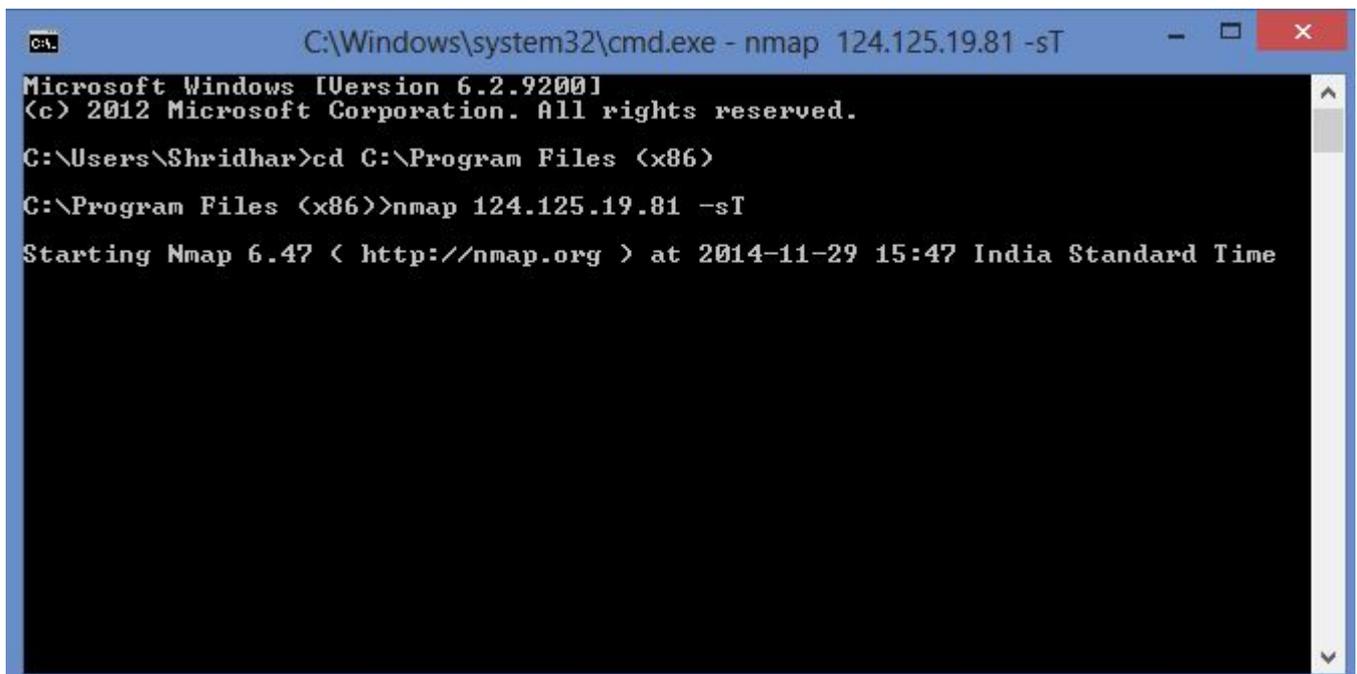
Honeypots can be connected to the production network to check the network vulnerabilities. If the attack is on the honeypot in the production network, then the attacker can all way to attack the honeypot in the production network and the network is prone to attacks.

Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. [13]

We will use the command on the command line:

```
nmap IP Address -sT
```

-sT command is used for a TCP connect scan.



```
C:\Windows\system32\cmd.exe - nmap 124.125.19.81 -sT
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.
C:\Users\Shridhar>cd C:\Program Files (x86)
C:\Program Files (x86)>nmap 124.125.19.81 -sT
Starting Nmap 6.47 < http://nmap.org > at 2014-11-29 15:47 India Standard Time
```

While the attacker would be busy running and attacking the ports we would go back to our machine where the honeypot scanner was running.

Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
11/29/2014	3:47:30 PM	124.125.19.81	54473	0.0.0.0	6101	TCP	0
11/29/2014	3:47:30 PM	124.125.19.81	54478	0.0.0.0	3005	TCP	0
11/29/2014	3:47:30 PM	124.125.19.81	54481	0.0.0.0	83	TCP	0
11/29/2014	3:47:31 PM	124.125.19.81	54492	0.0.0.0	7007	TCP	0
11/29/2014	3:47:31 PM	124.125.19.81	54500	0.0.0.0	2022	TCP	0
11/29/2014	3:47:31 PM	124.125.19.81	54502	0.0.0.0	4045	TCP	0
11/29/2014	3:47:31 PM	124.125.19.81	54511	0.0.0.0	12174	TCP	0
11/29/2014	3:47:31 PM	124.125.19.81	54512	0.0.0.0	666	TCP	0
11/29/2014	3:47:31 PM	124.125.19.81	54524	0.0.0.0	500	TCP	0
11/29/2014	3:47:31 PM	124.125.19.81	54528	0.0.0.0	2105	TCP	0
11/29/2014	3:47:31 PM	124.125.19.81	54529	0.0.0.0	33	TCP	0
11/29/2014	3:47:31 PM	124.125.19.81	54534	0.0.0.0	2605	TCP	0
11/29/2014	3:47:31 PM	124.125.19.81	54535	0.0.0.0	2045	TCP	0
11/29/2014	3:47:32 PM	124.125.19.81	54546	0.0.0.0	211	TCP	0
11/29/2014	3:47:32 PM	124.125.19.81	54547	0.0.0.0	7001	TCP	0
11/29/2014	3:47:32 PM	124.125.19.81	54550	0.0.0.0	1998	TCP	0
11/29/2014	3:47:32 PM	124.125.19.81	54563	0.0.0.0	79	TCP	0
11/29/2014	3:47:32 PM	124.125.19.81	54564	0.0.0.0	6004	TCP	0
11/29/2014	3:47:32 PM	124.125.19.81	54565	0.0.0.0	593	TCP	0
11/29/2014	3:47:32 PM	124.125.19.81	54566	0.0.0.0	7100	TCP	0
11/29/2014	3:47:32 PM	124.125.19.81	54573	0.0.0.0	20000	TCP	0
11/29/2014	3:47:32 PM	124.125.19.81	54596	0.0.0.0	212	TCP	0
11/29/2014	3:47:33 PM	124.125.19.81	54617	0.0.0.0	2042	TCP	0
11/29/2014	3:47:33 PM	124.125.19.81	54622	0.0.0.0	617	TCP	0
11/29/2014	3:47:33 PM	124.125.19.81	54627	0.0.0.0	106	TCP	0
11/29/2014	3:47:33 PM	124.125.19.81	54634	0.0.0.0	3269	TCP	0
11/29/2014	3:47:34 PM	124.125.19.81	54659	0.0.0.0	3128	TCP	0
11/29/2014	3:47:34 PM	124.125.19.81	54663	0.0.0.0	70	TCP	0
11/29/2014	3:47:34 PM	124.125.19.81	54667	0.0.0.0	9100	TCP	0
11/29/2014	3:47:34 PM	124.125.19.81	54674	0.0.0.0	4	TCP	0
11/29/2014	3:47:34 PM	124.125.19.81	54685	0.0.0.0	6699	TCP	0
11/29/2014	3:47:34 PM	124.125.19.81	54686	0.0.0.0	2034	TCP	0
11/29/2014	3:47:34 PM	124.125.19.81	54688	0.0.0.0	444	TCP	0
11/29/2014	3:47:35 PM	124.125.19.81	54708	0.0.0.0	7004	TCP	0
11/29/2014	3:47:35 PM	124.125.19.81	54709	0.0.0.0	1011	TCP	0
11/29/2014	3:47:35 PM	124.125.19.81	54711	0.0.0.0	9535	TCP	0
11/29/2014	3:47:35 PM	124.125.19.81	54722	0.0.0.0	1112	TCP	0
11/29/2014	3:47:35 PM	124.125.19.81	54742	0.0.0.0	9080	TCP	0
11/29/2014	3:47:35 PM	124.125.19.81	54744	0.0.0.0	2046	TCP	0
11/29/2014	3:47:35 PM	124.125.19.81	54745	0.0.0.0	179	TCP	0
11/29/2014	3:47:35 PM	124.125.19.81	54746	0.0.0.0	42	TCP	0
11/29/2014	3:47:35 PM	124.125.19.81	54755	0.0.0.0	6007	TCP	0
11/29/2014	3:47:35 PM	124.125.19.81	54760	0.0.0.0	389	TCP	0

When we look at the honeypot scanner we would see the attack date, time, remote id and port of the attacker as well as the local IP and local port at which the attack was directed.

7. Conclusion and Future Scope

Network security concerns are increasing day by day as the mode and style of attackers are evolving each day. This paper deals with countering such attacks measures by possibly tracing the attacker and its mode of attack. Honeypot approach is used which not only makes the attacker to go for an attack but also alert the network administrators of a possible intrusion by trailing the attacker. Honeypots can be used together with some other form of security such as an IDS to increase its efficiency.

Although a many times attacker may know that a honeypot is used in system to lure him. So further refinement can be done in such a way that attacker does not feels he is being trapped.

References

- [1] Miss.Swapnali Sundar Sadamate,," Honeypot Mechanism – the Autonomous Hybrid Solution for Enhancing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014 p.p 854-858
- [2] "Know Your Enemy: Honeynets.", available at <http://www.honeynet.org/papers/kye.html>.
- [3] Karthik, S., Samudrala, B. and Yang, A.T., "Design of Network Security Projects Using Honeypots.", Journal of Computing Sciences in Colleges, 20 (4)

- [4] A. Chandra, K. Lalitha, "Honeypots: A New Mechanism for Network Security", Department of Computer Science and Systems Engineering, Sree Vidyanikethan Engineering College A. Rangampet , Tirupati. Vol 04, Special Issue01; 2013. <http://ijpaper.com/>
- [5] Karthik Sadasivam, Banuprasad Samudrala, T. Andrew Yang. "Design of Network Security Projects using Honeypots", University of Houston
- [6] "Honeypots: Catching the Insider Threat", available at Lance Spitzner Honeypot Technologies Inc. lance@honeypots.com
- [7] "Honeypots" available at : http://en.wikipedia.org/wiki/Honeypot_%28computing%29
- [8] Iyatiti Mokube, Michele Adams, "Honeypots: Concepts, Approaches, and Challenges", Department of Computer Science, Armstrong Atlantic State University
- [9] L. Spitzner, "Honeypots: Tracking Hackers," Boston, USA: Addison Wesley, Parson Education, ISBN 0 321108957, 2003
- [10] Navneet Kambow, Lavleen Kaur Passi, "Honeypots: The Need of Network Security", International Journal of Computer Science and Information Technologies, Vol. 5 (5), 2014
- [11] Matthew L. Bringer, Christopher A. Chelmecki, and Hiroshi Fujinoki, "A Survey: Recent Advances and Future Trends in Honeypot Research", "I. J. Computer Network and Information Security", September 2012 in MECS
- [12] "Honeypot Definition" - PC Magazine available at: http://www.pcmag.com/encyclopedia_term/0,2542,t=honeypot&i=44335,00.asp, 24 March 2009
- [13] Kumar Shridhar, Nikhil Gautam, "A Prevention of DDos Attacks in Cloud Using Honeypot ", International Journal of Science and Research, Volume 3 Issue 11, November 2014, p.p 2378-2383
- [14] Network Mapper" available at : <http://nmap.org/>

Author Profile



Kumar Shridhar is currently enrolled in final year of his B.Tech programme (2011-2015) from Bhagwan Parshuram Institute of Technology. He is a certified objective C programmer and a certified ethical hacker. He is currently working on improving the network security issues. Beside these, he loves watching football and listening music



Mayank Jain is currently pursuing his B.Tech(2011-2015) from Bhagwan Parshuram Institute of Technology. He is an oracle certified java programmer and a certified .Net developer. He is currently working on improving his database and data mining skills. Besides these, he loves watching football and movies.