International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072

Honeyconf: Automated Script for generating Honeyd Configuration to Detect Intruders

Anu Kamboj[1], Ms. Renu Singla[2]

[1]M.Tech Student, Dept. Of CSE, Shri Ram College of Engg. & Mgmt, Palwal, Haryana, India
[2]Asst. Professor, Dept. Of CSE, Shri Ram College of Engg. & Mgmt, Palwal, Haryana, India

---

Abstract - *Network security is increased day by day with powerful technologies everywhere in this world for all purposes. Big organizations spend too much dollars for firewalls, encryption and on many other secured access devices which is totally money wasted because none of these measures where weakest link is. Honeypot is a unique security resource, whose values lies in being identify, detected, attacked and track the hackers. With the help of Low interaction Honeypot tool-Honeyd resolves security problems in our daily bases routines which we face in big organizations. Honeyd is a daemon framework for virtual honeypots that defend the files from intruder or illicit users with in a network. Honeyd configuration file detects intruders in the network through automated script which generates for honeyd. The main objective of this concept is to prohibit the anonymous users so they invented a new impressive technology for Intrusion Detection System (IDS) to defend the network from intruders. This is a total manual work, and knowledge of syntax understood by honeyd is expected along with other things like personality names, script names and locations for TCP and UDP ports simulation. All phases and setups are created to present their working profile at each stage and automated tool Honeyconf configuration file is generated for honeyd.*

Key Words: **Honeyconf, Honeypot, Honeyd, Autoconeyd, Intruder Detected**

1. INTRODUCTION

Security means protection from harm in today's era, it is very important to be secure and provides security to all like human, animals, offices, banks, information technology etc. Computer security is one of the main areas when we are dealing with information technology. Nobody wants that his/her system will be attacked and anybody will receive the stolen data. In past several years, we have seen the technology rapidly develop with new concepts in order to provide computer security. However a great deal of research has been focused on identifying, capturing and researching external threats. It is necessary to put high priority to system security, minimize vulnerabilities and secure the computer system against intrusion. We need to find out how attacker attacks actually so we will provide a security 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 the attackers [6]. The technology that is preventing data from the attackers by recording the activities done by attacker is called Honeypot.

2. HONEYPOT

Honeypot are the technologies that can be used to detect, identify and gather information on specific threats. There has been an extensive research into honeypot technologies primary for detection and information gathering against external threats. Honeypot is an information system resource whose values lie in unauthorized use of that resource. It is a unique security resource. If the enemy does not interact or use the honeypot, then it has little value. This technology is very different from most security mechanisms. Honeypots are very different, and this difference that makes them such a powerful tool. Honeypot do not solve a specific problem. Instead they are a highly flexible tool that has many applications to security. They can be used everything from showing down or stopping automated attacks, capturing new exploits to gathering intelligence on emerging threats or early warning and prediction. Honeypots can be everything from a windows program that can emulates common services to entire networks of real computers to be attacked. Anything or anyone interacting with the honeypot is anomaly, it should not be happening. Any interaction with the honeypot is assured unauthorized and most likely malicious. If the webserver honeypot is probed by external systems from the internet, you have identified a probe or attack, most likely the same one your other production webservers are facing. If your Honeypot is probed by one of the production webservers that can imply the production web server has been compromised by an attacker, and is now being used as a launching pad to compromise other systems.

Advantages of Honeypot

- Honeypots only collect data when someone or something is interacting with them. This makes the data honeypots collect much higher value, easier to manage and simpler to analyse.
- One of the greatest challenges with most detection technologies is the generation of false positives or false alerts. The larger the probability that a security technology produces a false positive the less likely the technology will be deployed. Honeypots dramatically reduce false positives.
- Another challenge of traditional technologies is failing to detect unknown attacks. This is a critical difference between honeypots and traditional computer security technologies which rely upon known signatures or upon statistical detection.
- It does not matter if an attack or malicious activity is encrypted, the honeypot will capture the activity. As more and more organizations adopt encryption within their environments this becomes a major issue. Honeypots can do this because the encrypted probes and attacks interact with the honeypot as end point, where the activity is decrypted by the honeypot.
- Honeypots are extremely adaptable with the ability to be used in a variety of environments to an entire network of computers designed to be broken into.

Disadvantages of Honeypot

- They are worthless if hackers are not send any packet trying to attack them.
- All type of honeypots have their different risks, And they are varies on builds and deploying the honeypot.

2.1 Types of Honeypots: There are two types are honeypots explained (I) Low Interaction honeypot (II) High Interaction honeypot

I. Low Interaction Honeypot

This type of honeypot is easiest to install, configure, deploy and maintain. They partially evaluate a service. E.g.-Unix or OS and limit the attacker's activities to the level of emulation provided by the software it emulates particular IT services or systems well enough to provide a realistic initial interaction, but does not execute a full version of those services or systems. It provides a less realistic target and often sufficient for use as a component distributed IOS to warm of imminent attack.

Advantages of low interaction honeypot

- Logging and analysing is simple.
- Only transactional information are available, no information about the attacks themselves. E.g.- time and date of an attack, protocol, source and destination IP as well as Port.

Disadvantages

- Very limited logging abilities.
- Captures only known attacks.
- Easily detectable by a skilled attacker.

II. High Interaction Honeypot

Provide an attacker with a real operating system where as nothing is emulated or restricted. Ideally you are rewarded with vast amount of information about attackers, their motivation, actions, tools, behavior, level of knowledge, origin, identity etc. A high interaction honeypot can be compromised completely, allowing an adversary to gain full access to the system and use it to launch further network attacks. In high interaction honeypots nothing is emulated everything is real. It provides a far more detailed picture of how an attack or intrusion progresses or how a particular malware execute in real-time.

Advantage

Learn as much as possible about the attacker, the attack itself and especially the methodology as well as tools used.

Disadvantage

Building, Configuring, deploying and maintaining a high interaction honeypot is very time consuming as it is involves a variety of different technologies that has to be customized.

Honeynets and Honeytokens are also types of honeypots which we are using:

Honeynets:

The most advanced and complex honeypots is honeynets. The primary purpose of honeynets is to capture extensive information on those threats both internal and external [11]. Honeynets are complex in that they are entire networks of computers to be attacked. The systems and applications within a honeynet can be the same systems found in our organizations. Within these systems, we can place additional information, such as files records in databases, log entries, any information we want the attacker to interact with. Honeynets have this flexibility because they are not standardized solutions.

Honeytokens:

The newest and most interesting implementation of honeypot is the honeytokens. First they are not a computer instead they are a digital entity. Even though they are not a computer, instead they share the same definition and concept of honeypots, no one should be interacting with them. Any interaction with honeytoken implies unauthorized or malicious activity. They are extremely flexible and have ability to adopt any environment. The reason for this is simple that the honeytoken can do anything much pretty which you want. It is simple as that, no fancy algorithms, no signatures to update, no rules to configure. You can load the records, monitors it. Honeytokens are extremely flexible because there is no right or wrong way to use them. Due to their flexibility, you can customize them to easily integrate into your environment.

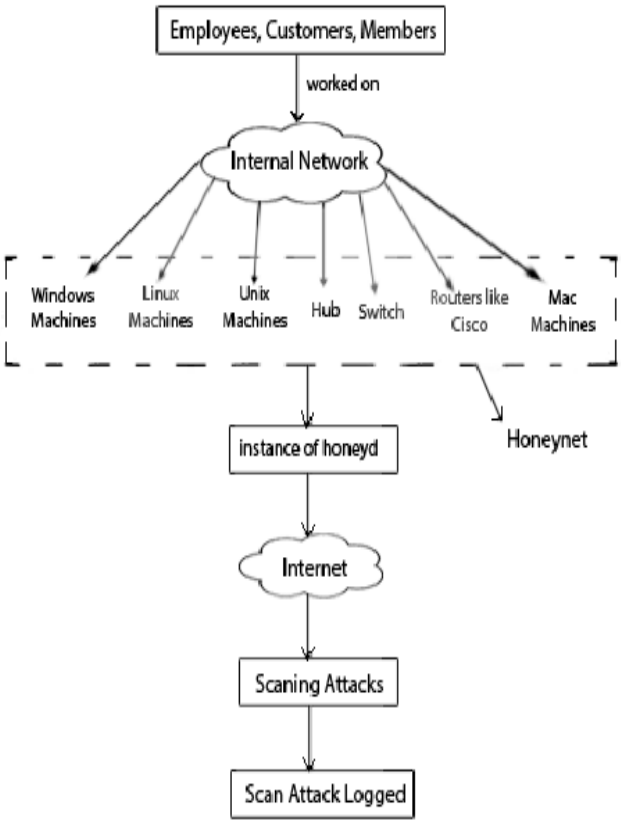

Fig -1: Logged Scanned through Honeyd

3. HONEYCONF ALL PHASES AND PROFILES HOW WORKS

All phases and profiles are worked step by step as shown in the flowchart:

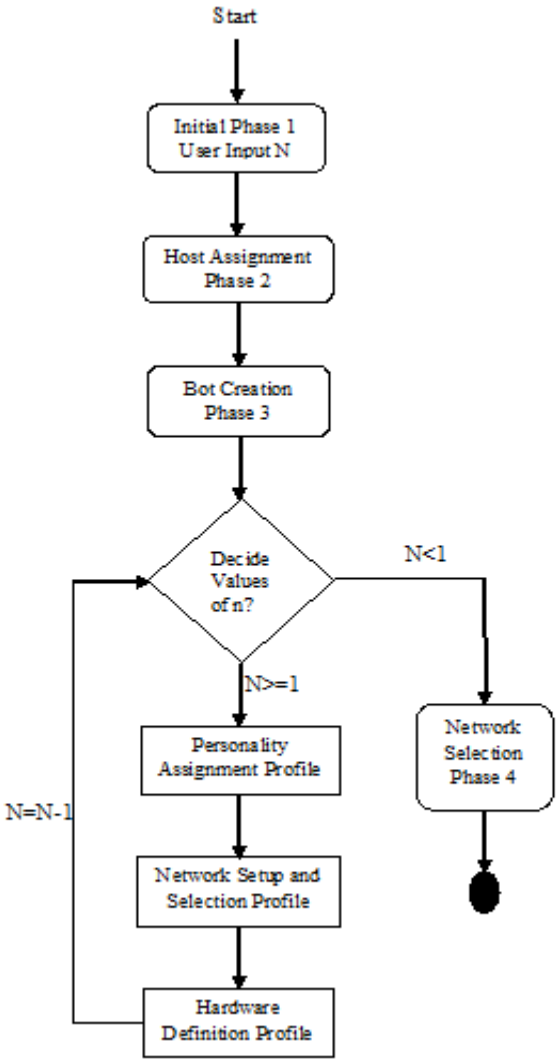

Fig -2: All Phases and Profiles of flowchart

3.1 Initial Phase1

A low interaction honeypot is created for simulation of various types of honeypots personalities, port numbers, default actions and execution of scripts on attacks. At initial Phase1 user give input to honeypot or virtual machines to deploy a honeypot. In this phase, premium task of user is to prove with the many number of honeypots he wishes to implement in his network.

3.2 Host Assignment Phase2

This is an important phase to manage network profile to deploy a honeypot within network. A host machine can have many interfaces at same time like WiFi, LAN, and Ethernet. All interface have set of IP address provides to their

respective router. Honeyd is supported with all LINUX/UNIX flavors, which tells about the which flavor is daemon running on.

3.3 Bot Creation Phase3

Bot creation phase is created for all personality of virtual machines. If user gives minimum input one for a single virtual machine bot creation phase is successfully created. Fyodor's Nmap tool manage and detect the fingerprints of all these virtual machines. Honeyd simulate the TCP/IP protocol stack of different operating systems to provide many services to all virtual honeypots to fool network fingerprinting tool like Nmap. It includes windows, Linux / UNIX, mac, routers and switches. Bot creation phase has divided into three other profiles:

3.3(a) Personality Assignment Profile

Honeyd read configuration file to assigns a personality of operating systems. Personality finds out behavior of the TCP/UDP network stacks and processed packets sent in the network. Personality assignment profile phase provides a list of profiles for user choice according to their requirement. Configuration file of personality should match exactly Nmap tool personality. And it's very difficult to remember all personalities with their exact syntax. For example selected personality is "Microsoft Windows 2000 Server SP3", the console file is written in exact syntax as:
Set windows3 personality "Microsoft Windows 2000 Server SP3"

3.3(b) Network Setup and Selection profile

Honeyd is example of low interaction honeypot. Different types of operating systems are simulated using honeyd. Here is provided port number list from 1-1024 for various types of protocols TCP/UDP with their services is explained in Honeyd to ease the working of honeyd. Rest of the port numbers 1025-65535 can still be selected along with ports which are not provided for configuration. Honeyd sent only TCP/UDP/ICMP packets. Some ports are given to the honeyd like 100 port for telnet service, 110 port for web server. Traffic is occurred on port 100. Ports are defined in configuration script file as:
Set windows3 tcp port 100 "scripts/router-telnet.pl"
Set windows3 udp port 110 "sh scripts/web.sh"

3.3(c) Hardware Definition Profile

All hardware have their unique MAC (Media access control) address which is assigned by manufacturer of the company on NIC (Network Interface card). MAC address have total 48 bits, First 24 bits for specific vendor and remaining 24 bit for unique identifier of each machine. This complete concept has been implemented in the **autoconeyd.** When we select more than one one honeypot then returned to Bot creation Phase. Configuration script file for MAC as:
Set windows3 ethernet "00:03:ff:55:8f:76"

3.4 Network Assignment Phase4

This is critical phase due to identify the system in the network. Network selection phase assigned IP addresses to virtual hosts when it's connected to network through honeyd configuration file. We use DHCP to assign dynamic IP address to virtual machines, it sends request to DHCP_REQUEST to router and router gives reply through DHCP_ACKNOWLEDGE and DHCP_REPLY. Honeyd configuration file bind IP address to honeypots but network interface allow only that series of IP addresses which is already not assigned to any system. The binding of IP address as:
bind 192.168.72.100 windows3

4. RESULTS

Honeyd.conf files are generated in Honeyconf for all phases and profiles with their information. Honeyconf script is written in python 3.4.3 high level language for security purpose. It contains all personality descriptions and text files. We deploy Honeyd.conf files on Ubuntu Version-14.04 LTS having 4 GB RAM with setup of 15 honeypots and detect intruders with their IP address. Honeyd.conf files are look like this:

```
create windows3
set windows3 default tcp action reset
set windows3 default udp action reset
set windows3 personality "Microsoft Windows 2000 Server SP3"
add windows3 tcp port 100 open
add windows3 udp port 110 open
set windows3 ethernet "00:03:ff:55:8f:76"
create apple2
set apple2 default tcp action reset
set apple2 default udp action reset
set apple2 personality "Apple Mac OS 8.0"
add apple2 tcp port 200 open
add apple2 udp port 210 open
set apple2 ethernet "00:17:fa:c3:ee:a1"
create router1
set router1 default tcp action reset
set router1 default udp action reset
set router1 personality "Cisco 2620 router running IOS 12.1(6)"
add router1 tcp port 300 open
add router1 udp port 310 open
set router1 ethernet "00:03:ba:6e:48:e9"


bind 192.168.72.110 window3
bind 192.168.72.111 apple2
bind 192.168.72.112 router1
```

Fig -3: Screenshot of Honeyd.conf files

Table1- : Number of Honeypots takes how much time to run files

Number of Honeypots taken	Time taken by honeyd in sec.	File Size in bytes	System Configuration
15	<1	1663	1 GB RAM, intel Pentium Dual core
70	5.8	7047	2 GB RAM, Intel® Core 2 Duo Processor
150	11	19293	4 GB RAM, intel core i3
300	19	31932	8 GB RAM, intel core i5

Table -2: Number of Intruders detected with IP and visits

3 days datewise	Number of attackers visit	IP Used	Crawlers Used
05-05-2016	126	62	Google
06-05-2016	62	18	Yahoo
07-05-2016	93	38	Bing

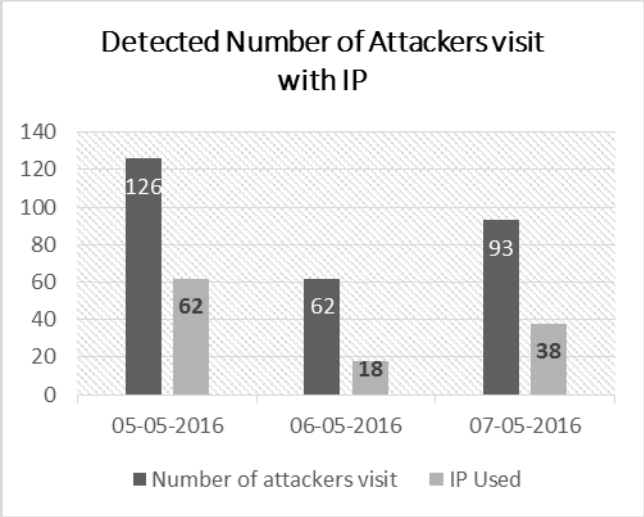

Chart -1: Number of intruders detected

5. FUTURE SCOPE

Honeyconf automated script generates the configuration file for honeyd is honeyd.conf for all phases and profiles. We will do automated configuration file on all systems simultaneously with security. We are unable to bind IP addresses because we don't know these are allocated to the systems in the network or not. So we provide manually IP address to all hosts.

6. CONCLUSIONS

Honeyd is a framework created for virtual honeypots and tested 150 honeypots with honeyd.conf file. Honeyconf is an automated script tool to detect intruders within the network and parsed files within seconds. There is no any need of network engineer or security expert for configuration of honeypot. Anyone can manage it easily to select options one by one for the execution of Honeyconf file.

REFERENCES

[1] Know Your Enemy: The Tools and Methodologies of the Script Kiddie. Project Honeynet, 2000.

[2] Know Your Tools: Use Picviz to Find Attacks. Lance Spitzner, Project Honeynet, 2009.

[3] Know Your Enemy III: They Gain Root. Project Honeynet, 2001.

[4] Fyodor, "Remote OS detection via TCP/IP stack fingerprinting", Phrack, vol. 8, no. 54, October 1998.

[5] Ashutosh Vashishth, Mukul Saxena and Usha Banerjee, "Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection", Volume 6– No.7, September 2010.

[6] Tejvir Kaur1, Vimmi Malhotra2, Dr. Dheerendra Singh "Comparison of network security tools- Firewall, Intrusion Detection System and Honeypot", Vol. 3 Issue 2, February 2014.

[7] A. Samrah, "Intrusion Detection Systems; Definition, Need and Challenges", October 31, 2003.

[8] K.Scarfone and P.Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," Gaithersburg, MD, Rep. NIST Special Publication 800-94,Feb. 2007.

[9] Ofir Arkin and Fyodor Yarochkin, "A "Fuzzy" Approach to Remote Active Operating System Fingerprinting", August 2002.

[10] Lance Spitzner, "Honeypots: Tracking Hackers Addison Wesley Professional", September 2002.

[11] Lance Spitzner, "Honeypots: Catching the Insider Threat", Dec 2003.