Honeypots Tools Study and Analysis

Sultan Al-Jameel and Adwan Alownie Alanazi

Department of Computer Science and Engineering,
University of Hail, Saudi Arabia

Abstract
The Honeypot is the mechanism that is made to learn more about the attackers like knowing about the method and pattern of attack and is also used to obtain very useful info about all intrusive activities. Honeypots usually categorized according to the interaction's level as (high, medium, low) interaction. The main purpose which is used as honey production and honey research. This paper includes a detailed study of two honeypot tools. The different honey pot findings are put in in this paper to illustrate how honey is working in a real environment and even how it reacts when undesirable interest obtain in this network, and these tools are used to improve the concept of security, protection and confidentiality within or outside the organization to avoid attacks, vulnerabilities and breaches.

Keywords: Honeypot, Security, low, medium, high, production, research, PentBox, honeydrive , attackers.

I. Introduction

With the emergence and development of the Internet day after day, the significant increase in the interconnectedness of computer systems and network , and the increase need in to sense of security, there is an increased need for security and firewall measures to safeguard are usually large the information and systems of the organization. For a time, security of the network was defensive by using all traditional devices of the network like firewalls, routers and finally systems for detecting all intrusion activities. honeypots occupied a different position on security because they were created to attract down hackers, investigate and record all their moves. This can help organizations and their IT personnel to learn all methods of the intruder (or what it's called black hat) so that they can 'harden' and strengthen systems and products against such attacks in the future. However, honeypots only will not be able to solve all the security issues of the system; but they can be considered as tools that can aid and complement the traditional devices of the network. [1]

The work and preparation for the hack and attack to the systems by hackers is always done in secret and within closed groups. And hackers always keep entry technologies hidden and not common to people. On the other hand, technical experts and those interested in cybersecurity can learn new technologies. So that they know the following: How was the hacking done, what tools were used, and how malware works. Hackers have a strong desire to hack any system. We can take advantage of this desire by setting "honeypot" traps.

The main goal of honeypot is to attract hackers to penetrable systems, monitor their full steps and closely identify them without impeding the systems that are in progress. Honeypot is a source or security resource, whether it is a firewall, router, switch, or server. The main goal of creating this honeypot is to penetrate it, gather information and monitor what happens inside it. The purpose of calling the honeypot by this name is that it is an attractive target for hackers, but at the same time they are a trap and they fall into it.

II. Honeypot

A honeypot is a system set up that is attached to the network as a bait to track cyber attackers and to discover, divert or learn all about attempts for hacking in order to gain unauthorized access to information systems. So the main function of a honeypot is to make itself to look as a value target or a service in the internet for attackers and then gather all information about them and warn defenders of all honeypot access attempts by any unauthorized users.

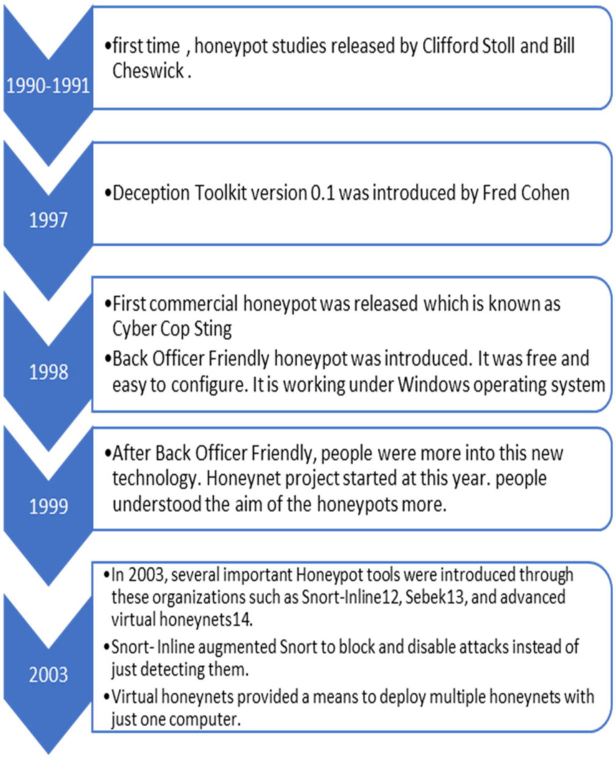
The main users of honeypots almost always wide companies and enterprises which are parts of cyber-security research, to solve and defend ongoing attacks from advanced threat done by those attackers. So honeypots are considered as a so of interest tool to all the organizations to

Manuscript received January 5, 2021
Manuscript revised January 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.1.21

have an active future defense against those attackers, and even for researches of cybersecurity which are made to know more and learn everything about the techniques and tools of the attackers.

1. History of honeypot

In 1986, Cliff Stoll was appointed to Lawrence Berkeley National Lab as Systems Director. One day, Cliff found that a group of accounts had been compromised and decided to create devices with holes to attract any hacker and identify him. And in 1990 he showed the whole world this new term which is Honeypot. [2]



1990-1991

- first time , honeypot studies released by Clifford Stoll and Bill Cheswick .

1997

- Deception Toolkit version 0.1 was introduced by Fred Cohen

1998

- First commercial honeypot was released which is known as Cyber Cop Sting
- Back Officer Friendly honeypot was introduced. It was free and easy to configure. It is working under Windows operating system

1999

- After Back Officer Friendly, people were more into this new technology. Honeynet project started at this year. people understood the aim of the honeypots more.

2003

- In 2003, several important Honeypot tools were introduced through these organizations such as Snort-Inline12, Sebek13, and advanced virtual honeynets14.
- Snort- Inline augmented Snort to block and disable attacks instead of just detecting them.
- Virtual honeynets provided a means to deploy multiple honeynets with just one computer.

Fig 1: history of honeypot

2. Honeypot Classification

The Honeypot are designed based on purpose and it is divided into 2 sections: production honeypot and research honeypot. And also designed based on level of interaction and it is divided into 3 sections: high interaction honeypot, medium interaction honeypot and least interact honeypot

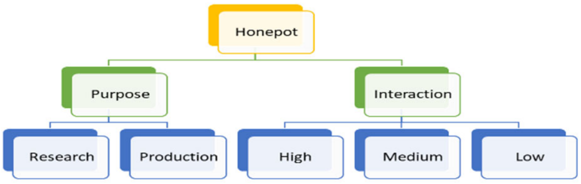


Fig 2 : classification of honeypot

2.1 Based on level of interaction

2.1.1 High interaction honeypot

The high-level interaction honeypot is usually having a very high grade of interact with the intrusive system. And it offers the attacker an extra realistic experience and collect more information about future attacks; and it can be also endangering the whole honeypot for capturing. There is effect in this kind, and the reason is that it does make the hacker delve too deeply into the honeypot, and able to making the hacker to enters the system and loads payload or shellcode . And hacker can do complete penetration process, it is true that it is very dangerous, as this may compromised contaminate the trap and may affect other devices connected to the same network. So, it is more secure so that it is difficult to detect easily, but its cost is high, and its advantages are:

- It is a complete encryption system and does not impose any limits in use.
- It allows the hacker to fully control the system when hacked, as he can install its programs and tools on it as if it were his own device.

And its shortcomings:

- It needs strong monitoring and great caution when placing it at any point in the network.
- It is a lot used in research and experiments to achieve the best results that serve the system. [3]

2.1.2 Medium interaction honeypot

Offers more activity than low interaction honeypots and less than high interaction. [4]

2.1.3 Low interaction honeypot

They can give the attackers a very little or little entrance to their operating systems. However, this type is a consists of a software package that emulates IT systems or services that are good enough to mislead the attacker only and no one else. Usually, most companies emulate protocols like IP and TCP, which could allow the attacker to assume they are not connected to a honeypot abode but rather a actual system. There is no effect in this type , and the reason is that it does not make the hacker delve too deeply into the honeypot , and will only receive requests without able to making the hacker to loads payload or shellcode .

TABLE I : LOW INTERACTION VS. HIGH INTERACTION

	Low – interaction	**High - interaction**
Installation	Easy	More difficult
Maintenance	Easy	Time consuming
Risk	Low	High
Need control	No	Yes
Data gathering	Limited	Extensive
Interaction	Emulated services	Full control

2.2 Based on the purpose

2.2.1 Production honeypot

Honeypots are basically intended to secure and protect the networks. production Honeypots can be built easily, use and propagate, because they need very fewer jobs. They protect systems by discovering attacks and notifying administrators. They are usually used to secure the organization inside it's environment. In this type intended that it makes it section of the protection methods in the network or acts as a kind of hacker intimidation. So that if more than one suspicious response arrives, I can transfer it to the honeypot , and in this way you have increased your level of protection by adding the honeypot to it.

It will add value to the quality of security for your network. Because it will recognize patterns of hacker attacks. And when you feel that there is an attack from an incoming hacker to the system, the production honeypot turns this attack into the trap (honeypot) and it will remove the danger from your network to the honeypot and start to monitor also and also and deal with the hacker so that you see the attacks and tricks that the attacker will power perform away from the internal network and transfer the risk from the possibility of hacking the network Interior to the honeypot trap. It isolates the intrusion from the internal network.

2.2.1 Research honeypot

In this type it is intended to be used for research purposes. Such as studying malware, the way it spreads, its operation, its goal, and work method in real-time . For the intent of research and learning.

These are not used for protecting networks. They are usually used and implanted for pure educational purposes like demonstration and to study and learn about all types the patterns, techniques and threats of the attackers. Research honeypots are drawing huge attention these days since they can be utilized to gather data around the actions of intruders and record this information for the research, warrior or polity organizations. [5]

3. The goals of honeypot

- The virtual-system must appear as real as possible and must catch unwanted intruders to reach to the study virtual machine.
- The virtualization system must be monitored to sure that it is not used for a major attack on other systems.
- The default system should look such a normal system, meaning it should contain files, directories and information that attract the attention of the attacker.[6]

4. Advantages of Honeypot

Honeypots are an important, useful, and effective method to discover weaknesses in basic or main systems. For example, Honeypots can demonstrate high-level of risk or threat that posed by hackers on IoT devices. By discovering vulnerabilities, this can affect the improvement, development and increase of security.

When using a honeypot, it can detect an early intrusion attempt into the main system or network. Before the main system or network is attacked form hackers and the main system or network is affected by that attack. When unauthorized access to the network is affected, it facilitates access to all devices connected to that network .

Honeypot makes it very easy to identify IP that may come from unauthorized access, such as suspicious or unsafe IP addresses that come from an unauthorized person or hacker. The main benefits from using honeypot improve security in way malicious addresses that came from unauthorized user (attacker) will be only appear and clearly identifiable, making it very easier to detect and identify the hackers.

Traditional Intrusion-Detection Systems (IDS) that can detect very many false and incorrect alerts. Honeypots can provide high security by linking them with other system and firewall logs in or link it the network. Honeypots could place before or after IDS is configured to producing fewer false detection and not useful that might waste of time. In this path, Honeypots could be of great help tool to improving and developing other cybersecurity systems. And it saves a lot of time that traditional intrusion-detection systems spend in detecting suspicious movement in the system or network. by the honeypot, the suspicious movement that comes from the hacker is determined, and whoever wants to access the mission information in the system is determined directly.

Honeypots could provide you reliable information about of how the different threats have evolved. They provide facts relationship to the attack and who to come, exploits, malware. For example, if email is intercepted, through honeypots could be known around spammers and phishing attacks. Hackers are constantly improving their stealth techniques and by using honeypots can learn advanced and new technologies; Honeypot helps detect newly threats, attacked and intrusions.

Honeypots great and helpful education tools for security employees. Honeypot is a safe, controlled environment to show how attackers operate and screen for mismatched types of intrusions and threats. With the site of attraction, the security employees will not be confused between legal traffic and threat in the network - security employee can be focusing 100% on the threat.

Honeypots can also detect insider threats. Most establishments and company spend more time to defending and making sure strangers and intruders cannot get in. Firewalls can be an ineffective and powerful tool when facing internal threat .

Through the honeypots it can provide many important information or data about internal or exterior threats and detect vulnerabilities and weakness in the system or network for example permissions or license that may will allow to insiders or outsider to exploiting the system.

The main advantages we can summarized in following main points:

- Honeypots can arrest attacks and analyze them to give additional datum about their types.
- Honeypots are used to understand a lot about the attacks and attackers that can be happen again in the future.
- Honeypots don't need massive data storage
- Honeypots can do selective focusing on just the malicious traffic which might facilitate the investigation a lot.

Finally, by creating honeypots, you help other computer and network for users to secure them. The more time attackers spend wasting efforts and attempts at honeypots, the less time they will have to break into systems and cause real harm to many users. [7]

5. Disadvantages of Honeypot

All technologies that are being used have many advantages, but they also have several disadvantages or weaknesses such as:

- The data can be captured only when there is active attack on the system by the hacker.
- When there is an active attack happening in another system, our honeypot would not be able to detect it.
- An experienced hacker will find out easily if he is attacking a real system or a honeypot. [8]

6. The risk of Honeypots:

In general, the pros of utilizing honeypots are much maximal the danger. Hackers and hackers at some point are seen as invisible threats and are not quickly detected - but when we use and prepare honeypots to run, you can see precisely what the hackers are doing, in real time, and you can also use this data and information to prevent them and prevent them from getting what they want.

While cyber security for honeypots will help in knowing what environment the security risk and threat is in, it is substantial to go on with the development and news in IT security, not just Accreditation on honeypots to inform you of threats.

Since the attraction can act as a launch pad for further infiltration, it must be ensured that all attractions and areas are secured. The "honey wall" can give basic security to traps and stop Targeted attacks against the source of attraction from entering your live system. Because it is possible for an intelligent attacker to use a honeypot as a method in your systems. This is why hubs can eternally exchange security controls, such as infiltration detection systems and firewalls.

Construction hacker can distract phishing attacks from an actual exploit targeting your output systems. By just "fingerprinting" an attraction, it can also provide bad information.

A well-formed and properly configured location of traps will trick the attackers because they suspect they have acquired arrival to the actual system. It shall possess the same aspect, feel, data, notifications, logins, and warning messages [9]

7. Applications domain of Honeypot

One of the three most prominent areas or filed of use the honeypot, and from filed that may be used as an instructional environment, we mean here meet the requirements that need for students universities, researchers in cybersecurity and specialists in information security are fulfilled so that they see how the breaches or attacked happen in real time or monitor malware. The honeypot provides a suitable environment for further learning.

The second filed may be used to attract hackers and to learn hackers' techniques and methods that used in penetration and gathering information and to avoid falling into security problems and developing our security system. And the third field or use. The honeypot can be used by monitoring any malicious program and how it spreads in the systems, for example in the case of new viruses appear where I do not know how they work or how to control these new viruses or even some malicious worms that spread in the networks. I can test them inside honeypot and see their effect. It is clearly in the system or within the network.

And the field or the last third use I can use these traps as a defence tool, but this field is of little use because the honeypot is not considered as security tool and it is easy to download or download it in the network like anti-virus. But if the hacker knows or discovers that there is a (honeypot) trap on the network, hackers will think a thousand times before enter to attack. A hacker knows that in the honeypot, all the movements that take place will be recorded, which will cause the identity of the hacker to be revealed

7.1 Honeypot in Educational Resources

In some universities, such as Brigham Young University, a Lab for network security tools has been set up for students and researchers to conduct their experiments. They track malicious traffic in network and is designed as a 'sandbox' to keep harmful activities out of the lab.

Through it, the honeypot was created to be notified of new threats, to secure the Lab, to learn the basics of security and to identify vulnerabilities with it.

7.2 Honeypot in Teaching and Research

An educational honeypot can be implemented in either a real honeypot or a virtual honeypot, or both. In the real honeypot, it must be ensured that all communications are carried out correctly and that no error occurs. When any wrong communication is made, the system will stop working and may lead to its failure. The real honeypot is a useful learning tool for building a single experiment and removing it in a short time due to its ease of preparation. And in the virtual honeypot, they are installed on emulation programs like VMware, VirtualBox, ... etc, and the main network is divided into subnets, and virtual ports are assigned to analyze network traffic. The virtual honeypot is more suitable for long and continuous research because it is easy to maintain.

7.3 Honeypot with IDS

Through the intrusion detection system (IDS), a distinction is made between traffic in the network, whether it is a client or an attacker.

There are two types of IDS - Misuse detection and anomaly disclosure

-In Misuse detecting: IDS analyzes all the different kinds of information from network traffic that it has collected and then matches it with a large database to confirm the attacks.

-In Anomaly detecting: the network traffic is monitored, analyzed, and compared with the baseline set by the system manager.

When adding a honeypot to an IDS, it simplifies the problem of detecting an (anomaly) from the normal.

Through the point of honeypot, the oddball disposal is directly recognized.

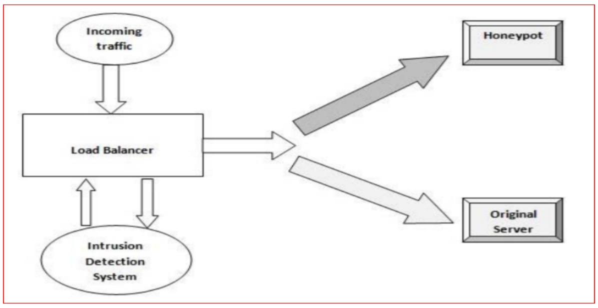


Fig 3: flow of packets through ids in honeypot.

In the above diagram, it is illustrated that the honeypot works with the IDS include the network. When the request is received, the received packets are verified by the database and then this connection is verified. If it carries harmful packets, the connection is closed and redirected to the honeypot, otherwise the packets are directed to the server.

7.4 Honeypot in network security

Honeypot technology is prepared to be penetrated, it is used in a different scenario such as an intrusion detection system, defense mechanism or reaction. In addition, it is deployed to consume the resources of the attackers and distract them from accessing production systems or servers.

In high level, the hacker interacts with real systems and can use all services and programs. Hackers are monitored, the tools they use and the vulnerabilities that are discovered through them. This type is deployed by virtualization software such as VMware, VirtualBox, Qemu, ...etc..

HoneyNet is an example of a high-level attraction site. It is a network of multiple systems that enables us to collect important information about attackers such as: keystrokes when they enter the system, private chatting, tools they use, to improve ,explore and develop an organization's systems.

In low level, there is no operating system that an attacker can compromise. This type is less vulnerable, as it helps reduce risks by enabling it to scan port, generate attack signatures, and collect malware. [10]

8. PLACEMENT OF HONEYPOT

- In front of the firewall (Internet)
- DMZ (De-Militarized Zone)
- Behind the firewall (intranet) [11]

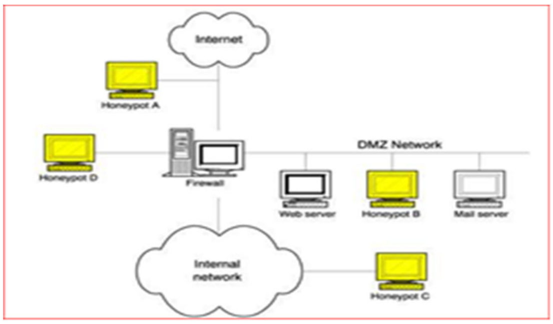


Fig 4: placement of honeypot.

III. HONEYPOT TOOLS

1. The working of honeypot

The honeypot works similar to actual computer system, with applications and information, designed to trick the hacker into thinking it is an easy target. For example, the honeypot can resemble a company's customers billing system - repeated aim for hackers for culprit who may want to discovery credit card information . Once in, the hacker can track them and evaluate their behavior for guide on how to production the actual network extra safe.

Honeypots are positioned to be attractive to hackers by intentionally creating security-vulnerabilities. Such as, a honeypot that might contain ports that may respond to port scanning or weakly passwords. The vulnerable ports that may be leave open to lure hackers inside the environment of honeypot rather than the direct access to secure network.

Honeypots is set up to fix a particular problem, such as being placed before or after a firewall to enhance and increase protection whether for the network or the router or this also applies to antivirus program. It is a very useful and important tool that let us to understand current threats to the network and detect the existence of new threats.

Finally, the honeypots are contain the monitoring and tracking tools so that every step of the activity that the hacker left the log can be logged and tracked, indicating these traces of the activity in full details.[12]

Here will talk about PentBox & Honeydrive3 tools for the honeypot:

2. PentBox (Penetration Testing Tool)

Pentbox can be defined as a security kit that hold the various tools which might help a penetration tester or ethical hacker to do their work without any difficulty. It is programmed in Ruby and directed to GNU/Linux systems, but can be compatible with MacOS, Windows systems, and all other systems where Ruby can work. It is usually open source and even free available.[13]

2.1 Tools

Cryptography-tools, Network-tools; **Honeypot in this tool,** Web, Ip grabber, Geolocation IP, Mass attack , and License and contact.

2.2 The target of apply Pentbox:

In this tool will clarify the method of setting up the honeypot in the Kali Linux, through tricked for attacker by a create open ports a hypothetical about IP address for mine, and display a message telling the attacker that in honeypot. AND you can see IP address for attacker.

2.3 The work requirements:

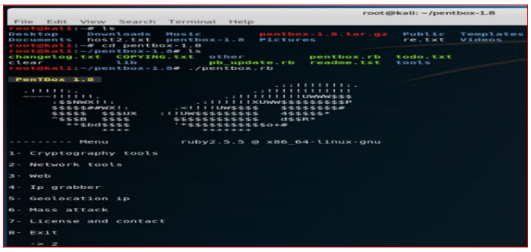
- Kali Linux
- PentBox tool and install honeypot

2.4 The steps for work:

1- You need to download PentBox tool by executing this command in terminal of kali Linux:

```
git clone https://github.com/technicaldada/pentbox)
```

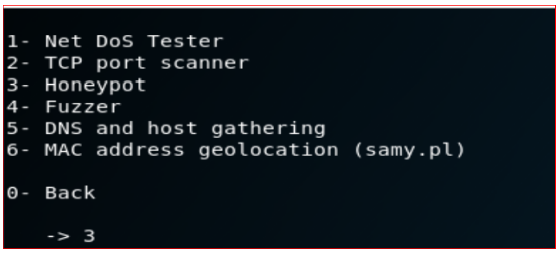
2- After the downloaded can display all the tools contained on pentbox and choose Network tools.



```
root@kali:~# ls
Desktop    Downloads  Music        pentbox-1.8.tar.gz  Public  Templates
Documents  host2.txt  pentbox-1.8  Pictures            re.txt  Videos
root@kali:~# cd pentbox-1.8
root@kali:~/pentbox-1.8# ls
changelog.txt  COPYING.txt  other           pentbox.rb  todo.txt
clear          lib          pb_update.rb    readme.txt  tools
root@kali:~/pentbox-1.8# ./pentbox.rb

 PenTBox 1.8

--------- Menu          ruby2.5.5 @ x86_64-linux-gnu

1- Cryptography tools
2- Network tools
3- Web
4- Ip grabber
5- Geolocation ip
6- Mass attack
7- License and contact
8- Exit

   -> 2
```

Fig 5: screenshots of pentbox tools.

3- The network tools contain several tools; Here you need Honeypot:



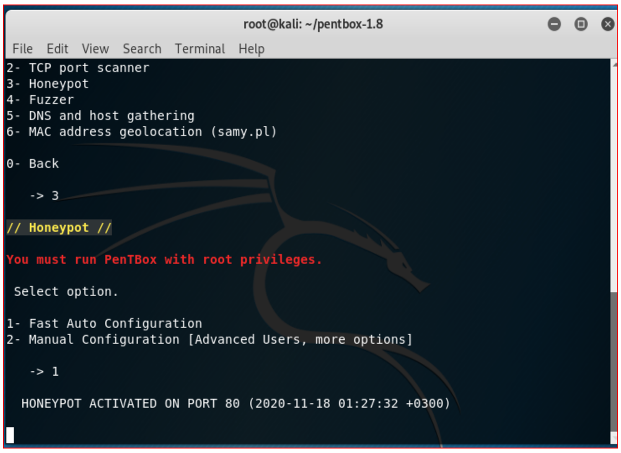
```
1- Net DoS Tester
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)

0- Back

   -> 3
```

Fig 6: screenshots of network tools and choose honeypot

4- After choose Honeypot; you select what option need.

2.4.1 Fast Auto Configuration:

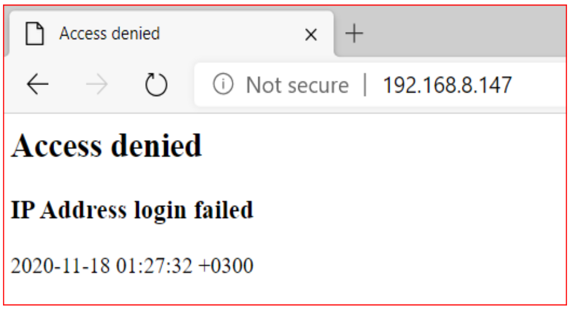
Select Auto Configuration starts the honeypot service on Port 80 which is the Web Service port



```
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)

0- Back

   -> 3

// Honeypot //

You must run PenTBox with root privileges.

 Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

   -> 1

  HONEYPOT ACTIVATED ON PORT 80 (2020-11-18 01:27:32 +0300)
```

Fig 7: screenshots of choose auto configuration.

In this step I need to know the Ip address of Kali Linux Using the command (ifconfing) and write this Ip address in web page (http://localhost) and show this message in attacker.



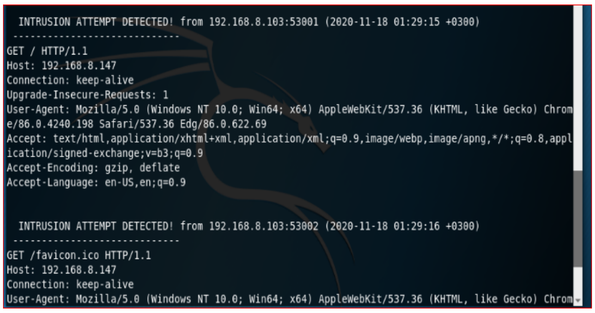
Access denied

IP Address login failed

2020-11-18 01:27:32 +0300

Fig 8: screenshots of success denial of serves.

I n same time, but in another side in honeypot to show warning message from the attacker and printing its data.



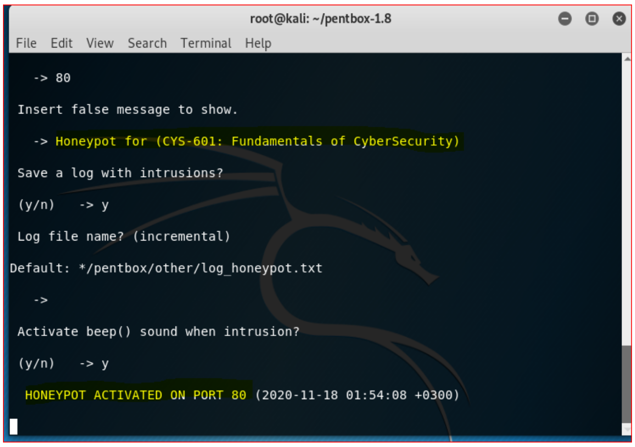
```
  INTRUSION ATTEMPT DETECTED! from 192.168.8.103:53001 (2020-11-18 01:29:15 +0300)
 -----------------------------
GET / HTTP/1.1
Host: 192.168.8.147
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/86.0.4240.198 Safari/537.36 Edg/86.0.622.69
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,appl
ication/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9


  INTRUSION ATTEMPT DETECTED! from 192.168.8.103:53002 (2020-11-18 01:29:16 +0300)
 -----------------------------
GET /favicon.ico HTTP/1.1
Host: 192.168.8.147
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
```

Fig 9: screenshots of info. Attacker in honeypot.

- Get statement specifies what the user is trying to extract from during the request. The default is favicon.ico.
- Host is the IP address
- User-Agent: Name of the Browser followed by the Windows OS is the browser engine used by Mozilla
- Accept: The type of the data the user wants to receive.
- Accept language - Language in which the data will be received.
- Connection: Type of connection. Persistent or Non-persistent. If persistent then connection is not closed after every request.

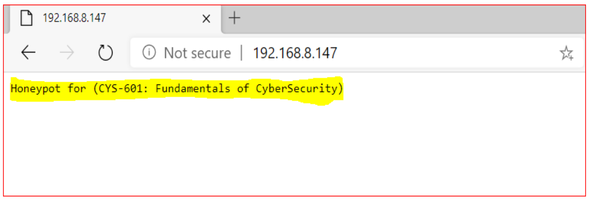
2.4.2 MANUAL CONFIGURATION:

In this step will be to insert port to open (we insert 80), and a false message to show. Then, Honeypot activated on port 80. If too went URL (http:// localhost) on web page will show this message. (Honeypot for (CYS-601: Fundamentals of CyberSecurity)).



```
  -> 80

 Insert false message to show.

   -> Honeypot for (CYS-601: Fundamentals of CyberSecurity)

 Save a log with intrusions?

 (y/n)   -> y

 Log file name? (incremental)

Default: */pentbox/other/log_honeypot.txt

   ->

 Activate beep() sound when intrusion?

 (y/n)   -> y

  HONEYPOT ACTIVATED ON PORT 80 (2020-11-18 01:54:08 +0300)
```

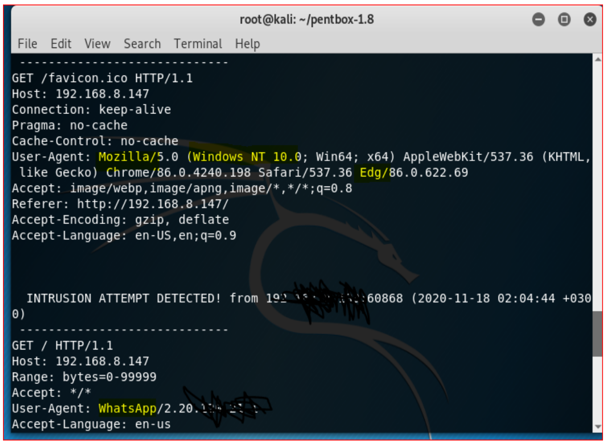
Fig 10: screenshots of setting manual configuration.



Honeypot for (CYS-601: Fundamentals of CyberSecurity)

Fig11: screenshot of message success honeypot.

In same time, but in another side in honeypot to show warning message from the attacker and printing its data.



```
 -----------------------------
GET /favicon.ico HTTP/1.1
Host: 192.168.8.147
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/86.0.4240.198 Safari/537.36 Edg/86.0.622.69
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Referer: http://192.168.8.147/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9



  INTRUSION ATTEMPT DETECTED! from 19[redacted]60868 (2020-11-18 02:04:44 +030
0)
 -----------------------------
GET / HTTP/1.1
Host: 192.168.8.147
Range: bytes=0-99999
Accept: */*
User-Agent: WhatsApp/2.20.[redacted]
Accept-Language: en-us
```

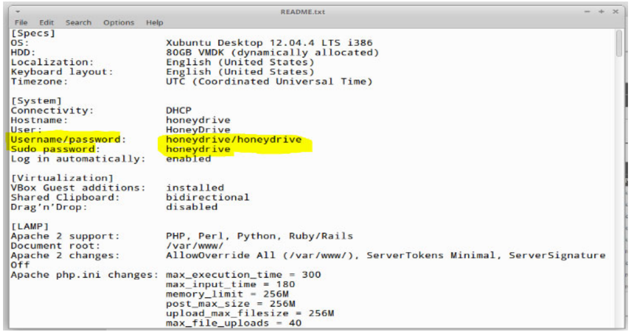
Fig 12: screenshots of info. Attacker in honeypot.

They can view all attacker who opened (http:// IP address) on different OS (Windows, Mac, Linux). or any one you want sending URL in WhatsApp. [14]

3 Honeydrive

HoneyDrive is the best honeypot Linux distro. It is usually considered as a virtual appliance (OVA) with Xubuntu Desktop 12.04.4 LTS edition installed. It holds over 10 pre- configured and pre-installed honeypot software packages like Dionaea, Kippo SSH honeypot and Amun malware honeypots, Glastopf web honeypot, Honeyd low-interaction honeypot and Wordpot, Conpot SCADA/ICS honeypot, Thug and PhoneyC honeyclients and more. It also includes several useful programs that are usually pre-built text, as well as units for processing, visualizing and analyzing data that are captured, like Honeyd-Viz, Kippo-Graph, STACK ELK, DionaeaFR and other. Finally, nearly 90 known forensics, malware analyzes and related web monitoring tools are also existing in the divide.[15]

The most significant file is the **README** file on desktop contains all the details to the configurations of the various honeypots and the malware scanning tools. The paths, passwords are all stored in the README files.



```
[Specs]
OS:                      Xubuntu Desktop 12.04.4 LTS i386
HDD:                     80GB VMDK (dynamically allocated)
Localization:            English (United States)
Keyboard layout:         English (United States)
Timezone:                UTC (Coordinated Universal Time)

[System]
Connectivity:            DHCP
Hostname:                honeydrive
User:                    HoneyDrive
Username/password:       honeydrive/honeydrive
Sudo password:           honeydrive
Log in automatically:    enabled

[Virtualization]
VBox Guest additions:    installed
Shared Clipboard:        bidirectional
Drag'n'Drop:             disabled

[LAMP]
Apache 2 support:        PHP, Perl, Python, Ruby/Rails
Document root:           /var/www/
Apache 2 changes:        AllowOverride All (/var/www/), ServerTokens Minimal, ServerSignature
Off
Apache php.ini changes: max_execution_time = 300
                         max_input_time = 180
                         memory_limit = 256M
                         post_max_size = 256M
                         upload_max_filesize = 256M
                         max_file_uploads = 40
```

Fig13: screenshot of readme files.

3.1 Kippo

It is considered as a SSH medium interaction Honeypot which is written in in Python.

The main work of Kippo is to record all the brute forces or attacks on the system, collect all the information about the entire shell interaction made by the attacker.

Kippo consists of a fake filesystem, tricking the attacker into thinking that it is a legitimate one.[16]

3.2 Main characteristics of Kippo:

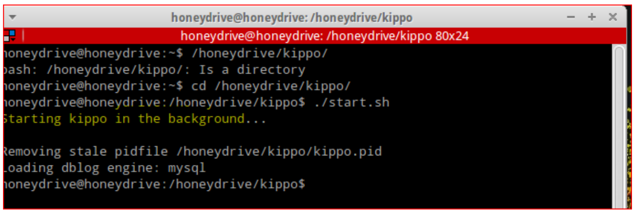
- It provides Fake file system and capability add or remove files with ability to add/remove files. The system resembles a Debian 5.0 installed

-Adding contents to important files like passwords, databases, etc.

-Session logs are stored, and complete analysis of the user is done using kippo-graph.

3.3 To Start Kippo

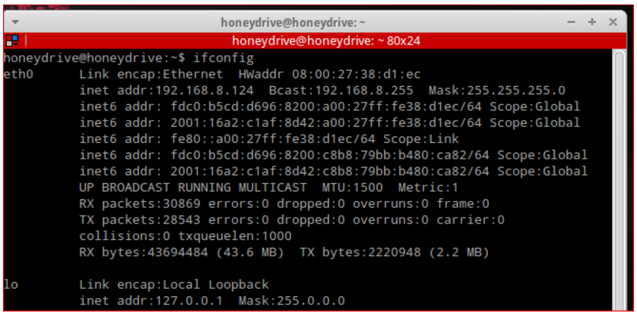
1.Browser to your /honeydrive/kippo folder.
2. Start kippo using the command ./start.sh
3. You will r receive a message which says kippo running in background.
4-Kippo successfully started.


honeydrive@honeydrive: /honeydrive/kippo
honeydrive@honeydrive: /honeydrive/kippo 80x24

```
honeydrive@honeydrive:~$ /honeydrive/kippo/
bash: /honeydrive/kippo/: Is a directory
honeydrive@honeydrive:~$ cd /honeydrive/kippo/
honeydrive@honeydrive:/honeydrive/kippo$ ./start.sh
Starting kippo in the background...

Removing stale pidfile /honeydrive/kippo/kippo.pid
Loading dblog engine: mysql
honeydrive@honeydrive:/honeydrive/kippo$
```

Fig 14: Screenshot of command to start ssh.

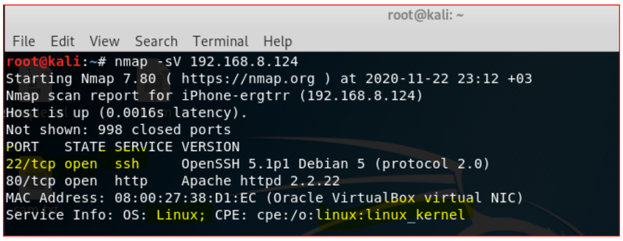
Using termial you can see IP address for honeydrive.



```
honeydrive@honeydrive:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:38:d1:ec
          inet addr:192.168.8.124  Bcast:192.168.8.255  Mask:255.255.255.0
          inet6 addr: fdc0:b5cd:d696:8200:a00:27ff:fe38:d1ec/64 Scope:Global
          inet6 addr: 2001:16a2:c1af:8d42:a00:27ff:fe38:d1ec/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe38:d1ec/64 Scope:Link
          inet6 addr: fdc0:b5cd:d696:8200:c8b8:79bb:b480:ca82/64 Scope:Global
          inet6 addr: 2001:16a2:c1af:8d42:c8b8:79bb:b480:ca82/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:30869 errors:0 dropped:0 overruns:0 frame:0
          TX packets:28543 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:43694484 (43.6 MB)  TX bytes:2220948 (2.2 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
```

Fig 15: Screenshot of command to show ipaddress.

And the attacker in Kali Linux you can see any ports open and show information using nmap tool.



```
root@kali:~# nmap -sV 192.168.8.124
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-22 23:12 +03
Nmap scan report for iPhone-ergtrr (192.168.8.124)
Host is up (0.0016s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.1p1 Debian 5 (protocol 2.0)
80/tcp open  http    Apache httpd 2.2.22
MAC Address: 08:00:27:38:D1:EC (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Fig 16: screenshots of command nmap tool on kali linux.

After viewing the open ports that can be attacked, here I will attack through SSH port using medusa tool.

3.4 What medusa tool and why SSH port:

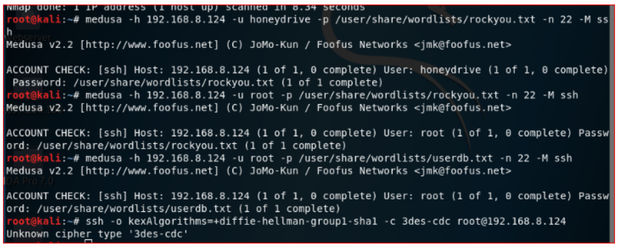
Medusa is a Brute-force tool to check if you can log in with a password or username from your list (List Passwords or List users)

The good thing about the tool is that it accepts many services like ssh ftp http and lots of services that allow brute-force attack.

Using this command to install in Kali Linux:

```
sudo apt-get install medusa
```

SSH was created to work as a replacement for both Telnet and even for shell protocols that are remote and unsecured which send information, especially passwords as plaintext, make them vulnerable to capture and discovery utilizing package analysis. [17]



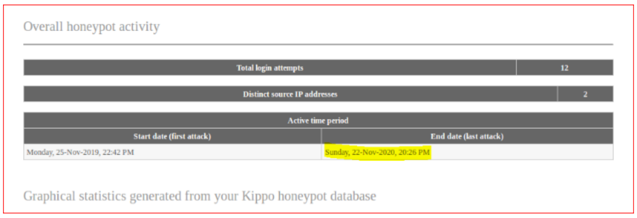
```
Nmap done: 1 IP address (1 host up) scanned in 8.34 seconds
root@kali:~# medusa -h 192.168.8.124 -u honeydrive -p /user/share/wordlists/rockyou.txt -n 22 -M ss
h
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 192.168.8.124 (1 of 1, 0 complete) User: honeydrive (1 of 1, 0 complete)
 Password: /user/share/wordlists/rockyou.txt (1 of 1 complete)
root@kali:~# medusa -h 192.168.8.124 -u root -p /user/share/wordlists/rockyou.txt -n 22 -M ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 192.168.8.124 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Passw
ord: /user/share/wordlists/rockyou.txt (1 of 1 complete)
root@kali:~# medusa -h 192.168.8.124 -u root -p /user/share/wordlists/userdb.txt -n 22 -M ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 192.168.8.124 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Passw
ord: /user/share/wordlists/userdb.txt (1 of 1 complete)
root@kali:~# ssh -o kexAlgorithms=+diffie-hellman-group1-sha1 -c 3des-cdc root@192.168.8.124
Unknown cipher type '3des-cdc'
```

Fig 17: screenshots of brute-force using medusa.

3.5 Kippo-gragh

The Kippo-Graph is a scenario visualizing statistics from the Kippo SSH honey pot. AND, data and statistics on the input are also displayed giving an overview of the work within the system and there is a live playback capability of the sessions captured.

In screenshots analysis of the attacker's operations:



Overall honeypot activity

Total login attempts	12

Distinct source IP addresses	2

Active time period	
Start date (first attack)	End date (last attack)
Monday, 25-Nov-2019, 22:42 PM	Sunday, 22-Nov-2020, 20:26 PM

Graphical statistics generated from your Kippo honeypot database

Fig 18: screenshots of total number attacker attempts accessed.

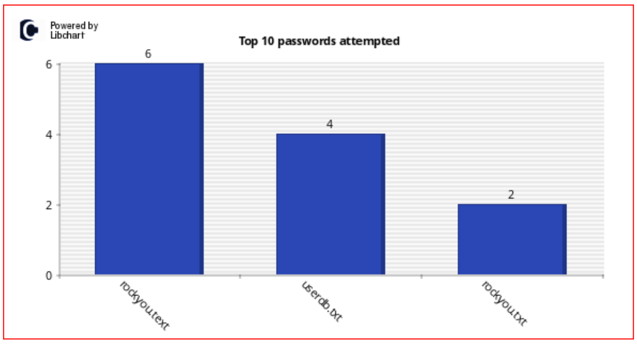


Fig 19: screenshots of top 10 passwords attempts.

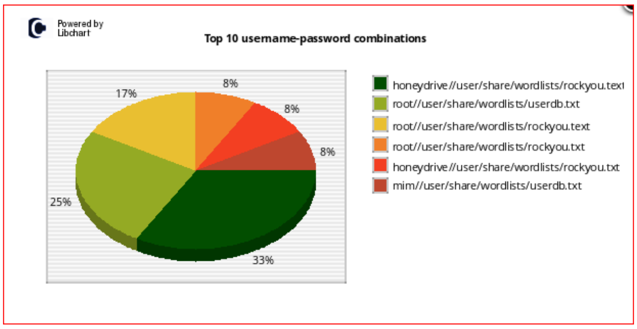


Fig 20: screenshots pf top 10 username/password combination.

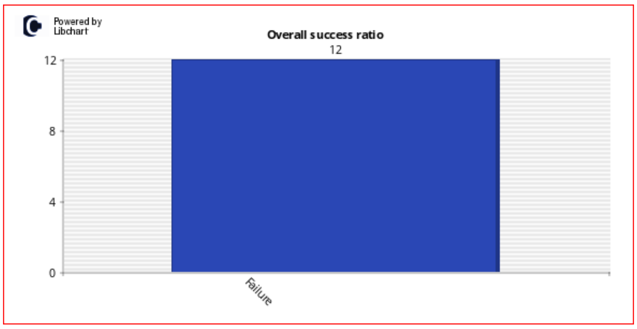


Fig 21: screenshots of overall failure/success ratio.

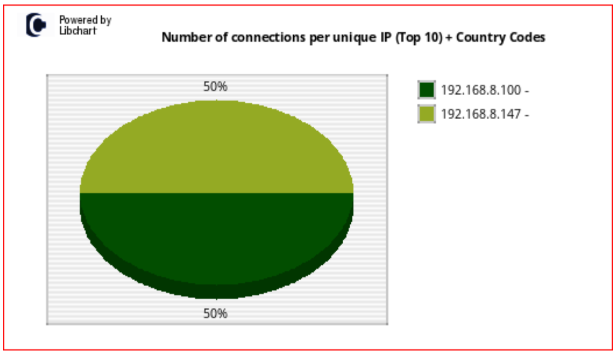
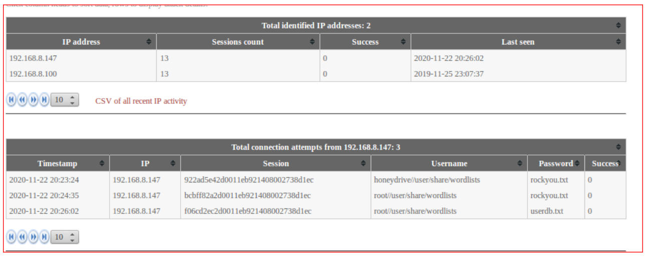


Fig 22: screenshots of connection ip address.



Total identified IP addresses: 2			
IP address	Sessions count	Success	Last seen
192.168.8.147	13	0	2020-11-22 20:26:02
192.168.8.100	13	0	2019-11-25 23:07:37

Total connection attempts from 192.168.8.147: 3					
Timestamp	IP	Session	Username	Password	Success
2020-11-22 20:23:24	192.168.8.147	922ad5e42d0011eb921408002738d1ec	honeydrive//user/share/wordlists	rockyou.txt	0
2020-11-22 20:24:35	192.168.8.147	bcbff82a2d0011eb921408002738d1ec	root//user/share/wordlists	rockyou.txt	0
2020-11-22 20:26:02	192.168.8.147	f06cd2ec2d0011eb921408002738d1ec	root//user/share/wordlists	userdb.txt	0

Fig 23: screenshots of total attempts connection from ip address.

4 Legal issues related to honeypot:

Most of research in this filed has complemented that there are two main legal spectrums that contemplate attractions:

1- Deception: A trap is when a person engages a criminal to do something that he was not supposed to do otherwise. Honeypots should generally be used as a defensive detective tool, not an abusive method of attracting intruders.

2. Privacy: The second major concern is what information is being tracked: operational data and transaction data.

Operational data includes things like user addresses, header information, etc., while the transactional data includes keystrokes, pages visited, information downloaded, chat logs, e-mail, etc., the operational data is safe to track without security threats because IDS routers and partitions Firearms are already following him. The primary concern is the transaction data. [18]

5. Security categories in Honeypots

Honeypots is a highly flexible and easy-to-use security tool with many different security applications. They don't fix a single problem. Instead, they have multiple uses, such as blocking, disclosing, or gathering information. Detecting, preventing and responding to attacks

5.1 Prevention

Honeypots cannot prevent an unexpected attack, but they can detect it. In some cases, this prevents hackers from directly attacking the server. Preventing robotic attacks such as heat-ups and automatic roots. It can provide protection by providing a firewall, also by using strong passwords, and setting encryption technologies, digital signatures and certificates, and it can also provide known security services to the organization or company.[19]

5.2 Detection

Honeypots provide intruder detection similar to the interference disclosure system's functionality to protect facilities when unauthorized activity appears. Determine where the failure was in prevention. The discovery helps us to know whether the system has been compromised or not, where it was breached and the identity of the hacker as well, but it will not prevent hackers and hackers from attacking and penetrating the network or the system.[20]

5.3 Response

Honeypots provide accurate evidence of malicious activity and give information about the attack to prevent any of these in the future and initiate countermeasures.

IV. Conclusion

Honeypots are usually considered a technology with a very high flexibility which that can be functional and useful in different situations. Honeypot can be applied in very many forms. The honeypot is determined as needed. If the need for a simple honeypot is to use a low-interaction honeypot and save yourself the high risks involved in a high-interaction honeypot, then the purpose and need you want should be clearly defined and based on which the type of trap to be used is determined.

They are security tools that have many advantages. Specially, they gather data, with high value information. In addition to their ability to work effectively in environments with resource intensive, and they are considered as uncomplicated devices and finally they are valuable as they work in capturing and detecting the unauthorized activity.

We showed in this paper many information about honeypot and advantages and disadvantages ,and we implemented the almost plural network security tools, namely honeypot from pentbox and HoneyDrive3 and Nmap on Kali Linux and uses them to test run on an experimental setup to demonstrate how each, and can displayed the result of the penetration testing and the details of the attacker's device and locations, and these tools are used to improve the concept of security, protection and confidentiality within or outside the organization to avoid attacks, vulnerabilities and breaches.

References

[1] Fruhlinger, J. (2019, April 01). What is a honeypot? A trap for catching hackers in the act. Retrieved November 7, 2020, from https://www.csoonline.com/article/3384702/what-is-a-honeypot-a-trap-for-catching-hackers-in-the-act.htm

[2] Honeypot (computing). (2020, November 13). Retrieved November 11, 2020, from https://en.wikipedia.org/wiki/Honeypot_(computing)

[3] Arora, M., & CatchUpdatesHi, F. M. (2020, September 05). What Are Honeypots? Various Types Of HoneyPots. Retrieved November 8, 2020, from https://catchupdates.com/honeypots/

[4] "A Honeypot For Assholes": Inside Twitter's 10-Year Failure To Stop Harassment. (n.d.). Retrieved November 13, 2020, from https://ontd-political.livejournal.com/11567255.html

[5] Livshitz, I. (2020, January 05). Low, Medium and High Interaction Honeypot Security. Retrieved November 10, 2020, from https://www.guardicore.com/2019/1/high-interaction-honeypot-versus-low-interaction-honeypot/

[6] Honeypots For Network Security Information Technology Essay - Free Essay Example by Essaylead. (2017, July 15). Retrieved November 11, 2020, from https://essaylead.com/honeypots-for-network-security-information-technology-essay-1428/

[7] Benefits of Honeypots – There's More to Honeypots Than Wasting Hackers' Time. (2018, August 22). Retrieved November 11, 2020, from https://www.webtitan.com/blog/honeypots-how-far-can-you-go-in-wasting-a-hackers-time/

[8] Skoudis, E. (2008, January 04). What security risks do enterprise honeypots pose? Retrieved October 13, 2020, from https://searchsecurity.techtarget.com/answer/What-security-risks-do-enterprise-honeypots-pose

[9] Honeypot (computing). (2020, November 13). Retrieved November 15, 2020, from https://en.wikipedia.org/wiki/Honeypot_(computing)

[10] How To Establish a Honeypot on Your Network - Step by Step. (2020, September 29). Retrieved November 13, 2020, from https://www.comparitech.com/net-admin/how-to-establish-a-honeypot-on-your-network/

[11] NG, C. K., Pan, L., & Xiang, Y. (2018). Honeypot Frameworks and Their Applications: A New Framework. Singapore: Springer Singapore.

[12] PentBox Tutorial (A Penetration Testing Tool). (n.d.). Retrieved November 17, 2020, from https://www.hackingarticles.in/pentbox-tutorial-a-penetration-testing-tool/

[13] Kaspersky. (2020, September 10). What is a honeypot? Retrieved November 6, 2020, from https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot

[14] Toolsmith: HoneyDrive - Honeypots in a Box. (2014, October 03). Retrieved November 18, 2020, from https://holisticinfosec.blogspot.com/2014/10/toolsmith-honeydrive-honeypots-in-box.html

[15] -, R., By, -, Ranjithhttp://kalilinuxtutorials.comA nonchalant person with a dexterity for writing and working as a Engineer., Ranjith, A nonchalant

[16] person with a dexterity for writing and working as a Engineer., . . . -, B. N. (2019, June 19). Kippo - SSH Honeypot To Log Brute Force Attacks. Retrieved November 19, 2020, from https://kalilinuxtutorials.com/kippo-honeypot-brute-force-attacks/

[17] Download HoneyDrive 3. (2014, July 29). Retrieved November 10, 2020, from https://linux.softpedia.com/get/System/Operating-Systems/Linux-Distributions/HoneyDrive-102674.shtml

[18] Arora, M., & CatchUpdatesHi, F. M. (2020, September 05). What Are Honeypots? Various Types Of HoneyPots. Retrieved November 11, 2020, from https://catchupdates.com/honeypots/

[19] Tripwire Guest AuthorsDec 29, 2. S. (2019, December 17). Honeypots: A Guide To Increasing Security. Retrieved November 20, 2020, from https://www.tripwire.com/state-of-security/security-data-protection/honeypots-guide-increasing-security/

[20] Kaspersky. (2020, September 10). What is a honeypot? Retrieved November 20, 2020, from https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot