Assignment No: 5

Title: Implementation of Honeypot.

Problem Statement: Study and Implementation of Honeypot.

Objectives:

1. To learn the concept of Honeypot

2. To study the representation, implementation of Honeypot

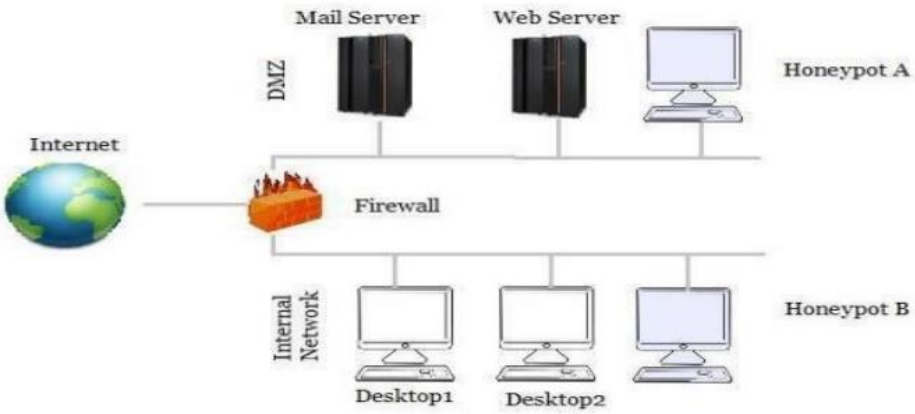
Theory:

Honeypot:

It is a computer system. There are files, directories in it just like a real computer. However, the aim of the computer is to attract hackers to fall into it to watch and follow their behavior. So we can define it as a fake system which looks like a real system. They are different than other security systems since they are not only finding one solution to a particular problem, but also they are eligible to apply variety of security problems and finding several approaches for them.

For example, they can be used to log Malicious activities in a compromised system; they can be also used to learn new threats for users and creating ideas how to get rid of those problems. Honeypots are security resources that have no production value; no person or resource should be communicating with them.

Any activity sent their way is suspect. Any traffic initiated by the honeypot means the system has most likely been compromised. Any traffic sent to the honeypot is most likely a probe, scan, or attack. With a honeypot, nothing is expected. To better understand the concepts of honeypots, let's take a look at the following example of honeypot deployments refer the figure :



The purpose here is to demonstrate to you that honeypots can come in many different flavors, and they can achieve different things. However, they are both honeypots because they share the same definition and concepts. With the intent using systems as a honeypots, to determine

if there is any unauthorized activity happening within your DMZ. Honeypots passively capture any traffic or activity that interacts with them .

Types of Honeypots:

There are two general types of honeypots:

Production honeypots :

Production honeypots are easy to use, capture only limited information, and are used primarily by companies or corporations. They are capturing a limited amount of information; mostly low interaction honeypots are used. security administrator watches the hacker's movements carefully and tries to lower the risks that may come from it towards the company.

Research honeypots :

Research honeypots are complex to deploy and maintain, capture extensive information, and are used primarily by research, military, or government organizations. The objective is to learn how to Protect a system better, they do not bring any direct value to the security of an organization Honeypots are increasingly used to provide early warning of potential intruders, identify flaws in security strategies, and improve an organization's overall security awareness.

"Honeypots can simulate a variety of internal and external devices, including Web servers, mail servers, database servers, application servers, and even firewalls. As a software development manager, we can regularly use honeypots to gain insight into vulnerabilities in both the software my team writes and the OS upon which we depend." A honeypot is a security resource whose value lies in being probed, attacked, or compromised. This means that whatever we designate as a honeypot, it is our expectation and goal to have the system probed, attacked, and potentially exploited.

Legal issues with honeypots:

While deploying and start using a honeypot, there are some legal issues that a person should know about. Every country has different laws regarding to honeypot usage and information capturing. These regulations are related to data security, collection of data and finally how to use honeypots. All these different laws are based on the quality of the data that a honeypot can capture and a person who is deploying it. Privacy and data leads us to confidentiality term in network security. Our example is being a network administrator in a company.

Practical implementation:

We are starting with low interaction honeypot and then continue on a middle level of interaction to finally conclude with a high level of interaction.

- Starting to honeypot: We started with Honeyd as low level interaction honeypot and then we will move on medium level interaction honeypots. Every honeypot has specific and different attitudes. We will explain them one by one.
- HoneyBOT : It is a medium interaction honeypot for windows.

A honeypot creates a safe environment to capture and interact with unsolicited and often malicious traffic on a network. HoneyBOT is an easy to use solution ideal for network security research or as part of an early warning IDS. The logging capability of a honeypot is far greater

than any other network security tool and captures raw packet level data even including the keystrokes and mistakes made by hackers.

The captured information is highly valuable as it contains only malicious traffic with little to no false positives. Honeypots are becoming one of the leading security tools used to monitor the latest tricks and exploits of hackers by recording their every move so that the security community can more quickly respond to new exploits.

- **How does it work?**
  HoneyBOT works by opening a range of listening sockets on your computer which are designed to mimic vulnerable services. When an attacker connects to these services they are fooled into thinking they are attacking a real server. The honeypot safely captures all communications with the attacker and logs these results for future analysis. Should an attacker attempt an exploit or upload a rootkit or trojan to the server the honeypot environment can safely store these files on your computer for malware collection and analysis purposes. Following figure shows implementation of honeypot.

- **Installing and Securing Your Honeypot**:
  A honeypot is intentionally put in harms way so it is critical to carry out some security precautions on your honeypot computer before deployment on any network. Install HoneyBOT on a dedicated computer or virtual machine. Update the operating system with security updates and use an antivirus product. You want your honeypot to be as free as possible from legitimate traffic so in broad terms we can consider any traffic to the honeypot to be malicious in nature. Remember that we are attracting attackers to intrude into this system so precautions are important.

- **Network Placement**:
  If you place HoneyBOT inside the internal network where it is secured by perimeter defences it should never to be attacked. Any malicious traffic captured in this situation would indicate that another computer inside the network is already compromised or that the perimeter defences have been breached. In this configuration HoneyBOT is acting as an intrusion detection system.

- **Windows Services, SMB and NetBIOS**:
  You should disable any Windows services that are not required for the machine to operate as they offer an attacker a possible avenue of attack. HoneyBOT cannot listen on a port that is already in use by a Windows service. Some of the services that you may choose to disable include Messenger, ClipBook, COM+, FTP Publishing, SMTP, SNMP, TCP/IP NetBIOS Helper, Telnet, WWW Publishing. SMB (CIFS) provides name resolution, network browsing and printing services over TCP/IP. To disable SMB open the Network Connections window, right click the adapter and select Properties and uninstall Client For Microsoft Networks and File And Printer Sharing. SMB services may also be provided over NetBIOS (NBT). To disable NetBIOS open the Device Manager window, select Show Hidden Devices, expand Non-Plug And Play Drivers and disable NetBios Over TCP/IP.

- **Firewall**:
  A firewall will prevent unsolicited connections from reaching your computer. In order for HoneyBOT to communicate you need to customise your firewall rules to allow incoming connections. If you are using a software firewall you should create an exception for HoneyBOT.

- **HoneyBOT Options**:
  Select Options from the View menu to configure HoneyBOT. Automatically Start Engine: The server engine will start automatically when the application is started. Enable Sound Alert: Plays a short sound each time an event occurs. Capture Binaries: If this option is enabled HoneyBOT will attempt to capture malware and other files and save them to the \HoneyBOT\Captures\ folder. If this option is enabled you should add an exception in your antivirus software to exclude this folder from its scan. Automatically Rotate Log: Each day at midnight HoneyBOT will save the current log file and start a new log file. Server Name: The alias name of the HoneyBOT server given to the remote machine.

- **Email Alerts**: Enter your email address and SMTP server information to receive daily email updates from HoneyBOT.

- **Exports:** Select the Export Logs to CSV option to create a daily extract of your log file as a CSV file. Exported logs are saved in the \HoneyBOT\Logs\ folder. You can also choose to participate in the centralised log program and have your log files uploaded to the HoneyBOT website.

- **Syslog :** Select to send connection events to a Syslog server. Enter the Syslog server IP address and port.

- **Bindings**: Only applicable to multihomed machines. Provides support for multiple networks so HoneyBOT can bind to one or all detected networks. Enter the IP address that you want HoneyBOT to bind to. If the IP address is not valid and more than one IP address is available you will be prompted to select an address when the server engine starts.

- **Updates:** Select to have HoneyBOT check for updates on startup. There are two update types that may occur. A service update is a minor update to the server listening services, if a service update is available you will be prompted to install the update. An application update notification will occur if a new version of HoneyBOT is available.

- **Services and Profiles** : Select to edit the TCP and UDP services started by the HoneyBOT engine. You can add a new port, edit and disable an existing port, or delete the port configuration entirely. By default HoneyBOT will open more listening ports than a typical computer and this may alert an attacker to its presence. You can choose to limit your honeypot exposure to just a handful of ports that more closely resembles a real operating system. By loading a profile you can quickly emulate common operation system setups like an SQL Server, IIS Server, Exchange Server, etc.

- **Whitelist :** You may find HoneyBOT is interacting with services on your network that are legitimate and not a cause for alarm. You can whitelist the source machine by adding the IP and port to the whitelist settings. When a machine is whitelisted HoneyBOT will no longer accept connections from that machine.

- **Debug :** The debug window will display application messages and socket events that occur during typical application operation.

- **Event Navigation**: The event tree on the left shows the ports that have been probed and remote addresses that have connected to HoneyBOT. The event list at the top right will display all connection attempts including the attributes of the connection. The packet list at the bottom displays each packet transmitted and received between the remote machine and the HoneyBOT server.

Advantages of honeypots:

1. There are many security solutions available in the market. Anyone can browse the variety of choices through internet and find the most suitable solution for their needs.
2. Honeypots can capture attacks and give information about the attack type and if needed, thanks to the logs, it is possible to see additional information about the attack.
3. New attacks can be seen and new security solutions can be created by looking at them. More examinations can be obtained by looking at the type of the malicious behaviors.
4. It helps to understand more attacks that may happen. Honeypots are not bulky in terms of capturing data.
5. They are only dealing with the incoming malicious traffic. Therefore, the information that has been caught is not as much as the whole traffic. Focusing only on the malicious traffic makes the investigation far easier.

Disadvantages of honey pots:

1. We can only capture data when the hacker is attacking the system actively. If he does not attack the system, it is not possible to catch information.
2. If there is an attack occuring in another system, our honeypot will not be able to identify it. So, attacks not towards our honeypot system may damage other systems and cause big problems. There is fingerprinting disadvantage of honeypots.
3. It is easy for an experienced hacker to understand if he is attacking a honeypot system or a real system. Fingerprinting allows us to distinguish between these two. It is a not a wanted result of our experiment.

Conclusion:

Hence, we have successfully studied concept of Honeypot in which we have set different network setting and set different drivers to identify unauthenticated access in our system.