IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Honeypot: A Way to Capture Attackers

Prashant Khanpara, Dr.Vivek Kumar Prasad

Computer Engineer, Professor-CSE Dept.
Department of computer science and engineering
Nirma University, Ahmedabad,India

Abstract : This article presents Honeypot, a novel network security mechanism. The basics of honeypots, their use in modern computer networks, including their employment in educational settings are all covered in this study. The different types of honeypots are described, like the Production honeypot, Research honeypot. The benefits and drawbacks of honeypots are further examined. Future research in the field of honeypots, including possible improvements to the framework, is considered.

Keywords: IDS (Intrusion detection system), Network security, Honeypots, Honeynets and Honeyd Virtual Honeypot.

I. INTRODUCTION :

Network security has grown more critical to individual windows users, businesses, and the military. The background of security provides a clearer knowledge of how security technology emerged, which was a key worry with the development of the internet. Numerous security dangers were made possible by the structure of the internet itself. The potential for assaults to be sent through the network can be decreased by changing the internet's design. Knowing the attack tactics makes it possible for the right security to develop. Network security in the context of networking refers to the rules and guidelines set forth by the network administrator to control and prevent illegal access to, use of, modification of, or denial of the computernetwork and its resources.

Data access on a network must be permitted, and thenetwork administrator has authority over this process. By choosing or receiving a credentials for authentication, members can access info and programmes that lie within their scope. Cryptography, encryption-decryption, biometrics, firewalls, intrusion detection systems (IDS), and honeypots are further techniques for network security.

Encryption: It involves transforming a plaintext into a codeword known as cipher message.
Decryption: It involves decryption of encrypted data in order to recover the original information.
Cryptography: Prior to the contemporary era, encrypting,the transformation of data from a understandable state to seeming absurd was almost synonymous.
Intrusion Detection System (IDS): It examines all trafficon the network to see any suspicious behavior that could point to a system or network assault by someone trying toaccess or breach a system.
Firewall: A system that restricts network access among a number of different networks.

Biometrics: In order to establish identification, this technology examines some certain set of a user's vital data.
HoneyPot: A honey pot is a type of Internet computer security measure that is specifically designed to draw in and "catch" users who try to break into the computers of others.

II. RELATED WORK :

The tools currently in use for identifying hackers are [1]:

- The Deception Toolkit Version 0.1, created by Fred Cohen, was the first solutions made available to the industry and was released in 1997.
- The Honeynet Project was established in 1999, and papers from the series "Know Your Enemy" were released.
- In order to trap and monitor worm activity, the honeypot was first used about 2000–2001. Many businesses have used honeypots to look for new risks and to look for assaults.
- A honeypot is deployed in 2002 to find and catch an undiscovered assault in the wild. The honeypot not only stops the user from entering accounts inappropriately, but also finds him. Additionally, it displays a list of assaults and tallies the number of appearances. According to certain studies, it can be utilized in the army to find unidentified patterns[3].

Categorization factor	Categories of Honeypot	Brief description
Purpose of Honeypot	Production Honeypot	A Production honeypot is one used within an organization and help to mitigate risk.
	Research Honeypot	A Research honeypot is used to gain the information about the hacker's or attacker's community and does not add any direct value to the organization.
Level of Interaction with Attacker	Low- Interaction Honeypot	The low-interaction honeypots are the easiest to implement. Basic services such as Telnet and FTP are emulated on low interaction honeypots.
	Medium- Interaction Honeypot	In terms of interaction, this is a little more advanced than low-interaction honeypots, but a little less advanced than high-interaction honeypots.
	High- Interaction Honeypot	High-Interaction honeypots are time-consuming to design, manage and maintain. These are generally used to gather the attacker's information for analysis. Information and evidence gathered for analysis are bountiful. The goal of a high interaction honeypot is to give the attacker access to a real operating system where nothing is emulated or restricted.

III. WHAT EXACTLY IS HONEYPOT?

- A computer system known as a "honey pot" is designed specifically to draw in and "capture" attackers who try to access other computers.
- It occasionally behaves like a genuine OS to the intruder to be poked or assaulted, or it includes some valuable data.
- It serves as a ruse. Your infiltrator's goal is to find the Honeypot and attempt to enterit. A honeypot's function is to identify attacks, gather information from them, and then utilize that knowledge to strengthen security.
- A network administrator learns about the hazards that are currently present on their network. A honeypot can be used to check for network or OS system vulnerabilities. Additionally, it may be used to monitor someone who has exposure to the Honeypot's activity.
- Honeypots are a special tool for understanding hacker strategies.

IV. TYPES OF HONEYPOTS :

Two criteria can be used to classify honeypots:

- The honeypot's purpose and
- The extent of contact with the assailant

Based on these two categorization criteria, the types of honeypots are summarized in the table below. Honeypots can be divided into two types based on their intended use: producing honeypots and research honeypots. We can divide honeypots into three groups based on the interaction.

A. CLASSIFICATION ACCORDING TO PURPOSE:

1. Production Honeypot:

Production The main purpose of honeypots [5] is detection. They often perform an advanced detection function as an extension to intrusion detection systems.

A honeypot makes it possible to defend the cost of afirewall. Someone from management could think there are no assaults on the network if there is no proof that there have been any. As a result, they can advise against making security investments as there are no dangers. A honeypot records information about attacks. Information about monthly occurred attacks data can be obtained from the system. Employee attacks are considerably more importantsince they often involve a network account with a variety of user privileges. Many times, networks are open to the local network but closed to the outside world. An individual with authorized access to the internal network might thus provide an ambiguous threat. You may determine if someone has harmful intents by looking at their behavior on honeypots. A network folder containing fictitious sensitive papers, for example, may be created. A worker with good intentions wouldn't duplicate the files, but if the files are recovered, it may be discovered that he is a hacker.

Another advantage, and maybe the most important, is that a Honeypot identifies threats that other security systems do not notice. An intrusion detection system (IDS) requires a database with regularly updated signatures assaults. Nepenthes is an example of a producing honeypot"[3].While they were working on "Nepenthes," Georg Wicherski created a programme called "mwcollect." In February 2006,Mwcollect was absorbed into Nepenthes. Its purpose is to detect assaults.

2. RESEARCH HONEYPOT:

In another case, a study honeypot [5] is utilized. To discover the strategies and methods of the attacker, a study honeypotis employed. When hacking a system, it serves as a watch post to observe how a hacker is acting. In this instance, the intrusive person is permitted to remain and spill his secrets. The honeypot operator learns about hacking resources and procedures. The techniques used by the hacker are often discovered by system administrators after a system has been

infiltrated, yet there is no documentation of their use. A honeypot provides an actual account of the attack's execution. Research honeypots are used to collect a lot of data, but they are difficult to setup and manage. They can take a long time. They are useful for learning about hackers but have minimal impact on an organization's actual security. They are often used by organizations interested inlearning more about risks research, such as colleges, government, the military, or huge enterprises. "Honeynets"are examples of such research honeypots. Simply put, a honeynet is a collection of two or more honeypots.

B. CATEGORIZATION BASED ON INTERACTION LEVEL

1) LOW-INTERACTION HONEYPOTS:

Low-interaction honeypots [4][12] are simple to install and setup to any service. The honeypot is simple to set up and manage. To protect users from completely exploiting the system, the administrators must maintain "patch management"[5] on the host computer and closely examine the alarm systems that notify the administrators of the assault. Patch management is a branch of systems administration that entails collecting, testing, and deploying many patches (code modifications) to a computer system under administration. Low-interaction honeypots pose the least danger. The low-interaction honeypot is only useful for collecting common attacks patterns and is useless for interacting with or uncovering unknown attack patterns.

HONEYD:

Honeyd [6][11] is a programmed that allows the creation of many virtual honeypots on a single system, each with its own set of features and services.

Honeyd is a free framework for creating virtual honeypots. Honeyd allows you to run honeypots with multiple personalities and applications on the same system. Honeyd emulates the IP stack of several operating systems and bindsa specified script to a desired port to mimics a certain service. From a Windows NT workstation to an AIX box (Advanced Interactive executive box), Honeyd is capable of convincing network fingerprinting tools that they are dealing with a legitimate OS. It is an IBM-developed commercial operating system based upon UNIX System V [6]. IP stacks from various routers can also be mimicked. Honeyd makes use of a Nmap fingerprint file. Nmap employs a tree of properties and values in data structures that consumers are unaware of when it keeps a fingerprint in memory. However, there is a special ASCII-encoded version that Nmap may produce for clients when a computer cannot be identified) [7] that is used to describe various types of their IP layers and OS. The intended OS and the appropriate TCP/IP flags are used to modify a packet's personality before Honeyd sends it into the IP stream. Moreover, Honeyd can simulate sophisticated network structures and their properties. Virtual networking topologies may be constructed using multiple router brands, internet connection delay, and packet drop. When mapping the network using tools such as trace route, internet traffic seems to be followed by the specified devices and network connections. VM are simple to set up. A operating system tells Honeyd what sort of operating system to use, how to respond to closed ports, and what type of service is listening on whatever port. Honeyd can connect a program to a network port. The program might be a typical shell script that emulates a specific service. Most scripts are constructed as state machines, in which a command resultsin a particular action or advances to a new state containingnew possibilities.

2) MEDIUM-INTERACTION HONEYPOTS:

This is somewhat more sophisticated than low grade interaction honeypots, but slightly less advanced than high level interaction honeypots in terms of interaction.Medium level Interaction honeypots still lack an actual operating system, but the false services they provide are more technically complex. Middle range interaction Honeypots, like lower - level interaction Honeypots, are implemented as a programme on the network host OS andjust the emulated services are made available to the public.However, because the simulated services on medium level interaction Honeypots are more powerful, the likelihood of failure is greater, making the usage of middle range interaction Honeypots riskier.

"Nepenthes" is an example of a medium contact honeypot [7][8].

NEPENTHES:

Nepenthes is a Honeypot with a medium degree of involvement that emulates known vulnerabilities and traps worms as they try to infect it.

Nepenthes not only detects the attacker, but also provides data on new strategies employed by the attacker. It gives false services to the attacker, who is more tech competent.It is more dangerous than a low-level honeypot.

3) HIGH- INTERACTION HONEYPOTS:

Designing, managing, and maintaining such types of honeypots takes time. The purpose of a high-level interaction honeypot is to provide the attacker with access to a real OS that is neither simulated or limited in any way.Because they provide a whole operating system, the danger is quite significant. An intruder might simply exploit the compromised platform to target other devices or cause bandwidth losses by generating massive traffic. "Honeynets" are an example of a high-interaction honeypot.

HONEYNET:

- A honeynet is made up of two or more honeypots on a network [10].
- A honeynet is typically used to monitor a bigger and/or more diversified network when a single honey trap maynot be adequate.
- Honeynets and honeypots are typically used as components of larger network intrusion detection systems.
- The Honeynet Project's founder Lance Spitzer published the paper "To Build a Honeypot" in 1999, which served as the foundation for the honeynet concept.
- A honeynet provides genuine OS in which attackers may interact, making it a high-interaction honeypot. This high level of contact may teach us a lot about invaders, including how they break in systems, how they interact, and why they attack systems.
- Honeynets achieve this by establishing a network of systems. Honeynets achieve this by establishing a network of systems.

- This network is highly confined, with complete control and collection of all incoming and outgoing traffic.
- Every system connected to the internet serves as a honeypot or a target for attacks.
- However, these honeypots are fully working systems, similar to those found in the majority of corporations today. When these systems are targeted, Honeynets record every action taken by the attacker.
- This data then informs us a lot about the risks we face today.

V. ADVANTAGES OF HONEYPOT:

When compared to the most widely utilized security techniques today, honeypots offer numerous different benefits [9][12].

- Small Data Sets - Only the traffic that arrives to honeypots is of interest. They don't care about determining whether or not packets are legitimate or about network traffic congestion. As a result, they only collect a little amount of data; there are no huge data logs or daily hundreds of warnings. even though the data set is little, the data is valuable.
- Minimal Resources - They use fewer resources since they only catch bad activity. A retired orinexpensive system can be used as a honeypot.
- They are quite flexible and fundamental. No complex algorithms need to be developed, statetables need to be updated, or signatures need to be kept up to date.

VI. DISADVANTAGES OF HONEYPOT:

- Honeypots contain a number of hazards and drawbacks. Although they are small in number, these drawbacks [9][12] prohibit honeypots from totally replacing your present security methods.
- Limited Vision - When an attacker interacts directly witha honeypot, the interaction is tracked and recorded as the only activity. Attacks on other system components won't be noticed until the honeypot is also in danger.
- Fingerprinting When an attacker is able to identify a honeypot's true identity based on specific anticipated characteristics or behaviours, this is known as fingerprinting. A small error, such as a misspelt word in service emulation, might serve as a honeypot signature.
- High degree of risk- There is a high level of danger with high level interaction honeypots since they provide an actual operating system to be explored or attacked.

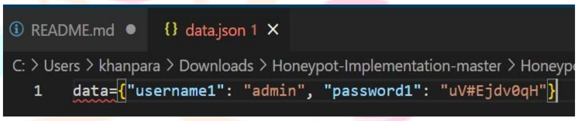
VII. FUTURE WORK:

I've given a basic summary of what honeypots are and what they're used for in this paper. I've spoken about the many varieties of honeypots, such as production honeypots, research honeypots, low level interaction honeypots, medium level interaction honeypots, and high-level interactionhoneypots. The amount of engagement of your honeypot, forexample, is determined by what you intend to utilize it for. Ahoneypot is a relatively new technology that is becoming increasingly popular, and will become even more so as practical solutions that are simple to operate and manage become available. Because they can be used to gather data onattackers and other threats, I assume they will be helpful in computer forensics investigations.

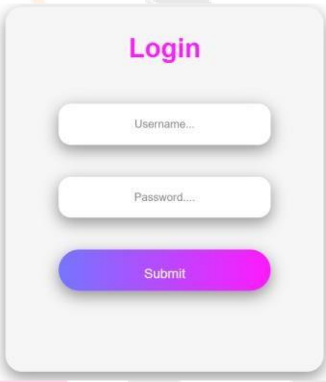
VIII. IMPLEMENTATION:

We attempted to construct a Honey-Pot-like server in this project that would function as a proxy server for any primary servers. Attacks conducted against any major servers are monitored using Honey-Pot. The system designers build the system update in order to close all system flaws by examining the types of assaults. As the title indicates, it will be a building that resembles a honeypot rather than a real honeypot. Not only will our system log IP addresses and locations, but it will also snapshot the user's computer so that the photos can be examined afterwards and the precise behaviors may be identified. This technique is required because, in additionto tracking the user's IP address, collecting pictures might provide a clear picture of any anomalous conduct.

1. First we run HashConversion.py file so it will create id and password for the login in json file. The username and password of a specific user are contained in this data stored in a JSON file, and this user may use these credentials to connect into a web server.

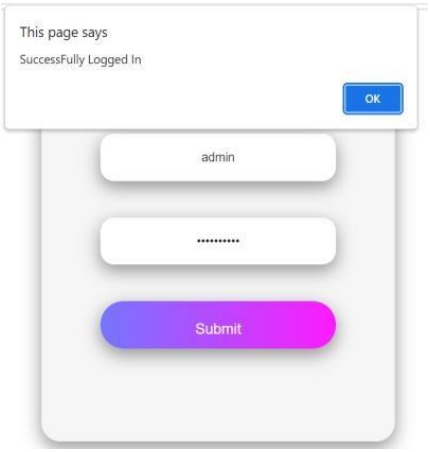


2. Now we input the credentials obtained from json data and go to the Login page.

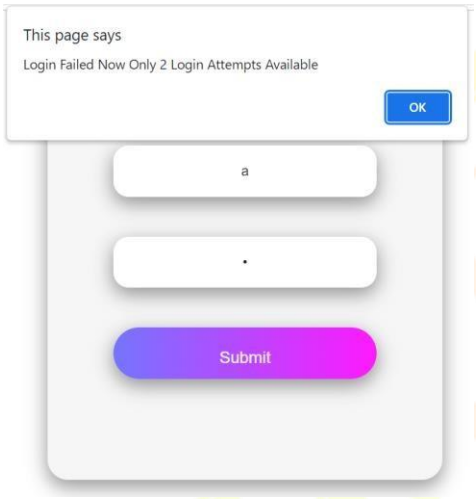


3. If your username and password are correct and we are logged in successfully then it will redirect us to nirma university website.

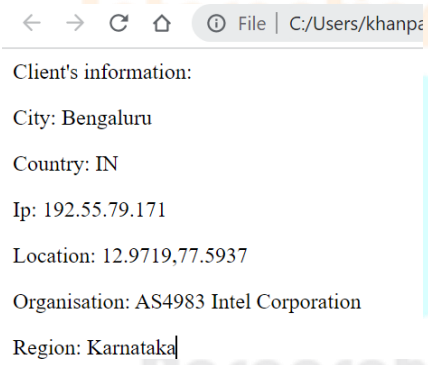
```
admin
vtop
1
\x03\x03\x16\x03\x03\x1612233werewewwwwdvc123wer
\x03\x03\x03\x03\x03\x16
\x13\x13\x13\x13\x13\x13cv2
\x16


                              <255>\x03\x03\x03\x16/
                                     \x1a\x1a\x1a\x1a\x1a\x1a\x1a
\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a
\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a
\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a
\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a
\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a
\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x1a
\x1a\x1a\x1a\x1a\x1a\x1a\x1a\x03\x03\x16 / /\x03\x03\x03\x16 \x16\x16
```



4. If either the password or the username is incorrect. After that, we are given three attempts to log in.



5. If a user enters incorrect credentials three times, the honeypot system is activated, and we save the user's IP address and all other information.



6. The keylogger.py will take screenshots and logs of the attacker's system.

Attacker's System Screenshot

Attacker's System Logfile

7. Captureimage.py will be used to take the attackers image.

IX. CONCLUSION:

The paper gives a broad review of honeypots and their uses. With examples, many sorts of honeypots are covered, including production, research, low level interaction, medium level interaction, and high-level interaction.
Honeypots are a relatively new technology with a lot of potential for upcoming work. In order to maximize their efficiency, honeypots can be used in conjunction with other well-known security measures like firewalls or intrusion detection systems(IDS).

X. REFERENCES:

[1]. "Know Your Enemy: Honeywall CDROMRoo 3rd Generation Technology," Lanz Spitzner, 2005.
[2]. "Improving network security with honeypots," Christian Doring.
[3]. "Honeypot security," Government of the Hong Kong Special Administrative Region, February 2008.
[4]. Honeypots: Fundamental Concepts, Classification, and Educational Applications in Information Security Education and Courses.
[5]. https://project.honeynet.org/papers/individual/Doering.pdf
[6]. https://security.rbaumann.net/download/honeyd.pdf
[7]. Setting Up a Honeypot - Nepenthes, Inc. Brian Allen (ballen at wustl.edu), Washington University in St. Louis Network Security Analyst.
[8]. https://www.pixel-house.net/midinthp.pdf
[9]. https://www.honeypots.net/.
[10]. https://www.honeynet.org/papers/kye.html.
[11]. https://www.honeyd.org/background.php.
[12]. https://cs.millersville.edu/~csweb/lib/userfiles/honeypot.pdf