Honeypot
A Bait for Hackers

ABSTRACT

In the digital realm , a Honeypot is a word used to describe a “fake” network that is created to attract undesired traffic. This is accomplished by dangling "goodies" in front of them to the point that they can’t resist trying to gain access to what they assume is a real network.

Presented by
Prasanna M
lavanya A

Under guidence of
Ayush Bagde

Cybersecurity
Expert

EthicalHacking
Trainer

3/8/2021

Contents

WHY DO YOU NEED A HONEYPOT ON YOUR NETWORK?

The main reason you need a honeypot on your network is because of the information it

yields; something that no intrusion detection or prevention system can provide you with. Armed with the information, and the alerts they register, network administrators will become aware of the sort of attacks they are targeted for and have the fore-knowledge to figure out what they need to do to strengthen their defenses.

With that being said, there are two types of honeypots:

Corporate honeypot – this is a honeypot that is set up in a production environment and serves as a tool for studying attacks to use the knowledge to further strengthen the internal network's security.

Research honeypot – this is a honeypot that is used by researchers and with the hopes of studying attack methodologies and other characteristics like motives for attacks. Then, for example, using the knowledge to create defense solutions (antiviruses, anti-malware, etc.) that can prevent similar attacks in the future.

The data types that honeypots capture from (or about) the attackers can include, but is not limited to:

- The **usernames**, **roles**, and **privileges** that the attackers use
- The **IP addresses** of the network or host that are being using for the attack
- What data is being **accessed**, **altered** or **deleted**
- The **actual keystrokes** the attackers type out, which lets administrators see exactly what they are doing

Honeypots also help with keeping the attention of hackers diverted from the main network, averting the full force of an attack, until the administrators are ready to put the appropriate counter-action in place.

PROS OF USING A HONEYPOT NETWORK

It is a low-cost security measure that could yield high-value information about your attackers.

Cons of Using a Honeypot Network

It is not easy to set up and configure and it would be pure insanity to try and do so without an expert on hand; it could backfire and expose the internal network to worse attacks.It goes without saying, though, that honeypots are arguably the best way to catch a hacker or an attack just as it is happening. It allows administrators to go through the whole process step-by-step, following it all in real-time with each alert.

Where to Find Honeypot Installation Instructions

In this article we will focus on the strategy needed to successfully implement a

honeypot on your network rather than the actual step-by-step installation of the software solutions themselves. But, for those who *do* need to see the honeypot solutions being installed, there are some great sites and videos out there. Our recommendations would be:

- **Windows** – for most of the world, this is the operating system (OS) of choice. And at Analytical Security, you get to set up a honeypot for this operating system and incorporate the cloud (Amazon AWS) in your network.
- **Linux** – if you are the hands-on, Linux type of person who loves to go under the roof and tinker under the hood

TAKE CARE!

- Right, now let us look at some issues you will need to be aware of and careful about before you go about implementing your honeypot.

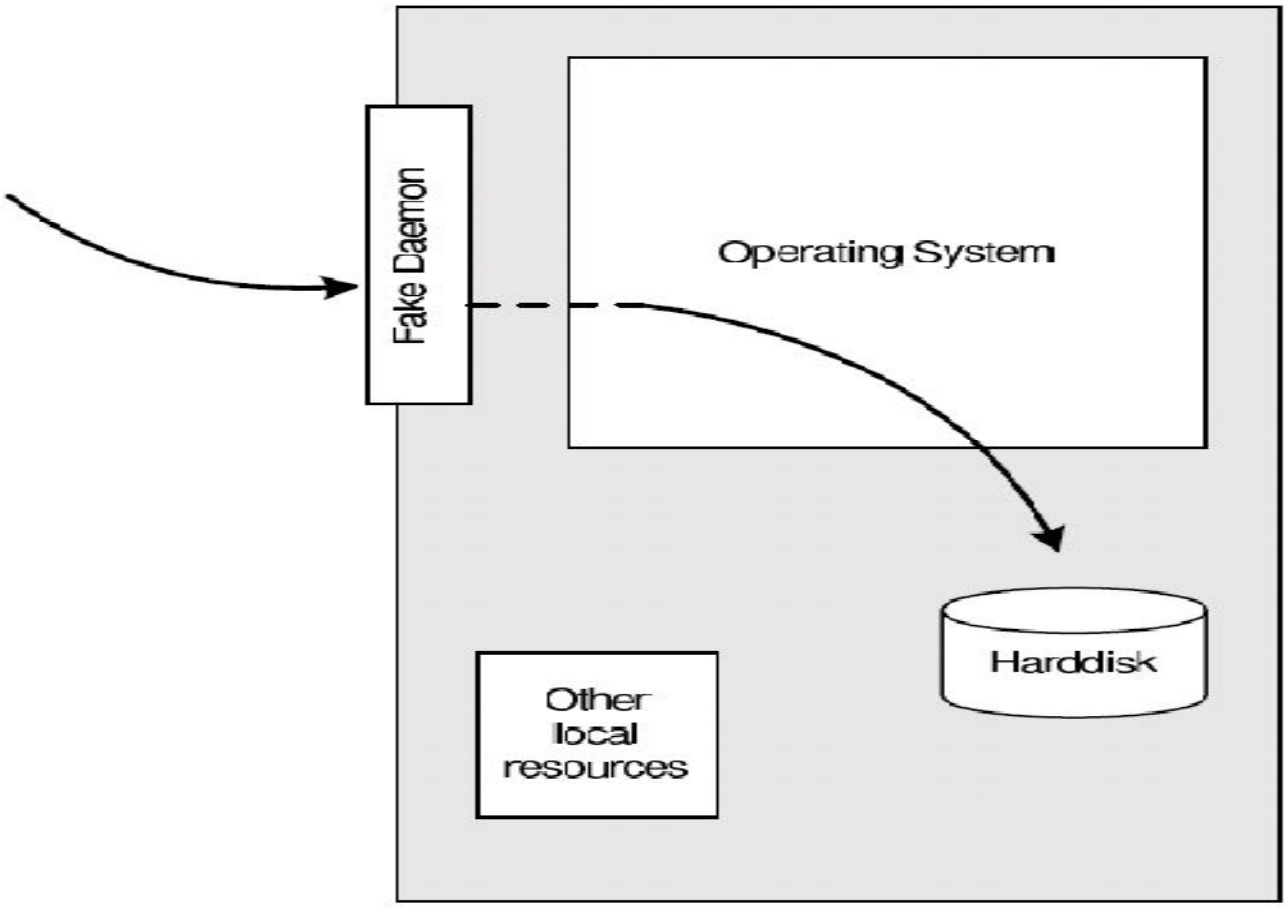
CONCEPTS:

LOW-INVOLVEMENT HONEY:

A low-level involvement honeypot typically only provides certain fake services. In a basic form, these services could be implemented by having a listener on specific port.

In such a way, all incoming traffic can easily be recognized and stored. With such a simple

solution it is not possible to catch communication of complex protocols. On a low-level honeypot there is no real operating system that attacker can operate on. This will minimize the risk significantly because the complexity of an operating system is eliminated. On the other hand, this is also disadvantage. It is not possible to watch an attacker interacting with operating system, which could be really interesting. A low-level honeypot is like one-way connection. We only listen, we do not ask any questions.

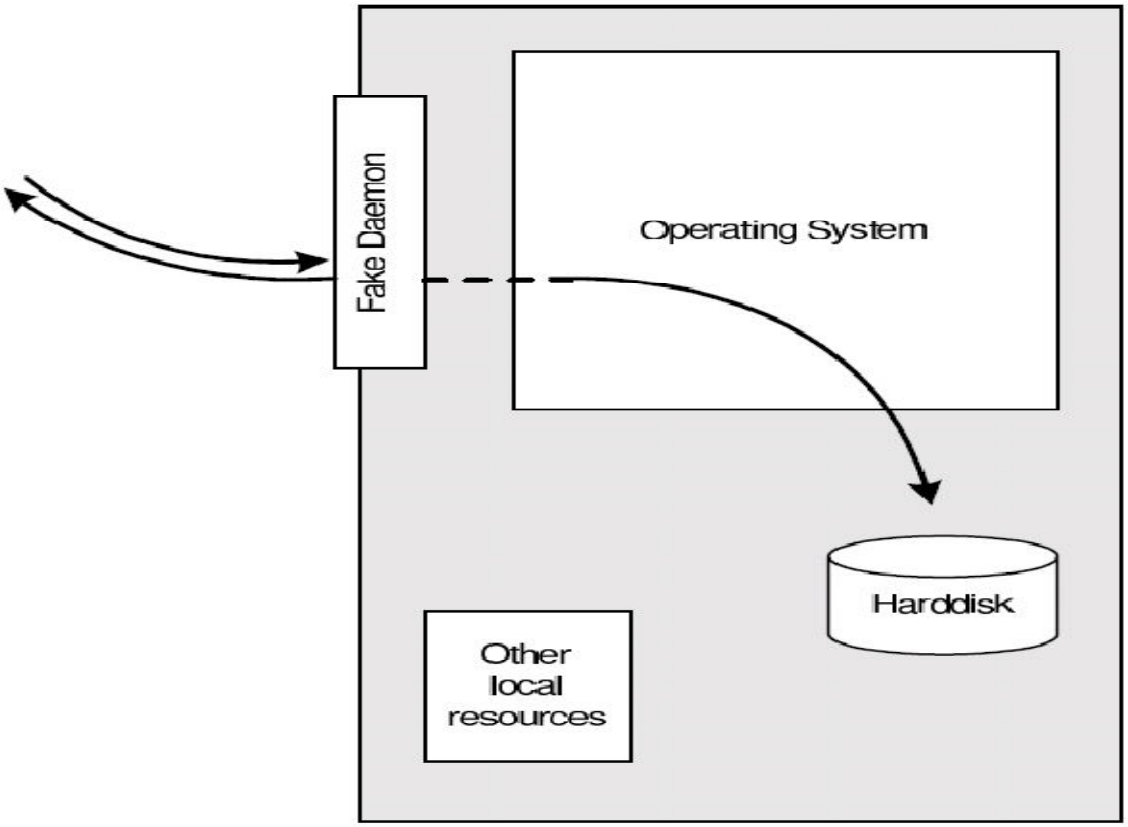


MID-INVOLVEMENT HONEYPOT

A mid-involvement honeypot provides more to interact with but still does not provide a real underlying operating system. The fake daemons are more sophisticated and have deeper knowledge about the specific services they provide. At the same

moment, the risk increases. The probability that attacker can find a security hole or vulnerability is getting bigger because the complexity of honeypot is increasing.

Through the higher level of interaction, more complexity attacks are possible and can therefore be logged and analysed. The attacker gets a better illusion of a real operating system. He has more possibilities to interact and probe the system. Developing a mid-involvement honeypot is complex and time consuming. Special care has to be taken for security check as all developed fake daemons need to be as secure as possible.



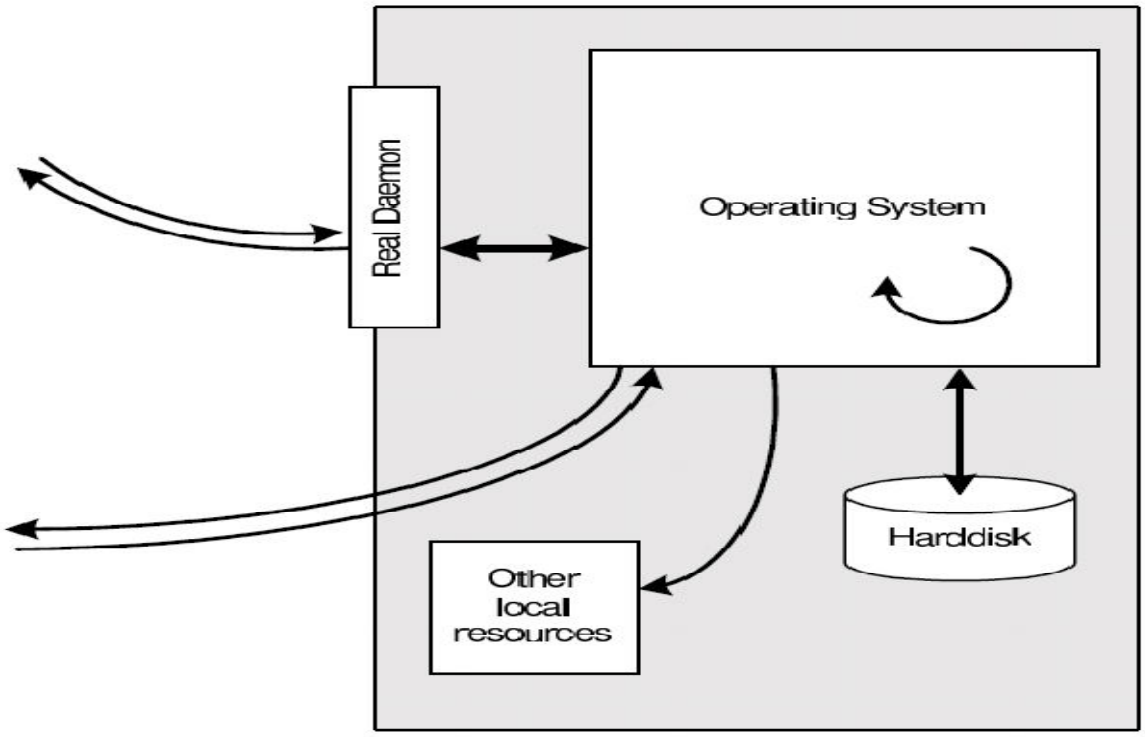
HIGH-INVOLVEMENT HONEYPOT

A high-involvement honeypot has a real underlaying operating system. This leads to much higher risk as the complexity increases rapidly. At the same time, the possibilities to gather the information, the possible attacks as well as the attractiveness increase a lot. As

soon as a hacker has gained access, his real work and therefore the interesting part begins.

A high-involvement honeypot is very time consuming. The system should be constantly under surveillance. A honeypot which is not under control is not of much help even become a danger or security hole itself. It is very important to limit a honeypot's access to local intranet, as the honeypot can be used by blackhats as if it was a real compromised system. Limiting outbound traffic is also important point to consider, as the danger once a system is fully compromised can be reduced.

By providing a full operating system to attacker, he has the possibilities to upload and install new files. This is where the high-involvement honeypot can show its strength, as all its actions can be recorded and analyzed.



HONEYPOT LOCATION

A honeypot does not need a certain surrounding environment, as it is a standard server with no special needs. A honeypot can be placed anywhere a server could be placed. But certainly,

some places are better for certain approaches as others.

A honeypot can be used on the Internet as well as the intranet, based on the needed service. Placing a honeypot on the intranet can be useful if the detection of some bad guys inside a private network is wished. If the main concern is the Internet, a honeypot can be placed at two locations:

1. In front of firewalls (Internet)
2. DMZ
3. Behind the firewall (Intranet)

By placing the honeypot in front of firewall the risk for the internal works does not increases. A honeypot will attract and generate lot of unwished traffic like port scans or attack patterns.

By placing a honeypot outside the firewall, such events do not get logged by the firewall and an internal IDS system will not generate alerts. Otherwise a lot of alerts would be generated on the firewall or IDS.

Probably the biggest advantage is that the firewall or IDS, as well as any other resources, have not to be adjusted as the honeypot is outside the firewall and viewed as any other machine on the external network. Running a honeypot does therefore not increase the dangers for the internal network nor does it introduce new risks.

The disadvantage of placing a honeypot in front of the firewall is that internal attackers cannot be located or trapped that easy. Placing a honeypot inside DMZ seems a good solution as

long as the other systems inside the DMZ can be secured against the honeypot.Most DMZs are not fully accessible as only needed services are allowed to pass the firewall. In such a case, placing the honeypot in front of the firewall should be favored as opening all corresponding ports on the fire is too time consuming and risky.

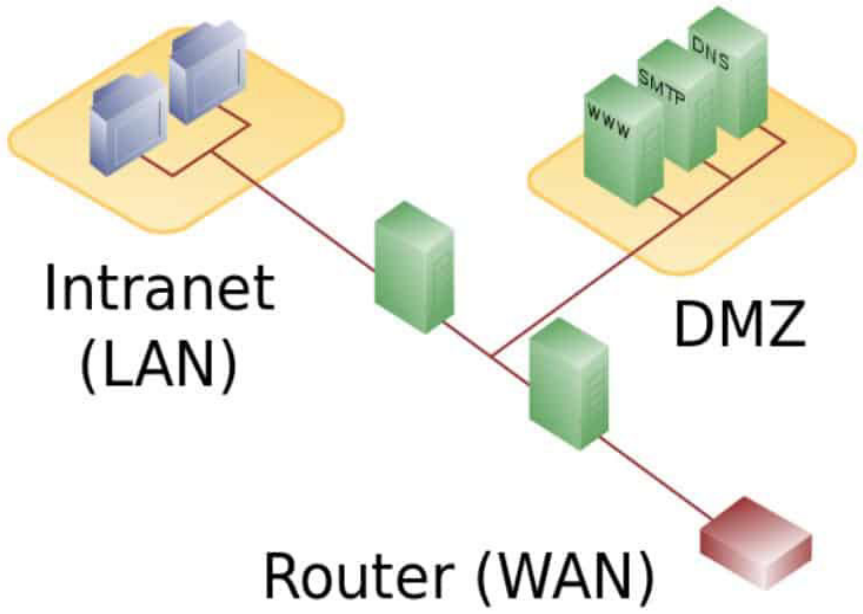
A honeypot behind a firewall can introduce new security risks to the internal network, especially if the internal network is not secured against the honeypot through additional firewalls. This could be a special problem if the Ips are used for authentication. By placing the honeypot behind a firewall, it is inevitable to adjust the firewall rules if access from internet should be permitted. The biggest problem arises as soon as the internal honeypot is compromised

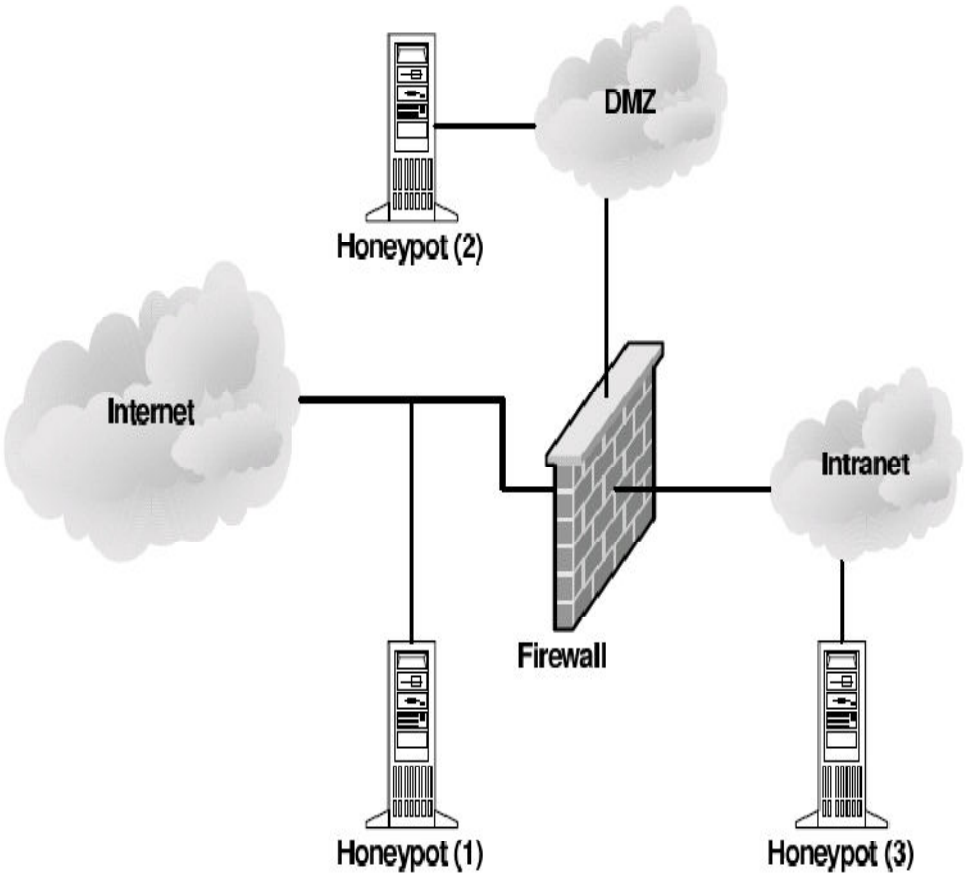
by an external attacker. He gains the possibility to access the internal network through the honeypot.This traffic will be unstopped by the firewall as it is regarded as traffic to the honeypot only, which in turn is granted. Securing an internal honeypot is therefore mandatory, especially if it is a high-involvement honeypot. The main reason for placing a honeypot behind a firewall could be to detect internal attackers.

The best solution would be to run a honeypot in its own DMZ, therefore with a preliminary firewall. The firewall could be connected directly to the internet or intranet, depending on the goal. This attempt enables tight control as well as flexible environment with maximal security.

PLACEMENT OF THE HONEYPOT

Arguably, the ideal place to create your honeypot is in the demilitarized zone. This is the area that is out of your main network, but still behind a router which faces the Internet.





HOST BASED INFORMATION GATHERING

This section will discussion possibilities that offer gain of information about ongoing on a honeypot by installing information gathering mechanisms on the honeypot itself.

Basic possibilities

Information gathering facilities can basically be grouped into two categories; facilities that generate streams of information and facilities that offer the information to peek into the system and get the information about a certain state of the honeypot.

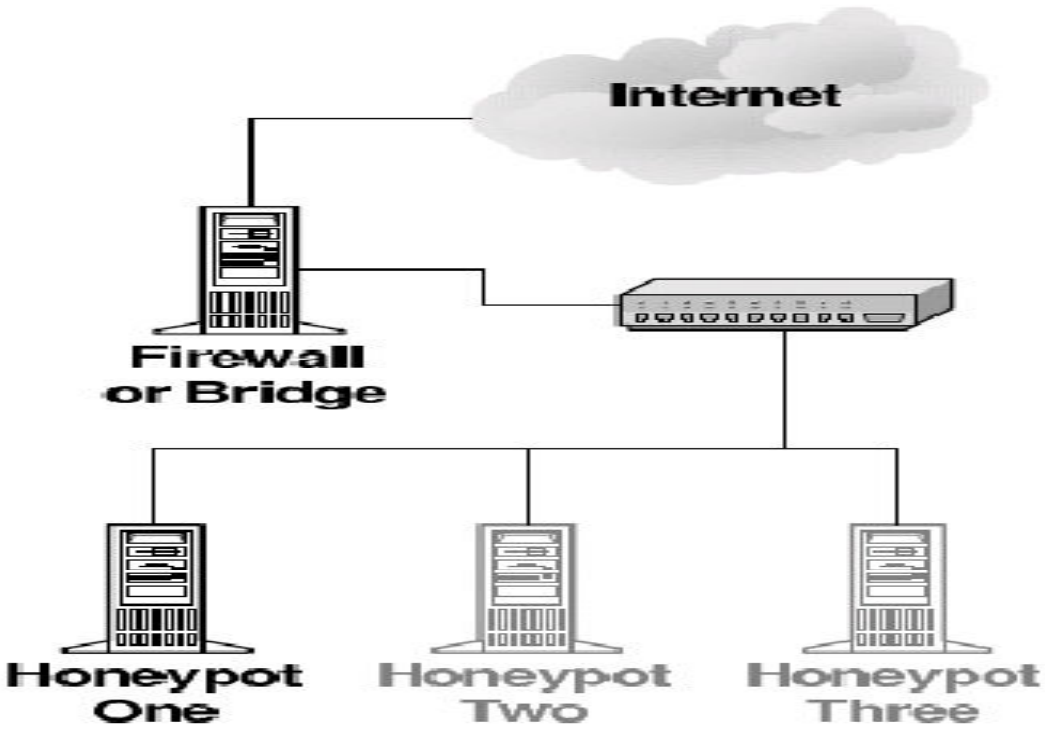
Microsoft Windows

One could think the large amount of observed attacks on systems running ms windows operating system makes them ideal for the honeypot, but unfortunately the structure of this operating system makes the data gathering rather difficult. Until today the source code of the operating system of Microsoft is not freely available, which means that changes to the operating system are very hard to achieve.

Unix derivates

Unix derivatives operating system offers interesting opportunities for deploying data gathering mechanisms since all of their components are available as source code.

Network based Information Gathering: Host based information gathering is always located at the host itself and is therefore vulnerable to detection and once detected it can also be disabled. Network based information gathering does not have to be located on the honeypot itself. It can also be implemented in an invisible way, as network traffic only gets analyzed but not manipulated. Network based information gathering is safer as it is harder to be detected and quiet impossible to disable.



DANGERS

Running a honeypot or honeynet is not something that should be underestimated- there are some dangers one must be aware of which basically are:

1. Unnoticed takeover of the honeypot by an attacker

2. Lost control over the honey pot installation.

3. Damage done to third party.

ATTRACTIVENESS

Being the owner of a honeypot can be an interesting experience, but what if the members of the blackhat community do not find their way to the honeypot or, even more dramatically, are not interested in the honeypot at all. Another approach to lure attackers is the offering of the interesting services on the honeypot. Of course the question arises, what an interesting services is or what it should look like.

ADVANTAGES

- Small Data sets→Honeypots only collect attack or unauthorized activity,

dramatically reducing the amount of data they collect. Organizations that may log thousands of alerts a day may only log a hundred alerts with honeypots. This makes the data honeypots collect much easier to manage and analyze.

- Reduced False Positives→Honeypots dramatically reduce false alerts, as they only capture unauthorized activity.
- Catching False Negatives→Honeypots can easily identify and capture new attacks never seen before.
- Minimal Resources→Honeypots require minimal resources, even on the largest of networks. This makes them an extremely cost effective solution.

- Encryption→Honeypots can capture encrypted attacks.

DISADVANTAGES

- Single Data Point→Honeypots all share one huge drawback; they are worthless if no one
- Attacks them. Yes, they can accomplish wonderful things, but if the attacker does not sent any packets to the honeypot, the honeypot will be blissfully unaware of any unauthorized activity.
- Risk→Honeypots can introduce risk to your environment. As we discuss later, different honeypots have different levels of risk.Some introduce very little risk, while others give the attacker entire platforms from which to

launch new attacks, Risk is variable,

depending on how one builds and deploys the

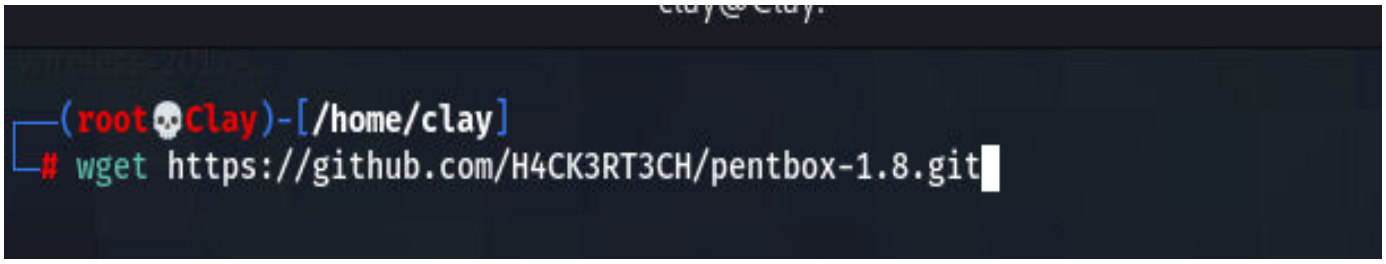
honeypot.

WHAT YOU'LL NEED

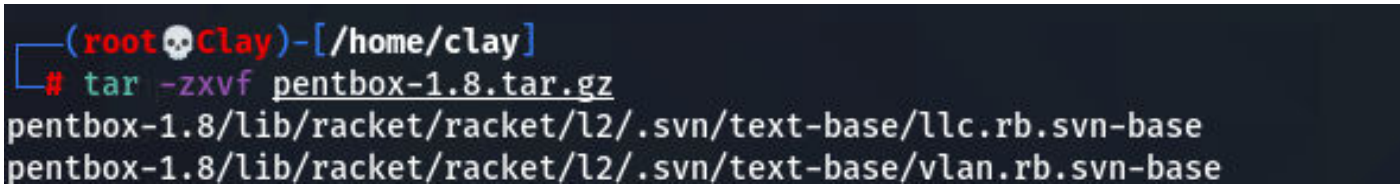
The only things you'll need are a running instance of Kali Linux and a user account with admin privileges.

HOW TO DOWNLOAD PENTBOX

Log in to your Kali Linux machine as an admin user. Open a terminal window and download pentbox with the command:



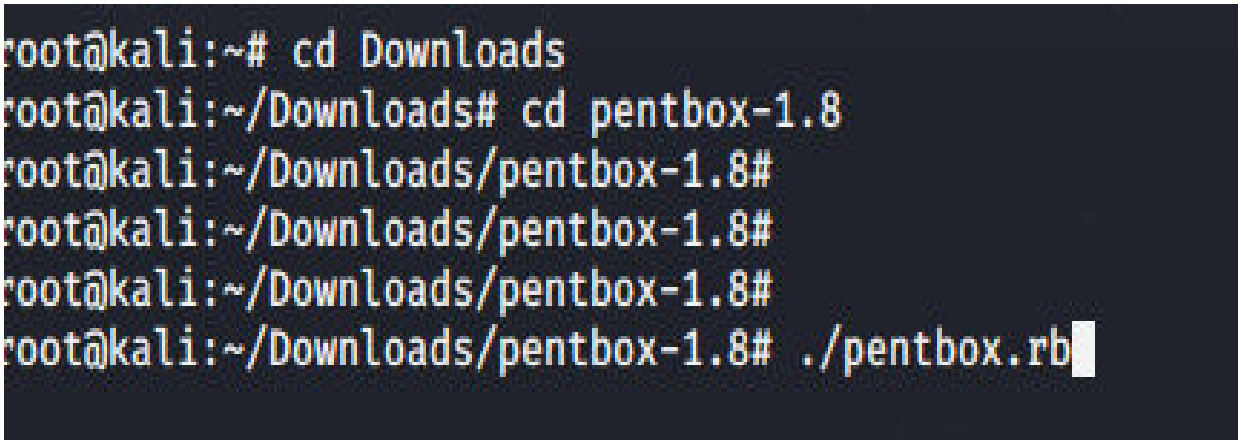
Once that file has finished downloading, extract the archive with the command:



This will create a new directory named pentbox-1-8. Change into that new directory with *cd pentbox-1.8*.

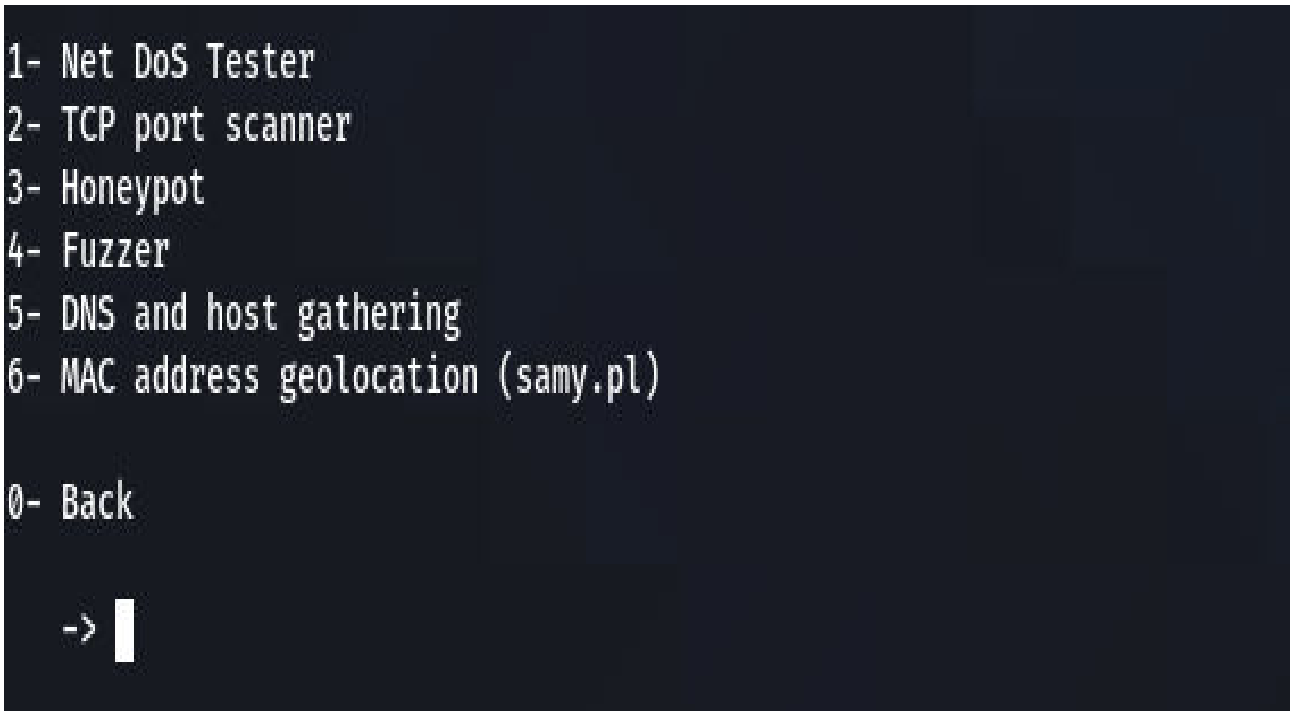
HOW TO RUN PENTBOX

The next step is to run the pentbox Ruby script with the command:



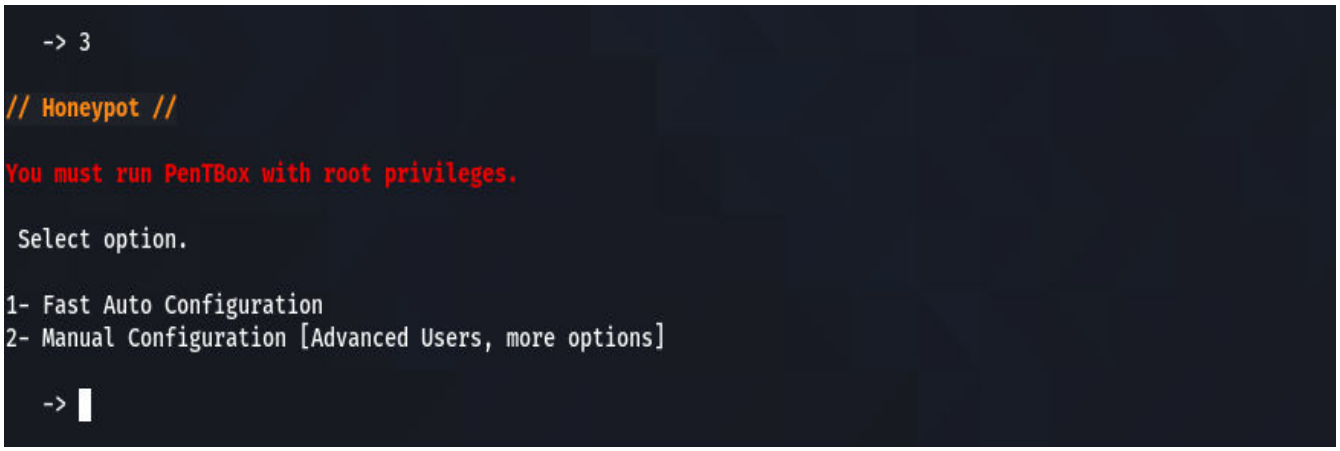
When you issue the command, you'll be greeted by a menu. From that menu select 2 (for Networking tools) and then 3 for Honeypot


PenTBox 1.8
.::!!!!!!!:.
.!!!!!:. .:!!!!!!!!!!!!
~~~~!!!!!!. .:!!!!!!!!!UWWW$$$
:$$NWX!!: .:!!!!!!XUWW$$$$$$$$P
$$$$$##WX!: .<!!!!UW$$$$ $$$$$$$$#
$$$$$ $$$UX :!!UW$$$$$$$$$ 4$$$$$*
^$$$B $$$$ $$$$$$$$$$ d$$R*
**$bd$$$$ '*$$$$$$$$$$o+#
**** *******
--------- Menu ruby2.7.2 @ 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
->
~~~~



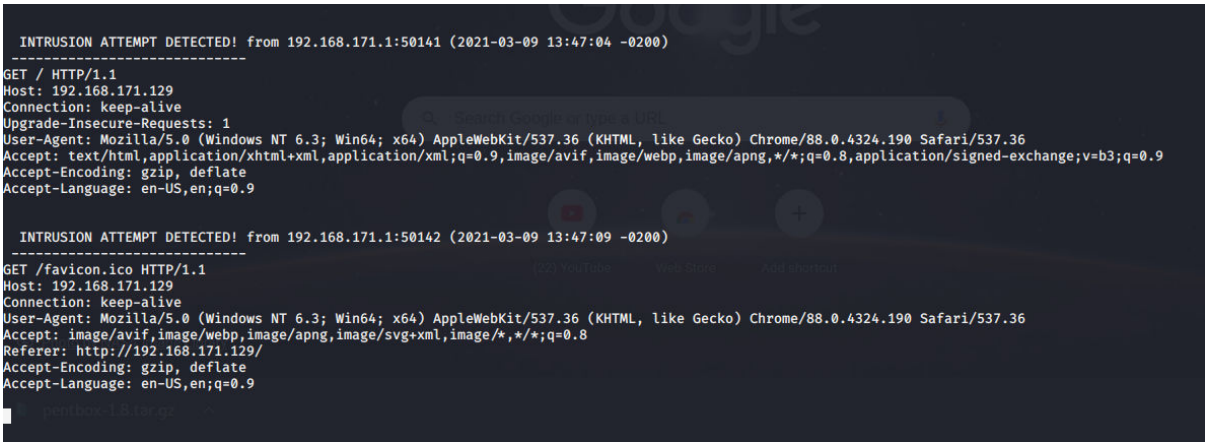
In the menu.select 1 (for Fast Auto Configuration).

This will launch a honeypot listening on port 80.



Go back to the terminal window on the Kali Linux machine and you should see the honeypot picked up the attempted connection


Not secure
192.168.171.129
Apps
Who Am I YIFY subt...
Ethical Hacking Job...
Feedspot
Access denied
IP Address login failed
2021-03-09 13:45:53 -0200

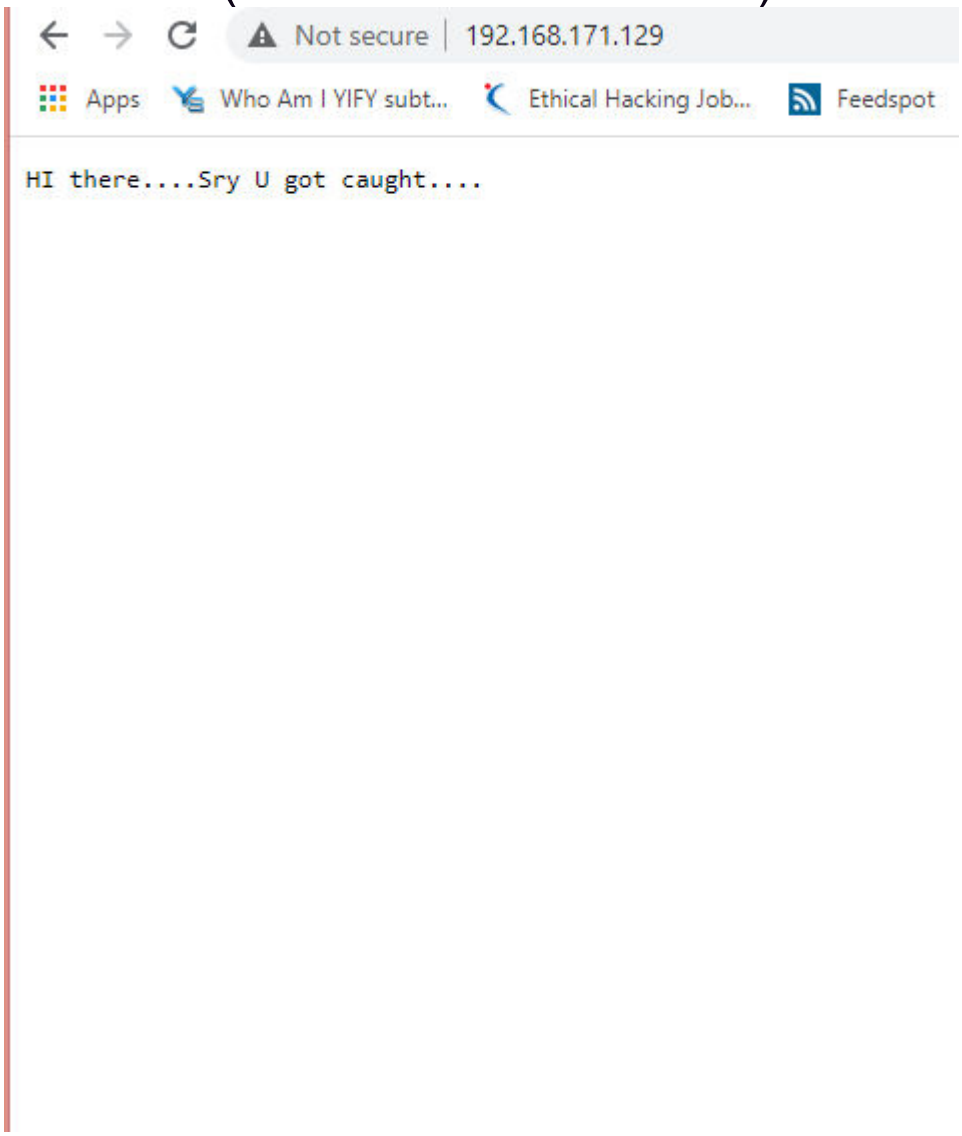


HOW TO LAUNCH A SPECIFIC INSTANCE

Now we want to launch a honeypot to listen on a specific port. Say you've had trouble with attacks on SSH. To deploy pentbox such that it's listening in on port 80, you'd run the script and select 2 and then 3, followed by 2. When prompted for a port to open, type 80

```
 Select option.

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

   → 2

 Insert port to Open.

   → 80

 Insert false message to show.

   → HI there....Sry U got caught....

 Save a log with intrusions?

 (y/n)   → y

 Log file name? (incremental)

Default: */pentbox/other/log_honeypot.txt

   → /pentbox/other/log_honeypot.txt

 Activate beep() sound when intrusion?

 (y/n)   → y

  HONEYPOT ACTIVATED ON PORT 80 (2021-03-09 13:53:45 -0200)


 Saving log error: No such file or directory.
```

You can then opt to save a log and then have a beep announce an intrusion. Once the honeypot is running, attempt to SSH into the Kali Linux machine (from another machine).



Then Honeypot is finally deployed successfully.

CONCLUSION

A honeypot is just a tool. How you use that tool is up to you. There are a variety of honeypot options, each having different value to organizations. We have categorized two types of honeypots, production and research.

Production honeypots help reduce risk in an organization. Research honeypots are different in that they are not used to protect a specific oraganization.

Instead they are used as a research tool to study and identify the threats in the Internet community. Regardless of what type of honeypot you use, keep in mind the ‘level of interaction’. This means that the more your honeypot can do and the more you can learn from it, the more risk that potentially exists. You will have to determine what is the best relationship of risk to capabilities that exist for you.Honeypots will not solve an oraganization’s security problems. Only best practices can do that. However, honeypots may be a tool to help contribute to those best practices


THANK YOU
Know hacking, but no hacking
SAFE COMPUTING