Honeypots

Be afraid

Be very afraid

What is Honeypot? ……

- A Honey Pot is an intrusion (unwanted) detection technique used to study hacker movement and interested to help better system defences against later attacks usually made up of a virtual machine that sits on a network or single client.
- A honey pot is a computer system on the Internet that is expressly set up to attract and "trap" people who attempt to find access into other people's computer systems.
  - This includes the hacker, cracker, and script
- A honeypot is a security resource whose value lies in being probed, attacked, or compromised.

……

- They can provide early warning about new attack and utilization trends and they allow in-depth examination of unwanted users during and after use of a honeypot.
- Many people have their own definition of what a honeypot is, or what it should accomplish.
  - Some feel its a solution to deceive attackers
  - Others feel its a technology used to detect attacks
  - While other feel honeypots are real computers designed to be hacked into and learned from .
- In reality, they are all correct.

Three goals of the Honey pot system

- The virtual system should look as real as possible, it should attract unwanted intruders to connect to the virtual machine for study.
- The virtual system should be watched to see that it isn't used for a massive attack on other systems.
- The virtual system should look and feel just like a regular system, meaning it must include files, directories and information that will catch the eye of the hacker.

How it works? ……

- Honeypots are, in their most basic form, fake information severs strategically-positioned in a test network, which are fed with false information made unrecognizable as files of classified nature.

- In turn, these servers are initially configured in a way that is difficult, but not impossible, to break into them by an attacker; exposing them deliberately and making them highly attractive for a hacker in search of a target.

- Finally, the server is loaded with monitoring and tracking tools so every step and trace of activity left by a hacker can be recorded in a log, indicating those traces of activity in a detailed way.

.....

- Honeypots are a highly flexible security tool with different applications for security. They don't fix a single problem. Instead they have multiple uses, such as prevention, detection, or information gathering

Main Function of Honeypot

- To divert the attention of the attacker from the real network, in a way that the main information resources are not compromised
- To build attacker profiles in order to identify their preferred attack methods, like criminal profile.
- To identify new vulnerabilities and risks of various operating systems, environments and programs which are not thoroughly identified at the moment.
- To capture new viruses or worms for future study.
- A group of Honeypots becomes a Honeynet.

Classification of HoneyPots

- Honeypots can be classified according to two criteria:
  - According to their Implementation Environment
  - According to their Level of Interaction.

- These classification criteria eases understanding their operation and uses when it comes to planning an implementation of one of them inside a network or IT infrastructure.

Implementation Environment

- Under this two category
  - Production Honeypots
  - Research Honeypots

Production Honeypots: …..

- Used to protect organizations in real production operating environments.
- Production honeypots are used to protect your network, they directly help secure your organization.
- Specifically the three layers of prevention, detection, and response. Honeypots can apply to all three layers. For prevention, honeypots can be used to slow down or stop automated attacks.

.....

- For example, the honeypot **Labrea Tarpit** is used to "tarpit" or slow down automated TCP attacks, such as worms.
- Against human attackers, honeypots can utilize psychological weapons such as deception (mislead) or deterrence (prevention) to confuse or stop attacks.

Research Honeypots: …..

- These Honeypots are not implemented with the objective of protecting networks.
- They represent educational resources of demonstrative and research nature whose objective is centered towards studying all sorts of attack patterns and threats.
- A great deal of current attention is focused on Research Honeypots, which are used to gather information about the intruders' actions.

.....

- For example, there is some non-profit research organization focused in voluntary security using Honeypots to gather information about threats in cyberspace.

Level of Interaction ……

- The term “Level of Interaction” defines the range of attack possibilities that a Honeypot allows an attacker to have.
- These categories help us understand not just the type of Honeypot which a person works with, but also help define the array of options in relation to the vulnerabilities intended for the attacker to exploit.
- It is used to start the construction of the attacker’s profile.

.....

- classified on the bases of their levels:-

1. HoneyD (Low-Interaction)
2. Honey net (High-Interaction)

Low-Interaction Honeypots

- Low-interaction honeypots are typically the easiest honeypots to install, configure, deploy, maintain, but customized to more specific attacks.
- Most importantly there is no interaction with the underlying operating system.
  - Nepenthes
  - Honeyd
  - Honeytrap
  - Web Applications

Advantages

- Good starting point.
- Easy to install, configure, deploy and maintain.
- Introduce a low or at least limited risk.
- Logging and analyzing is simple.

Disadvantages

- No real interaction for an attacker possible.
- Very limited logging abilities.
- Can only capture known attacks.
- Easily detectable by a skilled attacker

High-interaction Honeypots

- High-interaction honeypots are the extreme of honeypot technologies.
- Provide an attacker with a real operating system where nothing is emulated or restricted.
- Ideally you are rewarded with a vast amount of information about attackers, their motivation, actions, tools, behaviour, level of knowledge, origin, identity etc.
- It controls an attacker at the network level.

Advantages

- You will face real-life data and attacks so the activities captured are most valuable.
- Learn as much as possible about the attacker, the attack itself and especially the methodology as well as tools used.
- High-interaction honeypots could help you to prevent future attacks and get a certain understanding of possible threats.

Disadvantage

- Building, configuring, deploying and maintaining a high-interaction honeypot is very time consuming as it involves a variety of different technologies (e.g. IDS, firewall etc.) that has to be customized.
- Analyzing a compromised honeypot is extremely time consuming (40 hours for every 30 minutes an attacker spend on a system).
- A high-interaction honeypot introduces a high level of risk and - if there are no additional precautions in place - might put an organizations overall IT security at stake.

Intrusion Detection …..

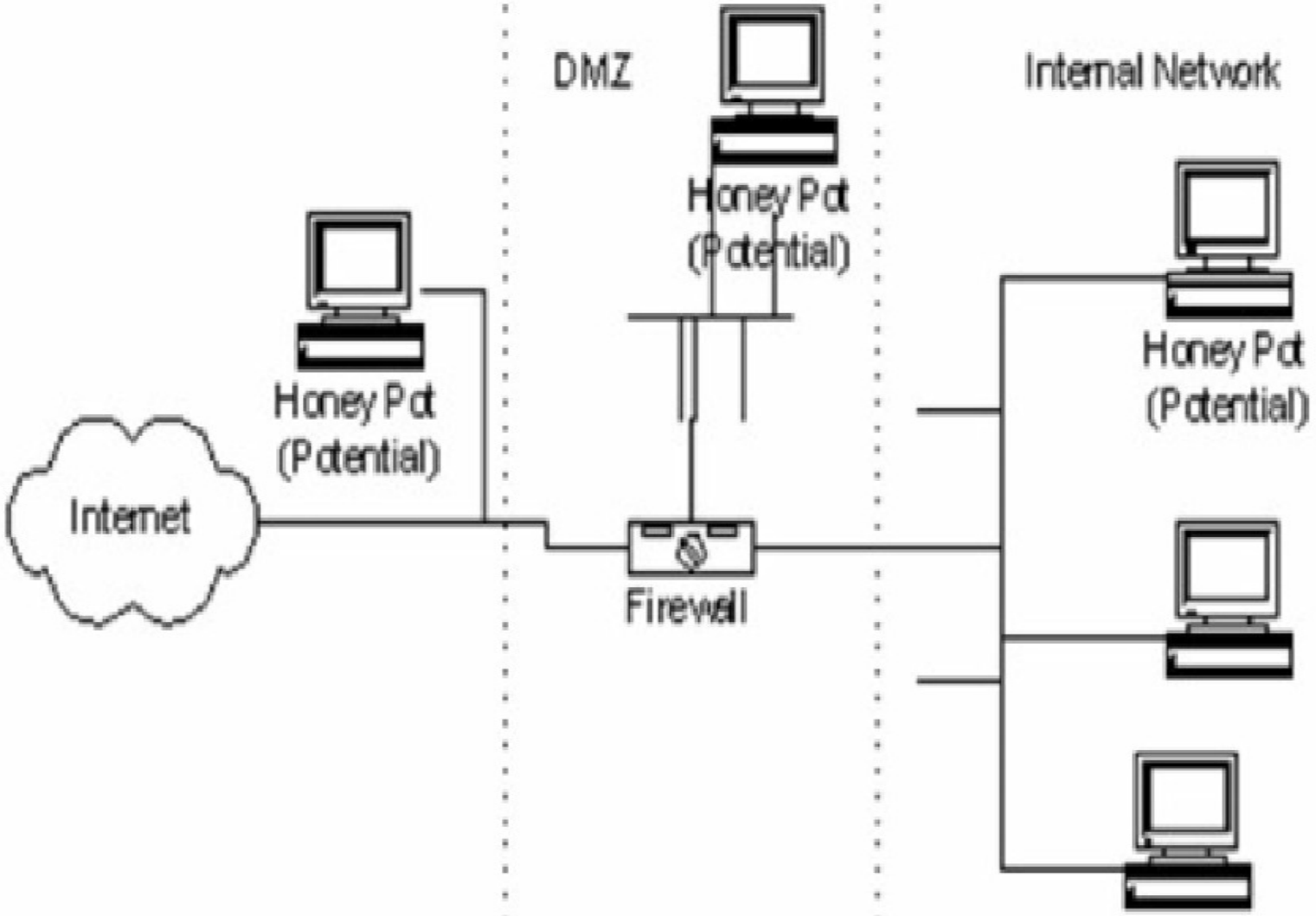
- **Intrusion Detection** is the art of detecting inappropriate, incorrect, or anomalous activity. Among other tools, an **Intrusion Detection System** (IDS) can be used to determine if a computer network or server has experienced an unauthorized intrusion

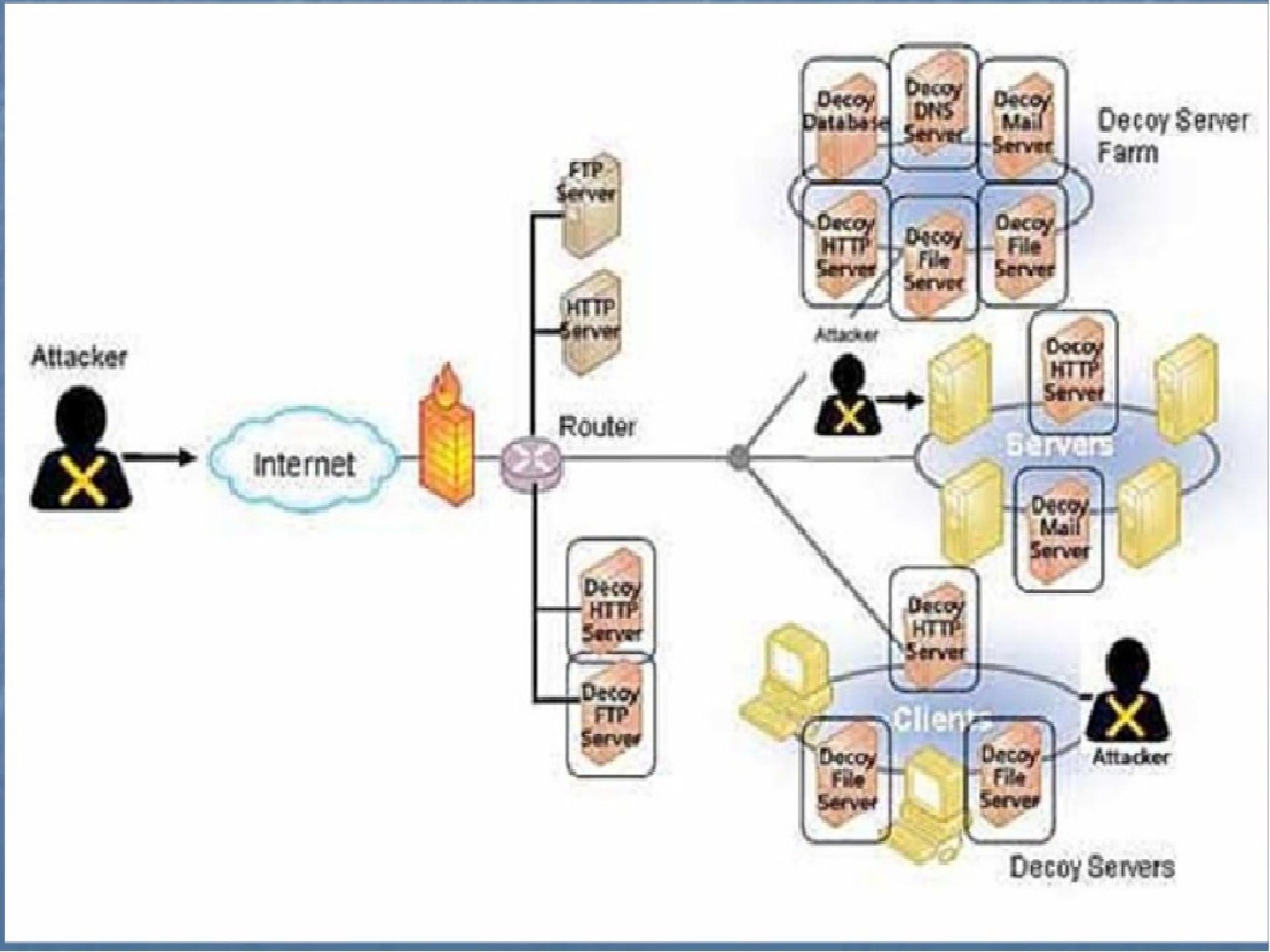
- An **Intrusion Detection System** provides much the same purpose as a burglar alarm system installed in a house. In case of a (possible) intrusion, the **IDS** system will issue some type of warning or alert. An operator will then tag events of interest for further investigation by the **Incident Handling** team

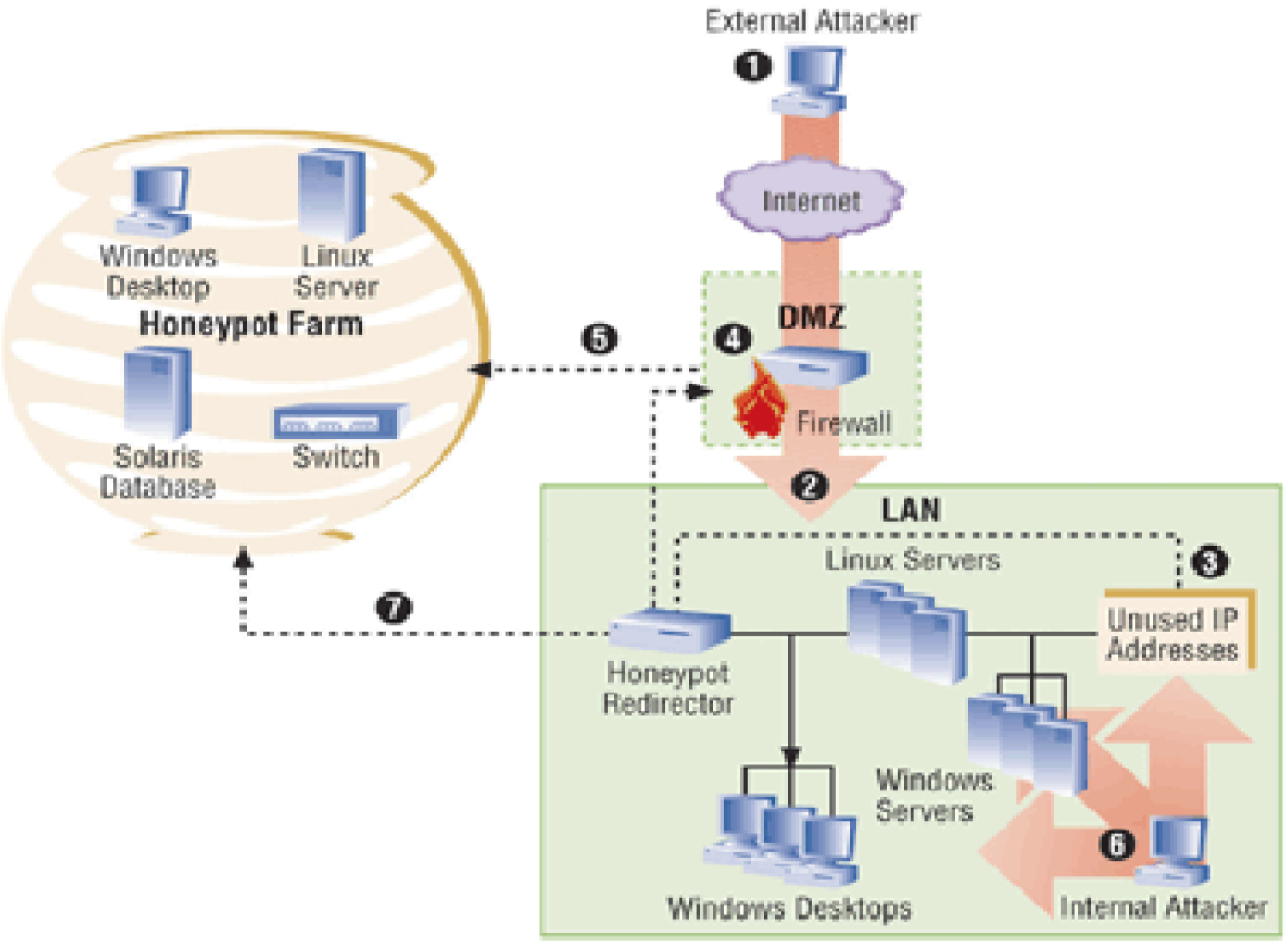
- Traditionally, there are two general types of **Intrusion Detection Systems:**

1. Host Based Intrusion Detection Systems (HIDS):
   - IDS systems that operate on a host to detect malicious activity on that host;

2. Network Based Intrusion Detection Systems (NIDS):
   - IDS systems that operate on network data flows.


DMZ
Internal Network
Honey Pot
(Potential)
Honey Pot
(Potential)
Honey Pot
(Potential)
Internet
Firewall


Attacker
Internet
Router
FTP Server
HTTP Server
Decoy HTTP Server
Decoy FTP Server
Decoy Database
Decoy DNS Server
Decoy Mail Server
Decoy HTTP Server
Decoy File Server
Decoy File Server
Decoy Server Farm
Attacker
Decoy HTTP Server
Servers
Decoy Mail Server
Decoy HTTP Server
Clients
Attacker
Decoy File Server
Decoy File Server
Decoy Servers


External Attacker
1
Internet
DMZ
4
Firewall
5
Windows Desktop
Linux Server
Honeypot Farm
Solaris Database
Switch
2
LAN
Linux Servers
3
Unused IP Addresses
7
Honeypot Redirector
Windows Servers
6
Windows Desktops
Internal Attacker

Advantages .....

- **New Tools and Tactics:** They are designed to capture anything that interacts with them, including tools or tactics never seen before, better known as “zero-days”.

- **Minimal Resources:** This means that resources can be minimum and still enough to operate a powerful platform to operate at full scale. i.e. A computer running with a Pentium Processor with 128 Mb of RAM can easily handle an entire B-class network.

- **Information:** Honeypots can gather detailed information, unlike other security incident analysis tools.

.....

- **IPv6 Encryption:** Unlike most security technologies, Honeypots also work in IPv6 environments. The Honeypot will detect an IPv6-based attack the same way it does with an IPv4 attack.

- **Simplicity:** Because of their architecture, Honeypots are conceptually simple. There is not a reason why new algorithms, tables or signatures must be developed or maintained.

Disadvantages ……

- **Limited Vision:** They can only scan and capture activity destined to interact directly with them. They do not capture information related to attacks destined towards neighboring systems, unless the attacker or the threat interacts with the Honeypot at the same time.

- **Risk:** Inherently, the use of any security technology implies a potential risk. Honeypots are no different because they are also subject to risks, specifically being hijacked and controlled by the intruder and used as a launch pad for subsequent attacks.

.....

- Biggest challenges which honeypot faces and most security technology, is configuring them.
- Honeypots can carry on risks to a network & must be handled with care.
- Honeypots can only track and capture activity that directly interacts with them. Therefore honeypots will not capture attacks against other systems.

Conclusion

- Honey pots are an extremely effective tool for observing hackers movements as well as preparing the system for future attacks.

- Although the down side to using Honeypots are amount of resource used, this is usually countered by implementing a central analysis module, but is still a security risk if that central module goes down.

Refrences

- http://www.authorstream.com/Presentation-Search/Tag/Honeypot
- http://www.honeyd.org/
- http://www.honeynet.org.mx/es/data/files/Papers/UAT_Honeypots_EN.pdf
- http://www.honeypots.net/honeypots/links
- http://www.securityfocus.com/infocus/1659
- http://www.slideshare.net/


Thanks