

Advanced Network Security

HoneyPot

Dr. Yaeghoobi

PhD. Computer Science & Engineering, Networking, India
dr.yaeghoobi@gmail.com



00 | **Introduction**

01 | **Honeypot Goals**

02 | **Operation**

03 | **Classification**

04 | **Implementation**

05 | **Advantage & Disadvantage**

Introduction

00



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**.

Intrusion Detection ...

- 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.

Types of IDS

- Host Based Intrusion Detection Systems (HIDS)
- Network Based Intrusion Detection Systems (NIDS)

History of Honeypot

- The idea of honeypots began with two publications, “The cuckoos egg” & “ An evening with Bredford”.
- “The cuckoos egg” was about catching a computer hacker that was searching for secrets in authors corporation.
- “An evening with Berdferd” is about a hackers moves through traps that the author used to catch him.

What is HoneyPot?

- According to Lance Spitzner, founder of the HoneyNet project, a honeypot is a system designed to learn how “black-hats” exploit weakness in an IT system.

- به گفته لنس اسپیتزر، بنیانگذار پروژه HoneyNet، یک ل هانی پات سیستمی است که با یادگیری چگونگی سوء استفاده "کلاه های سیاه" از ضعف سیستم IT طراحی شده است.

What is HoneyPot? ...

- A HoneyPot 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.

- HoneyPot یک تکنیک تشخیص نفوذ (ناخواسته) است که برای مطالعه حرکات هکرها مورد استفاده قرار می گیرد و علاقمند به کمک سیستم دفاعی در برابر حملات بعدی است. معمولاً از یک ماشین مجازی بر روی یک شبکه یا یک مشتری ساخته شده است.

Honeypot Goals

01



Goals of Honeypot System

- 1) The virtual system should look as real as possible, it should attract unwanted intruders to connect to the virtual machine for study.

- سیستم مجازی باید تا حد ممکن واقعی به نظر برسد، باید متجاوزان را ناخواسته به دستگاه مجازی برای مطالعه جذب کند.

Goals of Honeypot System...

- 2) The virtual system should be watched to see that it isn't used for a massive attack on other systems.

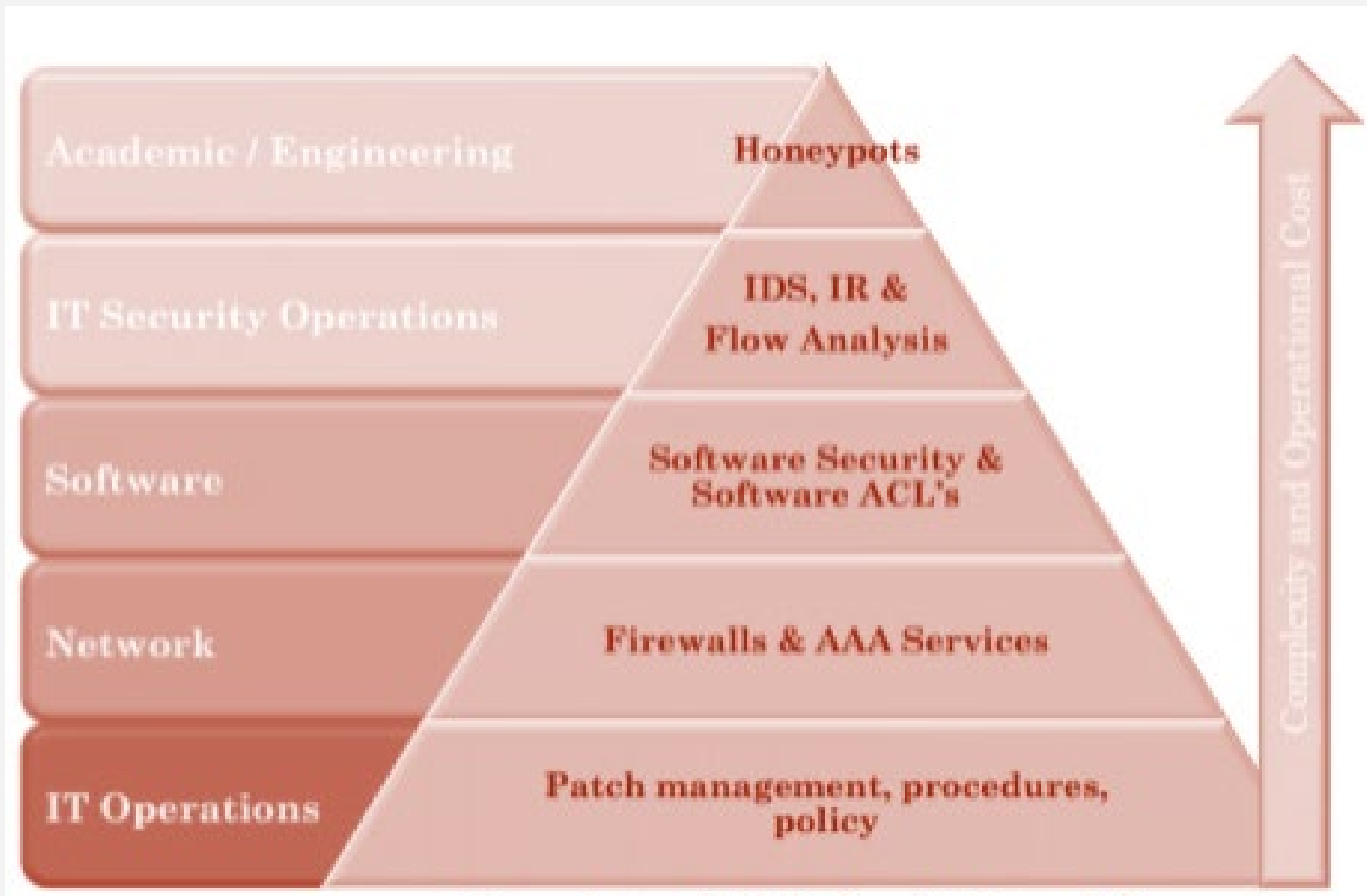
- سیستم مجازی باید رصد شود تا ببیند از آن برای حمله گسترده به سیستم های دیگر استفاده نمی شود.

Goals of Honeypot System...

- 3) 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 .

- سیستم مجازی باید دقیقاً مانند یک سیستم معمولی به نظر برسد و احساس شود، یعنی باید شامل پرونده ها، فهرست ها و اطلاعاتی باشد که چشم هکر را به خود جلب می کند.

Role of Honeypot



Operation

02



Honeypot Operating

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

- Honeypots در ابتدای ترین شکل آنها ، اطلاعاتی جعلی هستند که از لحاظ استراتژیکی در یک شبکه آزمایشی قرار می گیرند، که با اطلاعات دروغین تغذیه می شوند و به عنوان پرونده هایی با ماهیت طبقه بندی نشده قابل تشخیص نیستند.

Honeypot Operating ...

- 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.

- به نوبه خود، این سرورها در ابتدا به روشی تنظیم شده اند که دشوار اما غیرممکن نیست که توسط یک مهاجم هک شوند. در معرض قرار دادن آنها از روی عمد و جذب کردن هکر برای یافتن هدف هکرهاست.

Honeypot Operating ...

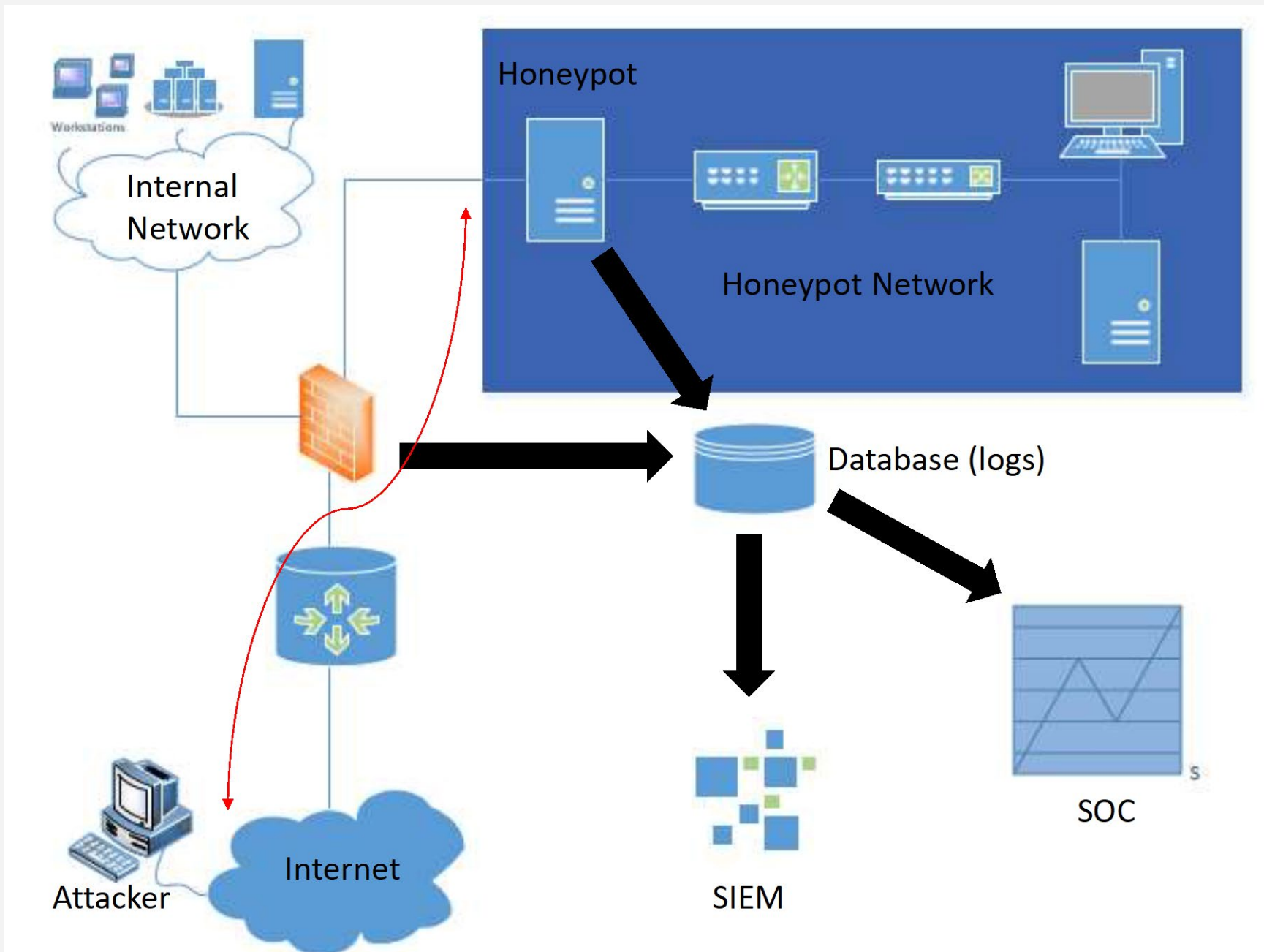
- Finally, the server is loaded with monitoring and tracking tools so every step and trace of activity left by a hacker can be recorded in a log, indicating those traces of activity in a detailed way.

- سرانجام، سرور از ابزارهای نظارتی و ردیابی بارگیری می شود، بنابراین هر مرحله و اثر فعالیت باقی مانده توسط یک هکر می تواند در یک پرونده ثبت شود، نشان می دهد که اطلاعات ثبت شده از فعالیت به روشی دقیق است.

Honeypot Operating ...

- 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.

- Honeypots یک ابزار امنیتی بسیار انعطاف پذیر با کاربردهای مختلف برای امنیت است. آنها یک مشکل واحد را برطرف نمی کنند. در عوض آنها کاربردهای مختلفی از قبیل پیشگیری، تشخیص یا جمع آوری اطلاعات دارند.



Security Categories

- **PREVENTION**

- A honeypot **cannot prevent an unpredictable** attack but it can detect it. One case where they prevent the **attacker is when he directly attack the server.**

◦ Honeypot نمی تواند از حمله غیرقابل پیش بینی جلوگیری کند اما می تواند آن را تشخیص دهد. یکی از مواردی که آنها از حمله کننده جلوگیری می کنند این است که هکر مستقیماً به سرور حمله کند.

Security Categories ...

- **DETECTION**

- Detecting intruders is similar to the **function of an alarm system** for Protecting facilities when an unauthorized activity appears.

◦ هنگام شناسایی یک فعالیت غیرمجاز، شناسایی مزاحمان شبیه به عملکرد سیستم هشدار دهنده است.

Security Categories...

- **RESPONSE**
 - Honeypots provide exact evidence of malicious activities and gives the information of the attack to prevent any such in the future and to start the countermeasures.
 - Honeypots شواهد دقیقی از فعالیت های مخرب ارائه می دهد و اطلاعات مربوط به حمله را برای جلوگیری از بروز چنین مواردی در آینده و شروع اقدامات متقابل ارائه می دهد.

Classification

03

Classification of HoneyPots

- Honeypot can be classified according to two :

According to their Implementation Environment

According to their Level of Interaction

با توجه به محیط اجرای آنها

با توجه به سطح تعامل آنها

- 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



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.

Production Honeypots ...

- 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**.
- Honeypots can utilize psychological weapons such as deception (mislead) or deterrence (prevention) to confuse or stop attacks.

• سلاح های روانی مانند فریب (گمراه) یا بازدارندگی (جلوگیری) برای سردرگمی یا متوقف کردن حملات استفاده کنند.

Research Honeypots

- The honeypot are **not implemented with the objective of protecting networks.**

• Honeypot با هدف محافظت از شبکه ها اجرا نمی شود.

- They represent educational resources of demonstrative and research nature whose objective is **cantered towards studying all sorts of attack patterns and threats.**

• آنها نمایانگر منابع آموزشی با ماهیت نمایش و تحقیق هستند که هدف آنها مطالعه انواع الگوهای حمله و تهدیدها است.

Research Honeypots ...

- 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.
- اصطلاح "سطح تعامل" طیف وسیعی از حملات را تعریف می کند که یک Honeypot اجازه می دهد تا یک مهاجم داشته باشد.
- 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.

Classified bases of Levels



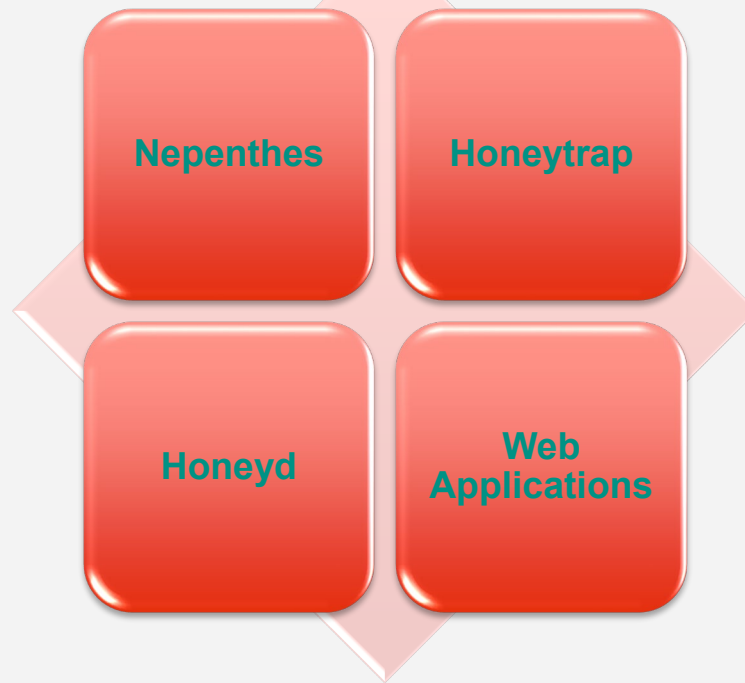
HoneyD
(Low-Interaction)



Honey net
(High-Interaction)

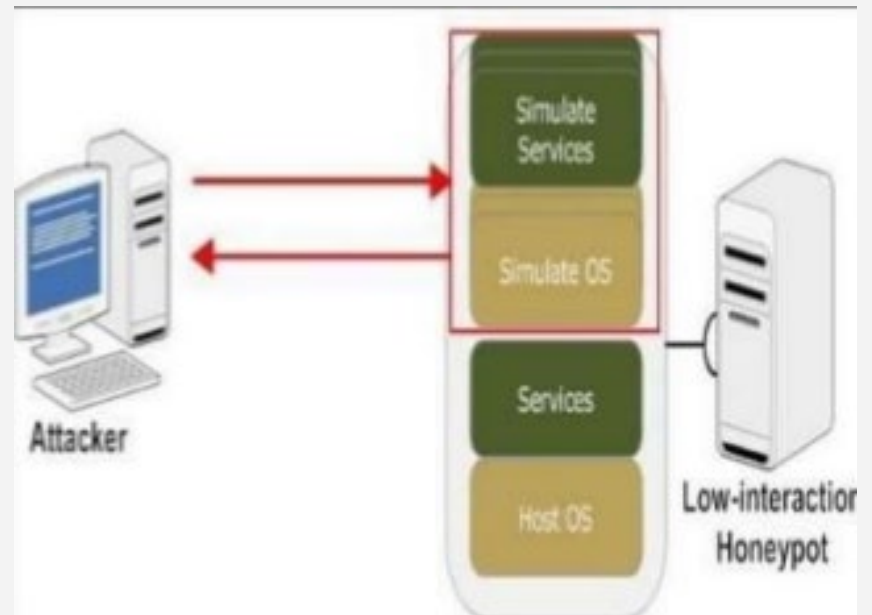
Low-Interaction Honeypot

- 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. هیچ تعامل با سیستم عامل ندارد.



Low-Interaction Honeypot ...

- *Emulate certain service and applications*
- *Identify Hostile IP*
- *Protect internet side of the network*
- *Capture limited information*



Low-Interaction Honeypot ...

- **Advantages**

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

- **Disadvantage**

- 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 **extreme** of honeypot technology
- Provide an attacker with a **real operating system** where nothing is emulated or restricted.

• یک سیستم عامل واقعی که در آن هیچ چیز شبیه سازی یا محدود نمی شود، به یک مهاجم ارائه دهید.

High-Interaction Honeypots ...

- It control an attacker at the **network level**.
- Information about attackers **motivation, actions, tools, behaviour, level of knowledge, origin, identity etc.**

• مهاجم را در سطح شبکه کنترل می کند.

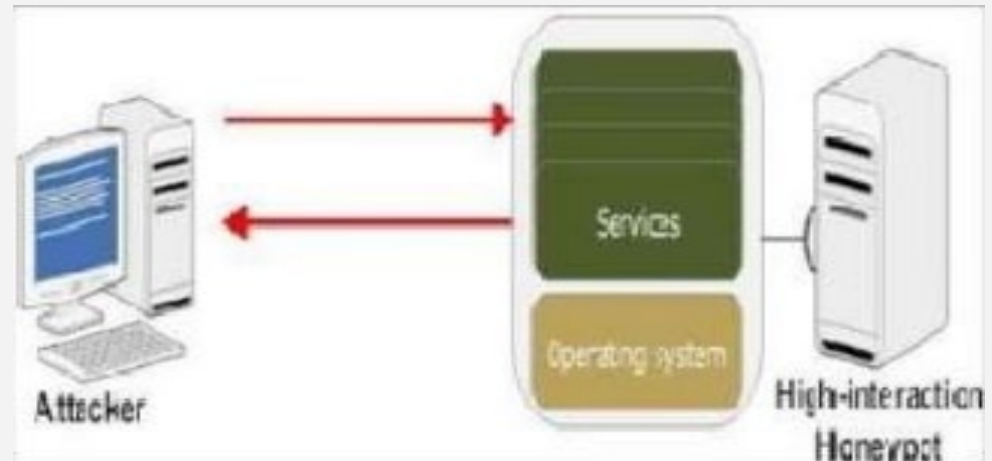
• اطلاعات مربوط به انگیزه مهاجمان، اقدامات، ابزارها، رفتار، سطح دانش، منشاء، هویت و غیره.

High-Interaction Honeypots ...

- **Honeynets**

- It provides **real systems, applications and services** for attackers to interact with, as opposed to low interaction honeypots such as honeyd.

◦ این سیستم ها، برنامه ها و سرویس های واقعی را برای مهاجمین فراهم می کند تا با آنها ارتباط برقرار کنند.



Advantage

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

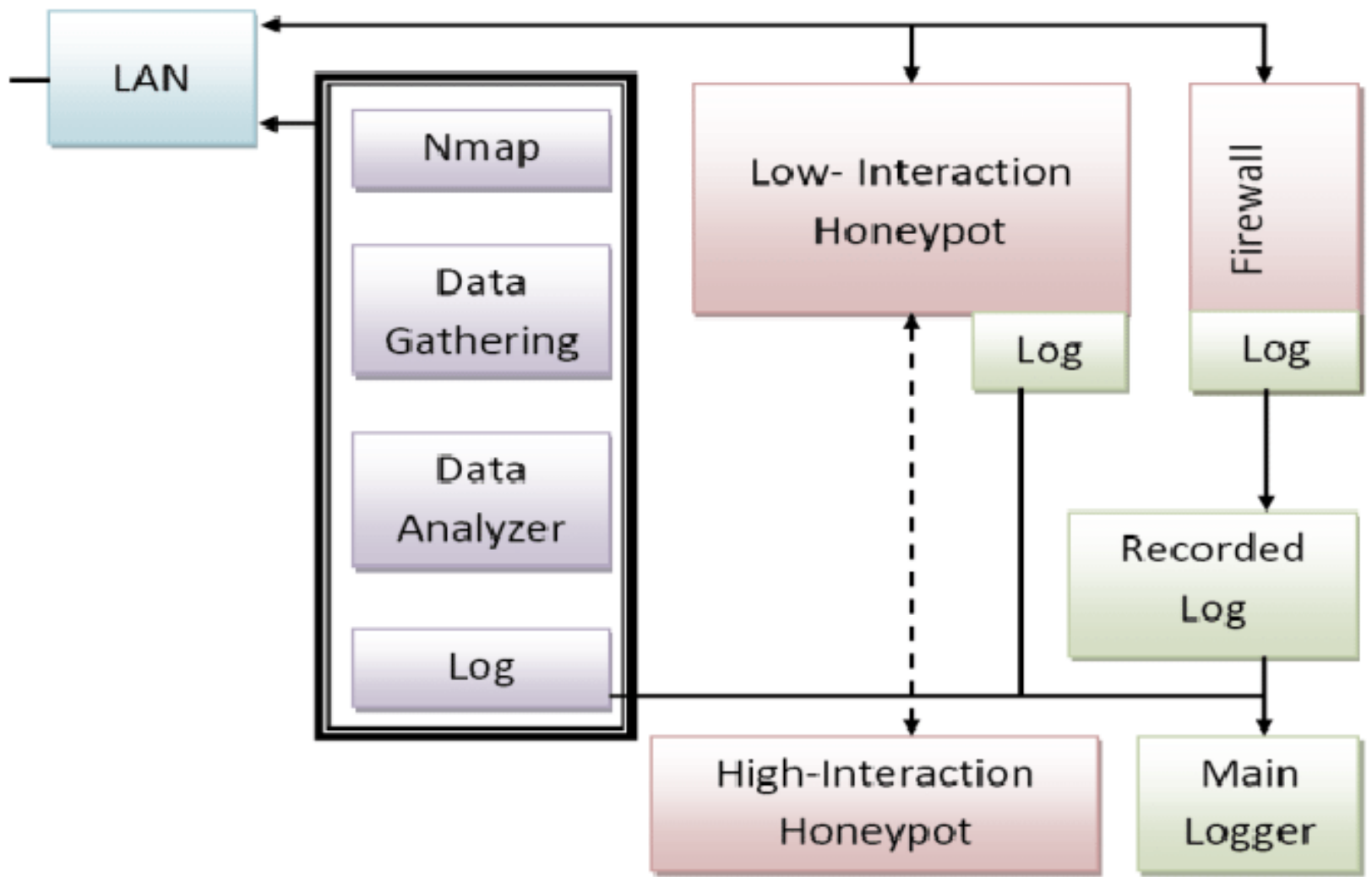
- **Building, configuring, deploying and maintaining** a high-interaction honeypot is very **time consuming** as it involves a variety of **different technologies** (e.g. IDS, firewall etc.) that has to be customized.
- **Analysing** a compromised honeypot is extremely **time consuming** (40 hours for every 30 minutes an attacker spend on a system).

Disadvantage ...

- Introduces a **high level of risk** and - if there are no additional precautions in place - might put an organizations overall IT security at stake.
- **Might lead to difficult legal situations.**

Comparision

Characteristics	Low-interaction Honeypot	High-interaction Honeypot
Degree of involvement	Low	High
Real OS	No	Yes
Risk	Low	High
Information Gathering	Connections	All
Compromised Wished	No	Yes
Knowledge to Run	Low	High
Knowledge to Develop	Low	High
Maintenance Time	Low	Very High



Implementation

04

Honeypot Implementation

- Honeypots are **digital network bait** and use deception to attract intruders to the system. A honeypot with **different layers** can be **slow down the attack**, thereby making the attack to be **detected easily**.

• Honeypots طعمه شبکه دیجیتال است و از فریب برای حمله به متجاوزان به سیستم استفاده می کند. Honeypots با لایه های مختلف می تواند حمله را کند نماید و از این طریق حمله را به راحتی تشخیص دهد.

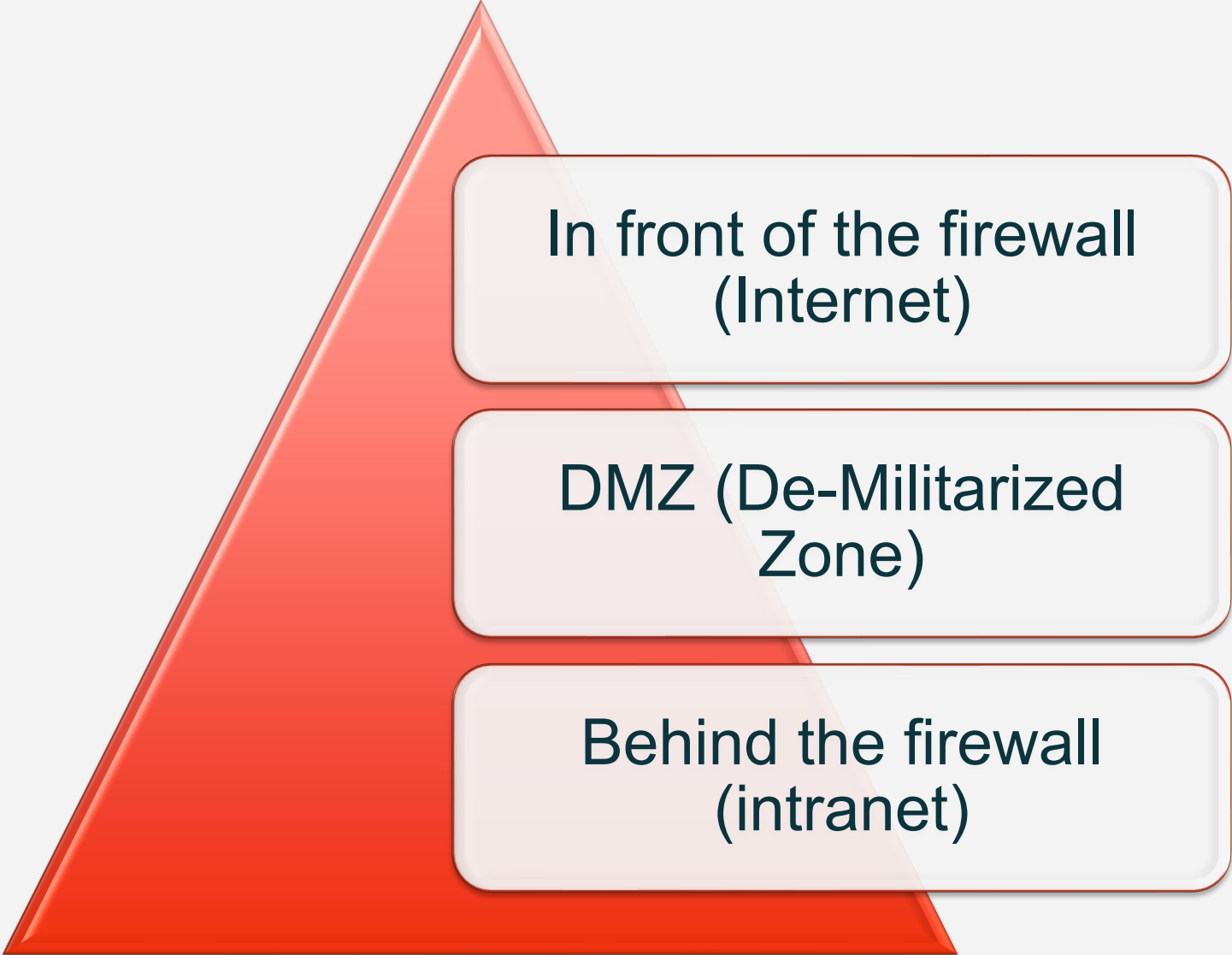
- *Intrusion detection and logging applications can be deployed within the honeypot.*

Honeypot Implementation ...

- The main concept of honeypot is to **learn from intruder's actions**. Additionally, honeypots are **not designed** to be the sole source of security for any network; *they should be used in conjunction with other security measures*.

- مفهوم اصلی honeypot یادگیری از اقدامات متجاوز است. علاوه بر این honeypot تنها منبع امنیتی برای شبکه طراحی نشده اند. آنها باید در کنار سایر اقدامات امنیتی استفاده شوند.

Place of Honeypot

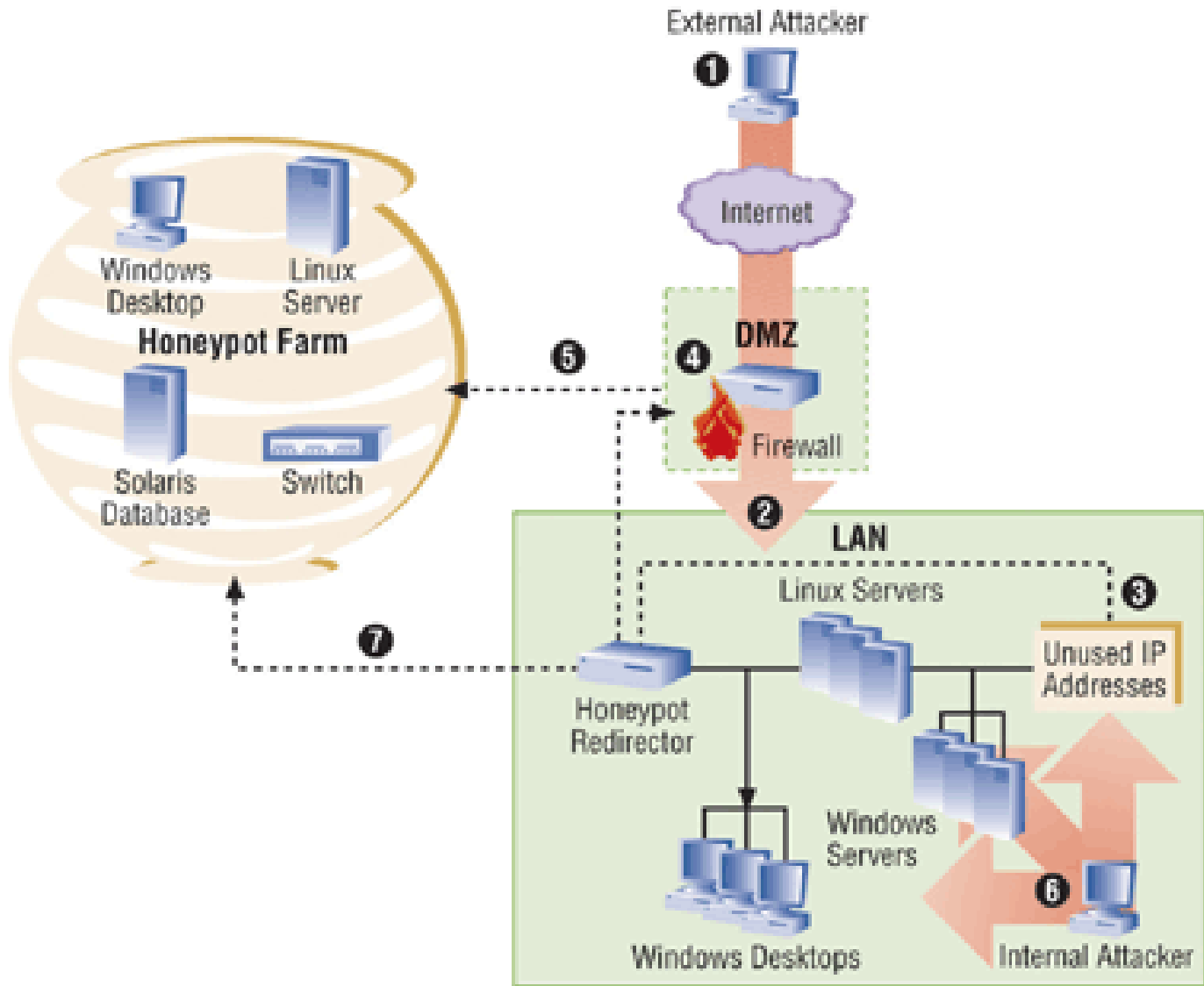


In front of the firewall
(Internet)

DMZ (De-Militarized
Zone)

Behind the firewall
(intranet)

Honeypot farm



Honeypot Farm ...

- **External attacker:** 1 Penetrates the DMZ and scans Network IP addresses 2 The direction appliance 3 monitors all unused address, and use Layer 2 VPN technology to enable the firewall 4 to redirect the intruder to the honeypot farm 5 which may have honeypot computers mirroring all types of real network devices.
- Similarly, an **internal attacker:** 6 scanning the network for vulnerable systems (such as open file shares) is redirected 7 by the honeypot appliance when he probes unused IP addresses.

**Advantage &
Disadvantage**

05



Advantages of Honeypots

- **Valuable Data Collection** جمع‌آوری داده‌های ارزشمند
 - Collect data **without noise**, usually **high value**. Makes data sets smaller and data analysis less complex.
- **Independent from Workload** مستقل از حجم کار
 - only need **to process traffic**.
 - they are **independent**

Advantages of Honeypots ...

- **Zero-Day-Exploit Detection** تشخیص استفاده روز صفر
 - capture everything that is used against them, i.e. **unknown strategies** and **zero-day-exploits**.
- **Reduced False Positives and Negatives**
 - کاهش مثبت و منفی کاذب
 - Any activity with server-honeypots is an anomaly, which is by definition an attack.
- **Flexibility** انعطاف پذیری
 - vast amount of **different honeypot software**.

Disadvantages of Honeypots

- **Limited Field of View** میدان دید محدود
 - have one common problem: they are **worthless if no one attacks them.**
- **Being Fingerprinted** اثر انگشت بودن
 - LIH emulate services, that means that their **services might behave different than the real services**
- **Risk to the Environment** خطر برای محیط
 - If honeypots get exploited, the higher the interaction level, the higher the possible misuse.

Distinction Between Security Concepts

Objective	Prevention	Detection	Reaction
Honeypot	+	++	+++
Firewall	+++	++	+
IDS	+	+++	+
IPS	++	+++	++
Anti-virus	++	++	++
Log-Monitoring	+	++	+
Cyber Security Standard	+++	+	+

Thanks for your Attention.