# HONEYPOTS

PRESENTED BY,
SARANYA.S
S7  CSE

# CONTENTS

- Introduction
- What are Honey pots?
- Classification
- Honeyd
- Honeynet
- Advantages of honeypot
- Disadvantages of honeypot
- Conclusion

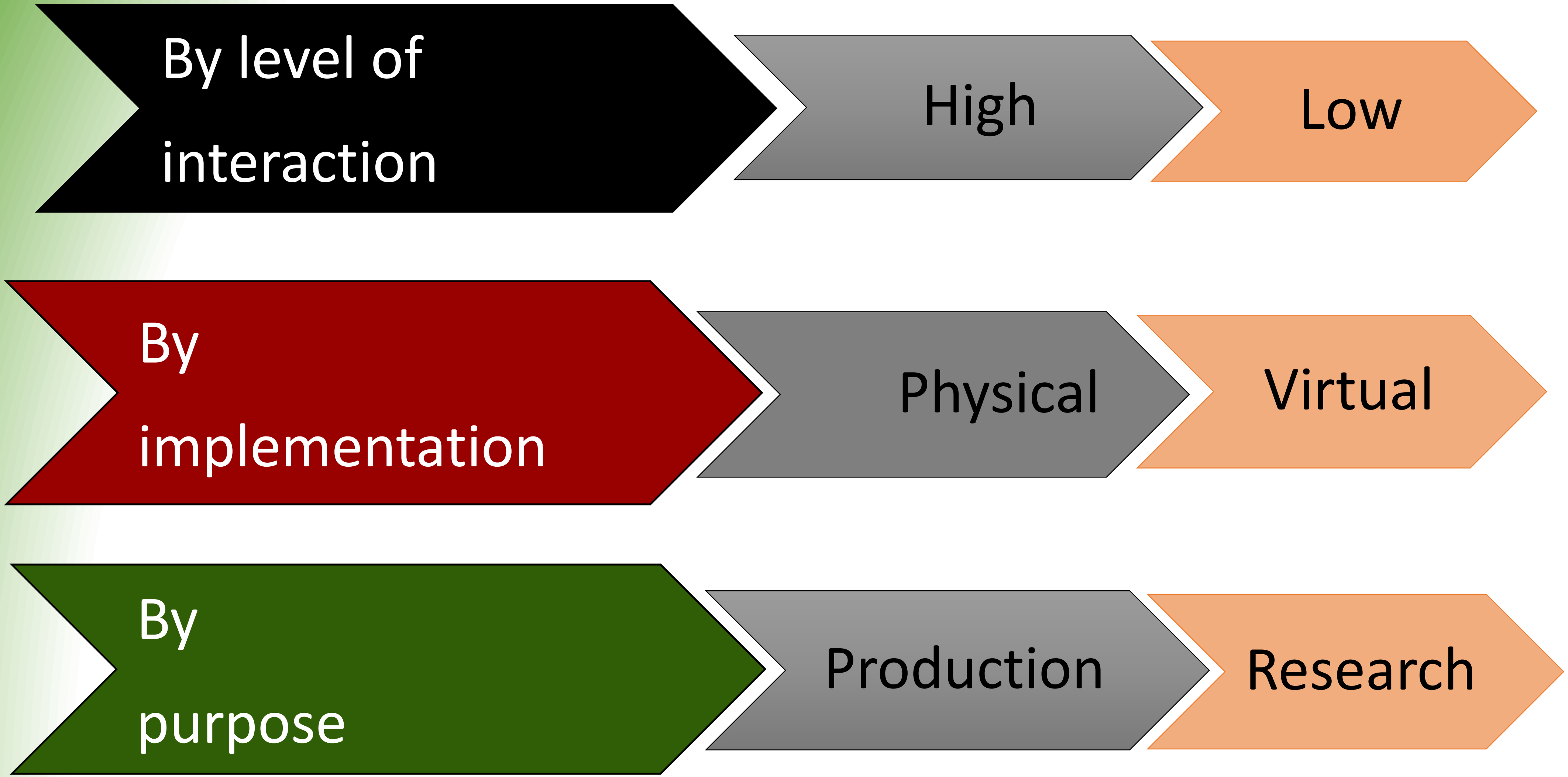
# INTRODUCTION

- The internet is growing very fast.
- New attacks every day
- The more you know about your enemy, the better you can protect yourself.
- The main goal of honeypot is to gather as much information as possible.

# WHAT ARE HONEYPOTS?

- Honeypot is an exciting new technology with enormous potential for the security community.
- ***According to Lance Spitzner, founder of honeypot project: "A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource."***
- Used for monitoring, detecting and analyzing attacks

# CLASSIFICATION



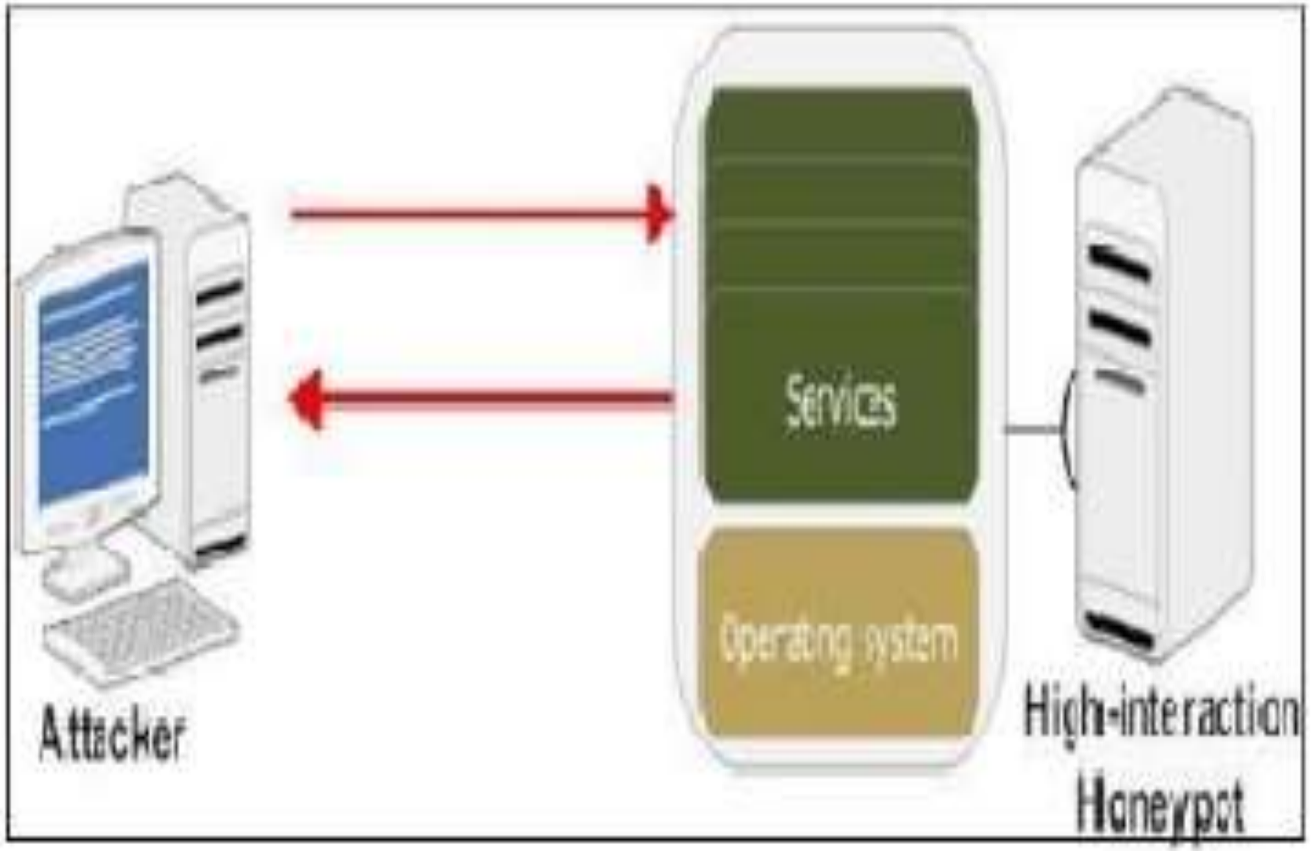
By level of interaction — High — Low

By implementation — Physical — Virtual

By purpose — Production — Research

# High interaction

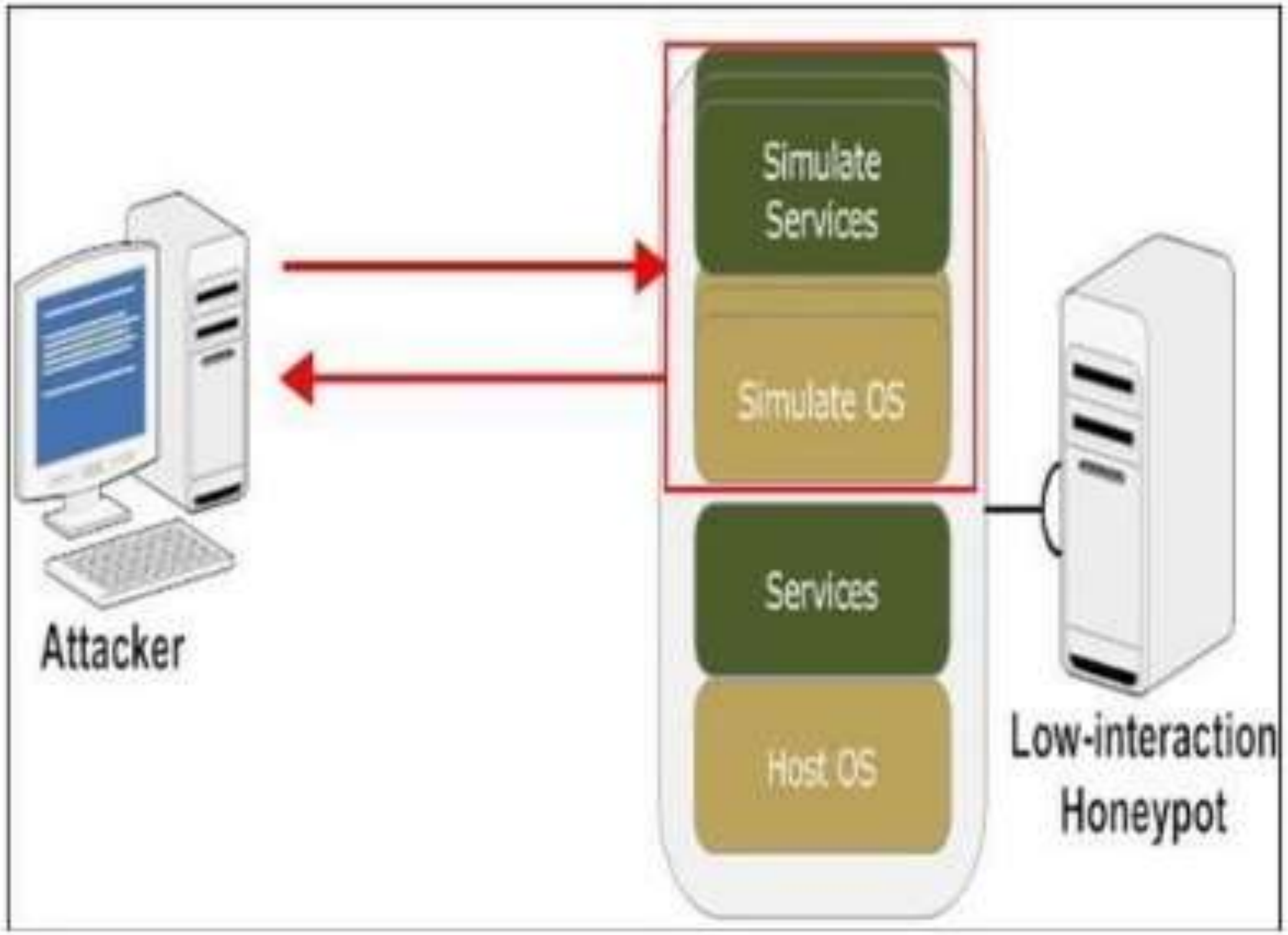
- Simulates all aspects of the OS: real systems.
- Can be compromised completely, higher risk.
- More Information
- Eg:-Honeynet



Architecture of high interaction honeypots

# Low interaction

- Simulates some aspects of the system
- Easy to deploy, minimal risk
- Limited Information
- Eg:- Honeyd



Architecture of low interaction honeypots

# Physical Honeypots

- Real machines
- Own IP Addresses
- Often high-interactive

# Virtual Honeypots

- Simulated by other machines that:
  - Respond to the network traffic sent to the honeypots
  - May simulate a lot of (different) virtual honeypots at the same time

# Production Honeypots

- Help to mitigate risk in your organizations
- 3 categories:

  1. Prevention

     - Keeping the bad guys out
     - Mechanism such as encryption prevent attackers from accessing critical information.

# Contd…

## 2. Detection

- Detecting the attacker when he breaks in.
- Challenges: False positive, False negative

## 3.Response

- Can easily be pulled offline

# Research  Honeypots

- Capture extensive information
- Used primarily by research, military, government organization.
- Used:
  - To capture automated threats, such  autorooters
  - To capture unknown tools or techniques
  - To  better understand attackers motives

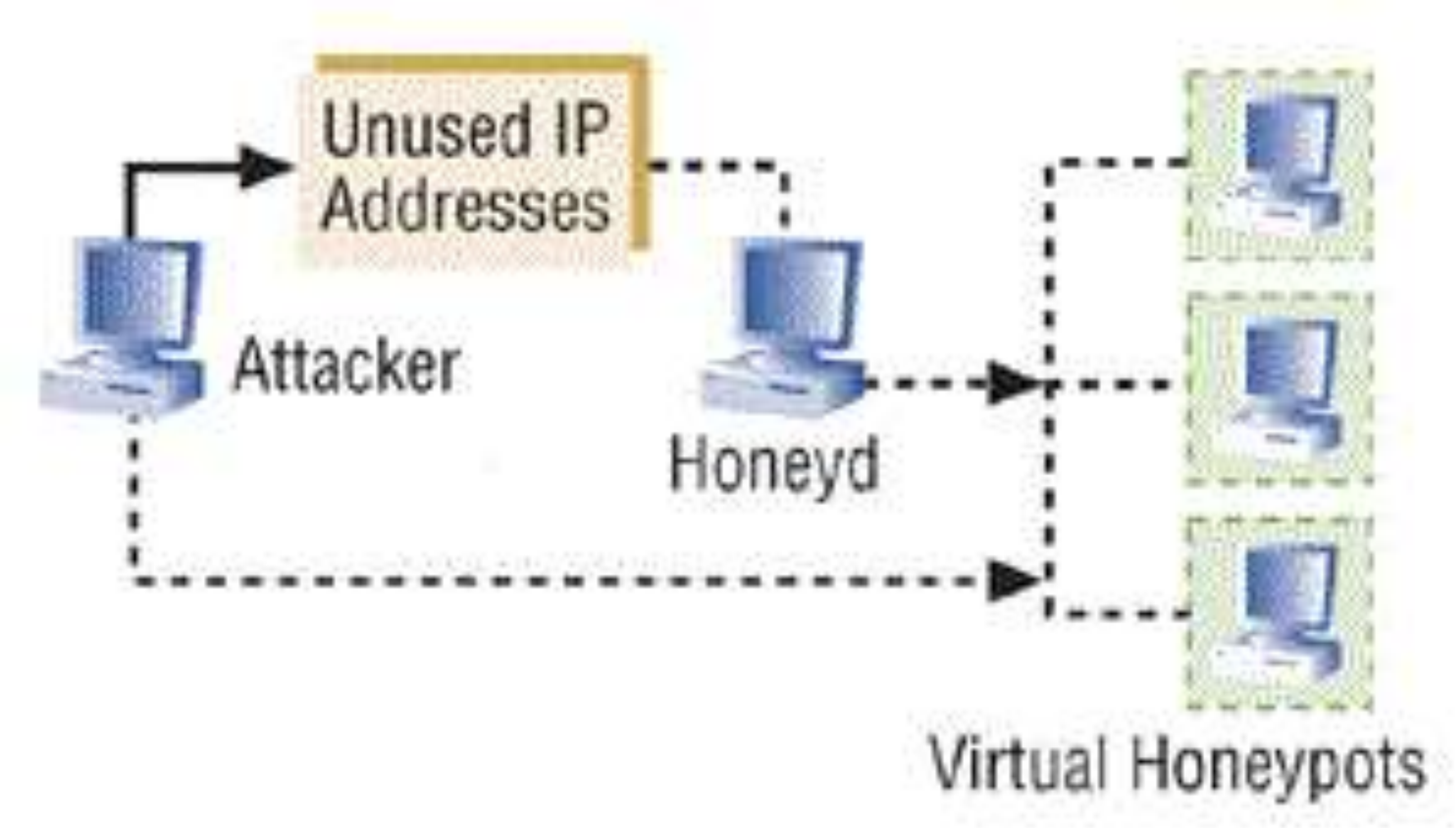
# HONEYD

- Open source software released under GNU General Public License.
- Able to simulate big network on a single host.
- Provides  simple functionality.

# A Honeyd config file

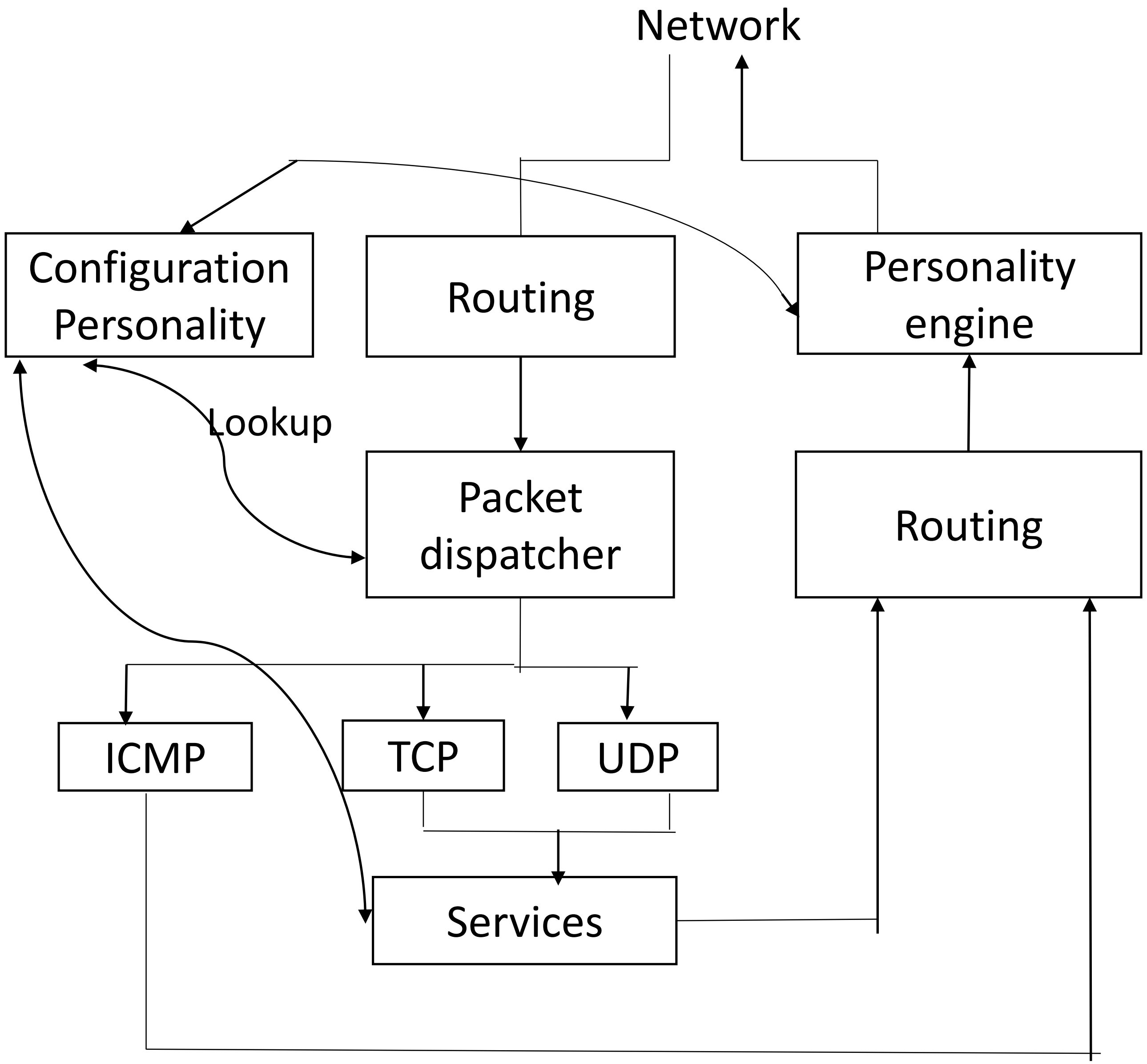
```
create windows
set windows personality "Windows NT 4.0 Server SP5-SP6"
set windows default tcp action reset
set windows default udp action reset
add windows tcp port 80 "perl scripts/iis-0.95/iisemul8.pl"
add windows tcp port 139 open
add windows tcp port 137 open
add windows udp port 137 open
add windows udp port 135 open
set windows uptime 3284460
bind 192.168.1.201 windows
```

# How Honeyd Works?



# Overview of honeyd architecture

- Packet dispatcher
- Configuration  database
- Protocol handlers
- Router
- Personality engine

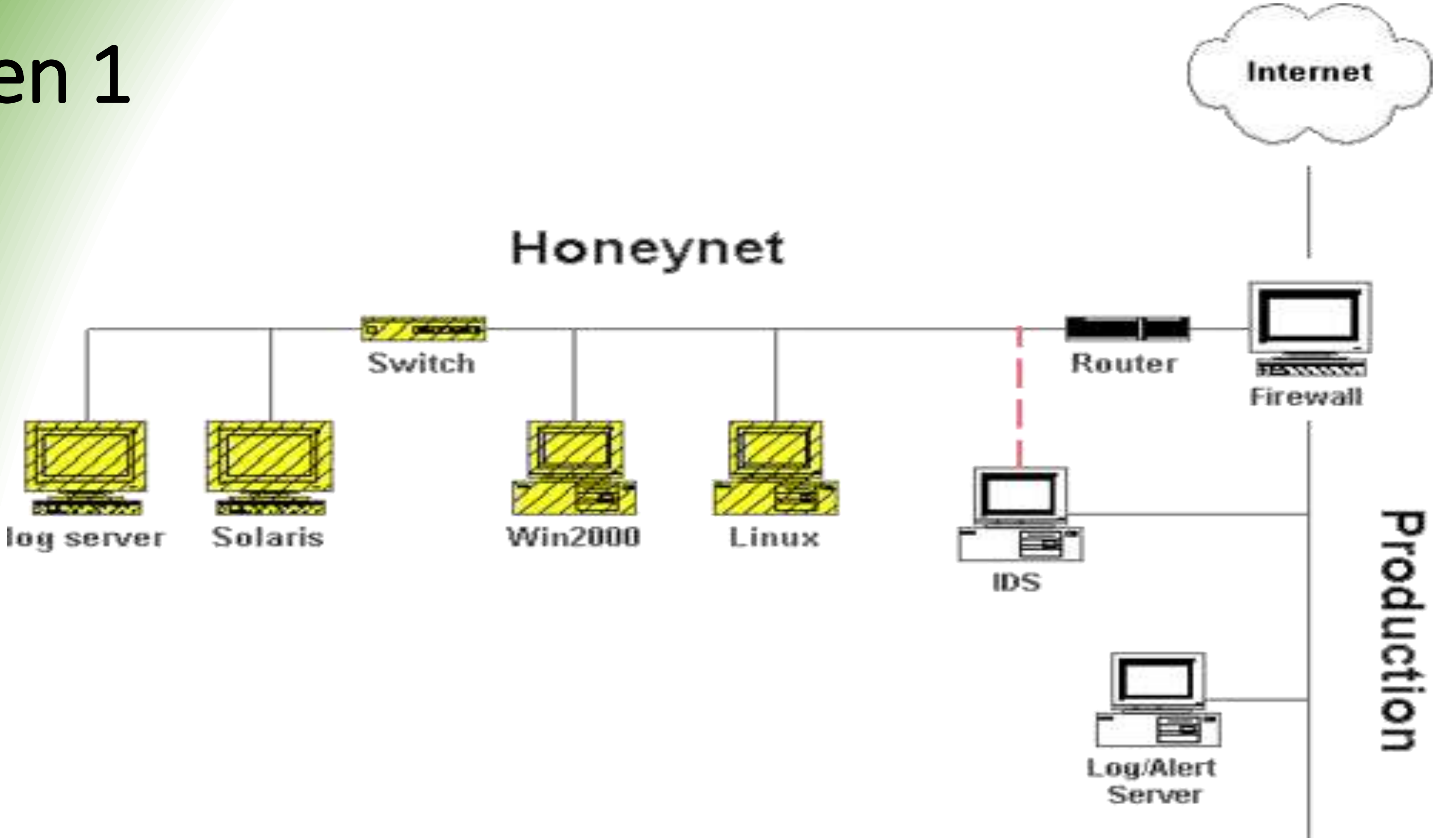


# HONEYNET

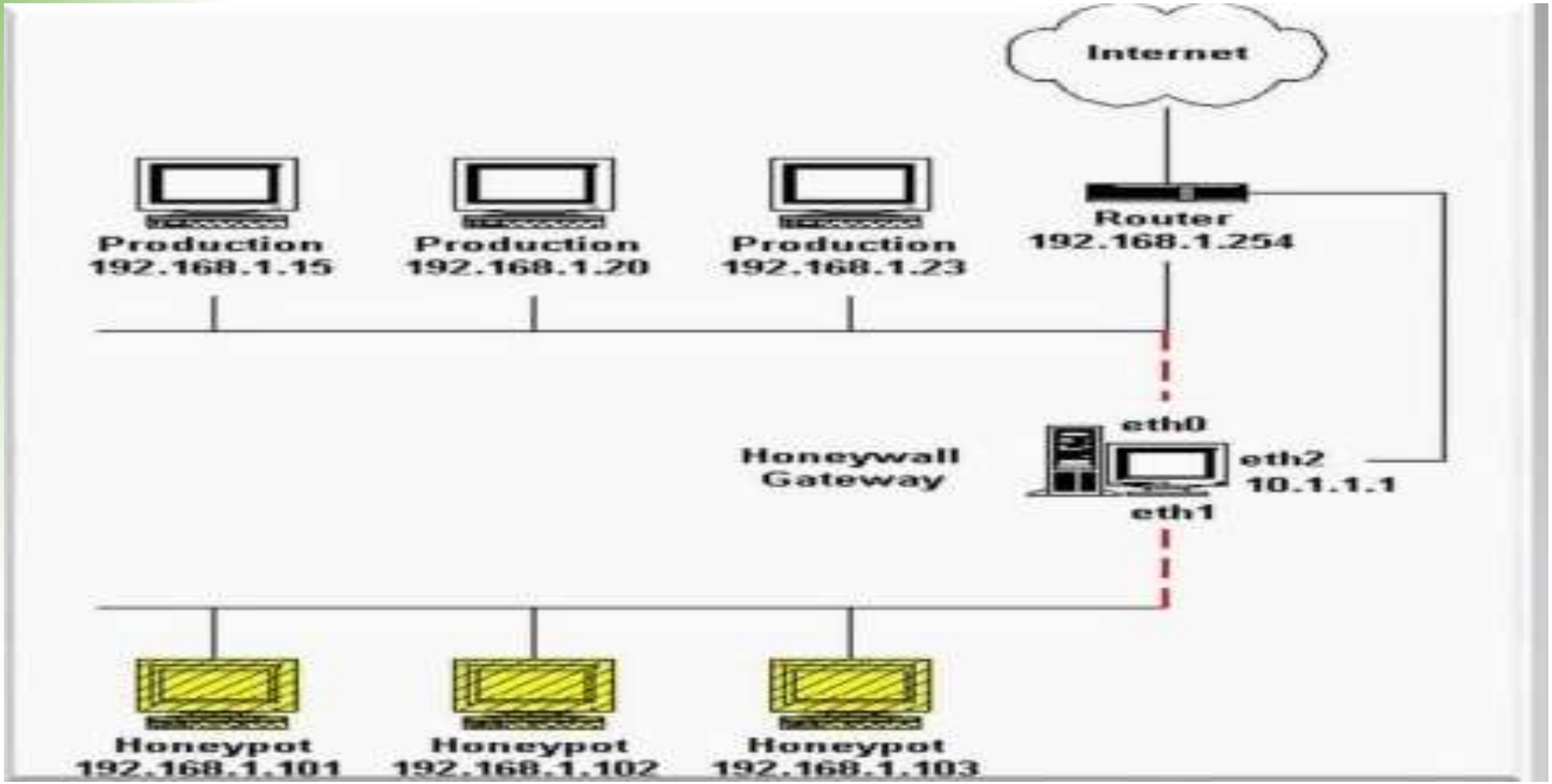
- High interaction honeypots
- Two or more honeypots on a network form a **honeynet**.
- It is basically an architecture, an entire network of computers designed to be  attacked.
- The key to the honeynet architecture  is  “Honey wall”.

# ARCHITECTURE OF HONEYNET

# Gen 1


Internet
Honeynet
Switch
Router
Firewall
log server
Solaris
Win2000
Linux
IDS
Production
Log/Alert Server

# Gen 2



Internet
Router
192.168.1.254
Production
192.168.1.15
Production
192.168.1.20
Production
192.168.1.23
eth0
Honeywall
Gateway
eth2
10.1.1.1
eth1
Honeypot
192.168.1.101
Honeypot
192.168.1.102
Honeypot
192.168.1.103

# Advantages of Honeypots

- ➢Collect small data sets of high value
- ➢Reduced false positive
- ➢Cost effective
- ➢Simplicity
- ➢Minimal resources

# Disadvantages of Honeypots

- Limited view
- Risk
- Finger Printing

# CONCLUSION

- Effective tool for observing hacker movements as well as preparing the system for future attacks.
- Flexible tool with different applications to security
- Primary value in detection and information gathering.

# REFERENCES

- R. R. Patel and C. S. Thaker, “Zero-day attack signatures detection using honey-pot,” International Conference on Computer Communication and Networks CSI-COMNET-2011, vol. 1, no. 1, pp. 4–27, 2011.
- Lance Spitzner. To build a honeypot. http://www.spitzner.net/honeypot.html.
- http://www.tracking-hackers.com/papers/honeypots.html
- The Honeynet Project, “Know Your Enemy: Statistics,” available online:http://honeynet.org/papers/stats
- http://www.honeynet.org
- http://project.honeypot.org

# QUESTIONS…….

# THANKYOU