

# Honeynets

## Introduction to Honeypot/Honeynet technologies and Its Historical Perspective

Alexandre Dulaunoy

ASBL CSRRT-LU (Computer Security Research and Response Team  
Luxembourg)

<http://www.csrrt.org/>

January 28, 2009

### Introduction

- Historical Perspective
- Historical Perspective
- Honeynets/pots - a definition ?

### Honeynets/pots - Types and variation

- Large classes of Honeynets
- Data capture versus Honeypots
- Low-interaction Honeypot
- High-interaction Honeypot
- Different usage of Honeynets

### Honeynets/pots - Advantages/ Disadvantages

### Conclusion

### Q and A

### Diagrams

# Introduction and Source of HoneyNet Research

Honeynets

Alexandre  
Dulaunoy

- ▶ With the introduction to new technologies, new opportunities were introduced to our society but also new related risks.
- ▶ The networks are growing and composed of a multitude hosts that could be compromised or used for non-legitimate use.
- ▶ A lot of potential attackers is waiting...
- ▶ To best defend yourself, it's to understand of the attackers (who? how? maybe why?).

## Introduction

Historical Perspective  
Historical Perspective  
Honeynets/pots - a definition ?

## Honeynets/pots - Types and variation

Large classes of Honeynets  
Data capture versus Honeypots  
Low-interaction Honeypot  
High-interaction Honeypot  
Different usage of Honeynets

## Honeynets/pots - Advantages/Disadvantages

Conclusion

Q and A

Diagrams

# Historical perspective

There were a lack of public information about the attackers of information systems. Attempts and publication were made between 1988 and 1999 like :

- ▶ Clifford Stoll - 1989 - The Cuckoo's Egg or the 75 cents issue.
  - ▶ Bill Cheswick's paper - 1991 - An Evening with Berferd
- during 1999, various people were thinking to get together to learn more about attackers. HoneyNet research started...

# Honeynet evolution

- ▶ 1997, DTK (Deception Toolkit)
- ▶ 1999, a single sacrificial computer,
- ▶ 2000, Generation I Honeynet,
- ▶ 2003, Generation II Honeynet,
- ▶ 2003, Honeyd software
- ▶ 2004, Distributed Honeynets, Malware Collector...

Building tools to learn from the attackers is a never ending circle.

Introduction

Historical Perspective

**Historical Perspective**

Honeynets/pots - a definition ?

Honeynets/pots -  
Types and  
variation

Large classes of  
Honeynets

Data capture versus  
Honeypots

Low-interaction  
Honeypot

High-interaction  
Honeypot

Different usage of  
Honeynets

Honeynets/pots -  
Advantages/  
Disadvantages

Conclusion

Q and A

Diagrams

# Honeynets/Honeypots - a definition ?

A (possible) definition : A honeypot is an (information) system resource whose values lies in an unauthorized or illicit usage of that resource.

A more computer-oriented definition :

*In computer terminology, a honeypot is a trap set to detect, deflect or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data or a network site that appears to be part of a network but which is actually isolated and protected, and which seems to contain information or a resource that would be of value to attackers.*

Introduction

Historical Perspective

Historical Perspective

Honeynets/pots - a  
definition ?

Honeynets/pots -  
Types and  
variation

Large classes of  
Honeynets

Data capture versus  
Honeypots

Low-interaction  
Honeypot

High-interaction  
Honeypot

Different usage of  
Honeynets

Honeynets/pots -  
Advan-  
tages/Disadvantages

Conclusion

Q and A

Diagrams

# Classification of Honeynets

Honeypots can generally be divided into different categories following the kind of interaction they have with the attackers

:

- ▶ low-interaction (honeyd, dtk, proxypot, ...)
- ▶ medium-interaction (nepenthes, mwcollect, ...)
- ▶ high-interaction (complete "vulnerable" operating system virtualized or not)

Honeynets can be composed by different kind of honeypots.

Introduction

Historical Perspective  
Historical Perspective  
Honeynets/pots - a definition ?

Honeynets/pots -  
Types and  
variation

Large classes of  
Honeynets

Data capture versus  
Honeypots  
Low-interaction  
Honeypot  
High-interaction  
Honeypot  
Different usage of  
Honeynets

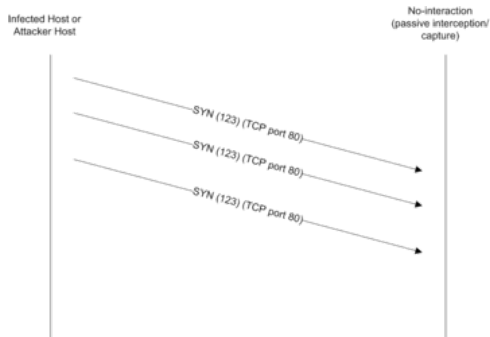
Honeynets/pots -  
Advan-  
tages/Disadvantages

Conclusion

Q and A

Diagrams

# Data capture versus Honeypots



Network data capture is a passive activity and there is no interaction with the potential attacker. The information collected is limited and doesn't help the classification of the potential attacks.

## Introduction

- Historical Perspective
- Historical Perspective
- Honeynets/pots - a definition ?

## Honeynets/pots - Types and variation

- Large classes of Honeynets
- Data capture versus Honeypots**
- Low-interaction Honeypot
- High-interaction Honeypot
- Different usage of Honeynets

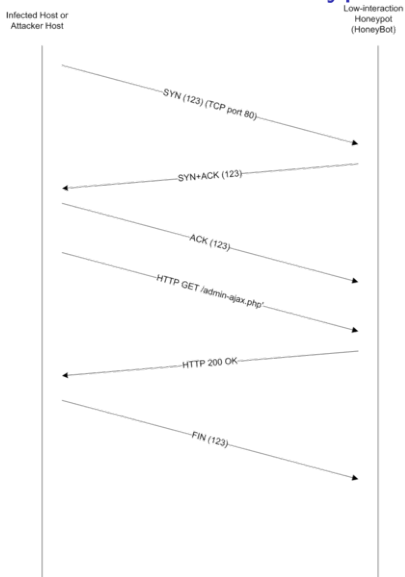
## Honeynets/pots - Advantages/Disadvantages

## Conclusion

## Q and A

## Diagrams

# Low-interaction Honeypot



The low-interaction is faking a part of a network services and by so having an interaction with the attacker.

Honeynets

Alexandre  
Dulaunoy

Introduction

- Historical Perspective
- Historical Perspective
- Honeynets/pots - a definition ?

Honeynets/pots -  
Types and  
variation

- Large classes of Honeynets
- Data capture versus Honeypots

**Low-interaction Honeypot**

- High-interaction Honeypot
- Different usage of Honeynets

Honeynets/pots -  
Advantages/  
Disadvantages

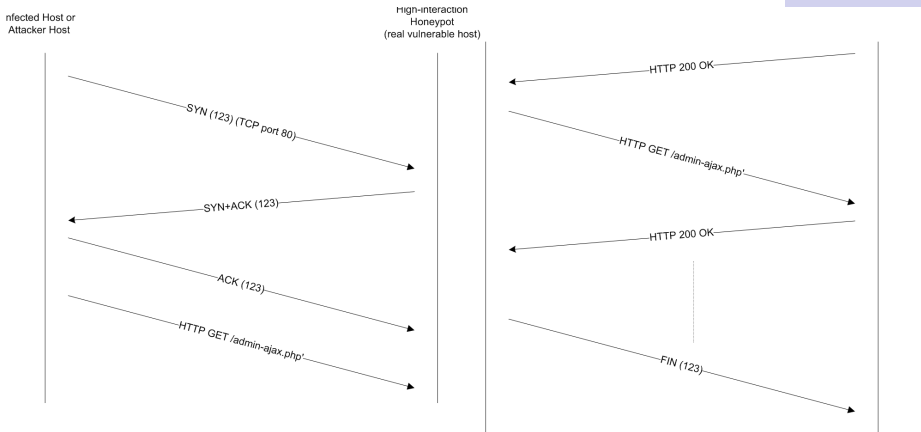
Conclusion

Q and A

Diagrams



# High-interaction Honeypot



The high-interaction honeypot is often working by proposing the real network service.

# The known usage of Honeynets

- ▶ Spam traps (to not mix with email/spam trap) is to catch Spammer trying to use open services (like HTTP proxy, misconfigured SPAM). From the information collected, you can build table of known spammer or see their approach on how they use Internet resources.
- ▶ Security Research. To learn on how and why they are attacking systems. To see the usage of compromised system. The main purpose is clearly to learn by seeing and improve our skills in computer security. -¿ Raise Awareness by giving out the results and Training.
- ▶ Security Mitigation. To use honeynets as a platform to divert attackers from some other systems. To get an early warning platform.

Introduction

Historical Perspective  
Historical Perspective  
Honeynets/pots - a definition ?

Honeynets/pots -  
Types and  
variation

Large classes of  
Honeynets  
Data capture versus  
Honeypots  
Low-interaction  
Honeypot  
High-interaction  
Honeypot  
Different usage of  
Honeynets

Honeynets/pots -  
Advan-  
tages/Disadvantages

Conclusion

Q and A

Diagrams

# Honeynets/pots - Advantages/Disadvantages

## Advantages :

- ▶ Honeypots are focused (small data sets)
- ▶ Honeypots help to reduce false positive
- ▶ Honeypots help to catch unknown attacks (false negative)
- ▶ Honeypots can capture encrypted activity (cf. Sebek)
- ▶ Honeypots work with IPv6
- ▶ Honeypots are very flexible (advantage/disadvantage?)
- ▶ Honeypots require minimal resources

## Disadvantages :

- ▶ Honeypots field of view limited (focused)
- ▶ Risk, risk... and risks.

### Introduction

Historical Perspective  
Historical Perspective  
Honeynets/pots - a definition ?

### Honeynets/pots - Types and variation

Large classes of Honeynets  
Data capture versus Honeypots  
Low-interaction Honeypot  
High-interaction Honeypot  
Different usage of Honeynets

### Honeynets/pots - Advantages/Disadvantages

### Conclusion

### Q and A

### Diagrams

# Conclusion

- ▶ Risks are part of Honeynet research and we have to manage it
- ▶ Honeynets are used to be better prepared to information system attacks
- ▶ Honeynets can early detect new threats and issues
- ▶ Honeynets are often a research playground to better learn security issues in information systems
- ▶ Honeynets are a source of in-depth information that classical information security system can't easily provide
- ▶ ... the area is still young and can provide new territories to better secure the information society.

Introduction

Historical Perspective  
Historical Perspective  
Honeynets/pots - a definition ?

Honeynets/pots -  
Types and  
variation

Large classes of  
Honeynets  
Data capture versus  
Honeypots  
Low-interaction  
Honeypot  
High-interaction  
Honeypot  
Different usage of  
Honeynets

Honeynets/pots -  
Advan-  
tages/Disadvantages

Conclusion

Q and A

Diagrams

# Q and A

- ▶ Thanks for listening.
- ▶ <http://www.csrirt.org.lu/>
- ▶ [adulau@foo.be](mailto:adulau@foo.be)

## Introduction

Historical Perspective  
Historical Perspective  
Honeynets/pots - a  
definition ?

## Honeynets/pots - Types and variation

Large classes of  
Honeynets  
Data capture versus  
Honeypots  
Low-interaction  
Honey-pot  
High-interaction  
Honey-pot  
Different usage of  
Honeynets

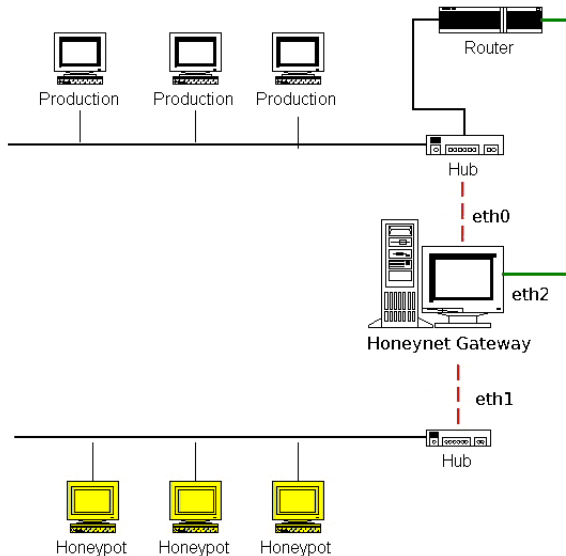
## Honeynets/pots - Advan- tages/Disadvantages

## Conclusion

## Q and A

## Diagrams

# Genl Honeynet + Mitigation



## Introduction

- Historical Perspective
- Historical Perspective
- Honeynets/pots - a definition ?

## Honeynets/pots - Types and variation

- Large classes of Honeynets
- Data capture versus Honeynets
- Low-interaction Honeypot
- High-interaction Honeypot
- Different usage of Honeynets

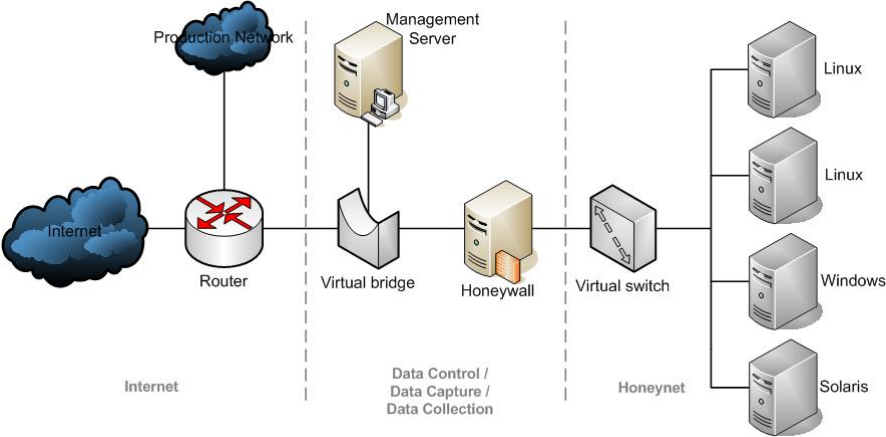
## Honeynets/pots - Advantages/Disadvantages

## Conclusion

## Q and A

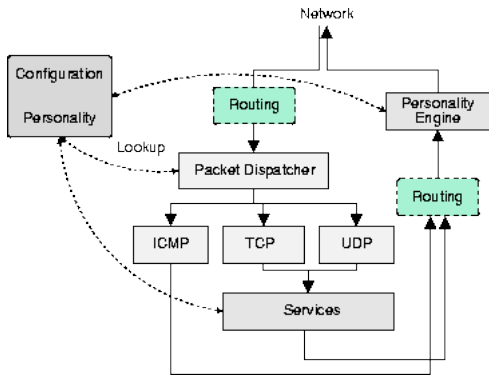
## Diagrams

# GenII Honeynet



Pakistan Honeynet Project – GenII Honeynet

# Honeyd design



from

<http://www.honeyd.org/>

## Introduction

- Historical Perspective
- Historical Perspective
- Honeynets/pots - a definition ?

## Honeynets/pots - Types and variation

- Large classes of Honeynets
- Data capture versus Honeypots
- Low-interaction Honeypot
- High-interaction Honeypot
- Different usage of Honeynets

## Honeynets/pots - Advantages/Disadvantages

## Conclusion

## Q and A

## Diagrams