

Pakistan Honeynet Project

Bank Scams: Latest Threat to Pakistani Online Banking

**Muhammad Omar Khan
Faiz Ahmad Shuja**

www.honey.net.org.pk

Muhammad Omar Khan

- System Security Engineer, CYBERNET
- Member, Pakistan Honeynet Project
- Member, PAKCON
- Pak Con 2004 CTF Hacking Contest Winner
- Involved in Security Research for last 4 years

Agenda

- Honeynet Project
 - Background
 - Basic Concepts
 - Tools and Technology
 - Generation III Honeynet
 - Phishing
 - Case Study

Honeynet Project

- Volunteer organization of security professionals.
- Open source, sharing all of the research and findings.
- Deploy networks around the world to be hacked.
- Goals
 - Awareness: To raise the awareness of threats that exists.
 - Information: For those already aware, to teach them and inform about threats.
 - Research: To give organization the capabilities to learn on their own.

Honeynet Research Alliance

- Started in 2002, the Alliance is a forum of organizations around the world actively researching, sharing and deploying honeypot technologies.
- Members (<http://www.honeynet.org/alliance/>)
 - Chinese Honeynet Project
 - The Spanish Honeynet Project
 - SIG² Internet Weather Forecast Centre
 - German Honeynet Project
 - Portugal Honeynet Project
 - Ga Tech Honeynet Project
 - French Honeynet Project
 - Italian Honeynet Project
 - **Pakistan Honeynet Project**
 - West Point Honeynet Project
 - UK Honeynet Project
 - Honeynet Project at the University of Texas at Austin
 - Brazilian Honeynet Project
 - Azusa Pacific University Honeynet
 - NetForensics Honeynet
 - Internet Systematics Lab Honeynet Project - Greece
 - Paladion Networks Honeynet Project - India
 - Florida HoneyNet Project

Agenda

- Honeynet Project
 - Background
 - Basic Concepts
 - Tools and Technology
 - Generation III Honeynets
 - Phishing
 - Case Study

Honeypots

- Formal Definition: A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.
 - An information gathering system, built to be compromised while being watched.
- Has no production value, anything going to or from a honeypot is likely a probe, attack or compromise.
 - Low False Positive Rate.
- Primary value to most organizations is information
 - Indication and Warnings to attack
 - Network Defense Intelligence (Info about attacker)

Types of Honeypots

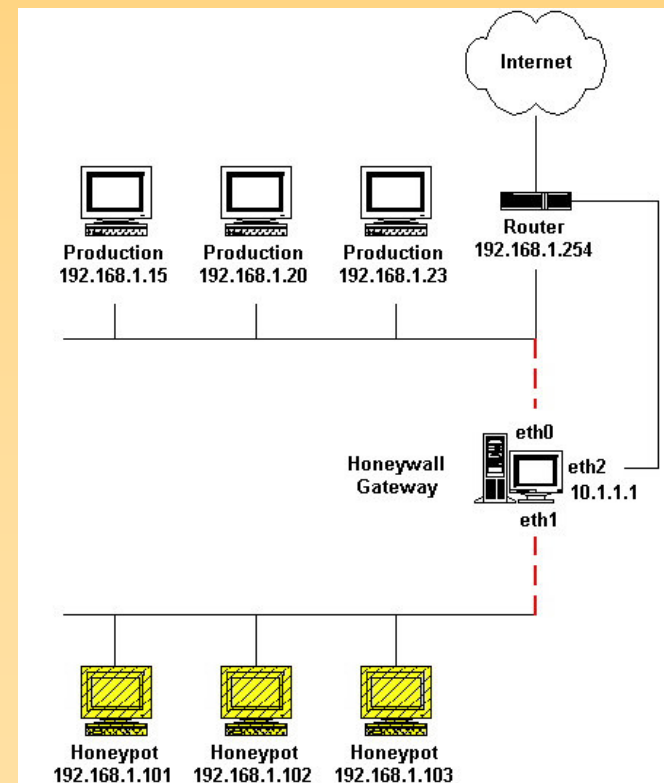
- Low-interaction
 - Emulates services, applications, and OS's.
 - Low risk and easy to deploy/maintain, but capture limited information.
- High-interaction
 - Real services, applications, and OS's
 - Capture extensive information, but high risk and time intensive to maintain.

Agenda

- HoneyNet Project
 - Background
 - Basic Concepts
 - Tools and Technology
 - Generation III HoneyNets
 - Phishing
 - Case Study

Building Blocks

- <http://www.honeynet.org/papers/honeynet/>
- A Honeynet is a network of high interaction Honeypots.
 - Data Control
 - Data Capture
 - Data Analysis



Data Control

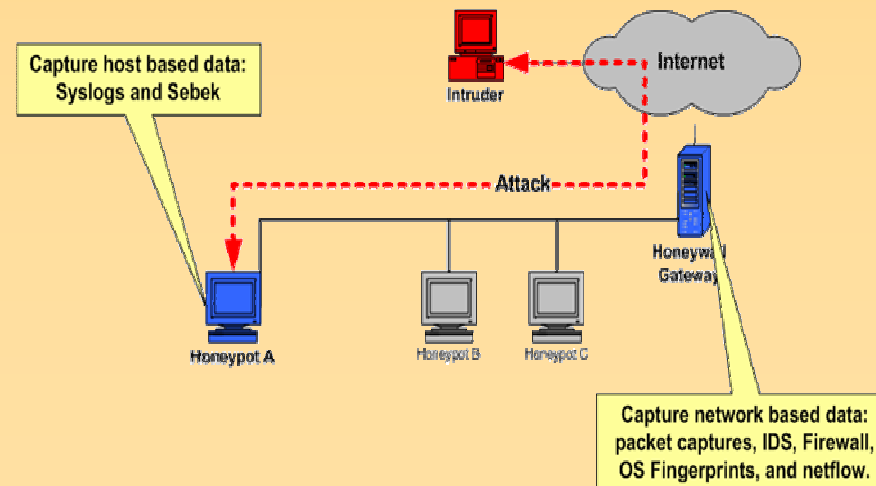
- Layer 2 bridge
- Iptables (packet limiting)
- Snort Inline (packet scrubbing)

Data Capture

- Snort
- Iptables logs
- Sebek
 - Designed to record volatile host data.
 - Specifically Keystrokes
 - Hidden kernel module or patch.

Sebek

- Sebek Data Capture tool
 - kernel space tool that monitors sys_read call
 - covertly exports data to server.
 - Used to monitor keystrokes, recover files, and other related activities even when session encryption used.
 - <http://www.honeynet.org/tools/sebek/>



Agenda

- Honeynet Project
 - Background
- Basic Concepts and
 - Tools and Technology
- Generation III Honeynets
 - Phishing
 - Case Study

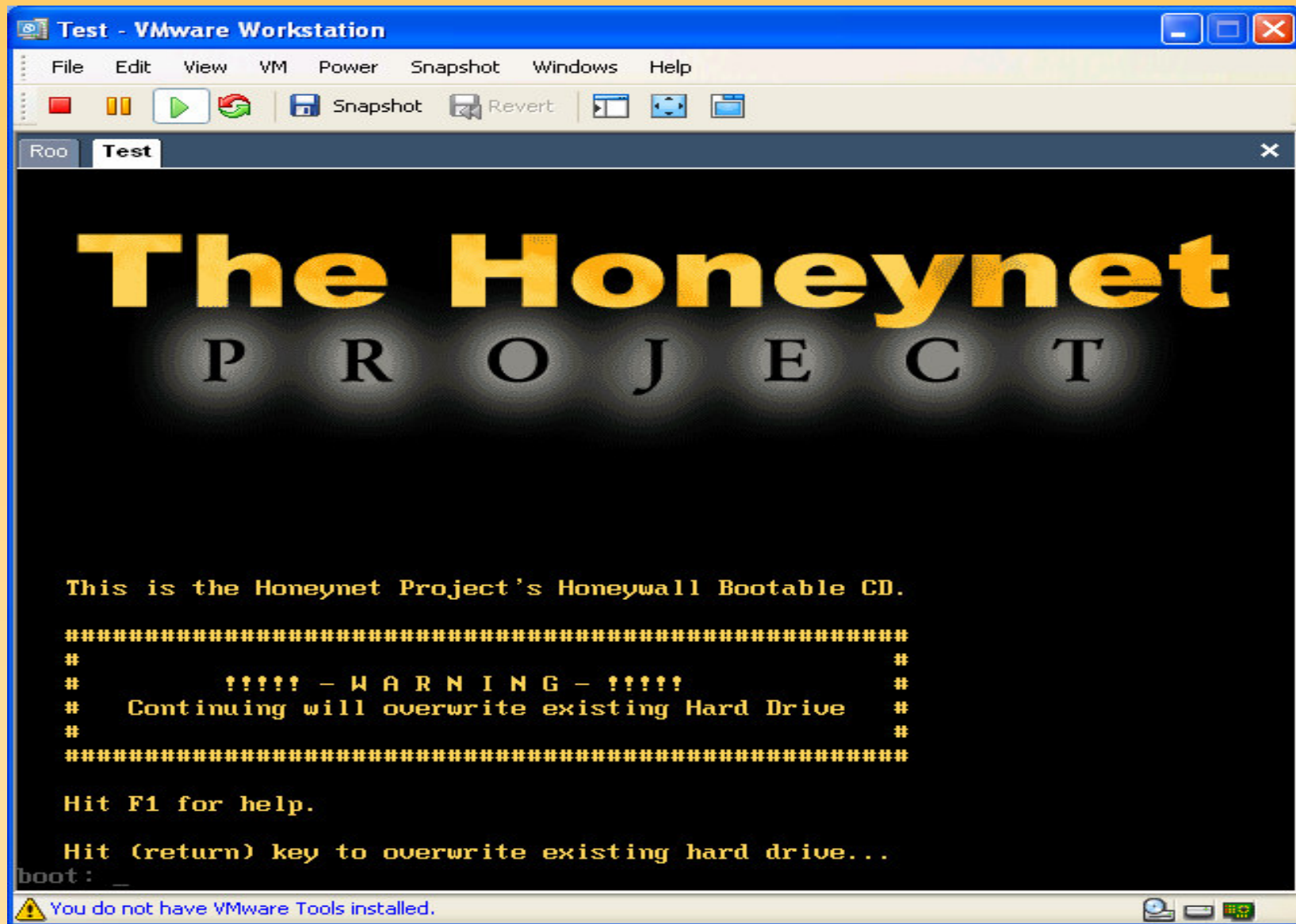
roo Bootable CDROM Honeywall

- Download
 - <http://www.honeynet.org/tools/cdrom/roo/download.html>
- Improvements of roo
 - Installation
 - Operation
 - Maintainability
 - Online Documentation
 - Data Capture
 - Data Analysis

Installation

- FC3 based
- Single CD, Bootable install iso (340 MB)
- Custom ks.cfg file (about 235 minimal rpms)
- 3-5 minutes install (hands off)
- Lockdown script runs on first boot
 - Bastille
 - CIS
 - NIST
- Auto-config on 1st boot via floppy.

Pakistan Honeynet Project



Operation of roo

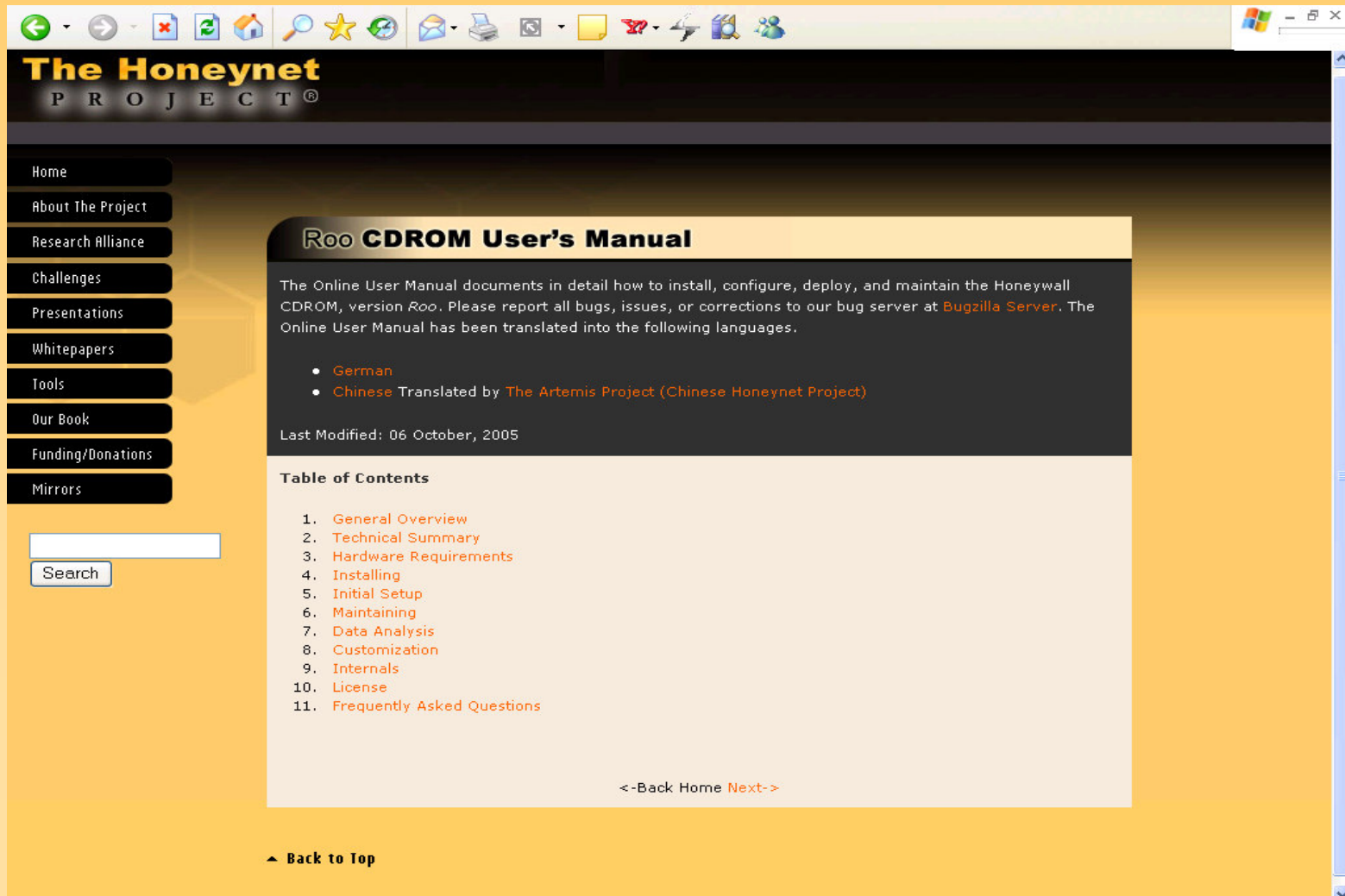
- Command line tools for operation
- Improved Console/SSH Dialogue Menu
- Shiny new Web User Interface (SSL)
 - Role Based Authentication
 - System Management
 - Status
 - Clear Logs
 - Configure
 - Data Analysis (walleye)

Maintainability of roo

- Entire System is RPM based
- Yum updatable
 - Fedora Core
 - DAG Repo
 - Honeynet.org Repo

roo Documentation

- <http://www.honeynet.org/tools/cdrom/roo/manual>
- <http://www.honeynet.org.pk/honeywall>



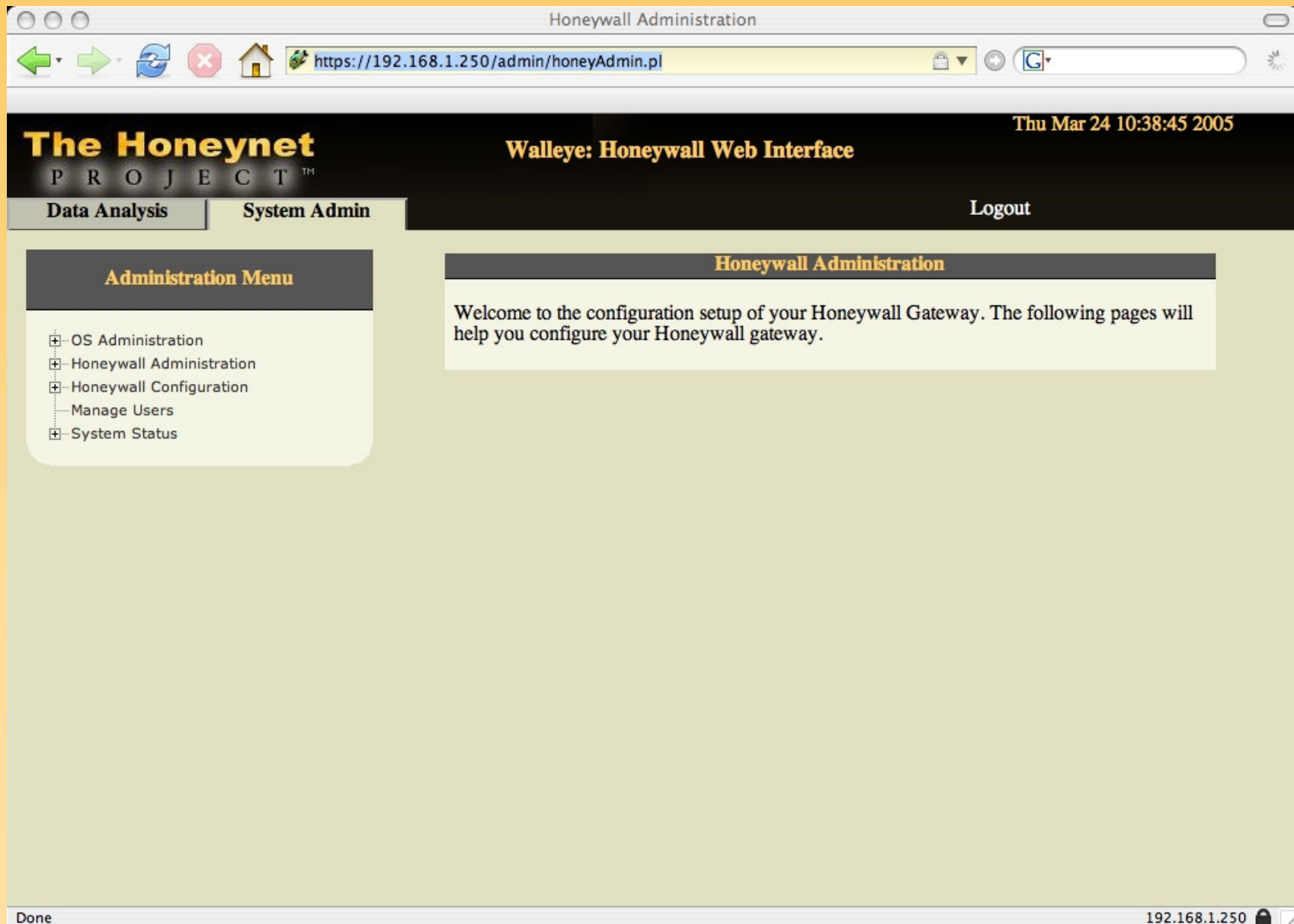
Walleye

“Eye on the Honeywall”

- Web based Honeynet data analysis tool
- Focus on big picture, Intrusion Sequence comprehension
- Don't attempt to be monolithic solution.

Pakistan Honeynet Project

Walleye



The screenshot shows a web browser window titled "Honeywall Administration". The address bar displays the URL <https://192.168.1.250/admin/honeyAdmin.pl>. The page header features the "The Honeynet PROJECT" logo on the left, the title "Walleye: Honeywall Web Interface" in the center, and the date "Thu Mar 24 10:38:45 2005" on the right. Below the header, there are three tabs: "Data Analysis", "System Admin" (which is active), and "Logout". The main content area is divided into two sections. On the left, under the heading "Administration Menu", there is a list of links: "OS Administration", "Honeywall Administration", "Honeywall Configuration", "Manage Users", and "System Status". On the right, under the heading "Honeywall Administration", there is a welcome message: "Welcome to the configuration setup of your Honeywall Gateway. The following pages will help you configure your Honeywall gateway." The browser's status bar at the bottom shows "Done" on the left and the IP address "192.168.1.250" on the right.

Honeywall Administration

[https://192.168.1.250/admin/honeyAdmin.pl](#)

The Honeynet
PROJECT™

Walleye: Honeywall Web Interface

Thu Mar 24 10:38:45 2005

Data Analysis System Admin Logout

Administration Menu

- OS Administration
- Honeywall Administration
- Honeywall Configuration
- Manage Users
- System Status

Honeywall Administration

Welcome to the configuration setup of your Honeywall Gateway. The following pages will help you configure your Honeywall gateway.

Done 192.168.1.250

Pakistan Honeynet Project

Mozilla Firefox

File Edit View Go Bookmarks Tools Help

← → ↺ × 🏠 🌐

https://192.168.41.10/walleye.pl

🔒 ⬇️ ⏪ Go 🔍

🐘 Getting Started 📡 Latest Headlines

The Honeynet
PROJECT®

Walleye: Honeywall Web
Interface

Wed Jun 15 10:33:19 2005
GMT
Logged in as admin

Data Analysis

System Admin

Logout

Online Sensors

Honeywall: 3232246026

Created: Tue May 31 05:14:31 2005 Last Update: Wed Jun 15 10:33:11 2005

Bidirectional		Total						
In	Out	In	Out					
con	ids	con	ids	con	ids	con	ids	
1 hour	0	0	4	1	0	0	45	41
48 hour	0	0	9	1	0	0	70	53

2000

1000

0

10:00 18:00 2:00 10:01

■ KBytes Transferred ■ N/10 Alerts

Search (short term soln)

Time

Start Jun 14 2005 10:33:19

End Jun 15 2005 10:33:19

IP Proto

ANY

⬇️

Either

Prefix

Port

0

Source

Prefix

Port

0

Destination

Prefix

Port

0

Result Format

Pcap File

⬇️

Submit Query

Done

192.168.41.10 🌐

Pakistan Honeynet Project

Mozilla Firefox
https://192.168.1.250/walleye.pl?act=overview&sensor=3232236026

The Honeynet
PROJECT™

Walleye: Honeywall Web Interface

Thu Mar 24 10:57:07 2005
Logged in as admin

[Data Analysis](#) | [System Admin](#) | [Logout](#)

Online Sensors

Honeywall: 3232236026
Created: Thu Mar 24 02:00:14 2005 Last Update: Thu Mar 24 10:55:30 2005

	Bidirectional				Total			
	In		Out		In		Out	
	con	ids	con	ids	con	ids	con	ids
1 hour	0	0	7	1	1	0	32	14
48 hour	0	0	8	1	2	0	100	14

KBytes Transferred N/10 Alerts

Honeywall: 3232236028
Created: Thu Mar 24 10:12:17 2005 Last Update: Thu Mar 24 10:55:31 2005

	Bidirectional				Total			
	In		Out		In		Out	
	con	ids	con	ids	con	ids	con	ids
1 hour	0	0	7	1	1	0	30	14
48 hour	0	0	7	1	1	0	30	14

KBytes Transferred N/10 Alerts

Sensor Details for 3232236026

Sensor ID: 3232236026
Install Date: Thu Mar 24 02:00:14 2005
State: online
Country:
Latitude:
Network Type:
Notes:

Sensor Name: Honeywall: 3232236026
Last Update: Thu Mar 24 10:55:30 2005
Timezone:
Longitude:

Local Top 25

Flags	Host	Connections	IDS events
	192.168.1.20	23	10
	192.168.1.241	6	4
	192.168.1.124	34	0
	192.168.1.120	33	0
	192.168.1.122	4	0

Remote Top 25

Host	Connections	IDS events
192.168.0.12	2	0

Done 192.168.1.250

Pakistan Honeynet Project

Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://192.168.41.10/walleye.pl?act=aggt&st=1118831504;et=1118831504

Getting Started Latest Headlines

https://192.168.4...232246026&bidi=1 BBC NEWS | Middle East | Iraq violence shift...

The Honeynet PROJECT® Walleye: Honeywall Web Interface Wed Jun 15 10:38:35 2005 GMT
Logged in as admin

Data Analysis System Admin Logout

June 2005

sun	mon	tue	wed	thu	fri	sat
		1	2	3	4	
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		
(Prior Month) (Next Month)						
Hour	Cons	IDS				
0:00	0	0				
1:00	0	0				
2:00	0	0				
3:00	0	0				
4:00	0	0				
5:00	0	0				
6:00	0	0				
7:00	0	0				
8:00	0	0				
9:00	0	0				
10:00	6	1				
11:00	0	0				
12:00	0	0				
13:00	0	0				
14:00	0	0				
15:00	0	0				
16:00	0	0				
17:00	0	0				
18:00	0	0				
19:00	0	0				
20:00	0	0				
21:00	0	0				
22:00	0	0				

Aggregated Flows: Observed from Sensor 3232246026 Between Wed Jun 15 10:31:44 2005 and Wed Jun 15 10:37:44 2005

(Previous Page)		Start	1							End	(Next Page)						
		Aggregate Totals												Individual Flow Maximums			
dst_ip	Flows	Alerts	SRC Ports	DST Ports	SRC pkts	SRC bytes	DST pkts	DST bytes	SRC pkts	SRC bytes	DST pkts	DST bytes					
192.168.1.10	6	1	6	6	184	16992	139	24320	142	13820	102	20895					

Done 192.168.41.10

Pakistan Honeynet Project

Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://192.168.41.10/walleye.pl?act=tree;sensor=3232246026;prc

Getting Started Latest Headlines

The Honeynet PROJECT®

Walleye: Honeywall Web Interface

Wed Jun 15 10:36:20 2005 GMT
Logged in as admin

Data Analysis System Admin Logout

Process Summary

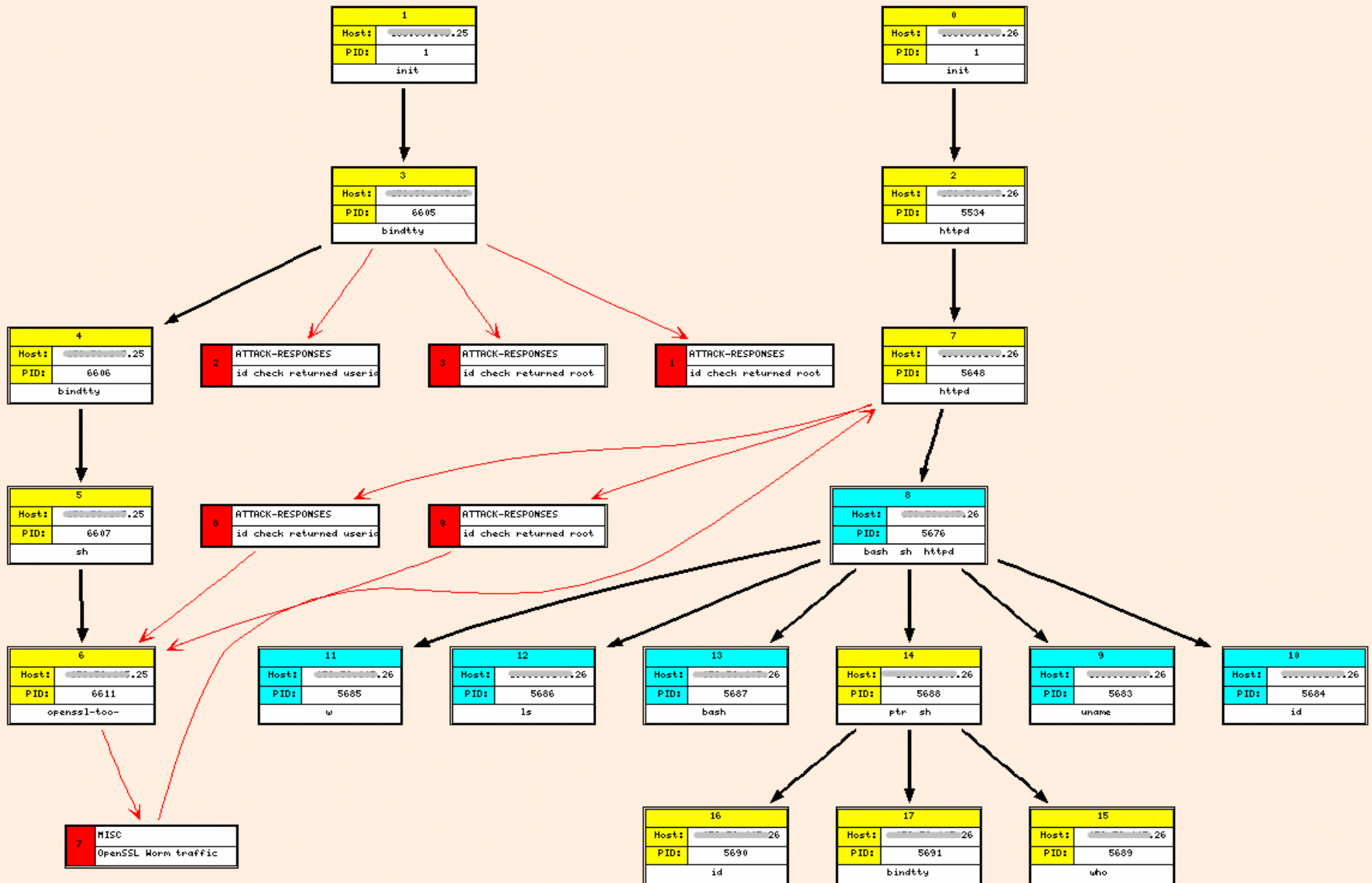
Host IP: 192.168.1.10 View this process's connections:
PID: 1712 View all connections from this process tree:
First: Tue Jun 14 20:32:55 2005 View Process Tree for this Process:
Last: Wed Jun 15 10:33:00 2005 View Details for this Process:
Commands: sshd

Process_Tree

```
graph TD; P1["386 2  
Host: 192.168.1.10  
PID: 8639  
sshd"] --> P2["388 7  
Host: 192.168.1.10  
PID: 8641  
bash sshd"]; P3["387 4  
Host: 192.168.1.10  
PID: 8640  
sshd"] --> P2; P2 --> P4["419 9  
Host: 192.168.1.10  
PID: 8675  
w"]; P2 --> P5["420 10  
Host: 192.168.1.10  
PID: 8676  
date"]; P2 --> P6["421 11  
Host: 192.168.1.10  
PID: 8677  
ps"]; P2 --> P7["422 12  
Host: 192.168.1.10  
PID: 8678  
cat"]
```

Done 192.168.41.10

Pakistan Honeynet Project

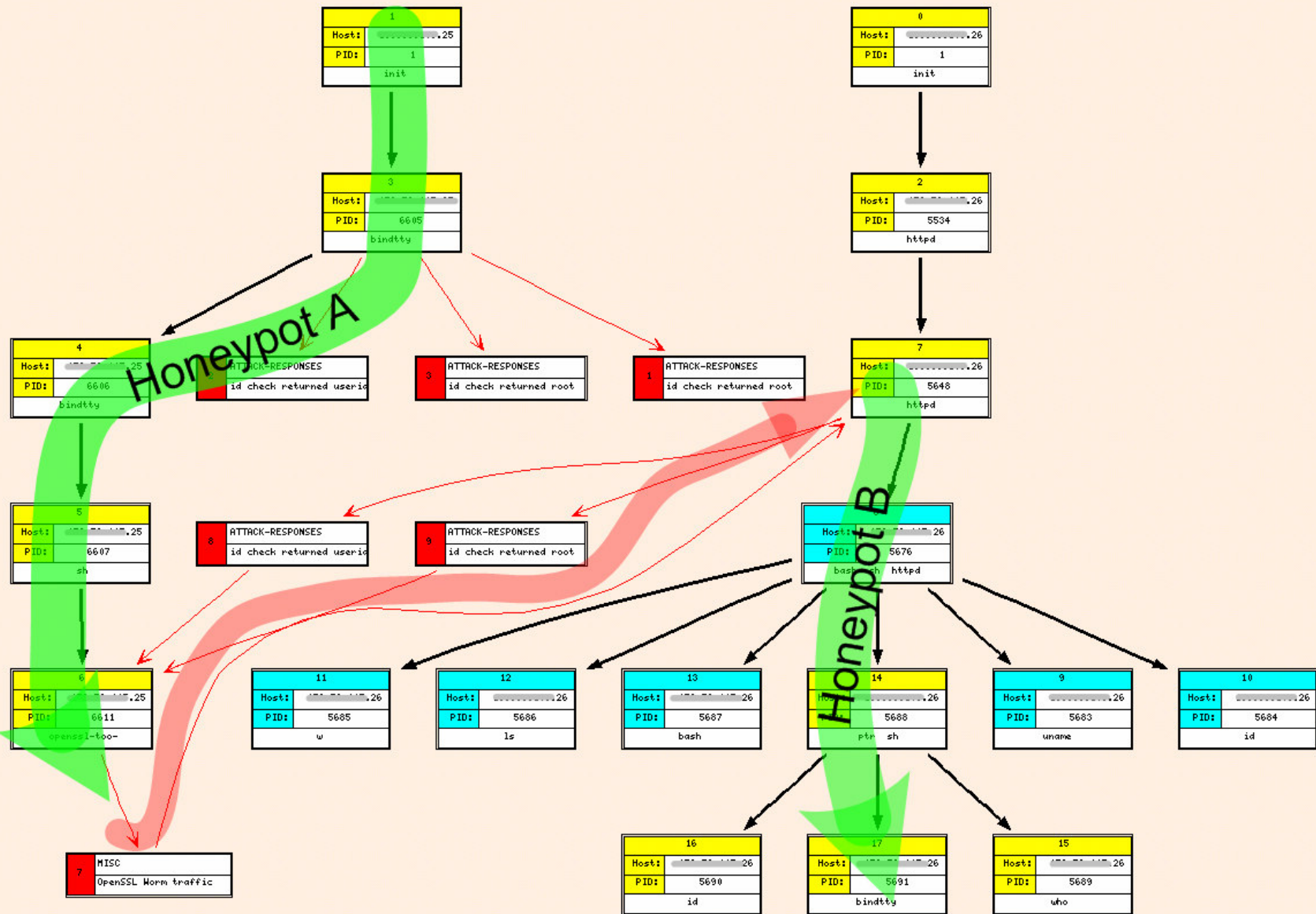


Sebek Data related to Snort Event: SID=1, CID=1520

What you are seeing?

- Display shows a process tree and its associated IDS events.
 - Created by querying on a single IDS event.
 - Yellow Boxes are root processes
 - Cyan Boxes are non-root processes
 - Red Boxes are IDS events
 - Red Arrow represents direction of flow associated with event
 - Only displaying IDS related flows.
- Graph automatically generated from DB with graphviz tool from ATT.
- Notice anything odd about the graph?

Pakistan Honeynet Project



Sebek Data related to Short Event: SID=1, CID=1520

Phishing

- The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information.
- Phishing attacks use both **social engineering** and **technical subterfuge** to steal consumers' personal identity data and financial account credentials

Phishing Phacts

- Fact: A research report in 2004, estimated that 57 million people had received online Phishing attacks, costing banks and credit-card issuers over **\$1.2 billion** in 2003 alone
- Predictions: Phishers are beginning to target employees within organizations, attempting to gather valuable network identification and passwords that can result in the loss of confidential information or lead to security breaches.

Event

- Compromise
- Downloads Phishing Website
- Hosts Phishing Website
- Downloads Mass Emailing Tool
- Sends Phishing Email
- Connects to IRC

Compromise

- SSH brute force attack
- Password was set very simple
- After getting access:
 - Downloads Phishing Website
 - Copies to /var/www/html
 - Publish it on web server
- After setting up phishing website:
 - Downloads Mass Mailer
 - Loads up address book
 - Starts sending email