

Allen Harper Edward Balas



BLACK HAT BRIEFINGS

GEN III Honeynets: The birth of roo

A Honeypot is a baiting system, designed for attackers to interact with. A honeynet, simply put, is a network of honeypots. The key component of a honeynet is the honeywall. The honeywall is used to provide the following capabilities:

- Data Capture. The ability to collect information about the attack.
- Data Control. The ability to restrict the amount of damage that can be done from one of your honeypots to another network.
- Data Analysis. The ability to conduct limited forensics analysis on the network traffic or compromised honeypots in order to discover the attackers methodology.
- Data Alerting. The ability to alert an analyst as to suspicious activity.

In 2001, Honeynet.org released a honeywall, called eeyore, which allowed for Gen II honeynets and improved both Data Capture and Data Control capabilities over the Gen I honeynets.

In the summer of 2005, Honeynet.org released a new honeywall, called roo, which enables Gen III honeynets. The new roo has many improvements over eeyore:

- Improved installation, operation, customization
- Improved data capture capability by introducing a new hflow database schema and pcap-api for manipulating packet captures.
- Improved data analysis capability by introducing a new web based analysis tool called walleye.
- Improved user interfaces and online documentation

The purpose of this presentation is to describe the new capabilities of Gen III honeynets and demonstrate the new roo. In addition, a road ahead will be discussed to describe a global honeygrid of connected honeynets.

Allen Harper is a Security Engineer for the US Department of Defense in Northern Virginia. He holds a MS in Computer Science from the Naval Post Graduate School. As a member of the Honeynet Project, Allen leads the development of the GEN III honeywall CDROM, now called roo. Allen was a co-author of Gray Hat, the ethical hackers handbook published by McGraw Hill and served on the winning team (sk3wl of root) at last year's DEFCON Capture the Flag contest.

Edward Balas is a security researcher within the Advanced Network Management Laboratory at Indiana University. As a member of the Honeynet Project, Edward leads the development of Sebek and several key GenIII Honeynet data analysis components. Prior to joining Indiana University, Edward worked for several years as a network engineer developing tools to detect and manage network infrastructure problems.

The HoneyNet

P R O J E C T

GEN III HoneyNets The Birth of roo

Allen Harper
Ed Balas

www.honeynet.org

— THE HONEYNET PROJECT —

Allen Harper

- Lead Developer (Gate Keeper) of Honeywall
- Co-Author *Gray Hat Hacking*.
- Ten years security experience, three as Security Engineer for DISA.
- Served on last year's DEFCON CTF team
 - Sk3wl of r00t
- Seventeen years in USMC.

2

Ed Balas

- Researcher at Indiana University's Advanced Network Management Lab
- Sebek lead
- Gen III Data Cap / Analysis lead
- Background in Network Engineering and Programming

3

Agenda

- ➔ Honeynet Project
 - History of Honeynets
 - GEN III Honeynets: Birth of roo
 - GEN III Data Capture
 - GEN III Data Analysis
 - Way Ahead
 - Demo
 - How Can You Help?

4

Honeynet Project

- Volunteer organization of security professionals.
- Open Source, share all of our research and findings.
- Deploy networks around the world to be hacked
- Everything we capture is happening in the wild.
- We have no agenda, no employees, nor any product or service to sell.
- Goals
 - Awareness: To raise awareness of the threats that exist.
 - Information: For those already aware, to teach and inform about the threats.
 - Research: To give organizations the capabilities to learn more on their own.

Honeynet Research Alliance

- Started in 2002 as forum for exchange, sharing
- **Members** (<http://www.honeynet.org/alliance/>)
 - South Florida Honeynet Project
 - Georgia Technical Institute
 - Azusa Pacific University
 - Paladion Networks Honeynet Project (India)
 - Internet Systematics Lab Honeynet Project (Greece)
 - Mexico Honeynet (Mexico)
 - Honeynet.BR (Brazil)
 - Irish Honeynet
 - Norwegian Honeynet
 - UK Honeynet
 - French Honeynet Project
 - Italian Honeynet Project

Agenda

- Honeynet Project
- ➔ History of Honeynets
- GEN III Honeynets: Birth of roo
- GEN III Data Capture
- GEN III Data Analysis
- Way Ahead
- Demo
- How Can You Help?

7

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
 - Indications and Warnings of attacks
 - Network Defense Intelligence (info about attacker)

8

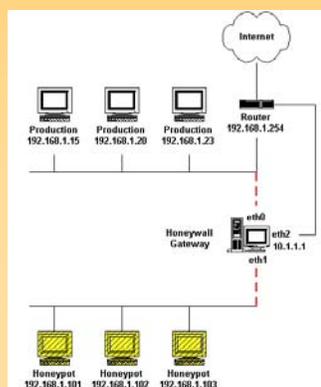
Honeypot Types

- 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.

Review of Gen II Honeynets

- <http://www.honeynet.org/papers/honeynet/>
- A Honeynet is network of high interaction Honeypots
- Gen II architecture defined by Honeynet Project
 - Data Control (no change in Gen III)
 - Layer 2 bridge
 - Iptables (packet limiting)
 - Snort Inline (packet scrubbing)
 - Data Capture (improved in Gen III)
 - Snort
 - Iptables logs
 - Sebek
 - Designed to record volatile host data.
 - Specifically keystrokes
 - Hidden kernel module or patch.
- eeyore Bootable CDROM Honeywall



Agenda

- Honeynet Project
- History of Honeynets
- ➔ GEN III Honeynets: Birth of roo
- GEN III Data Capture
- GEN III Data Analysis
- Way Ahead
- Demo
- How Can You Help?

11

Gen III Honeynets: Birth of roo

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

12

— THE HONEYNET PROJECT —

Installation of roo

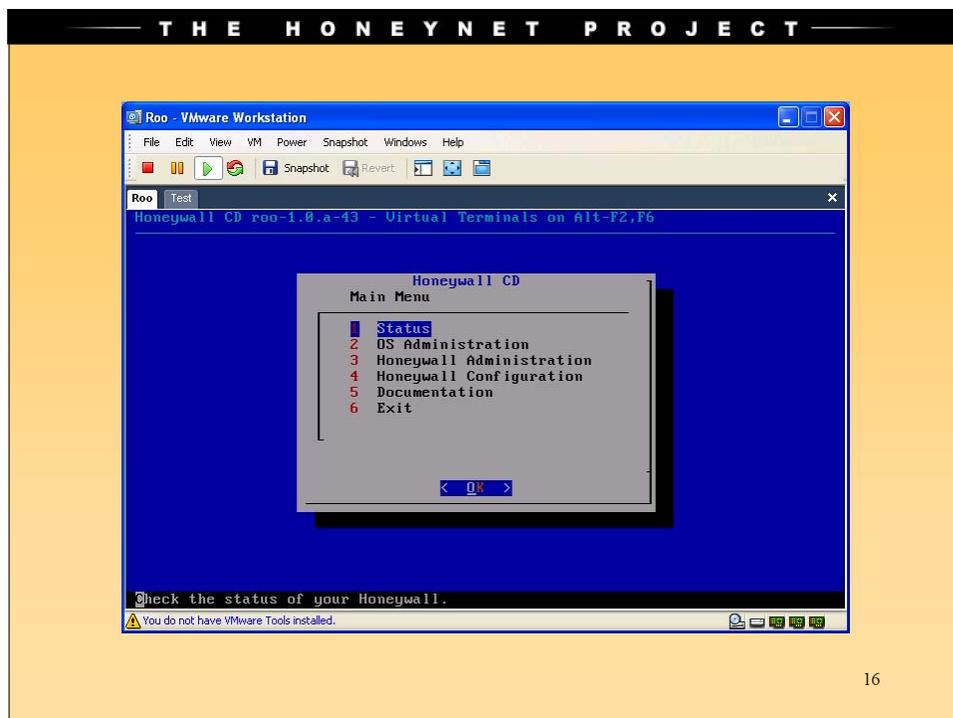
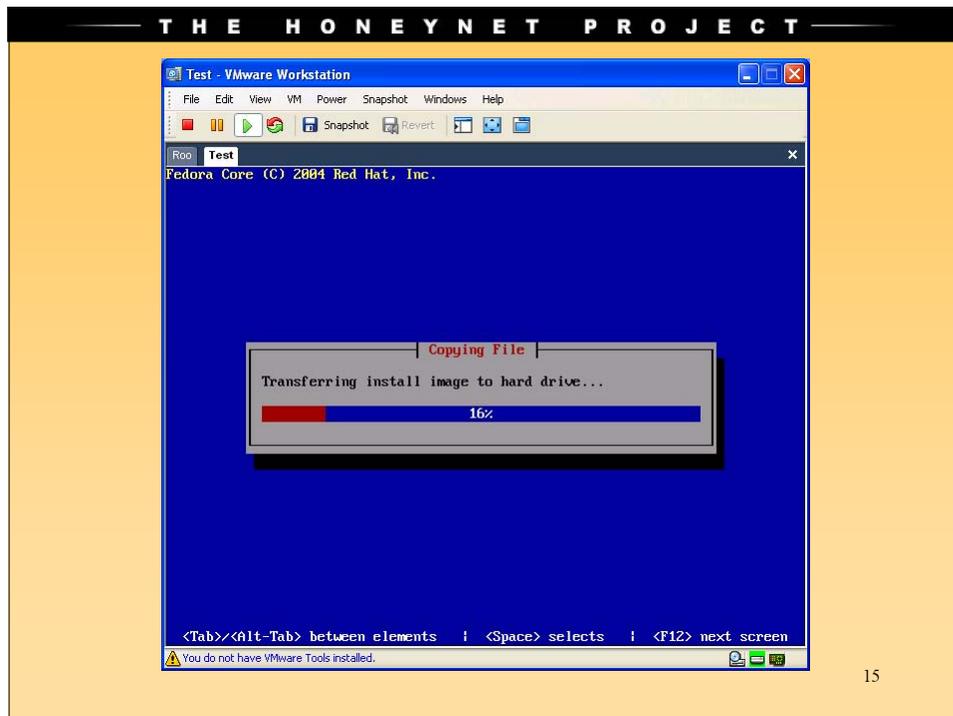
- FC3 Based
- Single CD, bootable install iso (340Mb)
- Custom ks.cfg file (about 235 minimal rpms)
- 3-5 minute install (hands off)
- Lockdown script runs on first boot.
 - Bastille
 - CIS
 - NIST
- Auto-config on 1st boot via floppy.

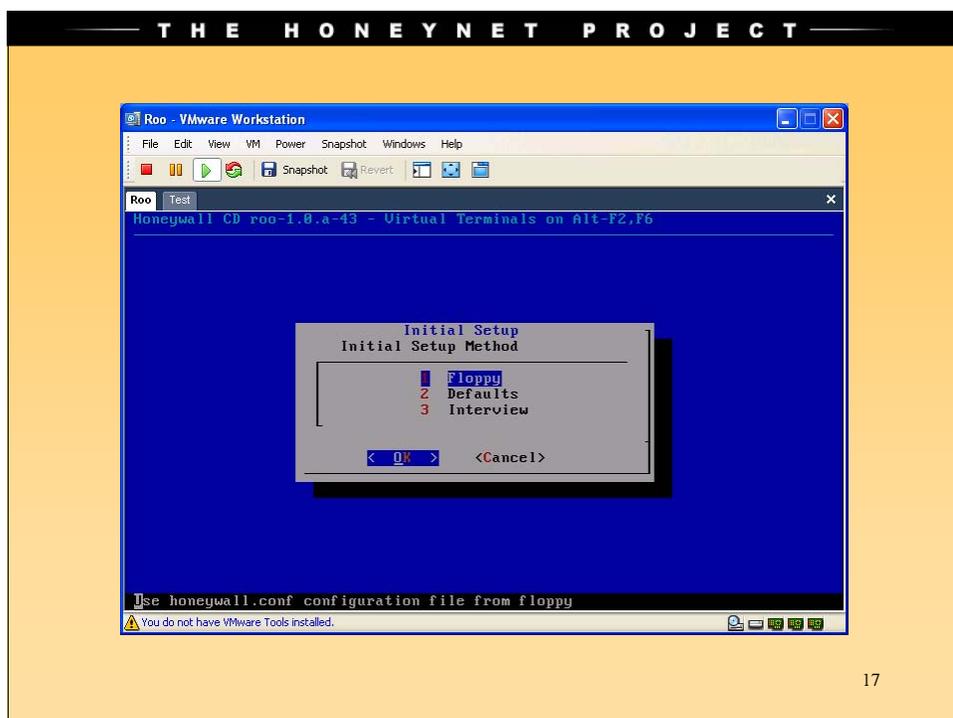
13

— THE HONEYNET PROJECT —

14

BLACK HAT BRIEFINGS



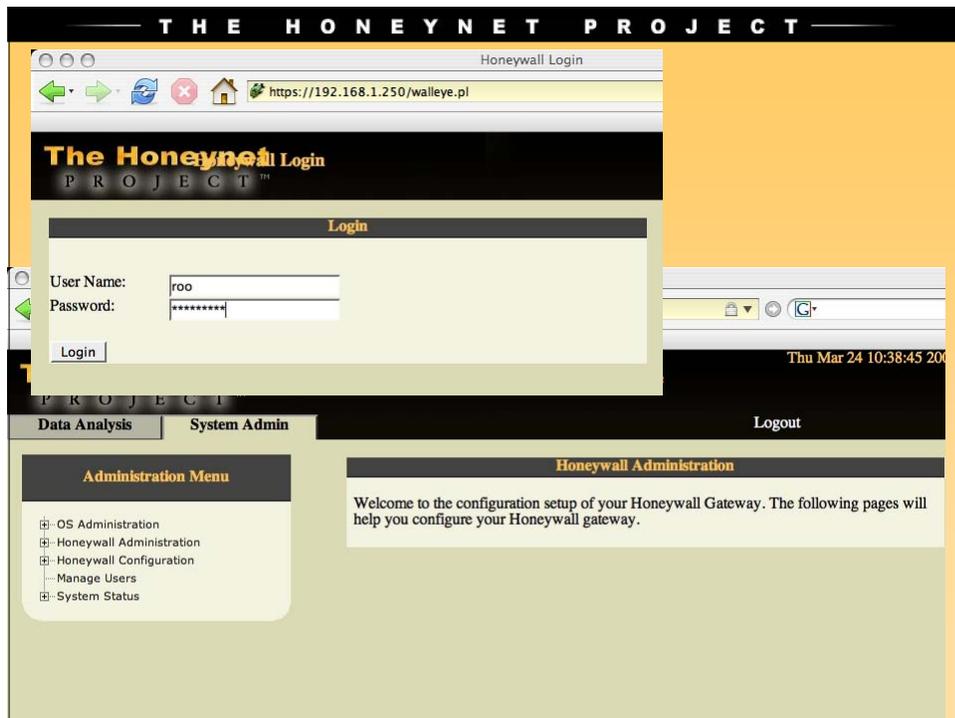


THE HONEYNET PROJECT

Operation of roo

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

18



THE HONEYNET PROJECT

Maintainability of roo

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

20

THE HONEYNET PROJECT

Customization of roo

- Stand-Alone Customization
 - Auto config on 1st boot via floppy
 - Dialog menu customization
 - Edit honeywall.conf file, portable to other honeywalls
- Factory Mode Customization
 - ./unpack-iso.sh <path to iso> <path to unpack>
 - Customize files
 - customization/custom.sh
 - customization/ssh-keys
 - customization/honeywall.conf
 - make iso
- Foundry Mode Customization
 - CVS Based
 - Synchronizes across multiple developers

21

THE HONEYNET PROJECT

Online Documentation of roo

- <http://www.honey.net.org/tools/cdrom/roo/manual>

22

Agenda

- Honeynet Project
- History of Honeynets
- GEN III Honeynets: Birth of roo
- ➔ GEN III Data Capture
- GEN III Data Analysis
- Way Ahead
- Demo
- How Can You Help?

23

Review of Gen II Data Capture

- Standard set of Data sources and related tool
 - Firewall logs
 - IDS alerts
 - Pcap data
- Provide a degree of consistency between honeynet researchers.

24

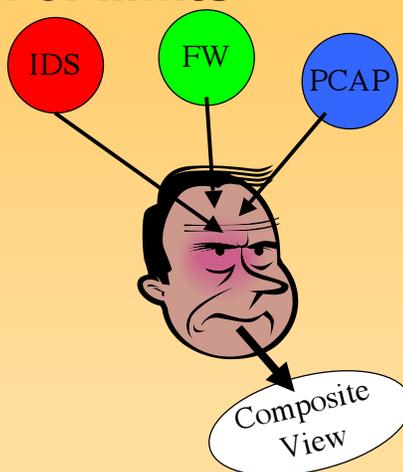
Gen II Data Capture Limits

- Data format defined by data capture tools
- No comprehensive data format
- No relationships between data structures can be stored.
- No API to gain access to data.
- Each data source had independent format causing stove pipe effect.
- **End result is slow and faulty event analysis**

25

Illustration of limits

- Each data type is processed by analyst
- Analyst manually fuses the data into composite view
- No easy way to share the new composite view.



26

Where we want to be

- We want to shift the Screening and Coalescing burden away from the human and onto the computer.
- Focus human effort on tasks best suited to the human.
- Comprehensive data model
- Near realtime ability to fuse multiple data sources
- Consistent API for data retrieval.

27

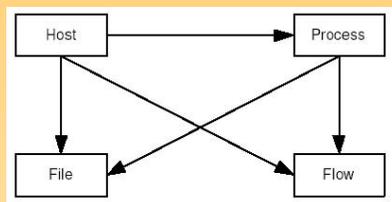
Proposed Architecture

- High level understanding of the intruders actions vs low level detailed intruder tool analysis.
- Fast Path-> high level relational data analysis
- Slow path-> low level tool analysis.

28

Gen III Fast path model

- Basically there are 4 basic abstractions in the data model.
 - Host
 - Process
 - Network Flow
 - File
- Identifying cross type relations is the key.
- The system should do the work



29

Gen III Slow path model

- Canonical raw data store
- Should provide a degree of location and storage format independence.
- Should provide mechanism to retrieve slow path data from specification of related fast path data.

30

Implementation

- Our implementation is made of three sections.
 - hflowd -> Data aggregation and modeling
 - pcap_api-> Slow path access
 - Walleye -> System to use these tools
- Host Data Capture was enhanced to identify needed relationships.

31

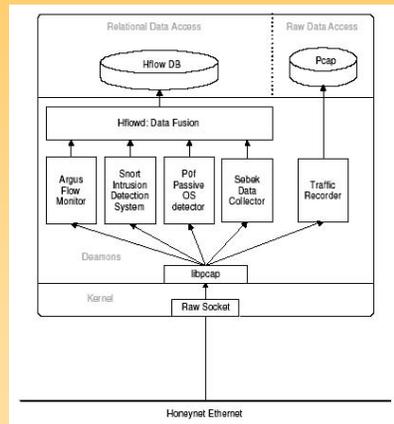
Sebek 3.X

- Three additional types of system call were monitored.
 - Open call associates file activity to a process.
 - Fork calls let us recreate the process tree.
 - Socket calls relate processes to a network flows.

32

Hflow Overview

- Simple perl daemon
- Automates data fusion
- Inputs:
 - Argus flows
 - Snort IDS events
 - Sebek socket records
 - p0f OS fingerprints
- Outputs:
 - normalized honeynet data uploaded into MySQL database.



33

Slow Path with pcap api

- Perl and C applications
- Provide CGI/CLI interface to pcap data
- Inputs
 - Hflow flow identifier
 - BPF + time range filter
- Output
 - Single dynamically generated pcap file with matching data.

34

What this gives us.

- Automatic identification
 - Type of OS initiating a flow
 - IDS events related to a flow
 - Honeypot processes and files related to a flow.
- Flow data acts as an index to the pcap data
 - Central theme of an event sequence can be identified
 - having to examining packet traces.
 - When packet traces needed, flow info helps facilitate retrieval.

35

Agenda

- Honeynet Project
- History of Honeynets
- GEN III Honeynets: Birth of roo
- GEN III Data Capture
- ➔ GEN III Data Analysis
- Way Ahead
- Demo
- How Can You Help?

36

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.

37

Basic concept

- Host activity display organized around process tree.
- Network activity display organized around notion of network flow.
- Provide easy navigation between the two.

38

THE HONEYNET PROJECT

Capabilities

- For an outbound connection, show me the causally related inbound connection.
- For an inbound connection, show me all related host activity.
- For this flow, get me the corresponding packet trace.
- For this process, show me the keystrokes of the user.

39

THE HONEYNET PROJECT

The screenshot displays the Honeywall Web Interface in a Mozilla Firefox browser window. The page title is "The Honeynet PROJECT" and the subtitle is "Walleye: Honey wall Web Interface". The user is logged in as "admin" on Thursday, May 26, 10:02:14, 2005 GMT. The interface includes navigation tabs for "Data Analysis", "System Admin", and "Logout".

Global Sensors

Honeywall: 20000126 (Created: Fri Mar 25 11:20:04 2005, Last Update: Thu May 26 10:02:07 2005)

Bidirectional		Total	
In	Out	In	Out
con	ids	con	ids
48 hour	482 79	184 0	1053 123 3149 2514

Sensor Details for 20000126

Sensor ID:	20000126	Sensor Name:	Honeywall: 20000126
Install Date:	Fri Mar 25 11:20:04 2005	Last Update:	Thu May 26 10:02:07 2005
State:	online	Timezone:	
Country:		Longitude:	
Latitude:			
Network Type:			
Notes:			

Local Top 25

Flags	Host	Connections	IDS events
	193.50.253	1478	1476
	193.50.21	444	406
Selected	193.50.20	437	399
	193.50.22	370	143

Remote Top 25

Host	Connections	IDS events
193.50.181	56	22
193.50.2	48	20
193.50.30	40	16
193.50.166	17	15
193.80.198	256	8
193.70.47	18	8
193.122.187	9	4
193.122.119	9	4
193.72.43	16	5
193.176.210	61	2
193.191.66	15	2
193.24.51	3	2
193.22.55	3	2
193.25	3	2
193.6.218	63	1
193.142	57	1
193.123	35	1
193.68	31	1
193.5	23	1
193.243	21	1
193.5.57	5	1
193.132	35	0

40

THE HONEYNET PROJECT

Connections Going to 10.0.0.21 Observed from Sensor 21000026 Between Wed May 25 19:00:00 2005 and Wed May 25 19:59:59 2005

Time	Protocol	Source IP	Source Port	Destination IP	Destination Port	Details
May 25 19:07:00	UDP	10.0.0.20	57685	10.0.0.21	1026	
May 25 19:07:00	TCP	10.0.0.20	47420	10.0.0.21	4444	
May 25 19:07:00	TCP	10.0.0.20	2875	10.0.0.21	4444	Microsoft-DS
May 25 19:07:00	TCP	10.0.0.20	40740	10.0.0.21	4444	Microsoft-DS
May 25 19:07:00	TCP	10.0.0.20	3177	10.0.0.21	4444	Microsoft-DS
May 25 19:07:00	TCP	10.0.0.20	40740	10.0.0.21	4444	Microsoft-DS
May 25 19:07:00	TCP	10.0.0.20	3447	10.0.0.21	40864	Microsoft-DS
May 25 19:07:00	TCP	10.0.0.20	3700	10.0.0.21	4444	Microsoft-DS
May 25 19:07:13	TCP	10.0.0.20	3951	10.0.0.21	16826	Microsoft-DS
May 25 19:07:00	UDP	10.0.0.20	34116	10.0.0.21	1026	
May 25 19:07:00	TCP	10.0.0.20	4161	10.0.0.21	4444	Microsoft-DS
May 25 19:07:00	TCP	10.0.0.20	1345	10.0.0.21	4444	Microsoft-DS
May 25 19:07:00	TCP	10.0.0.20	4161	10.0.0.21	4444	Microsoft-DS
May 25 19:07:00	TCP	10.0.0.20	1385	10.0.0.21	4444	Microsoft-DS

41

THE HONEYNET PROJECT

Process Summary

Process ID: 24
First: Fri May 13 12:45:03 2005
Last: Wed May 25 02:30:10 2005
Commands: cmd.exe

Process Tree

```
graph TD
    24[cmd.exe] --> 25[cmd.exe]
    24 --> 26[cmd.exe]
    24 --> 27[cmd.exe]
    24 --> 28[cmd.exe]
    24 --> 29[cmd.exe]
    24 --> 30[cmd.exe]
    24 --> 31[cmd.exe]
    24 --> 32[cmd.exe]
    24 --> 33[cmd.exe]
    24 --> 34[cmd.exe]
    24 --> 35[cmd.exe]
    24 --> 36[cmd.exe]
    24 --> 37[cmd.exe]
    24 --> 38[cmd.exe]
    24 --> 39[cmd.exe]
    24 --> 40[cmd.exe]
    24 --> 41[cmd.exe]
    24 --> 42[cmd.exe]
    24 --> 43[cmd.exe]
    24 --> 44[cmd.exe]
    24 --> 45[cmd.exe]
    24 --> 46[cmd.exe]
    24 --> 47[cmd.exe]
    24 --> 48[cmd.exe]
    24 --> 49[cmd.exe]
    24 --> 50[cmd.exe]
    24 --> 51[cmd.exe]
    24 --> 52[cmd.exe]
    24 --> 53[cmd.exe]
    24 --> 54[cmd.exe]
    24 --> 55[cmd.exe]
    24 --> 56[cmd.exe]
    24 --> 57[cmd.exe]
    24 --> 58[cmd.exe]
    24 --> 59[cmd.exe]
    24 --> 60[cmd.exe]
    24 --> 61[cmd.exe]
    24 --> 62[cmd.exe]
    24 --> 63[cmd.exe]
    24 --> 64[cmd.exe]
    24 --> 65[cmd.exe]
    24 --> 66[cmd.exe]
    24 --> 67[cmd.exe]
    24 --> 68[cmd.exe]
    24 --> 69[cmd.exe]
    24 --> 70[cmd.exe]
    24 --> 71[cmd.exe]
    24 --> 72[cmd.exe]
    24 --> 73[cmd.exe]
    24 --> 74[cmd.exe]
    24 --> 75[cmd.exe]
    24 --> 76[cmd.exe]
    24 --> 77[cmd.exe]
    24 --> 78[cmd.exe]
    24 --> 79[cmd.exe]
    24 --> 80[cmd.exe]
    24 --> 81[cmd.exe]
    24 --> 82[cmd.exe]
    24 --> 83[cmd.exe]
    24 --> 84[cmd.exe]
    24 --> 85[cmd.exe]
    24 --> 86[cmd.exe]
    24 --> 87[cmd.exe]
    24 --> 88[cmd.exe]
    24 --> 89[cmd.exe]
    24 --> 90[cmd.exe]
    24 --> 91[cmd.exe]
    24 --> 92[cmd.exe]
    24 --> 93[cmd.exe]
    24 --> 94[cmd.exe]
    24 --> 95[cmd.exe]
    24 --> 96[cmd.exe]
    24 --> 97[cmd.exe]
    24 --> 98[cmd.exe]
    24 --> 99[cmd.exe]
    24 --> 100[cmd.exe]
```

Related Network Connections

Time	Protocol	Source IP	Source Port	Destination IP	Destination Port	Details
May 25 12:45:03	TCP	10.0.0.20	32773	10.0.0.20	1982	
May 25 12:45:03	UDP	10.0.0.20	32770	10.0.0.20	domains	
May 25 19:07:00	TCP	10.0.0.20	4161	10.0.0.20	4444	Microsoft-DS

42

THE HONEYNET PROJECT

The Honeywall Web Interface
 Logged in as admin

Process Summary

Host IP: 192.168.1.20
 PID: 21310
 First: Fri May 20 04:47:18 2005
 Last: Fri May 20 04:48:41 2005
 Command: hwb
 unbl_D

Opened Files

Timestamp	File Name	User ID	Inode	File Desc
Fri May 20 04:47:18 2005	/dev/pts/1	0	3	3
Fri May 20 04:47:18 2005	/dev/tty	0	71849	3

Read Activity

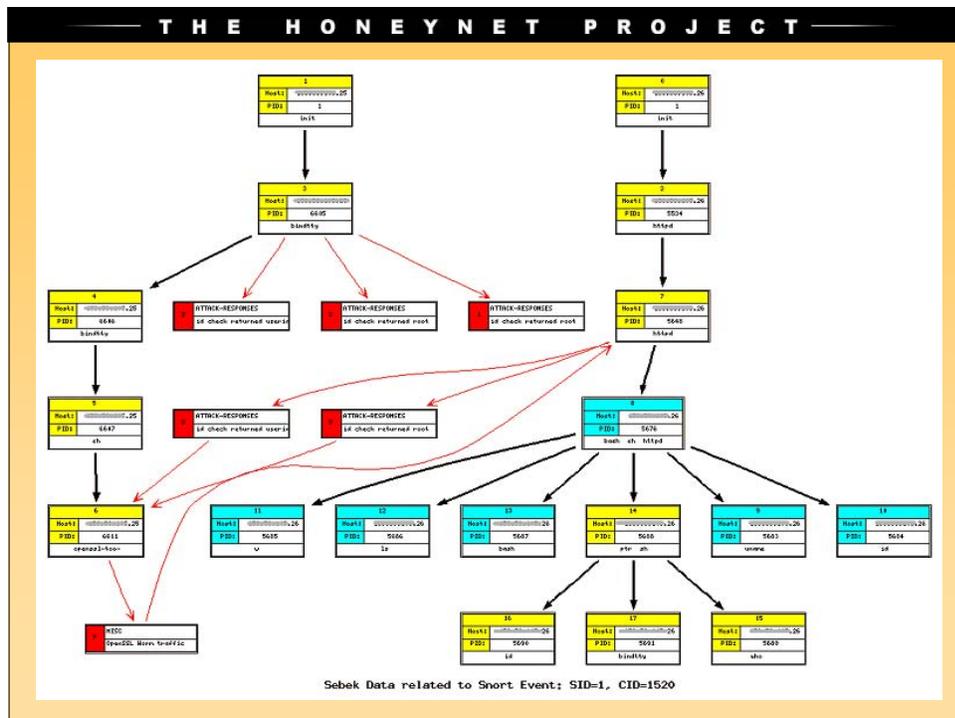
Read Details	FD	Inode	Time	UID	Bytes Read	Ave Read Len
	0	3	2005.05.20 04:47:21	0	113	1
	3	783906	2005.05.20 04:47:18	0	1	1
	3	783909	2005.05.20 04:47:19	0	1	1

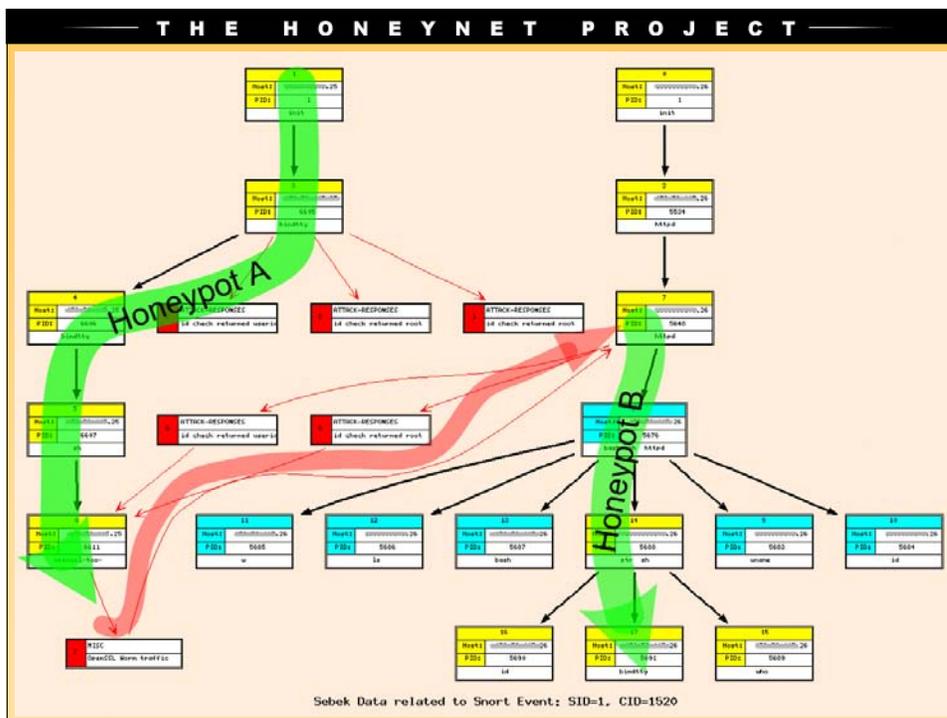
Read Details

```

04:04:24  unset HISTFILE
04:04:26  unset WATCH
04:04:30  history -nb[DEL]
04:04:31  w
04:04:36  cd /var/tmp[DEL] [DEL] p
04:04:37  ls
04:04:40  cd zmeu
04:04:51  ./[DEL] [DEL] [DEL]
         cat vuln.txt
  
```

43





THE HONEYNET PROJECT

Gen III Limitations

- We have added complexity and increased likelihood of failure
- Hflowd is the single point of failure.
- In case of total failure of Hflowd, the raw GenII data acts as failover.
- Don't yet support non-realtime data fusion.

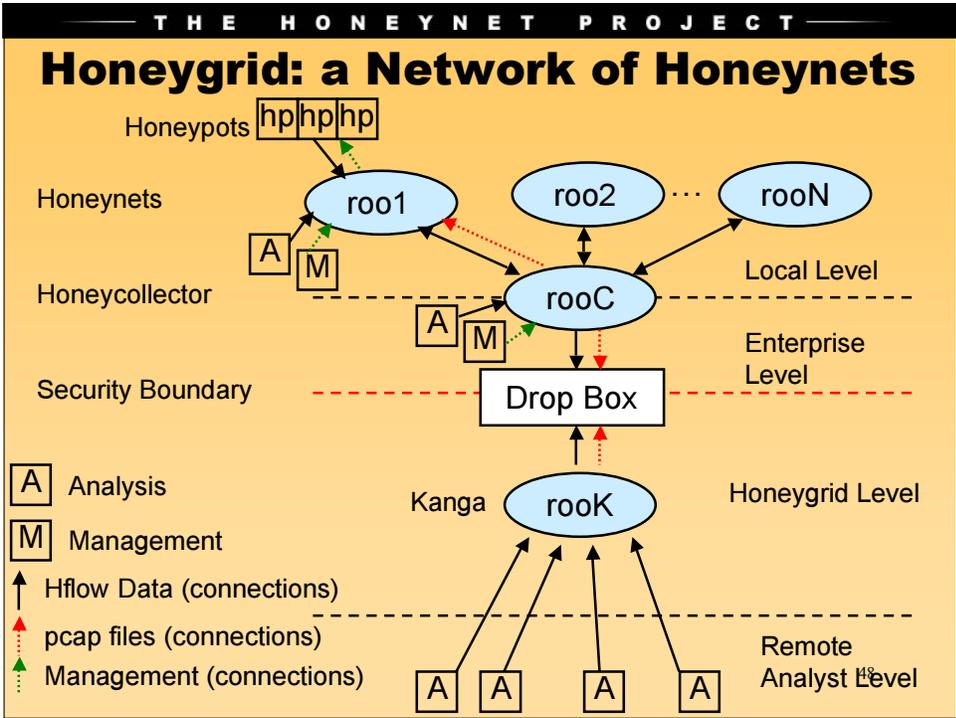
46

THE HONEYNET PROJECT

Agenda

- Honeynet Project
- History of Honeynets
- GEN III Honeynets: Birth of roo
- GEN III Data Capture
- GEN III Data Analysis
- ➔ Way Ahead
 - Demo
 - How Can You Help?

47



Possibilities of a Global Honeygrid

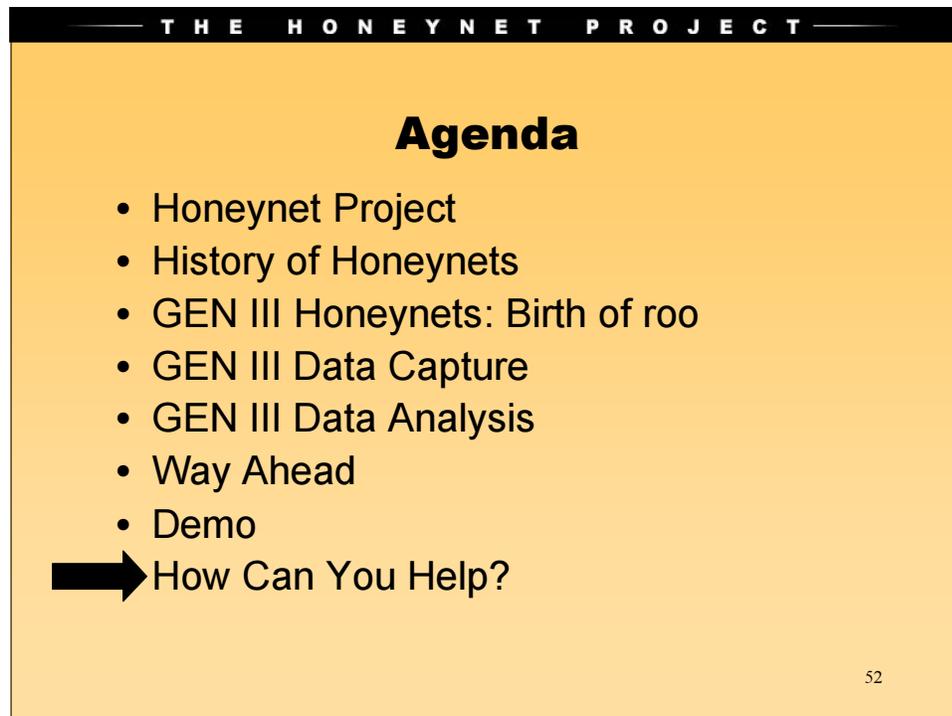
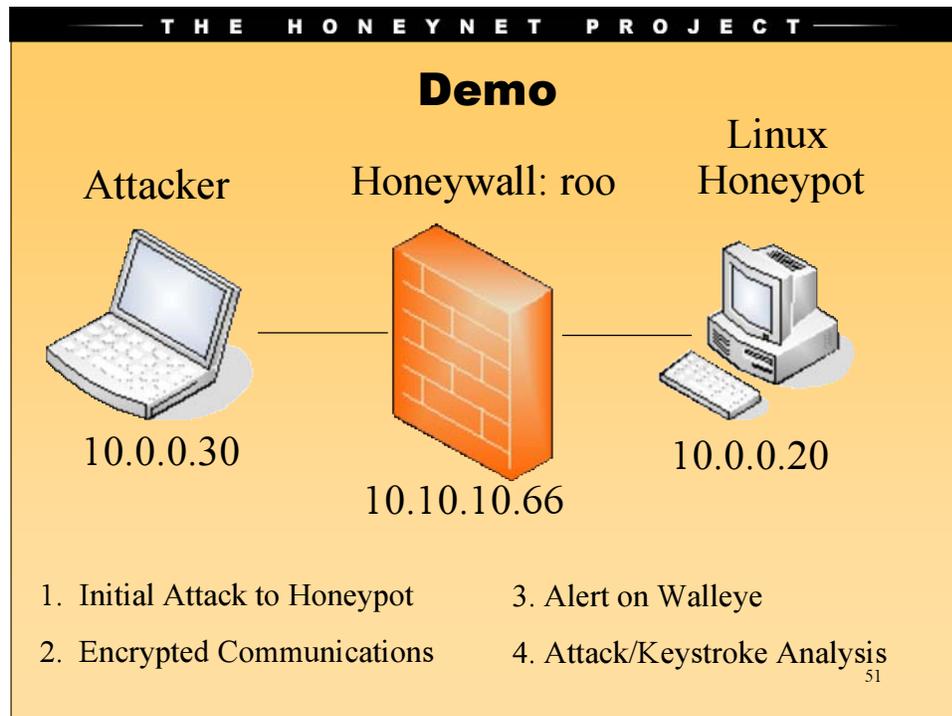
- Global Attack Trending
- Global Zero Day Discovery
- Global Attack Fingerprint Repository
 - Process Signature
 - Hflow Records

49

Agenda

- Honeynet Project
- History of Honeynets
- GEN III Honeynets: Birth of roo
- GEN III Data Capture
- GEN III Data Analysis
- Way Ahead
- ➔ Demo
 - How Can You Help?

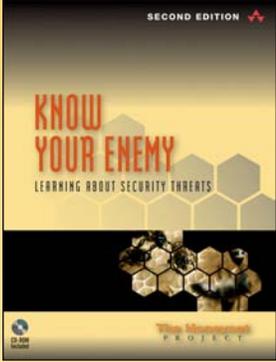
50



THE HONEYNET PROJECT

How Can You Help?

- Volunteer!
 - project@honeynet.org
- Honeypots Mailing list
 - honeypots@securityfocus.com
- Contribute Funding
 - <http://www.honeynet.org/funds/>
- Buy the Book



53

THE HONEYNET PROJECT

Contributing



YOU?

54

The Honeynet

P R O J E C T

Questions?

<http://www.honeynet.org>