Honeypots Workshop

Cristine Hoepers
General Manager
cristine@cert.br

Klaus Steding-Jessen
Technical Manager
jessen@cert.br

CERT.br – Computer Emergency Response Team Brazil
NIC.br - Network Information Center Brazil
CGI.br - Brazilian Internet Steering Committee

Agenda

- Background about the presenters
- Concepts
  - Honeypots, Honeynets, etc
- What we'll see in the hands-on
  - Honeypots similar to those of the Brazilian Honeypots Alliance
  - Two possible configurations

Background

CERT.br Mission

- Created in 1997 to *handle computer security incident reports and activities related to networks connected to the Internet in Brazil.*
  - National focal point for reporting security incidents
  - Establish collaborative relationships with other entities
  - Help new CSIRTs to establish their activities
  - Provide training in incident handling
  - Produce best practices' documents
  - Help raise the security awareness in the country

http://www.cert.br/mission.html

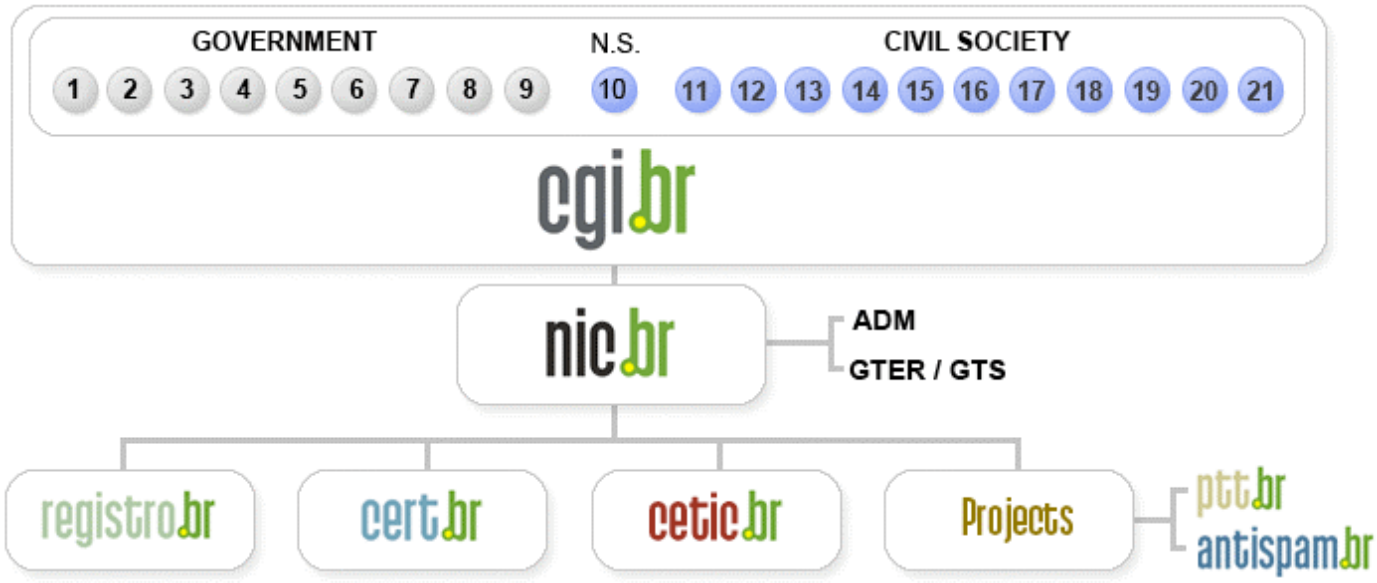
Our Parent Organization:
The Brazilian Internet Steering Committee - CGI.br

CGI.br is a multi-stakeholder organization that, among the diverse responsibilities, has the main attributions:

- to propose policies and procedures related to the regulation of Internet activities
- to recommend standards for technical and operational procedures
- to establish strategic directives related to the use and development of Internet in Brazil
- **to promote studies and technical standards for the network and services' security in the country**
- to coordinate the allocation of Internet addresses (IP) and the registration of domain names using <.br>
- **to collect, organize and disseminate information on Internet services, including indicators and statistics**

http://www.cgi.br/internacional/

Brazilian Internet Steering Committee (CGI.br) Structure



1 – Ministry of Science and Technology (Coordination)
2 – Ministry of Communications
3 – Presidential Cabinet
4 – Ministry of Defense
5 – Ministry of Development, Industry and Foreign Trade
6 – Ministry of Planning, Budget and Management
7 – National Telecommunications Agency
8 – National Council of Scientific and Technological Development
9 – National Forum of Estate Science and Technology Secretaries
10 – Internet Expert

11 – Internet Service Providers
12 – Telecommunication Infrastructure Providers
13 – Hardware and Software Industries
14 – General Business Sector Users
15 – Non-governmental Entity
16 – Non-governmental Entity
17 – Non-governmental Entity
18 – Non-governmental Entity
19 – Academia
20 – Academia
21 – Academia

Concepts

Honeypot

"A Honeypots is a security resource whose value lies in being probed, attacked or compromised."

Lance Spitzner

Honeypots: Tracking Hackers

- Possible uses
  - Detect automated probes and attacks
  - Capture tools, new worms, etc
  - Compare with IDS and firewall logs
  - Raise awareness
  - Identify infected/compromised machines

History

- 1988: ``Stalking the Wily Hacker'', Clifford Stoll
- 1989: ``The Cuckoo's Egg'', Clifford Stoll
- 1992: ``An Evening with Berferd'', Bill Cheswick
- 1992: ``There Be Dragons'', Steven M. Bellovin
- 1998: First honeypots:
  - Deception Toolkit (DTK), Cybercop Sting, NetFacade, and NFR BackOfficer Friendly
- 1999: The Honeynet Project started, with 30 members
- Sep/2001: Know Your Enemy book released
- Dec/2001:
  - The Honeynet Research Alliance was announced
  - Honeynet.BR Project started
- Jun/2002: Honeynet.BR joined The Honeynet Research Alliance

Advantages of the Technology

- There is no “normal’’ traffic. Everything is suspicious and potentially malicious.
- Less data to analyze than in IDS systems
- Can provide valuable information about attackers
- Can capture new types of malware

Disadvantages of the Technology

- There are potential risks for your network (depending on the type)
- Can be time consuming to maintain
- Narrow view -- sees only what is directed to it

Types of Honeypots

- Low-interaction
- High-interaction

Low-Interaction Honeypots

- Emulate some parts of services and systems
- The attacker does not have access to the real operating system
- The attacker “can’t” compromise the honeypot
- Easy to install and maintain
- Low risk
- Limited information gathering
- Examples:
  - listeners, service emulators, honeyd, Tiny Honeypot.

High-Interaction Honeypots

- More difficult to install and maintain
- High risk
- Need containment mechanisms
- Extensive information gathering
- Examples:
  - honeynets, virtual honeynets

Honeynet

"A Honeynet is nothing more than one type of honeypot. Specifically, it is a high interaction honeypot designed primarily for research, to gather information on the enemy. [...] A Honeynet is different from traditional honeypots, it is what we would categorize as a research honeypot."

Lance Spitzner

Know Your Enemy: Honeynets

"A honeynet is a research tool consisting of a network specifically designed for the purpose of being compromised, with control mechanisms that prevent this network from being used as a base for launching attacks against other networks."

Cristine Hoepers, Klaus Steding-Jessen, Antonio Montes

Honeypots Applied to the CSIRT Scenario

Honeynet Characteristics

- A network of multiple systems and applications
- Robust containment mechanism
  - may have multiple layers of control
  - sometimes called “honeywall”
- Data capture and alerting mechanisms

Honeynet Requirements

- No data pollution
  - i.e. no test or traffic generated by non-blackhats
- Data control
  - Must stop attacks from the honeynet to other systems
  - Need to be transparent to the attacker
    - Difficult to achieve with advanced attackers
  - Need to permit the attacker to work
    - download tools, connect to IRC, etc
  - Must have multiple layers of containment, to prevent from failure
- Data capture
- Data collection
- Alerting mechanism

Risks

Risks of Low-Interaction Honeypots

- Compromise of the real operating system running the honeypot
- The honeypot software may have vulnerabilities
- Attract attackers to your network

Risks of High-Interaction Honeypots

- A mistake in control or configuration can
  - permit your honeypot to be used to harm other networks
  - open a port to your organization network
- A compromise associated with your organization can affect its image
- Why they are so risky:
  - Level of interaction -- the attacker has full control of the machine
  - Complex to deploy and maintain
    - variety of technologies working together
    - multiple points of failure
  - New attacks and unexpected threats may not be contained or seen

When to Use Low-Interaction honeypots

- There is no sufficient hardware to set up a honeynet
- The risk of another type of honeypot is not acceptable
- The purpose is to
  - identify scans and automated attacks
  - fool script kiddies
  - distract attackers from important systems
  - collect attack signatures

When to Use High-Interaction honeypots

- The purpose is to observe the intruders activities and behaviour
  - Observe a real compromise
  - IRC conversations

- Need material for research and training in:
  - Artifact and forensic analysis

Low- x High-Interaction

	Low-Interaction	High-Interaction
Installation	Easy	More difficult
Maintenance	Easy	Time consuming
Risk	Low	High
Need for Control	No	Yes
Data gathering	Limited	Extensive
Intruder Interaction	Emulated services	Full control

In this Workshop

- Install, configure and examine a low-interaction honeypot
- Open source tools
  - OpenBSD as the base Operating System
  - OpenBSD `pf` firewall
  - Honeyd
  - `arpd`
  - Various listeners
  - Tcpdump
- This is the honeypot used in the Brazilian Honeypots Alliance Project

Brazilian Honeypots Alliance

Brazilian Honeypots Alliance
Distributed Honeypots Project

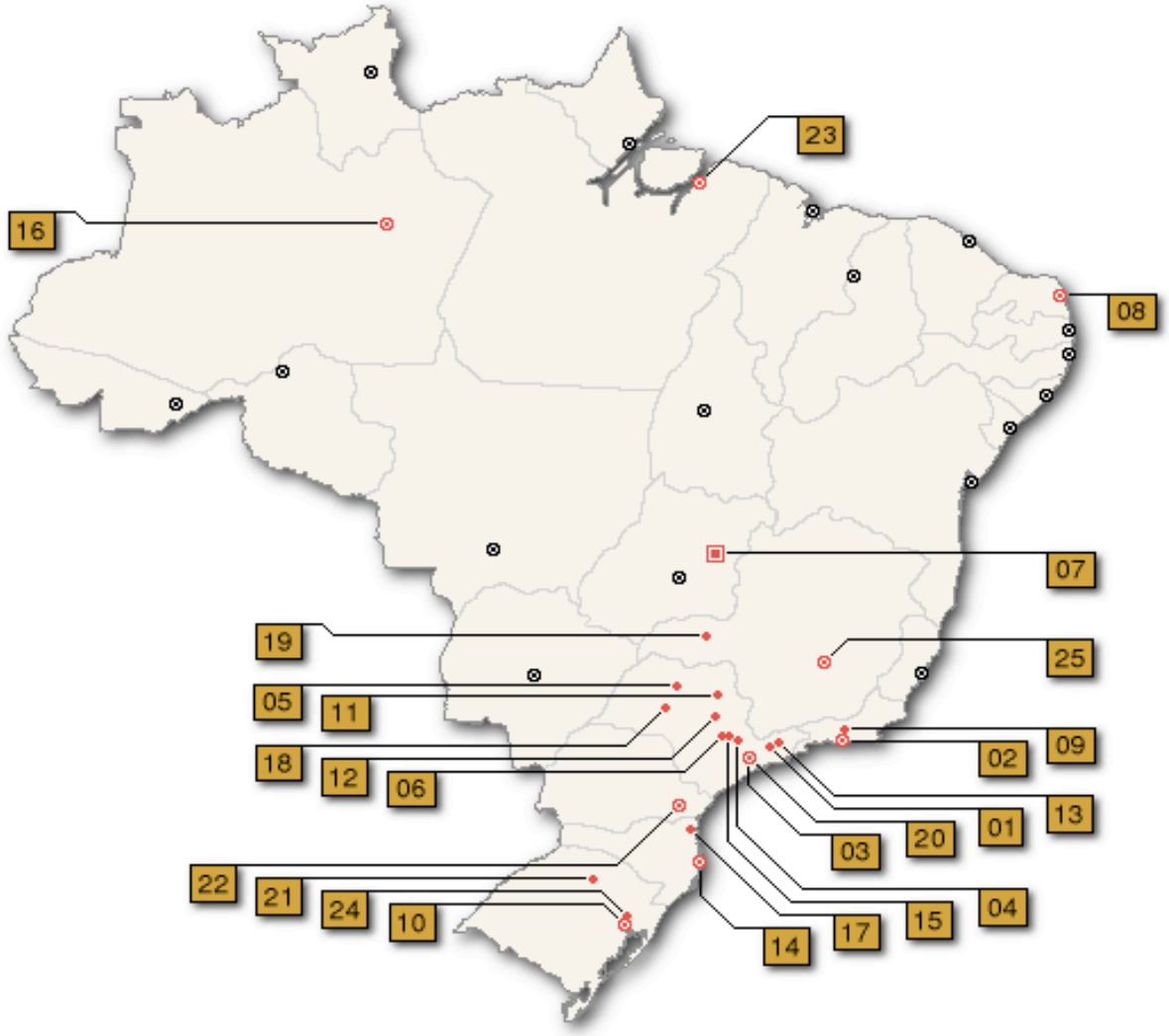
Main objective: to increase the capacity of incident detection, event correlation and trend analysis in the Brazilian Internet

- Joint Coordination: CERT.br and CenPRA/MCT
- 37 partner institutions:
  - Academic, government, industry, telecom and military networks
- Widely distributed across the country
- Based on voluntary work
- Maintain public statistics

  http://www.honeypots-alliance.org.br/

- Honeynet Research Alliance Member since June 2002
  http://honeynet.org/alliance/

Cities Where the Honeypots are Located



Partner Institutions (April/2007)

#	City	Institutions
01	São José dos Campos	INPE, ITA
02	Rio de Janeiro	CBPF, Embratel, Fiocruz, IME, PUC-Rio, RedeRio, UFRJ
03	São Paulo	ANSP, CERT.br, Diveo, Durand, UNESP, UOL, USP
04	Campinas	CenPRA, ITAL, UNICAMP, UNICAMP FEEC
05	São José do Rio Preto	UNESP
06	Piracicaba	USP
07	Brasília	Brasil Telecom, Ministry of Justice, TCU, UNB LabRedes
08	Natal	UFRN
09	Petrópolis	LNCC
10	Porto Alegre	CERT-RS
11	Ribeirão Preto	USP
12	São Carlos	USP
13	Taubaté	UNITAU
14	Florianópolis	UFSC DAS
15	Americana	VIVAX
16	Manaus	VIVAX
17	Joinville	UDESC
18	Lins	FPTE
19	Uberlândia	CTBC Telecom
20	Santo André	VIVAX
21	Passo Fundo	UPF
22	Curitiba	PoP-PR, PUC PR
23	Belém	UFPA
24	São Leopoldo	Unisinos
25	Belo Horizonte	Diveo

Main Characteristics of the Project

- Partners do not receive a “black box”
  - They have access to their honeypot
  - They can extend the honeypot’s configuration
- The honeypot does not capture production data
  - Only data directed to the honeypot is collected
- They can internally use the data captured by their own honeypot
  - As a complement to their IDS infrastructure
  - To detect infected machines, etc

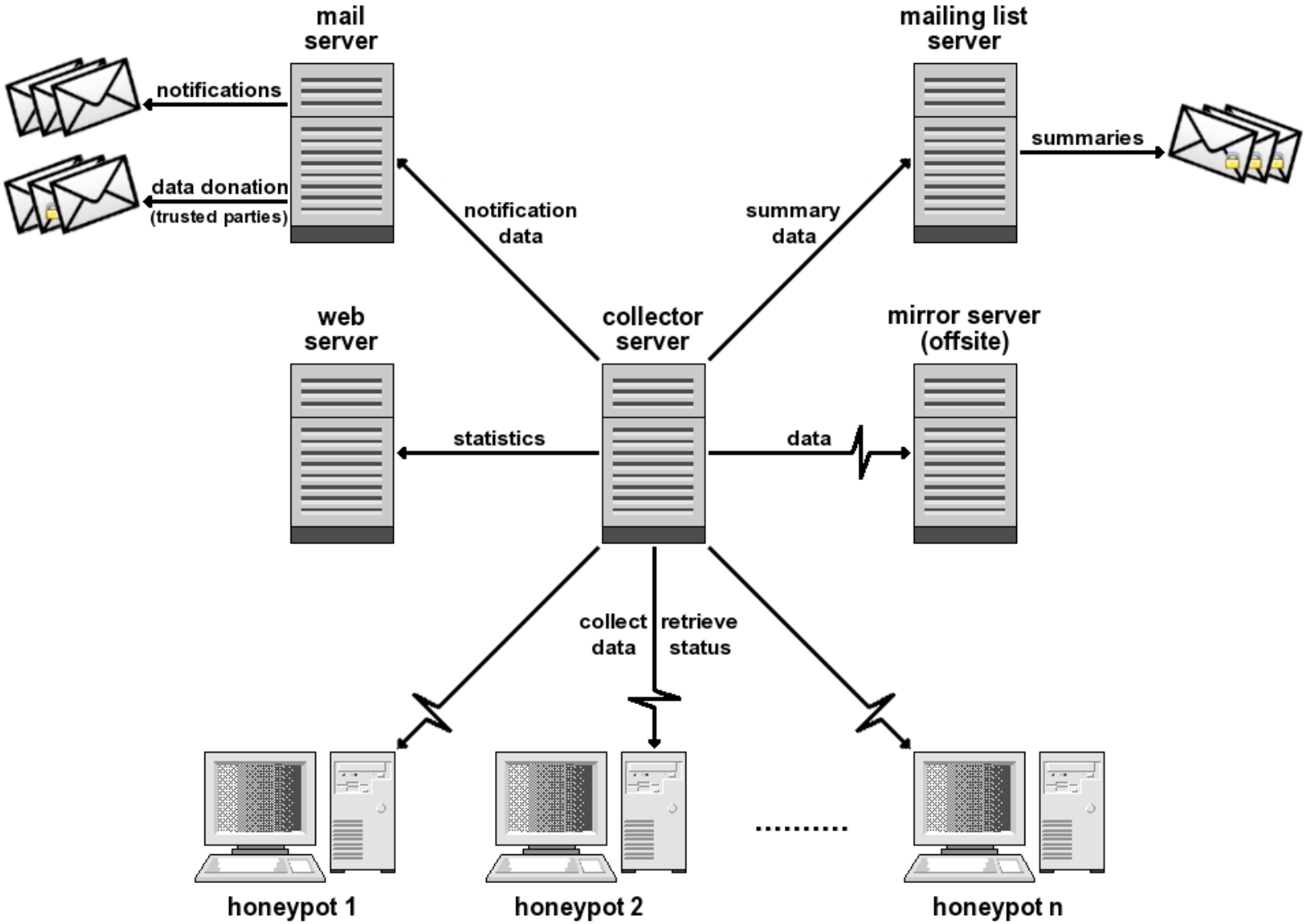
Details of the Honeypots

- OpenBSD as the base Operating System (OS)
- Honeyd
  - Emulates different OSs
  - Runs listeners to emulate services (IIS, ssh, smtp, etc)
- Proxy arp using `arpd`
- Payload logged using `pf`
- Each honeypot uses a netblock range (from /28 to /24)
  - 1 management IP
  - Other IPs are used to emulate different OSs and services
- Ability to collect malware samples
  - Listeners developed for: mydoom, subseven, socks, ssh, etc.
- Ability to implement spam traps

Why Use OpenBSD

- Familiarity
- number of security holes is extremely low, if compared with other operating systems
- good proactive security features
  - W^X, ProPolice, systrace, random lib loading order
- well-defined upgrade cicle (twice a year)
- runs in multiple architectures
  - i386, sparc, sparc64, amd64, etc
- one of the best available free packet filters
  - stateful, redundancy, integrated queueing (ALTQ), etc
- firewall logs in libpcap format

Architecture



Honeyd

Honeyd

"A framework for honeypots, that simulates virtual computer systems at the network level."

Niels Provos

Honeyd: A Virtual Honeypot Daemon

Honeyd Features

- Simulates computer systems running on unallocated network addresses
- Simulates several virtual hosts at the same time
- Permits the configuration of arbitrary services
- Simulates an OS at TCP/IP stack level
  - Fools `nmap`
- Supports dynamic redirection of a service
- Supports only IPv4 TCP, UDP and ICMP protocols
- Receive network data
  - Through a special route for the virtual IP addresses
  - Using proxy ARP (`arpd`)

Listeners

- Main goal
  - close the three-way handshake
  - log the activity
- Mainly two kinds
  - need to understand the protocol (http, ftp, etc)
  - just need to let a connection happen
- Listeners can be executed:
  - by honeyd, or
  - Just standalone

Hands-on

Format

- The remaining sessions will be hands-on
- Notebooks at the training area
  - Have OpenBSD and some basic tools installed
  - Need to install and configure the honeypot-related tools

References

- CERT.br
  http://www.cert.br/
- OpenBSD
  http://www.openbsd.org/
- Honeyd
  http://www.honeyd.org/
- Brazilian Honeypots Alliance
  http://www.honeypots-alliance.org.br/
- Previous presentations about the project
  http://www.cert.br/presentations/
- Honeynet Research Alliance
  http://www.honeynet.org/alliance/