



Honeynets, conociendo a tu enemigo...

Miguel José Hernández y López

miguel@honeynet.org.mx

www.honeynet.org.mx

Indice

miguel@honeynetmx:~# cat indice

- Tipos de Atacantes
- Métodos y motivos para un ataque
- Qué es un Honeypot?
- Honeynets
- Proyecto Honeynet México



:-)

The only way to stop a hacker, is to think like one...



HoneyNet
mexico Project

Tipos de Atacantes

Script Kiddies:

- Herramientas automatizadas
(scanners de vulnerabilidades)
- Tienden a no borrar huellas
- Ego

Blackhats:

- Métodos mas sofisticados
- 0h-days
- Tienden a no dejar huellas



HoneyNet
mexico Project

Métodos y Motivos para un Ataque


Script Kiddies:

- Uso de sistemas para colgar aplicaciones
- Uso de aplicaciones automatizadas
- Objetivos escogidos al azar
- El objetivo debe poseer determinada vulnerabilidad
- Ganar de la forma mas fácil posible -> root
- Sitios vulnerados, ranking dentro de la comunidad




HoneyNet
mexico Project

Métodos y Motivos para un Ataque

**zone-h**
unrestricted information

Hero-Z
the free hacker comics

search...



[Home](#) > [Digital Attacks Archive](#) > [Attackers Top List](#)Tuesday, 17 April 2007

MAIN MENU

- Home
- Digital Warfare
- Geopolitics
- ITsec News
- ITsec Advisories
- Test Drive
- 360°
- Digital Attacks Archive
 - ▶ [Attacks Archive](#)
 - ▶ [Attacks Archive](#) ★
 - ▶ [Attackers Top List](#)
 - ▶ [Attackers Top List](#) ★
 - ▶ [Attacks On Hold](#)
 - ▶ [Attack Notification](#)
- Zone-H events
- Publications
- Zone-H Friends/Partners
- Contact Us
- Search
- Download Area
- About this website
- Forum

ATTACKERS TOP LIST

This is the list of the first 50 attackers...

NO	ATTACKER	SINGLE DEF.	MASS DEF.	TOTAL DEF.	HOMEPAGE DEF.	SUBDIR DEF.
1	iskorpitx	17726	169781	187507	65012	122495
2	Fatal Error	10162	21208	31370	25797	5573
3	SPYKIDS	8717	21750	30467	29488	979
4	Secrethackers.org	7187	1424	8611	1876	6735
5	Thehacker	7064	35869	42933	37924	5009
6	BeLa	5854	4186	10040	5473	4567
7	aLpTurkTegin	5657	15363	21020	11914	9106
8	hackbsd crew	5369	8262	13631	7506	6125
9	Red Eye	5098	29925	35023	34730	293
10	ir4dex	4944	30530	35474	35375	99
11	Dengesiz Team	4361	4950	9311	3407	5904
12	TechTeam	4333	32033	36366	36353	13
13	core-project	4217	9536	13753	13694	59
14	Yusuf	4058	666	4724	684	4040
15	r00t_System	4055	19218	23273	21043	2230



HoneyNet
mexico Project

Fuente: Zone-H

Métodos y Motivos para un Ataque

“Hackean la página de AMLO 07/Julio/2006

La página del candidato a la Presidencia, Andrés Manuel López Obrador, aparece a las 07:40 horas hackeada publicando insultos al candidato.”

Fuente: <http://www.eluniversal.com>



Métodos y Motivos para un Ataque

Blackhats:

- Normalmente objetivos no escogidos al azar
- Posibilidad de utilizar 0h-days
- Utilizan sistemas como proxys para sus ataques
- Métodos y herramientas mas sofisticadas
(diferentes tipos de firewall bypassing, tecnicas para evadir IDS)



HoneyNet
mexico Project

Métodos y Motivos para un Ataque

Microsoft DNS RPC Buffer Overflow

Captura del 0hday: 07/Abril/2007

Microsoft publico la vulnerabilidad el 12/Abril/2007

La interfase de administración del RPC en el servicio de DNS de Microsoft Windows contiene un buffer overflow

Parche: 08/Mayo/2007

<http://www.microsoft.com/technet/security/advisory/935964.msp>



Fuente: eEye Digital Security

Cultura General

Aunque parezca mentira:

A finales del 2000:

- el tiempo estimado de vida de un RH 6.2 era de 72 hrs

A principios del 2002:

- se habia aumentado en un 100% el número de escaneos y de detecciones hechas por IDS's tipo Snort

A finales del 2002:

- una red SoHo podía ser escaneada más de 40 veces

Y ahora... 2007:

- quien no ha hecho un `cat /var/log/messages | grep sshd` ?



HoneyNet
mexico Project

Que es un Honeypot?

Recurso cuyo valor no reside en la producción o prestación de un servicio como habitualmente se conoce.

El valor de un Honeypot reside en ser atacado, probado y vulnerado.

Que obtendremos:

- pruebas del ataque al sistema
- descubrir nuevas vulnerabilidades
- despistar al atacante



HoneyNet
mexico Project

Que es un Honeypot?

Clasificación, dependiendo nivel de interacción...

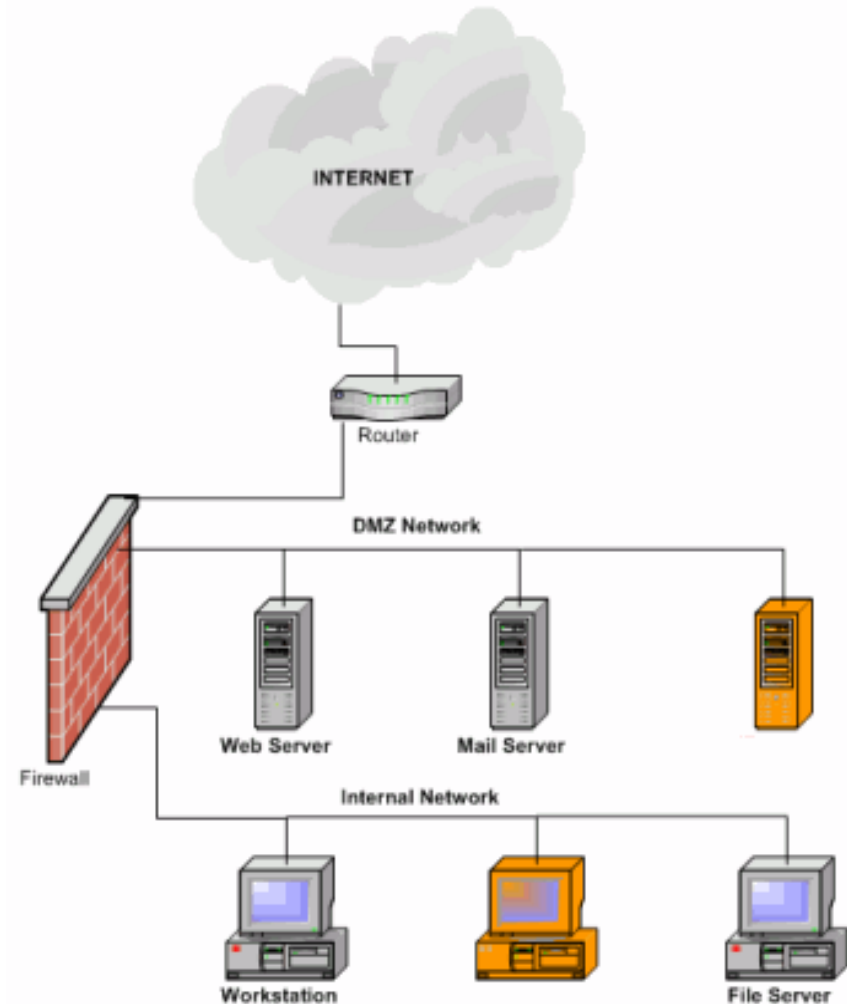
- Alta: aplicaciones reales
- Baja: emulación de servicios (honeyd, nepenthes)



HoneyNet
mexico Project

Que es un Honeypot?

Diagrama de un Red con Honeypots en la DMZ y Red Interna



HoneyNet
mexico Project

Honeynets: que son?

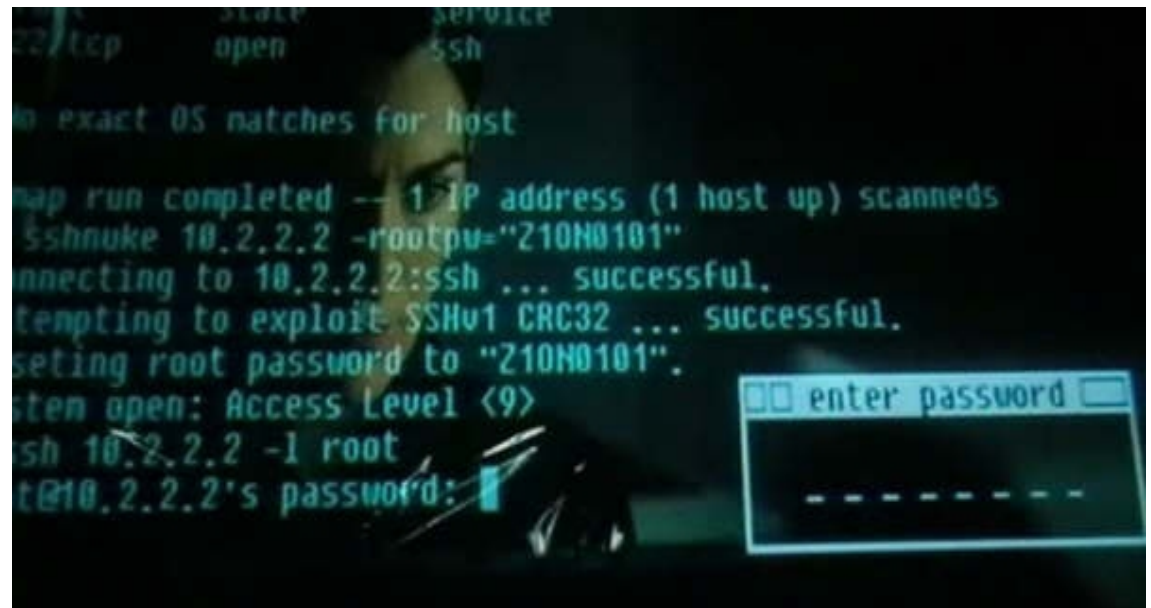
Redes diseñadas para ser atacadas y
recobrar así la información sobre posibles
atacantes.



HoneyNet
mexico Project

Honeynets: el problema

“How can we defend against an enemy, when we don't even know who the enemy is?”



```
state service
tcp open ssh
no exact OS matches for host
map run completed -- 1 IP address (1 host up) scanned
sshnuke 10.2.2.2 -rootpw="210N0101"
connecting to 10.2.2.2:ssh ... successful.
attempting to exploit SSHv1 CRC32 ... successful.
setting root password to "210N0101".
system open: Access Level <9>
ssh 10.2.2.2 -l root
t@10.2.2.2's password:
```



HoneyNet
mexico Project

Honeynets: misión

Nuevas técnicas de intrusión

0h-days

Valor principal: INFORMACION



HoneyNet
mexico Project

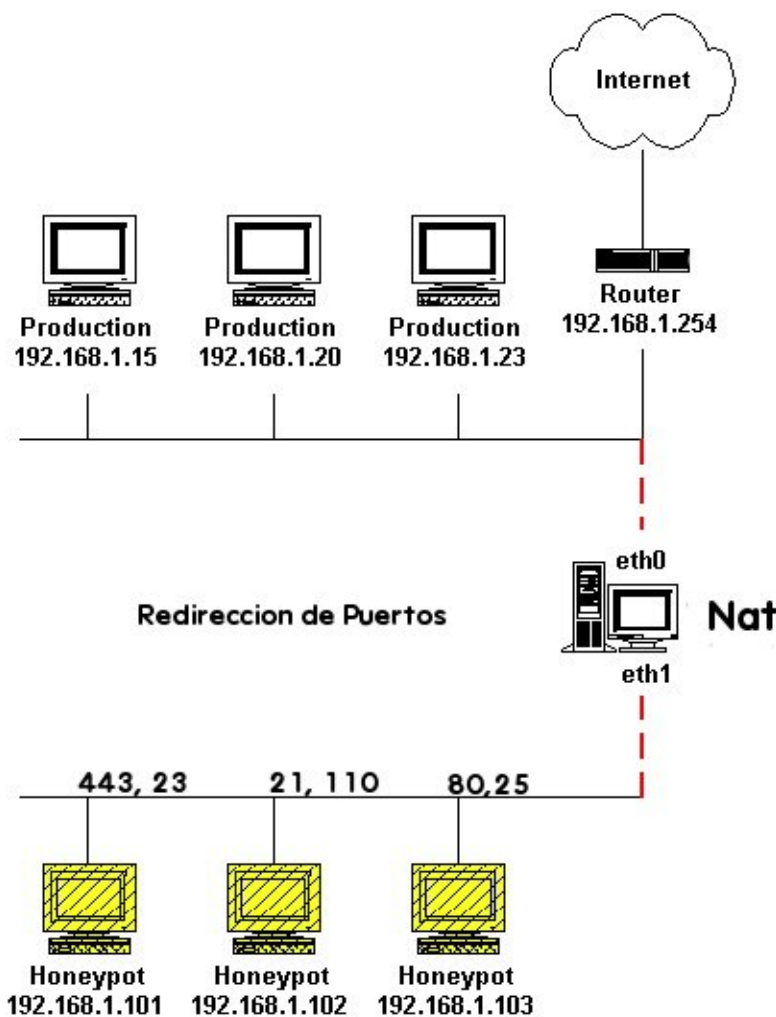
Honeynets: conceptos

- IPv6
- Generaciones
 - * Gen I (routing + nat)
 - * Gen II (bridging)
 - * Gen III (bridging+honeywall+sebek)
- Honeynets Virtuales
- Honeynets Distribuídas



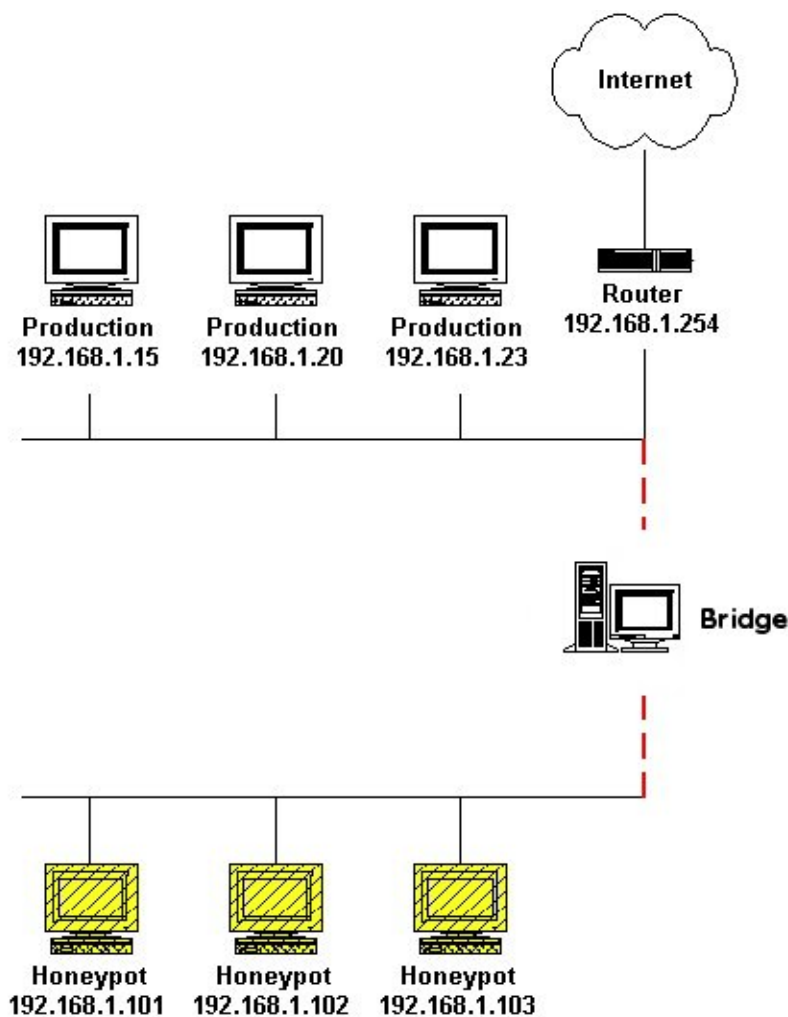
HoneyNet
mexico Project

Honeynets: Gen I



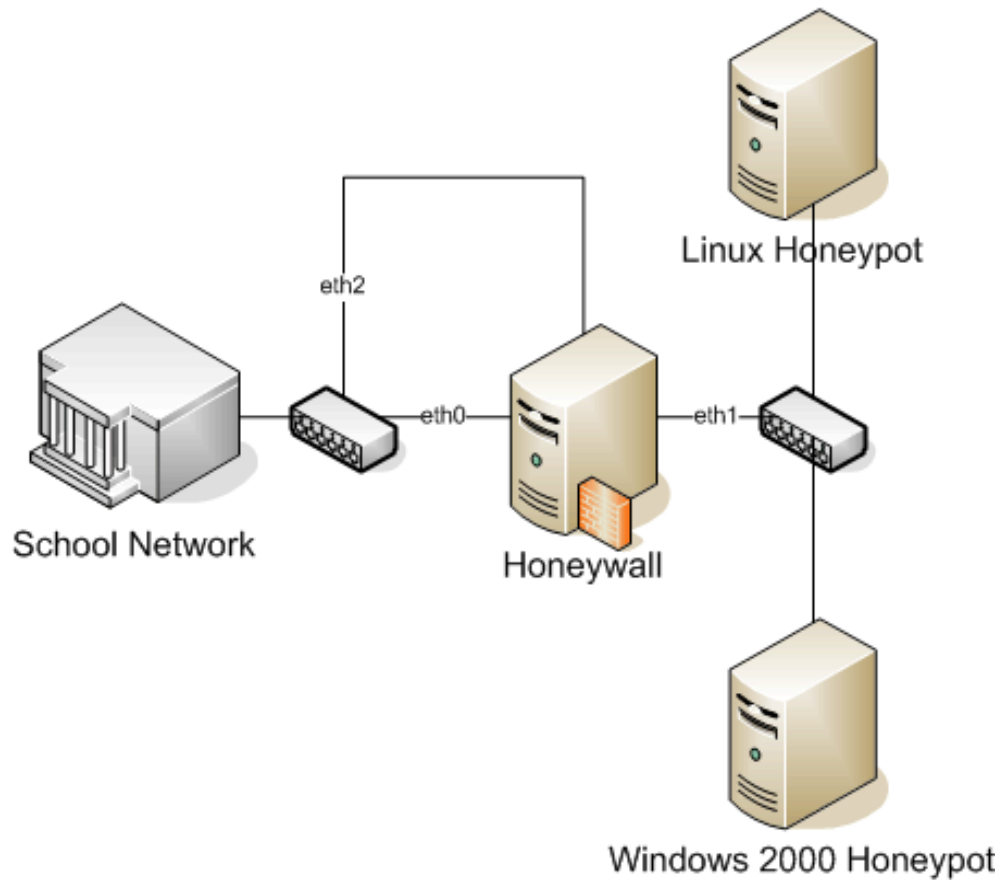
HoneyNet
Project
mexico

Honeynets: Gen II



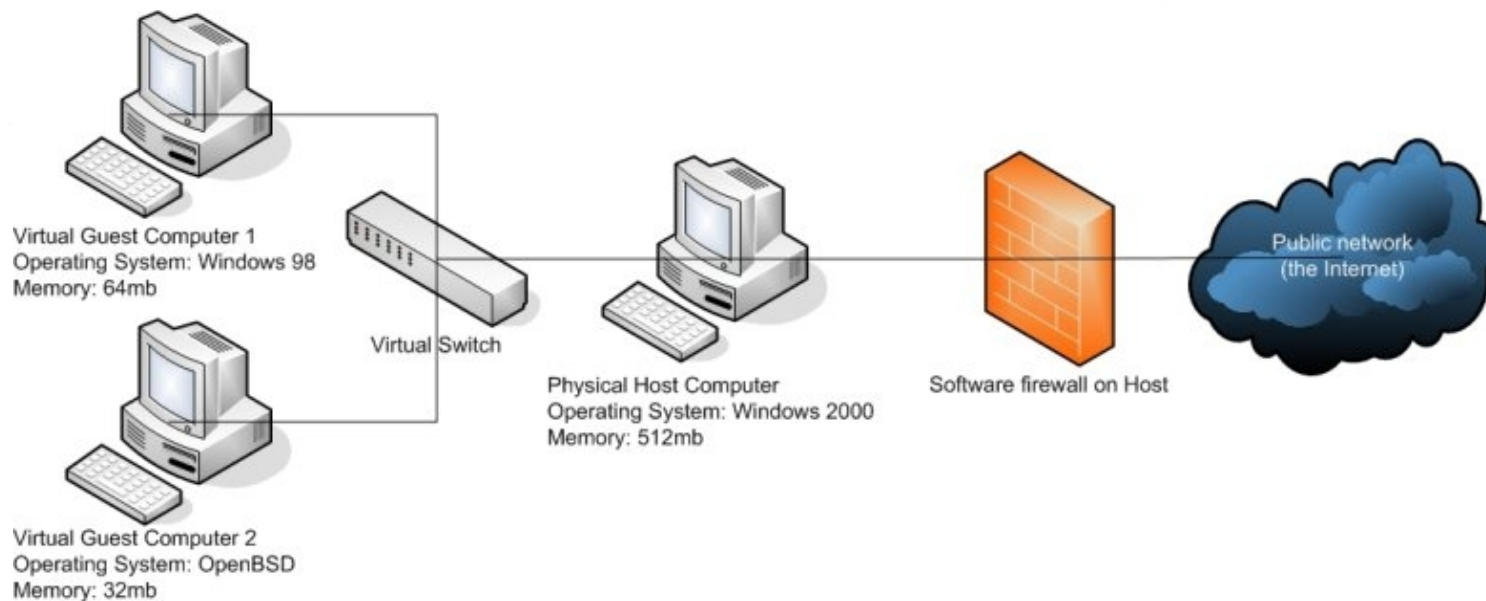
HoneyNet
mexico Project

Honeynets: Gen III



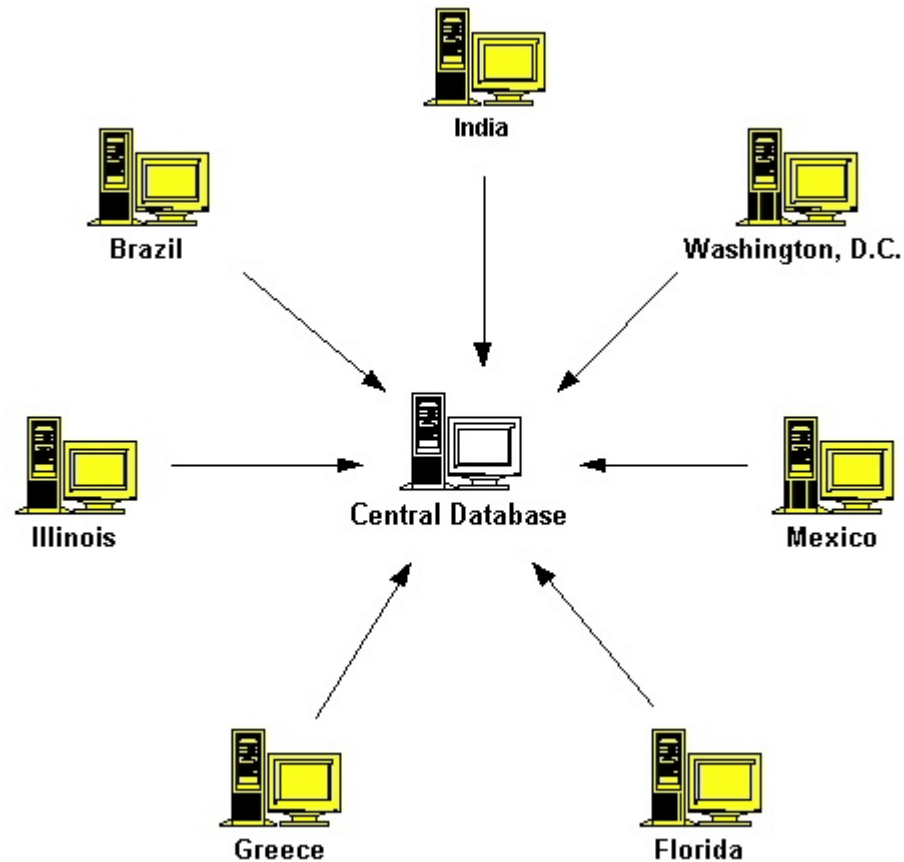
HoneyNet
mexico Project

Honeynets Virtuales



HoneyNet
mexico Project

Honeynets Distribuías



HoneyNet
mexico Project

Honeynets: HOWTO

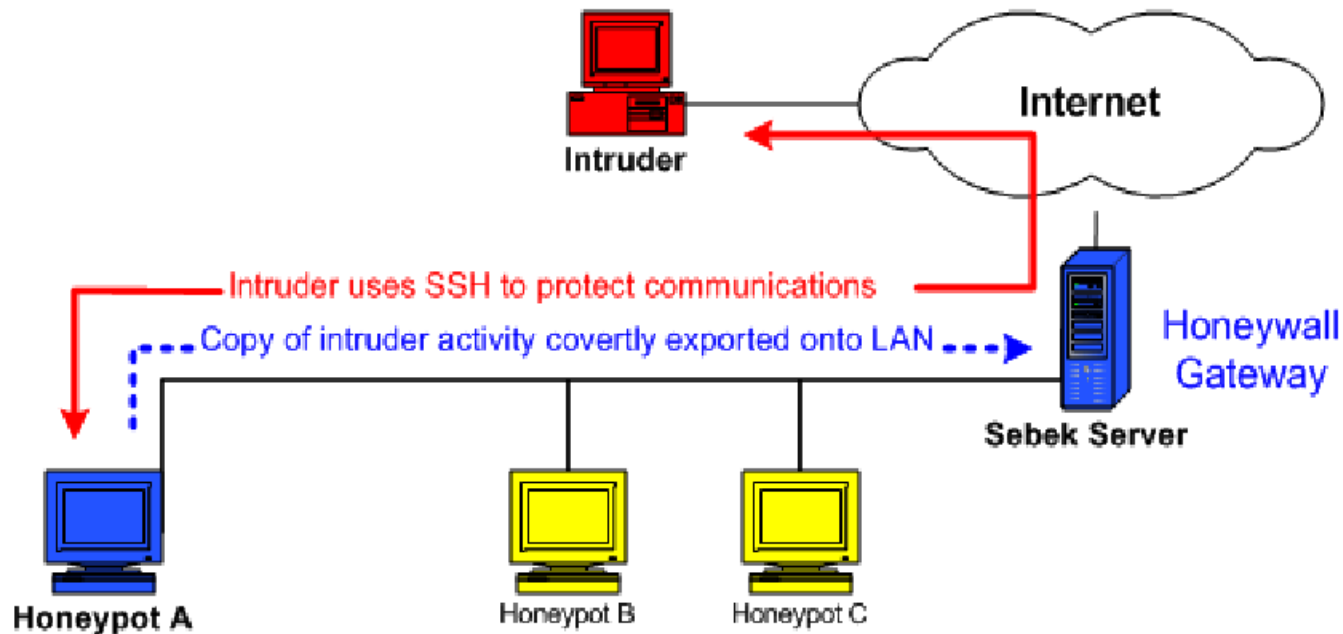
- HoneyWall Roo
 - * facil de implementar
 - * configurable
 - * Linux Fedora Core 3 (minimizado)

Sebek: herramienta de captura de datos basado en el kernel



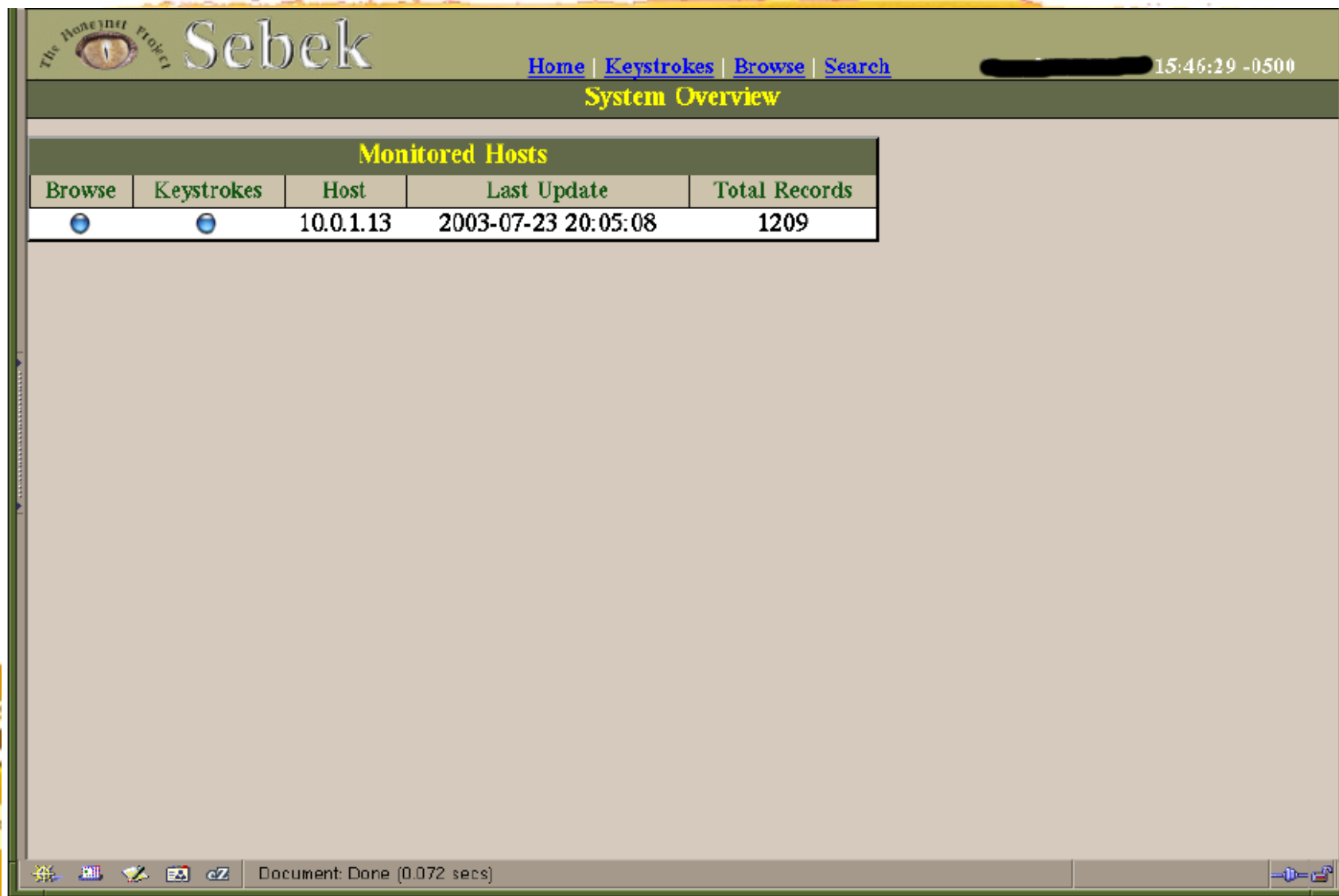
HoneyNet
mexico Project

Honeynets: Sebek (1)



HoneyNet
mexico Project

Honeynets: Sebek (2)





The screenshot displays the Sebek web interface. At the top left is the logo for 'The Honeynet Project' featuring a stylized eye, followed by the word 'Sebek' in a large serif font. To the right of the logo are navigation links: [Home](#), [Keystrokes](#), [Browse](#), and [Search](#). Further right is a blacked-out redaction box and the timestamp '15:46:29 -0500'. Below the navigation bar is a green header section with the text 'System Overview' in yellow. The main content area contains a table titled 'Monitored Hosts' in yellow. The table has five columns: 'Browse', 'Keystrokes', 'Host', 'Last Update', and 'Total Records'. There is one data row for host '10.0.1.13' with a last update of '2003-07-23 20:05:08' and '1209' total records. Each of the first two columns in the data row contains a small blue circular icon. The bottom of the interface shows a status bar with a taskbar on the left containing icons for a globe, a folder, a document, and a terminal, and a status message 'Document: Done (0.072 secs)' on the right.

The Honeynet Project **Sebek**


[Home](#) | [Keystrokes](#) | [Browse](#) | [Search](#) [Redacted] 15:46:29 -0500

System Overview

Monitored Hosts				
Browse	Keystrokes	Host	Last Update	Total Records
		10.0.1.13	2003-07-23 20:05:08	1209

Document: Done (0.072 secs)

Honeynets: Sebek (3)





Sebek

[Home](#) | [Keystrokes](#) | [Browse](#) | [Search](#)
15:46:40 -0500

Keystroke Summary View for IP: 10.0.1.13

Details	IP	PID	UID	COMMAND	FD	DATA
	10.0.1.13	1318	0	sh	0	[2003-07-23 20:04:33]# ls [2003-07-23 20:04:34]# less messages [2003-07-23 20:04:52]# cd /etc [2003-07-23 20:04:54]# mkdir ... [2003-07-23 20:04:57]# ls
	10.0.1.13	1323	0	less	3	[2003-07-23 20:04:35]# \000 [2003-07-23 20:04:50]# q
	10.0.1.13	1321	0	w	6	[2003-07-23 20:04:09]# w\000
	10.0.1.13	1271	500	bash	0	[2003-07-23 20:03:29]# ho[BS] [BS] who [2003-07-23 20:03:33]# w [2003-07-23 20:03:43]# ./malware [2003-07-23 20:03:47]# chmod ux[BS] +x mal [2003-07-23 20:03:52]# ./mal
	10.0.1.13	1312	500	w	6	[2003-07-23 20:03:33]# w\000
	10.0.1.13	1271	500	bash	3	[2003-07-23 20:03:24]# [BS] [BS]
	10.0.1.13	1304	500	tput	3	[2003-07-23 20:03:24]# \000
	10.0.1.13	1305	500	wc	0	[2003-07-23 20:03:24]# [BS]
	10.0.1.13	1307	500	tput	3	[2003-07-23 20:03:24]# \000
	10.0.1.13	1302	500	tput	3	[2003-07-23 20:03:24]# \000
	10.0.1.13	1252	0	mingetty	0	[2003-07-23 20:03:16]# blackhat
	10.0.1.13	1263	0	sshd	7	[2003-07-23 20:02:07]# \000\000\000
	10.0.1.13	1264	500	scp	0	[2003-07-23 20:02:07]# C0664 38802 malware [2003-07-23 20:02:09]# \000
	10.0.1.13	1263	0	sshd	3	[2003-07-23 20:02:09]# \000
		0	0	sshd	4	[2003-07-23 20:02:02]# SSH-2.0-OpenSSH_3.1p1


Document: Done (0.127 secs)


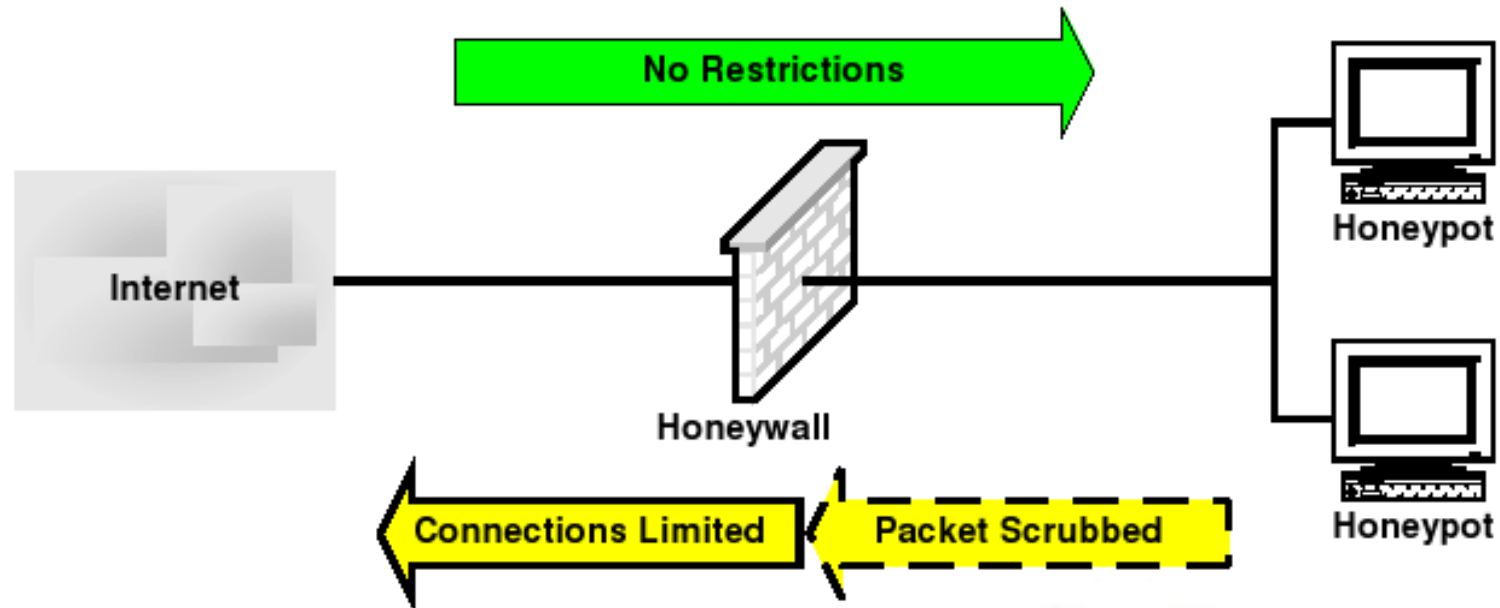
Honeynets: características

- * Control de flujo de datos (data control)
- * Captura de datos (data capture)
- * Análisis de datos (data analysis)



HoneyNet
mexico Project

Honeynets: control de flujo de datos



HoneyNet
mexico Project

Honeynets: captura de datos

* Captura toda la actividad en diferentes niveles:

- Actividad en la red
- Actividad en aplicaciones
- Actividad en el sistema



HoneyNet
mexico Project

Honeynets: análisis de datos

* Análisis forense



Proyecto Honeynet México



www.honeynet.org.mx

Proyecto Honeynet México

Somos una organización de investigación no lucrativa compuesta por profesionales de seguridad.

Made in México :-)



Proyecto Honeynet México

Instancia mexicana del Proyecto Honeynet
(Honeynet Research Alliance)



Honeynet
mexico Project

<http://www.honeynet.org>

Proyecto Honeynet México

Que hacemos?

- Montar Honeynets para que sean comprometidas
- Compartir la investigación y descubrimientos
- Difusion de que las amenazas existen
- Enseñar e informar
- Dotar a las organizaciones de las capacidades de aprender más por si mismos



Honeynet
mexico Project

Mejorar la SEGURIDAD en Internet sin costo

Proyecto Honeynet México

Honeynet Research Alliance

- UK Honeynet Project
- Phillipines Honeynet Project
- Brazil Honeynet Project
- Germany Honeynet Project
- New Zeland Honeynet Project
- Pakistan Honeynet Project
- Japan Honeynet Project
- **Mexico Honeynet Project :-)**
- West Point Honeynet
- UNC Charlotte Honeynet

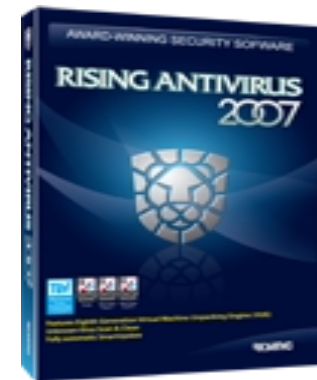


entre otros.....
Honeynet
mexico Project

Proyecto Honeynet México

Proyectos

- Honeynet Gen III
- GDH (Global Honeynet Distributed)
- Arania: escrita en perl, detecta ataques web
- sandbox nepenthes (malware)
- Colaboración con Rising Antivirus



Proyecto Honeynet México

Herramientas

- Honeynet Tools
www.honeynet.org/tools/
- Arania
www.honeynet.org.mx
- honeyd
www.honeyd.org
- nepenthes
nepenthes.mwcollect.org



Honeynet
mexico Project

Conclusiones

- Nadie va a hackear mi red porque uso un Checkpoint FW-1
ja! ja! ja! ja! ja! ja! ningún Firewall te protege de un servicio que este vulnerable a un 0h-day
- Nadie me va a hackear porque mi servidor siempre esta actualizado
ja! ja! ja! ja! ja! ja! no hay actualizaciones contra un 0h-day
- Mi red esta libre de malware que hay en Internet porque tengo en mi FW todo cerrado
ja! ja! ja! ja! ja! ja! y en tu LAN?



Las Honeynets nos ayudan a poder detectar todo esto

HoneyNet

Project

Proyecto Honeynet México



Honeynet
mexico Project

¡Muchas Gracias!

Miguel José Hernández y López

miguel@honeynet.org.mx

www.honeynet.org.mx



Honeynet
mexico Project