This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.

To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-sa/3.0/

Hugo González

@hugo_glez

http://atit.upslp.edu.mx/~hugo/

10 años UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

The Honeynet PROJECT

Colectando bichos con Nepenthes

Hugo F. González
hugo@honeynet.org.mx

http://creativecommons.org/licenses/by/2.5/mx/

Speaker :: Hugo F. González

- Miembro fundador del “Mexican Honeynet Project”, miembro profesional de ACM desde 2005.
- M.C. por el ITSLP en 2005.
- Asesor académico en la UPSLP.
- Usuario de SL desde hace mas de 7 años.
- Conferencista en eventos nacionales e internacionales.

Agenda

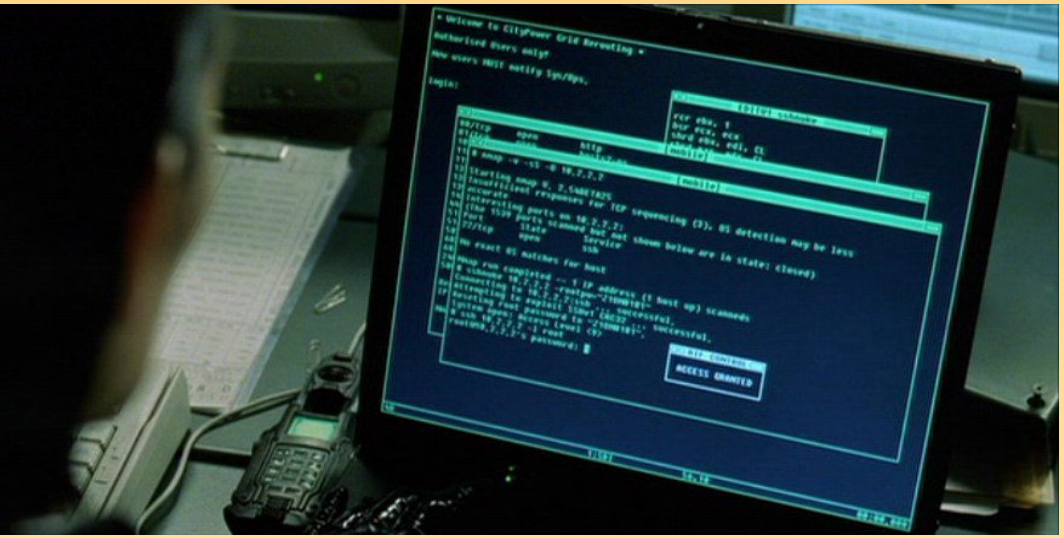
- Problema
- Introducción a Honeypots y su clasificación
- Nepenthes (la planta carnivora)
- Instalación y configuración
- Colectando bichos (malware)
- ¿Qué hago con los bichos?
- Conclusiones, P y R ...

Problema

- *El estado de la seguridad en Internet es pobre*
- Cualquiera puede ser un objetivo (virus, botnets ...)
- Los atacantes cada vez requieren menos conocimientos, existen muchas herramientas para ataques automáticos

Problema

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



Misión :: Conoce a tu enemigo!

Aprender sobre las técnicas de intrusión, herramientas de la comunidad blackhat.

Honeypot :: Definición

- A honeypot is a resource that is intended to be probed, attacked, or compromised. (Lance Spitzner)
- A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource, (Lance Spitzner)

Honeypot :: Clasificación

Interacción

- Alta: Sistemas Operativos reales

  Windows XP sin parches :)

- Baja: emulación

  honeyd, nepenthes

Nepenthes

Nepenthes :: Info

- Herramienta versatil para recolectar malware.
- Funciona de manera pasiva EMULANDO vulnerabilidades bien conocidas, además descarga el malware que intenta explotarlas.
- Detecta gusanos, bots y otro tipo de ataques.

- http://nepenthes.mwcollect.org

Nepenthes :: Módulos

- Resuelve DNS de forma asíncrona
- Emula vulnerabilidades
- Descarga archivos
- Envia los archivos descargados
- Dispara eventos
- Manejador de “Shellcodes”

Nepenthes :: funcionamiento

- Nepenthes necesita saber como funciona la vulnerabilidad, para crear una “interacción” con el ataque.
- Obtiene información sobre los archivos a descargar.
- Proporciona al atacante información para no ser descubierto.
- “Hace algo” con los archivos descargados

Nepenthes :: Usos

- Recolectar bichos
- Aprender de los bicho
- Incrementar la seguridad de tu red
- Demostrar que hay inseguridad en internet
- Estudiar los bichos
- Practicar técnicas de crackeo

Nepenthes :: Instalación

- Compilando :)
  - g++
  - libcurl, libmagic, libpcre, libadns, flex, bison
  - libpcap
- Usando los paquetes binarios
  - gentoo
  - debian y derivados
  - FreeBSD, OpenBSD

Nepenthes :: Configuración

- nepenthes.conf
- submit-norman.conf
- log-irc.conf
- xml-rpc

Bichos

- Malware muy diverso
- Diferentes propositos, atacan la misma vulnerabilidad.
- Casos especiales ...

- El proyecto de la UNAM ...

Bichos :: Reacción

- Ya tengo los bichos ...
- Mandarlos examinar (ofrecer el servico)
  - Sandbox
  - Norman
- Checarlos con un antivirus
- Buscar sus hash
- Analizarlos
- Ingeniería inversa **

Demostración en vivo de algunos bichos

Conclusiones

- La seguridad en internet es preocupante, TODOS podemos ser objetivos.
- Existen diversas motivaciones.
-
- “Lo que no se mide no se controla”
- Intentemos controlar “al menos esto”

Agradecimientos :: ~

Preguntas :: Respuestas

Hugo Francisco González Robledo
hugo@honeynet.org.mx

http://ardilla.zapto.org