Laboratorio de Investigación en Seguridad Informática

Si6

An Evening with kha0s

Sebastián García - sgarcia [at] citefa.gov.ar

Conferencia Internacional sobre Seguridad Informática
FIRST – ArCERT 4 de octubre de 2005

Instituto de Investigaciones Científicas y Técnicas de las FF AA
Div. Seguridad Informática – DINFO

Proyecto Paranoid

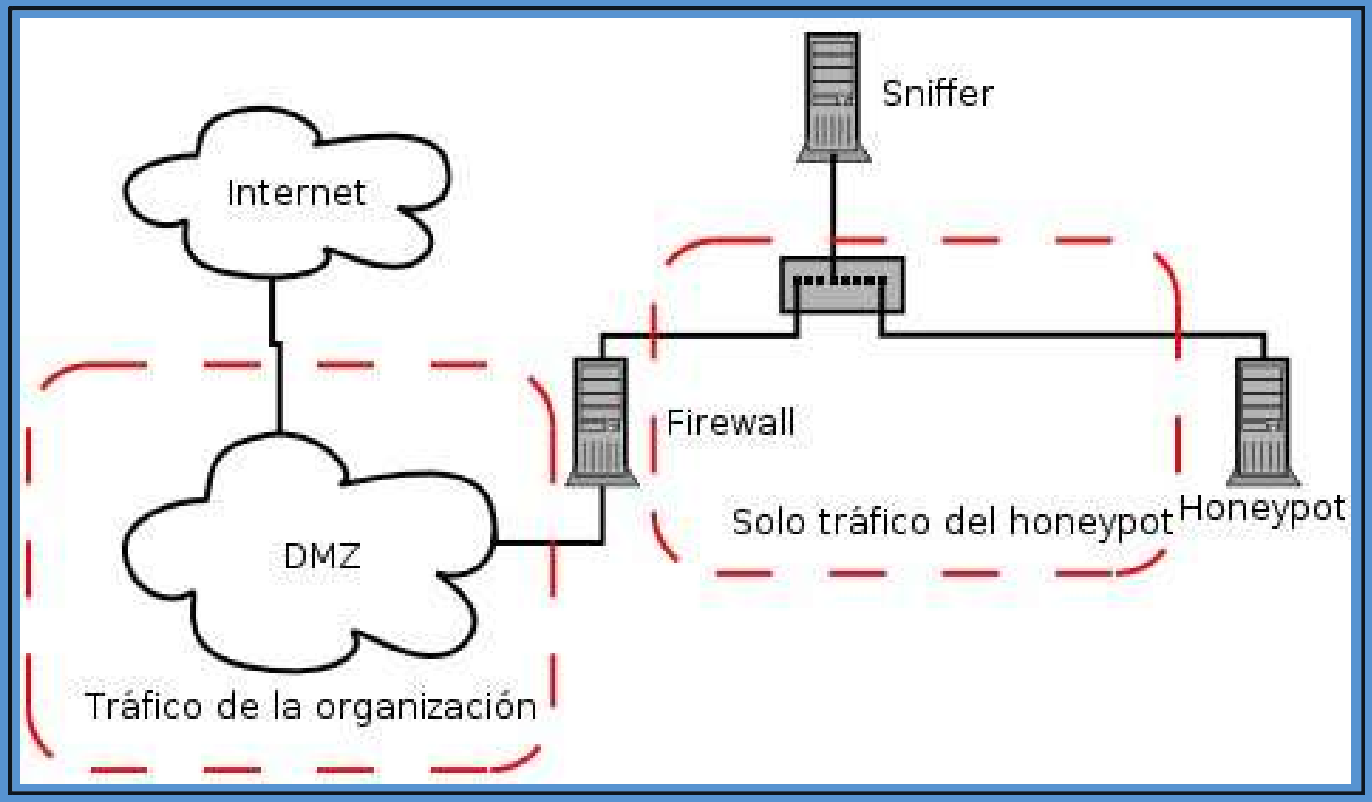
- Sólo clasificación e identificación, no razones ni herramientas.
- Criando Honeypots.
- Algunas decisiones sobre quién y comó podrá entrar.

En los hombros de los gigantes:

- William R. Cheswick, “An evening with Berferd”.
- Clifford Stoll, “The Cuckoo's Egg”.

La Camara Gesell - Arquitectura

- **El módulo keyloger:** Tcleo
- **El sniffer:** Tcpdump.
- **El Blanco:** Un linux instalado por omisión con más de 4 vulnerabilidades explotables.



Un honeypot simple es un honeypot estable

knock, knock... si6

El segundo día de funcionamiento recibimos la primera intrusión. Se había explotado la vulnerabilidad CAN-2003-0201 de samba que habíamos previsto.

Las primeras acciones fueron intentos de instalar un rootkit.

- No era conciente de la institución a donde ingresaba.
- No verificó si estaba siendo monitoreado.
- No sabía usar el sistema correctamente.
- Había modificado el exploit para que imprimiera:

> “wooooot! kha0s owns u :)”

Monitoreo constante.

Intrusos sí, usuarios no

- Los *usuarios* son clasificables, incluyendo el análisis por Keystroke Dynamics. Éstas son noticias viejas.

- Un *intruso* genera un patrón de comportamiento altamente clasificable debido al estado *mental* que supone transgredir las normas y comprometer un servidor. Su comportamiento y características biométricas difieren de su trabajo normal.

Clasificación básica de intrusos

Los intrusos tienen comportamientos diferentes:

Comandos iniciales: last, id, pwd, w, unset, screen -d -r, etc.

Comandos de salida: exit, kill -9 0, kill -9 $$, ^A en screen, ^D, rm -rf /*, killall -9 smbd, etc.

Uso de parámetros: ps afx -alf -fea, netstat -anp, ls -la -al -aF, tar -zxfv -tvfz, etc.

Uso de editores: en vi :wq! :q! ZZ, pico, emacs, mcedit, etc.

Sitios a los que acceden: exploits, rootkits, troyanos.

Clasificación básica de intrusos

Direcciones IP desde donde acceden:
Rumania, EEUU, Inglaterra, Polonia, etc.

Errores cometidos y su solución:
- Corregidos antes de terminar el comando.
- Ejecutados erróneamente y vueltos a tipear.

Secuencia de comandos: Qué comando primero, cuál después: [w, last], [cd /var/tmp/, wget], etc.

Uso de la shell: kha0s nunca usó el Tab de Autocompletion. set -o vi, unset, Tipo de Terminal, etc.

Balanceo Jerárquico de todos los métodos.

Clasificando el kha0s

- El primer y más frecuente visitante del honeypot.

  (A razón de 20 veces por mes, más de 120 veces en 6 meses).
- Altamente clasificable por sus acciones repetitivas y exploits.

  • wget, lynx y ftp fallidos a sitios .ro
  • kill -9 0, ps -fea
  • Los mismos troyanos
  • Evolución de ls a ls -a y finalmente a ls -ax
- Script Kiddie.

  (Desconocimiento de TCP/IP, redes, programación y linux.
  Utilizaba binarios infectados por worms).
- Inconciente del riesgo y oportunidades.

  (Sólo instala rootkits sin verificar si está o no en un honeypot).

Coleccionando Honeypots

Otros tres honeypots reportaron compromisos por un grupo de personas del mismo origen:

- Empresa japonesa de seguridad: www.lac.co.jp/business/sns/intelligente/sombria_e/smbr_2.pdf
- Un honeypot personal: thelostparadise.com/hoenypot/index.html
- El honeypot para el Segundo Reto de Análisis Forense de la Unam-Rediris (este honeypot capturó al usuario kha0s): www.seguridad.unam.mx/eventos/reto/uno_tecnico.pdf

Feliz Cumpleaños kha0s

Los script kiddies también se equivocan con las passwords

```
2005/04/06 15:19:29.834338 xx.xx.xx.xx:52813 -> 10.0.0.2:45295
 unset HISTFILE; echo "wooooot! kha0s owns u :)";uname -a;id;uptime;
           wooooot! kha0s owns u :)
           Linux nombre 2.4.18 #1 SMP Thu Mar 17 08:34:57 ART 2005 i686 unknown
           uid=0(root) gid=0(root) euid=65534(nobody) egid=65534(nogroup) groups=65534(nogroup)
           12:17:43 up 7 days,  8:05,  0 users,  load average: 0.00, 0.00, 0.00
 cd /var/tmp
 ftp xxxxxx.home.ro
 Password:
           a
           Name (xxxxxx.home.ro:root): Login incorrect.
           Login failed.

 user xxxxxx
           Password:
 25061981
           Login incorrect.
           Login failed.
           ?Invalid command.
T 2005/04/06 15:20:38.507264 10.0.0.2:45295 -> xx.xx.xx.xx:52813 [AP]
```

25061981

25 de Junio de 1981? 24 años

Un poco de paranoia

22 de abril

Ingresó al honeypot un intruso mucho más cuidadoso:

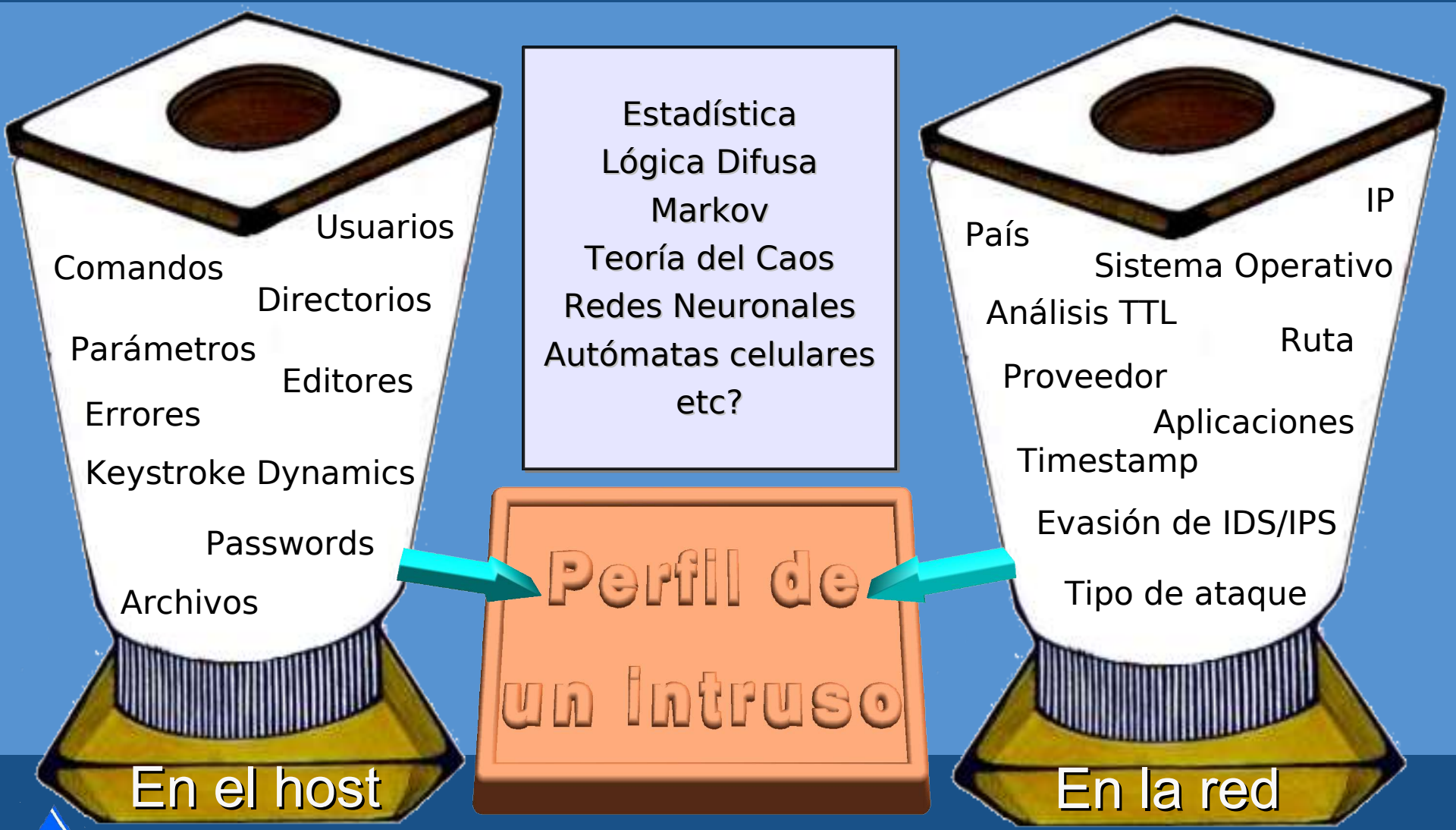
- Verificó el sistema en busca de 4 troyanos conocidos de linux.
- Instaló el programa chkrootkit.
- Verificó los módulos instalados.
- Instaló los 4 paquetes necesarios para ejecutar el tcpdump.
- Verificó los strings dentro de los binarios: login, telnet, ndc, ps, netstat, libps1.so, ls, lsof, find, etc.
- Intentó agregar usuarios a mano.
- Si bien no era experto, conocía el sistema y las aplicaciones.

Disección de una cadena de intrusiones

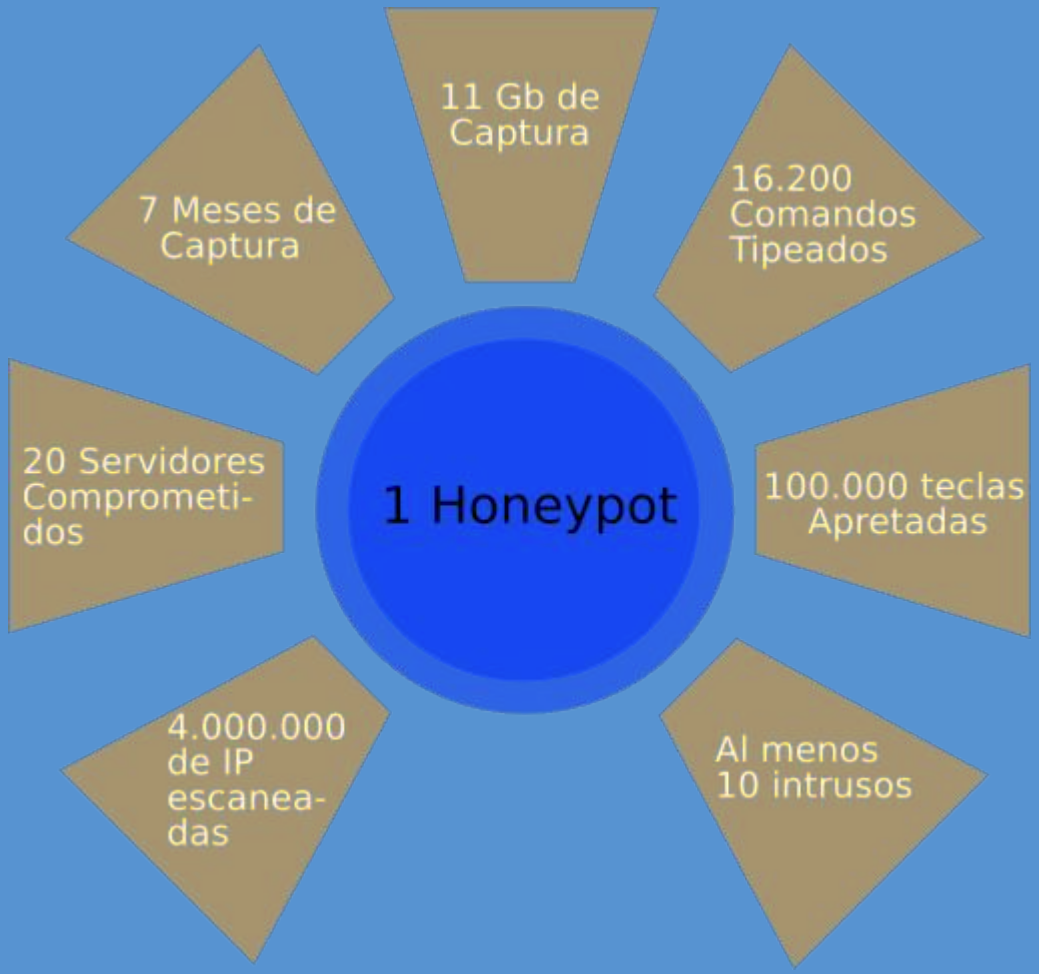
15 de mayo

- kha0s ingresó desde el honeypot hacia otros 20 servidores de Internet como resultado de su brute forcing de passwords ssh y los diferentes exploits.
- Llegó a ingresar hasta 3 servidores en cadena.
- El factor de análisis determinante fue el tiempo que se tardaba en escribir cada comando. Llegó a tardar casi 1 minuto para un comando wget.
- Realizó las mismas acciones en todos los servidores: instalación de rootkits y búsqueda de otros servidores vulnerables.
- En la mayoría de los casos ya había estado antes en ellos.

“I don't see the code anymore; I just see blondes, brunettes, red heads.”



Algunos Números



Berferd, el intruso de Cheswick de 1991, tenía un nivel de conocimiento más elevado que kha0s.

Siguiendo el paradigma actual, se acentúa la velocidad y cantidad de intrusiones.

Conclusiones

- El análisis siempre es complejo.
- Fue posible clasificar e identificar con técnicas básicas a la mayoría de los 10 intrusos.

Próximos Pasos

- Solamente accesos de intrusos de nivel técnico elevado.
- Participación en un ataque DDoS.
- Refinamiento de las técnicas complejas.

Preguntas

Copyright y Licencia