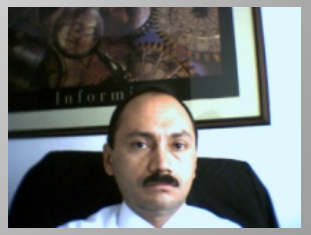
Honeypots: Herramientas forenses para trazar perfiles del enemigo

VII Jornada nacional de Seguridad Informática

Computación Forense: Rastreando la seguridad informática, junio 20, 21 y 22 de 2007

Armando Carvajal, Ing. Sistemas Unincca,
Especialista en software para redes de computadores Uniandes,
Maester en seguridad Informatica universidad Oberta de Catalunia Espania,
Gerente de consultoría Globaltek Security
e-mail: armando.carvajal@globalteksecurity.com



ACIS

Definición de honeypot 1/2

- Se define Honeypot como un recurso de red destinado a ser examinado, atacado y seguramente comprometido" por el atacante
- El honeypot proporciona información sobre el atacante antes de que se comprometan los sistemas reales

ACIS

Definición de honeypot 2/2

"A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource." (Lance Spitzner)

- **Krisztian Piller**

krisztianp2@yahoo.com
Sebastian Wolfgarten
sebastian.wolfgarten@de.ey.com
21C3, December 28, 2004, Berlin

ACIS

Definicion de “Honeynets” 1/5

- Se define una Honeynet como un conjunto de Honeypots altamente interactivos diseñados para la investigación y la obtención de información sobre atacantes
- Una Honeynet es una arquitectura, no un producto o un software determinado
- El objetivo es hacerle creer al atacante que está ante una red “real”, entonces se deben añadir los distintos elementos que conforman una arquitectura de red

Honeynets 2/5

- Tradicionalmente, la mayoría de los sistemas de seguridad han sido siempre de carácter defensivo
- IDS, Firewalls y demás soluciones se basan en la defensa de los sistemas de la organización, y cuando un ataque o vulnerabilidad es detectado de inmediato se procede a corregirlo
- Entonces el método tradicional no es proactivo es correctivo por lo tanto no hay mejora intrínseca o proactividad propia de los sistemas

ACIS

Honeynets 3/5

- Las Honeynets miran la forma de cambiar esta actitud mediante el estudio de los ataques y atacantes
- Obtener nuevos patrones de comportamiento y nuevos métodos de ataque con el objetivo de prevenirlos en los sistemas reales

ACIS

Honeynets 4/5

- Sin Honeynets, cada vez que se produzca un ataque “nuevo” y exitoso a un sistema real existente, este dejará de dar servicio y se verá comprometido
- Con las Honeynets, un ataque exitoso o nuevo no tiene porqué afectar a ningún sistema real

ACIS

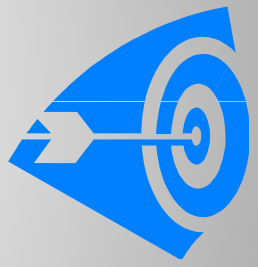
Honeynets 5/5

- Al igual que los Honeypots, la cantidad y calidad de información producida es muy importante, ya que cualquier actividad existente es sospechosa
- Entonces honeynets y honeypot no es lo mismo!!

ACIS

Que no hace un honeypot

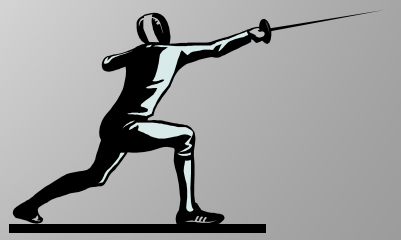
- No sirve para eliminar o corregir fallos de seguridad existentes
- No reemplaza un IDS
- Genera patrones para un IPS
- Si la red es vulnerable, añadir un Honeypot no resolverá esas fallas
- Evitar que un atacante fije su interés en nuestra red



ACIS

Caracteristicas de los honeypots

- Genera un volumen pequeño de datos
- Necesitan recursos informáticos mínimos
- Son elementos pasivos
- Son fuentes potenciales de riesgo para la red
- Muy bajo numero de falsos positivos



ACIS

Caracteristicas de los honeypots

- Usan una dirección IP como mínimo
- Los Honeypots tienen un limitado carácter preventivo
- Tienen un alto grado de detección por los intrusos de ahí que son conocidos como tarros de miel
- Son programables en cuanto a la reacción contra el atacante

ACIS

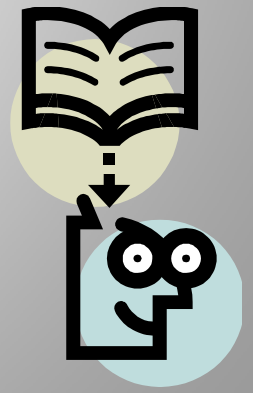
Clasificación o taxonomia

- Honeypot de producción (Production Honeypot System)
- Honeypot de investigación (Research Honeypot System)

ACIS

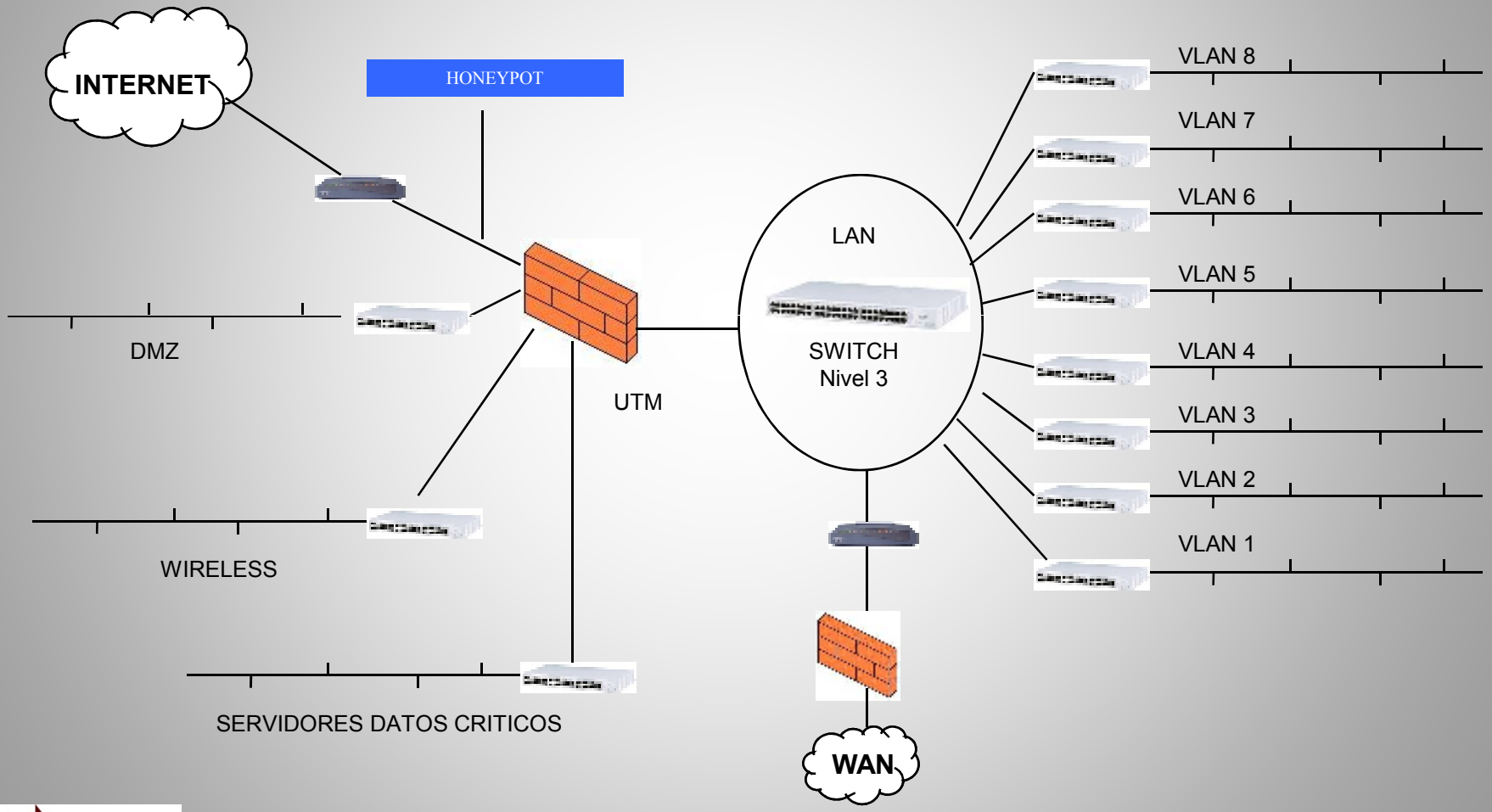
Ubicación en la red

- **Fuera del perímetro de proteccion:** Esta localización es la que menos riesgo suministra a la red
- Como este se encuentra fuera de la zona protegida por el firewall, puede ser atacado sin ningún tipo de peligro para el resto de la red
- Y hay peligro para los demás?



ACIS

HONEYPOT: FUERA DEL PERIMETRO DE PROTECCION



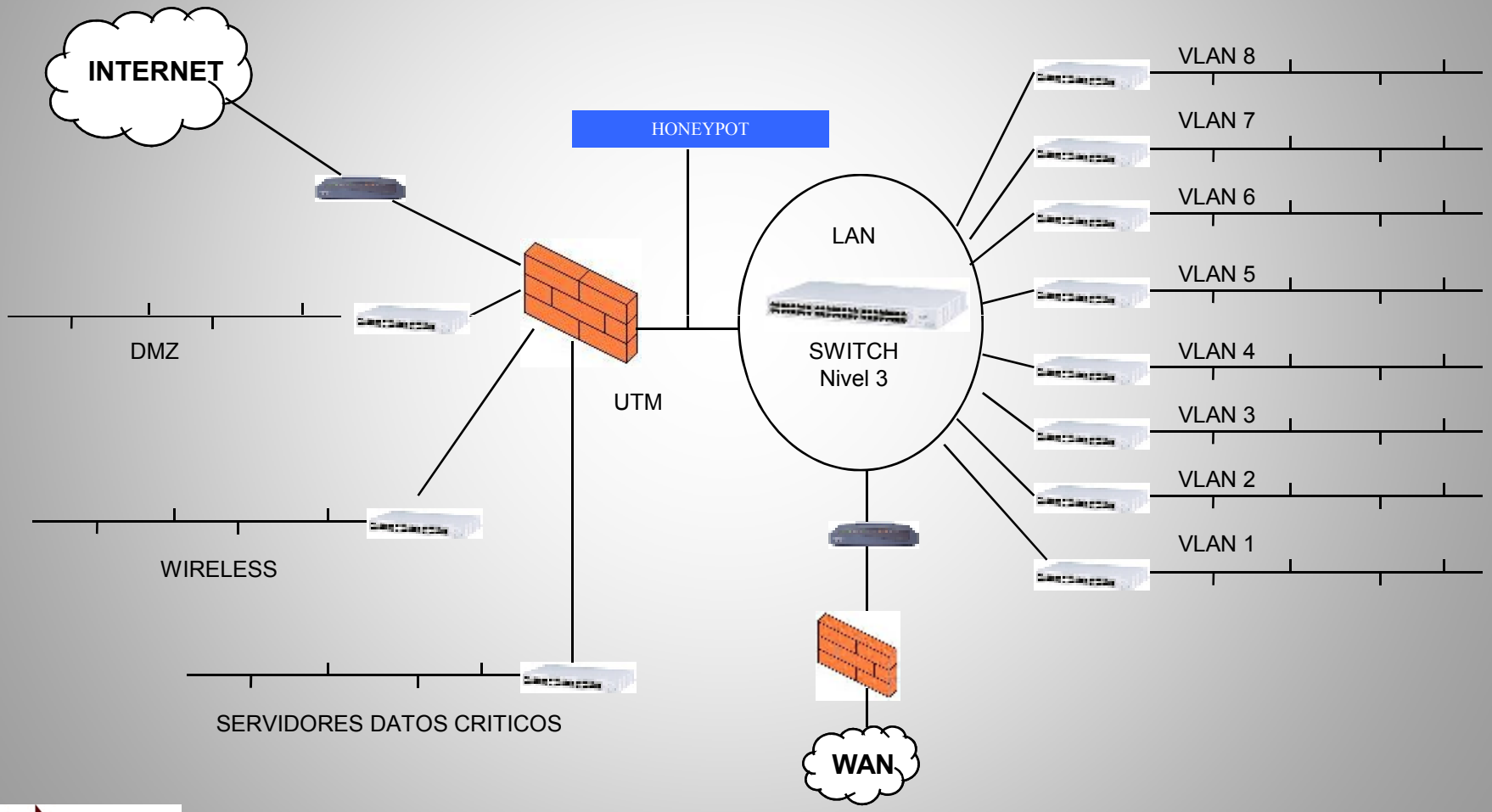
ACIS

Ubicación en la red

- **Detrás del firewall**: El acceso al Honeypot esta dirigido por las reglas de filtrado del firewall, su ubicación permite la detección de los atacantes internos, los firewalls mal configurados, las máquinas infectadas por gusanos y los atacantes externos

ACIS

HONEYPOT : DETRAS DEL FIREWALL

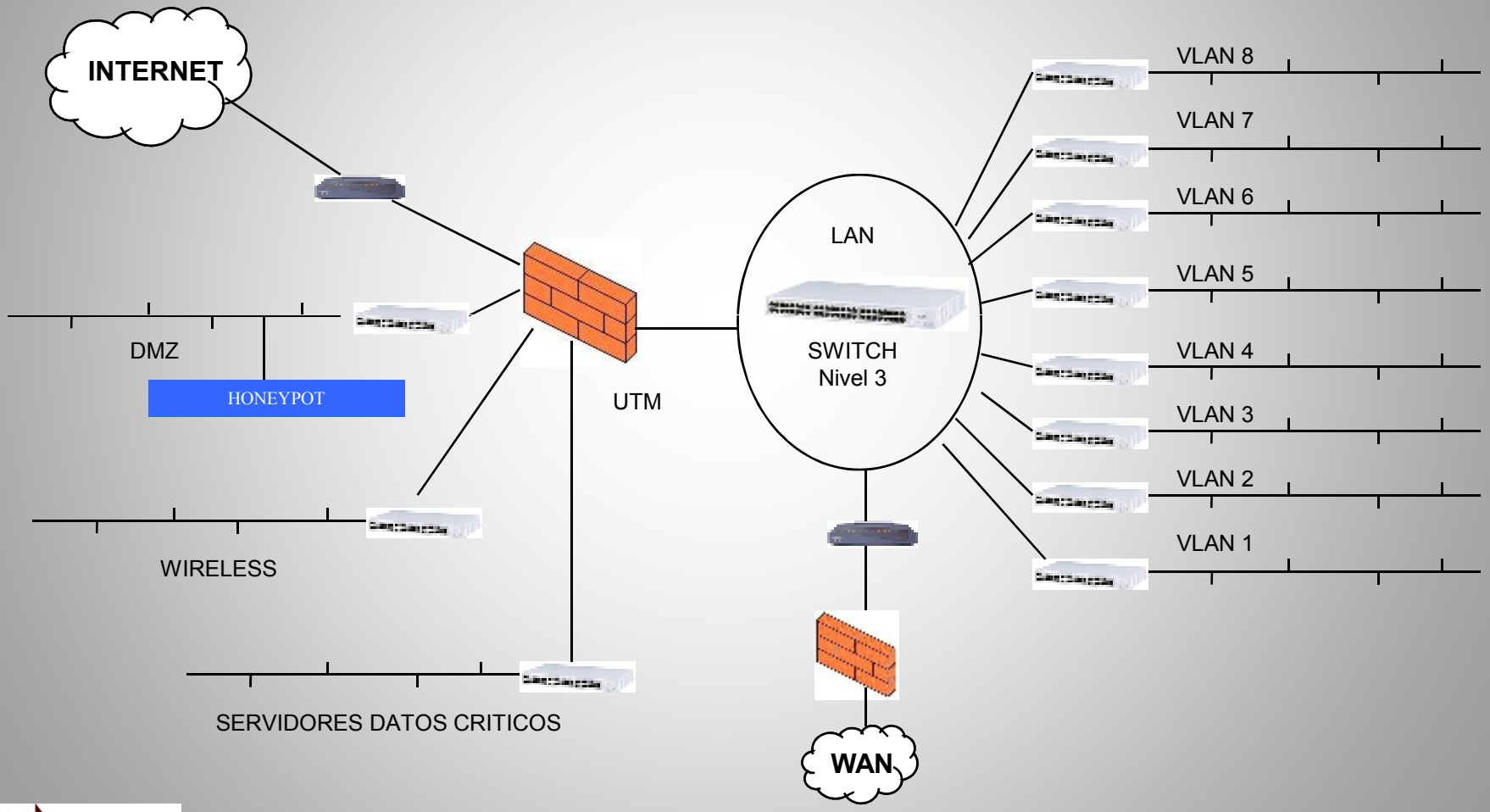


Ubicación en la red

- **En la zona desmilitarizada**: Es la ubicación ideal pues permite detectar ataques externos e internos con una reconfiguración del firewall

ACIS

HONEYPOT EN LA DMZ



Y lo legal es mi problema?

Yo soy tecnico!!

ACIS

Repercusiones legales

- El abogado Carlos Santiago Álvarez Cabrera en su artículo “Honeypots Aspectos penales”, Colombia, Diciembre de 2005, http://cyberlaws.blogspot.com, concluye respecto de las vulnerabilidades, que: La velocidad de los ataques esta en constante incremento debido a los “0 days vulnerabilityes”

Repercusiones legales

- “Trampa (Entrapment): Es el proceso realizado por los cuerpos policiales (law enforcement) de “inducir” a alguien a cometer un acto punible con el objetivo de iniciar la acción judicial pertinente”

Repercusiones legales

- “En este caso del Honeypot, aunque es un elemento pasivo creado por nosotros para ser atacado (sin que seamos parte de los cuerpos policiales)
- Si no deseamos perseguir judicialmente esta intrusión en el Honeypot, no realizamos ninguna trampa
- El objetivo del Honeypot es recibir los ataques, no recoger información para demandar a los atacantes del Honeypot”

ACIS

Repercusiones legales

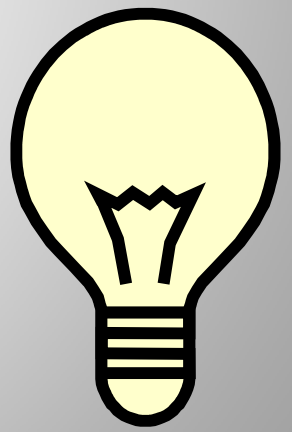
- “Privacidad (Privacy): La información recogida puede dividirse en información transaccional e información de contenido”

Repercusiones legales

- “Responsabilidad (Liability): Este aspecto hace referencia a las posibles demandas que podemos recibir en el caso de que un atacante utilice nuestro Honeypot como plataforma de lanzamiento de ataques
- Las demandas se basarían en que nosotros no hemos realizado unos mínimos esfuerzos de seguridad en nuestra red, sino que al contrario, facilitamos el acceso a nuestros recursos para que sean utilizados en todo tipo de ataques”

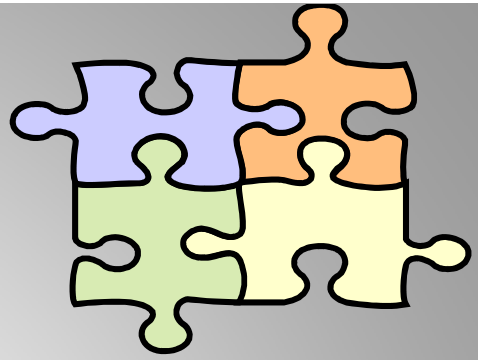
Utilidades

- Honeypots útiles para las investigaciones forenses específicamente en las investigaciones de inteligencia porque permiten analizar la actividad del atacante basados en el engaño
- Ideal para las fuerzas militares



ACIS

Utilidades

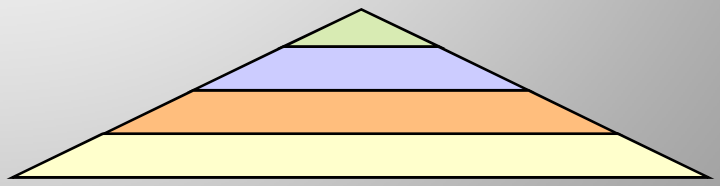


- Si ya se conoce la identidad del atacante y además usted va a tomar acciones en contra del atacante es importante recordar que antes de poner el honeypot se debe tener un permiso judicial contra el atacante
- Utilidad en sistemas en producción: Brindan protección, prevención, detección y respuesta a los ataques de baja interacción

ACIS

Utilidades

- Utilidad en la Investigación: Permite recolectar información, ayuda a definir tendencias respecto de las actividades del atacante, activación de sistemas tempranos de alarma, predicción de ataques e investigaciones criminales con alta interacción
- En concreto permiten ejercer el derecho a la legítima defensa



ACIS

Como ayudan

- Dado que su objetivo fundamental es la construcción de un perfil del atacante permite la detección de las **“0 days”** vulnerabilidades que son tan intimidantes como las amenazas desconocidas

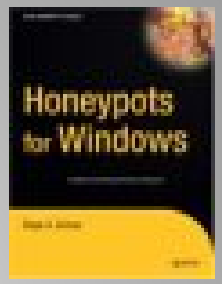
ACIS

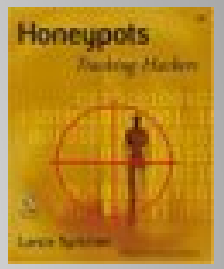
Como ayudan

- Por ejemplo si detectamos trafico masivo y desconocido en la red se puede intuir que el atacante ya esta adentro, entonces con un honeypots se puede capturar el username y el password del hacker, permiten la activación de keyloggins, la detección del email del atacante, permiten ver el contenido del chat del hacker con terceros, etc.
- **En concreto: Se puede establecer como funciona el atacante que es lo que hace y como me hace daño en forma detallada**

ACIS

Bibliografia





- www.honeypot.org
- www.honeynet.org
- Honeypots for windows, Roger A Grimes, 2005, Editorial Apress
- Honeypots, Tracking Hackers, Lance Spitzner, 2003, Addison Wesley

ACIS

Bibliografía

- Carlos Santiago Álvarez Cabrera, artículo "Honeypots Aspectos penales", Colombia, Diciembre de 2005, http://cyberlaws.blogspot.com
- Torres falkonert, Daniel Andres, "Técnicas de Informática Forense en la investigación de delitos de alta tecnología", sep 2003

ACIS

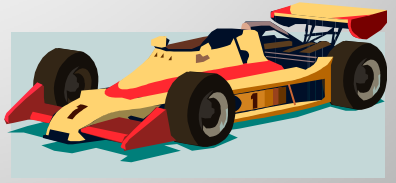
Laboratorio: Prueba de concepto

- **Objetivos:**
- Detectar intentos de ataques a nuestra red mediante el uso de honeypots
- En la actualidad, muchos de los ataques que se producen en las redes tienen lugar mediante un proceso en dos fases: un escaneo previo para detectar máquinas susceptibles de ser atacadas, y el ataque posterior
- El objetivo de este apartado es ser capaces de detectar esos ataques y guardar la información relevante

ACIS

Honeypot: Prueba de concepto

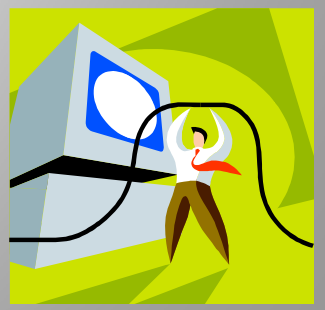
- En el caso real, la red de nuestra organización sería 192.168.100.0/24
- Lo que vamos a hacer es incluir en ella un conjunto de máquinas '**honeypot**' que permitan detectar los ataques que en ella se producen
- Usaremos linux "Back | track" de www.remote-exploit.org



ACIS

Honeypot: Prueba de concepto

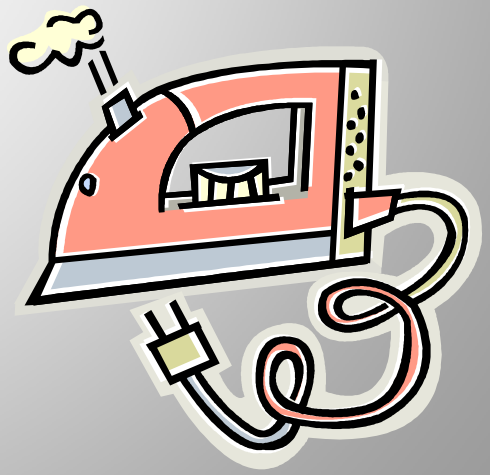
- Creación de un honeypot para capturar el tráfico del puerto 80 sobre el IP 192.168.100.3:
- Modifique el archivo **honey.cfg** para que:
- Responda al tráfico ICMP
- Tenga abierto el puerto 80 TCP
- Cuando reciba una petición por el puerto 80 TCP ejecute el comando sh /tmp/web.sh y guarde los intentos de ataque en un log



ACIS

Honeypot: Prueba de concepto

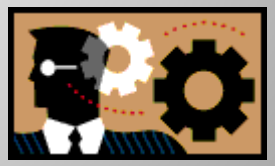
- create default
- set default personality “Windows 2003SP1"
- set default default tcp action block
- add default tcp port 80 "sh /tmp/web.sh"
- set default uid 1000 gid 1000
- bind 192.168.100.3 default
- set 192.168.100.3 uptime 1327650



ACIS

Honeypot: Prueba de concepto

- Notas:
- Es clave la instrucción set default default tcp action block para que el servidor web responda al requerimiento
- Si prueba todas las posibilidades únicamente “block” funcionara



ACIS

Honeypot: Prueba de concepto

- La ruta para el shell web.sh en knoppix-std es: **/usr/share/doc/honeyd/examples/web.sh**
- La ruta para el shell web.sh en Linux Auditor es: **/usr/share/honeyd/scripts/web.sh**

ACIS

Honeypots: Prueba de concepto

```
#!/bin/sh

DATE=`date`
cat   <<   _eof_
HTTP/1.0 200 OK
Date: $DATE
Server: Microsoft-IIS/5.0
Connection: close
Content-Type: text/plain


 Volume in drive C is Webserver
 Volume Serial Number is 3421-07F5
 Directory of C:\inetpub

01-20-02   3:58a      <DIR>          .
08-21-01   9:12a      <DIR>          ..
08-21-01  11:28a      <DIR>          AdminScripts
08-21-01   6:43p      <DIR>          ftproot
07-09-00  12:04a      <DIR>          iissamples
07-03-00   2:09a      <DIR>          mailroot
07-16-00   3:49p      <DIR>          Scripts
07-09-00   3:10p      <DIR>          webpub
07-16-00   4:43p      <DIR>          wwwroot
               0 file(s)              0 bytes
              20 dir(s)     290,897,920 bytes free
_eof_
```

Honeypots: Prueba de concepto

- honeyd -d -i lo -f honey.cfg -l log.honeyd
- Pruebe que el servidor web responda:
- telnet **192.168.100.3** 80
- Trying 192.168.100.3... Connected to 192.168.100.3. Escape character is '^]'.
- Digite: GET /, y dos veces la tecla enter
- Vera una pantalla del servidor MS Windows simulada por linux.

ACIS

Sniffer Tcpdump vera:

- 2006-01-25-18:39:06.0556 tcp(6) S 192.168.100.1 32804 192.168.100.3 80 [Linux 2.4 lo0]
  2006-01-25-18:39:06.0556 tcp(6) - 192.168.100.3 80 192.168.100.1 32804: 44 SA
  2006-01-25-18:39:09.0749 tcp(6) - 192.168.100.3 80 192.168.100.1 32804: 40 A
  2006-01-25-18:39:11.0026 tcp(6) - 192.168.100.3 80 192.168.100.1 32804: 40 A
  2006-01-25-18:39:11.0029 tcp(6) - 192.168.100.3 80 192.168.100.1 32804: 552 A
  2006-01-25-18:39:11.0029 tcp(6) - 192.168.100.3 80 192.168.100.1 32804: 552 A
  2006-01-25-18:39:11.0029 tcp(6) - 192.168.100.3 80 192.168.100.1 32804: 74 A
  2006-01-25-18:39:11.0029 tcp(6) - 192.168.100.3 80 192.168.100.1 32804: 40 FA
  2006-01-25-18:39:11.0032 tcp(6) - 192.168.100.3 80 192.168.100.1 32804: 40 A
  2006-01-25-18:39:21.0038 tcp(6) E 192.168.100.1 32804 192.168.100.3 80: 9 1058
- Estas son las pruebas del tipo de trafico que el atacante me envió al servicio

ACIS