Introducción al uso de Honeypots.

Diego Lendoiro Rodríguez <diego@inestable.org>

Jorge Iglesias García <mendigou@gmail.com>

SOME RIGHTS RESERVED

Indice

- honey@xornadas.usc:~#cat index
  - Tipos de atacantes (diferencias)
  - Métodos y motivos de un ataque
  - ¿Qué es un honeypot?
    - Definición y tipos
  - ¿Que papel juegan en nuestro sistema de seguridad?
    - Honeypots + Snort
  - Niveles de interacción (Clasificación)
  - Herramientas

Tipos de atacantes.

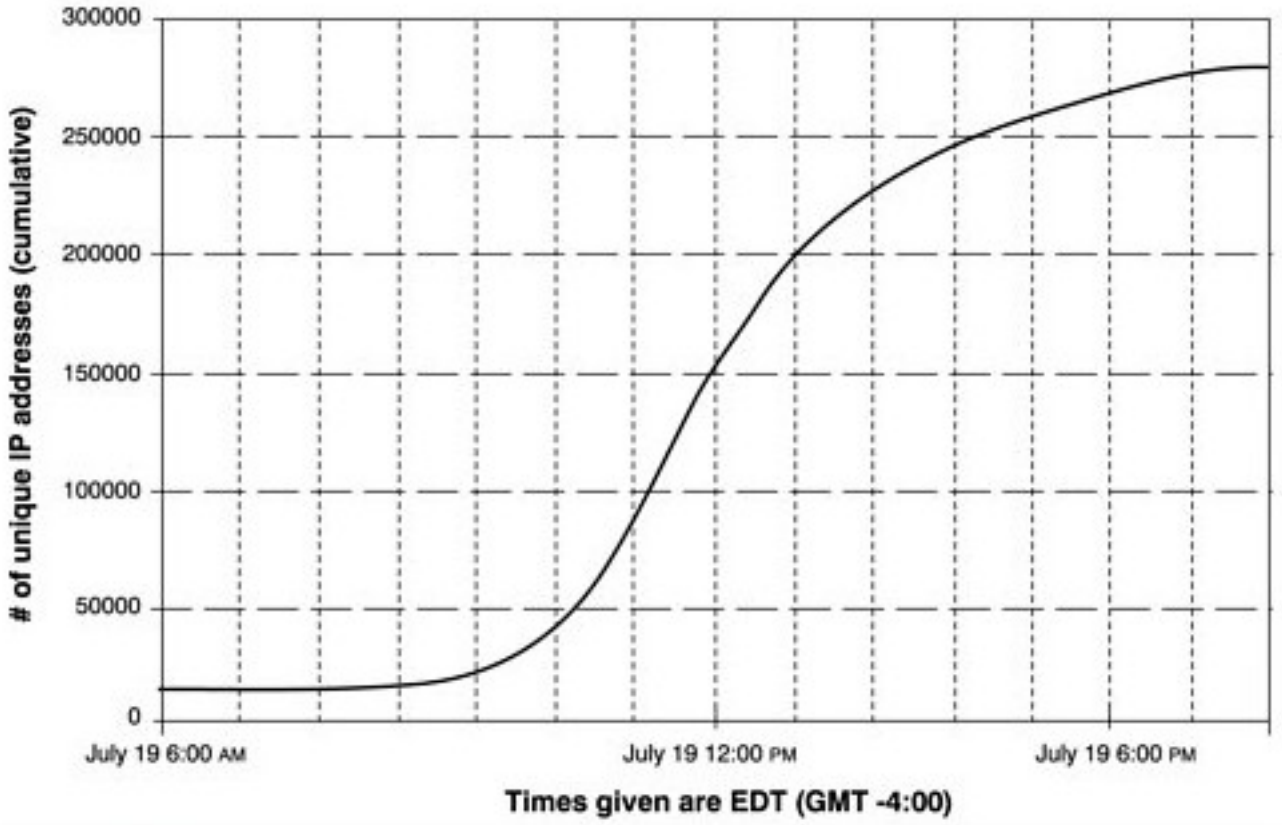
- Factor humano:
  - Script Kiddies:
    - Usan herramientas automatizadas (scripts, scanners de vulnerabilidades
    - Intrusiones “toscas” tienden a no borrar huellas
    - Preocupación por crackear el mayor número de máquinas posibles
  - Blackhats o intrusos experimentados:
    - Uso de métodos más sofisticados
    - Tienden a no dejar huellas

Tipos de atacantes.

- Y aunque parezca mentira:
- A finales de 2000:
  - El tiempo estimado de vida de una RH 6.2 era de 72 horas
- A principios de 2002:
  - Se había aumentado en un 100% el numero de scaneos y de detecciones hechas por IDS's tipo Snort
- A finales de 2002:
  - Una red SoHo podía ser scaneada más de 40 veces por distintos hosts.
- Ya en 2006:
  - Quién no ha hecho un cat /var/log/messages | grep sshd ?

Tipos de atacantes

Figure 2-4. Graph from CERT of IP addresses compromised by the CodeRed worm (Data for July 13, 2001 as represented to the CERT/CC; from: Incident data for CERT #36881. Used with permission.)

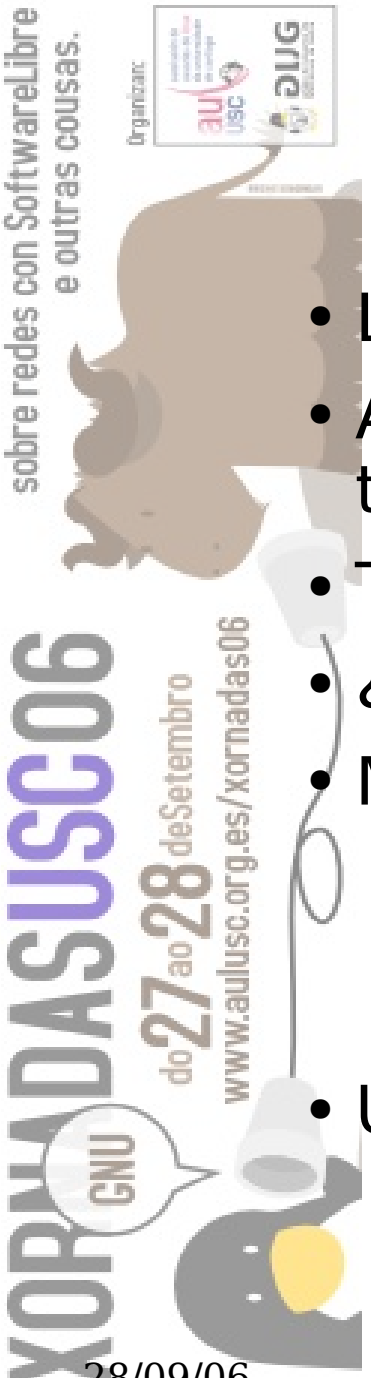


Métodos y motivos para un ataque

- Mótivaciones de los atacantes:
  - Script Kiddies:
    - Uso de sistemas para colgar diferentes tipos de aplicaciones.
    - Robo de datos sensible del usuario.
    - Uso de aplicaciones automatizadas.
    - Objetivos escogidos al azar
      - Perfil que debe cumplir el objetivo:
        - Poseer determinada vulnerabilidad para la cual poseen el exploit o script que consiga violar el sistema.

Métodos y motivos para un ataque

- Blackhats:
  - Normalmente objetivos no escogidos al azar
  - No deben de cumplir ningún requisito
  - Posibilidad de utilizar xploits o scripts NON-Full Disclosure
  - Eventualmente penetran sistemas que utilizarán como “proxy” para otros ataques.
  - Uso de métodos y herramientas más sofisticadas para realizar el ataque (diferentes tipos de firewall bypassing y otras técnicas para evadir IDS's)



En resumen:

- Los atacantes:
- Avanzados y no avanzados debido a las nuevas técnicas.
- TIENEN UN RIESGO CONSIDERABLE!!
- ¿Que podemos hacer para solucionarlo?
- Medidas de seguridad típicas:
  - Uso de conexiones cifradas (SSL)
  - Fuertes métodos de autentificación (2way factor)
  - Uso de IDS's (por ejemplo Snort)
- Uso de Honeypots
  - Herramienta complemententaria a las anteriores

¿Que es un Honeypot?

- Un recurso (STA o SERV) cuyo valor no reside en la producción o la prestación de un servicio como habitualmente se conoce.
- El valor de un honeypot reside en ser atacado, probado y vulnerado.
- Dicha condición nos permitirá:
  - Obtener pruebas del ataque al sistema.
  - Descubrir nuevos fallos.
  - Despistar al atacante sobre los servidores en producción que poseemos.

¿Que es un Honeypot?

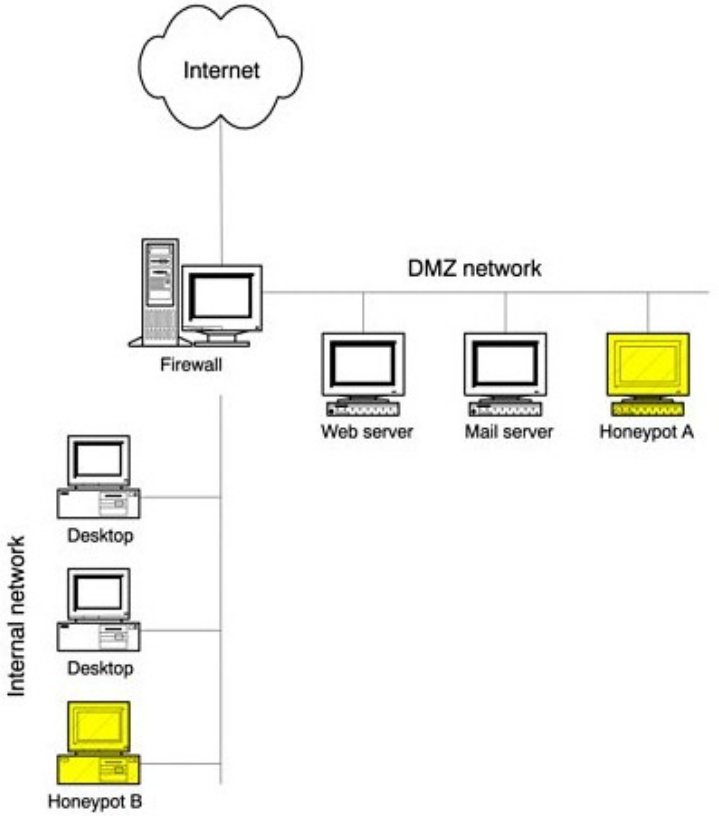
- Implementación de seguridad global a diferencia de firewalls o IDS's
- Permitir atajar bugs en nuestros servidores de producción.
  - Característica de prevención asociada con los honeypots (Una de los tres conceptos sobre seguridad definidos por Bruce Schneier Prevención, Detección y Respuesta)

¿Que es un Honeypot?

- Tipos de Honeypots
  - Dependiento de si decidimos utilizar un honeypot en producción o no:
  - Research Honeypots:
    - O Honeypots de investigación
    - Permiten averiguar más información sobre nuevas técnicas.
    - No tienen valor de producción en sí mismos.
  - Production Honeypots:
    - Honeypots a nivel de producción.
    - Permiten averiguar algo menos de información sobre el atacante (normalmente menor nivel de interacción)
    - Poseen valor como/para servidores de producción

Ejemplo: SoHo con Honeypots

Figure 3-1. Though vastly different in how they were built and what their purpose is, Honeypots A and B share the definition and concepts of a honeypot.



Modelos de seguridad

- Modelo de seguridad de Bruce Scheneier
  - Prevención
    - Uso de firewalls y otras medidas
    - Procesos de autentificación
      - En el caso de los Honeypots Poca aportación a este nivel de seguridad.
      - Uso como método disuasorio o de engaño
        - Válido únicamente con atacantes experimentados
  - Detección
    - Uso de ID's y herramientas de “log analysis”
      - Gran respuesta ante falsos positivos y falsos negativos

Modelos de seguridad

- Respuesta
  - En caso de un ataque exitoso:
    - Uso de herramientas forenses
    - Trazado inverso de las acciones del atacante
  - Problemas en servidores de producción:
    - El intenso tráfico puede hacer muy dificil y costoso en algunos casos el análisis forense
    - Los honeypots hacen mucho mas sencillo el análisis forense de los sistemas atacados

¿Cómo funcionan?

- Capturar un flujo de datos que NO DEBE estar ahí.
- Obtención de tráfico NO VÁLIDO (en el sentido de la producción)
- Dicho tráfico es estudiado con detenimiento empleando diversas ténicas como IDS's o aplicaciones de análisis forense

¿Cómo funcionan?

- Diferencias con firewalls y otras medidas de seguridad:
  - Flexibilidad:
    - Posibilidad de recolectar información para investigación sobre el atacante y descurbrir nuevos métodos de penetración.
    - Uso para disuadir a los atacantes de intentar penetrar deception / deterrence
    - Distraer a los atacantes de los sistemas en producción
    - Método de detección / prevención en caso de nuevos bugs.

Ventajas vs Desventajas

- Ventajas:
  - Recogida de información
    - Logs mucho menores
    - Información crítica en su 99%
  - Uso de recursos
    - Menos recursos frente a firewalls o IDS's
  - Simplicidad
    - No existe necesidad de establecer complejos sistemas.
  - Reinversión

Ventajas vs Desventajas

- Reinversión:
  - Un posible escenario:
    - Disponemos de una red con un firewall que ha estado funcionando un par de años
    - Llegado el momento Minglanillas (Tu jefe) decide que para que quiere seguir gastando tanto dinero en mantener dicho firewall si nunca ha tenido problemas.
    - Como todo buen BOFH atiendes su petición y paralelamente se implementa un Honeypot
    - RESULTADO: SE IMPLANTA DE NUEVO EL FWALL

Ventajas vs Desventajas

- Desventajas:
  - Punto de vista limitado.
    - Reacción solo ante ataques realizados directa o indirectamente contra el honeypot
  - Fingerprinting
    - Posibilidad de identificar un honeypot debido a ciertos comportamientos
  - Riesgo
    - Introducen un nivel de riesgo en nuestro sistema
    - El nivel de riesgo depende del nivel de interacción del honeypot

En resumen

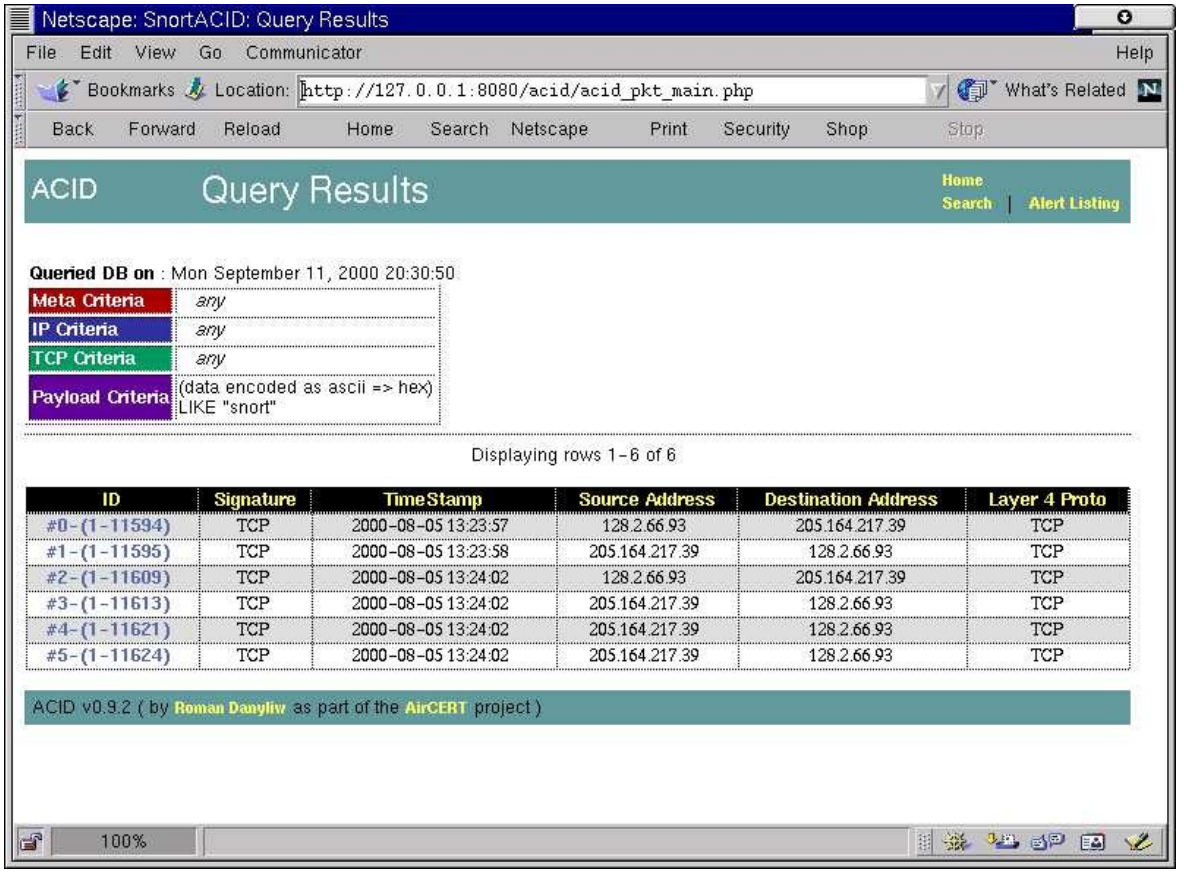
- Los honeypots:
  - Ante todo NO son una solución de seguridad
    - Son un COMPLEMENTO GLOBAL a nuestro sistema de seguridad
  - Debemos valorar sus ventajas y sus desventajas
  - Debemos valorar que tipo de honeypot queremos implementar

Honeypots + Snort

- Uso de Honeypots con IDS's
  - Uso combinado de IDS como Snort nos permitirá:
    - Detectar las alertas en nuestro honeypot
    - Tener una estadística detallada de todas las alertas (ACID)
    - Control detallado de las conexiones al honeypot

Honeypots + Snort

- ACID (Analysis Console for Intrusion Databases)



Niveles de interacción.

- Los dos tipos de honeypots se pueden clasificar en niveles de interacción:
  - Baja interacción
    - NFR Backofficer Friendly
    - Honeyd
  - Media interacción
    - Nephentes
    - Mwcollect
  - Alta interacción
    - Honeynets

Herramientas

- NFR Backofficer friendly
  - Honeypot de baja interacción
  - No está considerado por muchos un honeypot en sí.
  - Obtención de información limitada.
  - “Daemons” en escucha que sólo presentan banners.
  - Fácil instalación y configuración.

Herramientas

- Honeyd
  - Honeypot de baja interacción
  - Grandes posibilidades
    - Uso de templates para emular los OS's
  - Uso de fingerprinting
    - Uso de la base de datos de fingerprints de Nmap
  - Uso de blackholing
  - Capacidad de emular diferentes sistemas operativos.

Herramientas

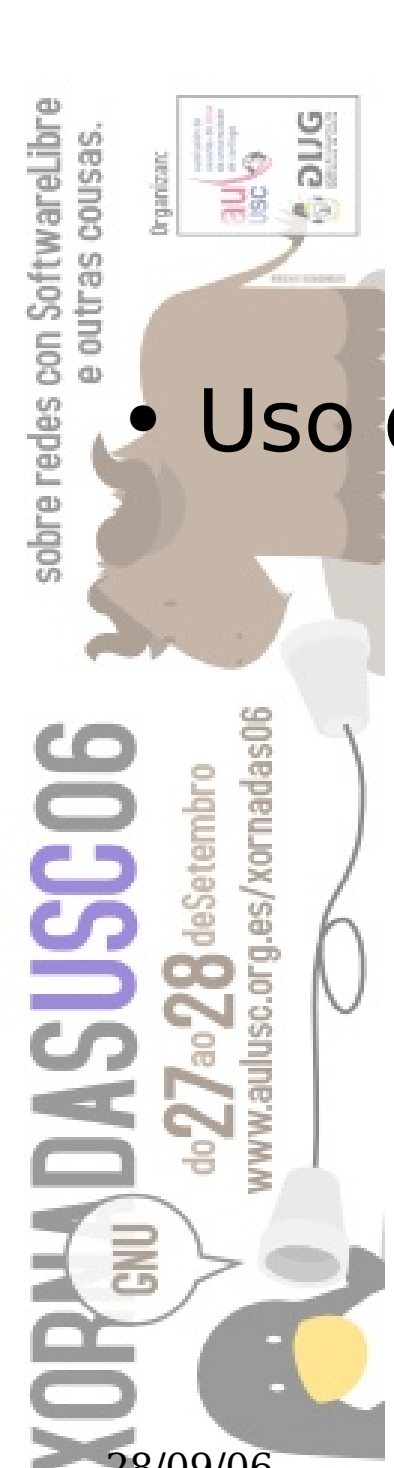
- Honeyd
  - Baja interacción
    - No emula un sistema completo.
    - Usa templates para generar los sistemas emulados.

```
# Example of a simple host template and its binding
create template
set template personality "AIX 4.0 - 4.2"
add template tcp port 80 "sh scripts/web.sh"
add template tcp port 22 "sh scripts/test.sh $ipsrc $dport"
add template tcp port 23 proxy 10.23.1.2:23
set template default tcp action reset

bind 10.21.19.102 template
```

Herramientas

- Uso de blackholing (Arpd)
  - Técnica que permite a un sistema (honeyd) emular máquinas virtuales sobre peticiones a ips no existentes.
  - DRY THEORY:
    - El atacante hace un scan de la red
    - Se generan por tanto peticiones ARP
    - Honeyd genera sus propias peticiones ARP sobre esas direcciones IP
    - ARP SPOOFING



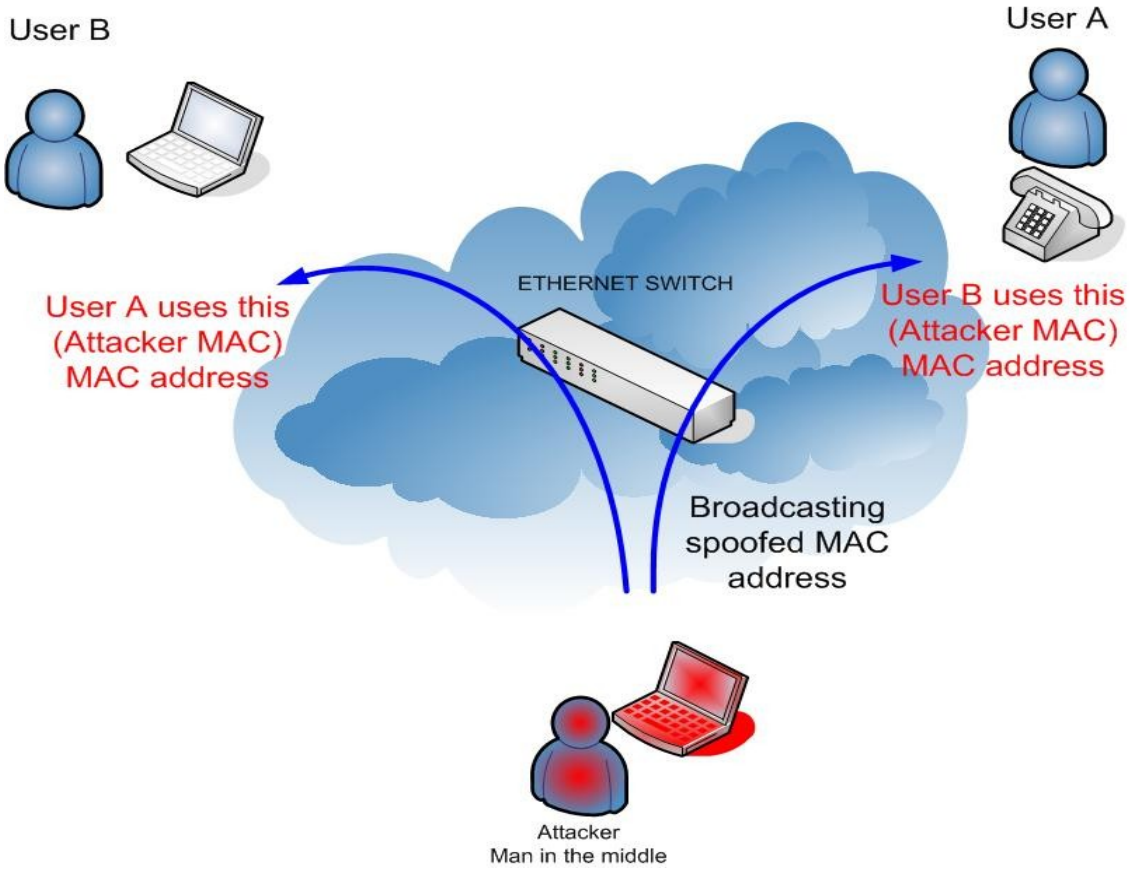
Herramientas

- Uso de blackholing

```
[geek@0x300 ~]$ arp -a
? (192.168.1.1) at 00:30:da:92:85:28 on ath0 [ethernet]
? (192.168.1.33) at 00:0f:20:93:7d:49 on ath0 permanent [ethernet]
```

Herramientas

- ARP SPOOFING



Herramientas

- Otros tipos de honeypots:
  - Interacción media:
    - HoneyTrap
    - Nepenthes
    - Mwcollect
  - Alta Interacción:
    - Implican emulación de sistemas completos, incluso redes completas de sistemas reales.
    - Honeynets

Referencias:

- Oh gran libro de sabiduría:
  - http://www.wikipedia.org
- Honeynet project & whitepapers
  - http://www.honeynet.org

Agradecimientos:

- Antes de nada decir que esto es un claro ejemplo de que los telecos no solo trabajamos en capa 2 ;-)
- Gracias a toda la gente de AULUSC y GLUG por estas Xornadas
- Gracias a los trabajos de la gente de la wikipedia, Honeynet project, Addison Wesley, SaNS, etc
- Todas las imágenes usadas pertenecen a sus respectivos dueños.
- Como siempre: CreativeCommons [by-nc-sa]