

# SSH SNIFFER

*Una experiencia educativa de  
investigación*

*[[www.ssh-sniffer.com.ar](http://www.ssh-sniffer.com.ar)]*



Sebastián García  
Leandro Ferrari  
Esteban Cano



22 de Agosto del 2008



Jornadas Regionales  
de Software Libre

# Itinerario

- Introducción
- Qué queremos enfatizar
- Historia del grupo
- Resolución técnica del problema
- Conclusiones

# Introducción

- Laboratorio de Investigación en Seguridad Informática Si6 - Citefa
- Proyecto de detección de intrusos
- Convenio con Universidad FASTA
- Creación del grupo de investigación extracurricular

# Qué queremos enfatizar

## 1. Proceso de investigación

→ Adaptación y aprendizaje

## 2. Metodología grupal

→ Cómo nos llevamos y organizamos

## 3. Desarrollo técnico

→ Cómo resolvimos el problema

• El grupo trabaja todos los aspectos

# Comienzo del grupo

- Una reunión para conocernos
- Reuniones virtuales
  - Cada 15 días con tarea para el hogar
  - Lectura de documentos y prácticas
  - Mensajeros
- Los primeros cuatro meses una reunión presencial por mes

# Comienzo del grupo

## Formación básica en seguridad

- Conceptos generales
- Sniffing
- Scanning
- Exploits
- Honeypots
- Linux
- Criptografía
- SSH

# Recursos

- Chat
- Grupo Yahoo, mailing list y archivos
- Backtrack (Live CD)
- Clase virtual
  - Requiere de una planificación más cuidada. Documentos, programas, tareas.

# SSH

- Protocolo cifrado cliente-servidor
  - Acceso a una shell
  - Copia de archivos
  - Túneles
- ¿Porqué lo utilizan los intrusos?
  - Metodología
    - Ingreso con un exploit
      - Cambio de clave de un usuario
      - Conexión con SSH
    - Cracking de passwords

# Introducción al problema

- Se necesitaba diferenciar automáticamente en SSH
  - Sesiones interactivas
    - Acceso exitoso manual o automático
  - Sesiones no interactivas
- Archivos de capturas de gran tamaño

# Resolución del problema

- Capturar suficientes intrusiones
  - Honeypot Si6: ~260 sesiones interactivas en 3 años
- Analizar manualmente las capturas de sesiones SSH buscando diferencias
- Técnicas simples aplicadas
  - Cantidad de Bytes de la conexión
  - Banner del cliente SSH

# Cantidad de Bytes

- Una característica prometedora
- Bytes de la sesión SSH completa
- Compara la cantidad de Bytes con un umbral límite
  - Si lo supera es una sesión Interactiva
  - Si no, es una sesión no Interactiva

# Banner del cliente

- Las herramientas automáticas usan normalmente un string fijo
  - “libssh” o “-MEDUSA-”
  - Medusa lo permite cambiar
- Esta técnica es rápida para filtrar conexiones automáticas
- Igualmente siempre se aplica la técnica de cantidad de Bytes

# Desarrollo

- Primer problema grupal
  - No había disposición a desarrollar!
- Se mejoró un pre-desarrollo del Si6
- Dos integrantes se alejaron del grupo debido a motivos personales

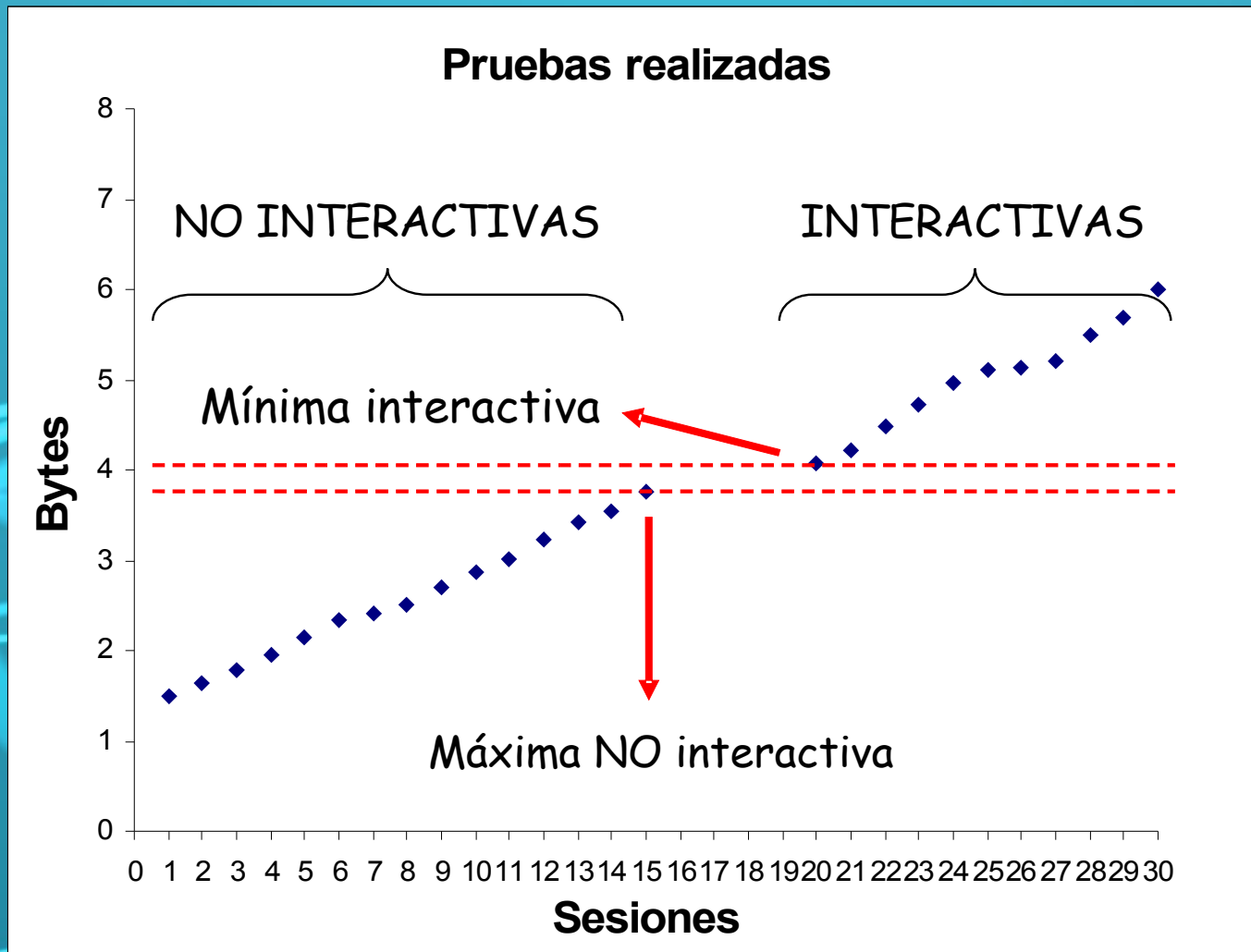
# Testing del software

- Verificación de técnicas de resolución
- Corrección de la herramienta
- Reuniones presenciales en el laboratorio
- Pruebas en simultáneo
- ¿Qué situaciones probar?

# Metodología de testing

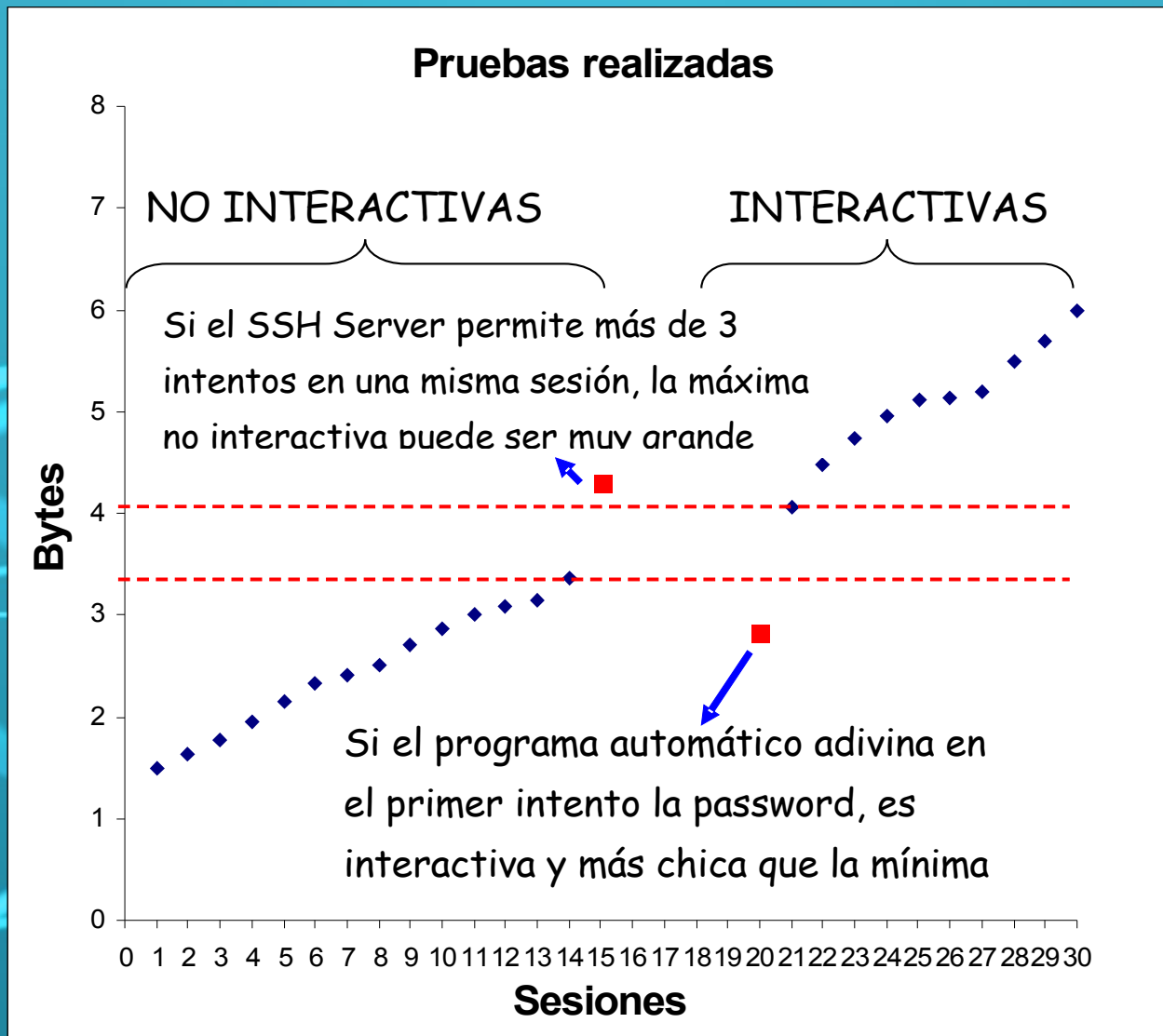
- Organización con Google Docs compartidos
- Tcpdumps con filtros para trabajar simultáneamente
- Estándar de nombres de archivos en las pruebas
- Análisis de cada captura
- Resultados en una planilla

# Búsqueda del umbral



**Umbral: 3970 Bytes**

# Problemas técnicos



# Problemas técnicos

→ 1er problema

→ El SSH server permite sólo tres intentos por omisión

→ 2do problema

→ Medusa explícitamente no completa el acceso. Sólo prueba el password. No es interactiva

# ssh-sniffer.py

- Análisis Offline y captura de la red
- Filtros pcap de paquetes
- Modo debug
- Identificación de sesiones por elección de técnicas
- Cambio del umbral a mano
- Agragado de strings nuevos para herramientas automáticas

# Ejemplo

```
ssh-sniffer.py -i 2007-06-06_SG_4.tcpdump -t all
```

```
192.168.1.179:1055      SSH-2.0-PuTTY_Release_0.60    ->  
192.168.1.248:22      SSH-1.99-OpenSSH_4.4
```

```
(Bytes: 169913, Id:1)
```

```
(1 total SSH conections, 1 interactive)
```

# Conclusiones

- Se solucionó el problema técnico
- Aprendizaje y experiencia en investigación
- Base para introducirse en temas más complejos
- Crecimiento grupal y superación
- Es posible generar grupos universitarios de investigación

# Mejoras futuras

- Performance
- No analiza el protocolo SSH
- Portabilidad no probada
- ¿Es posible distinguir humanos de automáticos?
- No funciona bien en capturas on-line

# Agradecimientos

- A todos los compañeros de investigación que participaron en el grupo
  - Federico Basualdo
  - Verónica Nisenbaum
  - Sebastián Montini
  - Sebastián de la Fuente
- Universidad FASTA
  - Decano Roberto Giordano Lerena
  - Lic. Sandra Cirimelo
- CITEFA y CafeLug

# Preguntas



**Algunos derechos reservados:**

**<http://creativecommons.org/licenses/by-nc-sa/2.5/ar/>**

