Demostración práctica de resolución de un incidente de seguridad

SANS Institute

AGENDA

- Quién soy
- Objetivo de la ponencia
- Caso práctico
- Fases incident handling
- Preguntas

QUIEN SOY

- **Rafael Alfaro March**
-  Equipo hacking ético ASC Madrid.
- Profesor nivel Mentor del SANS Institute
- GCIH, GPEN, GAWN, GCIA, GCFE, GCFA, GWAPT
- Contacto: ralfaro.march@gmail.com
- Twitter: rafaelalfar0

TEORÍA Y PRÁCTICA

- En teoría, teoría y práctica son iguales
- En la práctica, esto no tiene porqué ser así
- No tiene porque salir como se espera :)
- Por ejemplo, para hacer un mortal hacia atrás
- Efectuar una serie de pasos

TEORÍA Y PRÁCTICA

OBJETIVO

- Mostrar metodología y herramientas empleadas. Desde la técnica base.
- Del modo más ameno y divertido posible.
- Ejercicio colaborativo para resolver el problema planteado entre todos.
- Os pido atención y colaboración. La vergüenza la habéis dejado fuera, ¿o no?

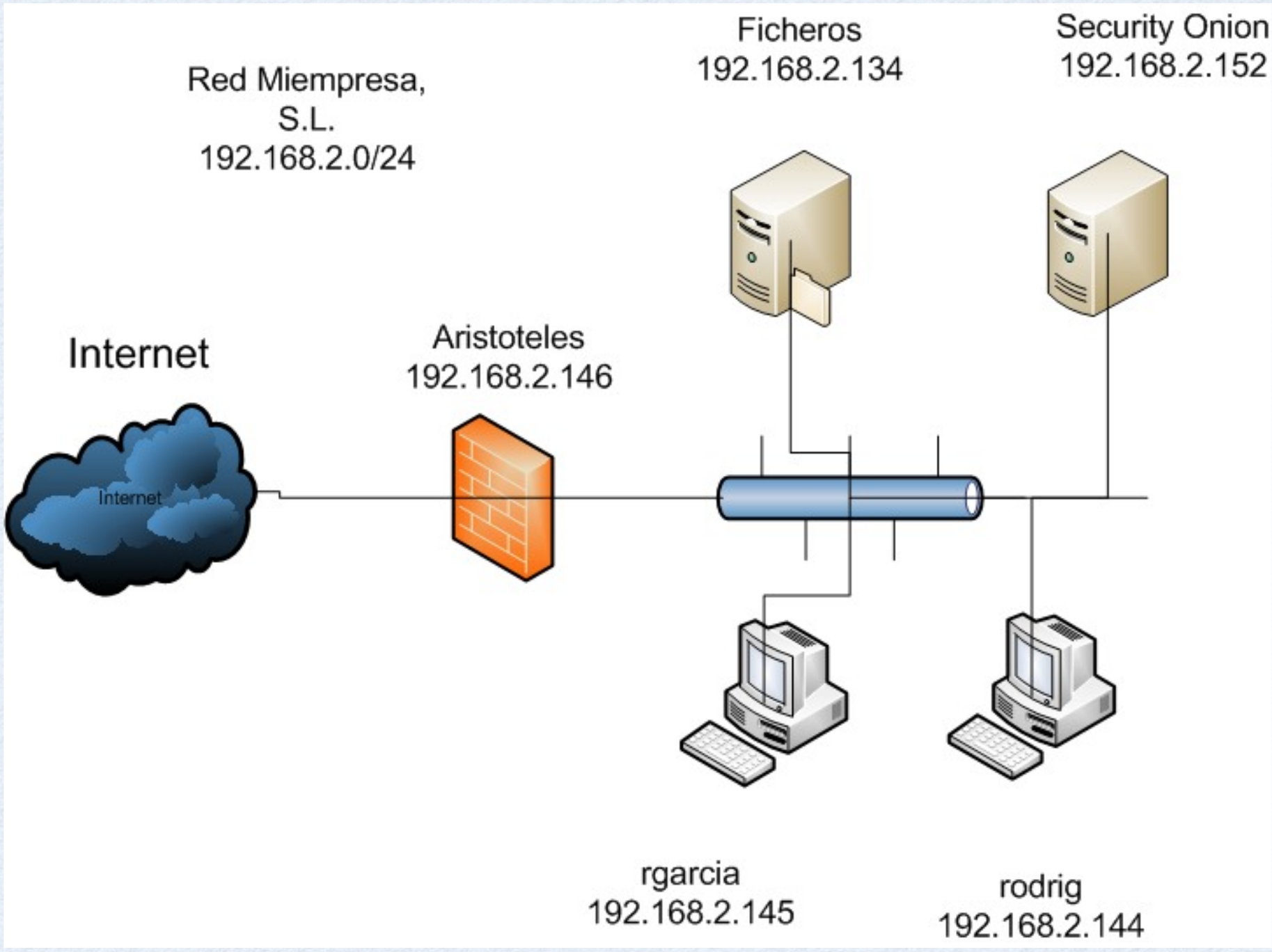
CASO PRÁCTICO

- Empresa asesoría fiscal y jurídica: Miempresa, S.L.
- Sin presencia en Internet
- Un contacto les informa de que se han filtrado informes suyos a través de pastebin

CASO PRÀCTICO

- **Antecedentes:**
- Hace 3 semanas fue despedido uno de los miembros de IT de la empresa
- Ayer contactaron con nuestra empresa, porque la información filtrada son informes confidenciales.

RED ORGANIZACIÓN



RED ORGANIZACIÓN

- Hablar de la política de red, proxy y filtrado de contenidos del mismo.

FASES

- ~~Preparación~~
- ~~Identificación~~
- Contención
- Erradicación
- Recuperación
- Lecciones aprendidas

CONTENCIÓN

Contención solución

- Captura de memoria y disco duro
- Aislar máquina
- Análisis logs
- Estudiar conexiones, usuarios, tareas programadas, programas instalados
- Pasar antivirus en las máquinas

ERRADICACIÓN

ERRADICACIÓN
SOLUCIÓN

- Eliminar backdoor
- Cambio reglas firewall: política denegar por defecto
- Cursar petición a pastebin para eliminar documentos
- Eliminar usuarios creados
- Analizar con antivirus

RECUPERACIÓN

RECUPERACIÓN SOL

- Volver a conectar a la red el servidor de ficheros
- Vuelta al trabajo

LECCIONES APRENDIDAS

LECCIONES APRENDIDAS

- ¿Prepara qué?
- ¿Identifica qué?
- Cambiar la política navegación web
- Cambiar filtrado firewall
- Cambiar política de contraseñas
- Instalar AV en servidores

¿PREGUNTAS?

GRACIAS POR VENIR

- **Referencias**

- Varias cheat sheets disponibles: en http://pen-testing.sans.org/resources/downloads

- Curso SEC 504: https://www.sans.org/course/hacker-techniques-exploits-incident-handling

REFERENCIAS

- Cheat sheets Windows y Linux disponibles en:
- http://pen-testing.sans.org/resources/downloads

- Curso SEC 504:
- https://www.sans.org/course/hacker-techniques-exploits-incident-handling
-