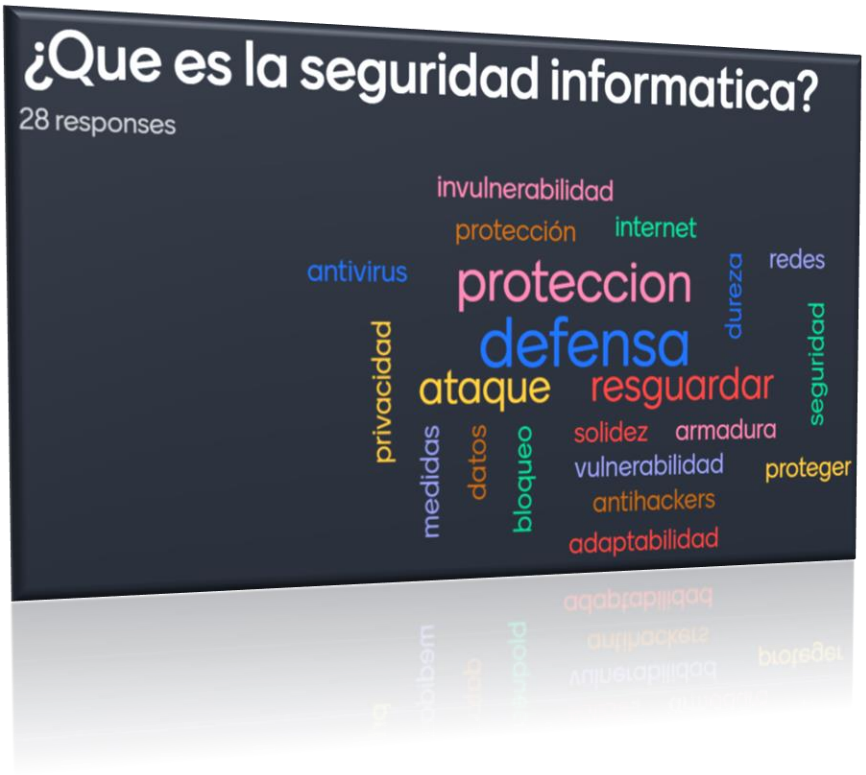
Universidad Paraguayo Alemana

UNIVERSIDAD PARAGUAYO ALEMANA
HEIDELBERG - ASUNCIÓN



Seguridad TICs

Prof.: Chrystian Ruiz Diaz

Contenido

Nota de Uso Académico 3
Ejercicio 1 - La Estafa: obtención de Documentos Confidenciales (50%) 4
John the Ripper 5
¿Qué es John the Ripper? 5
Funcionalidades principales 5
Modos de ataque 5
Uso de John the Ripper 6
Reiniciar el proceso de descifrado 6
Ejercicio 2 - La Entidad Financiera Vulnerable (50%) 7

Nota de Uso Académico

Este documento ha sido preparado exclusivamente para el uso académico del docente. Este documento no puede ser distribuido a ninguna otra parte ni utilizado para ningún otro propósito, diferente al establecido como alcance en el proyecto académico de la **UNIVERSIDAD PARAGUAYO ALEMANA**. El uso indebido del material fuera del ámbito académico no representa ninguna responsabilidad del docente.

Ejercicio 1 - La Estafa: obtención de Documentos Confidenciales (50%)

Introducción

Era un día común en el Departamento de Seguridad Informática cuando un equipo de investigadores forenses recibió una llamada urgente. Una empresa había sido víctima de una estafa, y se sospechaba que un atacante había transferido archivos confidenciales a través de su red. Durante la incautación del equipo del atacante, se capturó todo el tráfico de red en un archivo denominado `capture.pcapng`. La tarea del equipo de seguridad era analizar esta captura, identificar un archivo específico que contenía un hash MD5 crucial, y descifrar dicho hash para recuperar una contraseña que permitiera el acceso a documentos vitales del caso.

Análisis de la Captura de Tráfico de Red

El equipo comenzó cargando la captura de tráfico en Wireshark, una herramienta esencial para el análisis de red. Con la captura abierta, aplicaron filtros para centrarse en las transferencias de archivos, utilizando protocolos comunes como FTP y HTTP.

Con los filtros aplicados, comenzaron a revisar cada transferencia de archivo en busca de patrones que coincidieran con un hash MD5, una cadena de 32 caracteres hexadecimales.

Localización del Archivo con el Hash MD5

Entre las transferencias de archivos, encontraron un archivo que parecía contener información encriptada. Analizando los datos, identificaron un hash MD5 incrustado dentro del archivo. Este hash era la clave para acceder a la información confidencial.

Desencriptar el Hash MD5

Con el hash MD5 en su poder, el equipo se preparó para descifrarlo. Sabían que la herramienta adecuada para esta tarea era John the Ripper, una poderosa utilidad de recuperación de contraseñas. Primero, buscaron un archivo que podría tener el hash.

Luego, utilizando un diccionario "*`dictionary.txt`*", ejecutaron John the Ripper para intentar descifrar el hash.

```
john --wordlist=dictionary.txt --format=raw-md5 ejemplo.ext
```

John the Ripper comenzó a trabajar, probando cada palabra del diccionario contra el hash. En pocos minutos, reveló la contraseña...

Los archivos *`dictionary.txt`* y `capture.pcapng` pueden descargar del aula virtual y guardar en el mismo directorio del Kali donde abre una terminal. Con estos datos analizar y responder a la siguiente pregunta, documentar con captura de pantalla el hash localizado

¿Cuál es la contraseña texto legible original?

John the Ripper

John the Ripper es una herramienta de software libre y de código abierto utilizada principalmente para descifrar contraseñas. Es popular entre los profesionales de la seguridad y los administradores de sistemas debido a su capacidad para auditar la seguridad de las contraseñas. Aquí te dejo una descripción detallada de lo que es y cómo funciona:

¿Qué es John the Ripper?

John the Ripper, a menudo abreviado como "John", es una herramienta de auditoría de contraseñas diseñada inicialmente para sistemas Unix. Con el tiempo, se ha ampliado para incluir soporte para varios tipos de hashes de contraseñas y sistemas operativos. Es conocido por su eficiencia y flexibilidad, ya que puede trabajar con diferentes métodos de ataque y tiene soporte para una amplia variedad de algoritmos de hashing.

Funcionalidades principales

1. **Descifrado de contraseñas**: John puede intentar descifrar contraseñas utilizando diferentes métodos, como ataques de diccionario y ataques de fuerza bruta.
2. **Soporte para múltiples algoritmos de hash**: John soporta muchos formatos de hash, incluyendo pero no limitado a MD5, SHA-1, SHA-256, NTLM, bcrypt, y muchos más.
3. **Capacidad de personalización**: Los usuarios pueden personalizar los ataques utilizando reglas de transformación de diccionarios, máscaras y otras configuraciones avanzadas.
4. **Portabilidad**: Está disponible para múltiples plataformas, incluyendo Linux, Windows y macOS.

Modos de ataque

John the Ripper ofrece varios modos de ataque para descifrar contraseñas:

- **Modo de diccionario**: Utiliza un archivo de diccionario que contiene una lista de posibles contraseñas. John probará cada palabra del diccionario contra el hash de la contraseña.
- **Modo de fuerza bruta**: Intenta todas las combinaciones posibles de caracteres hasta encontrar la contraseña correcta. Este método es exhaustivo, pero puede ser lento.
- **Modo incremental**: Combina los modos de diccionario y fuerza bruta, aplicando transformaciones a las palabras del diccionario para generar nuevas combinaciones.

Uso de John the Ripper

Desencriptar el hash usando John the Ripper

```
john --wordlist=dictionary.txt --format=raw-md5 <ejemploNombreArchivo.ext>
```

- `--wordlist=dictionary.txt`: Especifica el archivo de diccionario que contiene las posibles contraseñas.
- `--format=raw-md5`: Especifica el formato del hash, en este caso, MD5.
- `ejemploNombreArchivo.ext=extension`: Archivo que contiene los hashes a descifrar (puede ser .txt, .html, etc, no usar los comodines “<>”).

Reiniciar el proceso de descifrado

Si deseas reiniciar el proceso de descifrado desde cero, puedes eliminar el archivo `john.pot` que almacena las contraseñas ya descifradas. Esto se encuentra generalmente en el directorio donde se ejecuta John the Ripper.

```
rm ~/.john/john.pot
```


Ejercicio 2 - La Entidad Financiera Vulnerable (50%)

Una entidad financiera de renombre decidió actualizar su plataforma de banca en línea para ofrecer mejores servicios a sus clientes. Contrataron a una empresa de software para implementar un sistema robusto que incluyera una interfaz moderna y funcionalidades avanzadas. El sistema, accesible a través de http://altoro.testfire.net/, prometía eficiencia y seguridad. Sin embargo, tras entrar en operación, comenzaron a experimentar varios incidentes de ciberseguridad que comprometían la integridad y confidencialidad de los datos financieros.

Alarmados por la situación, la entidad financiera decidió recurrir a la buena voluntad y la expertise de los estudiantes de Seguridad TICs. El objetivo era realizar pruebas de seguridad exhaustivas para identificar y mitigar las vulnerabilidades del sistema.

La Misión de los Estudiantes

Los alumnos, equipados con Kali Linux deberán abordar diferentes aspectos del análisis de seguridad y responder lo siguiente:

1 - Escaneo de Puertos y Servicios

2 - Obtención de Credenciales de Administración

3 - Explotación de Vulnerabilidades inyección SQL para login (Posibilidad de inyección SQL en los formularios de inicio de sesión y búsqueda**)**

4 – Dirección IP Pública del servidor en cuestión

