PRÁCTICA 5: Red Team

Lenguajes y Ciencias de la Computación.
ETSI Informática, Universidad de Málaga

EJERCICIO 1: Wireshark

El programa Wireshark (https://www.wireshark.org/), disponible en Kali Linux, es un capturador de paquetes de red y analizador de protocolos, el cual nos permite tanto adquirir aquellos paquetes de red que circulen por nuestros interfaces (Ethernet, red inalámbrica) como analizar el contenido de dichos paquetes.

A nivel de seguridad, esto nos permite acceder a la información intercambiada entre dos equipos, la cual – si no está protegida mediante protocolos como SSH, TLS, o IPsec – nos puede proporcionar información sensible tal y como contraseñas.

Para ciertos ejercicios, usaremos algunos módulos de la herramienta "metasploit" (https://www.metasploit.com/) para crear servidores de señuelo (para captura de credenciales) y analizar las tramas de red correspondientes a ellos.

USO BÁSICO DE WIRESHARK:
Para el ejercicio, hay que elegir el interfaz "loopback: lo".
Es posible filtrar los paquetes capturados indicando en protocolo en el campo de filtrado (indicado por el mensaje "Apply a display filter…")

EJERCICIO

1. *Ataque a HTTP*
   Creación del servidor: Creamos un servidor web utilizando el siguiente comando en la terminal: `python3 -m http.server`
   Objetivo: Capturar las peticiones del navegador
   Ejecución: Conectarse al servidor mediante un navegador web, y capturar la petición web y la respuesta del servidor usando Wireshark.
   Entrega: Adjuntar capturas de pantalla de la petición web y la respuesta del servidor.
2. *Ataque a FTP ("File Transfer Protocol")*
   Creación del "servidor": Creamos un servidor de señuelo FTP lanzando la consola de metasploit, y usando los comandos:
   a. `use auxiliary/server/capture/ftp`[1]
   b. `set srvhost 127.0.0.1`
   c. `set banner Servidor FTP de` [Poner aquí vuestro nombre y Apellidos]
   d. `exploit`[2]
   Objetivo: Capturar la contraseña del usuario
   Ejecución: Conectarse al servidor usando el comando `ftp`, y capturar el usuario y contraseña enviados usando Wireshark (**IMPORTANTE: Usad una contraseña falsa y no una de vuestras contraseñas**)
   Entrega: Adjuntar capturas de pantalla de las tramas donde se indica el nombre de usuario y contraseña.

[1] Indica a metasploit que queremos usar un módulo de ataque específico. Si queremos dejar de usar este módulo, hay que utilizar el comando `back`.
[2] Para parar este servidor (y otros similares), dentro de la consola de metasploit, llamamos al comando `jobs -l`, y posteriormente a `kill <numero de servidor>`.

3. *Ataque a TELNET*

   Creación del "servidor": Creamos un servidor de señuelo TELNET lanzando la consola de metasploit, y usando los comandos:

   a. `use auxiliary/server/capture/telnet`
   b. `set srvhost 127.0.0.1`
   c. `set banner Servidor TELNET de` [Poner aquí vuestro nombre y Apellidos]
   d. `exploit`

   Objetivo: Capturar la contraseña del usuario

   Ejecución: Conectarse al servidor usando el comando `telnet`, y capturar el usuario y contraseña enviados usando Wireshark (**IMPORTANTE: Usad una contraseña falsa y no una de vuestras contraseñas**)

   Entrega: Adjuntar capturas de pantalla de las tramas donde se indica el nombre de usuario y contraseña.

EJERCICIO 2: NMAP

IMPORTANTE: AUNQUE NO ESTÁ TIPIFICADO COMO DELITO, EL USO DE ESCANEO DE PUERTOS SE CONSIDERA COMO UN CIBERINCIDENTE SEGÚN EL REAL DECRETO 43/2021, Y SU USO SOBRE SERVIDORES QUE NO HAYAN AUTORIZADO PREVIAMENTE SU ANÁLISIS PUEDE PROVOCAR NO SÓLO EL "BANEO" EN EL ACCESO A UNA DICHO SERVIDOR (P.EJ. UNIVERSIDAD DE MÁLAGA), SINO TAMBIÉN EL CIERRE DEL SERVICIO DE VUESTRO PROVEEDOR DE INTERNET

LA EJECUCIÓN DE NMAP SOBRE OTRO SERVIDOR QUE NO SEA LA MÁQUINA VIRTUAL (127.0.0.1) SERÁ CONSIDERADA COMO UN CIBERINCIDENTE Y CONLLEVARÁ, COMO MÍNIMO, LA SUSPENSIÓN DE TODA LA PARTE PRÁCTICA

El programa nmap (https://nmap.org/) nos permite analizar los servicios de red activos de un equipo, en base a una técnica conocida como rastreo (o escaneo) de puertos – donde el programa realiza una conexión a todos los puertos de un equipo. Este programa se utiliza en las fases de "escaneo activo" y "recopilación de información" dentro de las tácticas de reconocimiento (Ver estudio de INCIBE en URL).

USO BÁSICO DE NMAP:
Ejecución de nmap

```
sudo nmap -v -A -O 127.0.0.1
```

- `sudo nmap`: Nombre de la herramienta, con permisos de administrador.
- `-v`: "Verbose": Muestra información adicional.
- `-A`: Activa la detección de la versión de los servicios, entre otros.
- `-O`: Activa la detección del Sistema Operativo, entre otros.
- `127.0.0.1`: Host que vamos a analizar.

EJERCICIO
Objetivo: Analizar Kali Linux, con diversos servicios activados.
Preliminares: Lanzar la consola metasploit (ver ejercicio 1), y lanzar *únicamente* el servidor de señuelo FTP.
Ejecución: lanzar el comando nmap sobre localhost (127.0.0.1), activando la detección de sistema operativo.
Entrega: Indicar los servicios activos en la máquina, así como los detalles del sistema operativo detectados por nmap.
NOTA: la ejecución del comando puede tardar un par de minutos, dado que intenta obtener información sobre un servicio falso.

EJERCICIO 3: John the Ripper

Como hemos mencionado en clase, las contraseñas deben almacenarse con una sal y siguiendo unas directrices específicas. Si estas directrices no se siguen, y una contraseña se almacena en el sistema utilizando una función hash (MD5, SHA1, SHA256…) es posible utilizar herramientas de recuperación de contraseñas para analizar dichos hashes y extraer las contraseñas asociadas.

Existen diversos tipos de herramientas de recuperación de contraseñas:

- **Ataque de fuerza bruta** (John the ripper): Prueba diferentes combinaciones de letras, números y símbolos). Es poco práctico.
- **Diccionario** (John the ripper): Usa ficheros que contienen contraseñas predefinidas / robadas ("diccionarios"). Es útil debido a la reutilización de contraseñas.
    - Mejorado con reglas: Añade reglas que expanden las contraseñas del diccionario (por ejemplo, sustituir las "a" por "4")
    - Mejorado con Spidering: Añade información del usuario extraída de la web u otras fuentes (por ejemplo, fecha de nacimiento).
- **Tablas Rainbow** (Ophcrack): Utiliza compilaciones de hashes de contraseñas robadas. Los ficheros resultantes son muy grandes (>100GB), pero es una estrategia extremadamente rápida para contraseñas sin sal.

Para esta práctica, utilizaremos la herramienta "John the Ripper" (https://www.openwall.com/john/), disponible en Kali Linux.

USO BÁSICO DE JOHN THE RIPPER:
En este enunciado sólo mostraremos el uso básico de John the Ripper en la terminal. Para una explicación del uso de John the Ripper, necesario para realizar este ejercicio, será necesario consultar estas páginas como referencia:

- Uso de John the Ripper: https://miloserdov.org/?p=5031
- Ejemplos de ejecución de John the Ripper: https://miloserdov.org/?p=5191
- Nuevas reglas en John the Ripper: https://miloserdov.org/?p=5477 (Sección "Examples of Rule-Based Attacks in John the Ripper")

Ejecución de John the Ripper:

```
john --wordlist=='dicc.txt' --format==formato --rules=reglas hash.txt
```

- `john`: Nombre del programa en la terminal
- `--wordlist=='dicc.txt'`: Indica el diccionario (`dicc.txt`) que usaremos en el análisis. Uno de los diccionarios más utilizados es rockyou – obtenidos de la red social rockyou (URL)
- `--format==formato`: Indica el formato del hash (p.ej. hash md5, hash formato office, etc).
- `--rules=reglas`: Indica las reglas que aplicaremos para mejorar el diccionario (Ver https://miloserdov.org/?p=5477). En Kali Linux, el fichero de configuración que debe cambiarse es `/etc/john/john.conf`

- `hash.txt`: Indica el fichero donde se guarda el hash que queremos analizar.

Notas sobre John the Ripper:

- Una vez encontrado un hash, este se guardará en el fichero `./.john/john.pot`.

EJERCICIO

Objetivo: Extraer las contraseñas de diversos hashes

Preliminares: Para poder usar el diccionario rockyou.txt (localizado en `/usr/share/wordlists`), es necesario antes descomprimirlo usando el comando `sudo gzip -d /usr/share/wordlists/rockyou.txt.gz`.

Ejecución: Los hashes a analizar son los siguientes:

a) **81dc9bdb52d04dc20036dbd8313ed055**

   Para adivinar esta contraseña, antes es necesario saber el formato que tiene. Para ello, podemos usar el comando `hash-identifier`, y luego buscar las salidas marcadas como "Possible hashes" (p.ej. md4) con la opción `--list=formats` y `grep` (p.ej. `john --list=formats | grep -i "md4"`)

   PISTA: El formato es un formato de subtipo RAW.

b) **a77eb3defefc90c462a8d7cf63b950c3a73e350a**

   Esta contraseña requiere de añadir una regla al fichero de reglas `/etc/john/john.conf`. En particular, la regla es `=0oo00` (sustituir la letra "o" en la primera posición de la contraseña por el número "0")

c) **6YmAFQjzlBmpUlNS1$ui9s3a7UO/eKK7BEhEeH9zc9VVKiG4QsLE45uJxjgPgagI7RJEAaUfnBwUC/tjTuOuOMTKJCy2GhBXhv7qUPa/**

   La ejecución de esta tarea tardará unos minutos. Se aconseja no utilizar ninguna regla adicional.

Entrega: Las contraseñas asociadas a dichos hashes.