**SEGURIDAD INFORMÁTICA**

**PRÁCTICA I (PARTE I)**

Los objetivos de esta práctica son los siguientes:

**I. DEMONIOS EN LINUX**

1. Estudiar los servicios (demonios) en Linux y el proceso de conexión cliente-servidor.
2. Instalar, arrancar y administrar dos tipos de demonios en Linux:
   1. Los demonios dependientes y gestionados por el súper demonio de red o súper servidor. Es este súper demonio el que escucha y arranca los demonios al llegar una petición al puerto correspondiente.
   2. Se elegirán en este caso los demonios ftpd y telnetd, que deberán arrancarse mediante el súper demonio de red Inetd.
   3. Los demonios *standalone*, llamados así porque funcionan de forma independiente del súper demonio de red.

Para ello instalaremos tres servicios: FTP/Telnet (ambos deberán arrancarse mediante el súper demonio de red Inetd) y SSH, (Open SSH)

**II. USO DEL WIRESHARK COMO SNIFFER**

1. Uso de un sniffer como el Wireshark para:
   1. Identificar los paquetes del Three-way handshake
   2. Identificar las características más importantes de los paquetes enviados: direcciones IP origen y destino, flags, número de secuencia y número ack (Leer artículo de la revista Hackxcrack “1-port\_scanning\_hxc.pdf”, pags. 59-61).
2. Capturar los paquetes con el nombre de usuario y contraseña en una sesión ftp y telnet (no cifrada) y en una sesión ssh y sftp (cifrada) para ver sus datos, en este caso los usuarios y contraseñas:
   1. En texto claro en telnet y en ftp
   2. Cifradas mediante claves pública y privada en SSH (ya explicaremos este método de cifrado en el curso más adelante)

**III. USO DE NMAP PARA ESCANEAR PUERTOS**

1. Aprender a usar nmap para escanear puertos
2. Entender los diferentes tipos de escaneo que hay y el uso de los distintos flags en los paquetes TCP/IP

**ACTIVIDADES**

**PARTE 1**

1. **Instalar un servidor telnet en Linux.**
   1. ¿Cómo funciona y cómo se instala?
      1. Lo lanza el súper demonio de red llamado **super demonio de red (inetd).**
      2. Este súper demonio se instala con la orden **sudo apt install openbsd-inetd**
      3. Después se instala el demonio servidor telnet con la orden **sudo apt install telnetd**
   2. Arrancar el servidor telnet (que en realidad es arrancar el súper demonio de red) con la orden **sudo /etc/init.d/openbsd-inetd start**
   3. ¿Cómo puedo saber si está arrancado o no?
      1. Mediante la orden systemctl **sudo systemctl status openbsd-inetd.service**
      2. Mirando los procesos que están ejecutándose en el sistema mediante la orden **INSERTAR ORDEN**
      3. Mediante nmap

**INSERTAR PANTALLAZO**

* + 1. Mediante cualquier otro método alternativo **telnet (ip del Kali) desde el cliente (Windows o mac)**
  1. ¿Qué puerto utiliza este servidor? **INSERTAR RESPUESTA**

1. **Instalar un cliente ftp en móvil, por ejemplo FTP manager en iOS o ProFTP en Android (también podríamos conectarnos mediante Filezilla en Windows, aunque en este caso hay que fijarse en que no use un método de cifrado).** 
   1. Otra opción más rápida pero menos amigable sería desde cualquier shell (en Windows, Mac o Linux) mediante la orden **INSERTAR ORDEN**
2. **Monitorización con un sniffer**
   1. Una vez que se ha logrado la conexión cliente-servidor, capturar mediante el wireshark los siguientes paquetes:
      1. Three-way handshake – Tres paquetes con los que se establece la conexión cliente-servidor - **INSERTAR PANTALLAZO CON LOS PAQUETES FILTRADOS**
      2. **INSERTAR PANTALLAZO** donde aparezcan los puertos del cliente y el servidor, junto con sus direcciones IP.
      3. USUARIO Y CONTRASEÑA - **INSERTAR PANTALLAZO EN LOS QUE SE VEAN LOS DOS PAQUETES**
      4. Capturar los paquetes con los que se cierra la conexión - **INSERTAR PANTALLAZO CON LOS PAQUETES FILTRADOS**

**NOTA: No serán válidas capturas que no estén bien filtradas de forma que se puedan encontrar de forma más o menos sencilla esos paquetes. Destacar esos paquetes con un trazo rojo ayuda, pero eso no es un filtro de Wireshark.**

1. **Escaneo de los puertos mediante nmap**
   1. Hacer un escaneo **FULL SCAN** al servidor ftp mediante nmap
   2. Identificar mediante wireshark y los filtros necesarios los paquetes mandados en ese escaneo a ese puerto en concreto. Para ello, debe aparecer:
      1. Un escaneo filtrado con éxito (a un puerto abierto)

**INSERTAR PANTALLAZO**

* + 1. Un escaneo filtrado a un puerto cerrado

**INSERTAR PANTALLAZO**

**NOTA: El resultado de estos pantallazos deben reflejar las diapositivas que hay en la teoría donde se explica este tipo de escaneo.**

**PARTE 2**

1. **Repetir los pasos 3 al 4 para el servidor telnet y conectarse al servidor telnet desde el móvil (mediante la app Termius, en iOS y Android). También nos podríamos conectar desde el CMD de Windows.**

**NOTA: La única diferencia es que hay que hacer un escaneo HALF SCAN para el servidor telnet y ver los paquetes (en especial los flags que están activados) que se mandan en este caso.**

**PARTE 3**

1. **Realizar el paso 3 (captura del Three-way handsake, fin de conexión y usuario y contraseña) para el servidor Open SSH, con sus correspondientes pantallazos.**
2. Contesta a las siguientes preguntas:
   1. Explica en pocas líneas qué es el servicio SSH y para qué sirve **INSERTAR RESPUESTA**
   2. ¿Qué puerto utiliza el servidor? ¿Qué puerto has utilizado tú como cliente? **INSERTAR RESPUESTA**
   3. ¿Cómo es su autenticación y cómo viajan los datos que se intercambian entre el cliente y el servidor? Explica en unas pocas líneas y con tus palabras qué método utilizamos para autenticarnos y qué algoritmo de cifrado de utiliza para ello. **INSERTAR RESPUESTA**
   4. **¿Has podido ver la contraseña en Wireshark? ¿Qué paquetes son los que definen la autenticación? Señálalos en tu captura. INSERTAR PANTALLAZO**
   5. ¿Hay un servicio análogo para el servicio ftp basado en SSH? **INSERTAR RESPUESTA**

**IMPORTANTE: Si se detecta que este último punto está copiado la práctica será calificada con un 0. Tenéis que leerlo, entenderlo y explicarlo con vuestras palabras.**

**INSTRUCCIONES**

* Entrega:
  + **Un archivo PDF** a partir de este documento de Word modificado con las respuestas escritas (las que están señaladas en rojo) y los pantallazos pedidos.
* Los ejercicios **SÓLO** podrán realizarse en grupos de dos alumnos como máximo. Si hay un grupo de tres se debe escribir un correo al profesor para notificárselo. **No se permiten entregas de prácticas por grupos de tres o más alumnos que no hayan sido notificadas en fecha al profesor.**
* El nombre del fichero entregado serán los apellidos de los alumnos separados por guion.
* Se deberán usar al menos dos equipos diferentes (cliente y servidor) o realizarlo mediante máquinas virtuales.
* **La fecha límite de entrega será el miércoles 11 de octubre a las 23 horas.**
* No se recogerán memorias entregadas fuera de fecha o por otro medio distinto de los indicados (como por ejemplo el mail). Debe entregarse en el apartado correspondiente en el campus virtual.