Introducción

Para comenzar buscamos información en internet sobre herramientas de análisis de redes. Al leer información nos damos cuenta que ya que no poseemos un nivel muy alto en este área de análisis podemos llegar a la conclusión que lo mas fácil es manejar herramientas gráficas ya que son mas intuitivas que las que las empleamos por consola.

Algunos conceptos básicos que debemos saber antes de comenzar son:

- **¿Que es un puerto?**:
  Un puerto es una zona en la que dos ordenadores (hosts) intercambian información.
- **¿Que es un servicio?**:
  Un servicio es el tipo de información que se intercambia con una utilidad determinada como ssh o telnet.
- **¿Que es un Firewall?**:
  Un firewall acepta o no el trafico entrante o saliente de un ordenador.
- **¿Que son paquetes SYN?**:
  Así por encima, pueden ser paquetes que abren un intento de establecer una conexión TCP.

Dado que como ya hemos dicho antes, nuestro nivel de análisis de redes no es muy alto, nos centraremos en dos herramientas básicas pero muy útiles, Ettercap y Nmap. Operaremos con ellas a un nivel básico para conocer estas herramientas y familiarizarnos con este tipo de herramientas y sus conceptos.

Ettercap

Ettercap es un sniffer para LANs . Soporta direcciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También hace posible la inyección de datos en una conexión establecida y filtrado al vuelo aun manteniendo la conexión sincronizada gracias a su poder para establecer un Ataque Man-in-the-middle (es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas).

Como usar Ettercap.

- 1.Para comenzar a utilizarlo debemos descargarlo, para ello abrimos terminal y escribimos:

```
sudo apt-get install ettercap-gtk
```

- 2.Una vez descargado ejecutamos el programa como root:

```
sudo ettercap -G
```

- 3.Para comenzar nos iremos a la pestaña **Sniff→Unified Sniffing**, donde seleccionaremos la interfaz que esta conectada a la red que queremos sniffar. Si no supiéramos cual es tenemos dos opciones, la profesional: Abrir terminal y escribir “route” o “ifconfig” y ver a cual estamos conectados; y la no profesional o tanteo: Ir probando hasta ver cual es.

- 4.A continuación seleccionamos la pestaña **Host→Scan for hosts**, para escanear los hosts que después seleccionaremos en la pestaña **Host→Host list** y se nos abrirá una lista de las **ips conectadas** y también la **ip del router** al que estamos conectados.
- 5.Seleccionamos en la lista la ip del ordenador que queremos analizar y pulsamos **Add to Target1** y después seleccionamos el router y marcamos **Add to Target2**
- 6.Nos dirigimos a la pestaña **Mitm→ARP Poisoning**. Ahora marcamos la pestaña **Sniff remote connections** y pulsamosa aceptar.
- 7.Y una vez hecho esto ya podemos comenzar a sniffar, para ello vamos a la pestaña **Start→Start sniffing**.
- 8.Y finalmente estaremos sniffando la información del ordenador deseado y para poder ver sus conexiones, loggins, etc vamos a la pestaña **View→Connections** y en la lista haciendo doble click podremos ver esas conexiones.

Zenmap

Zenmap es una aplicación gráfica para Nmap: un escáner de puertos que nos puede dar mucha información acerca de una máquina. Además de averiguar el estado de los puertos, podemos saber el servicio que se está corriendo en ese puerto y a veces hasta el sistema operativo que utiliza. Es una herramienta útil cuando no sabes si tienes algún programa que utilice los puertos o para saber qué puertos utiliza cada programa.

- 1.Para comenzar a usar esta herramienta la instalaremos escribiendo los siguientes comandos en el terminal:

```
sudo apt-get update
sudo apt-get install zenmap
```

- 2.Una vez instalada, la abrimos escribiendo lo siguiente en el terminal:

```
sudo zenmap
```

- 3.A continuación lo primero es seleccionar la ip del equipo que queremos analizar, para ello ponemos la dirección en target o si queremos sondear un rango ponemos dicho rango, Ejemplo: 192.168.0.0-230.
- 4.Después seleccionamos el tipo de escaneo que queremos realizar, por ejemplo: intense scan, quick scan... y pulsamos el boton Scan.
- 5.Dejamos que el programa recopile la información, y ya tendremos la informacion de los equipos deseados, como los puertos, el mapa de la red, el sistema operativo...

<color #bfbfc3>Publicado por Rodrigo Díaz y Carlos Herrero.</color>