Talleres del Módulo Footprinting

SCANING

TALLERES COMPLEMENTARIOS DE APLICADOS DE HERRAMIENTAS Y REFUERZO DE CONCEPTOS.

TALLER 1. ANGRY IP

Instale un Aplicativo ANGRYIP, Escanee la red local de sus máquinas instaladas en su escenario.

Instale la herramienta, y ejecute Angryip

Escriba la dirección IP del Objetivo representado en el SCOPE Ejemplo 192.168.10.1 a 192.168.10.20

De click en el botón START para iniciar el proceso de scaneo.

Documente lo encontrado de las direcciones vivas y muertas. E investigue otras evidencias

TALLER 2. USO DE NMAP

1. Instale la aplicación NMAP para Windows de sus tools o abra Backtrack para el lab
2. En la línea de comandos nmap digite : nmap –v A www.nombredelobjetivo.com
3. Documente todo lo encontrado
4. Luego digite los comandos referentes a los tipos de scaning estudiados en el curso y documente lo encontrado en cada ejercicio. La idea es que ejecute lo referente al scan TCP, SYN, FIN, XMAS, etc.

TALLER 3. USO DE NETSCANTOOLS PRO

1. Instale la herramienta NETSCANTOOLSPRO.exe y ejecútela en su máquina virtual
2. Escoja la herramienta PORTSCANER escanee la red local de sus equipos del escenario.
3. Documente lo encontrado y saque información adicional de la red escaneada.
4. Pruebe con otras opciones de la herramienta.

TALLER 4. USO DE SUPERSCAN 4

Instale la herramienta Superscan4.exe

En las opciones de hostname IP coloque el rango de red de su red local a escanear o la ip de un solo equipo

Realice la prueba de las dos formas y documente lo encontrado tratando de evidenciar ips, nombres de equipos, segmento de red, servicios y puertos habilitados entre otros datos posibles.