INTELIGENCIA ACTIVA

UNIVERSIDAD AUTONOMA DE CHIAPAS
LIDTS
ANÁLISIS DE VULNERABILIDADES
DOCENTE: DR. LUIS GUTIERREZ ALFARO
JAZMÍN MIJANGOS LÓPEZ
7° N MATRICULA: A200179

ANÁLISIS DE DISPOSITIVOS Y PUERTOS CON NMAP

NMAP ES LA MEJOR HERRAMIENTA DE ESCANEO DE PUERTOS Y DESCUBRIMIENTO DE HOSTS QUE EXISTE ACTUALMENTE. NMAP NOS PERMITIRÁ OBTENER UNA GRAN CANTIDAD DE INFORMACIÓN SOBRE LOS EQUIPOS DE NUESTRA RED, ES CAPAZ DE ESCANEAR QUÉ HOSTS ESTÁN LEVANTADOS, E INCLUSO COMPROBAR SI TIENEN ALGÚN PUERTO ABIERTO, SI ESTÁN FILTRANDO LOS PUERTOS (TIENEN UN FIREWALL ACTIVADO), E INCLUSO SABER QUÉ SISTEMA OPERATIVO ESTÁ UTILIZANDO UN DETERMINADO OBJETIVO.

PARAMETROS OPCIONES DE ESCANEO DE NMAP

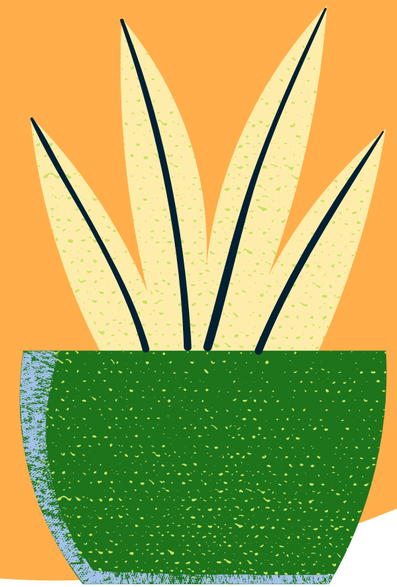
- SELECCIONAR OBJETIVOS: DIRECCIONES O RANGOS IP, NOMBRES DE SISTEMAS, REDES, ETC.
- DESCUBRIR SISTEMAS.
- TÉCNICAS DE ANÁLISIS DE PUERTOS.
- PUERTOS A ANALIZAR Y ORDEN DE ANÁLISIS.
- DURACIÓN Y EJECUCIÓN:
- DETECCIÓN DE SERVICIOS Y VERSIONES.
- EVASIÓN DE FIREWALLS/IDS.
- PARÁMETROS DE NUEL DE DETALLE Y DEPURACIÓN
- OPCIONES INTERACTIVAS
- SCRIPTS
- FORMATOS DE SALIDA

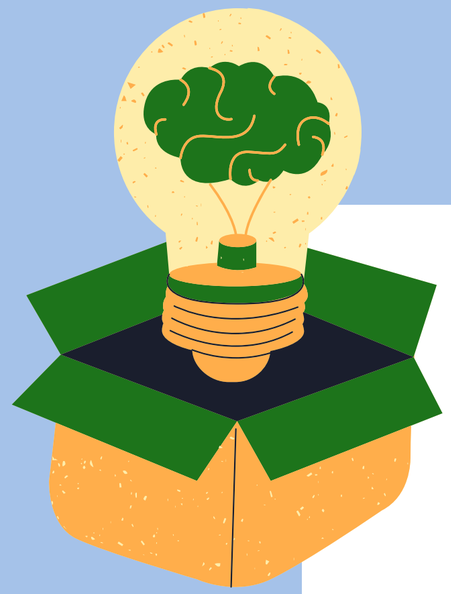
FULL TCP SCAN

ES UNA TÉCNICA DE EXPLORACIÓN DE PUERTOS QUE CONSISTE EN ENVIAR UN PAQUETE FIN A UN PUERTO DETERMINADO, CON LO CUAL DEBERÍAMOS RECIBIR UN PAQUETE DE RESET (RST) SI DICHO PUERTO ESTA CERRADO. ESTA TÉCNICA SE APLICA PRINCIPALMENTE SOBRE IMPLEMENTACIONES DE PILAS TCP/IP DE SISTEMAS UNIX.

STELTH SCAN

LOS TIPOS DE STEALTH SCAN SE REFIERE A AQUELLOS EN LOS QUE LOS PAQUETES DESIGNADOS PROVOCAN QUE EL SISTEMA OBJETIVO RESPONDA SIN TENER UNA CONEXIÓN COMPLETAMENTE ESTABLECIDA. LOS HACKERS UTILIZAN EL STEALTH SCAN O "ESCANEO SIGILOSO" PARA PODER ELUDIR EL SISTEMA DE DETECCIÓN DE INTRUSIONES (IDS), LO QUE LO CONVIERTE EN UNA AMENAZA MUY A TOMAR EN CUENTA.





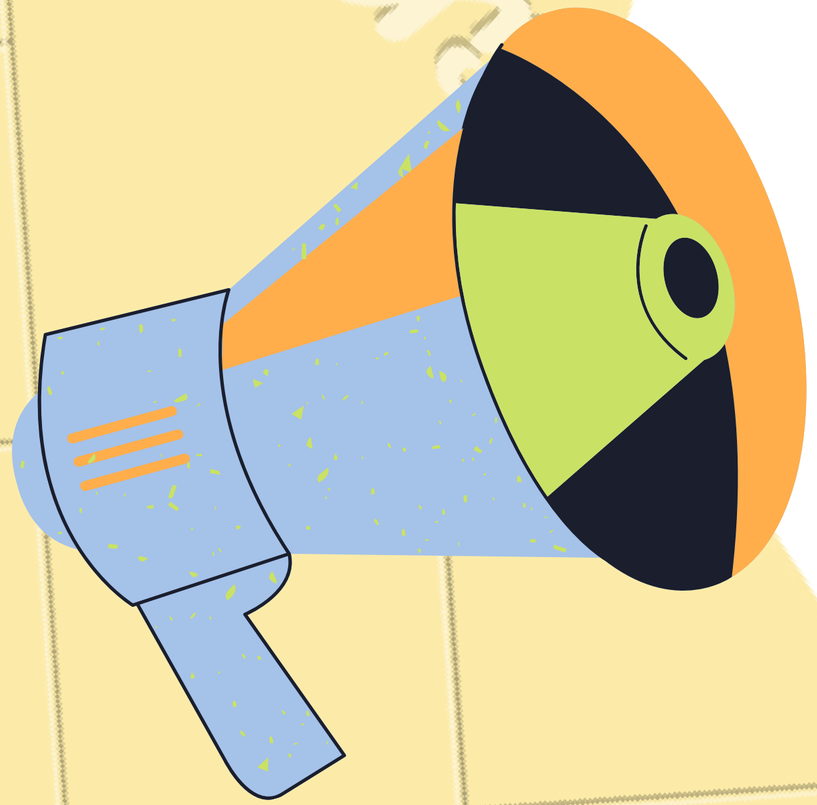
FINGERPRINTIG

EL FINGERPRINTING O LA HUELLA DIGITAL ES TODA AQUELLA INFORMACIÓN SISTEMÁTICA QUE DEJAMOS SOBRE UN DISPOSITIVO INFORMÁTICO CADA VEZ QUE LO UTILIZAMOS.
LOS DATOS OBTENIDOS PERMITEN DETERMINAR DE MANERA INEQUÍVOCA EL DISPOSITIVO EMPLEADO Y, DE ESTA FORMA, PODER LLEGAR A PERFILAR Y CONOCER LA ACTIVIDAD DEL USUARIO, YA SEA UNA PERSONA FÍSICA O JURÍDICA.

EXISTEN ALGUNAS TECNICAS DEL FINGERPRINTING:

-COOKIES: ES UNA TÉCNICA DE SEGUIMIENTO QUE CONSISTE EN FICHEROS QUE SE ENCUENTRAN EN EL DISPOSITIVO DEL USUARIO Y QUE SON CREADOS POR LA WEB DE UN PROVEEDOR DE SERVICIOS.
-SNIFFING: ES UNA TÉCNICA QUE PERMITE ESCUCHAR TODO LO QUE OCURRE EN UNA DETERMINADA RED.

ZENMAP



ZENMAP SE DEFINE COMO LA INTERFAZ GRÁFICA DE USUARIO OFICIAL DE NMAP, QUE PERMITE USAR EL PROGRAMA DE MANERA PRÁCTICA, CÓMODA, CLARA Y MÁS ORGANIZADA. ESTA INTERFAZ ES IDEAL PARA EXPERTOS Y PRINCIPIANTES, AUNQUE TAMBIÉN DEPENDE DEL GUSTO Y HAY QUIENES PREFIEREN SU USO DIRECTAMENTE EN LA CONSOLA.

ANÁLISIS TRACEROUTE

EL COMANDO TRACERT SE EJECUTA EN LA CONSOLA DE SÍMBOLO DE SISTEMA EN LOS SISTEMAS OPERATIVOS WINDOWS. GRACIAS A ESTE COMANDO, PODREMOS SEGUIR LA PISTA A LOS PAQUETES QUE VIENEN DESDE UN HOST. CUANDO EJECUTAMOS EL COMANDO «TRACERT» OBTENEMOS UNA ESTADÍSTICA DE LA LATENCIA DE RED DE ESOS PAQUETES, LO QUE ES UNA ESTIMACIÓN DE LA DISTANCIA (EN SALTOS) A LA QUE ESTÁN LOS EXTREMOS DE LA COMUNICACIÓN.