UNIVERSIDAD AUTONOMA DE CHIAPAS

CONCEPTOS

DIEGO GONZALEZ CARPIO

MATERIA: ANALISIS DE VULNERABILIDADES

PROFESOR: GUTIÉRREZ ALFARO LUIS

HERRAMIENTAS DE VULNERABILIDADES

NMAP

DEFINICIÓN: NMAP (NETWORK MAPPER) ES UNA HERRAMIENTA DE CÓDIGO ABIERTO UTILIZADA PARA DESCUBRIR DISPOSITIVOS EN UNA RED Y MAPEAR LOS SERVICIOS QUE ESTÁN EJECUTÁNDOSE EN ESOS DISPOSITIVOS.

USO: SE EMPLEA PARA REALIZAR ESCANEOS DE PUERTOS, IDENTIFICAR SISTEMAS OPERATIVOS, DETECTAR VERSIONES DE SOFTWARE, Y REALIZAR AUDITORÍAS DE SEGURIDAD.

JOOMSCAN

DEFINICIÓN: JOOMSCAN ES UNA HERRAMIENTA ESPECIALIZADA DISEÑADA PARA BUSCAR Y DETECTAR VULNERABILIDADES EN SITIOS WEB QUE UTILIZAN EL SISTEMA DE GESTIÓN DE CONTENIDOS JOOMLA.

USO: REALIZA UN ESCANEO EN BUSCA DE VULNERABILIDADES ESPECÍFICAS DE JOOMLA, PROPORCIONANDO INFORMACIÓN VALIOSA PARA LA SEGURIDAD DE SITIOS WEB.

WPSCAN

DEFINICIÓN: WPSCAN ES UNA HERRAMIENTA DE SEGURIDAD UTILIZADA PARA EVALUAR LA VULNERABILIDAD DE SITIOS WEB QUE ESTÁN CONSTRUIDOS CON WORDPRESS.

USO: ESCANEA INSTALACIONES DE WORDPRESS EN BUSCA DE DEBILIDADES, IDENTIFICANDO PROBLEMAS EN TEMAS, PLUGINS Y CONFIGURACIONES.

NESSUS ESSENTIALS

DEFINICIÓN: NESSUS ES UNA HERRAMIENTA DE ESCANEO DE VULNERABILIDADES QUE BUSCA IDENTIFICAR POSIBLES DEBILIDADES EN SISTEMAS INFORMÁTICOS. NESSUS ESSENTIALS ES UNA VERSIÓN GRATUITA CON FUNCIONALIDADES LIMITADAS.

USO: ANALIZA HOSTS EN BUSCA DE VULNERABILIDADES CONOCIDAS Y PROPORCIONA INFORMES DETALLADOS PARA AYUDAR A FORTALECER LA SEGURIDAD.

VEGA

DEFINICIÓN: VEGA ES UNA HERRAMIENTA DE PRUEBA DE SEGURIDAD DE APLICACIONES WEB QUE SE UTILIZA PARA ESCANEAR Y ENCONTRAR VULNERABILIDADES EN APLICACIONES WEB.

USO: DETECTA Y EVALÚA POSIBLES RIESGOS DE SEGURIDAD EN APLICACIONES WEB, INCLUYENDO VULNERABILIDADES COMUNES COMO INYECCIONES SQL, CROSS-SITE SCRIPTING (XSS) Y MÁS.

INTELIGENCIA MISCELÁNEO.

GOBUSTER

DEFINICIÓN: GOBUSTER ES UNA HERRAMIENTA DE ENUMERACIÓN QUE REALIZA ATAQUES DE FUERZA BRUTA EN URLS PARA DESCUBRIR DIRECTORIOS Y ARCHIVOS OCULTOS EN SITIOS WEB.

USO: ES UTILIZADO PARA BUSCAR PUNTOS DE ENTRADA NO AUTORIZADOS O POSIBLES VULNERABILIDADES EN UNA APLICACIÓN WEB. PUEDE SER ÚTIL EN AUDITORÍAS DE SEGURIDAD.

DUMPSTER DIVING

DEFINICIÓN: DUMPSTER DIVING SE REFIERE A LA PRÁCTICA DE BUSCAR INFORMACIÓN VALIOSA EN LA BASURA FÍSICA O DIGITAL. EN EL CONTEXTO DE LA SEGURIDAD INFORMÁTICA, IMPLICA BUSCAR INFORMACIÓN EN DOCUMENTOS IMPRESOS, DISCOS DUROS DESCARTADOS, O CUALQUIER OTRO MEDIO QUE PUEDA CONTENER DATOS CONFIDENCIALES.

USO: LOS ATACANTES PUEDEN BUSCAR INFORMACIÓN COMO CONTRASEÑAS, DOCUMENTOS INTERNOS, O CUALQUIER DATO SENSIBLE QUE HAYA SIDO DESCARTADO INCORRECTAMENTE.

INGENIERÍA SOCIAL

DEFINICIÓN: LA INGENIERÍA SOCIAL ES UNA TÉCNICA EN LA QUE LOS ATACANTES MANIPULAN A LAS PERSONAS PARA OBTENER INFORMACIÓN CONFIDENCIAL O INDUCIR ACCIONES ESPECÍFICAS. PUEDE INVOLUCRAR EL ENGAÑO, LA MANIPULACIÓN EMOCIONAL O LA EXPLOTACIÓN DE LA CONFIANZA.

USO: LOS CIBERDELINCUENTES PUEDEN UTILIZAR LA INGENIERÍA SOCIAL EN FORMA DE ATAQUES DE PHISHING, LLAMADAS TELEFÓNICAS FRAUDULENTAS, CORREOS ELECTRÓNICOS ENGAÑOSOS, ENTRE OTROS, PARA OBTENER ACCESO NO AUTORIZADO A SISTEMAS O INFORMACIÓN SENSIBLE.

INTELIGENCIA ACTIVA

VANÁLISIS DE DISPOSITIVOS Y PUERTOS CON NMAP

DEFINICIÓN: NMAP (NETWORK MAPPER) ES UNA HERRAMIENTA DE ESCANEO DE RED UTILIZADA PARA DESCUBRIR DISPOSITIVOS EN UNA RED Y MAPEAR LOS SERVICIOS QUE ESTÁN EJECUTÁNDOSE EN ESOS DISPOSITIVOS.

USO: CON NMAP, SE PUEDEN REALIZAR ANÁLISIS DETALLADOS DE DISPOSITIVOS Y PUERTOS, IDENTIFICANDO SISTEMAS EN UNA RED Y LOS SERVICIOS QUE ESTÁN ACTIVOS EN ESOS SISTEMAS.

PARÁMETROS Y OPCIONES DE ESCANEO DE NMAP

DEFINICIÓN: NMAP OFRECE UNA AMPLIA VARIEDAD DE PARÁMETROS Y OPCIONES PARA PERSONALIZAR Y ESPECIFICAR EL TIPO DE ESCANEO QUE SE DESEA REALIZAR. ESTOS INCLUYEN OPCIONES PARA VELOCIDAD, PROFUNDIDAD DE ESCANEO, TIPOS DE ESCANEO, Y MÁS.

USO: PERMITE A LOS USUARIOS ADAPTAR EL ESCANEO A SUS NECESIDADES ESPECÍFICAS, YA SEA PARA UN ESCANEO RÁPIDO O PARA UN ANÁLISIS MÁS EXHAUSTIVO.

FULL TCP SCAN

DEFINICIÓN: UN ESCANEO COMPLETO DE TODOS LOS PUERTOS TCP EN UN HOST. BUSCA ACTIVAMENTE TODOS LOS PUERTOS TCP DISPONIBLES.

USO: PROPORCIONA UNA VISIÓN COMPLETA DE LOS SERVICIOS Y PUERTOS EN UN SISTEMA, IDENTIFICANDO CUALQUIER SERVICIO QUE PUEDA ESTAR EJECUTÁNDOSE EN CUALQUIER PUERTO TCP.

STEALTH SCAN

DEFINICIÓN: UN ESCANEO DISEÑADO PARA SER SIGILOSO Y MINIMIZAR LA DETECCIÓN. UTILIZA TÉCNICAS COMO EL ESCANEO SYN PARA EVITAR GENERAR REGISTROS EN LOS SISTEMAS OBJETIVO.

USO: ÚTIL EN SITUACIONES DONDE SE BUSCA OBTENER INFORMACIÓN SIN ALERTAR A LOS SISTEMAS OBJETIVO DE LA ACTIVIDAD DE ESCANEO.

FINGERPRINTING

DEFINICIÓN: EL FINGERPRINTING EN EL CONTEXTO DE NMAP SE REFIERE A LA IDENTIFICACIÓN DE LA PILA TECNOLÓGICA Y VERSIONES DE SOFTWARE UTILIZADAS EN UN SISTEMA.

USO: PERMITE A LOS ANALISTAS DE SEGURIDAD ADAPTAR SUS ATAQUES A LAS VULNERABILIDADES ESPECÍFICAS DE LA CONFIGURACIÓN DEL SISTEMA.

ZENMAP

DEFINICIÓN: ZENMAP ES LA INTERFAZ GRÁFICA DE USUARIO (GUI) PARA NMAP. PROPORCIONA UNA FORMA VISUAL DE VER Y ANALIZAR LOS RESULTADOS DE LOS ESCANEOS REALIZADOS CON NMAP.

USO: FACILITA LA INTERPRETACIÓN DE LOS DATOS RECOPILADOS POR NMAP, PERMITIENDO UNA REPRESENTACIÓN GRÁFICA DE LA TOPOLOGÍA DE LA RED Y LOS SERVICIOS ENCONTRADOS.

ANÁLISIS TRACEROUTE

DEFINICIÓN: TRACEROUTE ES UNA HERRAMIENTA QUE RASTREA LA RUTA QUE TOMA UN PAQUETE DE DATOS DESDE EL ORIGEN HASTA EL DESTINO, IDENTIFICANDO LOS NODOS INTERMEDIOS.

USO: EN EL CONTEXTO DE NMAP, EL ANÁLISIS TRACEROUTE AYUDA A COMPRENDER LA TOPOLOGÍA DE LA RED, IDENTIFICANDO LOS SALTOS Y DISPOSITIVOS ENTRE EL ESCÁNER Y EL OBJETIVO.

EHHHHH GRACIAS