UNIVERSIDAD AUTONOMA DE CHIAPAS.

ACT. 1.1 INVESTIGAR LOS CONCEPTOS DE VULNERABILIDADES

MATERIA: ANALISIS DE VULNERABILIDADES

BRIAN MICHELL CORONEL OVILLA, A200726

GRADO Y GRUPO: 7N, LICENCIATURA EN L.I.D.T.S

DOCENTE: DR. LUIS GUTIERREZ ALFARO

LUGAR Y FECHA:
TUXTLA GUTIÉRREZ, CHIAPAS, 15/08/2023

HERRAMIENTAS DE VULNERABILIDADES:

NMAP

Es una herramienta de código abierto ampliamente utilizada para el escaneo de redes y la detección de dispositivos en una red. Fue creado por Gordon Lyon, también conocido como "Fyodor", y se utiliza para descubrir hosts activos, servicios en ejecución, puertos abiertos y otra información relacionada con la seguridad de una red.

JOOMSCAN

Es una herramienta de escaneo de seguridad diseñada específicamente para detectar y evaluar vulnerabilidades en sitios web que utilizan el sistema de gestión de contenido (CMS) Joomla. Joomla es una plataforma popular para la creación y administración de sitios web y blogs.

VEGA

Es una herramienta de código abierto utilizada para realizar pruebas de seguridad automatizadas en aplicaciones web. Su enfoque principal es la detección de vulnerabilidades en sitios web y aplicaciones en línea.

WPSCAN

Es una herramienta de código abierto diseñada específicamente para evaluar la seguridad de sitios web que utilizan WordPress, que es uno de los sistemas de gestión de contenido (CMS) más populares del mundo

NESSUS ESSENTIALS

Es una versión gratuita y limitada del popular escáner de vulnerabilidades Nessus, desarrollado por la empresa Tenable. Nessus es una herramienta ampliamente utilizada para llevar a cabo evaluaciones de seguridad y detectar vulnerabilidades en redes, sistemas y aplicaciones.

INTELIGENCIA MISCELÁNEO.

- ## GOBUSTER:

ES UNA HERRAMIENTA DE LÍNEA DE COMANDOS UTILIZADA PARA REALIZAR ATAQUES DE FUERZA BRUTA Y ENUMERACIÓN EN APLICACIONES WEB Y SERVIDORES. SU OBJETIVO PRINCIPAL ES DESCUBRIR RUTAS, DIRECTORIOS Y ARCHIVOS OCULTOS O NO ENLAZADOS, LO QUE PUEDE AYUDAR A IDENTIFICAR POSIBLES PUNTOS DE ENTRADA PARA ATAQUES O REVELAR INFORMACIÓN SENSIBLE EN UN SITIO WEB.

- ## DUMPSTER DIVING

ES UNA PRÁCTICA EN LA QUE LAS PERSONAS BUSCAN INFORMACIÓN VALIOSA O CONFIDENCIAL EN LA BASURA O LOS DESECHOS DE EMPRESAS U ORGANIZACIONES. ESTA ACTIVIDAD SE REALIZA CON EL PROPÓSITO DE OBTENER INFORMACIÓN ÚTIL, COMO DOCUMENTOS, REGISTROS, DISCOS DUROS, DISPOSITIVOS ELECTRÓNICOS U OTROS MATERIALES QUE PUEDEN CONTENER DATOS SENSIBLES.

- ## INGENIERÍA SOCIAL

ES UNA TÉCNICA UTILIZADA PARA MANIPULAR A LAS PERSONAS Y OBTENER INFORMACIÓN CONFIDENCIAL, ACCESO A SISTEMAS, O LLEVAR A CABO ACCIONES QUE DE OTRA MANERA PODRÍAN SER DIFÍCILES DE LOGRAR A TRAVÉS DE MÉTODOS TÉCNICOS O INFORMÁTICOS CONVENCIONALES. EN LUGAR DE EXPLOTAR VULNERABILIDADES EN SISTEMAS INFORMÁTICOS, LA INGENIERÍA SOCIAL EXPLOTA LAS DEBILIDADES Y LA PSICOLOGÍA HUMANAS.

INTELIGENCIA ACTIVA:

- ## ANÁLISIS DE DISPOSITIVOS Y PUERTOS CON NMAP

ES UNA PRÁCTICA COMÚN EN LA SEGURIDAD INFORMÁTICA Y EN LA ADMINISTRACIÓN DE REDES. NMAP ES UNA HERRAMIENTA DE CÓDIGO ABIERTO QUE SE UTILIZA PARA ESCANEAR REDES Y DESCUBRIR HOSTS ACTIVOS, ASÍ COMO PARA IDENTIFICAR LOS PUERTOS ABIERTOS Y LOS SERVICIOS QUE SE EJECUTAN EN ESOS PUERTOS.

- ## PARAMETROS OPCIONES DE ESCANEO DE NMAP

1. -P <PUERTOS>: ESPECIFICA LOS PUERTOS QUE DESEAS ESCANEAR. PUEDES PROPORCIONAR UN RANGO DE PUERTOS (POR EJEMPLO, 80-100) O UNA LISTA SEPARADA POR COMAS (POR EJEMPLO, 21,22,80).
2. -SS: ESCANEO SYN. REALIZA UN ESCANEO DE PUERTOS TCP UTILIZANDO EL MÉTODO SYN (SEMIÓPENO). ESTE ES EL ESCANEO PREDETERMINADO EN NMAP.
3. -ST: ESCANEO TCP COMPLETO. REALIZA UN ESCANEO DE PUERTOS TCP UTILIZANDO UNA CONEXIÓN COMPLETA.
4. -SU: ESCANEO UDP. REALIZA UN ESCANEO DE PUERTOS UDP PARA DESCUBRIR SERVICIOS QUE NO USAN TCP.
5. -SV: IDENTIFICACIÓN DE SERVICIOS. INTENTA IDENTIFICAR LOS SERVICIOS Y VERSIONES QUE SE ESTÁN EJECUTANDO EN LOS PUERTOS ABIERTOS.
6. -A: ESCANEO DE DETECCIÓN DE SISTEMA OPERATIVO Y VERSIÓN DE SERVICIO. INTENTA DETECTAR EL SISTEMA OPERATIVO Y LAS VERSIONES DE LOS SERVICIOS EN LOS PUERTOS ABIERTOS.
7. -O: DETECCIÓN DE SISTEMA OPERATIVO. INTENTA DETERMINAR EL SISTEMA OPERATIVO DEL OBJETIVO EN FUNCIÓN DE CARACTERÍSTICAS Y RESPUESTAS.
8. -T<NIVEL>: DEFINE EL NIVEL DE VELOCIDAD DEL ESCANEO. LOS NIVELES VAN DESDE 0 (SIGILOSO) HASTA 5 (INSENSATO). POR EJEMPLO, -T4 INDICA UN ESCANEO MÁS RÁPIDO.
9. -IL <ARCHIVO>: ESPECIFICA UN ARCHIVO QUE CONTIENE UNA LISTA DE OBJETIVOS PARA ESCANEAR.
10. -ON <ARCHIVO>: GUARDA LOS RESULTADOS DEL ESCANEO EN FORMATO NORMAL EN EL ARCHIVO ESPECIFICADO.
11. -OX <ARCHIVO>: GUARDA LOS RESULTADOS DEL ESCANEO EN FORMATO XML EN EL ARCHIVO ESPECIFICADO.
12. -OG <ARCHIVO>: GUARDA LOS RESULTADOS DEL ESCANEO EN UN FORMATO GREPPABLE EN EL ARCHIVO ESPECIFICADO.
13. --SCRIPT <SCRIPT>: EJECUTA UN SCRIPT NSE ESPECÍFICO DURANTE EL ESCANEO. POR EJEMPLO, --SCRIPT=HTTP-ENUM EJECUTARÁ EL SCRIPT DE ENUMERACIÓN HTTP.
14. -V: MODO VERBOSO. PROPORCIONA INFORMACIÓN DETALLADA SOBRE EL PROGRESO DEL ESCANEO.

INTELIGENCIA MISCELÁNEO.

- **FULL TCP SCAN**

SE REFIERE A UN ESCANEO EXHAUSTIVO DE TODOS LOS 65,535 PUERTOS TCP POSIBLES EN UN OBJETIVO. ESTE TIPO DE ESCANEO PUEDE LLEVAR MUCHO TIEMPO Y CONSUMIR RECURSOS CONSIDERABLES, POR LO QUE SE DEBE USAR CON PRECAUCIÓN Y GENERALMENTE SE RECOMIENDA SOLO CUANDO ES NECESARIO UN ANÁLISIS PROFUNDO Y COMPLETO DE LOS PUERTOS ABIERTOS EN UN SISTEMA O RED.

- **STELTH SCAN**

ES UN TIPO DE ESCANEO DE PUERTOS REALIZADO CON LA INTENCIÓN DE SER LO MÁS DISCRETO Y NO INTRUSIVO POSIBLE. EL OBJETIVO DE ESTE TIPO DE ESCANEO ES EVITAR QUE EL SISTEMA OBJETIVO DETECTE LA ACTIVIDAD DE ESCANEO Y, POR LO TANTO, REDUCIR LA POSIBILIDAD DE QUE SE GENERE UNA ALARMA DE SEGURIDAD.

- **FINGERPRINTIG**

SE REFIERE AL PROCESO DE RECOPILAR INFORMACIÓN DETALLADA SOBRE UN SISTEMA, APLICACIÓN O RECURSO EN LÍNEA PARA IDENTIFICAR CARACTERÍSTICAS ESPECÍFICAS QUE PUEDAN SER ÚTILES PARA IDENTIFICAR O CLASIFICAR DICHO SISTEMA. EL OBJETIVO ES OBTENER INFORMACIÓN DETALLADA SOBRE CÓMO ESTÁ CONFIGURADO EL SISTEMA, QUÉ SOFTWARE SE ESTÁ EJECUTANDO Y OTRAS CARACTERÍSTICAS DISTINTIVAS.

INTELIGENCIA MISCELÁNEO.

- ## ZENMAP

NMAP ES UNA HERRAMIENTA DE LÍNEA DE COMANDOS AMPLIAMENTE UTILIZADA PARA ESCANEAR REDES Y DESCUBRIR HOSTS ACTIVOS, IDENTIFICAR PUERTOS ABIERTOS Y SERVICIOS EN ESOS PUERTOS, Y REALIZAR ANÁLISIS DE SEGURIDAD EN SISTEMAS Y REDES.

- ## ANÁLISIS TRACEROUTE

ES UNA TÉCNICA UTILIZADA PARA RASTREAR LA RUTA QUE SIGUE UN PAQUETE DE DATOS A TRAVÉS DE LA RED DESDE UN PUNTO DE ORIGEN HASTA UN DESTINO. TRACEROUTE ES UNA HERRAMIENTA QUE MUESTRA UNA LISTA DE SALTOS (ROUTERS) QUE EL PAQUETE ATRAVIESA PARA LLEGAR AL DESTINO FINAL. CADA SALTO ES UN PUNTO EN LA RED DONDE EL PAQUETE ES REENVIADO DE UN ROUTER A OTRO EN SU CAMINO HACIA EL DESTINO.