Universidad
Autónoma de Chiapas
Análisis de vulnerabilidades

CONCEPTOS DE VULNERABILIDADES

FERNANDO DE JESÚS SÁNCHEZ ARIAS

HERRAMIENTAS DE VULNERABILIDADES:

nmap : herramienta para exploración de red y auditoria de seguridad , optimo para analizar rápidamente grandes redes. Utiliza paquetes IP “raw”(crudos) en formas originales para determinar que equipos se encuentran disponibles en una red, ofreciendo: mostrar (host disponibles y que servicios ‘aplicaciones nombre y versión’, que sistemas operativos ‘versiones’, tipo de paquete se utiliza con el firewall etc.

Joomscan : desarrollado con el objetivo de automatizar la tarea de detección de vulnerabilidad y garantía de confiabilidad en las implementaciones permitiendo un escaneo continuo y sin esfuerzo, dejando una huella mínima con su arquitectura ligera y modular, también puede detectar configuraciones erróneas y deficiencias a nivel de administrador.

WPScan : es un escáner de seguridad de WordPress de caja negra gratuito, con funciones de versión de WordPress instalada y cualquier vulnerabilidad asociada.

Nessus Essentials : igual de tipo escaneo de vulnerabilidades, de cumplimiento de detección de malware y Botnets además de generar informes, en la versión gratuita tiene limitantes.

Vega : escáner de seguridad, ayuda a encontrar secuencias de comandos entre sitios reflejadas, inyección SQL ciega, inclusión de archivos remotos, inyección Shell y otros, además de probar la seguridad TLS/SSL e identificar oportunidades para mejorar la seguridad de sus servidores en TLS, pruebas de proxy de intercepción para inspección táctica.

- Inteligencia Misceláneo.

Gobuster : utilizada para fuerza bruta: fuerza directorios y archivos URI en sitios web, subdominios DNS , nombre de host virtual en servidores web de destino, útil para pentésteres, hackers éticos y expertos forenses. También para pruebas de seguridad.

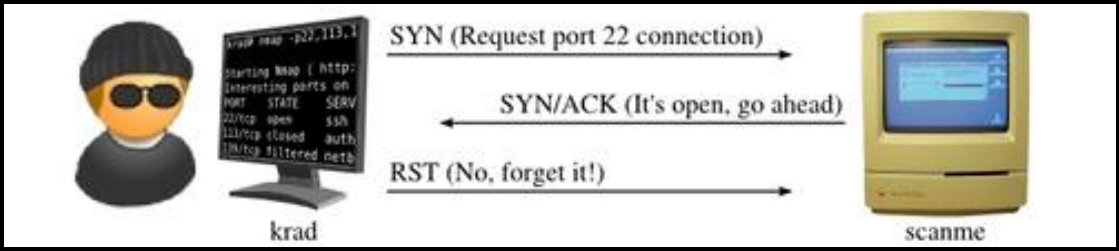
Dumpster diving : técnica utilizada para recuperar información que podría usarse para llevar a acabo un ataque o obtener acceso a una red desde elementos eliminados, en todo caso es para recopilar información para un ataque personalizado.

Ingeniería Social: técnica usado por cracker para engañar al cerebro huma no y hacer que actúe con un desencadenante, las actividades típicas son, ganar tu confianza, Curiosidad y urgencia , voz persuasiva (Autoridad, Prueba social, Gustos, similitudes, engaños compromiso , distracción) y el uso de las emociones.

Inteligencia Activa

Análisis de dispositivos y puertos con Nmap : Se podría hacer primero ver si se puede conectar al equipo con un ping y ver si es accesible con esta herramienta seria con - sn (nmap [ip]), una forma de hacerlo sin usar el ping seria usando el -P0, -Pn cual es la diferencia como primera debemos saber que el host este activo y ejecuta escaneos sin necesidad de enviar ping por decirlo es más silencioso en cambio el segundo es de fuerza bruta ya que realiza un escaneo mas exhaustivo y tiene más riesgos de ser descubierto. En si un escaneo se daría tipo: nmap –p 80 192.162.206.133 u de rango completo nmap –p 1-65535 192.162.206.133 ser recomienda nmap -p- [ip], esta es la primera entrada.

Escaneo de puerto especifico nmap -p [puerto] [ip]	Escaneo de puerto UDP nmap -sU -p [puerto][ip]	Escaneo en modo sigiloso nmap -sS [ip]



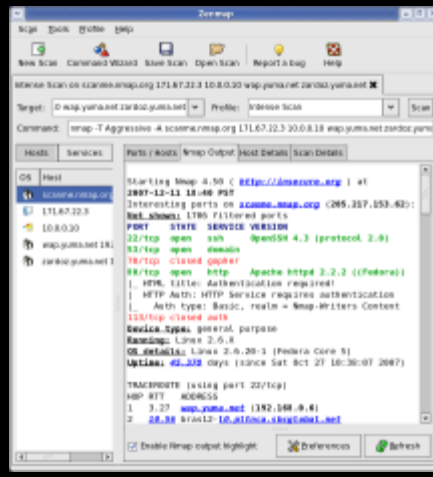
Parámetros opciones de escaneo de nmap: Los escaneos son desde el básico [IP].

Escaneos TCP.
Escaneo UDP.
Escaneo sigilosos.
Escaneos de detección.
Escaneos rápidos.
Escaneos de puertos y servicios.
Detección de sistemas operativos.
Escaneo con scripts.
Detección de vulnerabilidades.
Escaneo de ipv6.
Suplantación de direcciones MAC
Escpecificación de interfaz de red.
De tiempo de espera.

Full TCP scan: Termino usado para describir un escaneo exhaustivo de todos los puertos TCP, para lograrlo con nmap se tiene que especificar todos los puertos existentes en el comando siendo .
nmap -p 1-65535 [IP].

Stelh Scan : Termino usado para describir un escaneo sigiloso con los comando clave: -sA: TCP ACK Scan, -sS: TCP SYN Scan, -sW: TCP Window Scan

Zenmap: Gui oficial del escáner de seguridad Nmap. Es multiplataforma, es gratuita de código abierto, hace más fácil los escaneos repetitivos guardando perfiles y guarda una base de datos de búsqueda.



Análisis traceroute: Es una herramienta que permite el rastreo de ruta que los paquetes siguen desde una dirección IP de red en camino a un host determinado, usando el Tiempo de vida (TTL) este protocolo genera una respuesta ICMP TIME_EXCEEDED en cada nodo que tome.