Documentación Técnica: Suite de Automatización para Kali Linux

1. Introducción

Esta suite de scripts está diseñada para automatizar tareas comunes en auditorías de seguridad ofensiva utilizando Kali Linux. Los scripts están escritos en Bash y aprovechan herramientas estándar como **Nmap, TShark y TCPdump** para realizar escaneos de red, captura de tráfico y generación de reportes estructurados.

El objetivo principal es reducir el tiempo empleado en tareas repetitivas, garantizando consistencia en los resultados y facilitando la documentación de hallazgos.

2. Propósito General

Cada script cumple una función específica dentro del flujo de trabajo de un pentest:

Script:	Objetivo Principal:
Scan_nmap.sh	Automatizar escaneos avanzados con Nmap (TCP, UDP, detección de servicios).
Capture_logs.sh	Capturar tráfico de red en formato PCAP para un análisis posterior.
Parse_traffic.sh	Extraer métricas clave de los archivos PCAP y generar reportes MD.
Full_scan.sh	Es un escaneo completo con Nmap y a su vez una captura de tráfico.

3. Funcionamiento

3.1. scan_nmap.sh

Herramientas utilizadas: Nmap, XMLStarlet.

Proceso:

1- Ejecuta tres tipos de escaneos:

TCP SYN Scan (-sS): Identifica puertos abiertos en los 1000 puertos más comunes.

UDP Scan (-sU): Escanea los 100 puertos UDP más frecuentes.

Detección de versiones (-sV): Determina servicios y versiones en puertos abiertos.

2- Combina los resultados en un único archivo XML.
3- Genera un resumen en texto plano con puertos abiertos y banners.

Ejemplo de comando:

Usuario: *sudo ./scan_nmap.sh 192.168.1.1*

3.2. capture_logs.sh

Herramientas utilizadas: Tcpdump, Gzip.

Proceso:

1- Captura tráfico en la interfaz especificada, filtrando ruido (ARP, tráfico multicast).
2- Guarda la captura en formato PCAP con marca de tiempo.
3- Comprime el archivo con Gzip para ahorrar espacio.

Ejemplo de comando:

Usuario: *sudo ./capture_logs.sh eth0 60*

Importante: En este caso la captura se hace en la interfaz de red eth0 durante un tiempo de 60 segundos.

3.3. parse_traffic.sh

Herramientas utilizadas: TShark (CLI de Wireshark).

Proceso:

1- Analiza el archivo PCAP (o PCAP.gz) y extrae:
2- Estadísticas generales (paquetes, bytes).
3- Protocolos dominantes (TCP/UDP/HTTP).
4- Conversaciones activas (IPs origen/destino).
5- Genera un reporte en formato Markdown compatible con Git.

Ejemplo de comando:

Usuario: ./parse_traffic.sh captures/eth0_20250101_1200.pcap.gz

3.4. full_scan.sh

Funcionamiento:

1- Ejecuta scan_nmap.sh en segundo plano.
2- Inicia capture_logs.sh en paralelo.
3- Al finalizar, procesa la captura PCAP con parse_traffic.sh.

Ejemplo de comando:

Usuario: sudo ./full_scan.sh 192.168.1.1 eth0 120

Importante: Declarar la ip o rango a utilizar, además de la interfaz de red a utilizar y el tiempo.

4. Guía Paso a Paso descarga y set-up:

4.1. Configuración Inicial

Copiar los scripts a Kali Linux:

Usuario: chmod +x *.sh

Usuario: mkdir -p reports/nmap reports/traffic captures

Instalar dependencias (si no están presentes):

sudo apt update && sudo apt install nmap tshark xmlstarlet