Asignatura:
Hacking Ético

Título del Documento:

Guía de Procedimientos Técnicos - Numbers

Nombre:	Fecha:	Firma:
Mario de la Rosa García	**02/04/24**	
Gonzalo Pascual Romero	**02/04/24**	
David Lucas Sánchez	**02/04/24**	
Simón Armando Padrón	**02/04/24**	

Tabla de Contenidos

OSINT

Validación de objetivo: WHOIS, nslookup, dnsrecon, dig

Emails:
nslookup for SPF: nslookup -type=txt dominio.com
nslookup for DMARC: nslookup -type=txt _dmarc.dominio.com

Subdominios: Google, dig, nmap, sublist3r, Bluto, crt.sh, fierce.pl, knockpy

Fingerprinting: nmap, wappalyzer (plugin de navegador), WhatWeb, BuiltWith, netcat

Brechas de datos: haveibeenpwned, weleakinfo.com ($2 para 24 hrs de acceso)

Enumeración de usuarios/emails: theharvester.py, hunter.io (necesita cuenta)

Reconocimiento

Objetivo: Recopilar información sobre el objetivo del test, como direcciones IP, dominios, nombres de empleados, tecnologías utilizadas, etc.

Herramientas

- Google Hacking
  - Site
  - Intitle
  - Allintitle
  - inurl:.edu.co/robots.txt
- Maltego
- WhoIs
- Foca
- Análisis de metadatos
- Shodan.io
- Dominios.es
- CentralOPS

Enumeración

Objetivo: Definir el objetico que se desea atacar y los puntos críticos con vulnerabilidades que se pueden llegar a controlar, en esta etapa se hace una recolección de información más específica para sacar datos como sus sistemas operativos, los servicios que corren y sus respectivas versiones, rangos IP, DNS, detección de IDS y IPS o firewall.

Herramientas

- Nmap
  - Nmap -sn 192.168.22.0/24 (Escaneo hosts)
  - Nmap -O (sacar SO)

- Nmap -sCV IP (Escaneo completo a un host)
- Nmap -p 21 (Escaneo puertos)

  nmap -p 443 --script=ssl-enum-ciphers 10.10.10.X

· Feroxbuster (Directorios Web)
- feroxbuster –url 192.168.22.17
- feroxbuster --url http://192.168.22.17 -w /usr/share/wordlists/dirb/common.txt
- feroxbuster -u http://192.168.22.17 -x pdf -x js,html -x php txt json,docx

· Gobuster (Enumeración directorios)
- gobuster dir -u http://192.168.22.17 -w /usr/share/wordlists/dirb/common.txt

Análisis de vulnerabilidades

Objetivo: En esta fase se recopila la información obtenida anteriormente para clasificar las posibles vulnerabilidades del sistema objetivo

Vulnerabilidad local: Es el tipo de vulnerabilidad en la cual se debe tener acceso físico a la maquina o sistema objetivo para explotar una vulnerabilidad y posterior a esto elevar o escalar privilegios dentro del sistema y tener acceso a él sin ninguna restricción.

Vulnerabilidad remota: Es el tipo de vulnerabilidad en la cual se puede obtener acceso al sistema objetivo a través de la red sin necesidad de un acceso físico o local.

Herramientas

· Nessus (Escáner vulnerabilidades)
· Nikto (Escaneo de seguridad en webs)

nikto -h https://10.10.10.X

· Wpscan (Escaneo páginas wordpress)

Explotación

Objetivo: Aquí se utiliza la información obtenida en las fases anteriores y se aprovechan las vulnerabilidades encontradas en el sistema objetivo para tomar control de éste y escalar privilegios

Herramientas

- · **Metasploit**: herramienta de código abierto para pruebas de penetración y seguridad informática
- · **Hydra**: Hydra es una popular herramienta de prueba de penetración diseñada para realizar ataques de fuerza bruta y ataques de diccionario contra servicios de autenticación remotos
- · **JohnTheRipper**: herramienta de código abierto diseñada para realizar ataques de fuerza bruta contra contraseñas cifradas
- · **BurpSuite**: herramienta integral de seguridad web que incluye analizador de contenido, intrusión, spidering, proxy intercepting y escaneo automatizado
- · **SQLmap**: herramienta de código abierto diseñada para automatizar la detección y explotación de vulnerabilidades de inyección de SQL en aplicaciones web

- · **Explotación FTP**: proceso de identificar y aprovechar vulnerabilidades en servidores FTP para obtener acceso no autorizado o realizar acciones maliciosas
- · **Explotación SSH**: proceso de identificar y aprovechar vulnerabilidades en servidores SSH para obtener acceso no autorizado o realizar actividades maliciosas
    - ssh -i llave_privada usuario@ip
    - ssh usuario@ip

- **NetCat**: herramienta de red versátil y poderosa que permite la lectura y escritura de datos a través de conexiones de red utilizando los protocolos TCP/IP y UDP
    - nc -lvnp 4444
    - nc -lvp 4444

- **Kali linux**: distribución de Linux especializada en seguridad informática y pruebas de penetración

- **Searchsploit**: Como parte del marco Metasploit, Searchsploit permite a los investigadores de seguridad buscar exploits y payloads en la base de datos de Metasploit. Esto simplifica el proceso de encontrar exploits para vulnerabilidades conocidas en sistemas y aplicaciones, facilitando la investigación y la ejecución de pruebas de penetración. Con una interfaz de línea de comandos fácil de usar, Searchsploit proporciona acceso rápido a una amplia gama de exploits y facilita la identificación de amenazas potenciales en entornos de red.
    - searchsploit mariadb
    - searchsploit -m linux/local/34533.txt

- **scp**: Es una utilidad en sistemas basados en Unix y Linux que permite la transferencia segura de archivos entre hosts a través de SSH (Secure Shell). scp utiliza la misma autenticación y seguridad que SSH, lo que significa que los datos transferidos están cifrados durante la transmisión, proporcionando un alto nivel de seguridad.
    - scp root@ip:/home/usuario/ archivo.txt nombreguardado.txt
    - scp root@ip:/home/usuario/ archivo.txt .

- **gpg**: Es una herramienta de código abierto que cifra y firma digitalmente mensajes y archivos para mantener la privacidad y autenticidad en la comunicación electrónica. Permite la generación de claves, el cifrado de datos y la verificación de la autenticidad de mensajes. Es esencial para asegurar la seguridad de los datos en la comunicación digital.
    - gpg –batch –output id_rsa.gpg –passphrase passransom –symmetric id_rsa

- **CoverMyAss**: es una herramienta de post-explotación diseñada para cubrir tus rastros en varios sistemas operativos. Fue creada para la fase de "cubrir rastros" durante pruebas de penetración, antes de salir del servidor comprometido. Puedes ejecutar la herramienta en cualquier momento para encontrar los archivos de registro en el sistema y luego borrarlos más tarde. La herramienta te indica qué archivos se pueden borrar con los permisos de usuario actuales. Los archivos se sobrescriben repetidamente con datos aleatorios para dificultar la recuperación de datos incluso con sondas de hardware costosas.
    - ./covermyass
    - ./covermyass –write -n 10

Enumeración de directorios

Dirb
dirb http://10.10.10.X -r -o server.dirb

Gobuster:
gobuster dir -u http://10.10.10.X -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

wfuzz enumeración basada en web
Enumeración utilizando una wordlist
wfuzz -u http://10.10.10.X/FUZZ/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Enumerar datos login POST utilizando una passlist:
wfuzz -z file,wordlist/others/common_pass.txt -d "uname=FUZZ&pass=FUZZ" --hc 302

COMANDOS

- **python3 -m “servidor web” “puerto”**→ inicia un servidor web básico en el puerto 80 de la máquina local utilizando Python 3. Este servidor web puede ser útil para servir archivos estáticos o para probar rápidamente aplicaciones web simples en tu máquina local.
- **nc -lvnp “puerto”** → configura netcat para escuchar en el puerto de la máquina local, esperando conexiones entrantes. Este comando es útil cuando deseas

configurar un servidor simple para recibir conexiones entrantes en un puerto específico y observar las comunicaciones que llegan.

- **nmap -sn "ip"** → realizará un escaneo de ping en todas las direcciones IP de la red "ip" para determinar qué hosts están activos en la red, sin realizar un escaneo de puertos en esos hosts. Esto puede ser útil para identificar qué sistemas están disponibles en la red y son potencialmente accesibles para escaneos de puertos más detallados u otros fines de diagnóstico de red.
    - **nmap**: Es una herramienta de escaneo de red de código abierto que se utiliza para descubrir hosts y servicios en una red, así como para auditar la seguridad de una red.
    - -**sn**: Esta opción de Nmap indica que se debe realizar un "escaneo de ping", también conocido como escaneo de hosts activos. En lugar de escanear puertos en los hosts, Nmap simplemente envía paquetes de solicitud de eco ICMP (Protocolo de Mensajes de Control de Internet) a las direcciones IP especificadas y espera respuestas. Esta opción es útil para identificar qué hosts están activos en la red sin necesidad de escanear puertos.
- **nmap -sCV "ip"** → ejecutará un escaneo en el host con la dirección IP 192.168.22.5 utilizando los scripts de detección de versiones y los scripts estándar de Nmap, lo que permitirá identificar los servicios que se están ejecutando en el host, así como sus versiones y posibles vulnerabilidades. Además, mostrará información detallada sobre el proceso de escaneo. Este tipo de escaneo es útil para comprender mejor la configuración y la seguridad de un sistema en particular.
    - **-sCV**: Estas opciones son combinaciones que indican a Nmap que realice ciertas acciones durante el escaneo:
    - **-sC:** Realiza un escaneo utilizando los scripts de detección de versiones y los scripts de secuencia de comandos estándar de Nmap. Esto permite detectar servicios, versiones de software y posibles vulnerabilidades.
    - **-V:** Habilita el modo de "verbose" (detallado) para mostrar información detallada sobre el escaneo, incluidas las versiones de Nmap y las versiones de los servicios detectados.
- **dirsearch -u "servidor web"** → es una herramienta de código abierto diseñada para realizar búsquedas exhaustivas de directorios y archivos en servidores web. Es especialmente útil para identificar recursos ocultos, archivos de configuración sensibles, y posibles puntos de acceso vulnerables en aplicaciones web.
    - **-u <URL>:** especifica la URL del sitio web objetivo en el que se realizará la búsqueda.
- **Whois "servidor web"** → Es una herramienta útil para investigadores de seguridad, administradores de sistemas y cualquier persona interesada en obtener información sobre dominios y direcciones IP en Internet

- **nslookup “servidor web”** → Es una herramienta de línea de comandos utilizada para consultar y resolver nombres de dominio (DNS) en direcciones IP y viceversa. Proporciona una forma rápida y sencilla de obtener información sobre la resolución de nombres de dominio y la configuración del servidor DNS.
- **ftp “dirección ip”** → Este comando intentará establecer una conexión FTP con el servidor que tiene la dirección IP. Después de ejecutar este comando, generalmente se te pedirá que ingreses tu nombre de usuario y contraseña para iniciar sesión en el servidor FTP, a menos que el servidor permite conexiones anónimas
- **hydra -l trainerjeff -P /usr/share/wordlists/rockyou.txt** → Este comando está configurado para intentar iniciar sesión en un sistema utilizando el nombre de usuario "trainerjeff" y probando contraseñas del archivo "rockyou.txt" mediante un ataque de fuerza bruta

    - **-l trainerjeff**: Especifica el nombre de usuario que se utilizará en el intento de inicio de sesión. En este caso, el usuario es "trainerjeff".
    - **-P /usr/share/wordlists/rockyou.txt**: Especifica la ruta al archivo de lista de contraseñas que se utilizará para intentar iniciar sesión. En este caso, se está utilizando el archivo de lista de contraseñas "rockyou.txt" ubicado en "/usr/share/wordlists/", que es una lista de contraseñas comúnmente utilizada en el mundo de la seguridad informática para realizar pruebas de penetración.

SQL Injection

Manual

Para utilizar en los campos de un formulario de login:
`test' OR 1=1; --`
(se puede continuar con: SELECT * FROM Users WHERE email=’test’ OR 1=1; –’)

Sintaxis adicional para SQL injection

Sqlmap

`sqlmap -r login.req --level 5 --risk 3`
(login.req fichero de una intercepción de Burp suite de una petición de login)

Servicios

SMB

Probar anonymous login:
`smbclient -L \\\\10.10.10.X`

SSH

Guía SSH Pentesting

Active Directory

Responder (Envenenamiento LLMNR)

Bloodhound mapeo de AD

Kerberoasting

CrackMapExec spraying de contraseñas contra un AD

Integration-IT AD Cheatsheet

Exploits y Metasploit

searchsploit [nombre y versión de software] (se puede usar también la búsqueda de metasploit)

msf>search suggester

Metasploit Unleashed

Comandos útiles para Shell

Sacar una TTY Shell

Python

python3 -c "import pty;pty.spawn('/bin/bash')"

Bash

Sacar lista de ficheros interesantes en la home (flags):

find /home -printf -type f "%f\t%p\t%u\t%g\t%m\n" | column -t

Comprobación de aplicaciones ejecutadas (ejemplo “pam”):

dpkg -l | grep -i pam

sudo -l

history

Meterpreter shell desde un shell en segundo plano:

post/multi/manage/shell_to_meterpreter

Meterpreter

getuid

sysinfo

hashdump (necesita privilegios)

shell

load (tab para autocompletar y sacar lista: kiwi, incognito, etc.)

getsystem (priv esc)

Redes windows

arp -a

netstat -an

Escalado de privilegios

GetCap

getcap -r / 2>/dev/null

GTFOBins

Borrado de huellas

Covermyass

$ covermyass -h

Uso:

covermyass [parametros]

Ejemplos:

Sobreescribir logs 5 veces y luego ofuscar con 0s para esconder el proceso de borrado de huellas

covermyass --write -z -n 5

Flags:

-f, --filter strings File paths to ignore (supports glob patterns)

-h, --help help for covermyass

-n, --iterations int Overwrite N times instead of the default (default 3)

-l, --list Show files in a simple list format. This will prevent any write operation

--no-read-only Exclude read-only files in the list. Must be used with --list

-v, --version version for covermyass

--write Erase found log files. This WILL shred the files!

-z, --zero Add a final overwrite with zeros to hide shredding