



SEGURIDAD INFORMÁTICA

JOSÉ PABLO
HERNÁNDEZ

SEGURIDAD INFORMÁTICA


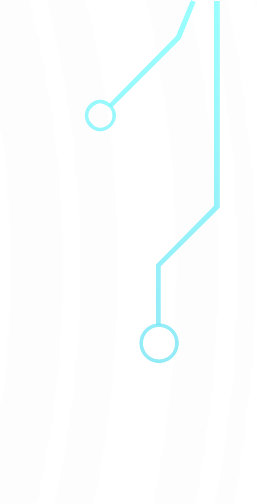
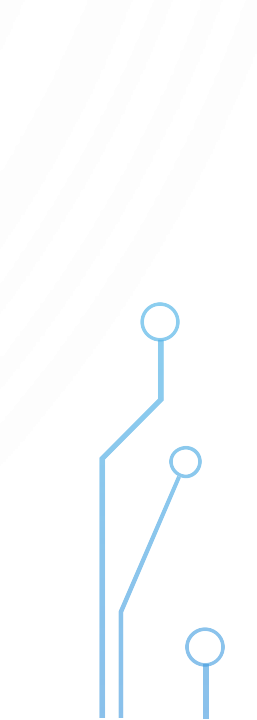
2.4.0.MF0487_3. Capítulo 4

Herramientas para la Auditoría de Sistemas

JOSÉ PABLO HERNÁNDEZ


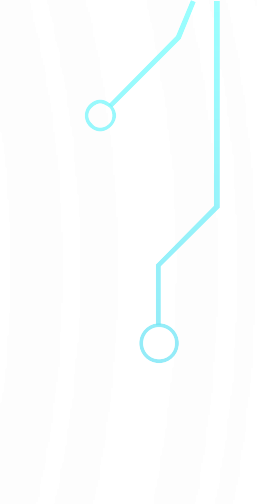
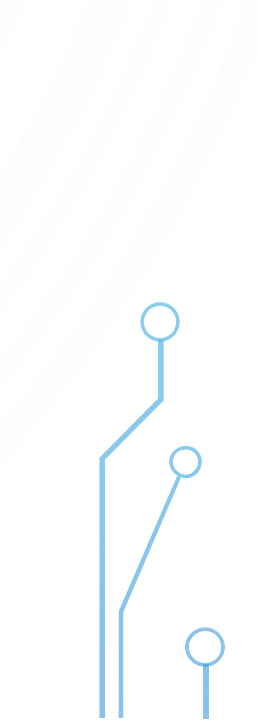


1. INTRODUCCIÓN

- **Experiencia del auditor**
 - **Herramientas variadas**
- 
- 
- 



2. HERRAMIENTAS PROPIAS DEL SISTEMA OPERATIVO

- **PING**
 - **TRACEROUTE (Linux), TRACERT (Windows)**
 - **Whois**
 - **NSLookup**
- 
- 
- 

2.1 PING

PING, de packet internet groper (rastreador de paquetes de red), se puede utilizar en cualquier sistema operativo accediendo mediante comandos.

Comprueba calidad, velocidad y latencia.



2.2 TRACEROUTE

La herramienta traceroute se utiliza para seguir la ruta de los paquetes en una red IP y el retardo que se produce en este tránsito.



2.3 WHOIS

whois se utiliza para realizar consultas en una base de datos de Internet con la finalidad de obtener información sobre alguna IP, algún dominio o alguna organización determinados.

Para Windows hay que descargarlo desde

<https://docs.microsoft.com/en-us/sysinternals/downloads/whois>

2.4 NSLOOKUP

Name System Lookup o NSlookup se utiliza como herramienta de diagnóstico para la detección de problemas de configuración en el DNS.

set type=A, para buscar registros A.

set type=PTR, para buscar registros reversos.

set type=MX, para buscar los registros Mail Exchange del correo.

set type=TXT, para buscar registros de texto como SPF o DKIM.

set type=CNAME, para buscar alias del dominio.

set debug

3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS

Nmap

Netcat

NBTSscan

3.1 NMAP

Nmap es gratuita y de código abierto.

- **Identifica los equipos que forman parte de una red y descubre servidores desconocidos.**
- **Identifica aquellos puertos abiertos de un equipo en concreto.**
- **Facilita información sobre los servicios que se están ejecutando en el sistema de información.**
- **Proporciona información sobre el sistema operativo instalado en el equipo indicado.**
- **También facilita algunas características específicas de los componentes hardware que forman parte de dicho equipo.**

3.2 NETCAT

Netcat funciona a través de comandos y tiene como función principal la apertura de puertos TCP/UDP y la escucha de los datos que se transmiten a través de ellos.

- **Chat:** poniendo uno de los equipos en modo servidor y otro equipo en modo cliente.
- **Envío y recepción de ficheros:** transmitir ficheros de un equipo cliente a un servidor.
- **Escaneo de puertos:** se puede optar por escanear todos los puertos de un equipo determinado o decidir qué puertos concretos escanear.
- **Servidor web:** con Netcat, puede utilizarse el equipo servidor un solo fichero HTML de forma puntual.
- **Ejecución de la herramienta en modo silencioso.**
- **Obtención de una shell para conocer las conexiones del equipo con el sistema operativo Unix.**

Ampliación



VER ENLACE:

[HTTPS://BLOG.DESDELINUX.NET/USANDO-NETCAT-ALGUNOS-COMANDOS-PRACTICOS/](https://blog.desdelinux.net/usando-netcat-algunos-comandos-practicos/)

3.3 NBTSCAN

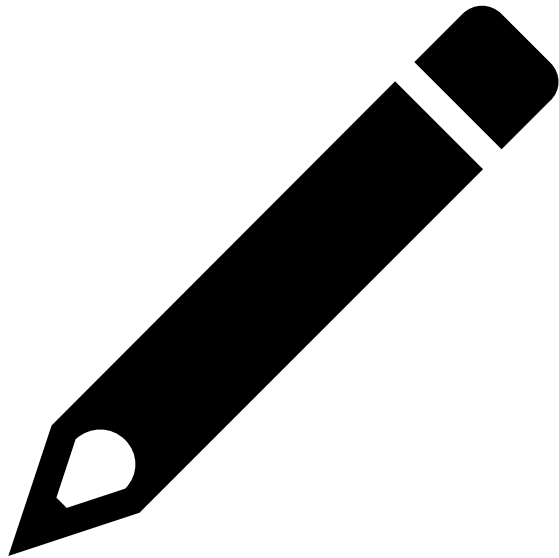
NBTScan es una herramienta que funciona con comandos y que escanea los servidores NetBIOS en una red TCP/IP local o remota.

Se puede utilizar en Windows y Linux, entre otros sistemas operativos, y es gratuita.

- **Escaneo de puertos.**
- **Búsqueda de servidores de nombres NetBIOS.**
- **Identificación de sistemas GNU/Linux que ejecutan servidores SAMBA.**
- **Construcción de listas compuestas exclusivamente por los servidores que comparten recursos.**
- **Acceso a un recurso compartido.**
- **Envío de archivos al recurso compartido.**

<http://www.unixwiz.net/tools/nbtscan.html>.

Ampliación

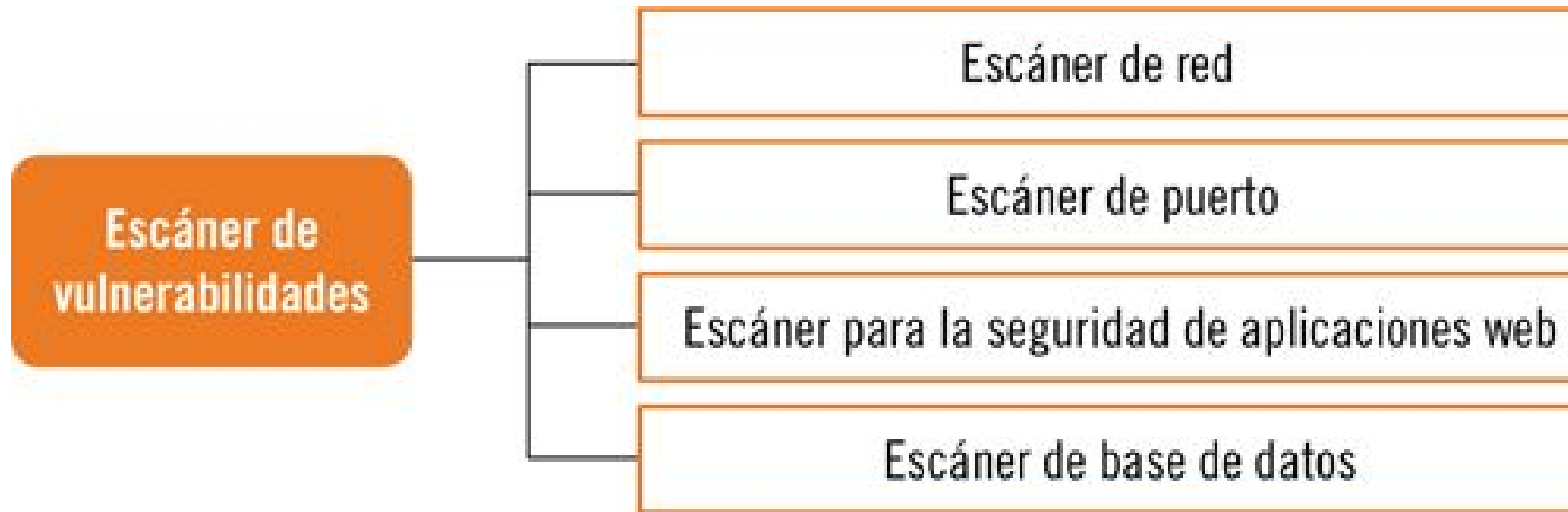


VER ENLACE:

[HTTPS://NULL-BYTE.WONDERHOWTO.COM/HOW-TO/ENUMERATE-NETBIOS-SHARES-WITH-NBTSCAN-NMAP-SCRIPTING-ENGINE-0193957/](https://null-byte.wonderhowto.com/how-to/enumerate-netbios-shares-with-nbtscan-nmap-scripting-engine-0193957/)

4. HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES

Las herramientas de análisis de vulnerabilidades se utilizan para conocer las vulnerabilidades de un sistema de información.



Nessus, OpenVAS

5. ANALIZADORES DE PROTOCOLOS

Los analizadores de protocolos, también llamados analizadores de red, son herramientas que analizan el tráfico de datos de una red en tiempo real o en momentos posteriores a la captura de los datos. Este análisis lo efectúan mediante la captura, decodificación y transmisión de paquetes.

WireShark

DSniff

Cain & Abel

IP Sniffer

Tcpdump

6. ANALIZADORES DE PÁGINAS WEB

En la actualidad, hay numerosos analizadores de páginas web en el mercado y cada uno tiene características distintas y detecta fallos diferentes, por lo que se recomienda utilizar varios de ellos para detectar el mayor número de vulnerabilidades posible.

Acunetix.

Dirb.

Parosproxy.

Virus Total.

URLVoid.

7. ATAQUES DE DICCIONARIO Y FUERZA BRUTA

Ataques de fuerza bruta: aquellos que pretenden recuperar una contraseña probando todas las combinaciones posibles hasta dar con la correcta.

Al ser muy numerosas las posibles combinaciones, este tipo de ataques son muy costosos y conllevan bastante tiempo hasta que se descubre la contraseña correcta.

Debido a estos costes elevados, se suelen combinar con ataques de diccionario.

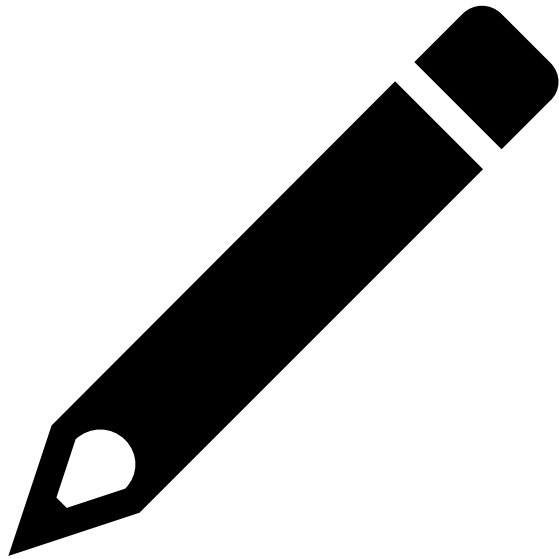
Ataques de diccionario: estos, por el contrario, no encuentran la contraseña probando todas las combinaciones posibles, sino que intentan averiguarla probando todas las palabras del diccionario.

John the Ripper.

Brutus.

OphCrack

Ejercicios



2.4.100.1.MF0487_3. EJERCICIOSCAPITULO_4.DOCX