

IFCT0109. SEGURIDAD INFORMÁTICA MF0487_3 AUDITORÍA DE SEGURIDAD INFORMÁTICA



UD04

USO DE HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS

CONTENIDOS

1. INTRODUCCIÓN
2. HERRAMIENTAS DEL SISTEMA OPERATIVO
3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS
4. HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES
5. ANALIZADORES DE PROTOCOLOS
6. ANALIZADORES DE PÁGINAS WEB
7. ATAQUES DE DICCIONARIO Y FUERZA BRUTA

1. INTRODUCCIÓN

LOS AUDITORES DE SEGURIDAD INFORMÁTICA, PARA DESARROLLAR SUS TAREAS Y BUSCAR POSIBLES FALLOS Y AMENAZAS DEL SISTEMA DE INFORMACIÓN, MUY FRECUENTEMENTE SE APOYAN EN HERRAMIENTAS QUE ANALIZAN CADA UNO DE LOS DISTINTOS ASPECTOS DE LA AUDITORÍA.

DEBIDO A LA GRAN VARIEDAD DE VULNERABILIDADES EXISTENTES, LAS HERRAMIENTAS ENCARGADAS DE SU DETECCIÓN Y ANÁLISIS SON ABUNDANTES Y VARIADAS.



1. INTRODUCCIÓN

AUNQUE LA EXPERIENCIA Y LOS CONOCIMIENTOS DEL AUDITOR SON IMPRESCINDIBLES PARA EL CORRECTO DESARROLLO DE LA AUDITORÍA, SIEMPRE ES RECOMENDABLE QUE EL AUDITOR DISPONGA DE **HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS, HERRAMIENTAS DE ANÁLISIS DE PROTOCOLOS, HERRAMIENTAS DE ATAQUE DE DICCIONARIO Y DE FUERZA BRUTA, ETC., ADEMÁS DE LAS HERRAMIENTAS INTERNAS DE CADA SISTEMA OPERATIVO.**

SE DESCRIBEN LAS HERRAMIENTAS PRINCIPALES PARA LA AUDITORÍA DE SISTEMAS Y LAS FUNCIONALIDADES DESTACADAS DE VARIAS DE ELLAS.



CONTENIDOS

1. INTRODUCCIÓN
- 2. HERRAMIENTAS DEL SISTEMA OPERATIVO**
3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS
4. HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES
5. ANALIZADORES DE PROTOCOLOS
6. ANALIZADORES DE PÁGINAS WEB
7. ATAQUES DE DICCIONARIO Y FUERZA BRUTA

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

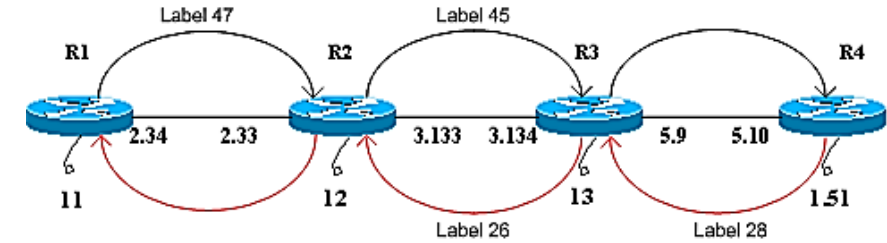
DENTRO DE LAS TAREAS DE LA AUDITORÍA INFORMÁTICA, ESTÁ LA COMPROBACIÓN DEL CORRECTO FUNCIONAMIENTO DE LAS REDES DEL SISTEMA DE INFORMACIÓN.

PARA ELLO, HAY DOS HERRAMIENTAS FUNDAMENTALES: **PING Y TRACEROUTE**, ENTRE OTRAS.



2. HERRAMIENTAS DEL SISTEMA OPERATIVO

EN AMBAS HERRAMIENTAS, SE PUEDE DETECTAR SI EXISTE ALGUNA ANOMALÍA DE RED, COMPROBAR EL ALCANCE DE ESTA ANOMALÍA Y, ADEMÁS, CUÁLES HAN SIDO LOS SERVICIOS QUE SE HAN HECHO INACCESIBLES POR LA INCIDENCIA.



2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA PING.

EL NOMBRE DE LA HERRAMIENTA PING PROVIENE DE **PACKET INTERNET GROPER (RASTREADOR DE PAQUETES DE RED)** Y SE PUEDE UTILIZAR EN CUALQUIER SISTEMA OPERATIVO ACCEDIENDO MEDIANTE COMANDOS.

SE UTILIZA FUNDAMENTALMENTE PARA COMPROBAR LA CALIDAD Y LA VELOCIDAD DE UNA RED DETERMINADA Y PARA COMPROBAR LA LATENCIA ENTRE DOS EQUIPOS.

SU FUNCIONAMIENTO ES BASTANTE SIMPLE: A TRAVÉS DEL COMANDO PING, LA HERRAMIENTA **ENVÍA UNA SERIE DE PAQUETES ICMP DE SOLICITUD Y RESPUESTA** Y DEVUELVE UNOS RESULTADOS EN LOS QUE SE PERMITE VERIFICAR SI EL DESTINO DE LOS PAQUETES ESTÁ ACTIVO.

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA PING

UTILIZANDO MICROSOFT WINDOWS, HABRÁ QUE ABRIR MS-DOS, SELECCIONANDO EL ACCESO DIRECTO DE SÍMBOLO DEL SISTEMA O ESCRIBIENDO EL COMANDO **CMD** EN EL CUADRO DE TEXTO DEL DESPLEGABLE.

EN LINUX Y OTROS SISTEMAS OPERATIVOS, EL PROCEDIMIENTO SERÁ EL MISMO DESDE LA **CONSOLA DE COMANDOS** DE CADA UNO DE ELLOS.

```
C:\Users\benit>ping 8.8.8.8
```

```
Haciendo ping a 8.8.8.8 con 32 bytes de datos:
```

```
Respuesta desde 8.8.8.8: bytes=32 tiempo=40ms TTL=116
```

```
Respuesta desde 8.8.8.8: bytes=32 tiempo=32ms TTL=116
```

```
Respuesta desde 8.8.8.8: bytes=32 tiempo=33ms TTL=116
```

```
Respuesta desde 8.8.8.8: bytes=32 tiempo=32ms TTL=116
```

```
Estadísticas de ping para 8.8.8.8:
```

```
Paquetes: enviados = 4, recibidos = 4, perdidos = 0  
(0% perdidos),
```

```
Tiempos aproximados de ida y vuelta en milisegundos:
```

```
Mínimo = 32ms, Máximo = 40ms, Media = 34ms
```

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA PING

VERIFICACIÓN DEL FUNCIONAMIENTO DE LA RED CON EL COMANDO PING

EL COMANDO PING DEBE IR SEGUIDO DE UNA DIRECCIÓN (IP, UNA URL, EL IP DE UNA RED LOCAL, ETC.) PARA COMPROBAR EL CORRECTO FUNCIONAMIENTO DE LA RED.

SEGÚN LA DIRECCIÓN QUE SE INTRODUZCA, SE VERIFICARÁ SU FUNCIONAMIENTO EN UNOS PUNTOS ESPECÍFICOS U OTROS, COMO SE MUESTRA EN LA TABLA SIGUIENTE.

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA PING

Comando	Verificación
Ping localhost	Se verifica si los protocolos TCP/IP están instalados y si funcionan correctamente.
Ping 192.168.1.1	Permite verificar el correcto funcionamiento del cableado general de la red.
Ping www.google.es	Introduciendo la dirección URL de una web, se puede verificar el correcto funcionamiento de las direcciones IP de los servidores DNS.

ADEMÁS, AÑADIENDO DESPUÉS DEL COMANDO PING LA DIRECCIÓN IP DEL EQUIPO LOCAL, SE PUEDE VERIFICAR SI ESTE HA SIDO AGREGADO CORRECTAMENTE A LA RED EVALUADA.

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA TRACEROUTE

SE UTILIZA PARA SEGUIR LA RUTA DE LOS PAQUETES EN UNA RED IP Y EL RETARDO QUE SE PRODUCE EN ESTE TRÁNSITO.

EN LINUX, SE EJECUTA EL COMANDO **TRACEROUTE** EN LA CONSOLA DE COMANDOS Y, EN WINDOWS, SE ESCRIBIRÁ EL COMANDO **TRACERT** DENTRO DE LA VENTANA DE MS-DOS QUE SURGE AL ESCRIBIR **CMD** EN EL SÍMBOLO DEL SISTEMA.

```
C:\Users\benit>tracert google.es

Traza a la dirección google.es [142.250.200.131]
sobre un máximo de 30 saltos:

 1    4 ms    3 ms    3 ms  192.168.1.1
 2   35 ms    5 ms    5 ms  192.168.144.1
 3    7 ms    5 ms    6 ms  133.red-81-41-252.staticip.rima-tde.net [81.41.252.133]
 4    *        *        *    Tiempo de espera agotado para esta solicitud.
 5    *        *        *    Tiempo de espera agotado para esta solicitud.
 6   29 ms   80 ms   30 ms  176.52.253.97
 7  111 ms   58 ms   30 ms  72.14.211.154
 8   42 ms   32 ms   33 ms  172.253.50.39
 9   29 ms   29 ms   29 ms  142.251.51.143
10   30 ms   29 ms   30 ms  mad41s14-in-f3.1e100.net [142.250.200.131]

Traza completa.
```

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA TRACEROUTE

DESPUÉS DEL COMANDO DEBE ESCRIBIRSE LA DIRECCIÓN URL O EL HOST DESTINO QUE SE QUIERA UTILIZAR PARA COMPROBAR LA RUTA QUE SIGUE EL PAQUETE DE DATOS.

POR EJEMPLO, SI SE QUIERE VERIFICAR LA RUTA HASTA LA URL **WWW.GOOGLE.ES** EN MICROSOFT WINDOWS, SOLO DEBE ESCRIBIRSE **TRACERT WWW.GOOGLE.ES**.

```
C:\Users\benit>tracert google.es

Traza a la dirección google.es [142.250.200.131]
sobre un máximo de 30 saltos:

 1  4 ms    3 ms    3 ms  192.168.1.1
 2  35 ms   5 ms    5 ms  192.168.144.1
 3  7 ms    5 ms    6 ms  133.red-81-41-252.staticip.rima-tde.net [81.41.252.133]
 4  *      *      *      Tiempo de espera agotado para esta solicitud.
 5  *      *      *      Tiempo de espera agotado para esta solicitud.
 6  29 ms   80 ms   30 ms  176.52.253.97
 7  111 ms  58 ms   30 ms  72.14.211.154
 8  42 ms   32 ms   33 ms  172.253.50.39
 9  29 ms   29 ms   29 ms  142.251.51.143
10  30 ms   29 ms   30 ms  mad41s14-in-f3.1e100.net [142.250.200.131]

Traza completa.
```

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA TRACEROUTE

TRACEROUTE O TRACERT MUESTRA TODOS LOS ROUTERS Y CORTAFUEGOS QUE SE HA ENCONTRADO EL PAQUETE DE DATOS HASTA LLEGAR AL DESTINO.

SI EN ALGUNO DE ESTOS OBSTÁCULOS SE PRODUJERA ALGÚN FALLO O HUBIERA UN RETARDO EXCESIVO, PODRÍA COMPROBARSE CON UN SIMPLE VISIONADO DE LOS RESULTADOS OFRECIDOS POR ESTA HERRAMIENTA.

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA PATHPING

PATHPING ES UNA MEZCLA DE PING Y TRACERT.

ES MÁS INFORMATIVO, YA QUE NOS DEVUELVE TAMBIÉN UNA SERIE DE ESTADÍSTICAS, POR LO QUE TARDA MÁS TIEMPO PARA EJECUTAR. DESPUÉS DE ENVIAR LOS PAQUETES A UN DESTINO DETERMINADO, SE ANALIZA LA RUTA TOMADA Y SE CALCULA LA PÉRDIDA DE PAQUETES, PROPORCIONANDO DETALLES ENTRE DOS HOSTS.

MUESTRA LA RUTA A UN HOST TCP/IP Y LAS PÉRDIDAS DE PAQUETES EN CADA ENRUTADOR DEL CAMINO, ADEMÁS DE INFORMACIÓN ACERCA DE LA LATENCIA DE RED Y PÉRDIDAS EN SALTOS INTERMEDIOS ENTRE ORIGEN Y DESTINO.

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA TRACeping

PATHPING ENVÍA VARIOS MENSAJES DE SOLICITUD DE ECO MEDIANTE EL PROTOCOLO ICMP A CADA ENRUTADOR ENTRE UN ORIGEN Y DESTINO DURANTE UN PERÍODO DE TIEMPO Y, A CONTINUACIÓN, CALCULA LOS RESULTADOS EN FUNCIÓN DE LOS PAQUETES DEVUELTOS DESDE CADA ENRUTADOR.

EL MODIFICADOR -N IMPIDE LA RESOLUCIÓN DNS DE LAS DIRECCIONES IP, LO QUE ACELERA LA PRESENTACIÓN DE LOS RESULTADOS.

CON -H ESPECIFICAMOS EL NÚMERO MÁXIMO DE SALTOS PARA LLEGAR AL DESTINO, EL VALOR PREDETERMINADO ES 30 SALTOS.

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA TRACEPING

```
C:\Users\SILVIA MENENDEZ>pathping google.es

Seguimiento de ruta a google.es [142.250.178.163]
sobre un máximo de 30 saltos:
 0  DESKTOP-UVS0NR6 [192.168.1.17]
 1  192.168.1.1
 2  10.195.56.1
 3      *      *      *

Procesamiento de estadísticas durante 50 segundos...
Origen hasta aquí   Este Nodo/Vínculo
Salto  RTT      Perdido/Enviado = Pct  Perdido/Enviado = Pct  Dirección
 0                                     DESKTOP-UVS0NR6 [192.168.1.17]
                                     0/ 100 = 0%  |
 1    9ms      0/ 100 = 0%      0/ 100 = 0%  192.168.1.1
                                     1/ 100 = 1%  |
 2 1131ms     1/ 100 = 1%      0/ 100 = 0%  10.195.56.1
```

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA MTR (MY TRACEROUTE) LINUX

ES UNA HERRAMIENTA DE DIAGNÓSTICO DE RED QUE COMBINA LAS FUNCIONALIDADES DE LOS COMANDOS TRACEROUTE Y PING. SE UTILIZA PARA DIAGNOSTICAR PROBLEMAS DE CONECTIVIDAD EN LA RED, **MOSTRANDO LA RUTA** QUE TOMA UN PAQUETE DESDE EL ORIGEN HASTA UN DESTINO ESPECÍFICO, AL TIEMPO QUE **MIDE LA LATENCIA Y LA TASA DE PÉRDIDA DE PAQUETES** EN CADA SALTO.

CARACTERÍSTICAS DE MTR:

- **MONITOREO CONTINUO:**
- **LATENCIA Y PÉRDIDA DE PAQUETES**
- **INTERFAZ INTERACTIVA**

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA MTR (MY TRACEROUTE) LINUX

-R (REPORT MODE):EJECUTA MTR EN MODO REPORTE, LO QUE SIGNIFICA QUE REALIZA UN NÚMERO FIJO DE PRUEBAS Y LUEGO MUESTRA UN RESUMEN EN LUGAR DE UN MONITOREO CONTINUO.

```
mtr -r example.com
```

-C (COUNT):ESPECIFICA EL NÚMERO DE PRUEBAS QUE MTR DEBE REALIZAR ANTES DE DETENERSE EN MODO REPORTE.

```
mtr -r -c 10 example.com
```

-W (WIDE REPORT):PROPORCIONA UN INFORME MÁS DETALLADO CON MÁS INFORMACIÓN EN CADA COLUMNA.

```
mtr -r -w example.com
```

-I (INTERVAL):ESTABLECE EL INTERVALO DE TIEMPO ENTRE CADA ENVÍO DE PAQUETES.

```
mtr -i 1 example.com
```

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA MTR (MY TRACEROUTE) LINUX

My traceroute

Hostname: 1,00 — + Pause Restart About Quit

Hostname	Loss	Snt	Last	Avg	Best	Worst	StDev
192.168.1.1	0,2%	411	9	6	4	69	5,26
192.168.144.1	3,2%	411	30	8	5	201	11,65
129.red-81-41-252.staticip.rima-tde.net	1,0%	411	7	8	4	118	7,98
???	100,0%	411	0	0	0	0	0,00
???	100,0%	411	0	0	0	0	0,00
176.52.253.97	0,2%	411	47	36	31	118	9,85
81.173.106.65	1,7%	410	32	34	30	108	6,51
192.178.110.75	2,0%	410	32	34	31	207	12,07
142.250.214.41	1,0%	410	34	34	31	132	8,76
mad41s10-in-f3.1e100.net	1,7%	410	33	34	31	158	9,98

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA NETSTAT

PERMITE CONOCER LAS CONEXIONES ESTABLECIDAS EN EL MOMENTO DE SU EJECUCIÓN, INDICANDO PROTOCOLO (TCP), DIRECCIONES EN FORMATO SOCKET DE ORIGEN Y DESTINO Y EL ESTADO DE LA CONEXIÓN.

```
C:\Windows\System32>netstat
```

```
Conexiones activas
```

Proto	Dirección local	Dirección remota	Estado
TCP	127.0.0.1:50288	kubernetes:50289	ESTABLISHED
TCP	127.0.0.1:50289	kubernetes:50288	ESTABLISHED
TCP	127.0.0.1:50290	kubernetes:50291	ESTABLISHED
TCP	127.0.0.1:50291	kubernetes:50290	ESTABLISHED
TCP	192.168.1.38:59503	do-42:https	ESTABLISHED
TCP	192.168.1.38:59517	do-42:https	ESTABLISHED
TCP	192.168.1.38:59556	do-42:https	ESTABLISHED
TCP	192.168.1.38:59579	52.108.80.31:https	ESTABLISHED
TCP	192.168.1.38:59583	192.168.1.40:8009	ESTABLISHED
TCP	192.168.1.38:59585	192.168.1.40:8009	ESTABLISHED

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA NETSTAT

AÑADIENDO EL MODIFICADOR -B PODEMOS VER EL EJECUTABLE ASOCIADO.

CON EL MODIFICADOR DE NETSTAT “INTERVAL”, PODEMOS ESPECIFICAR UN INTERVALO EN SEGUNDOS EN QUE NETSTAT SE EJECUTE DE NUEVO CON LO QUE LA INFORMACIÓN SE REFRESCA Y NOS MUESTRA LOS NUEVOS DATOS, YA QUE POR ESTE COMANDO SÓLO MUESTRA EL RESULTADO EN EL MOMENTO QUE SE REALIZA, ASÍ QUE SERÍA UNA FORMA DE HACERLO MÁS “EN TIEMPO REAL” CUANDO QUEREMOS OBSERVAR QUE SUCEDE CON DETERMINADAS CONEXIONES.

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA WHOIS

WHOIS ES UN PROTOCOLO DE COMUNICACIÓN ENTRE LOS” REGIONAL INTERNET REGISTRIES”, QUE ALMACENAN INFORMACIÓN DE REGISTRO SOBRE DIRECCIONES IP O DOMINIOS. ES UN PROTOCOLO TCP.

A TRAVÉS DE WHOIS PODEMOS OBTENER CIERTA INFORMACIÓN SOBRE LA ORGANIZACIÓN, AUNQUE A DÍA DE HOY POQUITO DEBIDO A LA PROTECCIÓN DE DATOS, AUNQUE EN ALGUNOS CASOS CON SUERTE PUEDES ENCONTRAR INFORMACIÓN SOBRE QUIEN HA REGISTRADO UN DOMINIO, CORREOS, TELÉFONO, ETC.

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA WHOIS

PODEMOS HACER WHOIS A UNA IP O A UN DOMINIO, Y SON COSAS TOTALMENTE DISTINTAS, UNA ES EL REGISTRO DEL DOMINIO Y OTRA ES EL REGISTRO DE LA IP.

EL COMANDO WHOIS **YA NO FUNCIONA EN WINDOWS**, SI EN LINUX, PERO EXISTEN MULTITUD DE APLICACIONES ONLINE QUE NOS FACILITAN ESTA TAREA.

APLICACIONES WEB PARA HACER WHOIS:

- [DOMAINTOOLS.COM](https://www.domaintools.com)
- [ICANN](https://www.icann.org)

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA WHOIS

```
pru@pru-VirtualBox:~$ whois ubuntu.org
Domain Name: UBUNTU.ORG
Registry Domain ID: D4022000000007374261-LROR
Registrar WHOIS Server:
Registrar URL: http://www.naugus.com
Updated Date: 2021-08-04T04:00:14Z
Creation Date: 2018-08-28T14:30:34Z
Registry Expiry Date: 2022-08-28T14:30:34Z
Registrar Registration Expiration Date:
Registrar: Naugus Limited, Inc.
Registrar IANA ID: 899
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Reseller:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant Organization: Domain Privacy Ltd.
Registrant State/Province: MA
Registrant Country: US
Name Server: NS1.PARKLOGIC.COM
Name Server: NS2.PARKLOGIC.COM
Name Server: NS3.PARKLOGIC.COM
Name Server: NS4.PARKLOGIC.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/wicf/)
>>> Last update of WHOIS database: 2022-03-13T04:42:48Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

Access to Public Interest Registry WHOIS information is provided to assist persons in determining the contents of a domain name registration record in the Public Interest Registry registry database. The data in this record is provided by Public Interest Registry for informational purposes only, and Public Interest Registry does not guarantee its accuracy. This service is intended only for query-based access. You agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to (a) allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass unsolicited, commercial advertising or solicitations to entities other than the data recipient's own existing customers; or (b) enable high volume, automated, electronic processes that send queries or data to the systems of Registry Operator, a Registrar, or Afilias except as reasonably necessary to register domain names or modify existing registrations. All rights reserved. Public Interest Registry reserves the right to modify these terms at any time. By submitting this query, you agree to abide by this policy.

The Registrar of Record identified in this output may have an RDNS service that can be queried for additional information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
```

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA NSLOOKUP

LA HERRAMIENTA **NAME SYSTEM LOOKUP** O **NSLOOKUP** SE UTILIZA COMO HERRAMIENTA DE DIAGNÓSTICO PARA LA DETECCIÓN DE PROBLEMAS DE CONFIGURACIÓN EN EL DNS.

ESTA DETECCIÓN LA REALIZA MEDIANTE CONSULTAS A UN SERVIDOR DNS PARA LA OBTENCIÓN DE INFORMACIÓN SOBRE ALGÚN DOMINIO O HOST DE UNA RED DETERMINADA.

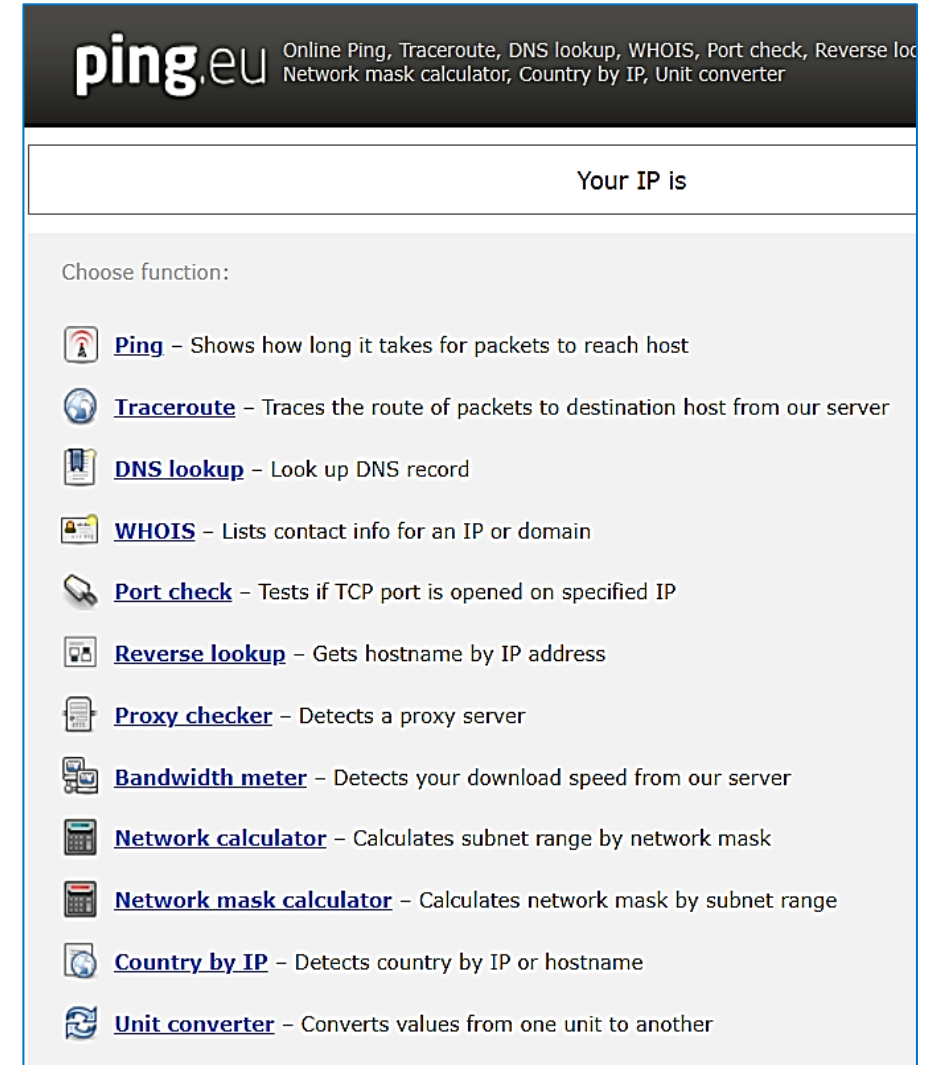
```
pru@pru-VirtualBox:~$ nslookup microsoft.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   microsoft.com
Address: 40.113.200.201
Name:   microsoft.com
Address: 40.112.72.205
Name:   microsoft.com
Address: 104.215.148.63
Name:   microsoft.com
Address: 40.76.4.15
Name:   microsoft.com
Address: 13.77.161.179
```


2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA NSLOOKUP

DISPONEMOS DE HERRAMIENTAS NSLOOKUP ONLINE COMO [PING.EU](https://ping.eu) Y [CENTRALOPS.NET](https://centralops.net), ADEMÁS AMBAS OFRECEN HERRAMIENTAS DE RED ADICIONALES COMO TRACEROUTE Y WHOIS..




The screenshot shows the homepage of **ping.eu**. The header includes the site name and a list of services: Online Ping, Traceroute, DNS lookup, WHOIS, Port check, Reverse lookup, Network mask calculator, Country by IP, and Unit converter. Below the header, there is a section for "Your IP is" and a "Choose function:" section. The "Choose function:" section lists 12 tools with their descriptions:

- Ping** – Shows how long it takes for packets to reach host
- Traceroute** – Traces the route of packets to destination host from our server
- DNS lookup** – Look up DNS record
- WHOIS** – Lists contact info for an IP or domain
- Port check** – Tests if TCP port is opened on specified IP
- Reverse lookup** – Gets hostname by IP address
- Proxy checker** – Detects a proxy server
- Bandwidth meter** – Detects your download speed from our server
- Network calculator** – Calculates subnet range by network mask
- Network mask calculator** – Calculates network mask by subnet range
- Country by IP** – Detects country by IP or hostname
- Unit converter** – Converts values from one unit to another

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA NSLOOKUP

Online service DNS lookup

 **DNS lookup** – Look up DNS record

IP address or host name: Go

Using domain server:
Name:
127.0.0.1

Address:
127.0.0.1#53

Aliases:

google.es has address **142.250.74.163**
google.es has IPv6 address 2a00:1450:400f:805::2003
google.es mail is handled by 0 smtp.google.com.

Other functions:
[Ping](#) | [Traceroute](#) | [DNS lookup](#) | [WHOIS](#) | [Port check](#) | [Reverse lookup](#) | [Proxy checker](#) | [Bandwidth meter](#) |
[Network calculator](#) | [Network mask calculator](#) | [Country by IP](#) | [Unit converter](#)

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA DIG

EL COMANDO QUE PUEDES USAR EN LINUX ES **DIG (DOMAIN INFORMATION GROPER)**.

EJEMPLOS DE USO CON DIG:

DIG XXX.COM

NOS MUESTRA LAS IP, DE TIPO A.

DIG MX XXX.COM

MUESTRA DIRECCIONES IP DE SERVIDORES MX (DE CORREO).

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA IPCONFIG

CON IPCONFIG PODEMOS REALIZAR VARIAS COSAS MEDIANTE SUS MODIFICADORES, PERO LO MÁS HABITUAL ES USARLO PARA CONOCER LA CONFIGURACIÓN TCP/IP DE UNA FORMA SIMPLE SOLO ESCRIBIENDO **IPCONFIG**, NOS DEVUELVE NUESTRA IP, LA MÁSCARA DE RED Y PUERTA DE ENLACE DEL ROUTER, Y CON **IPCONFIG /ALL** VEMOS UNA CONFIGURACIÓN MÁS COMPLETA.

TAMBIÉN NOS PERMITE LIBERAR Y RENOVAR LAS DIRECCIONES IP QUE HAN SIDO ASIGNADAS MEDIANTE UN SERVIDOR DHCP CON LOS MODIFICADORES **/RELEASE**, Y **/RENEW** PARA TODOS LOS ADAPTADORES DE RED O PARA UNO ESPECÍFICO.

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA IPCONFIG

EJEMPLOS:

```
ipconfig
```

MUESTRA INFORMACIÓN TCP/IP DE TODOS LOS ADAPTADORES DE RED.

```
ipconfig /all
```

MUESTRA INFORMACIÓN TCP/IP DETALLADA DE TODOS LOS ADAPTADORES DE RED.

```
ipconfig /renew
```

RENUEVA LA IP DE TODOS LOS ADAPTADORES ASIGNADA MEDIANTE DHCP.

```
ipconfig /renew el*
```

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA IPCONFIG

EJEMPLOS:

```
ipconfig /release *con*
```

LIBERA TODAS LAS CONEXIONES COINCIDENTES, POR EJEMPLO:
“CONEXIÓN CABLEADA ETHERNET 1” O “CONEXIÓN CABLEADA
ETHERNET 2”. SOLO PARA DIRECCIONES IP ASIGNADAS MEDIANTE DHCP.

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA IPCONFIG

WINDOWS ALMACENA LA CACHE DE RESOLUCIÓN DNS, ES DECIR LA RELACIÓN QUE EXISTE ENTRE LAS DIRECCIONES IP Y LOS SITIOS VISITADOS CON SUS NOMBRES DE DOMINIO, DE FORMA PREDETERMINADA SE RENUEVA CADA 24 MINUTOS.

- `ipconfig /displaydns`: MUESTRA EL CONTENIDO DE LA CACHÉ DE RESOLUCIÓN DNS.
- `ipconfig /flushdns`: VACÍA LA MEMORIA CACHÉ DE RESOLUCIÓN DNS.
- `ipconfig /registerdns`: ACTUALIZA TODAS LAS CONCESIONES DHCP Y VUELVE A REGISTRAR LOS NOMBRES DNS.

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA GETMAC (WINDOWS)

OBTIENE LA MAC (DIRECCIÓN FÍSICA) DEL EQUIPO DONDE SE EJECUTA.

ES UN IDENTIFICADOR ÚNICO DE 48 BITS PARA CADA DISPOSITIVO DE RED.
SUS SIGLAS **SIGNIFICAN MEDIA ACCESS CONTROL**.

LAS DIRECCIONES MAC ESTÁN FORMADAS POR 48 BITS REPRESENTADOS GENERALMENTE POR DÍGITOS HEXADECIMALES, COMO CADA HEXADECIMAL EQUIVALE A CUATRO BINARIOS ($48:4=12$), LA DIRECCIÓN ACABA SIENDO FORMADA POR 12 DÍGITOS AGRUPADOS EN SEIS PAREJAS SEPARADAS GENERALMENTE POR DOS PUNTOS, AUNQUE TAMBIÉN PUEDE HABER UN GUION O NADA EN ABSOLUTO.

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA GETMAC

UN EJEMPLO DE DIRECCIÓN MAC PODRÍA SER 00:1E:C2:9E:28:6B.

LA MITAD DE LOS BITS DE UNA DIRECCIÓN MAC, TRES DE LAS SEIS PAREJAS, IDENTIFICAN AL FABRICANTE, Y LA OTRA MITAD AL MODELO.

HAY BUSCADORES ESPECIALIZADOS PARA SABER EL FABRICANTE DE UN DISPOSITIVO DEPENDIENDO DE LOS PRIMEROS SEIS DÍGITOS DE SU MAC:

- [COFFER](#)
- [MACVENDORS](#)

COMO SON IDENTIFICADORES ÚNICOS, LAS MAC PUEDEN SER UTILIZADAS POR UN ADMINISTRADOR DE RED PARA PERMITIR O DENEGAR EL ACCESO DE DETERMINADOS DISPOSITIVOS A UNA RED.

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA ARP

EL COMANDO **ARP** RESULTA ÚTIL PARA VISUALIZAR LA CACHÉ DE RESOLUCIÓN DE DIRECCIONES, CONOCIDA COMO CACHÉ ARP, QUE SON BÁSICAMENTE LOS EQUIPOS CON LOS QUE SE HA COMUNICADO MI EQUIPO EN LA RED (LAN).

MUESTRA Y MODIFICA LAS TABLAS DE TRADUCCIÓN DE DIRECCIONES IP A DIRECCIONES FÍSICAS USADAS POR EL PROTOCOLO DE RESOLUCIÓN DE DIRECCIONES ARP.

EL ADDRESS RESOLUTION PROTOCOL SE DESCRIBE EN LA RFC 826 DONDE EXPLICA CÓMO SE LLEVA A CABO LA RESOLUCIÓN DE DIRECCIONES IPV4 EN DIRECCIONES MAC.

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA ARP

ARP ES IMPRESCINDIBLE PARA LA TRANSMISIÓN DE DATOS EN REDES ETHERNET POR DOS RAZONES: POR UN LADO, LAS TRAMAS DE DATOS (TAMBIÉN TRAMAS ETHERNET) DE LOS PAQUETES IP SOLO PUEDEN ENVIARSE CON AYUDA DE UNA DIRECCIÓN DE HARDWARE A LOS HOSTS DE DESTINO, PERO EL PROTOCOLO IP NO PUEDE OBTENER ESTAS DIRECCIONES FÍSICAS POR SÍ MISMO.

EN CASO DE QUERER AÑADIR LA COMBINACIÓN DE DIRECCIONES DE UN HOST O ELIMINARLA DE LA USAREMOS **-S Y -D**.

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA ARP

SE PUEDE CREAR UNA NUEVA ENTRADA ESTÁTICA CON EL SIGUIENTE COMANDO:

```
arp -s 10.0.2.15 00-AA-00-62-C6-09
```

también SE PUEDE ELIMINAR ESTA INFORMACIÓN DE LA CACHÉ ARP CON -D (DELETE)

```
arp -d 10.0.2.15
```

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA NETSH

NETSH SIGNIFICA SHELL DE RED, PERMITE MODIFICAR, ADMINISTRAR Y DIAGNOSTICAR LA CONFIGURACIÓN DE UNA RED. TENEMOS QUE EJECUTARLO CON PERMISOS DE ADMINISTRADOR EN LA CONSOLA DE COMANDOS (CMD).

NETSH ES UNA APLICACIÓN MUY EXTENSA QUE NOS PERMITE CONFIGURAR EL FIREWALL, ESPECIFICAR RANGOS DE PUERTOS DINÁMICOS TANTO PARA UDP COMO PARA TCP, VER CLAVES WIFI ALMACENADAS, CONFIGURAR EL PROTOCOLO TCP/IP, ENTRE OTRAS MUCHAS ACCIONES.

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA NETSH

EN EL SIGUIENTE EJEMPLO, PODEMOS VER LAS INTERFACES DE RED DEL EQUIPO.

```
netsh interface show interface
```

```
C:\Windows\System32>netsh interface show interface
```

Estado admin.	Estado	Tipo	Nombre interfaz
Habilitado	Conectado	Dedicado	Ethernet 2
Habilitado	Conectado	Dedicado	Ethernet 3
Habilitado	Desconectado	Dedicado	Conexión de área local
Habilitado	Desconectado	Dedicado	ProtonVPN TUN
Habilitado	Conectado	Dedicado	Wi-Fi
Habilitado	Desconectado	Dedicado	Ethernet

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA NETSH

ASIGNAR IP ESTÁTICA A UNA INTERFAZ DE RED

```
netsh interface ipv4 set address "wi-fi"static 192.168.1.40 255.255.255.0 192.168.1.1
```

DONDE:

INTERFACE IPV4 INDICA EL TIPO DE INTERFAZ A CONFIGURAR.

SET ADDRESS «WI-FI»: SELECCIONA LA DIRECCIÓN IP DE LA INTERFAZ LLAMADA EN ESTE CASO «WI-FI».

STATIC: INDICAMOS QUE LA DIRECCIÓN IP SE ASIGNARÁ DE FORMA FIJA O ESTÁTICA APORTANDO LOS VALORES DE IP, MÁSCARA Y PUERTA DE ENLACE DEL ROUTER.

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA NETSH

ASIGNAR IP ESTÁTICA A UNA INTERFAZ DE RED

```
netsh interface ipv4 set address "wi-fi"static 192.168.1.40 255.255.255.0 192.168.1.1
```

CONFIGURACIÓN DE RED DE LA INTERFAZ WI-FI DINÁMICA MEDIANTE DHCP

```
netsh interface ipv4 set address "Wi-Fi" dhcp
```

```
netsh interface ipv4 set dnsservers "Wi-Fi" dhcp
```

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA NETSH

MOSTRAR LA CONFIGURACIÓN SOLO PARA EL INTERFAZ DE NOMBRE WI-FI:

```
netsh interface ipv4 show address Wi-Fi
```

```
netsh interface ipv4 show dns Wi-Fi
```

VER PERFILES DE RED WI-FI

```
netsh wlan show profiles
```

DESPLEGAR LOS PERFILES DE UNA SOLA INTERFAZ

```
netsh wlan show profiles interface="nombre_interfaz"
```


2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA NETSH

CONOCER LA CONFIGURACIÓN DEL ADAPTADOR WI-FI

Conocer en detalle la configuración del controlador es importante en tareas de soporte ya que nos permiten saber con el soporte necesario. Podemos ver detalles específicos tales como nombre, dirección MAC, tipo de red, versión Wi-Fi, canal actual, porcentaje de la señal, velocidad de recepción, etc.

```
netsh wlan show interfaces
```

RECUPERAR CLAVES DE SEGURIDAD DE PERFILES ALMACENADOS

En algunas situaciones es posible que hayamos olvidado la clave de seguridad de un perfil WIFI:

```
netsh wlan show profile name="Perfil" key=clear
```

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA NETSH

BORRAR UN PERFIL DE RED WI-FI

SI TENEMOS ALMACENADOS DIVERSOS PERFILES A LOS QUE YA NO NOS CONECTAMOS, UNA SOLUCIÓN ES ELIMINARLOS PARA EVITAR CONEXIONES FALLIDAS.

```
netsh wlan delete profile name="nombre de perfil".
```

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA HOSTNAME

EL COMANDO HOSTNAME ES MUY SIMPLE Y NO TIENE MODIFICADORES, NOS MUESTRA EL NOMBRE DEL HOST, O LO QUE ES LO MISMO EL NOMBRE DEL EQUIPO.

HERRAMIENTA ROUTE

EL COMANDO ROUTE PERMITE VER Y MODIFICAR LA TABLA DE RUTAS.

ROUTE PRINT MUESTRA TODO EL CONTENIDO DE LA TABLA DE ENRUTAMIENTO IP.

ROUTE ADD SE UTILIZA PARA AÑADIR RUTAS A LA TABLA, Y **ROUTE DELETE** SE UTILIZA PARA BORRAR RUTAS DE LA TABLA.

2. HERRAMIENTAS DEL SISTEMA OPERATIVO

HERRAMIENTA NBTSTAT (WINDOWS)

MUESTRA ESTADÍSTICAS DEL PROTOCOLO Y CONEXIONES TCP/IP ACTUALES UTILIZANDO NBT (NETBIOS SOBRE TCP/IP). NBTSTAT ES UNA HERRAMIENTA QUE RESULTA DE UTILIDAD PARA SOLUCIONAR PROBLEMAS CON LA RESOLUCIÓN DE NOMBRES LLEVADA A CABO POR NETBIOS.

NBTSTAT SE PUEDE USAR EN REDES WIFI PÚBLICAS PARA RECOPIRAR TODAS LAS DIRECCIONES IP Y UTILIZARLAS EN LA FASE DE RECOPIACIÓN DE INFORMACIÓN LLAMADA FOOTPRINTING O EN UN ATAQUE A CUALQUIER DIRECCIÓN IP PÚBLICA, SE PUEDEN USAR PARA ENUMERAR TODAS LAS CONEXIONES TCP/IP EN LA MÁQUINA DE WINDOWS Y PARA SOLUCIONAR PROBLEMAS CON LA RESOLUCIÓN DE NOMBRES.

-N: MUESTRA NOMBRES LOCALES NETBIOS

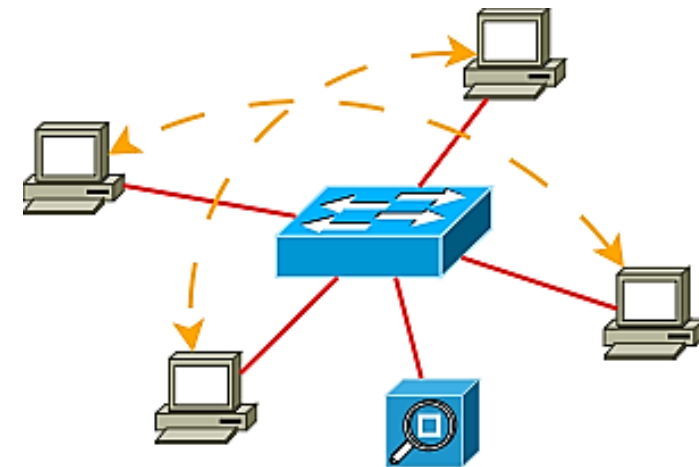
CONTENIDOS

1. INTRODUCCIÓN
2. HERRAMIENTAS DEL SISTEMA OPERATIVO
- 3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS**
4. HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES
5. ANALIZADORES DE PROTOCOLOS
6. ANALIZADORES DE PÁGINAS WEB
7. ATAQUES DE DICCIONARIO Y FUERZA BRUTA

3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS

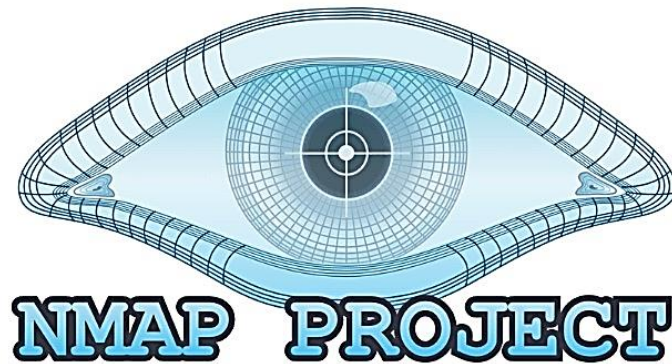
EN LAS TAREAS DE AUDITORÍA DE SEGURIDAD INFORMÁTICA, TAMBIÉN ES ÚTIL CONOCER EL TRÁFICO DE RED DEL SISTEMA DE INFORMACIÓN QUE SE ESTÁ AUDITANDO, ADEMÁS DE LOS PUERTOS Y SERVICIOS QUE SE UTILIZAN CADA VEZ QUE SE TRANSMITEN DATOS E INFORMACIÓN.

LA VARIEDAD DE HERRAMIENTAS CON FUNCIONES DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS ES MUY AMPLIA, SIENDO MUCHAS DE ELLAS GRATUITAS, DE CÓDIGO ABIERTO Y COMPATIBLES CON VARIOS SISTEMAS OPERATIVOS (WINDOWS, LINUX, ETC.).



3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS

DE ESTAS HERRAMIENTAS, CABE DESTACAR NMAP, NETCAT Y NBTSCAN.



```

root@pru-VirtualBox:/home/pru# nbtscan -r 10.0.2.0/24
Doing NBT name scan for addresses from 10.0.2.0/24

```

IP address	NetBIOS Name	Server	User	MAC address
10.0.2.0	Sendto failed: Permission denied			
10.0.2.8	PRU-PC	<server>	<unknown>	08:00:27:eb:5e:83
10.0.2.15	<unknown>	<server>	<unknown>	
10.0.2.12	DESKTOP-0DRKVVA	<server>	<unknown>	08:00:27:aa:b5:04
10.0.2.10	METASPLOITABLE	<server>	METASPLOITABLE	00:00:00:00:00:00
10.0.2.255	Sendto failed: Permission denied			

```

root@pru-VirtualBox:/home/pru#

```

```

$ nc -v -w2 -z 10.0.2.10 1-8000
10.0.2.10: inverse host lookup failed: Unknown host
(UNKNOWN) [10.0.2.10] 6697 (ircs-u) open
(UNKNOWN) [10.0.2.10] 6667 (ircd) open
(UNKNOWN) [10.0.2.10] 6000 (x11) open
(UNKNOWN) [10.0.2.10] 5900 (?) open
(UNKNOWN) [10.0.2.10] 5432 (postgresql) open
(UNKNOWN) [10.0.2.10] 3632 (distcc) open
(UNKNOWN) [10.0.2.10] 3306 (mysql) open
(UNKNOWN) [10.0.2.10] 2121 (iprop) open
(UNKNOWN) [10.0.2.10] 2049 (nfs) open
(UNKNOWN) [10.0.2.10] 1524 (ingreslock) open
(UNKNOWN) [10.0.2.10] 1099 (rmiregistry) open
(UNKNOWN) [10.0.2.10] 514 (shell) open
(UNKNOWN) [10.0.2.10] 513 (login) open
(UNKNOWN) [10.0.2.10] 512 (exec) open
(UNKNOWN) [10.0.2.10] 445 (microsoft-ds) open
(UNKNOWN) [10.0.2.10] 139 (netbios-ssn) open
(UNKNOWN) [10.0.2.10] 111 (sunrpc) open
(UNKNOWN) [10.0.2.10] 80 (http) open
(UNKNOWN) [10.0.2.10] 53 (domain) open
(UNKNOWN) [10.0.2.10] 25 (smtp) open
(UNKNOWN) [10.0.2.10] 23 (telnet) open
(UNKNOWN) [10.0.2.10] 22 (ssh) open
(UNKNOWN) [10.0.2.10] 21 (ftp) open

```


3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS

HERRAMIENTA NMAP

LA APLICACIÓN **NMAP** ES GRATUITA Y DE CÓDIGO ABIERTO Y SE UTILIZA PRINCIPALMENTE PARA LA EVALUACIÓN DE LA SEGURIDAD DE SISTEMAS DE INFORMACIÓN.

EL OBJETIVO Y LA UTILIDAD PRINCIPAL DE LA HERRAMIENTA **NMAP** ES EL *DESCUBRIMIENTO E IDENTIFICACIÓN DE POSIBLES APLICACIONES Y EQUIPOS NO AUTORIZADOS EN EL SISTEMA DE INFORMACIÓN.*

SE TRATA DE UNA HERRAMIENTA BASTANTE UTILIZADA PARA PREPARAR ATAQUES (A LOS DISPOSITIVOS DETECTADOS) QUE PUEDEN TENER EFECTOS PERJUDICIALES EN EL SISTEMA DE INFORMACIÓN.

3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS

HERRAMIENTA NMAP

SU FUNCIÓN PRINCIPAL ES EL **RASTREO DE PUERTOS** A TRAVÉS DE TAREAS COMO:

- 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. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS

HERRAMIENTA 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. CABE DESTACAR TAMBIÉN OTRAS FUNCIONES COMO:

- **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.

3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS

HERRAMIENTA NETCAT

- 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.

3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS

HERRAMIENTA NETCAT

LA LÍNEA BÁSICA DE COMANDOS PARA NETCAT ES:

NC [PARÁMETROS] [IP O PUERTO/RANGO DE PUERTOS QUE SE QUIEREN ANALIZAR]

ENTRE LOS PARÁMETROS DE NETCAT CABE DESTACAR LOS QUE SE MUESTRAN EN LA SIGUIENTE TABLA.

Parámetro	Descripción
-d	Permite que Netcat actúe en modo silencioso.
-l	Activa el modo escucha.
-p puerto	Especifica el puerto que se quiere analizar.
-v	Facilita información sobre la conexión.
-u	Indica a Netcat que utilice el protocolo UDP en lugar del TCP (protocolo utilizado por defecto).
-i segundos	Define un retraso (delay) de tiempo antes de enviar o recibir datos.
-w segundos	Controla cuánto tiempo debe esperar Netcat antes de terminar una conexión.
-r	Permite a Netcat elegir aleatoriamente los puertos locales y remotos.
-z	Escanea puertos.

EN LA SIGUIENTE IMAGEN, SE MUESTRA UN EJEMPLO DE NETCAT (NCAT):

3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS

HERRAMIENTA NETCAT

```
$ nc -v -w2 -z 10.0.2.10 1-8000
10.0.2.10: inverse host lookup failed: Unknown host
(UNKNOWN) [10.0.2.10] 6697 (ircs-u) open
(UNKNOWN) [10.0.2.10] 6667 (ircd) open
(UNKNOWN) [10.0.2.10] 6000 (x11) open
(UNKNOWN) [10.0.2.10] 5900 (?) open
(UNKNOWN) [10.0.2.10] 5432 (postgresql) open
(UNKNOWN) [10.0.2.10] 3632 (distcc) open
(UNKNOWN) [10.0.2.10] 3306 (mysql) open
(UNKNOWN) [10.0.2.10] 2121 (iprop) open
(UNKNOWN) [10.0.2.10] 2049 (nfs) open
(UNKNOWN) [10.0.2.10] 1524 (ingreslock) open
(UNKNOWN) [10.0.2.10] 1099 (rmiregistry) open
(UNKNOWN) [10.0.2.10] 514 (shell) open
(UNKNOWN) [10.0.2.10] 513 (login) open
(UNKNOWN) [10.0.2.10] 512 (exec) open
(UNKNOWN) [10.0.2.10] 445 (microsoft-ds) open
(UNKNOWN) [10.0.2.10] 139 (netbios-ssn) open
(UNKNOWN) [10.0.2.10] 111 (sunrpc) open
(UNKNOWN) [10.0.2.10] 80 (http) open
(UNKNOWN) [10.0.2.10] 53 (domain) open
(UNKNOWN) [10.0.2.10] 25 (smtp) open
(UNKNOWN) [10.0.2.10] 23 (telnet) open
(UNKNOWN) [10.0.2.10] 22 (ssh) open
(UNKNOWN) [10.0.2.10] 21 (ftp) open
```


3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS

HERRAMIENTA DE RED 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. NO OBSTANTE, NO ES UNA APLICACIÓN DE CÓDIGO LIBRE, YA QUE SU CREADOR NO HA PUBLICADO SU CÓDIGO FUENTE. DEL MISMO MODO QUE NETCAT.

3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS

HERRAMIENTA DE RED NBTSCAN

TAMBIÉN OFRECE MULTITUD DE FUNCIONALIDADES, DESTACANDO:

- ESCANEEO 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.

3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS

HERRAMIENTA DE RED NBTSCAN

SU FUNCIONAMIENTO BÁSICO ES BASTANTE SIMPLE: SE ENVÍAN PETICIONES DE ESTADOS DE NETBIOS A UNA DIRECCIÓN O A UN RANGO DE ESTAS Y PARA CADA SERVIDOR QUE RESPONDE SE OBTIENE LA SIGUIENTE INFORMACIÓN:

- SU DIRECCIÓN.
- SU NOMBRE NETBIOS.
- EL NOMBRE DE USUARIO CON LA SESIÓN INICIADA EN EL EQUIPO.
- SU DIRECCIÓN MAC.

EN LA SIGUIENTE IMAGEN, SE MUESTRA LA UTILIZACIÓN DEL COMANDO DE LA HERRAMIENTA NBTSCAN JUNTO CON SUS POSIBLES PARÁMETROS.

3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS

HERRAMIENTA DE RED NBTSCAN

```

root@pru-VirtualBox:/home/pru# nbtscan -r 10.0.2.0/24
Doing NBT name scan for addresses from 10.0.2.0/24

```

IP address	NetBIOS Name	Server	User	MAC address
10.0.2.0	Sendto failed: Permission denied			
10.0.2.8	PRU-PC	<server>	<unknown>	08:00:27:eb:5e:83
10.0.2.15	<unknown>		<unknown>	
10.0.2.12	DESKTOP-0DRKVVA	<server>	<unknown>	08:00:27:aa:b5:04
10.0.2.10	METASPLOITABLE	<server>	METASPLOITABLE	00:00:00:00:00:00
10.0.2.255	Sendto failed: Permission denied			

```

root@pru-VirtualBox:/home/pru#

```

3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS

HERRAMIENTA DE RED ADVANCED PORT SCANNER

ES UN EXPLORADOR DE REDES GRATUITO QUE PERMITE ENCONTRAR CON RAPIDEZ LOS PUERTOS ABIERTOS DE LOS EQUIPOS CONECTADOS A LA RED E IDENTIFICAR LAS VERSIONES DE LOS PROGRAMAS QUE SE ESTÁN EJECUTANDO EN LOS PUERTOS DETECTADOS.

EL PROGRAMA CUENTA CON UNA INTERFAZ MUY INTUITIVA Y UNA GRAN VARIEDAD DE FUNCIONALIDADES.

ADVANCED PORT SCANNER



ADVANCED PORT SCANNER

3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS

HERRAMIENTA DE RED NETSCANTOOLS

UNA HERRAMIENTA CON MÚLTIPLES UTILIDADES PARA DIFERENTES PROTOCOLOS, ICMP, ARP, SNMP, DNS, ENTRE OTROS.

- ESCANEA PUERTOS USANDO DIFERENTES MÉTODOS:
- CONEXIÓN COMPLETA TCP.
- TCP SYN SEMIABIERTO.
- UDP ICMP.
- TCP / UDP ICMP.
- COMBINANDO LAS FLAGS SYN, URG, PSH, FIN, ACK, RST..

NETSCANTOOLS



3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS

HERRAMIENTA DE RED ANGRY IP SCANNER

DEMÁS DE ESCANEAR PUERTOS TAMBIÉN ES CAPAZ DE BUSCAR INFORMACIÓN NETBIOS, DIRECCIONES IP, DETECTAR SERVIDORES WEB, ETC.

LOS RESULTADOS DEL ESCANEO SE PUEDEN GUARDAR EN CSV, TXT O XML.

ANGRY IP SCANNER



3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS

OTRAS HERRAMIENTAS DE RED: SNORT Y NETWORK MINER

SNORT

ES UNA DE LAS HERRAMIENTAS MÁS UTILIZADAS PARA DETECTAR INTRUSIONES EN LA RED, Y ES FRECUENTEMENTE UTILIZADA COMO ANALIZADOR.

DISPONE DE UN MOTOR BASTANTE POTENTE PARA LA DETECCIÓN DE INTRUSIONES, ATAQUES Y REALIZAR ESCANEOS DE PUERTOS PARA REGISTRAR TODOS LOS EVENTOS DESTACABLES Y GENERAR ALERTAS EN AQUELLOS EVENTOS QUE SUPONGAN UN PELIGRO PARA EL SISTEMA DE INFORMACIÓN.



3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS

OTRAS HERRAMIENTAS DE RED: SNORT Y NETWORK MINER

NETWORK MINER

ES ACTUALMENTE UNA DE LAS HERRAMIENTAS MÁS UTILIZADAS PARA EL ANÁLISIS FORENSE DIGITAL.

SU FUNCIONAMIENTO CONSISTE EN LA CAPTURA Y ANÁLISIS DE LOS PAQUETES DE DATOS QUE CIRCULAN POR UNA RED LOCAL (O RED LAN).



CONTENIDOS

1. INTRODUCCIÓN
2. HERRAMIENTAS DEL SISTEMA OPERATIVO
3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS
- 4. HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES**
5. ANALIZADORES DE PROTOCOLOS
6. ANALIZADORES DE PÁGINAS WEB
7. ATAQUES DE DICCIONARIO Y FUERZA BRUTA

4. HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES

LAS HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES SE UTILIZAN PARA CONOCER LAS VULNERABILIDADES DE UN SISTEMA DE INFORMACIÓN.

SE UTILIZAN SOBRE TODO EN LAS **AUDITORÍAS DE SEGURIDAD INFORMÁTICA**, YA QUE PERMITEN DESCUBRIR LOS PUNTOS DÉBILES DEL SISTEMA Y PROPONER MEDIDAS CORRECTIVAS QUE CUBRAN LAS VULNERABILIDADES.



4. HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES

LOS ESCÁNERES DE VULNERABILIDADES SE DISTINGUEN SEGÚN EL ELEMENTO QUE ESCANEAN PARA DETECTARLO, DISTINGUIENDO ENTRE:

- **ESCÁNER DE RED:** SE UTILIZA PARA ENCONTRAR VULNERABILIDADES DE UNA RED DE UN SISTEMA DE INFORMACIÓN.
- **ESCÁNER DE PUERTO:** BUSCA LOS PUERTOS ABIERTOS DE UNA RED QUE PUEDAN SER UTILIZADOS POR INTRUSOS COMO VÍAS DE ENTRADA.
- **ESCÁNER PARA LA SEGURIDAD DE APLICACIONES WEB:** DETECTA E IDENTIFICA LAS VULNERABILIDADES DE LAS APLICACIONES WEB PARA ESTIMAR SU RIESGO Y PODER MITIGARLO.

4. HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES

- **ESCÁNER DE BASE DE DATOS:** DETECTA VULNERABILIDADES DE LAS BASES DE DATOS, PROTEGIENDO UNO DE LOS ACTIVOS MÁS IMPORTANTES DE UNA ORGANIZACIÓN, LA INFORMACIÓN.

ENTRE LAS HERRAMIENTAS EXISTENTES ESTÁN: **NESSUS, METASPLOIT, BURP SUITE, ARMITAGE, NMAP (SCRIPTS NSE), AIRCRACK-NG, OPENVAS,**

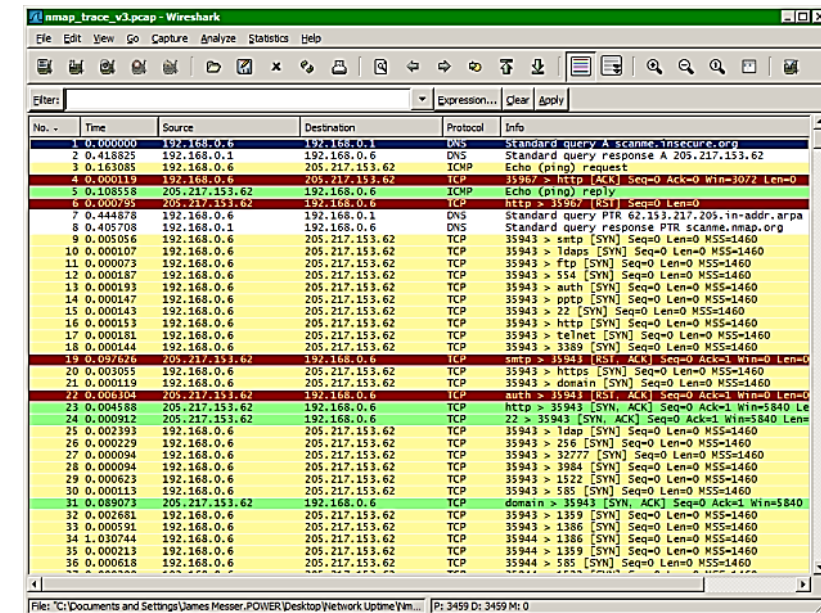
CONTENIDOS

1. INTRODUCCIÓN
2. HERRAMIENTAS DEL SISTEMA OPERATIVO
3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS
4. HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES
- 5. ANALIZADORES DE PROTOCOLOS**
6. ANALIZADORES DE PÁGINAS WEB
7. ATAQUES DE DICCIONARIO Y FUERZA BRUTA

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.

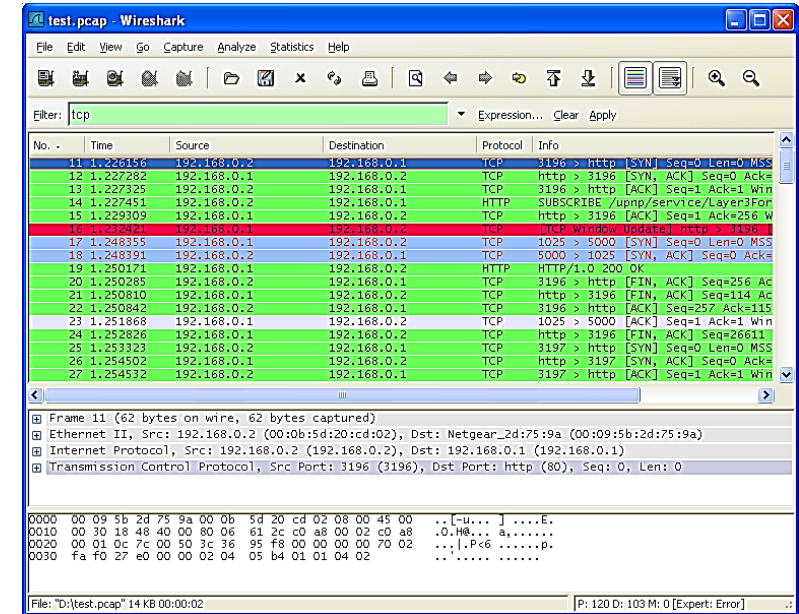


No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.6	192.168.0.1	DNS	Standard query A scanme.insecure.org
2	0.418825	192.168.0.1	192.168.0.6	DNS	Standard query response A 205.217.153.62
3	0.163085	192.168.0.6	205.217.153.62	ICMP	Echo (ping) request
4	0.000119	192.168.0.6	205.217.153.62	TCP	35943 > http [ACK] Seq=0 Ack=0 Win=1072 Len=0
5	0.108558	205.217.153.62	192.168.0.6	ICMP	Echo (ping) reply
6	0.000795	205.217.153.62	192.168.0.6	TCP	http > 3596 [RST] Seq=0 Len=0
7	0.444878	192.168.0.6	192.168.0.1	DNS	Standard query PTR 62.153.217.205.in-addr.arpa
8	0.405708	192.168.0.1	192.168.0.6	DNS	Standard query response PTR scanme.nmap.org
9	0.005056	192.168.0.6	205.217.153.62	TCP	35943 > smtp [SYN] Seq=0 Len=0 MSS=1460
10	0.000107	192.168.0.6	205.217.153.62	TCP	35943 > ldaps [SYN] Seq=0 Len=0 MSS=1460
11	0.000073	192.168.0.6	205.217.153.62	TCP	35943 > ftp [SYN] Seq=0 Len=0 MSS=1460
12	0.000187	192.168.0.6	205.217.153.62	TCP	35943 > 554 [SYN] Seq=0 Len=0 MSS=1460
13	0.000193	192.168.0.6	205.217.153.62	TCP	35943 > auth [SYN] Seq=0 Len=0 MSS=1460
14	0.000147	192.168.0.6	205.217.153.62	TCP	35943 > pptp [SYN] Seq=0 Len=0 MSS=1460
15	0.000143	192.168.0.6	205.217.153.62	TCP	35943 > 22 [SYN] Seq=0 Len=0 MSS=1460
16	0.000153	192.168.0.6	205.217.153.62	TCP	35943 > http [SYN] Seq=0 Len=0 MSS=1460
17	0.000181	192.168.0.6	205.217.153.62	TCP	35943 > telnet [SYN] Seq=0 Len=0 MSS=1460
18	0.000144	192.168.0.6	205.217.153.62	TCP	35943 > 3389 [SYN] Seq=0 Len=0 MSS=1460
19	0.000200	205.217.153.62	192.168.0.6	TCP	http > 35943 [RST] Seq=0 Ack=0 Len=0
20	0.003055	192.168.0.6	205.217.153.62	TCP	35943 > https [SYN] Seq=0 Len=0 MSS=1460
21	0.000119	192.168.0.6	205.217.153.62	TCP	35943 > domain [SYN] Seq=0 Len=0 MSS=1460
22	0.006104	205.217.153.62	192.168.0.6	TCP	auth > 35943 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
23	0.004588	205.217.153.62	192.168.0.6	TCP	http > 35943 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
24	0.000912	205.217.153.62	192.168.0.6	TCP	22 > 35943 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
25	0.002393	192.168.0.6	205.217.153.62	TCP	35943 > ldap [SYN] Seq=0 Len=0 MSS=1460
26	0.000229	192.168.0.6	205.217.153.62	TCP	35943 > 256 [SYN] Seq=0 Len=0 MSS=1460
27	0.000094	192.168.0.6	205.217.153.62	TCP	35943 > 32777 [SYN] Seq=0 Len=0 MSS=1460
28	0.000094	192.168.0.6	205.217.153.62	TCP	35943 > 3884 [SYN] Seq=0 Len=0 MSS=1460
29	0.000623	192.168.0.6	205.217.153.62	TCP	35943 > 1522 [SYN] Seq=0 Len=0 MSS=1460
30	0.000113	192.168.0.6	205.217.153.62	TCP	35943 > 585 [SYN] Seq=0 Len=0 MSS=1460
31	0.000073	205.217.153.62	192.168.0.6	TCP	domain > 35943 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
32	0.002451	192.168.0.6	205.217.153.62	TCP	35943 > 1359 [SYN] Seq=0 Len=0 MSS=1460
33	0.000591	192.168.0.6	205.217.153.62	TCP	35943 > 1386 [SYN] Seq=0 Len=0 MSS=1460
34	1.030744	192.168.0.6	205.217.153.62	TCP	35944 > 1386 [SYN] Seq=0 Len=0 MSS=1460
35	0.000213	192.168.0.6	205.217.153.62	TCP	35944 > 1359 [SYN] Seq=0 Len=0 MSS=1460
36	0.000618	192.168.0.6	205.217.153.62	TCP	35944 > 585 [SYN] Seq=0 Len=0 MSS=1460

5. ANALIZADORES DE PROTOCOLOS

UN ANALIZADOR DE PROTOCOLOS SE UTILIZA EN AUDITORÍAS DE SEGURIDAD, YA QUE TRATA DE IDENTIFICAR FALLOS O PROBLEMAS ANALIZANDO PAQUETES DE DATOS QUE SE TRANSMITEN EN LA RED.

GENERA INFORMES Y ESTADÍSTICAS QUE PERMITEN OBTENER UNA VISIÓN GLOBAL DEL FUNCIONAMIENTO DE LA RED.

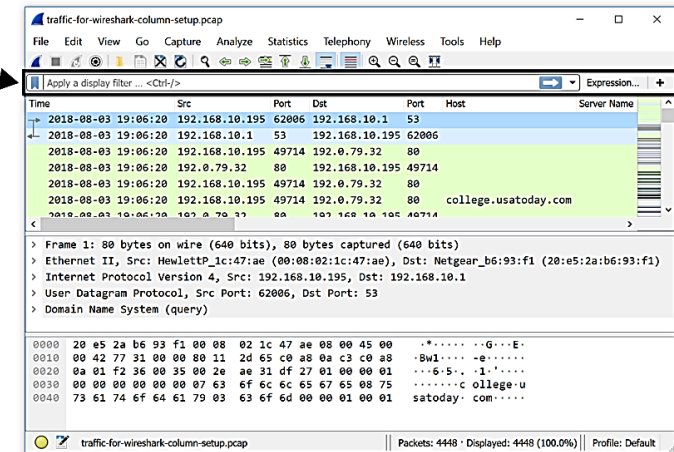


5. ANALIZADORES DE PROTOCOLOS

ALGUNOS DE LOS DATOS QUE FACILITAN ESTAS HERRAMIENTAS SON:

- COMPONENTES DEFECTUOSOS DE LA RED.
- ERRORES DE CONFIGURACIÓN.
- ERRORES DE CONEXIÓN.
- PROBLEMAS DE PROTOCOLO.
- TRÁFICO DE DATOS INUSUAL EN EL SERVIDOR DE LA RED.
- APLICACIONES QUE PUEDEN ENTRAR EN CONFLICTO.
- FLUCTUACIONES DEL TRÁFICO DE DATOS DE LA RED.
- MONITORIZACIÓN DE UNA O VARIAS REDES.

Display
filter →



5. ANALIZADORES DE PROTOCOLOS

ENTRE LAS HERRAMIENTAS EXISTENTES ESTÁN: **WIRESHARK, SOLARWINDS, PAESSLER PRTG, MANAGEENGINE, NETFLOW ANALYZER, TCPDUMP, WINDUMP, NETWORKMINER, COLASOFT CAPSA, TELERIK FIDDLER, KISMET**



5. ANALIZADORES DE PROTOCOLOS

ANALIZADOR DE PROTOCOLOS WIRESHARK

SE TRATA DE UNA HERRAMIENTA QUE SE GESTIONA A TRAVÉS DE UNA INTERFAZ GRÁFICA.

PERMITE IDENTIFICAR Y ANALIZAR EL TRÁFICO DE RED EN UN MOMENTO DETERMINADO Y ENTRE SUS CARACTERÍSTICAS PRINCIPALES DESTACAN:

- PERMITE ANALIZAR MÁS DE 480 PROTOCOLOS.
- CAPTURA DIRECTAMENTE LOS PAQUETES DE DATOS DESDE UNA INTERFAZ DE RED.
- CON EL ANÁLISIS DEL PAQUETE CAPTURADO, SE OBTIENE INFORMACIÓN DEL PROTOCOLO UTILIZADO.

5. ANALIZADORES DE PROTOCOLOS

ANALIZADOR DE PROTOCOLOS WIRESHARK

- PERMITE IMPORTAR Y/O EXPORTAR LOS PAQUETES DE DATOS CAPTURADOS A OTRAS APLICACIONES.
- FILTRA LOS PAQUETES DE DATOS ATENDIENDO A UNOS CRITERIOS DEFINIDOS POR EL USUARIO.
- OFRECE ESTADÍSTICAS DEL TRÁFICO DE RED.
- ES UNA HERRAMIENTA GRATUITA.
- SE PUEDE UTILIZAR EN VARIOS SISTEMAS OPERATIVOS COMO WINDOWS, LINUX, UNIX, ETC.

CONTENIDOS

1. INTRODUCCIÓN
2. HERRAMIENTAS DEL SISTEMA OPERATIVO
3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS
4. HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES
5. ANALIZADORES DE PROTOCOLOS
- 6. ANALIZADORES DE PÁGINAS WEB**
7. ATAQUES DE DICCIONARIO Y FUERZA BRUTA

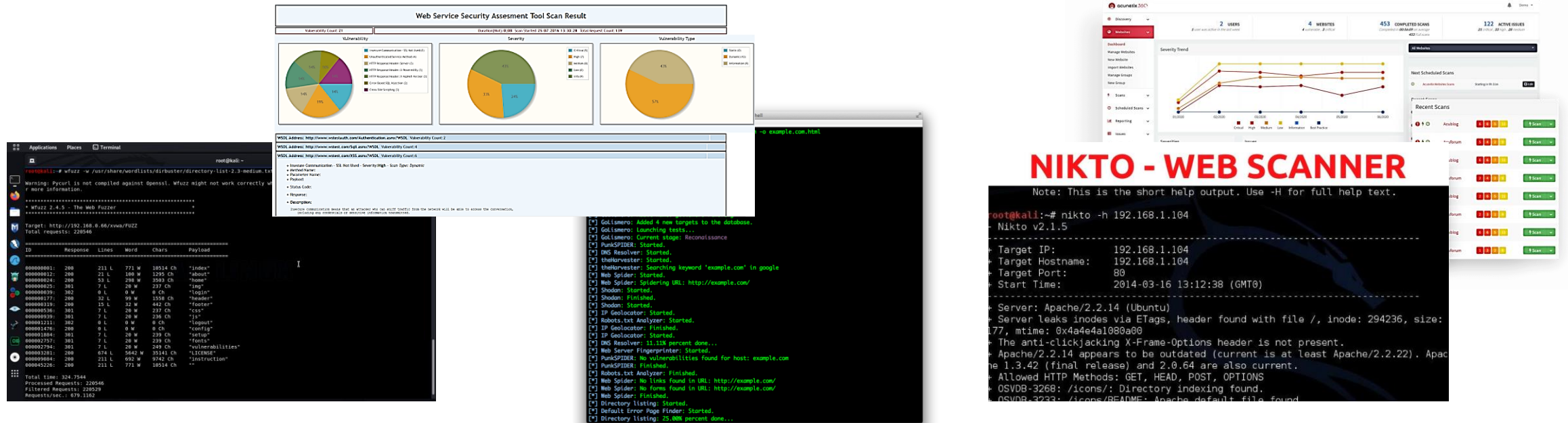
6. ANALIZADORES DE PÁGINAS WEB

LOS ANALIZADORES DE VULNERABILIDADES DE PÁGINAS WEB REALIZAN PRUEBAS EN SITIOS WEB O EN APLICACIONES WEB PARA DETECTAR SUS FALLOS Y VULNERABILIDADES Y EVITAR POSIBLES ATAQUES DE SEGURIDAD.

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.

6. ANALIZADORES DE PÁGINAS WEB

ENTRE LAS HERRAMIENTAS EXISTENTES ESTÁN: ACUNETIX, ARACHNI, XSSPY, W3AF, NIKTO, WFUZZ, OWASP ZAP, WAPITI, VEGA, SQLMAP, GRABBER, GOLISMERO



CONTENIDOS

1. INTRODUCCIÓN
2. HERRAMIENTAS DEL SISTEMA OPERATIVO
3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS
4. HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES
5. ANALIZADORES DE PROTOCOLOS
6. ANALIZADORES DE PÁGINAS WEB
- 7. ATAQUES DE DICCIONARIO Y FUERZA BRUTA**

7. ATAQUES DE DICCIONARIO Y FUERZA BRUTA

OTRAS HERRAMIENTAS UTILIZADAS FRECUENTEMENTE EN LAS AUDITORÍAS DE SEGURIDAD INFORMÁTICA SON AQUELLAS RELACIONADAS CON EL DESCUBRIMIENTO DE CONTRASEÑAS.

SI LA APLICACIÓN ES CAPAZ DE DESCUBRIR UNA CONTRASEÑA CON FACILIDAD, HAY MÁS RIESGO DE SUFRIR ATAQUES Y, POR TANTO, SERÁ NECESARIA UNA NUEVA CONTRASEÑA CON MÁS COMPLEJIDAD.

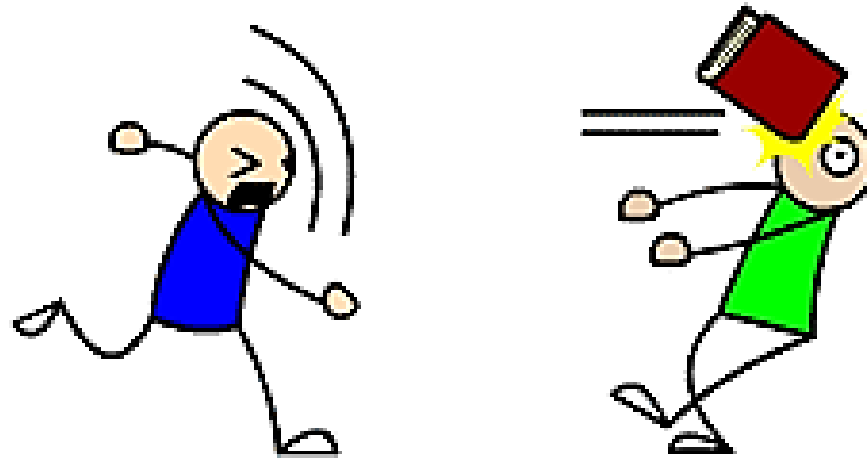


7. ATAQUES DE DICCIONARIO Y FUERZA BRUTA

LAS TÉCNICAS DE DESCUBRIMIENTO DE CONTRASEÑAS SE CLASIFICAN EN:

- ATAQUES DE FUERZA BRUTA
- ATAQUES DE DICCIONARIO

DICTIONARY ATTACK!



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.

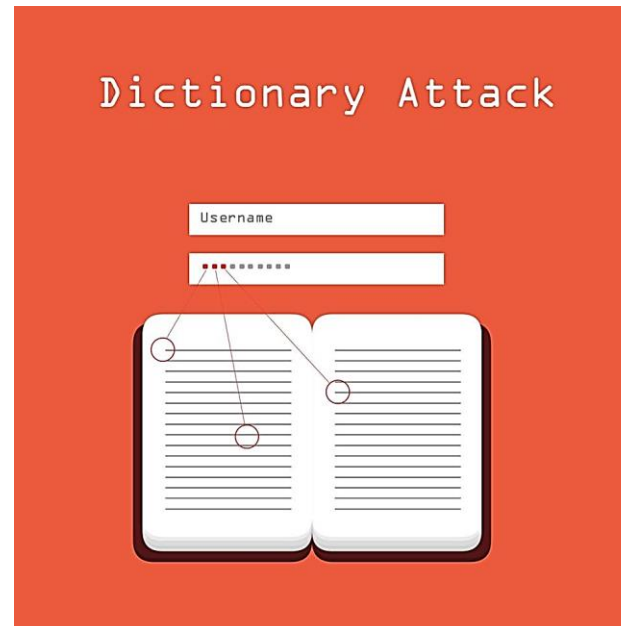
AL SER MUY NUMEROSAS LAS POSIBLES COMBINACIONES, ESTE TIPO DE ATAQUES SON MUY COSTOSOS Y CONLLEVAN BASTANTE TIEMPO HASTA QUE SE DESCUBRE LA CONTRASEÑA CORRECTA.

```
162.158.102.78 - - [04/Apr/2016:19:46:36 +0300] "POST /wp-login.php HTTP/1.0" 200 1526
3.0.04506.648; .NET CLR 3.5.21022)"
162.158.102.78 - - [04/Apr/2016:19:46:36 +0300] "POST /wp-login.php HTTP/1.0" 200 1526
3.0.04506.648; .NET CLR 3.5.21022)"
162.158.102.78 - - [04/Apr/2016:19:46:37 +0300] "POST /wp-login.php HTTP/1.0" 200 1526
3.0.04506.648; .NET CLR 3.5.21022)"
162.158.102.78 - - [04/Apr/2016:19:46:37 +0300] "POST /wp-login.php HTTP/1.0" 200 1526
3.0.04506.648; .NET CLR 3.5.21022)"
```

7. ATAQUES DE DICCIONARIO Y FUERZA BRUTA

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.



7. ATAQUES DE DICCIONARIO Y FUERZA BRUTA

CUANDO SE UTILIZAN CONTRASEÑAS COMPLEJAS LOS ATAQUES DE DICCIONARIO SON POCO EFECTIVOS, YA QUE DIFÍCILMENTE UNA CONTRASEÑA CON TODOS ESTOS ELEMENTOS ESTARÁ CONTENIDA EN ALGÚN DICCIONARIO.

EN ESTOS CASOS, SE RECOMIENDA EJECUTAR ATAQUES DE FUERZA BRUTA, AUNQUE CONLLEVEN MAYORES COSTES.

ENTRE LAS HERRAMIENTAS EXISTENTES ESTÁN: **GOBUSTER, BRUTEX, DIRSEARCH, CALLOW, SSB, THC-HYDRA, BURP SUITE, PATATOR, PYDICTOR, NCRACK, HASHCAT**

CONTENIDOS

1. INTRODUCCIÓN
2. HERRAMIENTAS DEL SISTEMA OPERATIVO
3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS
4. HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES
5. ANALIZADORES DE PROTOCOLOS
6. ANALIZADORES DE PÁGINAS WEB
7. ATAQUES DE DICCIONARIO Y FUERZA BRUTA

RESUMEN

EN LA AUDITORÍA DE SISTEMAS, FRECUENTEMENTE SE UTILIZAN HERRAMIENTAS QUE AYUDEN EN LA DETECCIÓN DE FALLOS Y VULNERABILIDADES QUE PERMITAN ESTIMAR EL RIESGO DEL SISTEMA DE INFORMACIÓN Y FORMULAR MEDIDAS CORRECTIVAS Y CONTROLES.

POR UNA PARTE, DENTRO DEL MISMO SISTEMA OPERATIVO DE LOS EQUIPOS SE ENCUENTRAN VARIAS HERRAMIENTAS DE AUDITORÍA, COMO **PING** O **TRACERROUTE**, QUE PERMITEN DETECTAR FALLOS Y ANOMALÍAS EN SU RED.

ADEMÁS, SE RECOMIENDA QUE EL AUDITOR DISPONGA DE HERRAMIENTAS QUE **ANALICEN LA RED, LOS PUERTOS Y LOS SERVICIOS** CONFIGURADOS EN ESTA PARA DETECTAR POSIBLES VÍAS DE ENTRADA DE INTRUSOS Y TRÁFICO DE RED INUSUAL QUE OFREZCA INDICIOS DE AMENAZA. EJEMPLOS DE ESTAS HERRAMIENTAS SON **NETCAT, NMAP Y NBTSCAN**.

TAMBIÉN SIRVEN PARA EVALUAR LA SEGURIDAD DE UNA RED **LOS ANALIZADORES DE PROTOCOLOS**, QUE ANALIZAN PAQUETES DE DATOS QUE SE TRANSMITEN EN LA RED PARA DETECTAR ERRORES DE CONFIGURACIÓN, DE CONEXIÓN, ETC.

RESUMEN

OTRA HERRAMIENTA FUNDAMENTAL Y DE GRAN UTILIDAD PARA EL AUDITOR ES **UN ANALIZADOR DE VULNERABILIDADES** CAPAZ DE IDENTIFICARLAS, EMITIR INFORMES CON LOS RESULTADOS OBTENIDOS Y FORMULAR PROPUESTAS DE SOLUCIÓN.

POR OTRA PARTE Y A NIVEL EXTERNO, EXISTEN LOS **ANALIZADORES DE PÁGINAS WEB**, CUYA FUNCIÓN PRINCIPAL ES CONOCER LA ESTRUCTURA DE LOS SITIOS WEB Y DETECTAR SUS VULNERABILIDADES PARA EVITAR QUE SUFRAN ATAQUES DE SEGURIDAD.

ESTAS HERRAMIENTAS, JUNTO CON LAS **HERRAMIENTAS DE ATAQUES DE DICCIONARIO Y FUERZA BRUTA**, SIRVEN PARA QUE EL AUDITOR DETECTE VÍAS DE ATAQUE E INTRUSIONES, QUE DEBERÁN SER SOLUCIONADAS PARA DISMINUIR EL RIESGO DEL SISTEMA DE INFORMACIÓN Y DE LA ORGANIZACIÓN EN GENERAL.

