IFCT0109. SEGURIDAD INFORMÁTICA

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

UD07

IDENTIFICACIÓN DE SERVICIOS

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN
3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS
4. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE TRÁFICO DE COMUNICACIONES PARA DETERMINAR EL USO REAL QUE HACEN LOS SISTEMAS DE INFORMACIÓN DE LOS DISTINTOS PROTOCOLOS, SERVICIOS Y PUERTOS

1. INTRODUCCIÓN

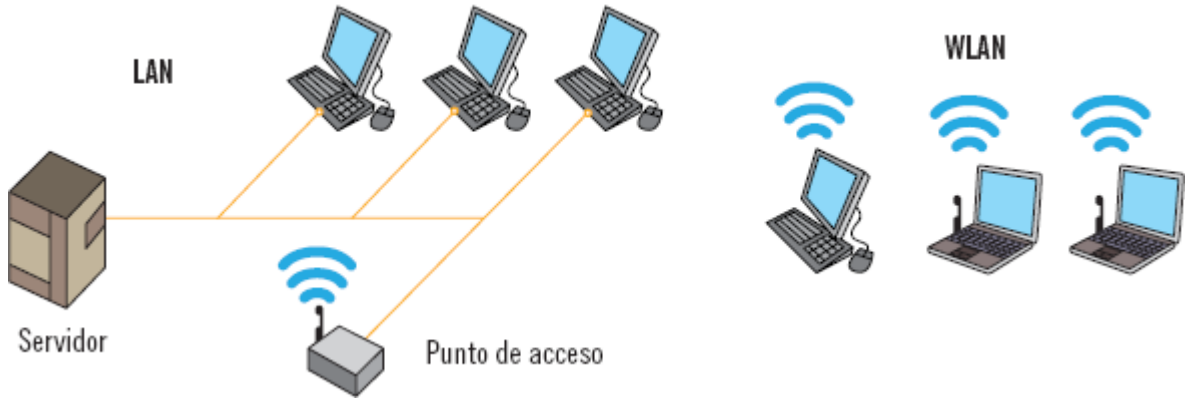
UNA EXTENSA ÁREA DE LA **SI** ES LA SEGURIDAD LÓGICA, ABORDANDO LA PROBLEMÁTICA DEL ACCESO LÓGICO.

EL PERÍMETRO DE LOS ACTIVOS SE EXTIENDE CON EL USO DE LAS REDES, NO EXISTIENDO EN LA PRÁCTICA UN LÍMITE CONCRETO Y CONTROLABLE CON EL USO DE INTERNET Y DE LAS COMUNICACIONES MÓVILES.

1. INTRODUCCIÓN

EL **MODELO CLIENTE-SERVIDOR** DE LAS APLICACIONES, Y EL **MODELO TRANSMISOR-RECEPTOR** DE LAS COMUNICACIONES, PERMITEN **PRIORIZAR LOS OBJETIVOS PREVISIBLES** PARA UN ATAQUE EXTERNO:

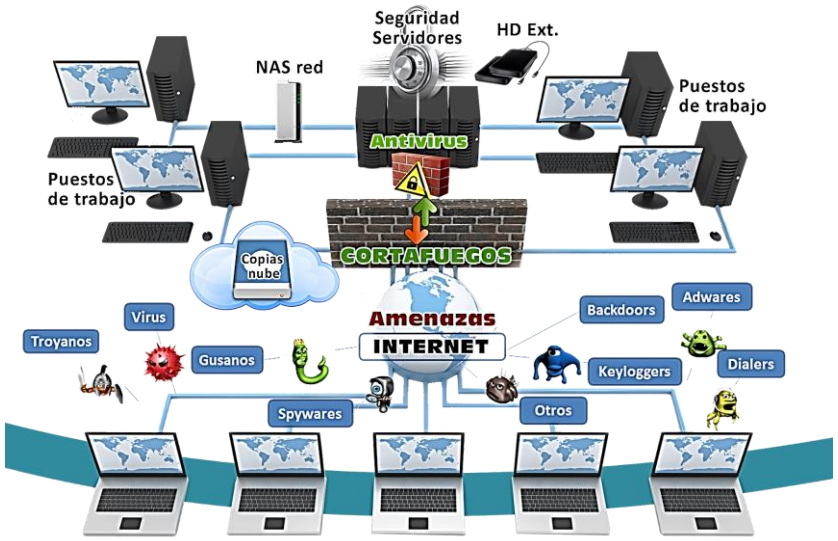
- **LAS INTERCONEXIONES ENTRE LAS DIFERENTES SUBREDES DE LA EMPRESA**
- **LA INTERCONEXIÓN ENTRE INTERNET Y LA LAN DE LA EMPRESA**



1. INTRODUCCIÓN

COMPLEMENTANDO LOS MECANISMOS DE ACCESO LÓGICO INTERNOS, PROCEDE **DAR UN PASO MÁS ALLÁ** DE ESTE DOMINIO LÓGICO, PARA ENFRENTAR OTRA ÁREA CRUCIAL DE LA SEGURIDAD LÓGICA.

ES **LA SEGURIDAD DE REDES**, QUE ESTÁ ESPECIALMENTE **ORIENTADA A ANALIZAR LAS VULNERABILIDADES DEL ACCESO LÓGICO EN LOS PUNTOS DE INTERCONEXIÓN A LA RED DE LOS EQUIPOS, Y EN LOS PUNTOS DE INTERCONEXIÓN DE LAS REDES ENTRE SÍ**.



1. INTRODUCCIÓN

LA METODOLOGÍA DE UN ATACANTE (REAL O SIMULADO), QUE PRODUCE UN INCIDENTE (INTENCIONADO O ACCIDENTAL), CON FINES LÍCITOS O NO (EVALUACIÓN ÉTICA DE SEGURIDAD O ASALTO,) **CONSTARÁ** USUALMENTE **DE LOS SIGUIENTES CUATRO PASOS**:

1. **AVERIGUAR LAS DIRECCIONES DE RED DEL OBJETIVO Y LOS SERVIDORES DE INTERÉS**
2. **RASTREAR MASIVAMENTE LA RED, EN BUSCA DE SERVIDORES VULNERABLES**
3. **ESTUDIAR LAS VULNERABILIDADES DETECTADAS, Y EXAMINAR DE NUEVO LA RED**
4. **EXPLOTAR LAS VULNERABILIDADES, SALTANDO LAS MEDIDAS DE SEGURIDAD**

CONTENIDOS

1. INTRODUCCIÓN
2. **IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN**
3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS
4. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE TRÁFICO DE COMUNICACIONES PARA DETERMINAR EL USO REAL QUE HACEN LOS SISTEMAS DE INFORMACIÓN DE LOS DISTINTOS PROTOCOLOS, SERVICIOS Y PUERTOS

2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN

LAS **ARQUITECTURAS DE RED ANTERIORES** A INTERNET NECESITABAN QUE EL MEDIO DE TRANSMISIÓN FUERA EL MISMO, **FUNCIONANDO** EN GRAN PARTE **COMO UN TODO**, DE MANERA QUE NO PUDIERA FALLAR NINGUNA PARTE, Y SOLO PODÍAN USARSE POR APLICACIONES ESPECÍFICAS.

EN **1973**, EL DEPARTAMENTO DE DEFENSA DE ESTADOS UNIDOS COMENZÓ A **DESARROLLAR TECNOLOGÍAS DE REDES DE COMUNICACIONES QUE PERMITIERAN CONECTAR REDES CON SISTEMAS DE TRANSMISIÓN DIFERENTES**, QUE TUVIERAN **TOLERANCIA A FALLOS**, EN CASO DE QUE UNA PARTE DE LA RED NO ESTUVIERA DISPONIBLE, **Y** QUE PERMITIERAN LA **EJECUCIÓN DE DIVERSAS APLICACIONES**.

2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN

EN COLABORACIÓN CON ALGUNAS UNIVERSIDADES, EN **1980** SE ÚLTIMA UN CONJUNTO DE PROTOCOLOS QUE SE DENOMINARÍAN **TCP/IP**, QUE SE USA EXTENSAMENTE **A PARTIR DE LA DÉCADA DE LOS 80**, DERIVANDO LOS SISTEMAS Y REDES INTERCONECTADOS MEDIANTE ESTA ARQUITECTURA EN UNA RED QUE HA IDO CRECIENDO DESDE ENTONCES (**INTERNET)**.

TCP/IP DEFINE LAS COMUNICACIONES, ORGANIZÁNDOLAS EN DIFERENTES NIVELES O CAPAS QUE, DE MENOR A MAYOR NIVEL DE ABSTRACCIÓN, CONCLUYEN EN LA DEFINICIÓN DE UNA SERIE DE SERVICIOS Y APLICACIONES SOFTWARE, QUE PARA OPERAR SE SIRVEN DE LOS ELEMENTOS DEFINIDOS EN NIVELES INFERIORES.

2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN

MODELO OSI

EXISTE UN ESTÁNDAR INTERNACIONAL, DENOMINADO **MODELO DE INTERCONEXIÓN DE SISTEMAS ABIERTOS**, O **MODELO OSI**, DESARROLLADO POR ISO, EN LA NORMA **X.200**.

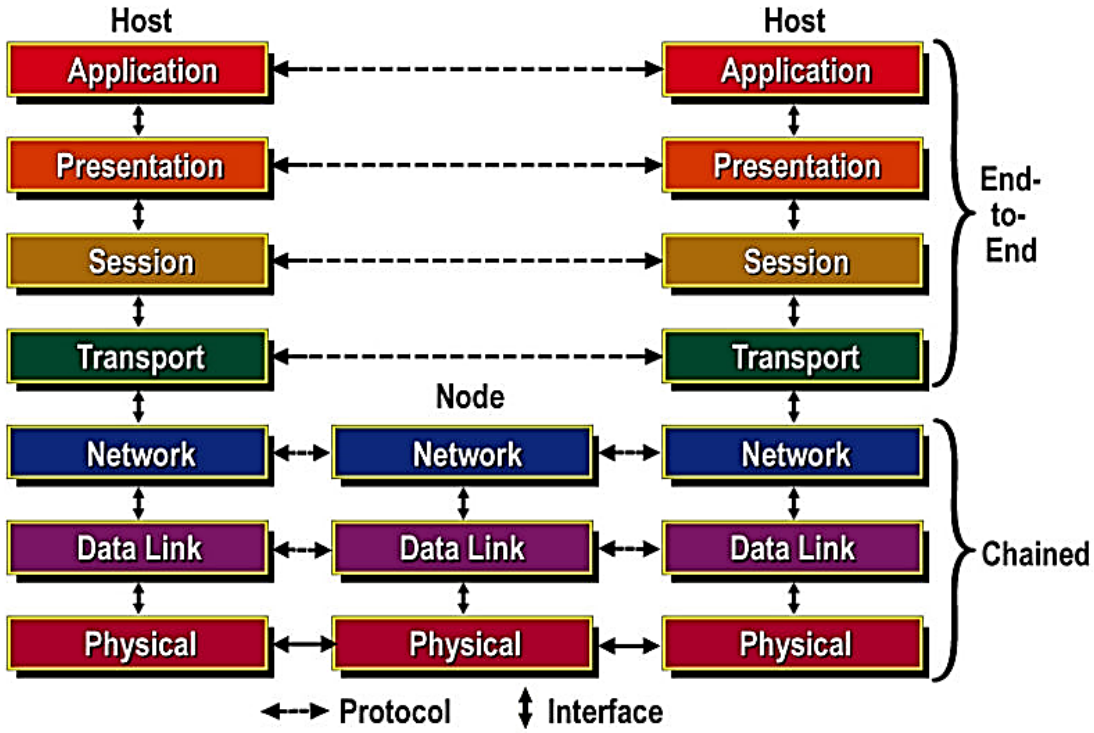
EL MODELO OSI ORGANIZA EN 7 NIVELES O CAPAS LAS FUNCIONES QUE DEBE PRESTAR UN SISTEMA DE COMUNICACIONES ENTRE NODOS, ORGANIZÁNDOLO DE LA MANERA MÁS GENERAL POSIBLE, Y SIN CONCRETAR CÓMO IMPLEMENTAR EN LA PRÁCTICA CADA FUNCIÓN.

POR LO TANTO, EL MODELO OSI DE 7 CAPAS, **SE EMPLEA PARA ESTUDIAR** PRÁCTICAMENTE **CUALQUIER ARQUITECTURA DE RED**.

2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN

MODELO OSI

- NIVEL 1: CAPA FÍSICA
- NIVEL 2: CAPA DE ENLACE
- NIVEL 3: CAPA DE RED
- NIVEL 4: CAPA DE TRANSPORTE
- NIVEL 5: CAPA DE SESIÓN
- NIVEL 6: CAPA DE PRESENTACIÓN
- NIVEL 7: CAPA DE APLICACIÓN



2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN

MODELO OSI

CAPA FÍSICA, DEBE PROPORCIONAR CONEXIONES (FIABLES O NO) PUNTO A PUNTO

CAPA DE ENLACE, DEBE PROPORCIONAR UNA CONEXIÓN FIABLE, PUNTO A PUNTO

CAPA DE RED, DEBE PROPORCIONAR DIRECCIONAMIENTO Y ENRUTAMIENTO PARA LA ENTREGA, FIABLE O NO, DE DATAGRAMAS ENTRE PUNTOS DE LA RED

CAPA DE TRANSPORTE, DEBE PROPORCIONAR ENTREGA FIABLE DE PAQUETES ENTRE PUNTOS DE LA RED

CAPA DE SESIÓN, DEBE MANEJAR LAS SESIONES ENTRE APLICACIONES INTERNAS AL NODO

CAPA DE PRESENTACIÓN, DEBE PRESENTAR LA INFORMACIÓN CON INDEPENDENCIA DEL NODO.

CAPA DE APLICACIÓN, PROTOCOLOS, FUNCIONES O SERVICIOS QUE USAN LA RED

2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN

ARQUITECTURA TCP/IP

LA **ARQUITECTURA DE RED TCP/IP** ESTÁ FORMADA POR UN CONJUNTO DE PROTOCOLOS QUE DESCRIBEN CÓMO DEBEN REALIZARSE LAS DISTINTAS OPERACIONES DE MANERA ESTÁNDAR ENTRE ELEMENTOS PARA INTEROPERAR. LOS PROTOCOLOS **SE AGRUPAN EN CUATRO GRUPOS, NIVELES O CAPAS**, QUE FORMAN UN MODELO DE RED, QUE SE DENOMINA **MODELO TCP/IP:**

- **CAPA 1, O CAPA DE ACCESO AL MEDIO O DE ENLACE**
- **CAPA 2, O CAPA DE INTERNET**
- **CAPA 3, O CAPA DE TRANSPORTE**
- **CAPA 4, O CAPA DE APLICACIÓN**

2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN

ARQUITECTURA TCP/IP

- **CAPA DE ACCESO AL MEDIO**, QUE DICTA QUE DEBE EXISTIR UN PROTOCOLO PARA CONECTAR EL NODO A LA RED.
- **CAPA DE INTERNET**, QUE PERMITE QUE LOS NODOS ENVÍEN PAQUETES A LA RED, Y QUE ESTOS LLEGUEN (ORDENADOS O NO, CON ERRORES O NO) A SU DESTINO, QUIZÁ POR DIFERENTES CAMINOS. EL PROTOCOLO MÁS IMPORTANTE ES EL **IP**.

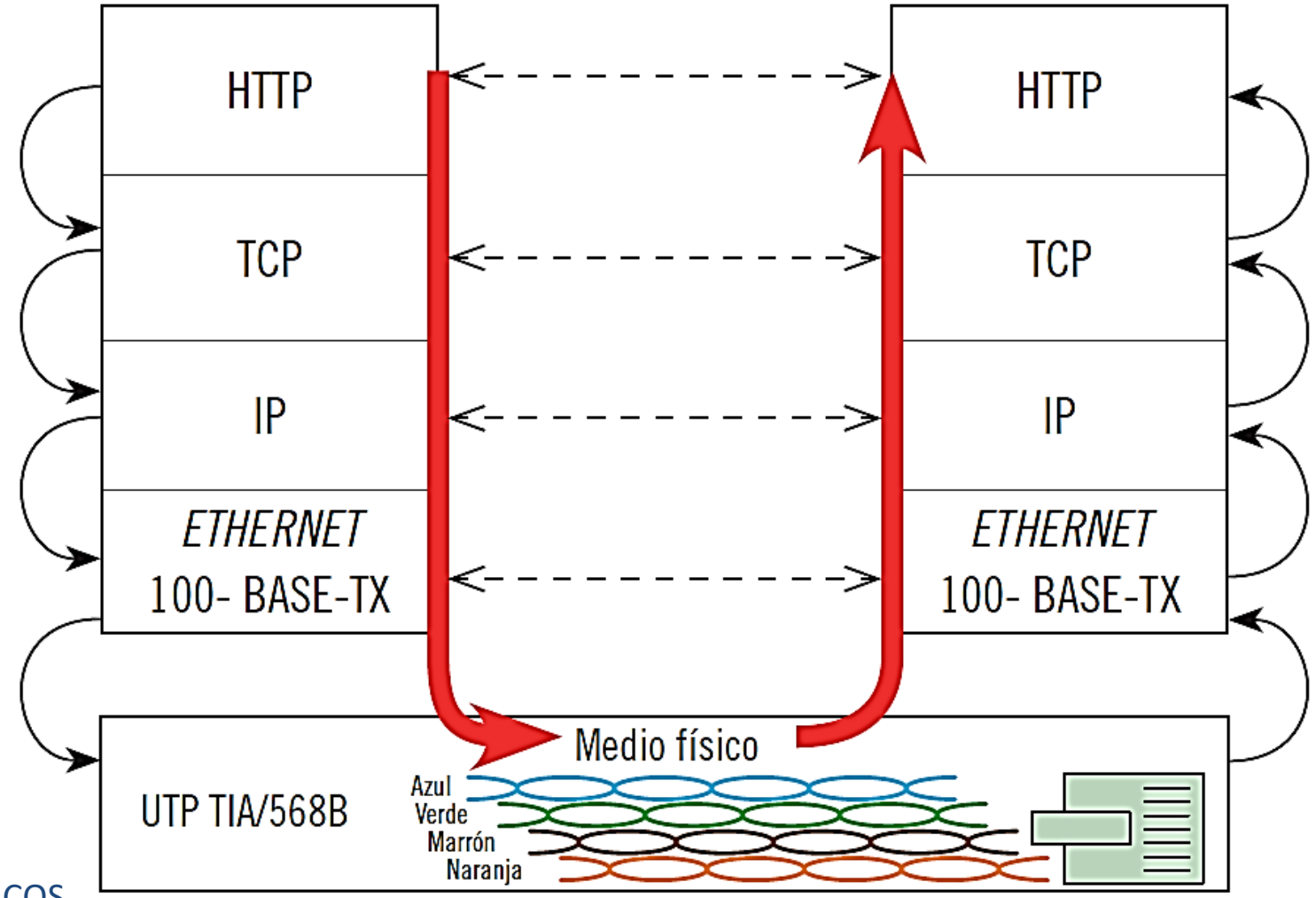
2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN

ARQUITECTURA TCP/IP

- **CAPA DE TRANSPORTE**, QUE PERMITE QUE LOS NODOS ESTABLEZCAN UNA CONVERSACIÓN (RESOLUCIÓN DE LOS ERRORES Y ORDENACIÓN DE LOS PAQUETES). LOS PROTOCOLOS MÁS IMPORTANTES SON **TCP** (ORIENTADO A ESTABLECER O MANTENER LA CONVERSACIÓN MEDIANTE UNA CONEXIÓN FIABLE NODO A NODO), Y **UDP** (QUE NO ESTÁ ORIENTADO AL ESTABLECIMIENTO DE UNA CONEXIÓN NODO A NODO, Y QUE NO ES FIABLE).
- **CAPA DE APLICACIÓN**, QUE ENTREGA UNOS PROTOCOLOS DE RED DISPONIBLES PARA LAS APLICACIONES DEL USUARIO. EL MÁS CONOCIDO ES EL PROTOCOLO **HTTP**, QUE EMPLEAN LAS APLICACIONES DE NAVEGACIÓN WEB.

2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN

ARQUITECTURA TCP/IP



2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN

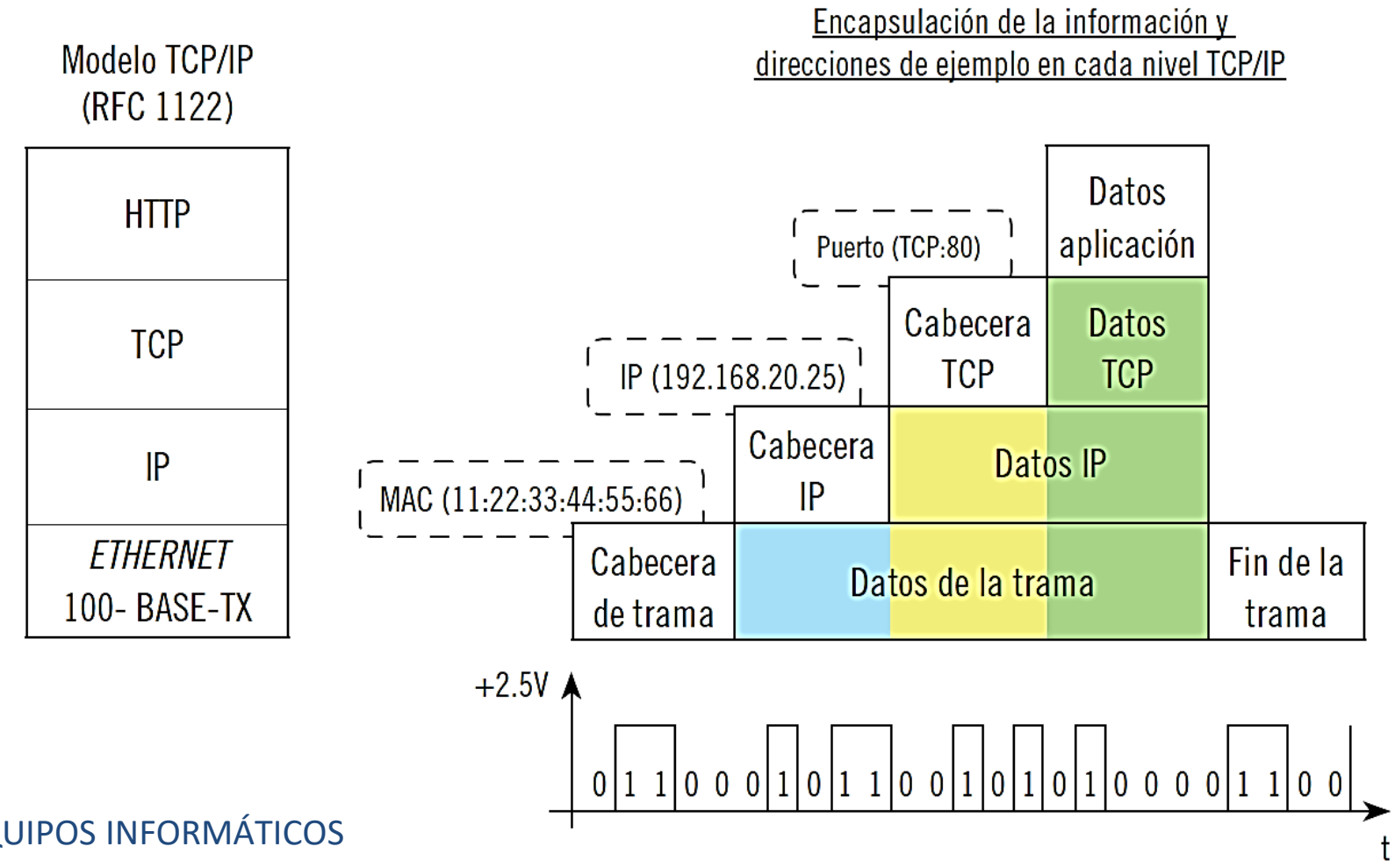
ARQUITECTURA TCP/IP

CUANDO **LA INFORMACIÓN** PASA DE LAS CAPAS SUPERIORES A LAS INFERIORES, **SE ENCAPSULA**, DE MANERA QUE VA AUMENTANDO LA LONGITUD, PORQUE *EN CADA CAPA INFERIOR SE AÑADE LA INFORMACIÓN PROPIA DE LA CAPA* (CABECERA QUE INCLUYE LA DIRECCIÓN DEL NODO EN EL FORMATO DE CADA CAPA), *A LA INFORMACIÓN PROCEDENTE DE LA CAPA SUPERIOR.*

EN EL EXTREMO RECEPTOR, EL PROCESO ES EL INVERSO, Y SE EXTRAEN LOS DATOS QUE SE PASAN A LA CAPA SUPERIOR.

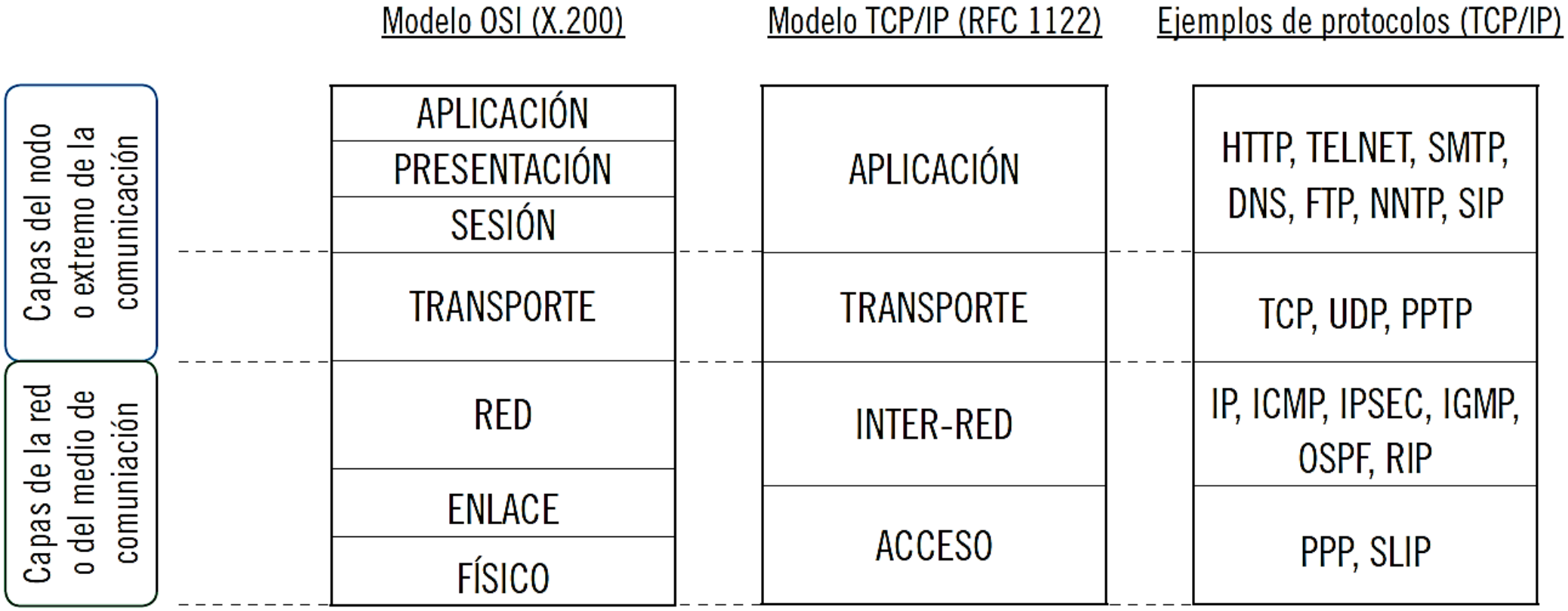
2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN

ARQUITECTURA TCP/IP



2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN

MODELO OSI VS ARQUITECTURA TCP/IP



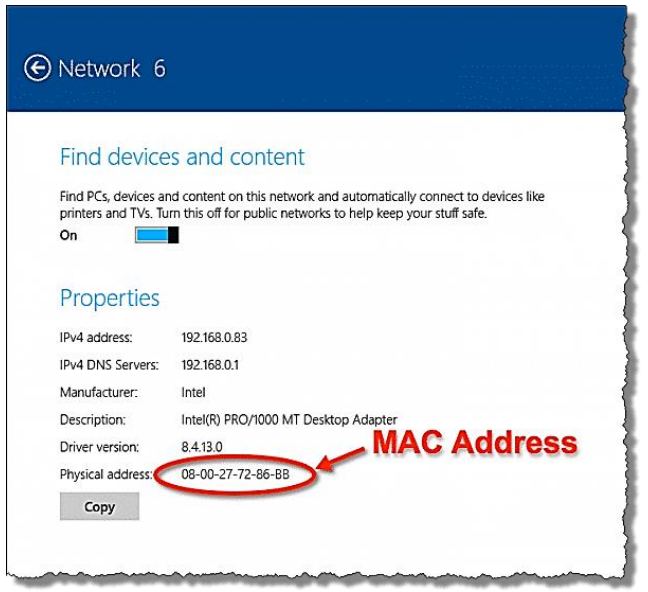
2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN

PROTOCOLOS, SERVICIOS Y PUERTOS MÁS HABITUALES

CADA NODO DE LA RED DISPONE DE UNA DIRECCIÓN.

EN LA **CAPA DE ACCESO** SE USA LA **DIRECCIÓN MAC** (MEDIUM ACCESS CONTROL), DEL ADAPTADOR DE RED QUE CONECTA EL NODO AL MEDIO FÍSICO

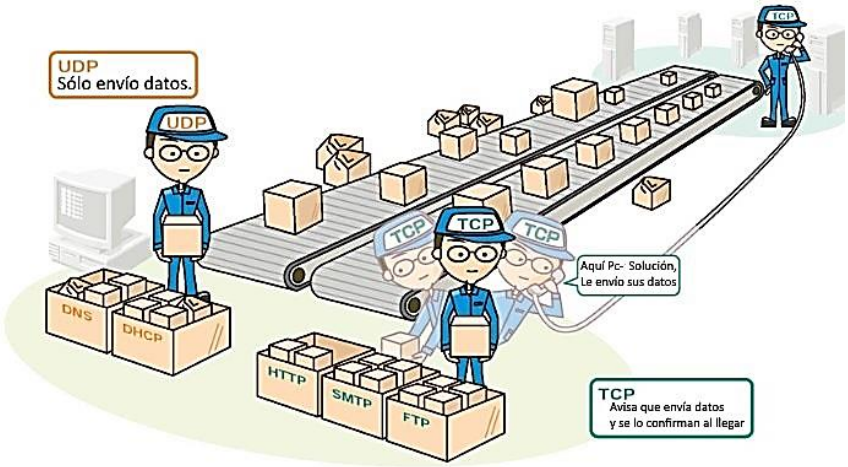
EN LA **CAPA DE INTERNET** SE USA LA **DIRECCIÓN IP** (INTERNET PROTOCOL), QUE SE CONFIGURA PARA CADA CONEXIÓN DE RED.



2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN

PROTOCOLOS, SERVICIOS Y PUERTOS MÁS HABITUALES

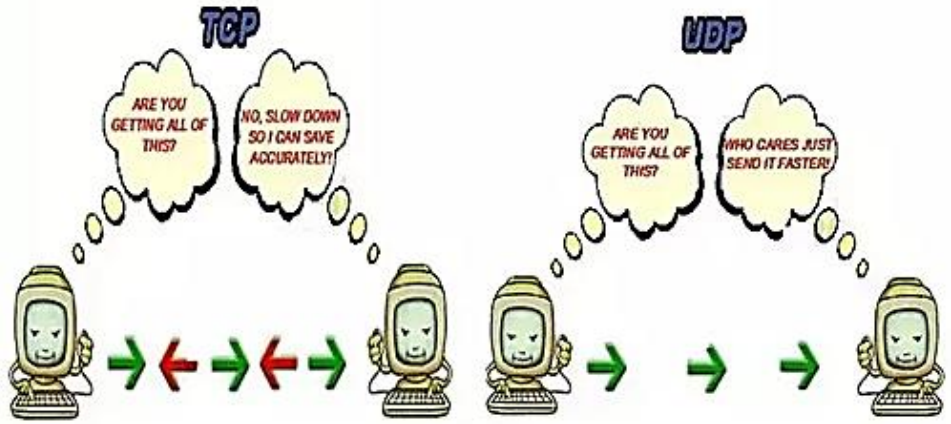
SE NECESITA **DIFERENCIAR LAS DISTINTAS CONVERSACIONES** QUE SE MANTIENEN POR LA CONEXIÓN DE RED; DE OTRA FORMA, COMO TODOS LOS MENSAJES VAN DIRIGIDOS A LA MISMA DIRECCIÓN IP.



2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN

PROTOCOLOS, SERVICIOS Y PUERTOS MÁS HABITUALES

PARA DIFERENCIAR LAS DISTINTAS APLICACIONES QUE USAN UNA MISMA CONEXIÓN DE RED, SE EMPLEAN **LOS PUERTOS**, QUE SON COMO **UNA DIRECCIÓN EN LA CAPA DE TRANSPORTE**, EXISTIENDO **PUERTOS TCP**, Y **PUERTOS UDP**.



2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN

PROTOCOLOS, SERVICIOS Y PUERTOS MÁS HABITUALES

LOS PROTOCOLOS MÁS FRECUENTES (HTTP, FTP, ETC.), **EMPLEARÁN UNOS PUERTOS POR DEFECTO**, DONDE LOS CLIENTES DE LAS APLICACIONES INTENTARÁN ESTABLECER LA COMUNICACIÓN, PORQUE ES DONDE ESPERAN QUE LES RESPONDA EL SERVIDOR DE APLICACIONES.

EXISTEN **65.535** PUERTOS DISPONIBLES PARA LOS PROTOCOLOS (TCP Y UDP), DIVIDIENDO LOS PUERTOS EN TRES RANGOS:

- **PUERTOS DE SISTEMA O PUERTOS BIEN CONOCIDOS: 0-1023**
- **PUERTOS DE USUARIO O PUERTOS REGISTRADOS: 1024-49151**
- **PUERTOS DINÁMICOS O PRIVADOS O EFÍMEROS: 49152-65535**

2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN

PROTOCOLOS, SERVICIOS Y PUERTOS MÁS HABITUALES

Servicios de sistema	Protocolo	Puerto	Servicios de sistema	Protocolo	Puerto
Transferencia de ficheros	FTP SSH	21 (TCP)	Servicio de nombres Netbios	NBT	137 (TCP, UDP)
Interprete de ordenes seguras	TELNET	22 (TCP, UDP)	Servicio de datagrama Netbios	NBT	138 (TCP, UDP)
Terminal remoto		23 (TCP)	Servicio de sesión Netbios	NBT	139 (TCP, UDP)
Envío de correo	SMTP	25 (TCP)	Acceso a correo electrónico	IMAP	143 (TCP)
Consultar de dominio o de IP	WHOIS	43 (TCP)	Transferencia de ficheros	BFTP	152 (TCP)
Servicio de nombres	DNS	53 (TCP, UDP)	Gestión de red	SNMP	161 (TCP, UDP)
Configuración de red dinámica	DHCP	67 (UDP)	Chat	IRC	194 (TCP, UDP)
Configuración de red dinámica	DHCP	68 (UDP)	Acceso ligero a servicio de directorio	LDAP	389 (TCP, UDP)
Transferencia de ficheros	TFTP	69 (UDP)	Navegación web segura	HTTPS/SSL	443 (TCP)
Usuarios conectados a un servidor	FINGER	79 (TCP, UDP)	Compartición de ficheros Windows	SMTP	445 (TCP, UDP)
Navegación web	HTTP	80 (TCP)	Envío de correos seguro	SMTP/SSL	465 (TCP)
Autenticación	KERBEROS	88 (TCP)	Logs del sistema	SYSLOG	514 (UDP)
Lectura y descarga de correo electrónico	POP3	110 (TCP)	Información de enrutamiento	RIP	520 (UDP)
Transferencia de ficheros	SFTP	115 (TCP)	Terminal remoto seguro	TELNET/SSL	992 (TCP, UDP)
Noticias	NNTP	119 (TCP, UDP)	Acceso a correo electrónico seguro	IMAP4/SSL	993 (TCP, UDP)
Sincronización de hora	NTP	123 (TCP, UDP)	Lectura y descarga de correo seguro	POP3/SSL	995 (TCP, UDP)

2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN

PROTOCOLOS, SERVICIOS Y PUERTOS MÁS HABITUALES

PUERTO 1194: ESTE PUERTO ESTÁ TANTO EN TCP COMO EN UDP, ES UTILIZADO POR EL POPULAR PROTOCOLO OPENVPN PARA LAS REDES PRIVADAS VIRTUALES.
PUERTO 1723: ES USADO POR EL PROTOCOLO DE VPN PPTP.
PUERTO 1812: SE UTILIZA TANTO CON TCP COMO CON UDP, Y SIRVE PARA AUTENTICAR CLIENTES EN UN SERVIDOR RADIUS.
PUERTO 1813: SE UTILIZA TANTO CON TCP COMO CON UDP, Y SIRVE PARA EL ACCOUNTING EN UN SERVIDOR RADIUS.
PUERTO 2049: ES UTILIZADO POR EL PROTOCOLO NFS PARA EL INTERCAMBIO DE FICHEROS EN RED LOCAL O EN INTERNET.
PUERTOS 2082 Y 2083: ES UTILIZADO POR EL POPULAR CMS CPANEL PARA LA GESTIÓN DE SERVIDORES Y SERVICIOS, DEPENDIENDO DE SI SE USA HTTP O HTTPS, SE UTILIZA UNO U OTRO.
PUERTO 3074: LO USA EL SERVICIO ONLINE DE VIDEOJUEGOS DE MICROSOFT XBOX LIVE.
PUERTO 3306: PUERTO USADO POR LAS BASES DE DATOS MYSQL.
PUERTO 3389: ES EL PUERTO QUE USA EL ESCRITORIO REMOTO DE WINDOWS, MUY RECOMENDABLE CAMBIARLO.
PUERTO 4662 TCP Y 4672 UDP: ESTOS PUERTOS LOS USA EL MÍTICO PROGRAMA EMULE, QUE ES UN PROGRAMA PARA DESCARGAR TODO TIPO DE ARCHIVOS.
PUERTO 4899: ESTE PUERTO LO USA RADMIN, QUE ES UN PROGRAMA PARA CONTROLAR REMOTAMENTE EQUIPOS.
PUERTO 5000: ES EL PUERTO DE CONTROL DEL POPULAR PROTOCOLO UPNP, Y QUE POR DEFECTO, SIEMPRE DEBERÍAMOS DESACTIVARLO EN EL ROUTER PARA NO TENER NINGÚN PROBLEMA DE SEGURIDAD.
PUERTOS 5400, 5500, 5600, 5700, 5800 Y 5900: SON USADOS POR EL PROGRAMA VNC, QUE TAMBIÉN SIRVE PARA CONTROLAR EQUIPOS REMOTAMENTE.
PUERTOS 6881 Y 6969: SON USADOS POR EL PROGRAMA BITTORRENT, QUE SIRVE PARA E INTERCAMBIO DE FICHEROS.
PUERTO 8080: ES EL PUERTO ALTERNATIVO AL PUERTO 80 TCP PARA SERVIDORES WEB, NORMALMENTE SE UTILIZA ESTE PUERTO EN PRUEBAS.
PUERTOS 51400: ES EL PUERTO UTILIZADO DE MANERA PREDETERMINADA POR EL PROGRAMA TRANSMISSION PARA DESCARGAR ARCHIVOS A TRAVÉS DE LA RED BITTORRENT.
PUERTO 25565: PUERTO USADO POR EL FAMOSO VIDEOJUEGO MINECRAFT.

CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN
3. **UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS**
4. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE TRÁFICO DE COMUNICACIONES PARA DETERMINAR EL USO REAL QUE HACEN LOS SISTEMAS DE INFORMACIÓN DE LOS DISTINTOS PROTOCOLOS, SERVICIOS Y PUERTOS

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

LAS APLICACIONES, PROTOCOLOS Y SERVICIOS, OFRECEN **VULNERABILIDADES** QUE, CONVENIENTEMENTE **EXPLOTADAS**, MATERIALICEN UN INCIDENTE DE SEGURIDAD.

ES CRUCIAL **REDUCIR AL MÍNIMO** LAS VÍAS DE ACCESO LÓGICO A **LAS POTENCIALES VULNERABILIDADES**, ES DECIR, **MINIMIZAR LOS PUERTOS DE ACCESO A LA RED**.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

ESTO SE LOGRA:

- **ELIMINANDO TODOS LOS SERVICIOS QUE NO SE NECESITEN, PROHIBIENDO EL ACCESO POR DEFECTO A TODOS LOS PUERTOS**
- **HABILITANDO SOLO LOS SERVICIOS Y SU ACCESO A TRAVÉS DE PUERTOS DE COMUNICACIONES CUANDO REALMENTE SE NECESITE**

PARA CONFIRMAR TANTO EL ESTADO INICIAL DE LA RED, COMO QUE ESTAS ACCIONES SON EFECTIVAS, **ES PRECISO EMPLEAR HERRAMIENTAS DE RED PARA ANALIZAR** QUÉ PUERTOS ADMITEN CONEXIONES, Y QUÉ SERVICIOS RESPONDEN A TRAVÉS DE ELLOS.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

WINDOWS Y LINUX INCORPORAN **HERRAMIENTAS DE RED** EN LÍNEA DE COMANDOS, QUE RESULTAN DE MÁXIMA UTILIDAD PARA **CONOCER EL ESTADO DE LA CONEXIÓN DE RED** DEL EQUIPO DONDE SE EJECUTAN, O BIEN PARA **EVALUAR LAS POSIBILIDADES DE CONEXIÓN** HASTA OTRO EQUIPO.

LAS **UTILIDADES** DE RED SON PUNTO DE PARTIDA DE TODO ANÁLISIS DE SEGURIDAD DE RED:

PING	**IPCONFIG/IFCONFIG**	**ROUTE**
TRACERT/TRACEROUTE	**NSLOOKUP**	**ARP**
PATHPING	**NETSTAT**	

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

PING

ORIENTADA AL DIAGNÓSTICO DE CONEXIÓN, ESTA UTILIDAD **SE EMPLEA PARA COMPROBAR LA CONEXIÓN A NIVEL DE RED CON EL NODO** CUYA DIRECCIÓN SE INDIQUE.

FUNCIONA DIRECTAMENTE EN LA CAPA DE RED, EMPLEANDO EL PROTOCOLO DE MENSAJES DE CONTROL **ICMP** (INTERNET CONTROL MESSAGE PROTOCOL), QUE ES PARTE DEL **PROTOCOLO IP.**

COMO HERRAMIENTA DE DIAGNÓSTICO ES MUY VALIOSA, PUES PERMITE COMPROBAR PAULATINAMENTE LA CONEXIÓN, DESDE EL ÁMBITO INTERNO HASTA INTERNET.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

PING

```
C:\Users\Usuario>ping www.google.es

Haciendo ping a www.google.es [216.58.215.131] con 32 bytes de datos:
Respuesta desde 216.58.215.131: bytes=32 tiempo=34ms TTL=116
Respuesta desde 216.58.215.131: bytes=32 tiempo=37ms TTL=116
Respuesta desde 216.58.215.131: bytes=32 tiempo=32ms TTL=116
Respuesta desde 216.58.215.131: bytes=32 tiempo=31ms TTL=116

Estadísticas de ping para 216.58.215.131:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 31ms, Máximo = 37ms, Media = 33ms
```

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

PING

- **IP 127.0.0.1 O LOCALHOST:** *PERMITE REVISAR LA CORRECTA INSTALACIÓN DE PROTOCOLOS TCP/IP EN EL NODO*.
- **IP DEL NODO:** *PERMITE ASEGURAR QUE LA TARJETA DE RED FUNCIONA*, YA QUE EL MENSAJE SALE Y REGRESA AL EQUIPO.
- **IP DE OTRO NODO DE LA LAN:** *PERMITE ASEGURAR QUE HAY CONEXIÓN CON OTRO NODO*, ES DECIR, QUE PARTE DE LA LAN FUNCIONA.
- **IP DE LA PASARELA** (MÁQUINA QUE CONECTA A INTERNET, O GATEWAY): *PERMITE CONFIRMAR QUE PUEDE HABER CONEXIÓN HACIA INTERNET*
- **IP DE UN SERVIDOR DNS** DEL PROVEEDOR DE LA CONEXIÓN A INTERNET (ISP): *PERMITE CONFIRMAR QUE HAY CONEXIÓN A INTERNET*

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

TRACERT/TRACEROUTE

ORIENTADA AL DIAGNÓSTICO DE LA RUTA DE CONEXIÓN. EMPLEANDO EL CAMPO **TTL** (TIME TO LIVE) DE LOS PAQUETES O DATAGRAMAS DEL PROTOCOLO DE RED IP, **PERMITE AVERIGUAR QUÉ RUTA SIGUE UN PAQUETE HASTA ALCANZAR SU DESTINO**.

TRAZA LA RUTA ENTRE UN ORIGEN Y UN DESTINO. INFORMA LAS DIRECCIONES IP DE TODOS LOS ROUTERS IMPLICADOS.

EN SISTEMAS WINDOWS, ESTA APLICACIÓN SE DENOMINA **TRACERT**

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

TRACERT/TRACEROUTE

```
C:\Users\Usuario>tracert www.google.es

Traza a la dirección www.google.es [216.58.215.131]
sobre un máximo de 30 saltos:

  1     5 ms     4 ms     5 ms  192.168.1.1
  2     8 ms     6 ms     6 ms  192.168.144.1
  3     7 ms     6 ms     6 ms  129.red-81-41-252.staticip.rima-tde.net [81.41.252.129]
  4     *        *        *     Tiempo de espera agotado para esta solicitud.
  5     *        *        *     Tiempo de espera agotado para esta solicitud.
  6    32 ms    40 ms    32 ms  176.52.253.97
  7    33 ms    32 ms    32 ms  72.14.211.154
  8    35 ms    33 ms    34 ms  172.253.50.39
  9    68 ms    34 ms    35 ms  142.250.239.27
 10   124 ms    91 ms    41 ms  mad41s04-in-f3.1e100.net [216.58.215.131]
```

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

PATHPING

COMBINA LA FUNCIONALIDAD DE **TRACERT** Y **PING**. UTILIZADA PARA ENCONTRAR ROUTERS QUE PUEDAN ESTAR CAUSANDO PROBLEMAS EN TU RED, ESTA HERRAMIENTA FUE DESARROLLADA POR MICROSOFT, POR LO QUE **SÓLO ESTÁ DISPONIBLE EN SISTEMAS WINDOWS.**

FUNCIONA ENVIANDO PAQUETES AL DESTINO FINAL Y A LOS ROUTERS EN EL CAMINO, PARA LUEGO INFORMAR DE LA LATENCIA Y LA PÉRDIDA DE PAQUETES EN CADA SALTO.

PARA USARLO, ESCRIBIR **PATHPING** SEGUIDO DE LA URL O LA DIRECCIÓN IP EN LA LÍNEA DE COMANDOS.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

PATHPING

```
C:\Users\Usuario>pathping www.google.es

Seguimiento de ruta a www.google.es [216.58.215.131]
sobre un máximo de 30 saltos:
  0  DESKTOP-VQFHACJ [192.168.1.40]
  1  192.168.1.1
  2  192.168.144.1
  3  129.red-81-41-252.staticip.rima-tde.net [81.41.252.129]
  4     *        *        *
Procesamiento de estadísticas durante 75 segundos...
             Origen hasta aquí   Este Nodo/Vínculo
Salto  RTT    Perdido/Enviado = Pct  Perdido/Enviado = Pct  Dirección
  0                                                DESKTOP-VQFHACJ [192.168.1.40]
                                   0/ 100 =  0%   |
  1   20ms     0/ 100 =  0%     0/ 100 =  0%  192.168.1.1
                                 100/ 100 =100%   |
  2  ---     100/ 100 =100%     0/ 100 =  0%  192.168.144.1
                                   0/ 100 =  0%   |
  3  ---     100/ 100 =100%     0/ 100 =  0%  129.red-81-41-252.staticip.rima-tde.net [81.41.252.129]

Traza completa.
```

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

IPCONFIG/IFCONFIG

LA UTILIDAD DE LÍNEA DE COMANDO **IPCONFIG** MOSTRARÁ INFORMACIÓN DETALLADA SOBRE LA RED A LA QUE ESTÁ CONECTADO.

TAMBIÉN AYUDA CON LA RECONFIGURACIÓN DE SU DIRECCIÓN IP A TRAVÉS DE LA LIBERACIÓN Y RENOVACIÓN.

```
C:\Users\Usuario>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de Ethernet Ethernet 2:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::466e:eb6e:1013:6d8c%2
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.56.1
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . :

Adaptador de Ethernet Ethernet 3:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::fb6b:a98c:ff5f:7e75%21
   Dirección IPv4 de configuración automática: 169.254.39.98
   Máscara de subred . . . . . . . . . . . . : 255.255.0.0
   Puerta de enlace predeterminada . . . . . :

Adaptador de LAN inalámbrica Conexión de área local* 1:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 10:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::38b:fe9:cb6e:d24c%18
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.1.40
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.1.1

Adaptador de Ethernet Conexión de red Bluetooth:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :
```

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

IPCONFIG/IFCONFIG

IPCONFIG /ALL LE DARÁ INFORMACIÓN MÁS DETALLADA.

A TRAVÉS DE **IPCONFIG/ALL** PODEMOS ENCONTRAR SERVIDORES DNS, SI TENEMOS DHCP HABILITADO, DIRECCIÓN MAC, JUNTO CON OTRA INFORMACIÓN ÚTIL. TODO LO BUENO QUE HAY QUE SABER SI TENEMOS PROBLEMAS PARA CONECTARNOS A INTERNET.

OTRAS HERRAMIENTAS DE IPCONFIG QUE SON ÚTILES INCLUYEN **IPCONFIG /RELEASE** Y **IPCONFIG /RENEW**.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

NSLOOKUP / DIG

ORIENTADA A OBTENER INFORMACIÓN DE UN DOMINIO O DE UNA DIRECCIÓN IP, ESTE COMANDO REALIZA CONSULTAS A UN SERVIDOR DE NOMBRE (**DNS**), PARA AVERIGUAR LA TRADUCCIÓN DE UN NOMBRE DE INTERNET O DOMINIO, A SU DIRECCIÓN IP; O VICEVERSA.

EN LINUX, EL COMANDO EMPLEADO ES **DIG**. LAS CONSULTAS SE PUEDEN REALIZAR SOBRE LOS DISTINTOS TIPOS DE REGISTROS, QUE EL SERVIDOR DE NOMBRES (DNS) TENGA REGISTRADOS, LO QUE FACILITA LA EVALUACIÓN DE CUÁNTA INFORMACIÓN ESTÁ DISPONIBLE SOBRE UN SERVICIO CONCRETO DE UN DOMINIO.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

NSLOOKUP

```
C:\Users\Usuario>nslookup www.google.com
Servidor:  250.red-80-58-61.staticip.rima-tde.net
Address:  80.58.61.250

Respuesta no autoritativa:
Nombre:  www.google.com
Addresses:  2a00:1450:4003:80f::2004
          142.250.200.100
```

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

DIG

```
root@pru-VirtualBox:/home/pru# dig www.google.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58654
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         103     IN      A       216.58.215.132

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: dom mar 12 04:27:24 WET 2023
;; MSG SIZE  rcvd: 59
```

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

NETSTAT

ORIENTADO **A CONOCER TODAS LAS CONEXIONES ACTIVAS** DEL NODO DONDE SE EJECUTA, **NETSTAT** PERMITE SABER EN UN MOMENTO DADO QUÉ PUERTOS TCP Y UDP SE ESTÁN USANDO, ADEMÁS DE ESTADÍSTICAS DE DICHO USO.

LA HERRAMIENTA EXISTE EN LINUX Y EN WINDOWS, Y EXISTEN APLICACIONES QUE LA EMPLEAN Y LE PROPORCIONAN UN INTERFAZ GRÁFICO.

LA APLICACIÓN ENTREGA INFORMACIÓN DE APOYO PARA ESTUDIAR LAS CONEXIONES.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

NETSTAT

```
C:\Users\Usuario>netstat

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    127.0.0.1:57546        kubernetes:57547       ESTABLISHED
  TCP    127.0.0.1:57547        kubernetes:57546       ESTABLISHED
  TCP    127.0.0.1:57548        kubernetes:57549       ESTABLISHED
  TCP    127.0.0.1:57549        kubernetes:57548       ESTABLISHED
  TCP    192.168.1.40:53068     ec2-44-228-230-125:https  ESTABLISHED
  TCP    192.168.1.40:53069     20.54.37.64:https      ESTABLISHED
  TCP    192.168.1.40:53071     mad41s10-in-f10:https  ESTABLISHED
  TCP    192.168.1.40:53073     104.18.10.248:https    ESTABLISHED
  TCP    192.168.1.40:53083     20.54.36.229:https     ESTABLISHED
  TCP    192.168.1.40:53132     192.168.1.39:8009      ESTABLISHED
  TCP    192.168.1.40:53147     52.108.50.36:https     ESTABLISHED
  TCP    192.168.1.40:53157     192.168.1.39:8009      ESTABLISHED
  TCP    192.168.1.40:53159     1drv:https             ESTABLISHED
  TCP    192.168.1.40:53172     wo-in-f188:5228        ESTABLISHED
  TCP    192.168.1.40:53177     ws-in-f188:5228        ESTABLISHED
  TCP    192.168.1.40:53185     192.168.1.39:8009      ESTABLISHED
  TCP    192.168.1.40:53197     do-42:https            ESTABLISHED
  TCP    192.168.1.40:53203     do-42:https            ESTABLISHED
  TCP    192.168.1.40:53205     do-42:https            ESTABLISHED
  TCP    192.168.1.40:53593     mad07s23-in-f10:https  CLOSE_WAIT
  TCP    192.168.1.40:53619     1drv:https             ESTABLISHED
  TCP    192.168.1.40:53624     51.105.71.136:https    TIME_WAIT
  TCP    192.168.1.40:53630     mad41s11-in-f14:https  ESTABLISHED
  TCP    192.168.1.40:53636     13.107.21.239:https    TIME_WAIT
  TCP    192.168.1.40:53640     52.109.88.184:https    ESTABLISHED
  TCP    192.168.1.40:53641     1drv:https             ESTABLISHED
  TCP    192.168.1.40:53642     13.89.178.27:https     ESTABLISHED
  TCP    192.168.1.40:53643     52.109.28.107:https    TIME_WAIT
  TCP    192.168.1.40:53647     52.109.28.107:https    TIME_WAIT
  TCP    192.168.1.40:53648     51.105.71.136:https    ESTABLISHED
  TCP    192.168.1.40:53651     ec2-54-148-147-19:https  TIME_WAIT
  TCP    192.168.1.40:53652     52.109.76.225:https    TIME_WAIT
  TCP    192.168.1.40:53653     mad41s14-in-f10:https  TIME_WAIT
  TCP    192.168.1.40:53654     ip252:https            ESTABLISHED
  TCP    192.168.1.40:53656     204.79.197.239:https   ESTABLISHED
```

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

ROUTE

EL COMANDO ROUTE ES OTRA HERRAMIENTA DE DIAGNÓSTICO DE RED PARA SOLUCIONAR PROBLEMAS, DISPONIBLE EN WINDOWS, LINUX, SISTEMAS TIPO UNIX, IBM OS Y REACTOS.

SE UTILIZA PARA **VISUALIZAR Y REALIZAR CAMBIOS EN LAS TABLAS DE ENRUTAMIENTO**. VIENE CON MUCHOS PARÁMETROS, CON LOS CUALES PUEDES LIMPIAR LA TABLA DE ENRUTAMIENTO, ESTABLECER EL DESTINO DE LA RED, EL COMANDO PARA USAR IPV4 O IPV6, Y MÁS.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

ROUTE

```
C:\Users\Usuario>route print -4
===========================================================================
IListe de interfaces
  7...c0 18 03 87 34 0d ......Realtek Gaming GbE Family Controller
  2...0a 00 27 00 00 02 ......VirtualBox Host-Only Ethernet Adapter
 21...0a 00 27 00 00 15 ......VirtualBox Host-Only Ethernet Adapter
 14...d4 54 8b d4 89 e8 ......Microsoft Wi-Fi Direct Virtual Adapter
 12...d6 54 8b d4 89 e7 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 18...d4 54 8b d4 89 e7 ......Intel(R) Wi-Fi 6 AX201 160MHz
 20...d4 54 8b d4 89 eb ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Tabla de enrutamiento
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de enlace   Interfaz  Métrica
          0.0.0.0          0.0.0.0      192.168.1.1     192.168.1.40     50
        127.0.0.0        255.0.0.0      En vínculo         127.0.0.1    331
        127.0.0.1  255.255.255.255      En vínculo         127.0.0.1    331
  127.255.255.255  255.255.255.255      En vínculo         127.0.0.1    331
      169.254.0.0        255.255.0.0      En vínculo     169.254.39.98    281
    169.254.39.98  255.255.255.255      En vínculo     169.254.39.98    281
  169.254.255.255  255.255.255.255      En vínculo     169.254.39.98    281
      192.168.1.0    255.255.255.0      En vínculo      192.168.1.40    306
     192.168.1.40  255.255.255.255      En vínculo      192.168.1.40    306
    192.168.1.255  255.255.255.255      En vínculo      192.168.1.40    306
      192.168.56.0    255.255.255.0      En vínculo      192.168.56.1    281
      192.168.56.1  255.255.255.255      En vínculo      192.168.56.1    281
    192.168.56.255  255.255.255.255      En vínculo      192.168.56.1    281
        224.0.0.0        240.0.0.0      En vínculo         127.0.0.1    331
        224.0.0.0        240.0.0.0      En vínculo      192.168.56.1    281
        224.0.0.0        240.0.0.0      En vínculo     169.254.39.98    281
        224.0.0.0        240.0.0.0      En vínculo      192.168.1.40    306
  255.255.255.255  255.255.255.255      En vínculo         127.0.0.1    331
  255.255.255.255  255.255.255.255      En vínculo      192.168.56.1    281
  255.255.255.255  255.255.255.255      En vínculo     169.254.39.98    281
  255.255.255.255  255.255.255.255      En vínculo      192.168.1.40    306
===========================================================================
Rutas persistentes:
  Ninguno
```

```
root@pru-VirtualBox:/home/pru# route -4
Tabla de rutas IP del núcleo
Destino         Pasarela        Genmask         Indic Métric Ref    Uso Interfaz
default         _gateway        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
```

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

ARP

LA UTILIDAD ARP AYUDA A DIAGNOSTICAR LOS PROBLEMAS ASOCIADOS CON EL **PROTOCOLO DE RESOLUCIÓN DE DIRECCIONES** (**ARP**).

LOS HOSTS TCP/IP UTILIZAN ARP PARA DETERMINAR LA DIRECCIÓN FÍSICA (MAC) QUE CORRESPONDE A UNA DIRECCIÓN IP ESPECÍFICA. E

ESCRIBA **ARP** CON LA OPCIÓN **–A** PARA MOSTRAR LAS DIRECCIONES IP QUE HAN SIDO RESUELTAS A DIRECCIONES MAC RECIENTEMENTE.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS BÁSICAS DE TRABAJO EN RED

ARP

```
C:\Users\Usuario>arp -a

Interfaz: 192.168.56.1 --- 0x2
  Dirección de Internet          Dirección física      Tipo
  192.168.56.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.22             01-00-5e-00-00-16     estático
  224.0.0.251            01-00-5e-00-00-fb     estático
  224.0.0.252            01-00-5e-00-00-fc     estático
  239.255.255.250        01-00-5e-7f-ff-fa     estático

Interfaz: 192.168.1.40 --- 0x12
  Dirección de Internet          Dirección física      Tipo
  192.168.1.1            f4-69-42-19-84-d0     dinámico
  192.168.1.39           1c-53-f9-0b-2c-21     dinámico
  192.168.1.41           b0-52-16-cd-6a-0b     dinámico
  192.168.1.255          ff-ff-ff-ff-ff-ff     estático
  224.0.0.2              01-00-5e-00-00-02     estático
  224.0.0.22             01-00-5e-00-00-16     estático
  224.0.0.251            01-00-5e-00-00-fb     estático
  224.0.0.252            01-00-5e-00-00-fc     estático
  239.255.255.250        01-00-5e-7f-ff-fa     estático
  255.255.255.255        ff-ff-ff-ff-ff-ff     estático

Interfaz: 169.254.39.98 --- 0x15
  Dirección de Internet          Dirección física      Tipo
  169.254.255.255        ff-ff-ff-ff-ff-ff     estático
  224.0.0.22             01-00-5e-00-00-16     estático
  224.0.0.251            01-00-5e-00-00-fb     estático
  224.0.0.252            01-00-5e-00-00-fc     estático
  239.255.255.250        01-00-5e-7f-ff-fa     estático
  255.255.255.255        ff-ff-ff-ff-ff-ff     estático
```

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS DE ANÁLISIS DE PUERTOS

LAS HERRAMIENTAS VISTAS PERMITEN **CONFIRMAR LA CONECTIVIDAD** CON UN NODO ICMP (**PING**), **CONOCER LA RUTA** HASTA UN DESTINO (**TRACEROUTE**), REVISAR LAS CONEXIONES LOCALES EXISTENTES (**NETSTAT**), Y **BUSCAR INFORMACIÓN PÚBLICA** SOBRE EL DESTINO (**NSLOOKUP**). AHORA, ES PRECISO INTRODUCIR HERRAMIENTAS ESPECÍFICAS PARA ANALIZAR NODOS REMOTOS.

EXISTEN MUCHAS APLICACIONES DE ANÁLISIS DE PUERTOS Y SERVICIOS, DE ENTRE LAS CUALES SE INTRODUCIRÁN A CONTINUACIÓN LAS MÁS RELEVANTES.

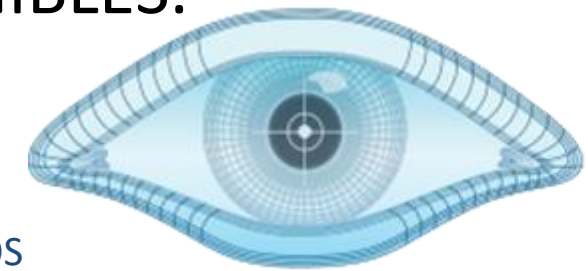
3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS DE ANÁLISIS DE PUERTOS

NMAP

DISPONIBLE PARA SISTEMAS WINDOWS Y LINUX, ES LA HERRAMIENTA DE USO MÁS EXTENDIDO, SIENDO SU EMPLEO CASI UN ESTÁNDAR DE FACTO.

PERMITE LLEVAR A CABO UN COMPLETO ANÁLISIS DE TODA UNA RED, DE UN RANGO DE DIRECCIONES, O DE UNA SOLA DIRECCIÓN IP, CENTRÁNDOSE EN DETERMINAR QUÉ PUERTOS Y SERVICIOS SE ENCUENTRAN DISPONIBLES.



NMAP

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS DE ANÁLISIS DE PUERTOS

NMAP

INCORPORA DIFERENTES PERFILES, PARA LLEVAR A CABO ANÁLISIS MÁS LIGEROS O MÁS EXHAUSTIVOS.

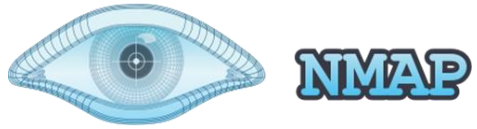
NMAP INTERPRETA LA MAYORÍA DE PROTOCOLOS ESTÁNDAR EMPLEADOS EN LA ACTUALIDAD, LO QUE LE PERMITE DEVOLVER INFORMACIÓN MUCHO MÁS COMPLETA QUE UN LISTADO DE PUERTOS ABIERTOS.

NMAP

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS DE ANÁLISIS DE PUERTOS

NMAP

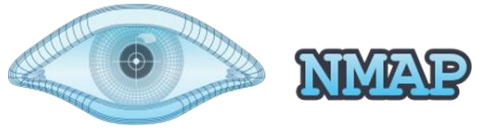


SI BIEN DISPONE DE UN INTERFAZ GRÁFICO, ES COMÚN EJECUTARLO EN LÍNEA DE COMANDOS, LO QUE LE PERMITE AJUSTAR SU FUNCIONAMIENTO DESDE UN SIMPLE ESCÁNER, PARA AVERIGUAR QUE EQUIPOS ESTÁN OPERATIVOS EN LA RED LOCAL, HASTA INTENTAR AVERIGUAR DETALLES CONCRETOS DE MÁQUINAS EXTERNAS.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS DE ANÁLISIS DE PUERTOS

NMAP



A CONTINUACIÓN, SE RESUMEN MUY BREVEMENTE SU SINTAXIS:

NMAP [TIPO(S) DE ANÁLISIS] [OPCIONES] {ESPECIFICACIÓN DE OBJETIVOS}

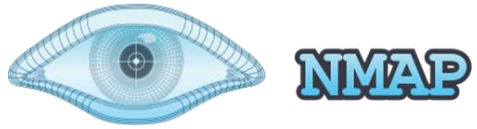
ESPECIFICACIÓN DE OBJETIVO

SE PUEDEN INDICAR NOMBRES DE SISTEMA, DIRECCIONES IP, REDES, ETC. EJEMPLO: “SCANME.NMAP.ORG”, “8.8.8.8”, “192.168.1.7-192.168.1.115”, ETC.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS DE ANÁLISIS DE PUERTOS

NMAP



DESCUBRIMIENTO DE HOSTS

-sL: LISTA LOS OBJETIVOS A ANALIZAR.

-sP: DETERMINA SI EL OBJETIVO RESPONDE A PING O ESTÁ “VIVO”.

-P0: ASUME QUE TODOS LOS OBJETIVOS ESTÁN VIVOS.

-PS/PA/PU [LISTADEPUERTOS]: ANÁLISIS TCP SYN, ACK O UDP DE LOS PUERTOS INDICADOS.

-PE/PP/PM: SOLICITA UN ANÁLISIS ICMP DEL TIPO HECHO, MARCA DE FECHA, Y MÁSCARA DE RED.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS DE ANÁLISIS DE PUERTOS

NMAP

ESPECIFICACIÓN DE PUERTOS

-p <RANGO DE PUERTOS>: SONDEAR LOS PUERTOS INDICADOS.

EJEMPLO:-P22;-P1-65535;-PU:53,111,137,T:21-25,80,139,8080.

-F: ANALIZAR LOS PUERTOS LISTADOS EN EL ARCHIVO NMAP-SERVICES.

-r: ANALIZAR LOS PUERTOS SECUENCIALMENTE, NO AL AZAR.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS DE ANÁLISIS DE PUERTOS

NMAP

DETECCIÓN DE SERVICIOS

-sV: SONDEAR PUERTOS ABIERTOS, PARA OBTENER INFORMACIÓN DE SERVICIO/VERSIÓN.

--VERSION-INTENSITY <NIVEL>: FIJAR DE 0 (LIGERO) A 9 (PROBAR TODAS LAS SONDAS).

--VERSION-LIGHT: LIMITAR A LAS SONDAS MÁS PROBABLES (INTENSIDAD 2).

--VERSION-ALL: UTILIZAR TODAS LAS SONDAS (INTENSIDAD 9).

--VERSION-TRACE: PRESENTAR ACTIVIDAD DETALLADA DEL ANÁLISIS (PARA DEPURAR).

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS DE ANÁLISIS DE PUERTOS

NMAP

DETECCIÓN DEL SISTEMA OPERATIVO

-O: ACTIVAR LA DETECCIÓN DE SISTEMA OPERATIVO (SO).

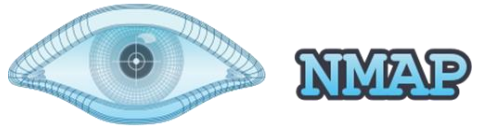
--OSSCAN-LIMIT: LIMITAR LA DETECCIÓN DE SO A OBJETIVOS PROMETEDORES.

--OSSCAN-GUESS: ADIVINAR EL SO DE LA FORMA MÁS AGRESIVA.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS DE ANÁLISIS DE PUERTOS

NMAP



OTRAS OPCIONES

-A: HABILITA LA DETECCIÓN DE SO Y DE VERSIÓN.

--PRIVILEGED: ASUMIR QUE EL USUARIO TIENE TODOS LOS PRIVILEGIOS.

-T [0-5]: SELECCIONAR PLANTILLA DE TEMPORIZADO (LOS NÚMEROS ALTOS SON MÁS RÁPIDOS).

-S <DIRECCIÓN_IP>: FALSIFICAR LA DIRECCIÓN IP ORIGEN.

-E <INTERFAZ>: UTILIZAR LA INTERFAZ INDICADA.

-g/--SOURCE-PORT <NUMPUERTO>: UTILIZAR EL NÚMERO DE PUERTO DADO.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS DE ANÁLISIS DE PUERTOS

NMAP

OTRAS OPCIONES

--SPOOF-MAC <DIRECCIÓN MAC >: FALSIFICAR LA DIRECCIÓN MAC.

-OA <NOMBRE_BASE>: GUARDAR EN LOS TRES FORMATOS PRINCIPALES AL MISMO TIEMPO.

-v: AUMENTAR EL NIVEL DE MENSAJES DETALLADOS (-VV PARA AUMENTAR EL EFECTO).

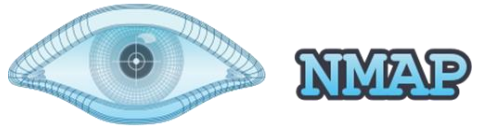
-V: MUESTRA EL NÚMERO DE VERSIÓN.

-h: MUESTRA LA AYUDA.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS DE ANÁLISIS DE PUERTOS

NMAP



DETECTA TODOS LOS EQUIPOS "VIVOS" EN LA RED LOCAL.

EJEMPLO: NMAP –sT –P0-1023 DIRECCIÓN_IP_REMOTA

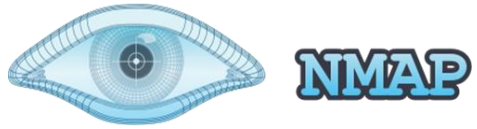
DETECTA TODOS LOS PUERTOS DE SISTEMA ABIERTOS DE UNA MÁQUINA REMOTA, SEGÚN EL PROCEDIMIENTO 3-WAY HANDSHAKE.

EJEMPLO: NMAP –sT –P0-1023 –sV DIRECCIÓN_IP_REMOTA

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS DE ANÁLISIS DE PUERTOS

NMAP



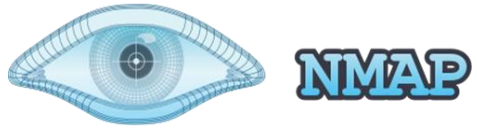
DETECTA TODOS LOS PUERTOS DE SISTEMA ABIERTOS DE UNA MÁQUINA REMOTA, SEGÚN EL PROCEDIMIENTO 3-WAY HANDSHAKE, Y ANALIZA LA VERSIÓN DE LOS SERVICIOS ENCONTRADOS.

EJEMPLO: NMAP –sT –P0-1023 –sV –O DIRECCIÓN_IP_REMOTA

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS DE ANÁLISIS DE PUERTOS

NMAP



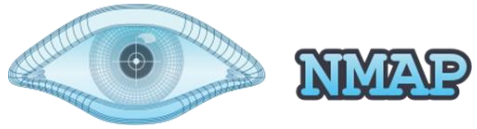
DETECTA PUERTOS, SERVICIOS, SUS VERSIONES, E INTENTA AVERIGUAR EL SISTEMA OPERATIVO DE LA MÁQUINA REMOTA.

PARA OBTENER TODA ESTA INFORMACIÓN, NMAP EMPLEA UN PROFUNDO ANÁLISIS DE LOS PAQUETES DEVUELTOS, Y PUEDE LLEGAR A REALIZAR PRUEBAS MUY EXHAUSTIVAS. DEBE TENERSE EN CUENTA QUE LA REALIZACIÓN DE SONDEOS EXHAUSTIVOS SOBRE UNA MÁQUINA AJENA PUEDE CONSIDERARSE UNA ACTIVIDAD PELIGROSA, INCLUSO SER CONSTITUTIVA DE DELITO, DE MANERA QUE EL LECTOR DEBE SER ESPECIALMENTE CUIDADOSO CON EL EMPLEO DE ESTA, Y OTRAS HERRAMIENTAS DE SEGURIDAD.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS DE ANÁLISIS DE PUERTOS

NMAP



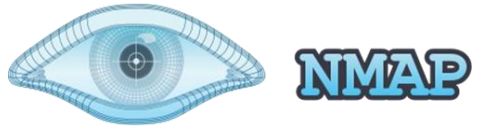
EN GENERAL, LOS SISTEMAS DE SEGURIDAD DEBERÍAN ESTAR PREPARADOS PARA RECHAZAR LA MAYORÍA DE ESTOS ANÁLISIS, O AL MENOS LOS MÁS INMEDIATOS.

POR EJEMPLO, ES HABITUAL QUE EL FIREWALL DE UNA EMPRESA NO RESPONDA EL PING, Y QUE, REGISTRE LA DIRECCIÓN IP QUE SE LO SOLICITA, PARA PROHIBIR POSTERIORES INTENTOS DE CONEXIÓN PROCEDENTES DE ESA DIRECCIÓN. TAMBIÉN ES MUY PROBABLE QUE UN EQUIPO DE SEGURIDAD PERIMETRAL SE CONFIGURE PARA NO ACEPTAR UN SONDEO ESTÁNDAR DE PUERTOS MEDIANTE 3-WAY HANDSHAKE.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS

HERRAMIENTAS DE ANÁLISIS DE PUERTOS

NMAP



AUNQUE LA HERRAMIENTA NMAP ESTÁ PROGRAMADA PARA SU EJECUCIÓN DESDE LA LÍNEA DE COMANDOS, LO QUE PERMITE UNA EJECUCIÓN MÁS ÁGIL, O PODER INCLUIRLA EN ARCHIVOS DE PROCESOS POR LOTES, O EN PLANIFICADORES DE TAREAS, TAMBIÉN PUEDE EMPLEARSE CON UN INTERFAZ GRÁFICO, DISPONIBLE EN LAS ÚLTIMAS VERSIONES.

CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN
3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS
4. **UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE TRÁFICO DE COMUNICACIONES PARA DETERMINAR EL USO REAL QUE HACEN LOS SISTEMAS DE INFORMACIÓN DE LOS DISTINTOS PROTOCOLOS, SERVICIOS Y PUERTOS**

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE TRÁFICO DE COMUNICACIONES PARA DETERMINAR EL USO REAL QUE HACEN LOS SISTEMAS DE INFORMACIÓN DE LOS DISTINTOS PROTOCOLOS, SERVICIOS Y PUERTOS

AHORA CORRESPONDE **CONOCER EL USO REAL QUE SE REALIZA DE LOS DISTINTOS SERVICIOS**, PARA PROHIBIR LAS COMUNICACIONES EN TODOS LOS PUERTOS QUE NO SE NECESITEN, Y PARA CONOCER SI SE ESTÁ LLEVANDO A CABO ALGUNA COMUNICACIÓN POR UN PUERTO NO PREVISTO.

SE REVISARÁ UN COMANDO DEL SISTEMA OPERATIVO QUE PERMITE ESTO DE MODO SENCILLO, PARA IR INTRODUCIENDO HERRAMIENTAS PAULATINAMENTE MÁS COMPLEJAS.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE TRÁFICO DE COMUNICACIONES PARA DETERMINAR EL USO REAL QUE HACEN LOS SISTEMAS DE INFORMACIÓN DE LOS DISTINTOS PROTOCOLOS, SERVICIOS Y PUERTOS

TCPDUMP

TCPDUMP NOS **PERMITIRÁ CAPTURAR TODO EL TRÁFICO DE RED DE UNA O VARIAS INTERFACES**, E INCLUSO TAMBIÉN INTERFACES VIRTUALES COMO LAS QUE CREAMOS AL USAR REDES PRIVADAS VIRTUALES.

ESTE PROGRAMA NO SOLAMENTE SE ENCARGA DE CAPTURAR TODO EL TRÁFICO, SINO QUE TAMBIÉN PODEMOS ANALIZARLO EN TIEMPO REAL A MEDIDA QUE LO VA CAPTURANDO, TODO ELLO A TRAVÉS DE LA LÍNEA DE COMANDOS

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE TRÁFICO DE COMUNICACIONES PARA DETERMINAR EL USO REAL QUE HACEN LOS SISTEMAS DE INFORMACIÓN DE LOS DISTINTOS PROTOCOLOS, SERVICIOS Y PUERTOS

TCPDUMP

ES COMPATIBLE CON LINUX, BSD, MACOS.

HACE USO DE LA BIBLIOTECA **LIBPCAP** PARA CAPTURAR LOS PAQUETES QUE CIRCULAN A TRAVÉS DE UNA INTERFAZ EN CUESTIÓN.

ES NECESARIO TENER PERMISOS DE SUPERUSUARIO.

LO MEJOR QUE TIENE **TCPDUMP** SON LOS **FILTROS**, VAMOS A **PODER FILTRAR TODO EL TRÁFICO PARA VER SOLAMENTE LO QUE A NOSOTROS NOS INTERESE**.

SON EXPRESIONES QUE VAN DETRÁS DE LAS OPCIONES DE CAPTURA, Y NOS PERMITE MOSTRAR SOLAMENTE LO QUE ESTAMOS BUSCANDO.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE TRÁFICO DE COMUNICACIONES PARA DETERMINAR EL USO REAL QUE HACEN LOS SISTEMAS DE INFORMACIÓN DE LOS DISTINTOS PROTOCOLOS, SERVICIOS Y PUERTOS

TCPDUMP

LOS PRINCIPALES USOS QUE LE PODEMOS DAR A UNA HERRAMIENTA COMO TCPDUMP SON LOS SIGUIENTES:

- CAPTURAR TODA LA INFORMACIÓN Y ALMACENARLA PARA SU POSTERIOR ESTUDIO.
- DEPURAR APLICACIONES EN TIEMPO REAL QUE USAN LA RED PARA COMUNICARSE.
- COMPROBAR QUE EL TRÁFICO DE RED ES EL ESPERADO TENIENDO EN CUENTA SU USO.
- CAPTURAR Y LEER LOS DATOS DE OTROS EQUIPOS DE LA RED, AUNQUE EN ESTE CASO TENDRÍAMOS QUE HACER TÉCNICAS COMO EL ARP SPOOFING O SIMILAR.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE TRÁFICO DE COMUNICACIONES PARA DETERMINAR EL USO REAL QUE HACEN LOS SISTEMAS DE INFORMACIÓN DE LOS DISTINTOS PROTOCOLOS, SERVICIOS Y PUERTOS

TCPDUMP

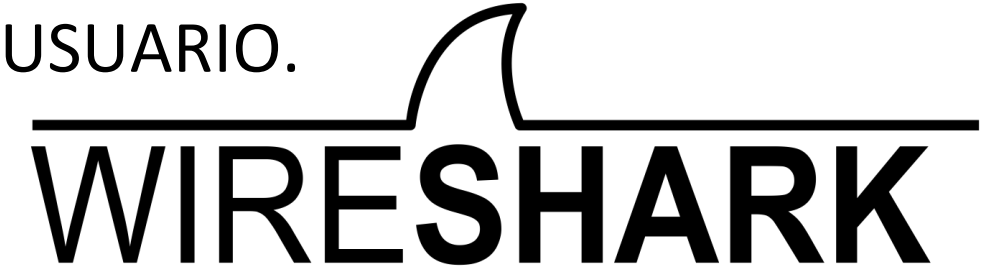
```
root@pru-VirtualBox:/home/pru# tcpdump -i enp0s3 -v
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
05:14:56.958361 IP (tos 0x0, ttl 128, id 40280, offset 0, flags [none], proto UDP (17), length 78)
    192.168.1.37.netbios-ns > 192.168.1.255.netbios-ns: UDP, length 50
05:14:56.959681 IP6 (flowlabel 0x63753, hlim 1, next-header UDP (17) payload length: 41) fe80::38b:fe9:cb6e:d24c.51260 > ff02::1:
05:14:56.959682 IP (tos 0x0, ttl 1, id 59411, offset 0, flags [none], proto UDP (17), length 61)
    192.168.1.37.51260 > 224.0.0.252.hostmon: UDP, length 33
05:14:56.958815 IP (tos 0x0, ttl 64, id 13369, offset 0, flags [DF], proto UDP (17), length 83)
    pru-VirtualBox.60487 > 250.red-80-58-61.staticip.rima-tde.net.domain: 18230+ [1au] PTR? 255.1.168.192.in-addr.arpa. (55)
05:14:56.964159 IP (tos 0x0, ttl 58, id 0, offset 0, flags [DF], proto UDP (17), length 60)
    mad41s11-in-f10.1e100.net.443 > 192.168.1.37.62283: UDP, length 32
05:14:56.972513 IP (tos 0x0, ttl 128, id 53588, offset 0, flags [DF], proto UDP (17), length 61)
    192.168.1.37.62283 > mad41s11-in-f10.1e100.net.443: UDP, length 33
05:14:56.990629 IP (tos 0x0, ttl 1, id 37618, offset 0, flags [none], proto UDP (17), length 67)
    192.168.1.37.mdns > 224.0.0.251.mdns: 0 A (QM)? BRWB05216CD6A0B.local. (39)
05:14:56.990908 IP6 (flowlabel 0x081d8, hlim 1, next-header UDP (17) payload length: 47) fe80::38b:fe9:cb6e:d24c.mdns > ff02::fb.
D6A0B.local. (39)
05:14:56.991201 IP (tos 0x0, ttl 1, id 37619, offset 0, flags [none], proto UDP (17), length 67)
    192.168.1.37.mdns > 224.0.0.251.mdns: 0 A (QM)? BRWB05216CD6A0B.local. (39)
05:14:56.991459 IP6 (flowlabel 0x081d8, hlim 1, next-header UDP (17) payload length: 47) fe80::38b:fe9:cb6e:d24c.mdns > ff02::fb.
D6A0B.local. (39)
05:14:56.995574 IP (tos 0x0, ttl 55, id 57650, offset 0, flags [DF], proto UDP (17), length 160)
    250.red-80-58-61.staticip.rima-tde.net.domain > pru-VirtualBox.60487: 18230 NXDomain 0/1/1 (132)
05:14:56.994643 IP (tos 0x0, ttl 64, id 13370, offset 0, flags [DF], proto UDP (17), length 72)
    pru-VirtualBox.60487 > 250.red-80-58-61.staticip.rima-tde.net.domain: 18230+ PTR? 255.1.168.192.in-addr.arpa. (44)
05:14:57.030771 IP (tos 0x0, ttl 56, id 57654, offset 0, flags [DF], proto UDP (17), length 149)
    250.red-80-58-61.staticip.rima-tde.net.domain > pru-VirtualBox.60487: 18230 NXDomain 0/1/0 (121)
05:14:57.030795 IP (tos 0x0, ttl 64, id 65375, offset 0, flags [DF], proto UDP (17), length 82)
    pru-VirtualBox.41749 > 250.red-80-58-61.staticip.rima-tde.net.domain: 4652+ [1au] PTR? 37.1.168.192.in-addr.arpa. (54)
05:14:57.068028 IP (tos 0x0, ttl 246, id 45525, offset 0, flags [none], proto UDP (17), length 141)
```

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE TRÁFICO DE COMUNICACIONES PARA DETERMINAR EL USO REAL QUE HACEN LOS SISTEMAS DE INFORMACIÓN DE LOS DISTINTOS PROTOCOLOS, SERVICIOS Y PUERTOS

WIRESHARK

TANTO PARA SISTEMAS WINDOWS COMO LINUX, ESTA HERRAMIENTA **ES EL CAPTURADOR DE PAQUETES MÁS EXTENDIDO**, Y ES CASI UN ESTÁNDAR.

SU FUNCIONAMIENTO BÁSICO SUPONE **EMPEZAR A CAPTURAR DATOS PARA POSTERIORMENTE PROCESARLOS**, APLICANDO EL AMPLIO CONJUNTO DE PROTOCOLOS QUE ES CAPAZ DE INTERPRETAR, DE MANERA QUE PUEDE PRESENTAR LA INFORMACIÓN DE UNA FORMA FÁCILMENTE INTERPRETABLE PARA EL USUARIO.



3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE TRÁFICO DE COMUNICACIONES PARA DETERMINAR EL USO REAL QUE HACEN LOS SISTEMAS DE INFORMACIÓN DE LOS DISTINTOS PROTOCOLOS, SERVICIOS Y PUERTOS

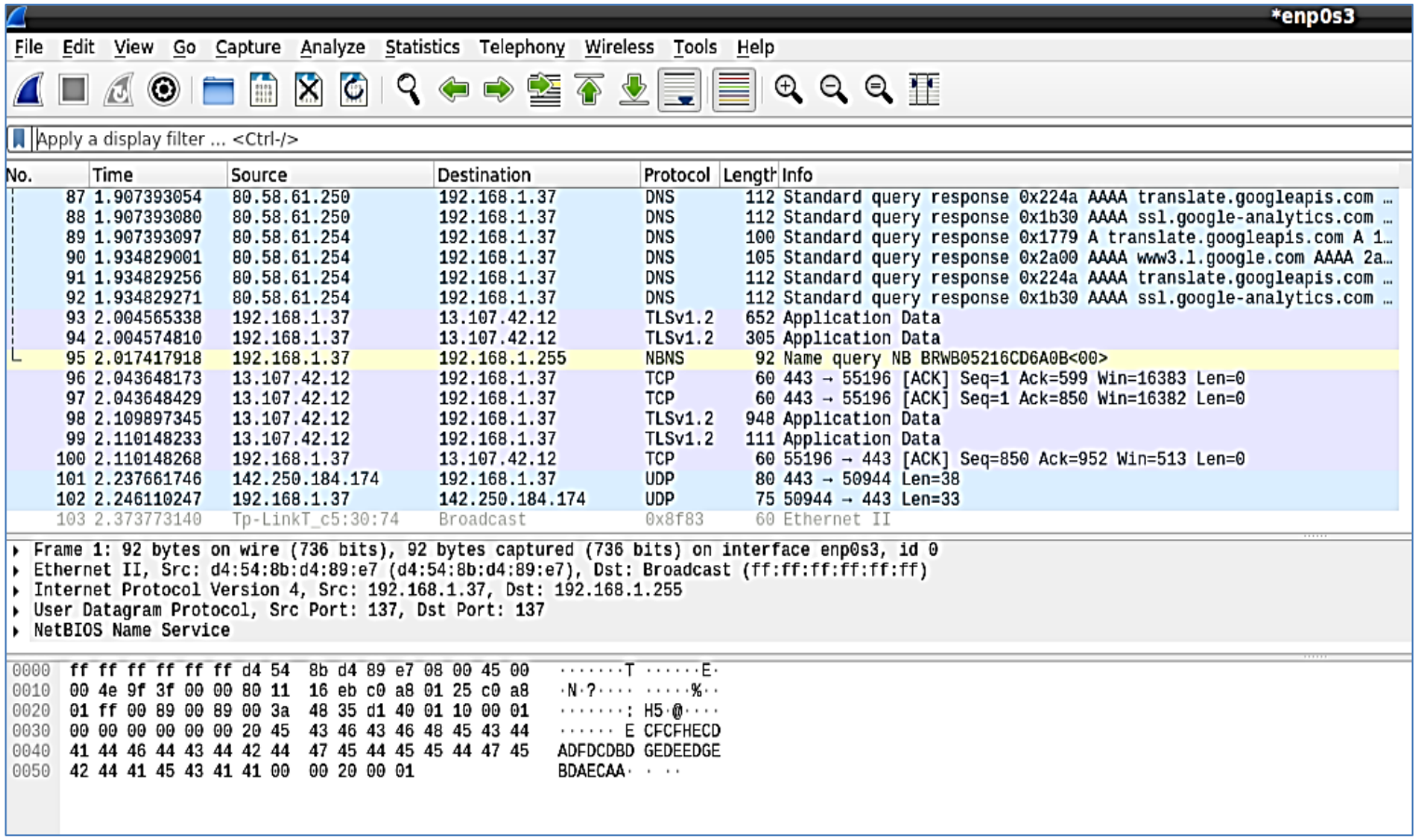
WIRESHARK

PARA ANALIZAR EL TRÁFICO, LA APLICACIÓN **PERMITE CONSTRUIR FILTROS QUE ELIMINEN TODO EL TRÁFICO QUE NO INTERESA**, POR EJEMPLO, PORQUE CORRESPONDA A SERVICIOS CONOCIDOS QUE NO SE QUIERAN ANALIZAR. DE OTRA MANERA, EL VOLUMEN DE INFORMACIÓN ES TAN ALTO, QUE PUEDE RESULTAR COMPLEJO EXTRAER RESULTADOS.

EN GENERAL, HASTA QUE UNA APLICACIÓN DE CAPTURA DE TRÁFICO NO SE REDUZCA A LAS CONDICIONES DE ESTUDIO EXACTAS QUE SE REQUIEREN ANALIZAR, SU USO PUEDE RESULTAR LABORIOSO.

3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE TRÁFICO DE COMUNICACIONES PARA DETERMINAR EL USO REAL QUE HACEN LOS SISTEMAS DE INFORMACIÓN DE LOS DISTINTOS PROTOCOLOS, SERVICIOS Y PUERTOS

WIRESHARK



ESTO ES TODO