Sumario

UT 02 – Apéndice: Exploradores de red

Introducción a las herramientas de red

Este apéndice se incluye en la Unidad de Trabajo como material adicional (de estudio no obligatorio) para proporcionar al alumno información y herramientas relacionadas con la administración de redes.

Para obtener información acerca del comportamiento de un sistema, redes de comunicaciones, puertos abiertos, otros equipos conectados a la red, etc... se utilizan diferentes herramientas. Veamos algunas de ellas.

Explorar un segmento de red: nmap

El siguiente artículo muestra algunos ejemplos de uso de la herramienta nmap:

http://rm-rf.es/nmap-linux-uso-ejemplos/

Por ejemplo, para mostrar los puertos disponibles en un equipo:

```
$ nmap 192.168.0.219
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-09 18:45 CET
Nmap scan report for Audax (192.168.0.219)
Host is up (0.00013s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2049/tcp  open  nfs
10000/tcp open  snet-sensor-mgmt
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

Mostrar las rutas e interfaces de red de un equipo:

```
# nmap --iflist 192.168.1.100

Starting Nmap 5.21 ( http://nmap.org ) at 2014-09-26 18:45 CEST
************************INTERFACES************************
DEV  (SHORT) IP/MASK        TYPE     UP MAC
lo   (lo)    127.0.0.1/8    loopback up
eth0 (eth0)  192.168.1.100/24 ethernet up XX:XX:XX:XX:XX:XX

**************************ROUTES**************************
DST/MASK      DEV  GATEWAY
192.168.1.0/0  eth0
169.254.0.0/0 eth0
0.0.0.0/0     eth0 192.168.1.1
```

Explorar el propio sistema: netstat

La herramienta netstat proporciona información del propio sistema en el que se ejecuta, como conexiones abiertas, puertos, etc...

https://www.linux-party.com/29-internet/8969-20-comandos-netstat-para-administradores-de-redes-linux

Por ejemplo, para ver los puertos activos:

```
$ netstat -at
Conexiones activas de Internet (servidores y establecidos)
Proto  Recib Enviad Dirección local         Dirección remota       Estado
tcp        0      0 localhost:mysql         0.0.0.0:*              ESCUCHAR
tcp        0      0 0.0.0.0:netbios-ssn     0.0.0.0:*              ESCUCHAR
tcp        0      0 0.0.0.0:41131           0.0.0.0:*              ESCUCHAR
tcp        0      0 0.0.0.0:39213           0.0.0.0:*              ESCUCHAR
tcp        0      0 localhost:24271         0.0.0.0:*              ESCUCHAR
tcp        0      0 0.0.0.0:sunrpc          0.0.0.0:*              ESCUCHAR
tcp        0      0 0.0.0.0:webmin          0.0.0.0:*              ESCUCHAR
tcp        0      0 0.0.0.0:33173           0.0.0.0:*              ESCUCHAR
tcp        0      0 localhost:domain        0.0.0.0:*              ESCUCHAR
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*              ESCUCHAR
tcp        0      0 localhost:ipp           0.0.0.0:*              ESCUCHAR
tcp        0      0 0.0.0.0:db-lsp          0.0.0.0:*              ESCUCHAR
tcp        0      0 0.0.0.0:microsoft-ds    0.0.0.0:*              ESCUCHAR
tcp        0      0 0.0.0.0:41021           0.0.0.0:*              ESCUCHAR
tcp        0      0 localhost:17600         0.0.0.0:*              ESCUCHAR
tcp        0      0 0.0.0.0:nfs             0.0.0.0:*              ESCUCHAR
tcp        0      0 localhost:51235         0.0.0.0:*              ESCUCHAR
tcp        0      0 localhost:17603         0.0.0.0:*              ESCUCHAR
tcp        0      0 Audax:39326             213.229.137.37:imap2   CLOSE_WAIT
tcp        0      0 localhost:43250         localhost:51235        TIME_WAIT
tcp        1      0 Audax:46316             ec2-52-203-89-21.:https CLOSE_WAIT
tcp        0      0 Audax:60260             wa-in-f109.1e100.:imaps ESTABLECIDO
```

Estadísticas por protocolo:

```
$ netstat -s
Ip:
    Forwarding: 2
    131905 total packets received
    1 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    126382 incoming packets delivered
    114337 requests sent out
    22 outgoing packets dropped
    3 dropped because of missing route
```

```
Icmp:
    1921 ICMP messages received
    1012 input ICMP message failed
    histograma de entrada ICMP:
        destination unreachable: 1082
        echo requests: 839
    1892 ICMP messages sent
    0 ICMP messages failed
    histograma de salida ICMP:
        destination unreachable: 1053
        echo replies: 839
IcmpMsg:
        InType3: 1082
        InType8: 839
        OutType0: 839
        OutType3: 1053
Tcp:
    6563 active connection openings
    1014 passive connection openings
    2019 failed connection attempts
    466 connection resets received
    18 connections established
    77693 segments received
    91235 segments sent out
    214 segments retransmitted
    0 bad segments received
    3399 resets sent
Udp:
    75158 packets received
    43 packets to unknown port received
    0 packet receive errors
    25297 packets sent
    0 receive buffer errors
    2 send buffer errors
    IgnoredMulti: 716
```

Análisis avanzado: wireshark (anteriormente ethereal)

Para poder usar la herramienta wireshark hay que tener permisos suficientes, además de cumplir con la legislación oportuna. Podría ser ilegal realizar ciertas operaciones de análisis de red con esta herramienta.

El siguiente artículo es una pequeña introducción a la instalación y uso de wireshark:

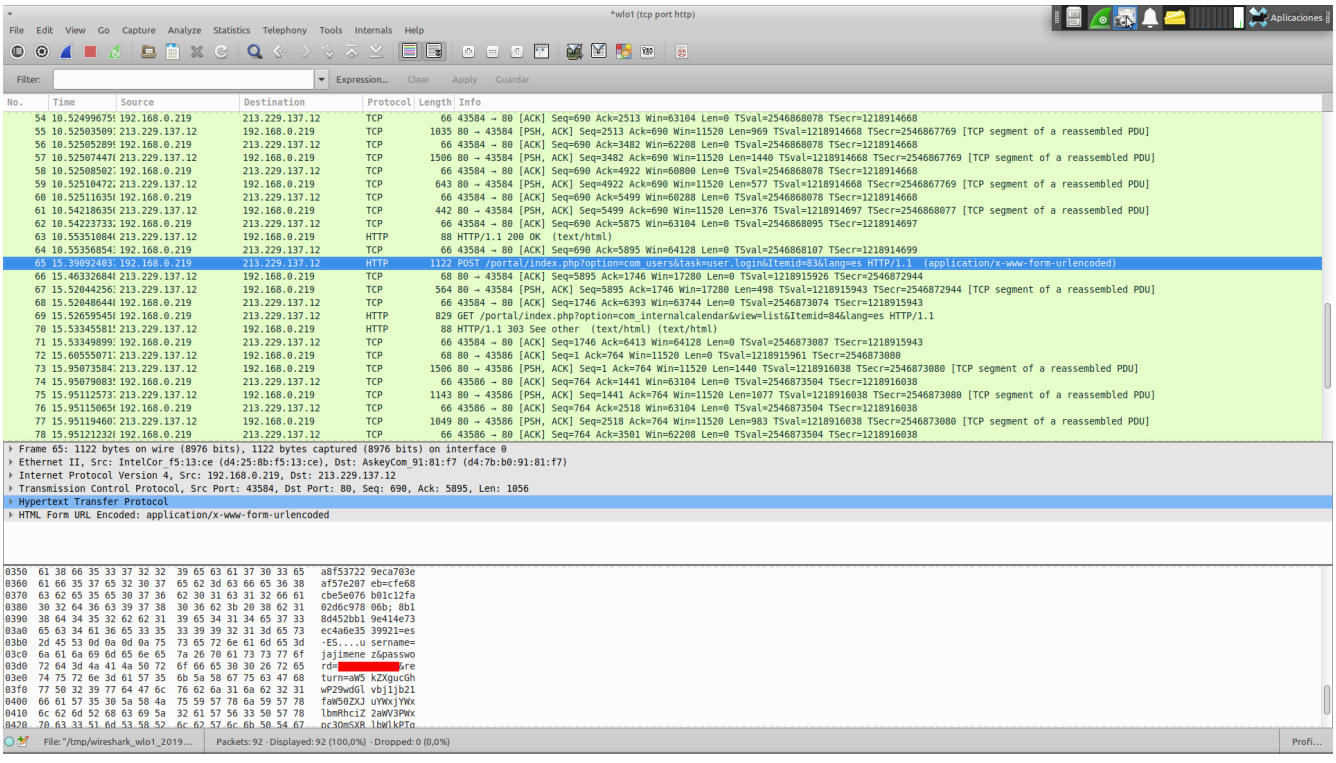
https://geekytheory.com/curso/wireshark/instalar-wireshark

Si queremos usar esta herramienta con un usuario diferente de root hay que darle permisos, añadiéndolo al grupo “wireshark”:

```
$    usermod -a -g wireshark jose
```

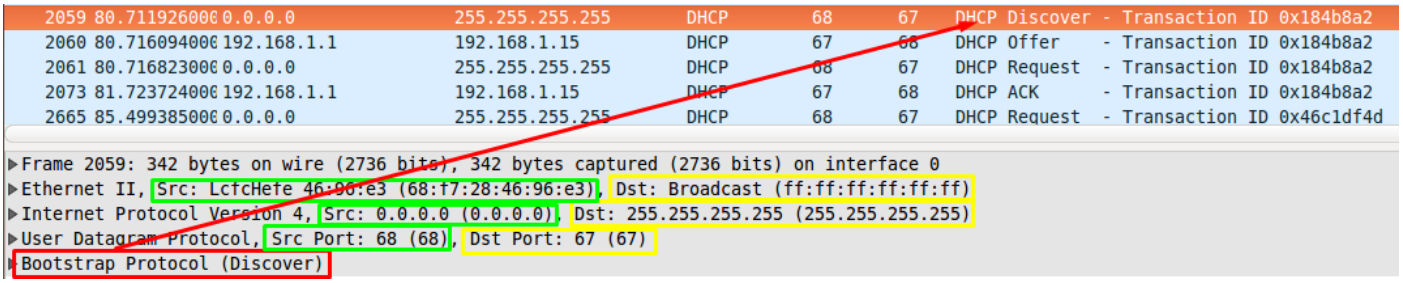
Existe una utilidad similar, en modo comando: **tshark** (hay que ejecutarla como root, mediante “sudo tshark”).

Veamos un ejemplo sobre la captura de las tramas en una red durante una conexión HTTP no segura. En este ejemplo se ve cómo la contraseña del usuario viaja sin encriptar por la red, y por tanto se podría capturar con una herramienta como wireshark:

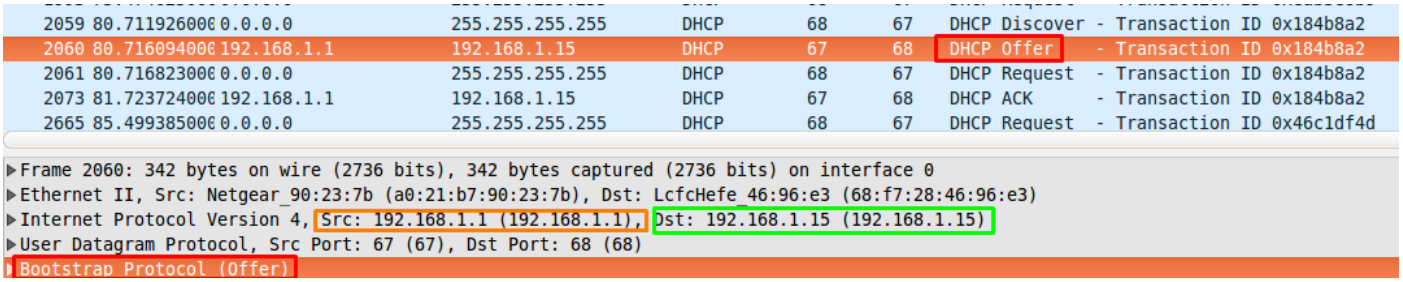


Ahora veamos un ejemplo de captura de tramas durante el proceso de asignación de parámetros de red por DHCP:

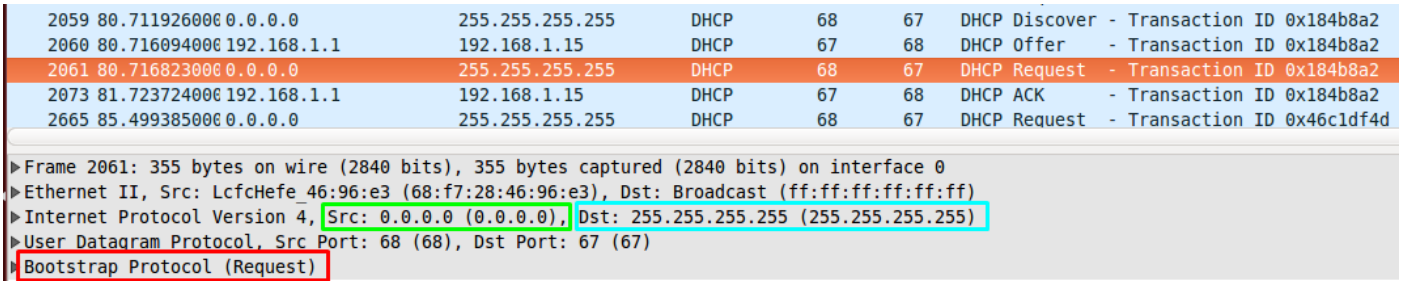
Paso 1: DHCP DISCOVER



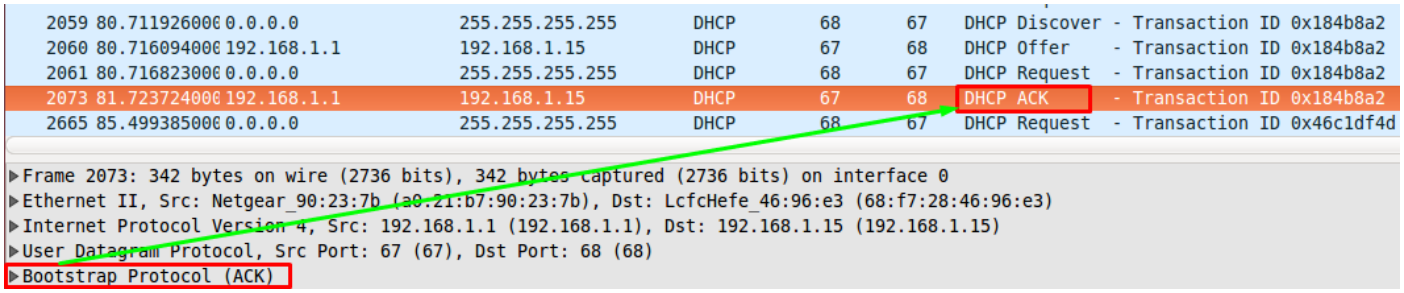
Paso 2: DHCP OFFER



Paso 3: DCHP REQUEST



Paso 4: DHCP ACK



Tutoriales y ejemplos de análisis de redes

Para finalizar, enlazamos algunos artículos relacionados con herramientas de análisis de red:

https://seguridadyredes.wordpress.com/2008/02/14/analisis-de-red-con-wireshark-interpretando-los-datos/

https://seguridadyredes.wordpress.com/2008/04/30/tshark-wireshark-en-linea-de-comandos-i-parte/

Y aquí tenemos dos artículos más, relativos al uso de nmap y netstat:

https://infosegur.wordpress.com/unidad-5/servicios-de-red-nmap-y-netstat/

https://superuser.com/questions/1065478/what-is-the-difference-between-nmap-and-netstat