



PRACTICA 4

C.E.S ACADEMIA LOPE DE VEGA

CFGS: 2º Administración de Sistemas Informáticos en Red

Curso: 2017/2018

Asignatura: Seguridad y Alta Disponibilidad

Prof. Miguel Angel González

Autor: Rafael Osuna Ventura

WIRESHARK

Wireshark es un analizador de protocolos open-source diseñado por Gerald Combs y que actualmente está disponible para plataformas Windows y Unix. Su principal objetivo es el análisis del tráfico de datos.

Wireshark es de software libre y puede ejecutarse en la mayoría de sistemas operativos Unix y compatibles incluyendo Linux, Solaris, Android, Mac OS X, NetBSD, FreeBSD, Microsoft Windows, entre otros.

Este programa nos permite solucionar o prevenir posibles problemas existentes en nuestra red. También nos puede ser muy útil si lo enfocamos de una forma didáctica, ya que nos permite ver los diferentes protocolos con sus cabeceras. Y, por último, nos puede servir para intentar robar información.



Wireshark posee una interfaz muy fácil de usar y una gran variedad de filtros de búsqueda para facilitarte la misma respecto a los 1100 protocolos que se soportan actualmente.

Existen dos tipos de filtros:

- filtros de captura: son los que se establecen para mostrar solo los paquetes que cumplan los requisitos indicados en el filtro. Si no utilizamos ningún wireshark por defecto nos capturará todo el tráfico existente. Algún ejemplo puede ser para filtrar un host en concreto o capturar solo el trafico broadcast.
- filtros de visualización: son los que establecen un criterio sobre los paquetes que estamos capturando y que nos aparecen en pantalla, es decir, con estos filtros solo nos aparecerá en pantalla lo que nosotros deseemos ver aunque se está capturando todo el tráfico.

Los filtros más comunes son los que hacen referencia a algunos protocolos como: telnet, dns, msnm (mensajería instantánea), ip, ftp,tcp,etc.

Para utilizar wireshark solo deberemos seleccionar el modo de conexión por el que vamos a capturar el tráfico, es decir wifi o ethernet, establecer un filtro si así lo deseamos y luego le daremos a comenzar.

Tras realizar la captura nos aparecen en pantalla 3 zonas:

-1ªZona: se encuentra en la parte superior y es el listado de los paquetes capturados. La información de este listado se hace en columnas, como el tiempo que se ha tardado en capturar el paquete, el origen y destino, información extra....

-2ªZona: se encuentra en la parte del medio y se nos muestra los datos del frame capturados.

-3ªZona: se encuentra en la parte inferior y nos permite separar la cada una de las cabeceras del frame de la zona 2.

1ªZona

No.	Time	Source	Destination	Protocol	Length	Info
2523	19.182145	85.214.155.142	192.168.0.102	HTTP	535	HTTP/1.1 200 OK (text/html)
2519	19.143453	85.214.155.142	192.168.0.102	HTTP	433	HTTP/1.1 200 OK (text/html) (text/html)
2514	19.070066	192.168.0.102	85.214.155.142	HTTP	581	GET /aulavirtual/calendar/overlib.cfg.php HTTP/1.1
2512	19.069138	85.214.155.142	192.168.0.102	HTTP	1119	HTTP/1.1 200 OK (text/html)
2496	19.001097	192.168.0.102	85.214.155.142	HTTP	651	GET /aulavirtual/login/environment.php?sesskey=gb9zkD282&flashversion=27.0.0 HTTP/1.1
2476	18.771754	192.168.0.102	85.214.155.142	HTTP	710	GET /aulavirtual/ HTTP/1.1
2475	18.766824	85.214.155.142	192.168.0.102	HTTP	990	HTTP/1.1 303 See Other (text/html)
2473	18.418029	192.168.0.102	85.214.155.142	HTTP	888	POST /aulavirtual/login/index.php HTTP/1.1 (application/x-www-form-urlencoded)
2451	8.013479	85.214.155.142	192.168.0.102	HTTP	220	HTTP/1.1 200 OK (text/html)
2435	7.737139	192.168.0.102	85.214.155.142	HTTP	684	GET /aulavirtual/login/index.php HTTP/1.1
2433	6.488802	85.214.155.142	192.168.0.102	HTTP	535	HTTP/1.1 200 OK (text/html)

2ªZona

```
Transmission Control Protocol, Src Port: 60182, Dst Port: 80, Seq: 2992, Ack: 66196, Len: 834
  Source Port: 60182
  Destination Port: 80
  [Stream index: 7]
  [TCP Segment Len: 834]
  Sequence number: 2992 (relative sequence number)
  [Next sequence number: 3826 (relative sequence number)]
  Acknowledgment number: 66196 (relative ack number)
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
  Window size value: 67
  [Calculated window size: 17152]
  [Window size scaling factor: 256]
```

3ªZona

```
0030 00 43 4a e2 00 00 50 4f 53 54 20 2f 61 75 6c 61 .C)...PO ST /aula
0040 76 69 72 74 75 61 6c 2f 6c 6f 67 69 6e 2f 69 6e virtual/ login/in
0050 64 65 78 2e 70 68 70 20 4b 54 50 2f 31 2e 31 dex.php HTTP/1.1
0060 0d 0a 4b 6f 73 74 3a 20 61 63 61 64 65 6d 69 61 .Host: academia
0070 6c 6f 70 65 64 65 76 65 67 61 2e 6f 72 67 0d 0a lopedeve ga.org..
0080 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 Connecti on: keep
0090 2d 61 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d -alive.. Content-
00a0 4c 65 6e 67 74 68 3a 20 35 34 0d 0a 43 61 63 68 Length: 54..Cach
00b0 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 e-Contro l: max-a
00c0 67 65 3d 30 0d 0a 4f 72 69 67 69 6e 3a 20 68 74 ge=0..Or igin: ht
00d0 74 70 3a 2f 2f 61 63 61 64 65 6d 69 61 6c 6f 70 tp://aca demialop
00e0 65 64 65 76 65 67 61 2e 6f 72 67 0d 0a 55 70 67 edevega. org..Upg
00f0 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 rade-Ins ecure-Re
0100 71 75 65 73 74 73 3a 20 31 0d 0a 43 6f 6e 74 65 quests: 1..Conte
```

De cara a la interfaz de usuario wireshark utiliza un código de colores para clasificar cada entrada:

- Gris: información sobre flujos normales
- Cian: situaciones importantes fuera de lo normal
- Amarillo: hay que prestar atención
- Rojo: problemas graves.

Cabe destacar el uso de herramientas externas ya que estas nos ayudan a procesar de forma más rápida las capturas realizadas con wireshark cuando el nivel de estas sea muy amplio. Algunas de estas herramientas son snort.

Ahora vamos a realizar una prueba de concepto para comprobar las funcionalidades de wireshark. Para ello vamos a realizar una conexión al aula virtual del instituto y vamos a iniciar sesión. De esto esperamos obtener información sobre dicha conexión, tal como mi usuario y contraseña. Vamos a aplicar un filtro en los protocolos para que se nos muestren solo los datos con protocolo http.

No.	Time	Source	Destination	Protocol	Length	Info
2523	19.182145	85.214.155.142	192.168.0.102	HTTP	535	HTTP/1.1 200 OK (text/html)
2519	19.143453	85.214.155.142	192.168.0.102	HTTP	433	HTTP/1.1 200 OK (text/html) (text/html)
2514	19.070066	192.168.0.102	85.214.155.142	HTTP	581	GET /aulavirtual/calendar/overlib.cfg.php HTTP/1.1
2512	19.069138	85.214.155.142	192.168.0.102	HTTP	1119	HTTP/1.1 200 OK (text/html)
2496	19.001097	192.168.0.102	85.214.155.142	HTTP	651	GET /aulavirtual/login/environment.php?sesskey=gb9zKdD2B2&flashversion=27.0.0 HTTP/1.1
2476	18.771754	192.168.0.102	85.214.155.142	HTTP	710	GET /aulavirtual/ HTTP/1.1
2475	18.766824	85.214.155.142	192.168.0.102	HTTP	990	HTTP/1.1 303 See Other (text/html)
2473	18.418029	192.168.0.102	85.214.155.142	HTTP	888	POST /aulavirtual/login/index.php HTTP/1.1 (application/x-www-form-urlencoded)
2451	8.013479	85.214.155.142	192.168.0.102	HTTP	220	HTTP/1.1 200 OK (text/html)
2435	7.737139	192.168.0.102	85.214.155.142	HTTP	684	GET /aulavirtual/login/index.php HTTP/1.1
2433	6.488072	85.214.155.142	192.168.0.102	HTTP	535	HTTP/1.1 200 OK (text/html)
2432	6.373515	192.168.0.102	85.214.155.142	HTTP	581	GET /aulavirtual/calendar/overlib.cfg.php HTTP/1.1
2430	6.369699	85.214.155.142	192.168.0.102	HTTP	1128	HTTP/1.1 200 OK (text/html)
2411	6.056754	192.168.0.102	85.214.155.142	HTTP	639	GET /aulavirtual/ HTTP/1.1
2410	6.052113	85.214.155.142	192.168.0.102	HTTP	809	HTTP/1.1 303 See Other (text/html)
2409	5.837435	192.168.0.102	85.214.155.142	HTTP	704	GET /aulavirtual/login/logout.php?sesskey=BGF8qChmlG HTTP/1.1
1620	3.377448	85.214.155.142	192.168.0.102	HTTP	1045	HTTP/1.1 200 OK (text/css)
1494	3.265584	85.214.155.142	192.168.0.102	HTTP	535	HTTP/1.1 200 OK (text/html)
1339	3.142558	192.168.0.102	85.214.155.142	HTTP	581	GET /aulavirtual/calendar/overlib.cfg.php HTTP/1.1
1118	2.947640	85.214.155.142	192.168.0.102	HTTP	1490	HTTP/1.1 200 OK (text/html)
1111	2.932582	192.168.0.102	85.214.155.142	HTTP	653	GET /aulavirtual/theme/custom_corners/styles.php HTTP/1.1
646	2.534414	192.168.0.102	85.214.155.142	HTTP	616	GET /aulavirtual/ HTTP/1.1

Esto es lo que obtendríamos, ahora vamos a buscar en el archivo en el que aparece que hemos iniciado sesión para intentar obtener información, y encontramos que aparecen nuestros datos con los cuales hemos accedido. Esto demuestra lo fácil que puede ser robar una contraseña.

Wireshark · Packet 2473 · wireshark_7FF9E3E4-6B25-4C49-8C94-7A1EE972F9A5_20171019223547_a14376

```
> Frame 2473: 888 bytes on wire (7104 bits), 888 bytes captured (7104 bits) on interface 0
> Ethernet II, Src: IntelCor_80:eb:84 (7c:b0:c2:80:eb:84), Dst: Tp-LinkT_8b:9f:90 (18:a6:f7:8b:9f:90)
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 85.214.155.142
> Transmission Control Protocol, Src Port: 60182, Dst Port: 80, Seq: 2992, Ack: 66196, Len: 834
> Hypertext Transfer Protocol
  > HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "username" = "rafaosuna"
    > Form item: "password" = "Rafaespejo.1"
    > Form item: "testcookies" = "1"
```

NETWORKMINER

NetworkMiner se trata de una herramienta que se utiliza para el análisis forense de datos. La característica principal es la opción de analizar una captura de paquetes tanto de forma activa como pasiva, es decir, podemos capturar el tráfico directamente y analizarlo o analizar el tráfico de una captura que hallamos realizado con otra herramienta, por ejemplo, Wireshark.

Tiene muchas funcionalidades, pero caben destacar:

- Visualización de todos los archivos que al capturar paquetes son descargados (tipo json,html o cualquier otro archivo que pueda abrir nuestro navegador)

- Fácil visualización de las capturas

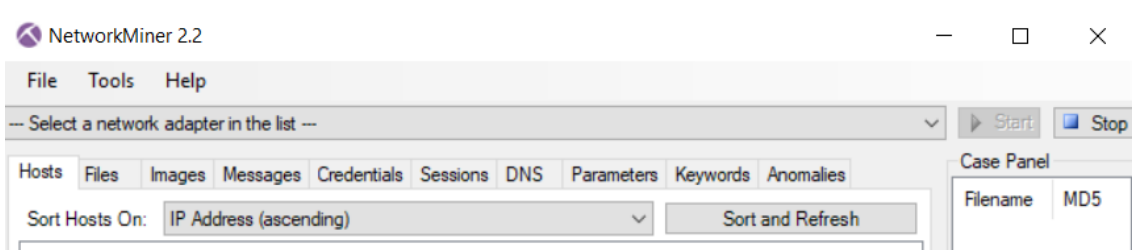
- Facilidad para ver las cookies recogidas respecto al host al que pertenecen, así como otros datos que hacen referencia a estas.

- Pestaña dedicada a DNS

- Extracción de imágenes

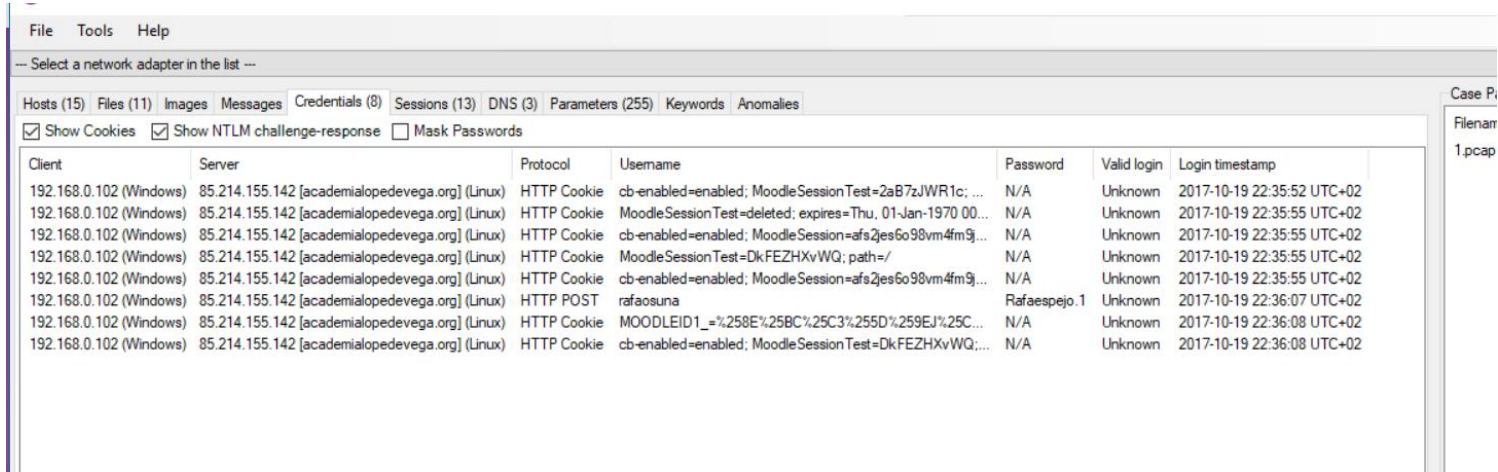


NetworkMiner posee una interfaz muy intuitiva que nos clasifica la información en diferentes pestañas. Por ejemplo, en la pestaña host se nos muestra las características del host con una gran información sobre este, se nos muestra el sistema operativo que usa, así como el puerto por el que escucha y si está utilizando algún servidor, como podría ser apache.



Procedemos a realizar una prueba de concepto, para ello utilizaremos la captura de tráfico realiza antes en wireshark y observaremos que datos nos proporciona networkminer de ella.

Vemos que obtenemos también los datos con los que he iniciado sesión. En la pestaña sesión podemos observar a la hora que se ha realizado la conexión.



The screenshot shows the NetworkMiner application interface. The 'Sessions' tab is selected, displaying a list of login attempts. The table includes columns for Client, Server, Protocol, Username, Password, Valid login, and Login timestamp. The data shows multiple failed login attempts from 192.168.0.102 to 85.214.155.142 using various usernames and passwords. The last entry shows a successful login for 'rafaosuna' at 2017-10-19 22:36:07 UTC+02.

Client	Server	Protocol	Username	Password	Valid login	Login timestamp
192.168.0.102 (Windows)	85.214.155.142 [academialopedevaga.org] (Linux)	HTTP Cookie	cb-enabled=enabled; MoodleSessionTest=2aB7zJWR1c; ...	N/A	Unknown	2017-10-19 22:35:52 UTC+02
192.168.0.102 (Windows)	85.214.155.142 [academialopedevaga.org] (Linux)	HTTP Cookie	MoodleSessionTest=deleted; expires=Thu, 01-Jan-1970 00...	N/A	Unknown	2017-10-19 22:35:55 UTC+02
192.168.0.102 (Windows)	85.214.155.142 [academialopedevaga.org] (Linux)	HTTP Cookie	cb-enabled=enabled; MoodleSession=afs2jes6o98vm4fm9...	N/A	Unknown	2017-10-19 22:35:55 UTC+02
192.168.0.102 (Windows)	85.214.155.142 [academialopedevaga.org] (Linux)	HTTP Cookie	MoodleSessionTest=DkFEZHxvWQ; path=	N/A	Unknown	2017-10-19 22:35:55 UTC+02
192.168.0.102 (Windows)	85.214.155.142 [academialopedevaga.org] (Linux)	HTTP Cookie	cb-enabled=enabled; MoodleSession=afs2jes6o98vm4fm9...	N/A	Unknown	2017-10-19 22:35:55 UTC+02
192.168.0.102 (Windows)	85.214.155.142 [academialopedevaga.org] (Linux)	HTTP POST	rafaosuna	Rafaespejo.1	Unknown	2017-10-19 22:36:07 UTC+02
192.168.0.102 (Windows)	85.214.155.142 [academialopedevaga.org] (Linux)	HTTP Cookie	MOODLEID1_=%258E%25BC%25C3%255D%259EJ%25C...	N/A	Unknown	2017-10-19 22:36:08 UTC+02
192.168.0.102 (Windows)	85.214.155.142 [academialopedevaga.org] (Linux)	HTTP Cookie	cb-enabled=enabled; MoodleSessionTest=DkFEZHxvWQ;...	N/A	Unknown	2017-10-19 22:36:08 UTC+02