

Se hace en VM a menos que vaya a ser versión estable.

Operación con sniffers:
Wireshark, Microsoft Network
Monitor y NetworkMiner
TCPDUMP
Capturas en Windows
NTOPNG para Linux



Alfredo Abad
PARP401-Sniffers.pptx
UA: 7-nov-2022

Objetivo de la práctica

- Conocer algunos de los escuchadores de red (sniffers) más comunes en la gestión de redes
- Determinar las condiciones necesarias para la escucha de la red
- Trabajar con ficheros de captura en formatos estándar
- Aprender a buscar información concreta dentro de los ficheros de captura
- Tomar conciencia de la necesidad de una ética profesional

Wireshark

The image shows the Wireshark network protocol analyzer interface. The main window displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Info. The packets are color-coded: blue for DNS and green for TCP. The selected packet (No. 1) is expanded, showing the Ethernet II header and the raw packet data in hexadecimal and ASCII.

Packet List:

| No. | Time | Source | Destination | Protocol | Info |
|-----|-----------|----------------|----------------|----------|-------------------------|
| 11 | 15.047027 | 208.67.222.222 | 192.168.1.101 | DNS | Standard query response |
| 12 | 15.647269 | 192.168.1.101 | 208.67.222.222 | DNS | Standard query A www. |
| 13 | 15.937059 | 208.67.222.222 | 192.168.1.101 | DNS | Standard query response |
| 14 | 15.937457 | 192.168.1.101 | 75.126.43.232 | TCP | 45861 > www [SYN] Seq |
| 15 | 16.314591 | 75.126.43.232 | 192.168.1.101 | TCP | www > 45861 [SYN, ACK |
| 16 | 16.314665 | 192.168.1.101 | 75.126.43.232 | TCP | 45861 > www [ACK] Seq |
| 17 | 16.314984 | 192.168.1.101 | 75.126.43.232 | TCP | [TCP segment of a rea |
| 18 | 16.315020 | 192.168.1.101 | 75.126.43.232 | TCP | [TCP segment of a rea |
| 19 | 16.724366 | 75.126.43.232 | 192.168.1.101 | TCP | www > 45861 [ACK] Seq |
| 20 | 16.732070 | 75.126.43.232 | 192.168.1.101 | TCP | www > 45861 [ACK] Seq |
| 21 | 18.072290 | 192.168.1.101 | 208.67.222.222 | DNS | Standard query A www. |
| 22 | 18.360176 | 208.67.222.222 | 192.168.1.101 | DNS | Standard query response |
| 23 | 18.445066 | 192.168.1.101 | 208.67.222.222 | DNS | Standard query AAAA w |
| 24 | 18.448504 | 192.168.1.101 | 208.67.222.222 | DNS | Standard query A www. |

Packet Details:

- Frame 1 (42 bytes on wire, 42 bytes captured)
- Ethernet II, Src: D-Link 0a:f6:44 (00:17:9a:0a:f6:44), Dest: Cisco-Li 6a:c6:8b (00:18:30:6a:c6:8b)

Raw Data:

| Offset | Hex | ASCII |
|--------|-------------------------------------------------|-------------------|
| 0000 | 00 18 39 6a c6 8b 00 17 9a 0a f6 44 08 06 00 01 | ..9j.... ...D.... |
| 0010 | 08 00 06 04 00 01 00 17 9a 0a f6 44 c0 a8 01 65 |D...e |
| 0020 | 00 00 00 00 00 00 c0 a8 01 01 | |

Frame (frame), 42 bytes P: 582 D: 582 M: 0 Drops: 0



<https://noticiasseguridad.com/importantes/como-interceptar-el-trafico-de-usb/>

CÓMO INTERCEPTAR EL TRÁFICO DE USB UTILIZANDO WIRESHARK

Hay una nueva versión (sucesor de Network Monitor) que se denomina Microsoft Message Analyzer, compatible con W10 (se descarga de Microsoft Connect)

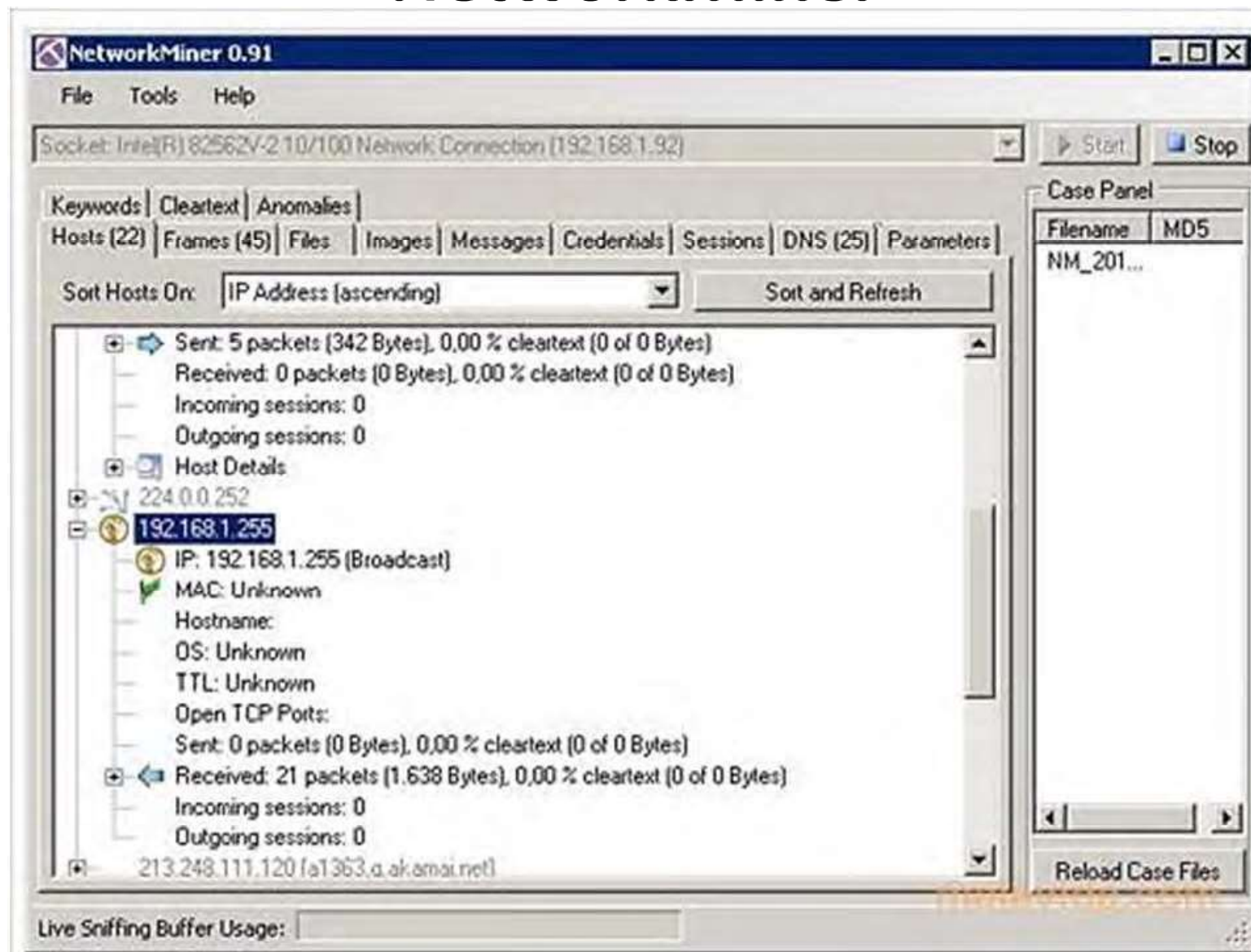
The screenshot displays the Microsoft Message Analyzer application interface. The top menu bar includes File, Home, Troubleshooting, Add Rule, Manage Columns, View Options, Windows, Save, Restore, Report Issue, and Community. The main window is titled 'Skype: Analysis Grid' and shows a 'Trace Session 1: Analysis Grid' with a table of network messages. The table columns are MessageNumber, Timestamp, TimeLapsed, Source, Destination, Module, and Summary. The messages are filtered by 'Skype' and show various protocols like TCP, UDP, and WiFi. A detailed view of a selected message (Message 173) is shown in the bottom right, displaying the packet structure and hex data. The packet details include SourcePort (51413), DestinationPort (61428), Length (38), Checksum (58388), and Payload (Binary[13,2,66,161,31,65,210,...]). The hex data shows the raw bytes of the packet, including the Ethernet II header and the IP/TCP payload.

| MessageNumber | Timestamp | TimeLapsed | Source | Destination | Module | Summary |
|---------------|-----------------------------|------------|---------------|---------------|-----------------|---------------------------------------------------------------------------|
| 153 | 10/13/2012 11:46:05.9482378 | 0,0000016 | 192.168.0.107 | 192.168.0.107 | TCP | Flags:S., Port: 45324 - 51413, Len: 0, Seq Range: 3367324516 |
| 156 | 10/13/2012 11:46:05.9483868 | 0,0000015 | 192.168.0.107 | 192.168.0.107 | UDP | 61428 - 51413, Len: 38 |
| 163 | 10/13/2012 11:46:06.0446954 | 0,0000026 | 192.168.0.107 | 192.168.0.107 | UDP | 51413 - 61428, Len: 28 |
| 165 | 10/13/2012 11:46:06.0449445 | 0,0000016 | 192.168.0.107 | 192.168.0.107 | UDP | 61428 - 51413, Len: 1430 |
| 169 | 10/13/2012 11:46:06.0478344 | 0,0000025 | 192.168.0.107 | 192.168.0.107 | WiFi | Management Beacon |
| 171 | 10/13/2012 11:46:06.0486870 | 0,0000026 | 192.168.0.107 | 192.168.0.107 | TCP | Flags: ...A...., Port: 51413 - 45297, Len: 0, Seq Range: 1428278974 |
| 173 | 10/13/2012 11:46:06.1498749 | 0,0000025 | 192.168.0.107 | 192.168.0.107 | WiFi | Management Beacon |
| 173 | 10/13/2012 11:46:06.1498749 | 0 | | | WiFiChannelInfo | RSSI = -55dBm, Rate = 1.0Mbps |
| 173 | 10/13/2012 11:46:06.1498749 | 0 | | | NetNdisProvider | MiniportIndex: 13, LowerIndex: 13 |
| 173 | 10/13/2012 11:46:06.1498749 | 0 | | | NetNdisProvider | {9de35b12-1202-467c-b047-ed308fb776c3}, EventID: 1001, ProcessID: 1001 |
| 174 | 10/13/2012 11:46:06.1498774 | 0 | | | NetNdisProvider | MiniportIndex: 13, LowerIndex: 13, FrameSize: 141 |
| 175 | 10/13/2012 11:46:06.1508585 | 0,0000026 | 192.168.0.107 | 192.168.0.107 | UDP | 51413 - 61428, Len: 38 |
| 177 | 10/13/2012 11:46:06.1511205 | 0,0000025 | 192.168.0.107 | 192.168.0.107 | UDP | 51413 - 61428, Len: 57 |
| 183 | 10/13/2012 11:46:06.1514821 | 0,0000025 | 192.168.0.107 | 192.168.0.107 | TCP | Flags: ...A..S., Port: 51413 - 45321, Len: 0, Seq Range: 1023181347 |
| 183 | 10/13/2012 11:46:06.1516377 | 0,0000021 | 192.168.0.107 | 192.168.0.107 | TCP | Flags: ...A...., Port: 45321 - 51413, Len: 0, Seq Range: 2601037722 |
| 186 | 10/13/2012 11:46:06.1533420 | 0,0000041 | 192.168.0.107 | 192.168.0.107 | UDP | 61428 - 51413, Len: 222 |
| 190 | 10/13/2012 11:46:06.1560058 | 0,0000031 | 192.168.0.107 | 192.168.0.107 | TCP | Virtual Data Segment, Port: 45321 - 51413, Len: 97, Seq Range: 2601037722 |

| Name | Value | Type | Bit Offset | Bit Length |
|-----------------|-----------------------------------|--------|------------|------------|
| SourcePort | 51413 | UInt16 | 0 | 16 |
| DestinationPort | 61428 | UInt16 | 16 | 16 |
| Length | 38 | UInt16 | 32 | 16 |
| Checksum | 58388 | UInt16 | 48 | 16 |
| Payload | Binary[13,2,66,161,31,65,210,...] | Binary | 64 | 240 |

Hex Data: 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000010 00 00 00 00 71 09 00 00 C5 FF FF FF 40 00 00 00
000020 00 00 00 00 00
Total Bytes: 102 Fragment Start Offset: 64, Fragment Length: 38
000000 00 00 00 00 00 00 00 00 5A 00 00 00 08 42 2C 00
000010 00 24 07 C6 4C 38 00 02 6F 6D 9C 3A 00 AE EC ED
000020 42 E8 C0 C4 AA 03 00 00 00 00 00 00 00 45 00 3A
000030 0E F8 00 00 32 11 08 93 4F 86 AF 56 C0 A5 01 78
000040 E 0 1 0 . 8 . . ! B | A 0 f
Byte Count: 38 Message Offset: 64 Protocol Offset: 0

NetworkMiner





- Total Network Monitor: <https://www.softinventive.com/total-network-monitor/>
- OpenNMS: <https://www.opennms.com/>
- PRTG Network Monitor: <https://www.paessler.com/prtg>
- Free Network Analyzer:
https://www.colasoft.com/download/products/capsa_free.php

OTRAS HERRAMIENTAS Y MONITORES ALTERNATIVOS

<https://windowserver.wordpress.com/2014/08/05/windows-server-2012-r2-resolucin-de-nombres-de-mquina-incluye-capturas-de-red-explicadas/>

EJEMPLO:
RESOLUCIÓN DE NOMBRES DE
SISTEMAS EN WINDOWS VISTOS DESDE
WIRESHARK

Escenario

- La infraestructura que se utilizará para esta demostración es sencilla:
 - DC1.ad.guillermomod.com.ar
Windows Server 2012 R2
Controlador de Dominio
Servicio DNS
Servicio WINS (para resolución NetBIOS)
IPv4: 192.168.2.201/24
IPv6: por omisión (Link-local)
 - CL1.ad.guillermomod.com.ar
Windows 8.1
Cliente del Dominio
Configurado DNS a DC1
Configurado WINS a DC1
IPv4: 192.168.2.1/24
IPv6: por omisión (Link-local)

Pruebas de red

- En CL1 se ha instalado el analizador de protocolo [Microsoft Network Monitor 3.4](#) que es de descarga gratuita para hacer las capturas de red
- Para forzar a que el sistema utilice todos los métodos de resolución posibles, ejecutaré un comando que acepta tanto nombre NetBIOS, como “Hostname” o FQDN, como es “PING” usando un nombre no-especificando de qué tipo es
 - Por tanto ,el comando será “**PING NoExiste**” y veremos qué formas de resolución utiliza sobre la red
- Como la parte que hace en memoria no podremos verla en la red, vamos a aclararla:
 - Cuando tiene que resolver un nombre de tipo “Hostname/FQDN” siempre lo primero que se revisa es si la información no está ya presente en memoria
 - Puede estar en memoria porque fue resuelta anteriormente y aún resta tiempo para tenerla “cacheada”, o porque está incluida en el archivo HOSTS ya que la implementación de Microsoft es mantener en este “cache” el contenido del archivo
 - Si de esta forma no consigue resolver el nombre, procederá como se muestra en las siguientes capturas
 - Cuando tiene que resolver un nombre de tipo NetBIOS, también lo primero que hace es ver si la información no está “cacheada” en memoria
 - Puede estar en memoria por haber sido resuelta anteriormente, este tiempo es fijo de 10 minutos

Primera prueba

- Como tiene que contactar a DC1 que es servidor tanto de DNS como de WINS, lo primero que debe hacer el cliente es resolver la “MAC Address” de DC1, que hace a través del protocolo ARP
- Podemos observar en el “frame 3” que es un “Broadcast” a nivel Ethernet preguntando por la “MAC Address” de 192.168.2.201, y adjuntando su propia “MAC Address” para que la guarde DC1

Como DC1 ya conoce la “MAC Address” de CL1, le responde por ARP, pero esta vez con tráfico dirigido a nivel Ethernet en el “frame 4”

Microsoft Network Monitor 3.4 - C:\Users\administrator\Documents\Network Monitor 3\Captures\1-NoExiste-Hostname-Ping.cap

File Edit View Frames Filter Experts Tools Help

New Capture Open Capture Save As Reassemble

1-NoExiste-Hostname-Ping.cap Capture1 Start Page Parsers

Display Filter

Apply Remove History Load Filter Save Filter Clear Text

Frame Summary

Find Color Rules Aliases Columns

| Frame Number | Time Date Local Adjusted | Time Offset | Process Name | Source | Destination | Protocol Name | Description |
|--------------|--------------------------|-------------|--------------|--------------------------------|--------------------|---------------|-------------------------------------------------------------------------------------------------|
| 1 | 2:37:42 PM 7/2/2014 | 4.3194827 | | | | NetmonFilter | NetmonFilter:Updated Capture Filter: None |
| 2 | 2:37:42 PM 7/2/2014 | 4.3194827 | | | | NetworkInfoEx | NetworkInfoEx:Network info for , Network Adapter Count = 1 |
| 3 | 2:37:42 PM 7/2/2014 | 4.3194827 | | 192.168.2.1 | 192.168.2.201 | ARP | ARP:Request, 192.168.2.1 asks for 192.168.2.201 |
| 4 | 2:37:42 PM 7/2/2014 | 4.3208491 | | 192.168.2.201 | 192.168.2.1 | ARP | ARP:Response, 192.168.2.201 at 00-0C-29-C0-AF-22 |
| 5 | 2:37:42 PM 7/2/2014 | 4.3208599 | | 192.168.2.1 | 192.168.2.201 | DNS | DNS:QueryId = 0x73D2, QUERY (Standard query), Query for NoExiste.ad.guillermob.com.ar of type 1 |
| 6 | 2:37:42 PM 7/2/2014 | 4.3211617 | | 192.168.2.201 | 192.168.2.1 | DNS | DNS:QueryId = 0x73D2, QUERY (Standard query), Response - Name Error |
| 7 | 2:37:42 PM 7/2/2014 | 4.3212915 | System | 192.168.2.1 | 192.168.2.201 | NbtNs | NbtNs:Query Request for NOEXISTE <0x00> Workstation Service |
| 8 | 2:37:42 PM 7/2/2014 | 4.3214319 | | FE80:0:0:0:F417:2A8E:C3D3:37AD | FF02:0:0:0:0:0:1:3 | LLMNR | LLMNR:QueryId = 0x6A36, Standard, Query for NoExiste of type Host Addr on class Internet |
| 9 | 2:37:42 PM 7/2/2014 | 4.3215099 | System | 192.168.2.201 | 192.168.2.1 | NbtNs | NbtNs:Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service |
| 10 | 2:37:42 PM 7/2/2014 | 4.3215704 | | 192.168.2.1 | 224.0.0.252 | LLMNR | LLMNR:QueryId = 0x6A36, Standard, Query for NoExiste of type Host Addr on class Internet |
| 11 | 2:37:42 PM 7/2/2014 | 4.3217457 | | FE80:0:0:0:F417:2A8E:C3D3:37AD | FF02:0:0:0:0:0:1:3 | LLMNR | LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type AAAA on class Internet |
| 12 | 2:37:42 PM 7/2/2014 | 4.3218321 | | 192.168.2.1 | 224.0.0.252 | LLMNR | LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type AAAA on class Internet |
| 13 | 2:37:42 PM 7/2/2014 | 4.3432576 | System | 192.168.2.1 | 192.168.2.255 | NbtNs | NbtNs:Query Request for NOEXISTE <0x00> Workstation Service |
| 14 | 2:37:43 PM 7/2/2014 | 4.7348111 | | FE80:0:0:0:F417:2A8E:C3D3:37AD | FF02:0:0:0:0:0:1:3 | LLMNR | LLMNR:QueryId = 0x6A36, Standard, Query for NoExiste of type Host Addr on class Internet |
| 15 | 2:37:43 PM 7/2/2014 | 4.7355721 | | 192.168.2.1 | 224.0.0.252 | LLMNR | LLMNR:QueryId = 0x6A36, Standard, Query for NoExiste of type Host Addr on class Internet |
| 16 | 2:37:43 PM 7/2/2014 | 4.7356763 | | FE80:0:0:0:F417:2A8E:C3D3:37AD | FF02:0:0:0:0:0:1:3 | LLMNR | LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type AAAA on class Internet |
| 17 | 2:37:43 PM 7/2/2014 | 4.7357501 | | 192.168.2.1 | 224.0.0.252 | LLMNR | LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type AAAA on class Internet |
| 18 | 2:37:43 PM 7/2/2014 | 5.0937984 | System | 192.168.2.1 | 192.168.2.255 | NbtNs | NbtNs:Query Request for NOEXISTE <0x00> Workstation Service |

Frame Details

Frame: Number = 4, Captured Frame Length = 60, MediaType = ETHERNET

Ethernet: Etype = ARP, DestinationAddress: [00-0C-29-E9-AE-7A], SourceAddress: [00-0C-29-C0-AF-22]

- DestinationAddress: VMware, Inc. E9AE7A [00-0C-29-E9-AE-7A]
- SourceAddress: VMware, Inc. C0AF22 [00-0C-29-C0-AF-22]
- EthernetType: ARP, 2054(0x806)
- UnknownData: Binary Large Object (18 Bytes)
- Arp: Response, 192.168.2.201 at 00-0C-29-C0-AF-22

Hex Details

Decode As Width

| | | |
|------|-------|--|
| 0000 | 00 0C | |
| 0002 | 29 E9 | |
| 0004 | AE 7A | |
| 0006 | 00 0C | |
| 0008 | 29 C0 | |
| 000A | AF 22 | |
| 000C | 00 00 | |

Frame Comments

Version 3.4.2350.0

Displayed: 19 Captured: 19 Focused: 4 Selected: 1

ENG 5:41 PM
LAA 7/18/2014

Y en el “frame 6” el servidor DNS le responde que ese nombre no existe (“Name error”)

Microsoft Network Monitor 3.4 - C:\Users\administrator\Documents\Network Monitor 3\Captures\1-NoExiste-Hostname-Ping.cap

File Edit View Frames Filter Experts Tools Help

New Capture Open Capture Save As Reassemble Layout Parser Profiles Options How Do I

1-NoExiste-Hostname-Ping.cap Capture1 Start Page Parsers

Display Filter

Apply Remove History Load Filter Save Filter Clear Text

Frame Summary

Find Color Rules Aliases Columns

| Frame Number | Time Date Local Adjusted | Time Offset | Process Name | Source | Destination | Protocol Name | Description |
|--------------|--------------------------|-------------|--------------|--------------------------------|------------------|---------------|-------------------------------------------------------------------------------------------------|
| 1 | 2:37:42 PM 7/2/2014 | 4.3194827 | | | | NetmonFilter | NetmonFilter:Updated Capture Filter: None |
| 2 | 2:37:42 PM 7/2/2014 | 4.3194827 | | | | NetworkInfoEx | NetworkInfoEx:Network info for , Network Adapter Count = 1 |
| 3 | 2:37:42 PM 7/2/2014 | 4.3194827 | | 192.168.2.1 | 192.168.2.201 | ARP | ARP:Request, 192.168.2.1 asks for 192.168.2.201 |
| 4 | 2:37:42 PM 7/2/2014 | 4.3208491 | | 192.168.2.1 | 192.168.2.1 | ARP | ARP:Response, 192.168.2.201 at 00-0C-29-C0-AF-22 |
| 5 | 2:37:42 PM 7/2/2014 | 4.3208599 | | 192.168.2.1 | 192.168.2.201 | DNS | DNS:QueryId = 0x73D2, QUERY (Standard query), Query for NoExiste.ad.guillermob.com.ar of type 1 |
| 6 | 2:37:42 PM 7/2/2014 | 4.3211617 | | 192.168.2.201 | 192.168.2.1 | DNS | DNS:QueryId = 0x73D2, QUERY (Standard query), Response - Name Error |
| 7 | 2:37:42 PM 7/2/2014 | 4.3212915 | System | 192.168.2.1 | 192.168.2.201 | NbtNs | NbtNs:Query Request for NOEXISTE <0x00> Workstation Service |
| 8 | 2:37:42 PM 7/2/2014 | 4.3214319 | | FE80:0:0:0:F417:2A8E:C3D3:37AD | FF02:0:0:0:0:1:3 | LLMNR | LLMNR:QueryId = 0x6A36, Standard, Query for NoExiste of type Host Addr on class Internet |
| 9 | 2:37:42 PM 7/2/2014 | 4.3215099 | System | 192.168.2.201 | 192.168.2.1 | NbtNs | NbtNs:Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service |
| 10 | 2:37:42 PM 7/2/2014 | 4.3215704 | | 192.168.2.1 | 224.0.0.252 | LLMNR | LLMNR:QueryId = 0x6A36, Standard, Query for NoExiste of type Host Addr on class Internet |
| 11 | 2:37:42 PM 7/2/2014 | 4.3217457 | | FE80:0:0:0:F417:2A8E:C3D3:37AD | FF02:0:0:0:0:1:3 | LLMNR | LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type AAAA on class Internet |
| 12 | 2:37:42 PM 7/2/2014 | 4.3218321 | | 192.168.2.1 | 224.0.0.252 | LLMNR | LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type AAAA on class Internet |
| 13 | 2:37:42 PM 7/2/2014 | 4.3432576 | System | 192.168.2.1 | 192.168.2.255 | NbtNs | NbtNs:Query Request for NOEXISTE <0x00> Workstation Service |
| 14 | 2:37:43 PM 7/2/2014 | 4.7348111 | | FE80:0:0:0:F417:2A8E:C3D3:37AD | FF02:0:0:0:0:1:3 | LLMNR | LLMNR:QueryId = 0x6A36, Standard, Query for NoExiste of type Host Addr on class Internet |
| 15 | 2:37:43 PM 7/2/2014 | 4.7355721 | | 192.168.2.1 | 224.0.0.252 | LLMNR | LLMNR:QueryId = 0x6A36, Standard, Query for NoExiste of type Host Addr on class Internet |
| 16 | 2:37:43 PM 7/2/2014 | 4.7356763 | | FE80:0:0:0:F417:2A8E:C3D3:37AD | FF02:0:0:0:0:1:3 | LLMNR | LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type AAAA on class Internet |
| 17 | 2:37:43 PM 7/2/2014 | 4.7357501 | | 192.168.2.1 | 224.0.0.252 | LLMNR | LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type AAAA on class Internet |
| 18 | 2:37:43 PM 7/2/2014 | 5.0037094 | System | 192.168.2.1 | 192.168.2.255 | NbtNs | NbtNs:Query Request for NOEXISTE <0x00> Workstation Service |

Frame Details

Frame: Number = 6, Captured Frame Length = 160, MediaType = ETHERNET

Ethernet: Etype = Internet IP (IPv4), DestinationAddress: [00-0C-29-E9-AE-7A], SourceAddress: [00-0C-29-C0-AF-22]

DestinationAddress: VMware, Inc. E9AE7A [00-0C-29-E9-AE-7A]

SourceAddress: VMware, Inc. C0AF22 [00-0C-29-C0-AF-22]

EthernetType: Internet IP (IPv4), 2048(0x800)

IPv4: Src = 192.168.2.201, Dest = 192.168.2.1, Next Protocol = UDP, Packet ID = 16619, Total IP Length = 136

Udp: SrcPort = DNS(53), DstPort = 58844, Length = 126

Dns: QueryId = 0x73D2, QUERY (Standard query), Response - Name Error

Hex Details

Decode As Width

0000 00 0C 29 E9 AE 7A 00 0C 29 C0 AF 22

0002 29 E9 AE 7A 00 0C 29 C0 AF 22

0004 AE 7A 00 0C 29 C0 AF 22

0006 00 0C 29 C0 AF 22

0008 29 C0 AF 22

000A AE 7A 00 0C 29 C0 AF 22

000C 00 0C 29 E9 AE 7A 00 0C 29 C0 AF 22

Frame Comments

Version 3.4.2350.0

Displayed: 9 Captured: 19 Focused: 6 Selected: 1

ENG 5:46 PM 7/18/2014

WINS le responderá que no tiene registrado a nadie con ese nombre. Pero antes que WINS responda, va a intentar resolver por LLMNR. De todas formas podemos verificar en el “frame 9” la no resolución

Microsoft Network Monitor 3.4 - C:\Users\administrator\Documents\Network Monitor 3\Captures\1-NoExiste-Hostname-Ping.cap

File Edit View Frames Filter Experts Tools Help

New Capture Open Capture Save As Reassemble Layout Parser Profiles Options How Do I

1-NoExiste-Hostname-Ping.cap Capture1 Start Page Parsers

Display Filter

Apply Remove History Load Filter Save Filter Clear Text

Frame Summary

Find Color Rules Aliases Columns

| Frame Number | Time Date Local Adjusted | Time Offset | Process Name | Source | Destination | Protocol Name | Description |
|--------------|--------------------------|-------------|--------------|--------------------------------|----------------------|---------------|-------------------------------------------------------------------------------------------------|
| 1 | 2:37:42 PM 7/2/2014 | 4.3194827 | | | | NetmonFilter | NetmonFilter:Updated Capture Filter: None |
| 2 | 2:37:42 PM 7/2/2014 | 4.3194827 | | | | NetworkInfoEx | NetworkInfoEx:Network info for , Network Adapter Count = 1 |
| 3 | 2:37:42 PM 7/2/2014 | 4.3194827 | | 192.168.2.1 | 192.168.2.201 | ARP | ARP:Request, 192.168.2.1 asks for 192.168.2.201 |
| 4 | 2:37:42 PM 7/2/2014 | 4.3208491 | | 192.168.2.201 | 192.168.2.1 | ARP | ARP:Response, 192.168.2.201 at 00-0C-29-C0-AF-22 |
| 5 | 2:37:42 PM 7/2/2014 | 4.3208599 | | 192.168.2.1 | 192.168.2.201 | DNS | DNS:QueryId = 0x73D2, QUERY (Standard query), Query for NoExiste.ad.guillermob.com.ar of type h |
| 6 | 2:37:42 PM 7/2/2014 | 4.3211617 | | 192.168.2.201 | 192.168.2.1 | DNS | DNS:QueryId = 0x73D2, QUERY (Standard query), Response - Name Error |
| 7 | 2:37:42 PM 7/2/2014 | 4.3212915 | System | 192.168.2.1 | 192.168.2.201 | NbtNs | NbtNs:Query Request for NOEXISTE <0x00> Workstation Service |
| 8 | 2:37:42 PM 7/2/2014 | 4.3214319 | | FE80:0:0:0:F417:2A8E:C3D3:37AD | FF02:0:0:0:0:0:0:1:3 | LLMNR | LLMNR:QueryId = 0x6A36, Standard, Query for NoExiste of type Host Addr on class Internet |
| 9 | 2:37:42 PM 7/2/2014 | 4.3215099 | System | 192.168.2.201 | 192.168.2.1 | NbtNs | NbtNs:Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service |
| 10 | 2:37:42 PM 7/2/2014 | 4.3215704 | | 192.168.2.1 | 224.0.0.252 | LLMNR | LLMNR:QueryId = 0x6A36, Standard, Query for NoExiste of type Host Addr on class Internet |
| 11 | 2:37:42 PM 7/2/2014 | 4.3217457 | | FE80:0:0:0:F417:2A8E:C3D3:37AD | FF02:0:0:0:0:0:0:1:3 | LLMNR | LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type AAAA on class Internet |
| 12 | 2:37:42 PM 7/2/2014 | 4.3218321 | | 192.168.2.1 | 224.0.0.252 | LLMNR | LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type AAAA on class Internet |
| 13 | 2:37:42 PM 7/2/2014 | 4.3432576 | System | 192.168.2.1 | 192.168.2.255 | NbtNs | NbtNs:Query Request for NOEXISTE <0x00> Workstation Service |
| 14 | 2:37:43 PM 7/2/2014 | 4.7348111 | | FE80:0:0:0:F417:2A8E:C3D3:37AD | FF02:0:0:0:0:0:0:1:3 | LLMNR | LLMNR:QueryId = 0x6A36, Standard, Query for NoExiste of type Host Addr on class Internet |
| 15 | 2:37:43 PM 7/2/2014 | 4.7355721 | | 192.168.2.1 | 224.0.0.252 | LLMNR | LLMNR:QueryId = 0x6A36, Standard, Query for NoExiste of type Host Addr on class Internet |
| 16 | 2:37:43 PM 7/2/2014 | 4.7356763 | | FE80:0:0:0:F417:2A8E:C3D3:37AD | FF02:0:0:0:0:0:0:1:3 | LLMNR | LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type AAAA on class Internet |
| 17 | 2:37:43 PM 7/2/2014 | 4.7357501 | | 192.168.2.1 | 224.0.0.252 | LLMNR | LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type AAAA on class Internet |
| 18 | 2:37:43 PM 7/2/2014 | 5.0037084 | System | 192.168.2.1 | 192.168.2.255 | NbtNs | NbtNs:Query Request for NOEXISTE <0x00> Workstation Service |

Frame Details

Frame: Number = 9, Captured Frame Length = 98, MediaType = ETHERNET

Ethernet: Etype = Internet IP (IPv4), DestinationAddress: [00-0C-29-E9-AE-7A], SourceAddress: [00-0C-29-C0-AF-22]

IPv4: Src = 192.168.2.201, Dest = 192.168.2.1, Next Protocol = UDP, Packet ID = 16620, Total IP Length = 84

Udp: SrcPort = NETBIOS Name Service(137), DstPort = NETBIOS Name Service(137), Length = 64

NbtNs: Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service

Hex Details

Decode As Width

0000 00 0C ...

0002 29 E9 ...

0004 AE 7A ...

0006 00 0C ...

0008 29 C0 ...

000A AE 22 ...

000C 00 00 ...

Frame Comments

Version 3.4.2350.0

Displayed: 19 Captured: 19 Focused: 9 Selected: 1

ENG 5:48 PM 7/18/2014

Y simultáneamente hace el mismo intento por IPv4 como se observa en los “frames 10, 12, 15 y 17”

Microsoft Network Monitor 3.4 - C:\Users\administrator\Documents\Network Monitor 3\Captures\1-NoExiste-Hostname-Ping.cap

File Edit View Frames Filter Experts Tools Help

New Capture Open Capture Save As Reassemble

1-NoExiste-Hostname-Ping.cap Capture 1 Start Page Parsers

Display Filter

Apply Remove History Load Filter Save Filter Clear Text

Frame Summary

Find Color Rules Aliases Columns

| Frame Number | Time Date Local Adjusted | Time Offset | Process Name | Source | Destination | Protocol Name | Description |
|--------------|--------------------------|-------------|--------------|--------------------------------|--------------------|---------------|----------------------------------------------------------------------------------------------------|
| 1 | 2:37:42 PM 7/2/2014 | 4.3194827 | | | | NetmonFilter | NetmonFilter:Updated Capture Filter: None |
| 2 | 2:37:42 PM 7/2/2014 | 4.3194827 | | | | NetworkInfoEx | NetworkInfoEx:Network info for , Network Adapter Count = 1 |
| 3 | 2:37:42 PM 7/2/2014 | 4.3194827 | | 192.168.2.1 | 192.168.2.201 | ARP | ARP:Request, 192.168.2.1 asks for 192.168.2.201 |
| 4 | 2:37:42 PM 7/2/2014 | 4.3208491 | | 192.168.2.201 | 192.168.2.1 | ARP | ARP:Response, 192.168.2.201 at 00-0C-29-C0-AF-22 |
| 5 | 2:37:42 PM 7/2/2014 | 4.3208599 | | 192.168.2.1 | 192.168.2.201 | DNS | DNS:QueryId = 0x73D2, QUERY (Standard query), Query for NoExiste.ad.guillermob.com.ar of type Host |
| 6 | 2:37:42 PM 7/2/2014 | 4.3211617 | | 192.168.2.201 | 192.168.2.1 | DNS | DNS:QueryId = 0x73D2, QUERY (Standard query), Response - Name Error |
| 7 | 2:37:42 PM 7/2/2014 | 4.3212915 | System | 192.168.2.1 | 192.168.2.201 | NbtNs | NbtNs:Query Request for NOEXISTE <0x00> Workstation Service |
| 8 | 2:37:42 PM 7/2/2014 | 4.3214319 | | FE80:0:0:0:F417:2A8E:C3D3:37AD | FF02:0:0:0:0:0:1:3 | LLMNR | LLMNR:QueryId = 0x6A36, Standard, Query for NoExiste of type Host Addr on class Internet |
| 9 | 2:37:42 PM 7/2/2014 | 4.3215099 | System | 192.168.2.201 | 192.168.2.1 | NbtNs | NbtNs:Query Response, Requested name doesn't exist for NOEXISTE <0x00> Workstation Service |
| 10 | 2:37:42 PM 7/2/2014 | 4.3215704 | | 192.168.2.1 | 224.0.0.252 | LLMNR | LLMNR:QueryId = 0x6A36, Standard, Query for NoExiste of type Host Addr on class Internet |
| 11 | 2:37:42 PM 7/2/2014 | 4.3217457 | | FE80:0:0:0:F417:2A8E:C3D3:37AD | FF02:0:0:0:0:0:1:3 | LLMNR | LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type AAAA on class Internet |
| 12 | 2:37:42 PM 7/2/2014 | 4.3218321 | | 192.168.2.1 | 224.0.0.252 | LLMNR | LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type AAAA on class Internet |
| 13 | 2:37:42 PM 7/2/2014 | 4.3432576 | System | 192.168.2.1 | 192.168.2.255 | NbtNs | NbtNs:Query Request for NOEXISTE <0x00> Workstation Service |
| 14 | 2:37:43 PM 7/2/2014 | 4.7348111 | | FE80:0:0:0:F417:2A8E:C3D3:37AD | FF02:0:0:0:0:0:1:3 | LLMNR | LLMNR:QueryId = 0x6A36, Standard, Query for NoExiste of type Host Addr on class Internet |
| 15 | 2:37:43 PM 7/2/2014 | 4.7355721 | | 192.168.2.1 | 224.0.0.252 | LLMNR | LLMNR:QueryId = 0x6A36, Standard, Query for NoExiste of type Host Addr on class Internet |
| 16 | 2:37:43 PM 7/2/2014 | 4.7356763 | | FE80:0:0:0:F417:2A8E:C3D3:37AD | FF02:0:0:0:0:0:1:3 | LLMNR | LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type AAAA on class Internet |
| 17 | 2:37:43 PM 7/2/2014 | 4.7357501 | | 192.168.2.1 | 224.0.0.252 | LLMNR | LLMNR:QueryId = 0x7E37, Standard, Query for NoExiste of type AAAA on class Internet |
| 18 | 2:37:43 PM 7/2/2014 | 5.0937984 | System | 192.168.2.1 | 192.168.2.255 | NbtNs | NbtNs:Query Request for NOEXISTE <0x00> Workstation Service |
| 19 | 2:37:44 PM 7/2/2014 | 5.8445615 | System | 192.168.2.1 | 192.168.2.255 | NbtNs | NbtNs:Query Request for NOEXISTE <0x00> Workstation Service |

Frame Details

Frame: Number = 10, Captured Frame Length = 68, MediaType = ETHERNET

Ethernet: Etype = Internet IP (IPv4), DestinationAddress: [01-00-5E-00-00-FC], SourceAddress: [00-0C-29-E9-AE-7A]

IPv4: Src = 192.168.2.1, Dest = 224.0.0.252, Next Protocol = UDP, Packet ID = 5124, Total IP Length = 54

Udp: SrcPort = 58071, DstPort = Linklocal Multicast Name Resolution(5355), Length = 34

LLMnr: QueryId = 0x6A36, Standard, Query for NoExiste of type Host Addr on class Internet

Hex Details

Decode As Width

| | |
|------|-------|
| 0000 | 01 00 |
| 0002 | 5E 00 |
| 0004 | 00 FC |
| 0006 | 00 0C |
| 0008 | 29 E9 |

Frame Comments

Version 3.4.2350.0

Displayed: 19 Captured: 19 Focused: 10 Selected: 1

ENG 6:04 PM
LAA 7/18/2014

Conclusión del ejemplo

- Resumiendo, al indicarle un nombre no calificado, siendo parte de un Dominio y teniendo configurado tanto DNS como WINS, el sistema utiliza varios métodos, tanto de resolución NetBIOS como de Hostname/FQDN
- La resolución de nombres de red es algo que hay que prestarle mucha atención
 - Es habitual que cuando se experimenta un largo tiempo hasta poder conectarse a una máquina, pero luego todo funciona normalmente, se deba a un problema de resolución de nombres
 - Por ejemplo si no lo puede resolver por DNS y termine resolviendo por “Net Broadcasts”
- Información adicional:
 - [Link-local Multicast Name Resolution \(LLMNR\)](#)
 - [Multicast Address](#)

Descripción de las utilidades

- Se trata de tres utilidades que se utilizan como escuchadores de red
 - **TCPDUMP**: entorno GNU/Linux
 - **Windump**: semejante a TCPDUMP para entorno Windows
 - **FING**: Ofrece información muy ordenada y se suele utilizar con redes WiFi

Ejemplos de utilización (II)


- Capturar paquetes con origen y destino en una IP
tcpdump -i eth0 host 192.168.1.12
- Capturar paquetes con destino en una MAC
tcpdump ether dst XX:XX:XX:XX:XX:XX
- Capturar paquetes que vengan desde una red
tcpdump dst net 192.168.1.0

Ejemplos de utilización (IV)

- Capturar peticiones DNS
tcpdump udp and dst port 53
- Capturar peticiones LDAP
tcpdump tcp port ldap

Captura desde eth0

```
aabad@pruebas: ~  
aabad@pruebas:~$ sudo tcpdump -i eth0  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
```



```
aabad@pruebas: ~  
ags [FP.], seq 8579, ack 465, win 64239, length 0  
17:04:41.303883 IP pruebas.local.48875 > 168.219.106.212.static.jazztel.es.www: Fl  
ags [.], ack 8580, win 35040, length 0  
17:04:41.306950 IP mad01s08-in-f2.1e100.net.https > pruebas.local.42015: Flags [FP  
.], seq 1, ack 28, win 64239, length 0  
17:04:41.306966 IP pruebas.local.42015 > mad01s08-in-f2.1e100.net.https: Flags [.]  
, ack 2, win 26280, length 0  
17:04:41.327627 IP we-in-f138.1e100.net.www > pruebas.local.34890: Flags [FP.], se  
q 89835, ack 622, win 64239, length 0  
17:04:41.327647 IP pruebas.local.34890 > we-in-f138.1e100.net.www: Flags [.], ack  
89836, win 62780, length 0  
17:04:41.341762 IP privet.canonical.com.www > pruebas.local.52606: Flags [FP.], se  
q 1, ack 1, win 64239, length 0
```

Captura desde una MAC

```
aabad@pruebas: ~  
aabad@pruebas:~$ sudo tcpdump ether dst 00:0c:29:c2:d2:cc  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes  
17:13:03.351949 IP 192.168.111.2.domain > pruebas.local.44537: 49765 2/0/0 CNAME w  
ww-cctld.l.google.com., A 173.194.34.216 (83)  
17:13:03.437061 IP 192.168.111.2.domain > pruebas.local.38275: 55973 NXDomain 0/0/  
0 (46)  
17:13:03.437062 IP mad01s08-in-f24.1e100.net > pruebas.local: ICMP echo reply, id  
29102, seq 1, length 64  
17:13:03.479951 IP 192.168.111.2.domain > pruebas.local.40641: 18721 1/0/0 PTR mad  
01s08-in-f24.1e100.net. (84)  
17:13:03.598298 IP 192.168.111.2.domain > pruebas.local.45522: 32254 NXDomain 0/0/  
0 (44)  
17:13:04.401055 IP mad01s08-in-f24.1e100.net > pruebas.local: ICMP echo reply, id  
29102, seq 2, length 64  
17:13:04.455365 IP 192.168.111.2.domain > pruebas.local.52528: 5171 1/0/0 PTR mad0  
1s08-in-f24.1e100.net. (84)  
17:13:05.473917 IP mad01s08-in-f24.1e100.net > pruebas.local: ICMP echo reply, id  
29102, seq 3, length 64  
17:13:05.557002 IP 192.168.111.2.domain > pruebas.local.55555: 12345 1/0/0 PTR  
www-cctld.l.google.com. (84)  
17:13:08.644497 IP 192.168.111.2.domain > pruebas.local.55555: 12345 1/0/0 PTR  
www-cctld.l.google.com. (84)  
aabad@pruebas:~$ ping www.google.es  
PING www-cctld.l.google.com (173.194.34.216) 56(84) bytes of data.  
64 bytes from mad01s08-in-f24.1e100.net (173.194.34.216): icmp_req=1 ttl=128 tim  
e=83.9 ms  
64 bytes from mad01s08-in-f24.1e100.net (173.194.34.216): icmp_req=2 ttl=128 tim  
e=46.1 ms  
64 bytes from mad01s08-in-f24.1e100.net (173.194.34.216): icmp_req=3 ttl=128 tim  
e=117 ms  
^C  
--- www-cctld.l.google.com ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2003ms  
rtt min/avg/max/mdev = 46.195/82.455/117.189/29.003 ms  
aabad@pruebas:~$
```

Operación

- Sobre un sistema Linux, practica escuchas con TCPDUMP
- Intenta hacer algo semejante con Windump y con Fing
- Construye con cada utilidad un sencillo manual de usuario sobre cómo usar cada una de las utilidades
- Nomenclatura identificativa de práctica:
 - **PARP401B-Sniffers-tcpdump**

Objetivo de la práctica

- Conocer algunas herramientas de Windows que permiten la escucha de la red
- Aprender a salvar capturas en formatos legibles por las aplicaciones de análisis

Operación con netsh trace

Administrador: C:\Windows\system32\cmd.exe

C:\>md SYSADMIT

1

C:\>netsh trace start persistent=yes capture=yes tracefile=C:\SYSADMIT\Trazas-Red.etl

Configuración de seguimiento:

2

Estado: En ejecución
Archivo de seguimiento: C:\SYSADMIT\Trazas-Red.etl
Anexar: Desactivar
Circular: Activar
Tamaño máx.: 250 MB
Informe: Desactivar

C:\>netsh trace stop

3

Seguimientos correlativos... listo
Generando recolección de datos... listo
El archivo de seguimiento y otros datos de solución de problemas se compilaron como "C:\SYSADMIT\Trazas-Red.cab".
Ubicación del archivo = C:\SYSADMIT\Trazas-Red.etl
La sesión de seguimiento se detuvo correctamente.

C:\>dir C:\SYSADMIT /B

4

Trazas-Red.cab
Trazas-Red.etl

Contenido del fichero .cab

- Si descomprimos el fichero CAB, veremos toda una serie de ficheros correspondientes a los reports generados
- Entre los formatos de los ficheros de los reports veremos: TXT, XML, EVTX (Visor de eventos), entre otros
- También encontraremos el fichero: report.html con enlaces a los reports generados, muy útil para disponer de un índice de los mismos
 - Ver fichero report.html en diapo siguiente

Contenido del fichero ETL

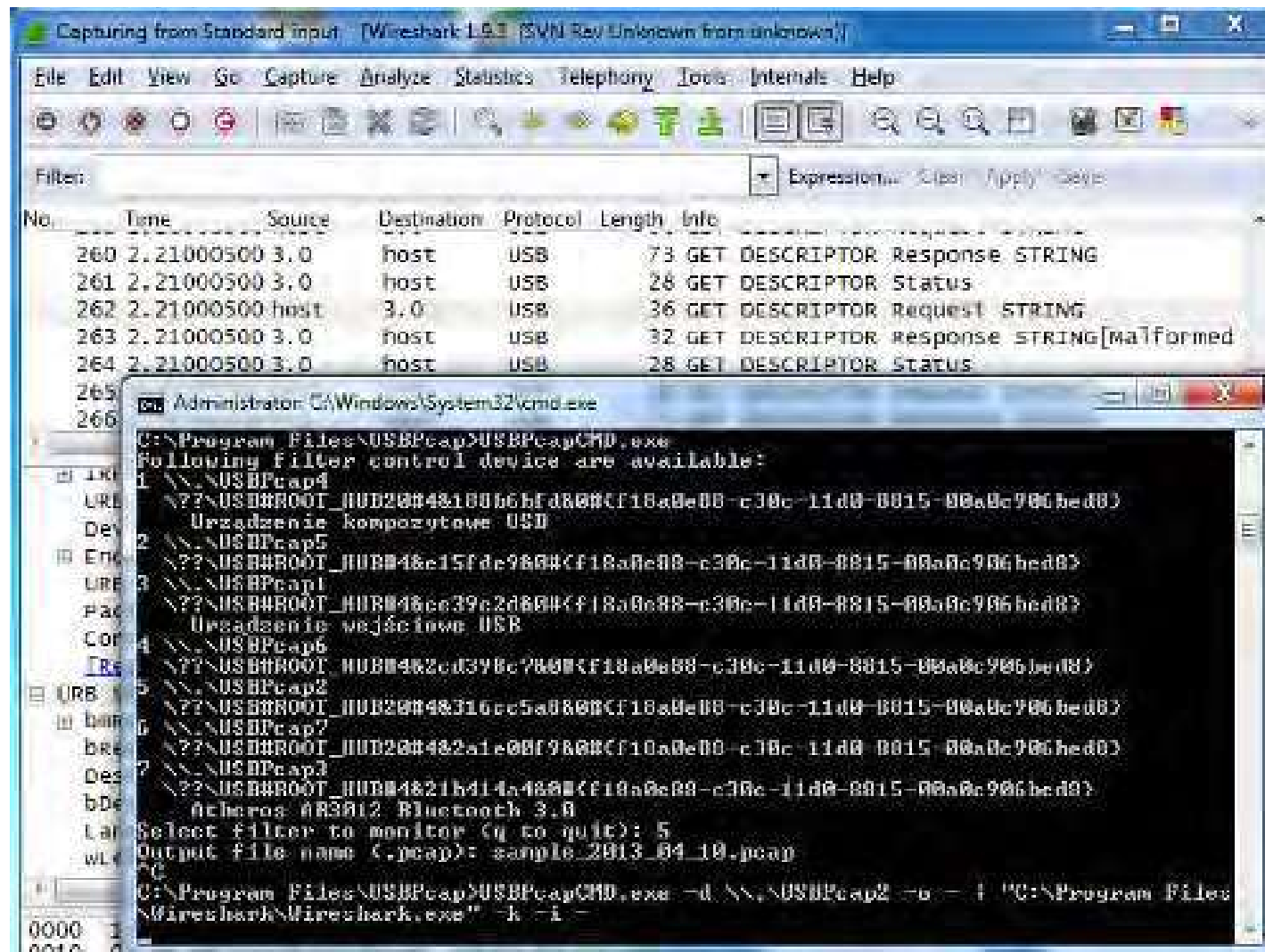
- El fichero ETL generado puede ser analizado con "Microsoft Message Analyzer", herramienta gratuita que podemos descargar de la web de Microsoft
- Con "Microsoft Message Analyzer" podremos analizar el tráfico capturado, filtrarlo, etc...
- Con "Microsoft Message Analyzer" también podemos exportar el fichero ETL a formato CAP. Con formato CAP podremos leer el fichero desde Wireshark
- Vista ejecución de "Microsoft Message Analyzer" (ver diapo siguiente)

Algunos parámetros de netsh trace

- **persistent:**
 - Los valores posibles son yes o no, el valor por defecto es no
 - Si configuramos el valor persistent a yes, conseguiremos que la captura siga aunque reiniciemos el equipo
 - Solo se detendrá la captura cuando ejecutemos: netsh trace stop
- **maxSize:**
 - Valor en MB correspondiente al fichero generado, el valor por defecto es de 250
 - Si configuramos 0, corresponde a ilimitado
- **fileMode:**
 - Circular, significa que la captura, al llegar al valor especificado como maxSize por defecto 250MB, empezará a sobrescribirse la información

Sugerencia de estudio

- USBPcap: aplicación Windows libre para realizar capturas
 - Se puede descargar desde <https://desowin.org/usbpcap/index.html>



¿Qué es ntopng?

- Ntopng is a free and open source software for monitoring network traffic that provides a web interface for real-time network monitoring. It is the next generation version of the original ntop that shows the network usage, similar to what the popular top Unix command does
- It supports different operating system like, Unix, Linux, Mac OS, BSD and Windows
- We will use Ubuntu Server

Configure Ntopng

- After installing Ntopng, you will need to modify Ntopng default configuration file located at /etc/ntopng/ntopng.conf:
 - **sudo nano /etc/ntopng/ntopng.conf**
- Make the following changes:
 - **-G=/var/run/ntopng.pid**
 - **##Specifies the network interface or collector endpoint to be used by ntopng for network monitoring.**
 - **-i=enp0s3**
 - **##Sets the HTTP port of the embedded web server.**
 - **-w=3000**
- Save and close the file, then create a ntopng.start file:
 - **sudo nano /etc/ntopng/ntopng.start**
- Add the following lines as per your network:
 - **--local-networks "192.168.0.0/24" ## give your local IP Ranges here.**
 - **--interface 1**
- Save and close the file, then restart Ntopng and enable it to start on boot time:
 - **sudo systemctl start ntopng**
 - **sudo systemctl enable ntopng**

Existe versión ntopng para Windows

- Puede obtenerse información y descargarse desde :
 - <https://www.ntop.org/products/traffic-analysis/ntop/>



Para entregar

- Una vez finalizada la práctica deberás entregar:
 - El informe de práctica con los detalles de ejecución según la plantilla de prácticas
 - Las pantallas más significativas que demuestren la ejecución (no necesariamente del ejemplo, pero si hay que utilizar el resto de herramientas con un escenario imaginado por ti)