WireShark

Server Exploits - Module 2

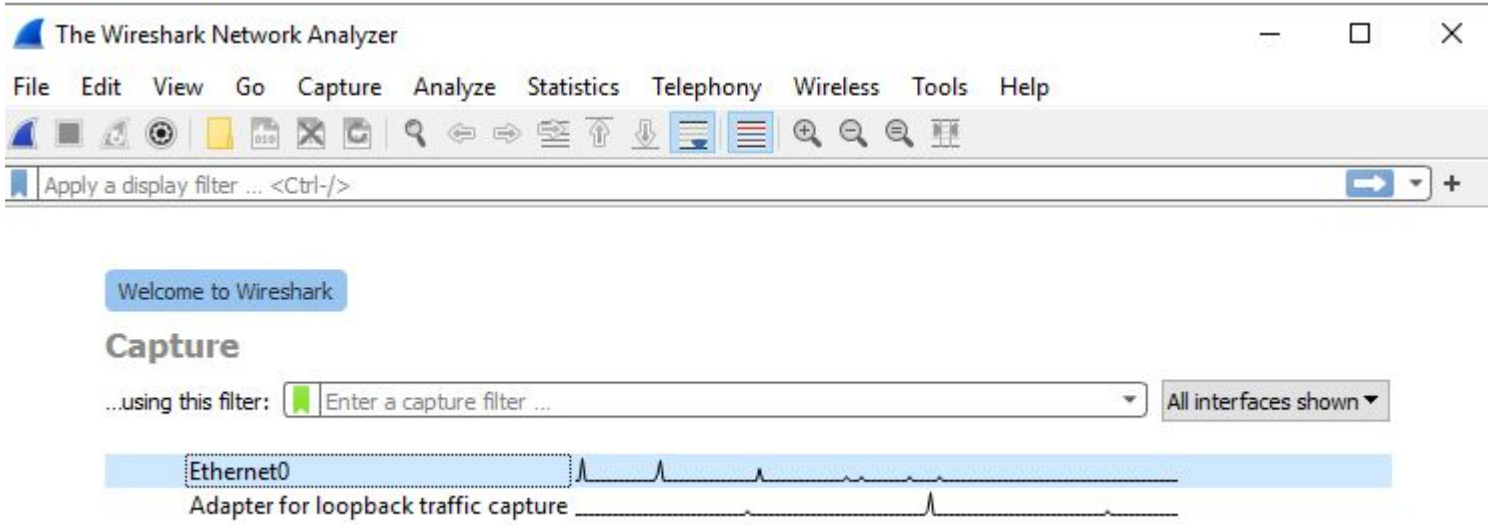
How to use - Looking at HTTP

Wireshark

You can install WIreshark on your DC via Wireshark's website. Once you run it, you'll see the options to capture on Ethernet 0 and Adapter for loopback traffic. Loopback traffic is for connections from the DC to itself, so we aren't interested in that. All connections from your DC to your workstation will be over Ethernet 0.

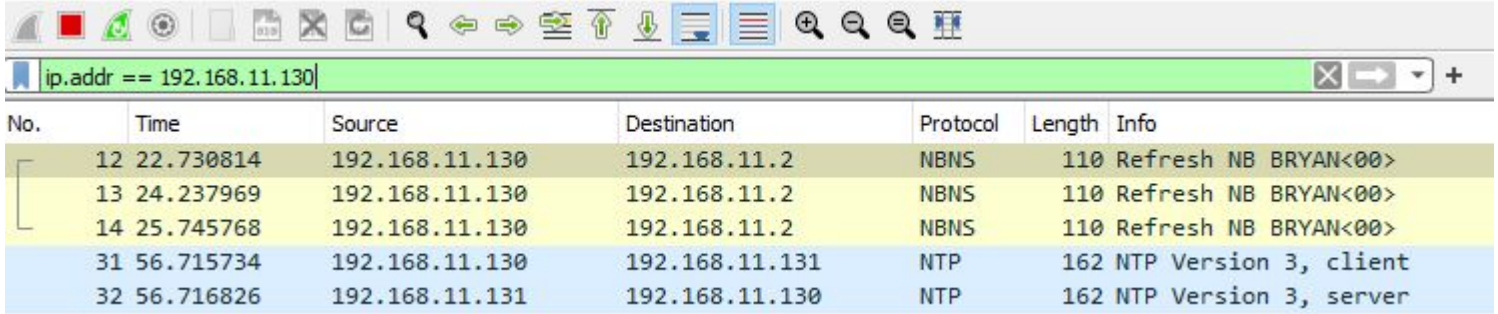
Don't worry if your network adapter isn't called Ethernet 0. It may go under a different name, but you will likely only have one adapter to choose from. Select Ethernet 0 and click the Blue shark fin in the top left to start capturing packets.

Wireshark


The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Ethernet0
Adapter for loopback traffic capture

Wireshark

You will likely see packets already coming and going from your network. We will filter these packets to only see traffic between your DC and workstation. Type the following filter, replacing my IP address for the IP address of your workstation and hit Enter.



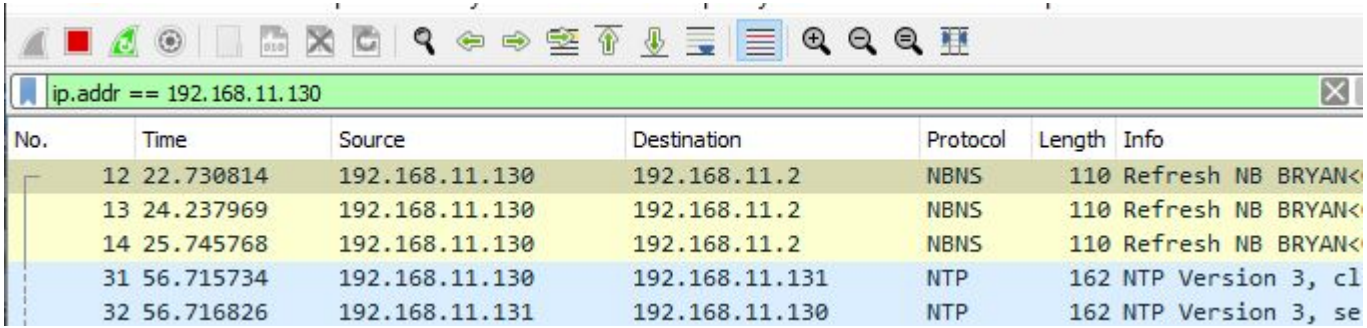
Wireshark

Now open Powershell on your DC and send a command over Win-RM. I use the ipconfig command.

```
PS C:\Users\Administrator> Invoke-Command -computername DOMAINCLIENT.bryan.local -ScriptBlock {ipconfig}
```

Wireshark

You will see many packets captured on Wireshark. You can click the red square to stop recording packets after you command is run.



No.	Time	Source	Destination	Protocol	Length	Info
12	22.730814	192.168.11.130	192.168.11.2	NBNS	110	Refresh NB BRYAN<
13	24.237969	192.168.11.130	192.168.11.2	NBNS	110	Refresh NB BRYAN<
14	25.745768	192.168.11.130	192.168.11.2	NBNS	110	Refresh NB BRYAN<
31	56.715734	192.168.11.130	192.168.11.131	NTP	162	NTP Version 3, cl
32	56.716826	192.168.11.131	192.168.11.130	NTP	162	NTP Version 3, se

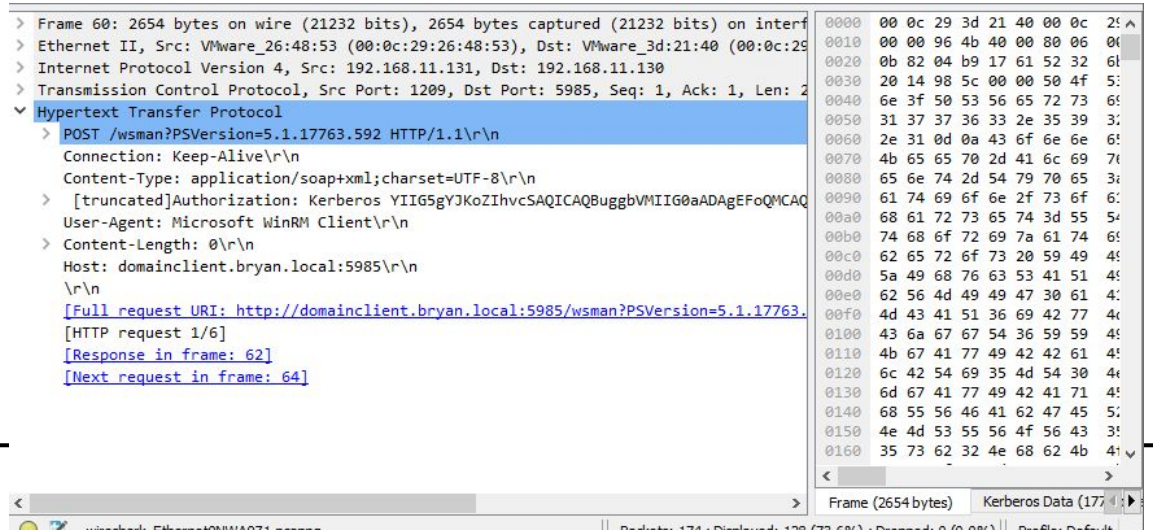
Wireshark

Scroll down until you see TCP packets. The first 3 are the TCP handshake, which we went over in module 1. Once the TCP connection between the DC and workstation is made, the DC sends an HTTP request to the Workstation. Click on this packet.

57	204.182412	192.168.11.131	192.168.11.130	TCP	66	1209 → 5985 [SYN, ECE, CWR] Seq=0 Win=6
58	204.182688	192.168.11.130	192.168.11.131	TCP	66	5985 → 1209 [SYN, ACK] Seq=0 Ack=1 Win=
59	204.182735	192.168.11.131	192.168.11.130	TCP	54	1209 → 5985 [ACK] Seq=1 Ack=1 Win=21022
60	204.182825	192.168.11.131	192.168.11.130	HTTP	2654	POST /wsman?PSVersion=5.1.17763.592 HTT
61	204.182980	192.168.11.130	192.168.11.131	TCP	60	5985 → 1209 [ACK] Seq=1 Ack=2601 Win=21
62	204.186374	192.168.11.130	192.168.11.131	HTTP	395	HTTP/1.1 200
63	204.187596	192.168.11.131	192.168.11.130	TCP	341	1209 → 5985 [PSH, ACK] Seq=2601 Ack=342
64	204.187640	192.168.11.131	192.168.11.130	HTTP	8272	POST /wsman?PSVersion=5.1.17763.592 HTT
65	204.187792	192.168.11.130	192.168.11.131	TCP	60	5985 → 1209 [ACK] Seq=342 Ack=11106 Win
66	204.413285	192.168.11.130	192.168.11.131	TCP	1514	5985 → 1209 [ACK] Seq=342 Ack=11106 Win

Wireshark

You'll be able to see what is included in this packet. This is the start of Win-RM's authentication over HTTP. Because this is an HTTP packet, this data is sent unencrypted. Anyone performing an adversary-in-the-middle attack could see this information in plaintext. Not good.



How to use - Looking at HTTPS

Wireshark

HTTPS is a little more complicated than HTTP. First, packets will be sent over TLS (hopefully TLS 1.2 and not 1.0). After the TCP handshake, TLS will do its own handshake. This is a Client Hello, Server Hello and certificate exchange. This is the preliminary steps to sharing encryption keys between the client and server so that traffic to and from the client and the server can be encrypted. On the next slide is an example of the TCP and TLS handshake from me visiting nscc.ca (IP address 204.16.56.102)

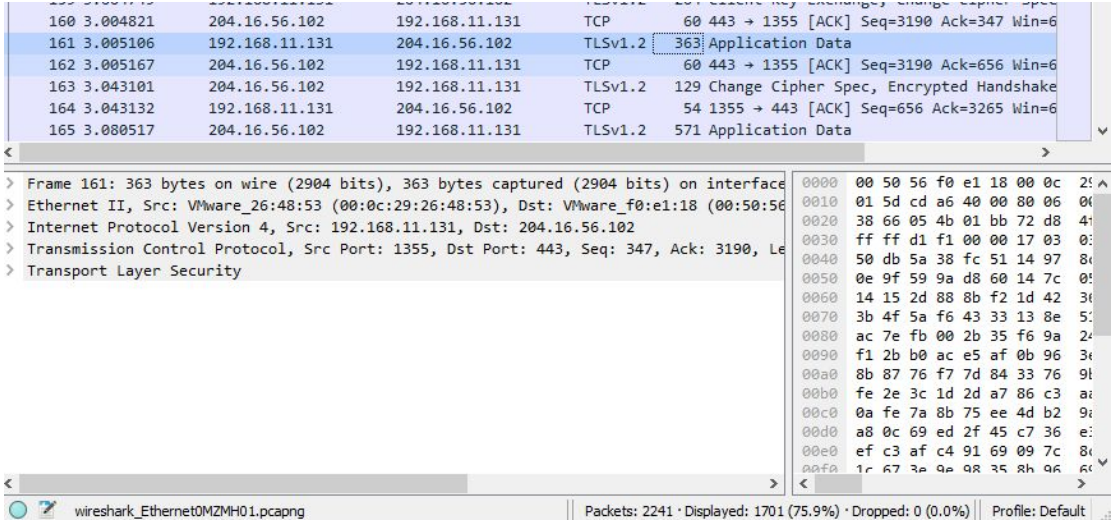
Wireshark

ip.addr == 204.16.56.102

No.	Time	Source	Destination	Protocol	Length	Info
16	0.814294	192.168.11.131	204.16.56.102	TCP	54	1349 → 80 [ACK] Seq=263 Ack=134 Win=655
17	0.815214	192.168.11.131	204.16.56.102	TCP	54	1349 → 80 [FIN, ACK] Seq=263 Ack=134 Wi
18	0.815305	204.16.56.102	192.168.11.131	TCP	60	80 → 1349 [ACK] Seq=134 Ack=264 Win=642
129	2.718230	192.168.11.131	204.16.56.102	TCP	66	1355 → 443 [SYN, ECE, CWR] Seq=0 Win=65
130	2.756430	204.16.56.102	192.168.11.131	TCP	60	443 → 1355 [SYN, ACK] Seq=0 Ack=1 Win=6
131	2.756516	192.168.11.131	204.16.56.102	TCP	54	1355 → 443 [ACK] Seq=1 Ack=1 Win=65535
132	2.760679	192.168.11.131	204.16.56.102	TLSv1.2	250	Client Hello
133	2.760821	204.16.56.102	192.168.11.131	TCP	60	443 → 1355 [ACK] Seq=1 Ack=197 Win=6424
134	2.799005	204.16.56.102	192.168.11.131	TCP	1514	443 → 1355 [ACK] Seq=1 Ack=197 Win=6424
135	2.799005	204.16.56.102	192.168.11.131	TLSv1.2	1441	Server Hello, Certificate
136	2.799036	192.168.11.131	204.16.56.102	TCP	54	1355 → 443 [ACK] Seq=197 Ack=2848 Win=6
137	2.799626	204.16.56.102	192.168.11.131	TLSv1.2	396	Server Key Exchange, Server Hello Done
138	2.799638	192.168.11.131	204.16.56.102	TCP	54	1355 → 443 [ACK] Seq=197 Ack=3190 Win=6
159	3.004749	192.168.11.131	204.16.56.102	TLSv1.2	204	Client Key Exchange, Change Cipher Spec

Wireshark

Once the TLS handshake is complete, the client can send encrypted data as an Application Data packet to the server. I've highlighted one here.



Wireshark

If you expand the Transport Layer Security (TLS) dropdown, you can see the data being sent. However, all you can see is encrypted data because the data is being sent over HTTPS. An attacker doing an adversary-in-the-middle attack would have to decrypt this data to get the information. If it’s encrypted with TLS 1.2 and a strong cipher, this could take a really long time (years) to crack.

Wireshark

161	3.005106	192.168.11.131	204.16.56.102	TLSv1.2	363 Application Data

```
Frame 161: 363 bytes on wire (2904 bits), 363 bytes captured (2904 bits) on interface
Ethernet II, Src: VMware_26:48:53 (00:0c:29:26:48:53), Dst: VMware_f0:e1:18 (00:50:56
Internet Protocol Version 4, Src: 192.168.11.131, Dst: 204.16.56.102
Transmission Control Protocol, Src Port: 1355, Dst Port: 443, Seq: 347, Ack: 3190, Le
Transport Layer Security
  TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 304
    Encrypted Application Data: 4aec22607c50db5a38fc5114978c371779884584e90e9f599ad
    [Application Data Protocol: Hypertext Transfer Protocol]
```

```
0030  ff ff d1 f1 00 00 17 03  03
0040  50 db 5a 38 fc 51 14 97  8c
0050  0e 9f 59 9a d8 60 14 7c  05
0060  14 15 2d 88 8b f2 1d 42  30
0070  3b 4f 5a f6 43 33 13 8e  51
0080  ac 7e fb 00 2b 35 f6 9a  24
0090  f1 2b b0 ac e5 af 0b 96  3e
00a0  8b 87 76 f7 7d 84 33 76  9b
00b0  fe 2e 3c 1d 2d a7 86 c3  aa
00c0  0a fe 7a 8b 75 ee 4d b2  9a
00d0  a8 0c 69 ed 2f 45 c7 36  e3
00e0  ef c3 af c4 91 69 09 7c  8c
00f0  1c 67 3e 9e 98 35 8b 96  69
0100  4d b9 fa ff 1c 78 0a 08  0c
0110  a3 e3 d6 b6 fd d7 39 ab  bb
0120  90 eb 96 7a ff 55 1e 07  7a
0130  3b dd 2e 10 ac b5 0d e8  25
0140  3d c7 94 a4 9a 4b 9f 8a  13
0150  e0 03 30 f6 92 ac f9 05  ec
0160  ff d9 47 ca 9b 7d 2c 2b  85
```

Payload is encrypted application data (tls.app_data), 304 bytes | Packets: 2241 · Displayed: 1701 (75.9%) · Dropped: 0 (0.0%) | Profile: Default

Wireshark

You can view the specific cipher by going to a “Change Cipher Spec” packet and looking in the TLS dropdown under handshake Protocol. In the next example, you can see we are using a strong Elliptical Curve cipher (EC).

Wireshark

159	3.004749	192.168.11.131	204.16.56.102	TLSv1.2	204 Client Key Exchange, Change Cipher Spec
160	3.004821	204.16.56.102	192.168.11.131	TCP	60 443 → 1355 [ACK] Seq=3190 Ack=347 Win=6
161	3.005106	192.168.11.131	204.16.56.102	TLSv1.2	363 Application Data

```
> Frame 159: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits) on interf
> Ethernet II, Src: VMware_26:48:53 (00:0c:29:26:48:53), Dst: VMware_f0:e1:18 (00:50
> Internet Protocol Version 4, Src: 192.168.11.131, Dst: 204.16.56.102
> Transmission Control Protocol, Src Port: 1355, Dst Port: 443, Seq: 197, Ack: 3190,
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 70
    v Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 66
      v EC Diffie-Hellman Client Params
          Pubkey Length: 65
          Pubkey: 0400a5dba2215fbdace96b716ac4e98ded1a07fdfe04355259471c42c3ef7db
  v TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
```

```
0000  00 50 56 f0 e1 18 00 0c  2
0010  00 be cd a5 40 00 80 06  0
0020  38 66 05 4b 01 bb 72 d8  4
0030  ff ff d1 52 00 00 16 03  0
0040  04 00 a5 db a2 21 5f bd  a
0050  ed 1a 07 fd fe 04 35 52  5
0060  22 c6 52 b7 5d 2d 9d af  e
0070  10 41 4f 89 24 c1 c8 4d  8
0080  a8 14 03 03 00 01 01 16  0
0090  00 bb 1b 0c 50 86 0c 54  3
00a0  6b d1 6a 46 e1 b8 5d a2  5
00b0  60 05 01 1e 4c 58 2a 90  1
00c0  61 16 08 49 57 38 1d 1a  9
```

Text item (text), 66 bytes | Packets: 2241 · Displayed: 1701 (75.9%) · Dropped: 0 (0.0%) | Profile: Default