**Introduction to Network Traffic Analysis with Wireshark**

#### Question 1: What is the *DESTINATION* *port* of the packet in question? Hint the DESTINATION IP address IS 65.165.167.86. The SQL Server Browser service listens on this port for incoming connections.

1434

#### Question 2: Name the protocol used to spread the SQL Slammer Worm in this packet.

UDP or User Datagram Protocol

Note: UDP use the IP protocol, the same as TCP. TCP establishes a connection to know what packets were sent and received. UDP is connectionless, firing off packets and forgetting them (not checking if received). It is primarily used for establishing low-latency and loss-tolerating connections between applications on the internet. It speeds up transmissions by enabling the transfer of data before an agreement is provided by the receiving party.

#### Question 3: In Packet No. 5, what URL was queried for its DNS information?

#### Hint: look under “Domain Name System (response)” and expand the “Queries” tab.

google.com

#### Question 4: In Packet No. 5 (and all of these DNS packets), what protocol is used?

UDP

#### Question 5: What is the IP address of the Domain Name Server (i.e. the computer that handles the phonebook lookups)? This computer is the source of the DNS responses (answers).

192.168.70.20

#### Question 6: Give the of SSID of two devices.

This is the “text” name of the devices. Any two of the following 42 SSIDs works!

|  |
| --- |
| 000000000000 |
| 111111111111 |
| 222222222222 |
| 333333333333 |
| 444444444444 |
| 555555555555 |
| 666666666666 |
| 777777777777 |
| 888888888888 |
| !!!!!!!!!!!! |
| ############ |
| $$$$$$$$$$$$ |
| %%%%%%%%%%%% |
| &&&&&&&&&&&& |
| \*\*\*\*\*\*\*\*\*\*\*\* |
| @@@@@@@@@@@@ |
| ^^^^^^^^^^^^ |
| AAAAAAAAAAAA |
| BBBBBBBBBBBB |
| CCCCCCCCCCCC |
| DDDDDDDDDDDD |
| EEEEEEEEEEEE |
| FFFFFFFFFFFF |
| GGGGGGGGGGGG |
| HHHHHHHHHHHH |
| IIIIIIIIIIII |
| JJJJJJJJJJJJ |
| KKKKKKKKKKKK |
| LLLLLLLLLLLL |
| MMMMMMMMMMMM |
| NNNNNNNNNNNN |
| PPPPPPPPPPPP |
| QQQQQQQQQQQQ |
| RRRRRRRRRRRR |
| SSSSSSSSSSSS |
| TTTTTTTTTTTT |
| UUUUUUUUUUUU |
| VVVVVVVVVVVV |
| WWWWWWWWWWWW |
| XXXXXXXXXXXX |
| YYYYYYYYYYYY |
| ZZZZZZZZZZZZ |

#### Question 7: What is the SSID being used for the device with the BSS Id: Netgear\_45:44:56 (00:1f:33:45:44:56)

SSSSSSSSSSSS

#### Question 8: What is the channel being used by the WAP with the BSSID Netgear\_45:44:56?

6 - this is the channel for all of the WAPs. It looks like one piece of hardware being re-used with MAC spoofing.

#### Question 9: How many of these APs in the approved device whitelist?

Two of the 42 are in the whitelist.

#### Question 10: Are there any rouge APs (yes/no)? This would be any APs on the network that are NOT on the approved whitelist.

Yes!!

#### Question 11: If rogue wireless access points (WAPs) exist, how many?

40 of the 42 are not on the whitelist, and are considered rogue.