How can you view active network connections on both Linux and Windows machines?

**For windows you can go to the command prompt and use the “Netstat” command to find the active connections. For linux you will use the “ss” commands which will display the network socket related information on a linux system.**

What RFCs define the DNS protocol? BONUS: When is DNS sent via TCP?

DNS is sent via TCP for zone transfers.

**Dozens of RFCs define DNS protocol:**

Example:

**8618**

**8598**

|  |
| --- |
| **8567** |

**Bonus: The TCP is used when information being exchanged is larger than 512 bytes.**

Why is it important to monitor DNS traffic in an organization?

**Monitoring DNS traffic will allow the organization to identify security attacks and enable successful blocking of attacks and fixing vulnerabilities.**

Why would a incident responder want to view both active network connections on a computer, as well as what ports applications or processes a computer may be listening on?

**It will give you information about the services and processes on the system that are waiting to service network requests. Also the incident responder can detect any running malware on the system.**