Team: Team 02 - ASU

Inject Number: 15

Inject Duration: 60 Minutes

Inject Start Date/Time: Sat, 28 Jan 2017 11:29:12 -0800

From: Felonius Gru

To: IT Staff

Subject: Install and Use Wireshark

The auditor had a question about the traffic hitting our Domain Control. They have asked for you to install WireShark and perform a packet capture of about 3MB in size. Please configure Wireshark to make sure the capture only contains the traffic originating or destined for the DC.

Upload your capture file to the Blue Team Portal Page and provide a separate document outlining what the data is telling us. Is the machine under attack or compromised?

Thank you.

Felonius Gru