Team: Team 8

Inject Number: 34

Inject Duration: 40 Minutes

Inject Start Date/Time: Sat, 13 Feb 2021 19:15:31 +0000

From: IT Director

To: To Infrastructure Team

Subject: INRP - Forensic Investigation

Use Wireshark to monitor the traffic on the Debian Email host. Analyzing the packet capture, develop a report about traffic anomalies, identifying where
they are coming from (host addresses) and what exploit is being attempted. These source host addresses are compromised hosts that you need to attend to.

Include a screen capture of example packet decodes that illustrate this traffic.

Thank you.

IT Director