Team: Team 3

Inject Number: 12

Inject Duration: 120 Minutes

Inject Start Date/Time: Sat, 04 Mar 2017 16:03:29 +0000

From: CIO

To: Infrastructure Team

Subject: 001 Traffic Analysis

For each server, use a packet-capture tool to analyze 5 minutes of network traffic bi-directionally to the device. Respond with a memo that:

1.) Shows a screen shot that documents a sample of packet capture traffic.
2.) An analysis as to if this traffic looks legitimate. Discuss how you determined that.
3.) For traffic that was deem not authorized/legitimate, what steps are you going to take to mitigate it.

Thank you.

CIO