Team: Team 3

Inject Number: 47

Inject Duration: 60 Minutes

Inject Start Date/Time: Sat, 24 Mar 2018 14:36:05 -0500

From: IT Director

To: Infrastructure Team

Subject: [F-223] Outbound Connections

The CIO is concerned that data exfiltration or backdoor access might be occurring. Use the FW and Splunk logs to look for suspicious connections and take steps to mitigate these.
Write a memo that documents how you did the analysis (with screen shots), what was found, and how did you mitigate these connections. Include an assessment as to what damage these connections likely did.

Thank you.

IT Director