**Final Project for CIT  
ThriveDX Cybersecurity Boot Camp at UB**

Adam Nowak - 8/22/2022  
[www.linkedin.com/in/adam-michael-nowak](http://www.linkedin.com/in/adam-michael-nowak)

# Scenario

An organization’s monitoring system identified suspicious download activities captured in a honeypot named Cowrie. The Splunk system recorded the event, but the system cannot be accessed because its operator, who was the head of the security investigation team, was recently released from the company. You were hired as a security analyst not long after.

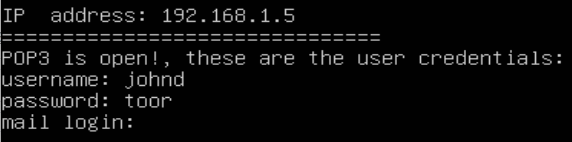
Due to the recent events, there was not enough time to provide you with all the information required to freely access the system. However, the system administrator was able to provide you with access to the mail server and told you that all the data needed to access the system is stored on that server.

Your objective is to connect to the Splunk system, investigate the events, and identify a suspicious message to obtain the flag.

# Task 1: Connect to the Mail Server

In this task, you will connect to the mail server and retrieve the important emails.

1. Inspect the Ubuntu VM and note the message about the POP3 protocol.



2. Which port does POP3 use?

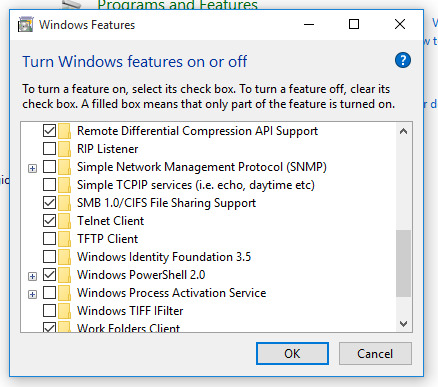
**Port 110**

3. Use Telnet to connect to the POP3 service via PowerShell. Were you successful? Why?

**It did not work. Telnet was not installed as a default**

4. Install Telnet in the Windows 10 VM.

**By accessing the Windows Features I was able to turn on the Telnet Client.**

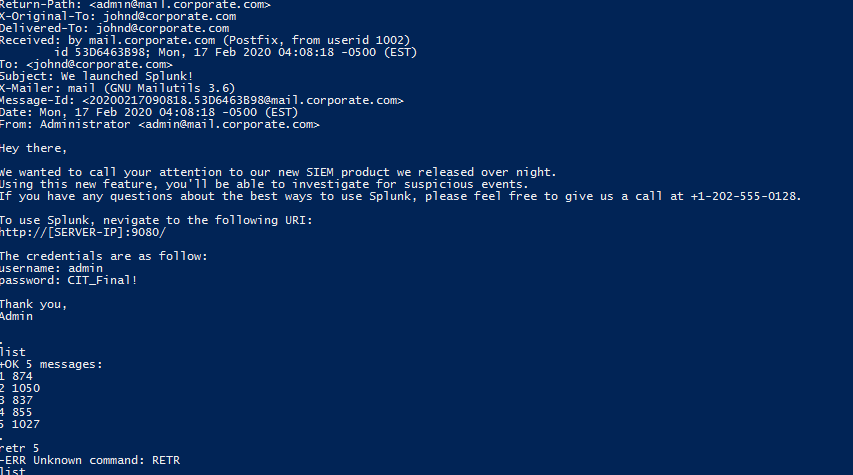


5. Try to establish the connection again and log in once connected.

**Using the command “***telnet 192.168.1.5 110***” in PowerShell allowed me to gain access since both machines are on the same network. Port 110 in this command is the POP3 port.**

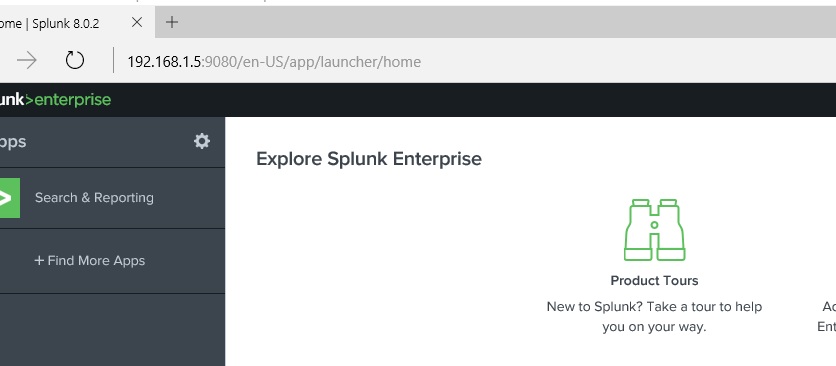
6. List the existing emails and investigate them to search for interesting information.

**The 4th email contained the relevant information - a URL that would take us to the next step.**



7. Enter the provided URL and log into the system.

**I used Splunk to begin this investigation.**

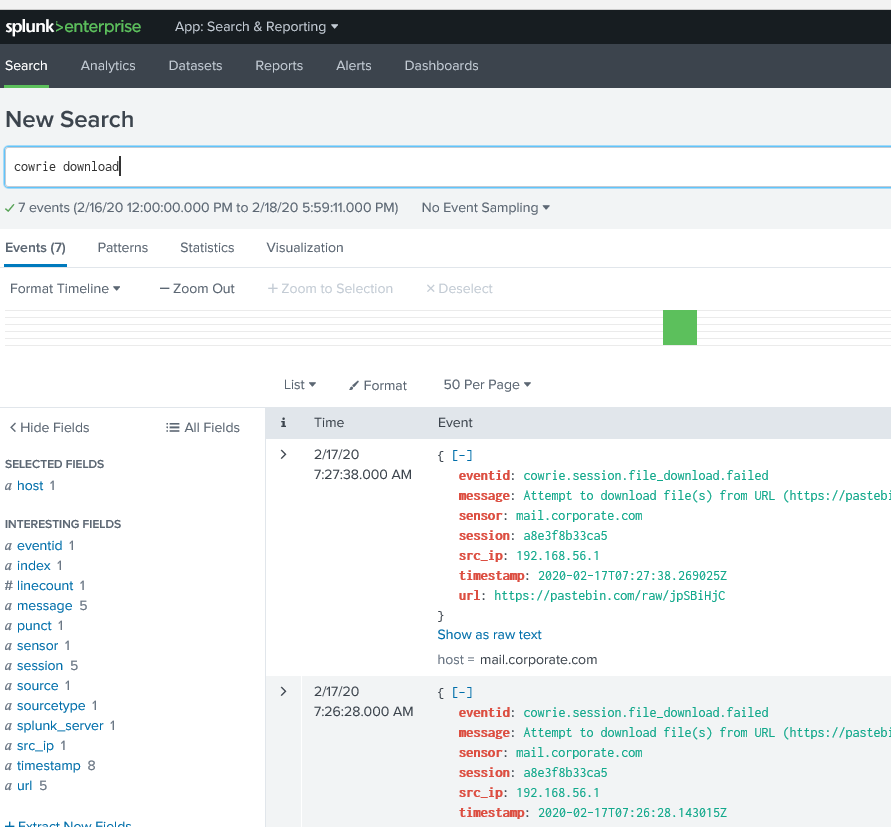


# Task 2: Search for Suspicious Activity

In this task, you will search for recorded suspicious activity in the organization.

1. In the platform, search for records of the download attempt and investigate them to identify the potential sources.

**I searched for the words “download” and “cowrie”, the name of the honeypot in question.**



2. Access the located sources to search for interesting information in them.

**This revealed a URL that had something interesting in it.**





3. Decipher the messages located in the URLs and identify the flag.

**Using a BASE64 decoder on the hash provided the two messages.**

