**California State University Long Beach**

**CYBER SECURITY**

**LB-CS-O5-CIT: Cyber Infrastructure and Technology**

**Final Project: Capture The Flag Challenge**

# KENNETH DAVIS

**January 2021**



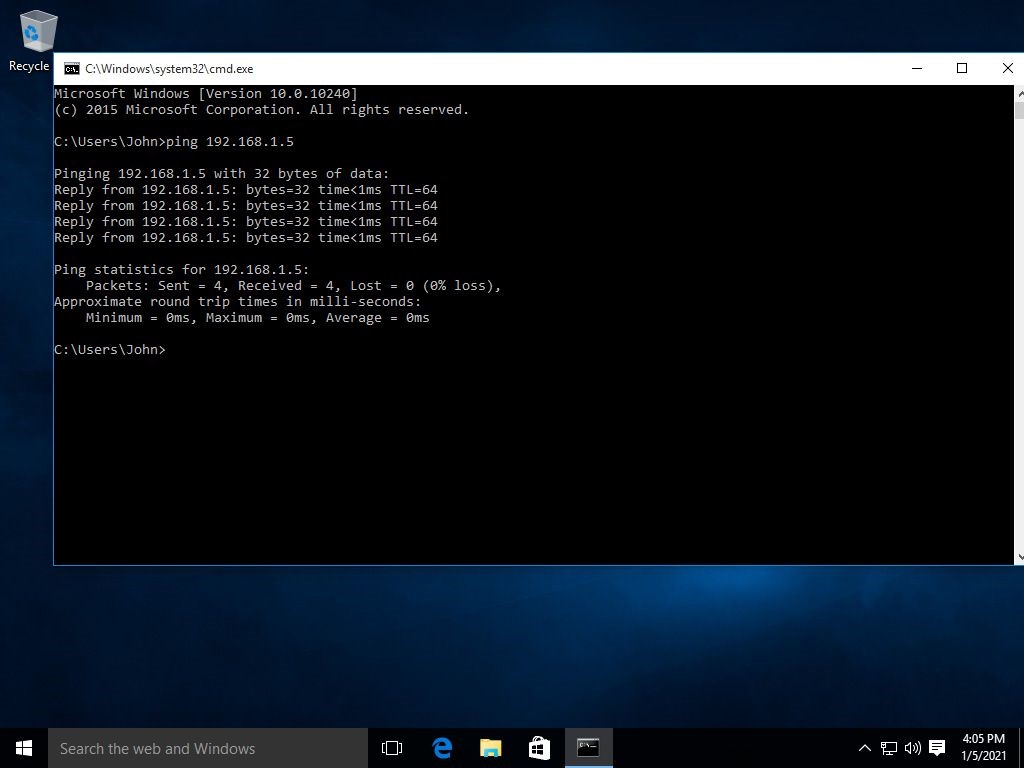
**Project Summary**

* An organization’s monitoring system identified suspicious download activities captured in a honeypot that was named Cowrie. The event was recorded by the Splunk system, 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 wasn’t enough time to provide you with all the information required to access the system freely. 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.
* STEPS TAKEN TO CAPTURE THE FLAG -

● Telnet was used to connect to the Email server (POP3) to retrieve emails containing SPLUNK Login Info.

* Logged into SPLUNK and reviewed logs to find suspicious entries with suspicious download failures
* Researched the URLs of the Download Failures which led to suspicious hashes
* Hashes converted in

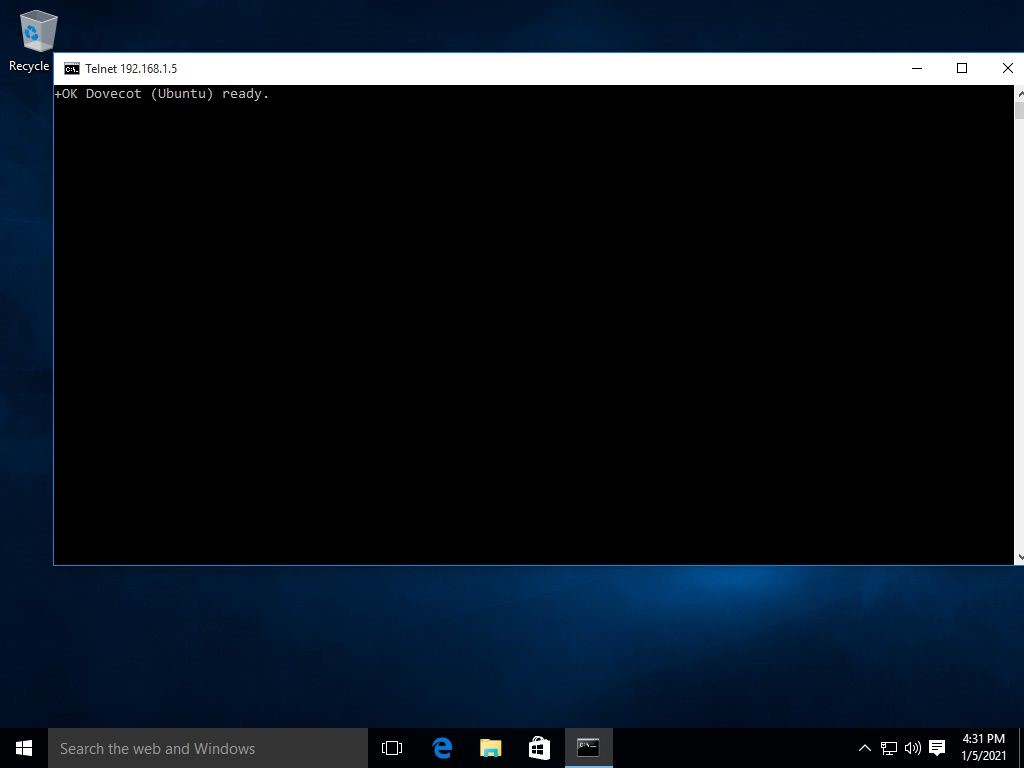
**Figure 1 - Windows 10 Ping to Ubuntu**



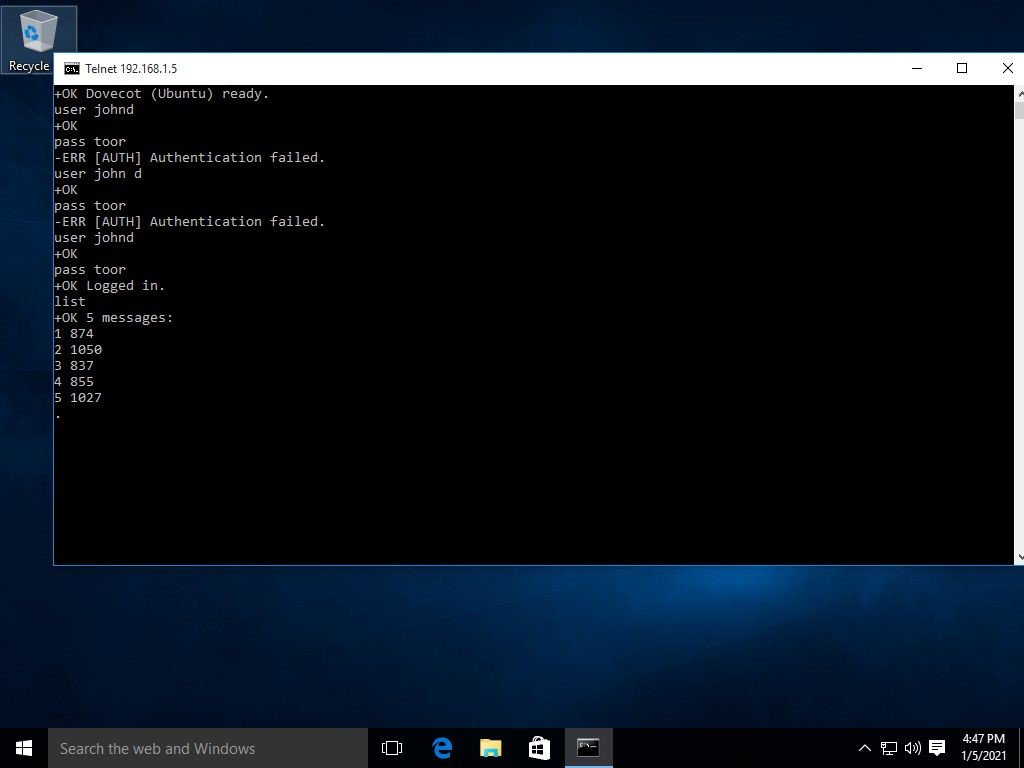
**Task 1**

1. 
2. **POP3 uses port 110**
3. **Telnet connection unsuccessful due to Telnet not Being installed.**
4. **Telnet installed on Windows 10 machine through Control Panel**

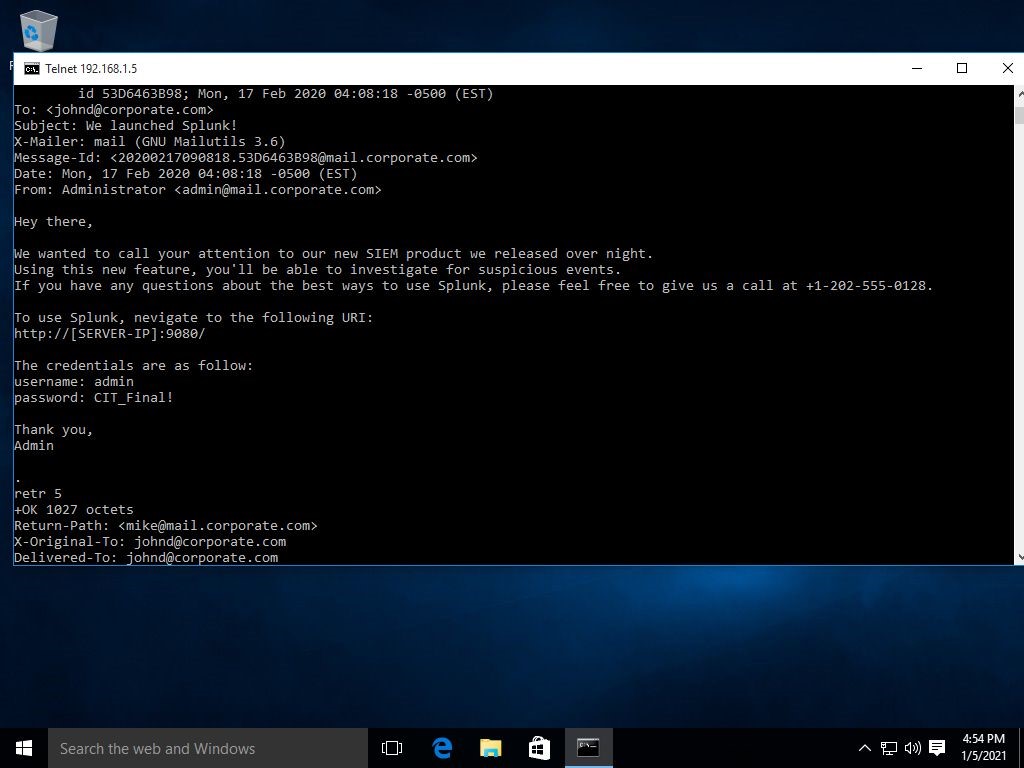
**Connection Successful with Telnet to POP3 mail server**



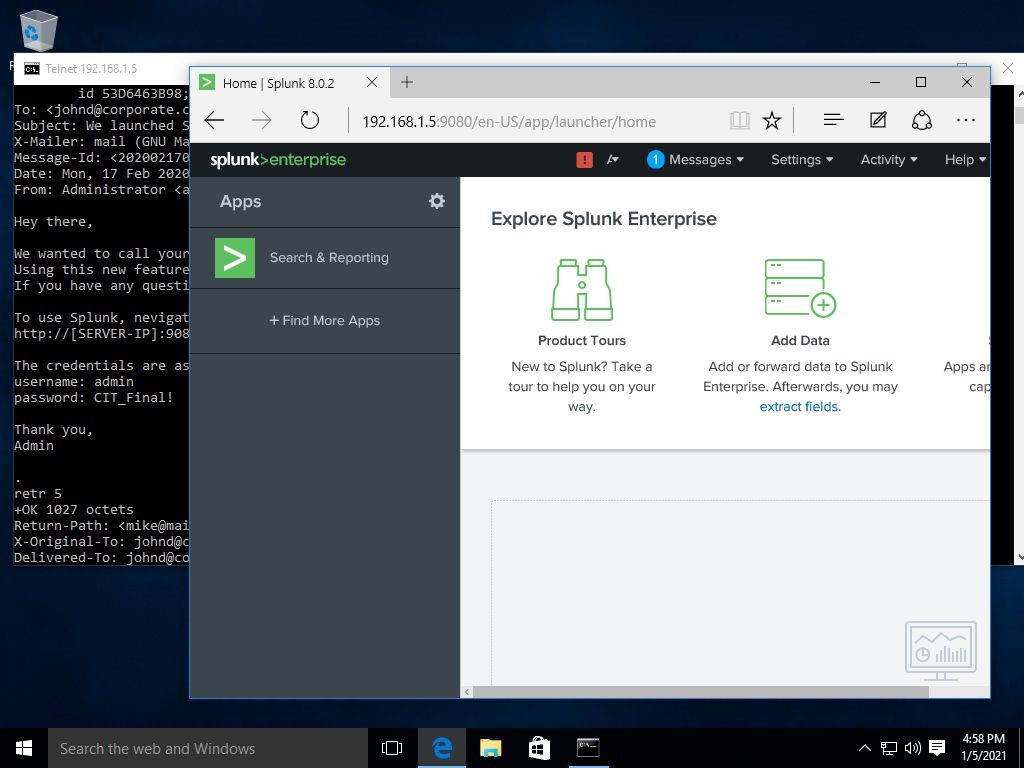
**Login to email account successful and emails listed**



**Using retr command to inspect emails, Email # 4 gave login info to Splunk**

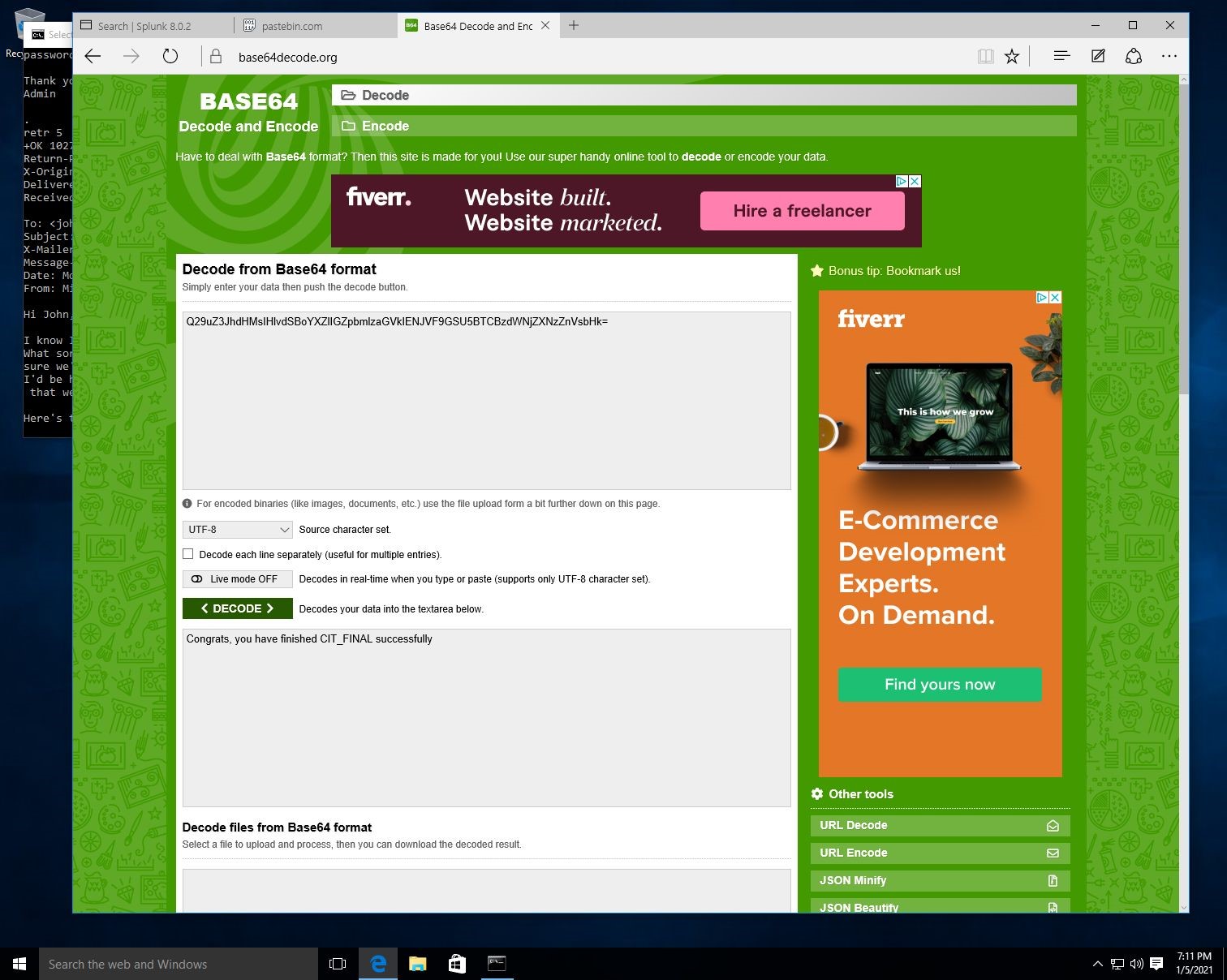


**Login to Splunk successful with info found in email**



**Task 2**

**1. I searched through the emails that were downloaded from Johns inbox. I noticed with the last message that had a strange subject line, with weird letters. I started to investigate the source the email came from, and around the date the email was received. Upon investigation I noticed that searching the email returned events that noted there was a download failure. The URL stuck out also since it had pastebin included. Searching the URL revealed different encrypted messages, which ultimately led me to the FLAG!**



**2.**