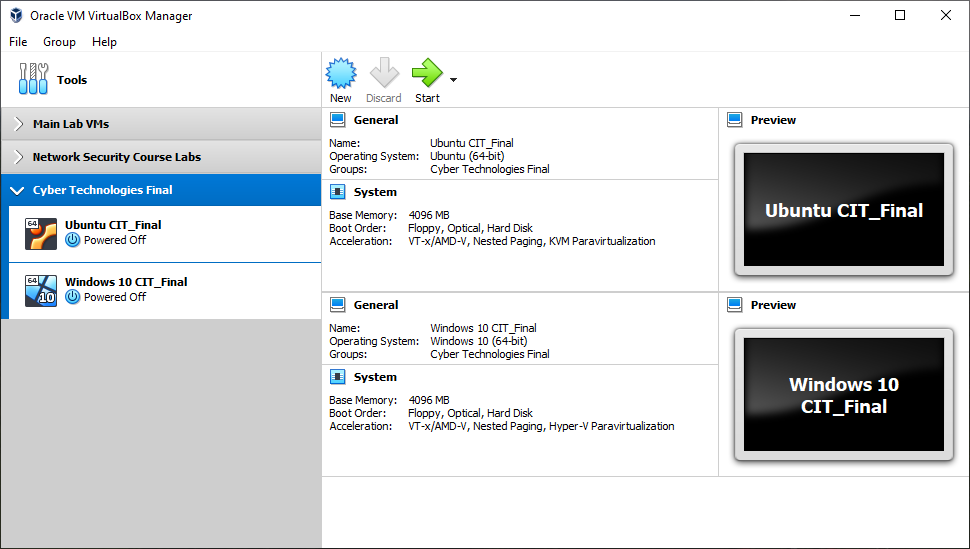
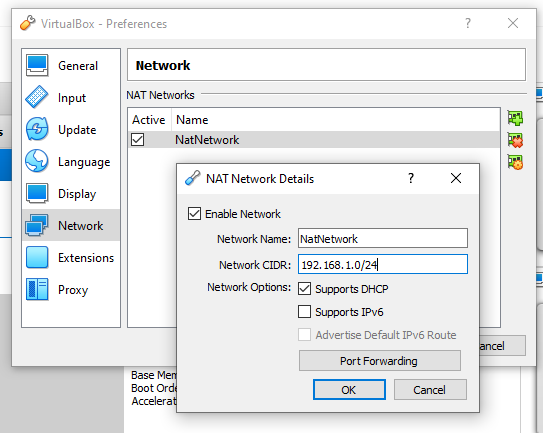
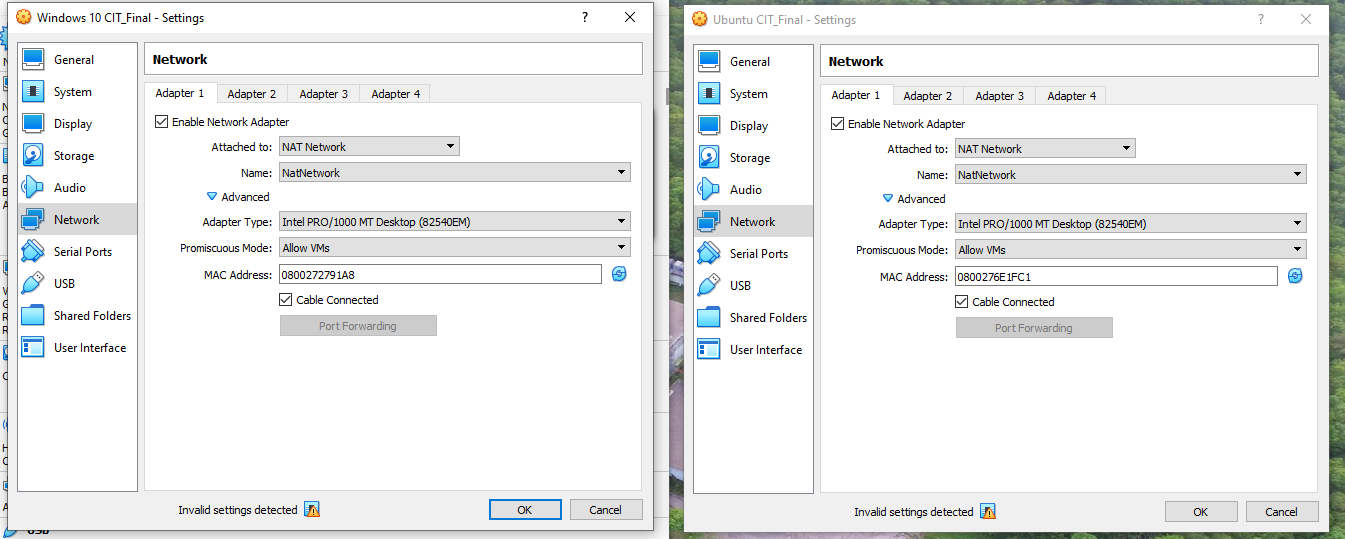
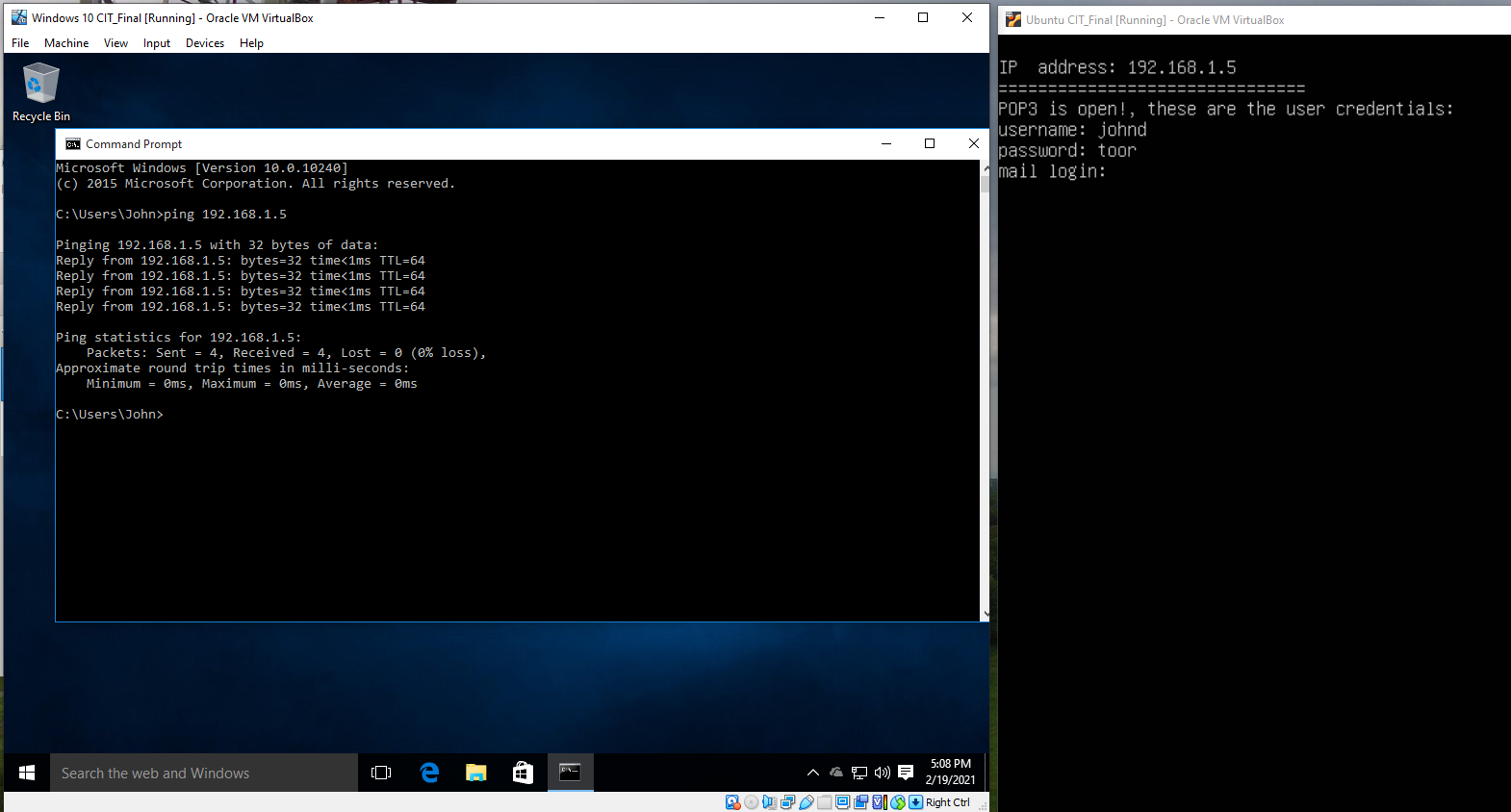
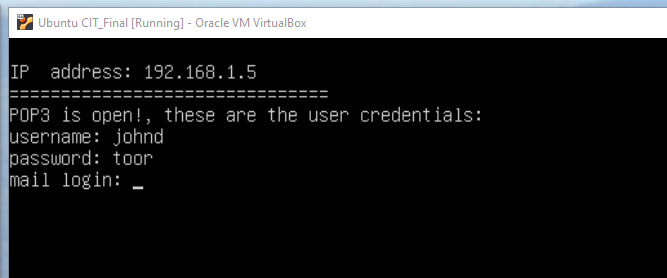
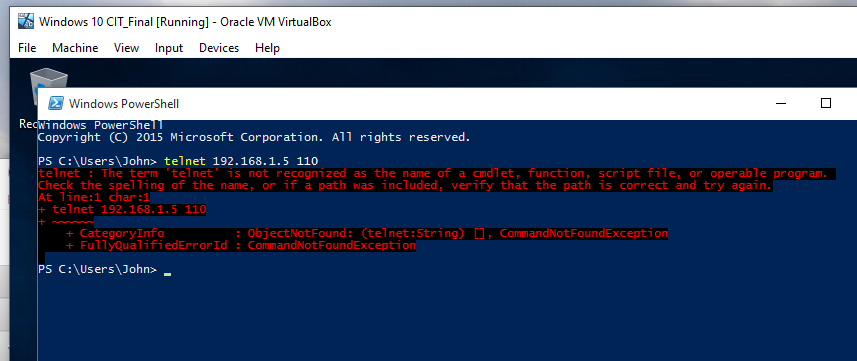
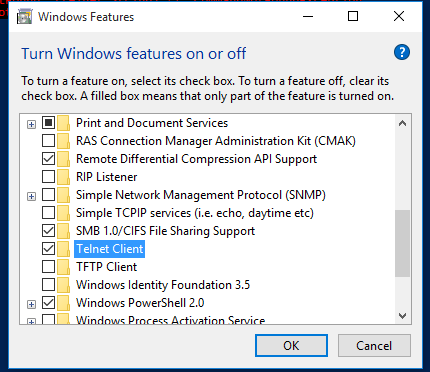
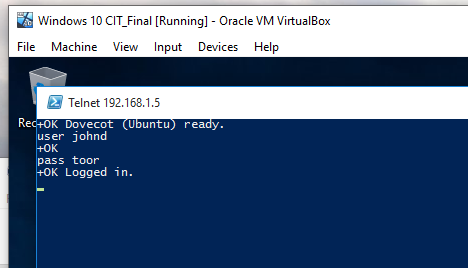
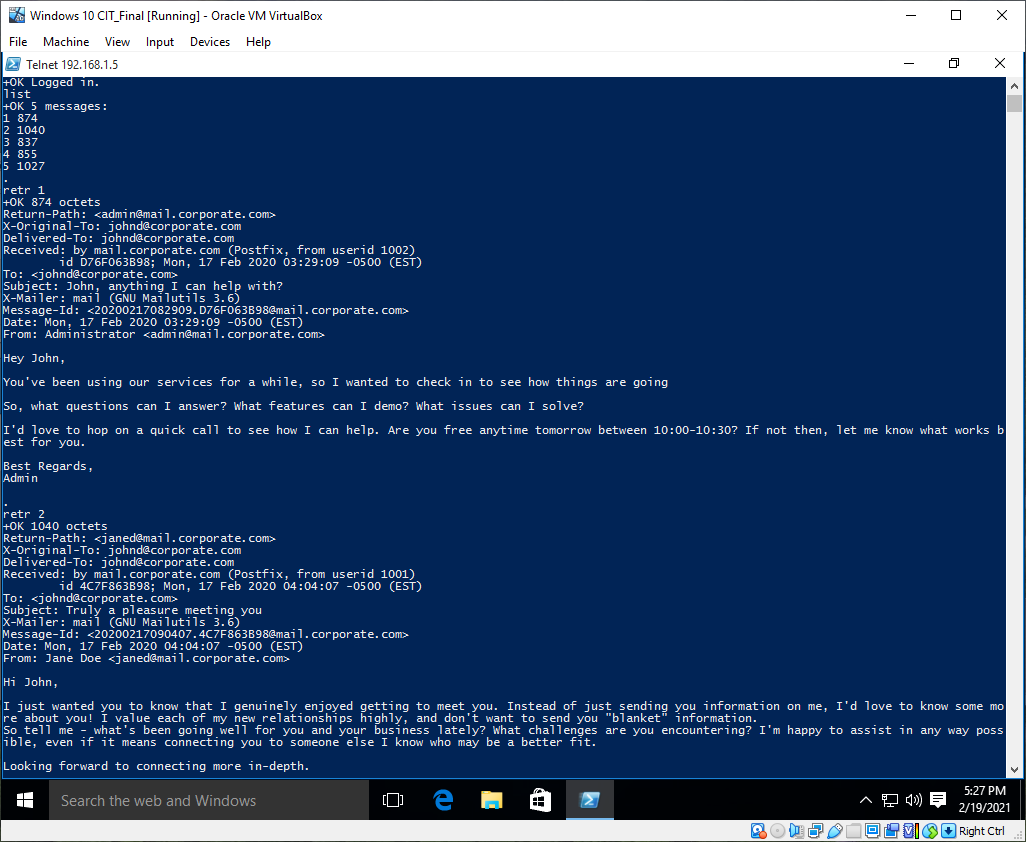
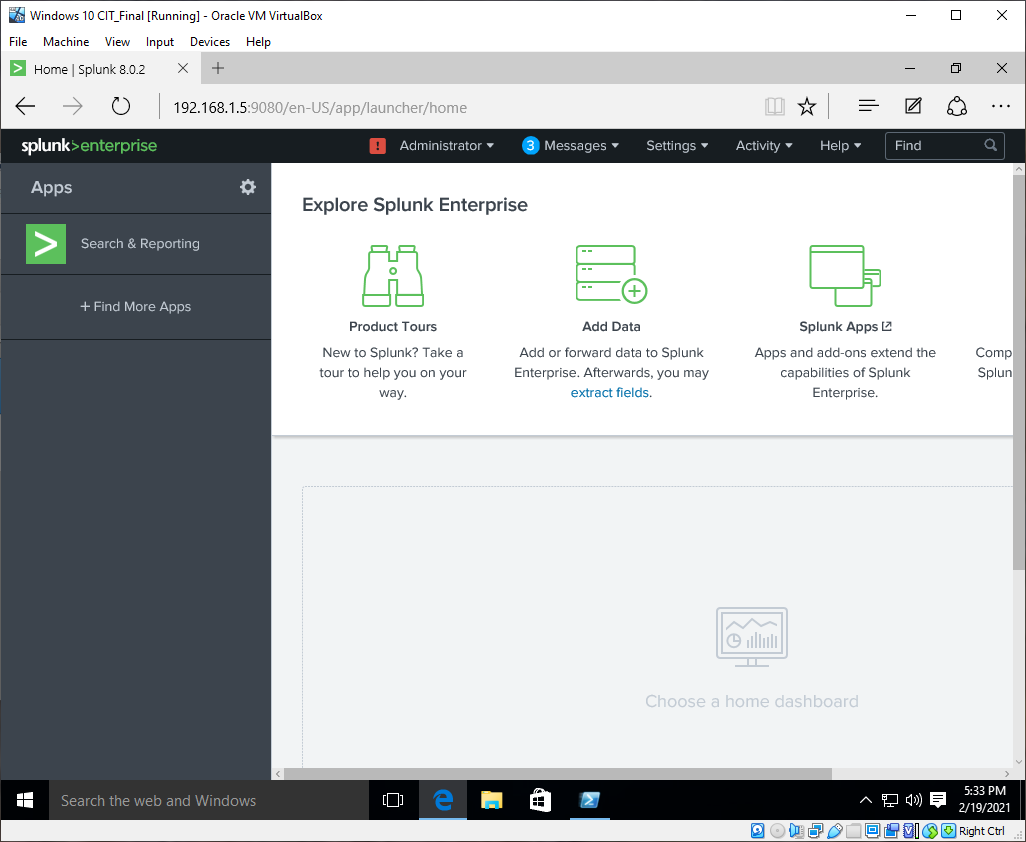
**Scenario:** An organization’s monitoring system identified suspicious download activities captured in a honeypot that was named Cowrie. The event was recorded by the Splunk system, but the system cannot be accessed because its operator, who was the head of the security investigation team, was recently released from the company. Due to the recent events, there was not enough time to provide the information required to access the system freely. However, the system administrator was able to provide access to the mail server and stated that all the data needed to access the system is stored on that server. This project’s objective is to connect to the Splunk system, investigate the events, and identify a suspicious message to obtain the *flag*.

**Environment Setup:**

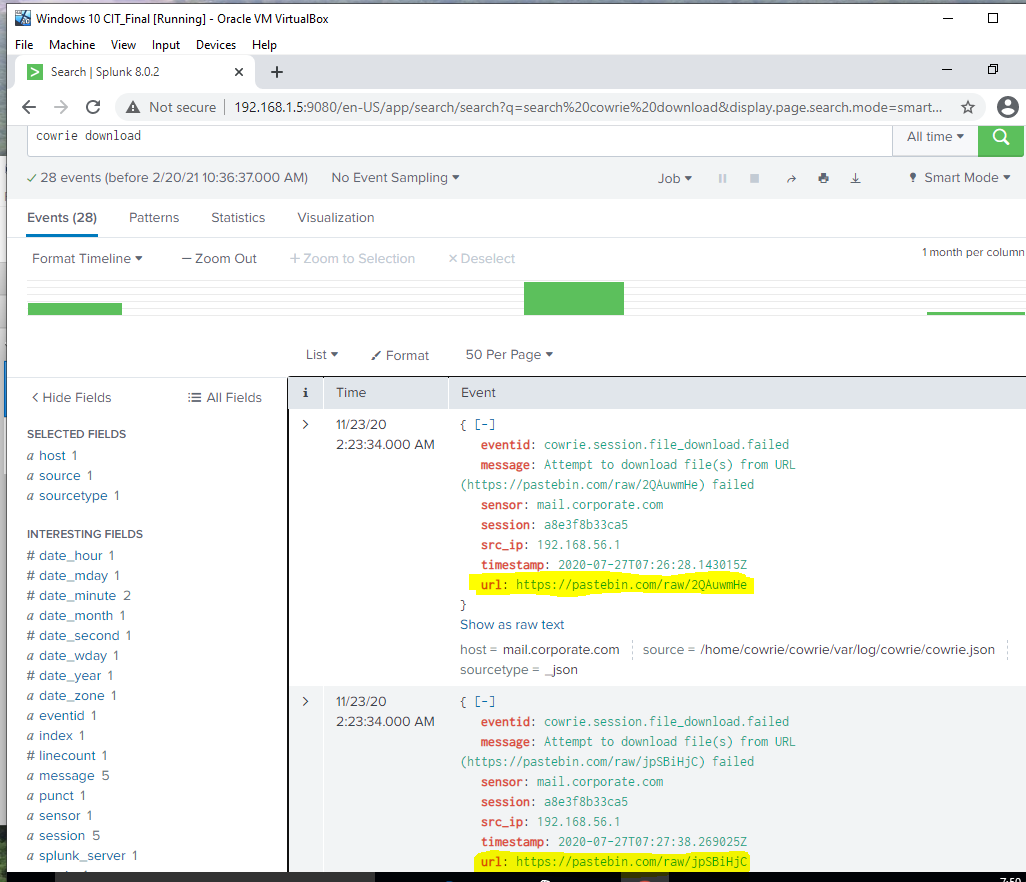
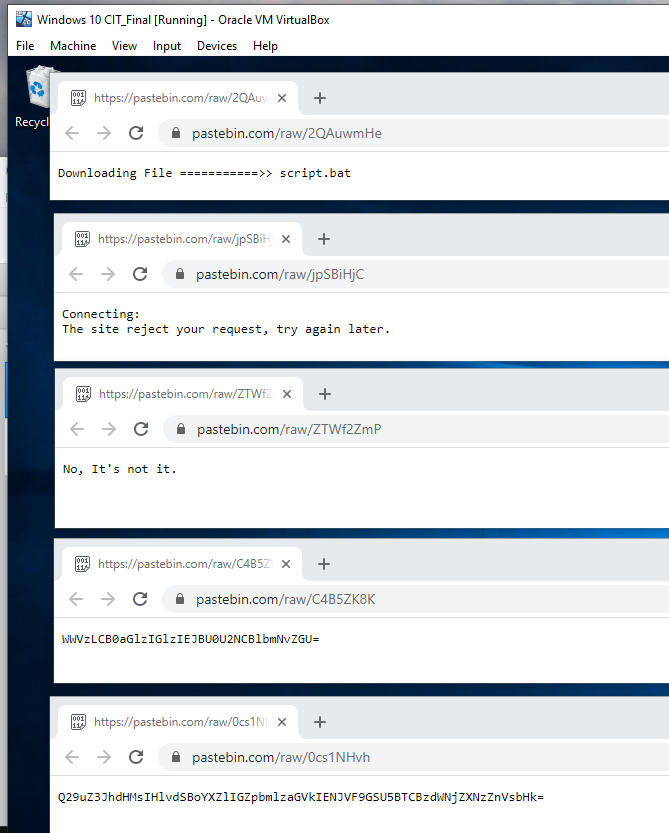
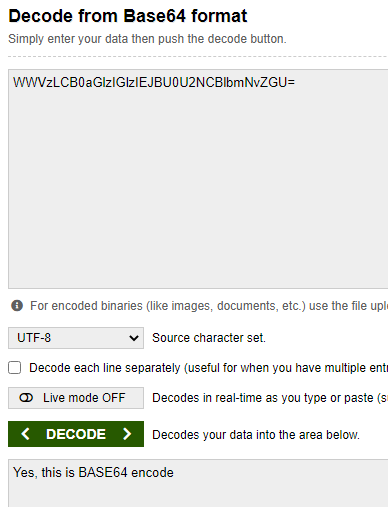
1. Two virtual machines were imported into VirtualBox: a Windows system and an Ubuntu system.
2. The NAT network for both virtual machines was configured to use the 192.168.1.0/24 subnet.
3. Both virtual machines were configured with a NAT adapter on the previously-setup subnet.
4. Both virtual machines were started, and the IP address of the Ubuntu system was noted. Ping was used from the Windows system to verify that both machines can communicate.

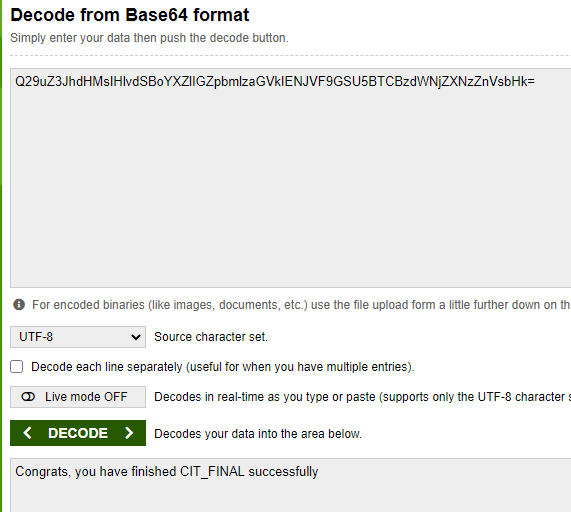
**Task 1: Connect to the Mail Server**  
*Objective: Connect to the mail server and retrieve the relevant emails.*

1. Upon startup, the Ubuntu VM prompts that the POP3 port is open, and provides the login credentials.
2. POP3 uses port 110 by default.
3. From the Windows system, I was initially unable to use PowerShell to connect to the POP3 service via Telnet because the feature was not installed within Windows.
4. The Telnet client was installed onto the Windows system.
5. A Telnet connection was successfully established onto the mail server, and login was successful using the information provided in the message from step 1.
6. The existing emails were listed and investigated, in order to search for interesting information.  
     
   The credentials for the Splunk application were found in message 4.
7. The provided URL and credentials were used to successfully log into the Splunk system.



**Lab Task 2: Search for Suspicious Activity**  
*Objective: Search the SIEM for recorded suspicious activity in the organization.*

1. In Splunk, a search with the query cowrie download was made to find records of the suspicious activity. Returned events show several failed download attempts from various PasteBin URLs. There were 28 total events, and, amongst those, downloads were attempted from 5 different sources (all on PasteBin).
2. The five PasteBin URLs were accessed for further investigation. Three of them appeared to contain irrelevant information, and the other two contained text that seemed to be either encoded or hashed.
3. I first tried to run the two “interesting” texts through reverse hashing tools, but the strings were not the correct length for any known hashing algorithm. I then assumed that the messages were encoded and not hashed (which would make more sense in this scenario, since the messages/“flags” were meant to be decoded and hashing is generally one-way), and ran the strings through a Base64 decoder. The first string (ending in “ZGU”) decoded to say “Yes, this is BASE64 encode,” verifying the correct encoding algorithm, and the second string proved to be the flag for this project, decoding to “Congrats, you have finished CIT\_FINAL successfully.”



**Flag:** Q29uZ3JhdHMsIHlvdSBoYXZlIGZpbmlzaGVkIENJVF9GSU5BTCBzdWNjZXNzZnVsbHk=