Project One

Gerrell Bones
24th OCT 2023
Project 1
CNT 4403

Required Challenges (Required)

> **Item #1:** The bad apple's IP address:

TODO: 192.168.1.4

> **Item #2:** The subject lines of three different phishing emails:

1. **TODO: C: RCPT TO: <xxxxxx@xxxxx.co.uk>**
2. **TODO: from: "Xxxxxx xxxx" <xxxxxx@xxxxx.co.uk>, subject: Testing testing 1 2 3 (Multiple attachments), (text/plain)**
3. **TODO: C: MAIL FROM: <xxxxxx@xxxxx.co.uk>**

> **Item #3:** An explanation of how you went about finding the bad apple from just the .pcap files: (Please be specific about what filters/searches you used!)

TODO: I followed the path of the content inside of the file, the IP was used throughout the attack. You can trace back to when it signed in and began sending the emails to it sending the email to receive data from the user at the very end.