CYBERATTACKS LABS

Task 1

Perform an email header analysis. You will be given an email. The task will be to identify the various headers and body of the email and determine if the email is a genuine email or a phishing email

- Phishing Assignment Outcome- An excel sheet named after the email subject, which contains IOCs and possible screenshots of:
- IP addresses (origin)
- IP addresses (CnC)
- Subject Line
- Domains Embedded
- Attachments and their type
- Dropper Files (% temp)
- Fake Sender name
- Original Sender Email address
- Associated Hashes

Please use outlook and windows VM-
https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/
(please ask for outlook client download link)

Task 2

Perform malware analysis. You will be given a piece of malware for investigate. The task will be to analyze the piece of malware and prepare a report accordingly. Please feel free to choose any malware report template from the internet. Check for the good ones like Mandiant, Threat Intel and Kroll as few examples

Download files:

https://drive.google.com/drive/folders/1rsLD08fFWJ-hRnEIRNmPdk5oughHVqvm?usp=sharing

[Password : infected]

Task 3 (Optional to attempt)

The Cyberkill chain is one of the important concepts designed to help security professionals to understand the various stages of an attack. Read about the various stages here and prepare a small report from your understanding, 200-300 words report. You can even pick any recent attacks and try to evaluate.