Social Engineering Write-Up

Name: ZAHIDAH AZ-ZAHRA BINTI SAFARIZAM

ID: 52215226218

Platform: TryHackMe

Exercise: Phishing Analysis Fundamentals

1. Objective
   To identify the components involved in sending an email and to understand how to analyze email headers.

2. Tools/Platform Used
   - TryHackMe
   - CyberChef
   - Base64.Guru

3. Steps Taken
   1. Identified the email headers and email body.
   2. Analyzed key email header fields such as From, Subject, Date, and To.
   3. Viewed the raw email content to examine detailed header information.
   4. Identified suspicious elements within the email details.
   5. Analyzed the email body for attachments and content types.
   6. Interacted with attachments by decoding files and defanging URLs.

4. Findings/What I learned
   - Learned how to view the raw source of an email, including the header and body.
   - Understood the importance of analyzing email content for attachments, encoded data, and other suspicious elements.
   - Gained a better understanding of the relationship between the email sender and recipient information.

5. Conclusion
   This exercise strengthened my understanding of email structure and phishing analysis techniques. It showed how attackers can also manipulate email elements and emphasized the need to analyse email headers, email content and email attachments attentively to identify phishing attacks.

6. Evidence
7.

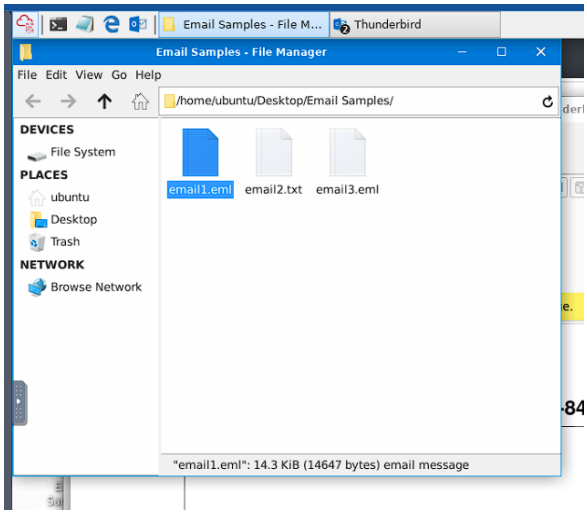

Figure 1: Types of email

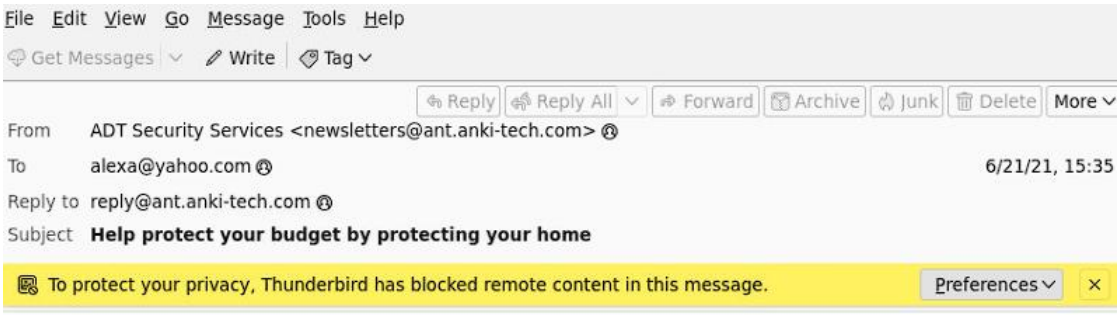

Figure 2: email1.eml

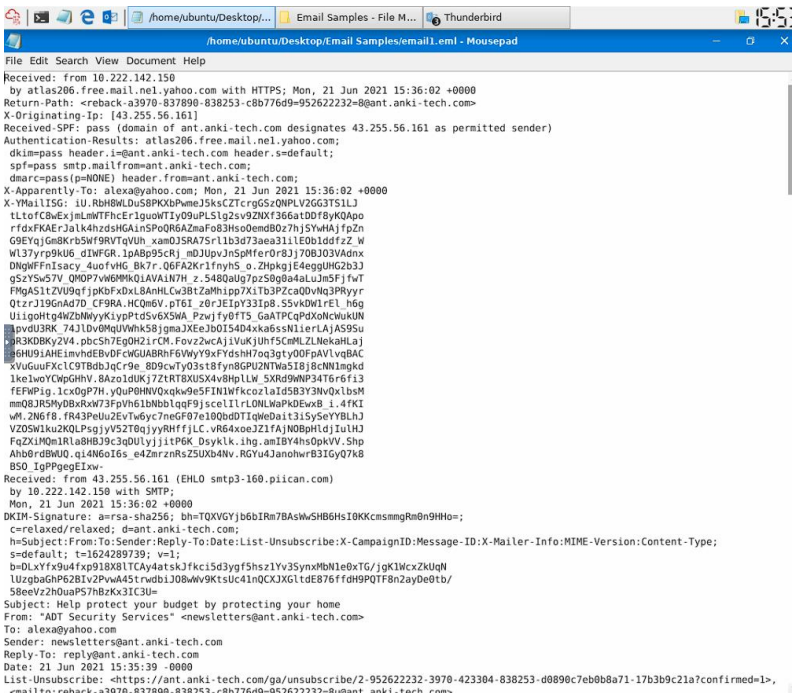

Figure 3: email1.eml raw details

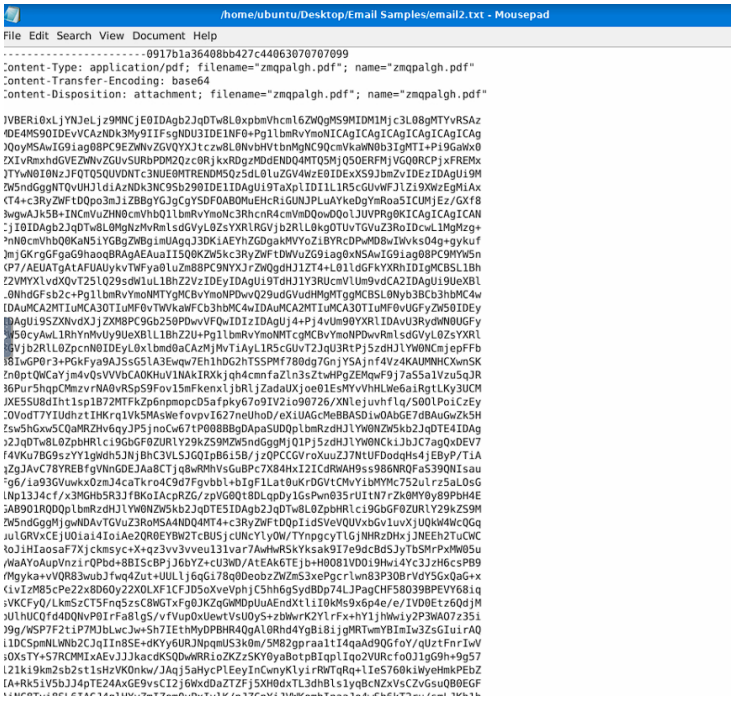

Figure 4: email2.eml

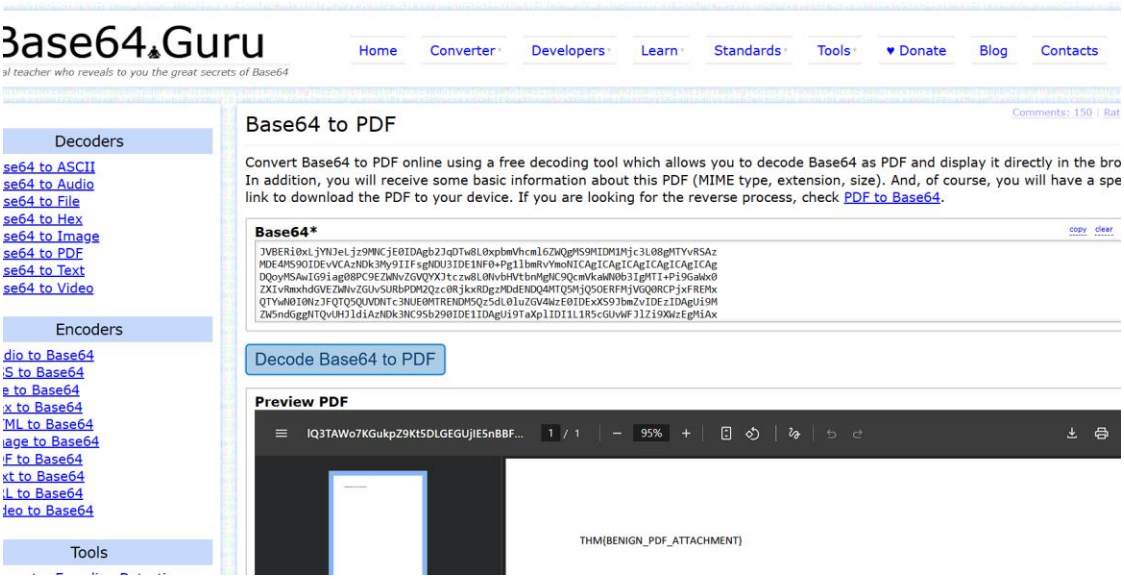

Figure 5: Decode email2.eml .pdf content-type

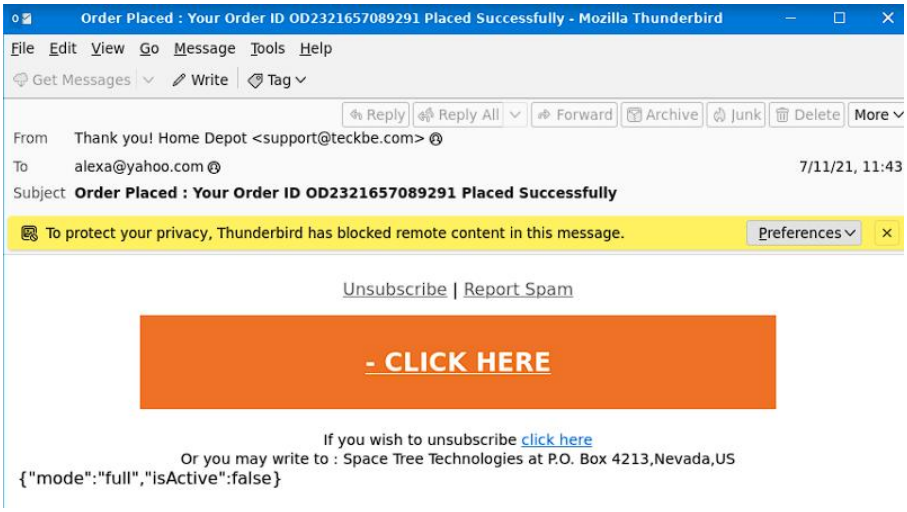

Figure 6: email3.eml

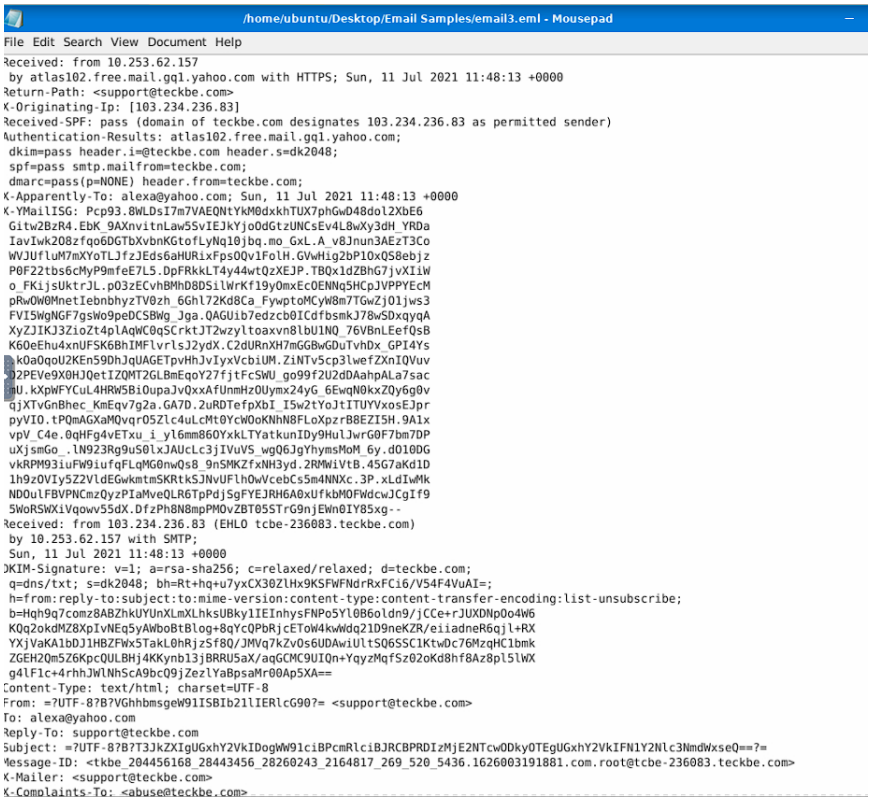

Figure 7: email3.eml raw details

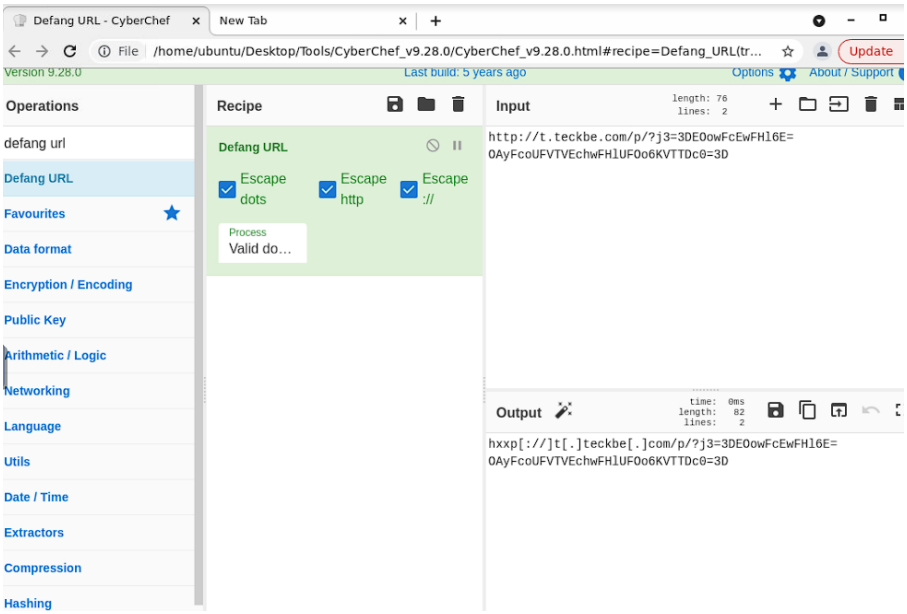

Figure 8: Defang URL for email3.eml

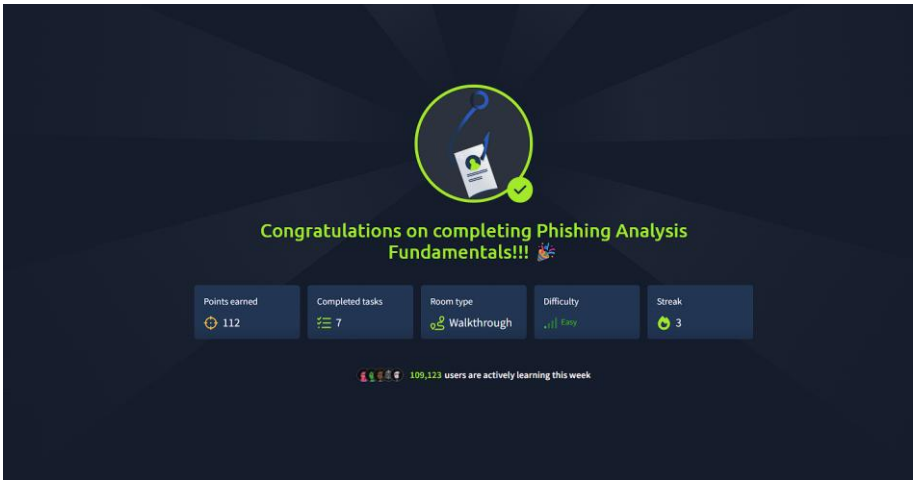

Figure 9: Complete Task