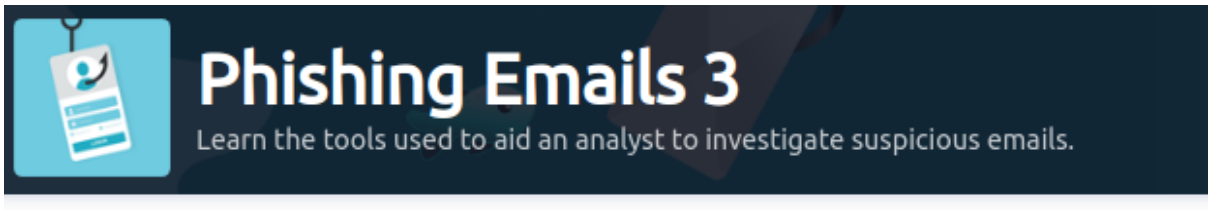
TRY HACK ME: Phishing Emails 3 Write-Up



Task 1 Introduction-

We will look at various tools that will aid us in analyzing phishing emails. We will:

1. Look at tools that will aid us in examining email header information.
2. Cover techniques to obtain hyperlinks in emails, expand the URLs if they're URL shortened.
3. Look into tools to give us information about potentially malicious links without directly interacting with a malicious link.
4. Cover techniques to obtain malicious attachments from phishing emails and use malware sandboxes to detonate the attachments to understand further what the attachment was designed to do.

Warning: The samples throughout this room contain information from actual spam and/or phishing emails. Proceed with caution if you attempt to interact with any IP, domain, attachment, etc.

Answer to the questions of this section-

No Answer needed

Task 2 What information should we collect?-

Below is a checklist of the pertinent information an analyst (you) is to collect from the email header:

1. Sender email address
2. Sender IP address
3. Reverse lookup of the sender IP address
4. Email subject line
5. Recipient email address (this information might be in the CC/BCC field)
6. Reply-to email address (if any)
7. Date/time

Afterward, we draw our attention to the email body and attachment(s) (if any).

Below is a checklist of the artifacts an analyst (you) needs to collect from the email body:

1. Any URL links (if an URL shortener service was used, then we'll need to obtain the real URL link)
2. The name of the attachment
3. The hash value of the attachment (hash type MD5 or SHA256, preferably the latter)

Warning: Be careful not to click on any links or attachments in the email accidentally.

Answer to the questions of this section-

No Answer needed

Task 3 Email header analysis –

Usage: Copy and paste the entire email header and run the analysis tool.

Messageheader: https://toolbox.googleapps.com/apps/messageheader/analyzeheader

Another tool is called **Message Header Analyzer.**

Message Header Analyzer: https://mha.azurewebsites.net/

you can also use https://mailheader.org/

Even though not covered in the previous Phishing rooms, a Message Transfer Agent (MTA) is software that transfers emails between sender and recipient. Read more about MTAs here. Since we're on the subject, read about MUAs (Mail User Agent) here.

Note: The option on which tool to use rests ultimately on you. It is good to have multiple resources to refer to as each tool might reveal information that another tool may not reveal.

The tools below can help you analyze information about the sender's IP address:

IPinfo.io: https://ipinfo.io/

URLScan.io: https://urlscan.io/

You can use other tools that provide the same functionality and more, such as URL2PNG and Wannabrowser.

Talos Reputation Center: https://talosintelligence.com/reputation

Answer to the questions of this section-

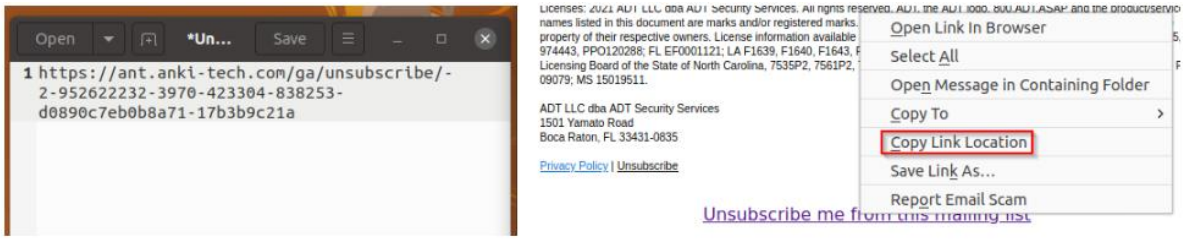
capticalone.com

Task 4 Email body analysis –

Now it's time to direct your focus to the email body. This is where the malicious payload may be delivered to the recipient either as a link or an attachment.

Links can be extracted manually, either directly from an HTML formatted email or by sifting through the raw email header.

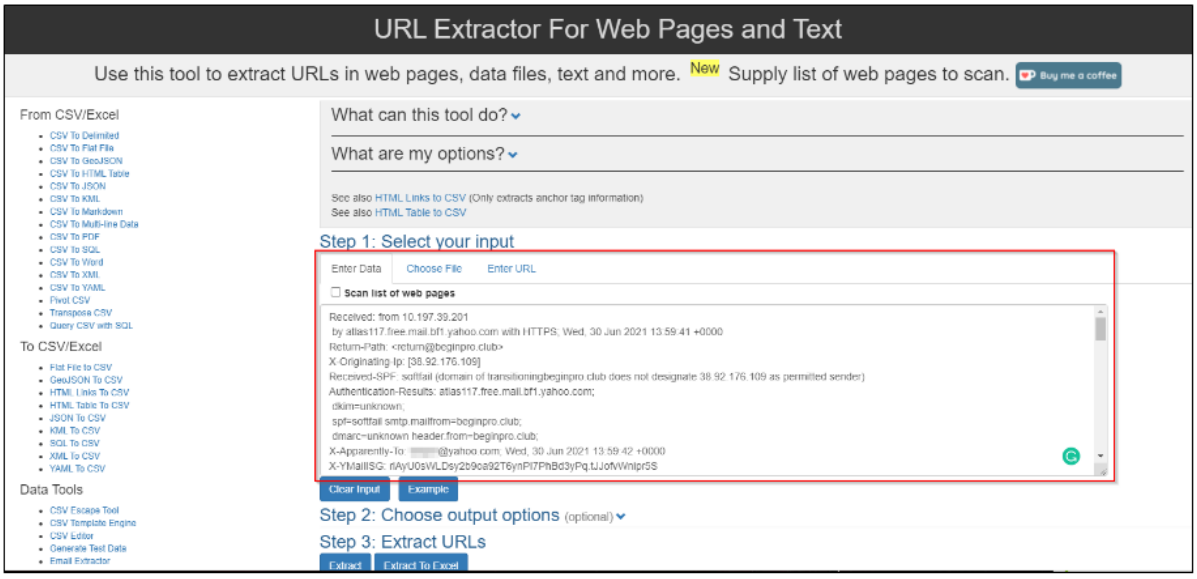
Below is an example of obtaining a link manually from an email by right-clicking the link and choosing Copy Link Location.



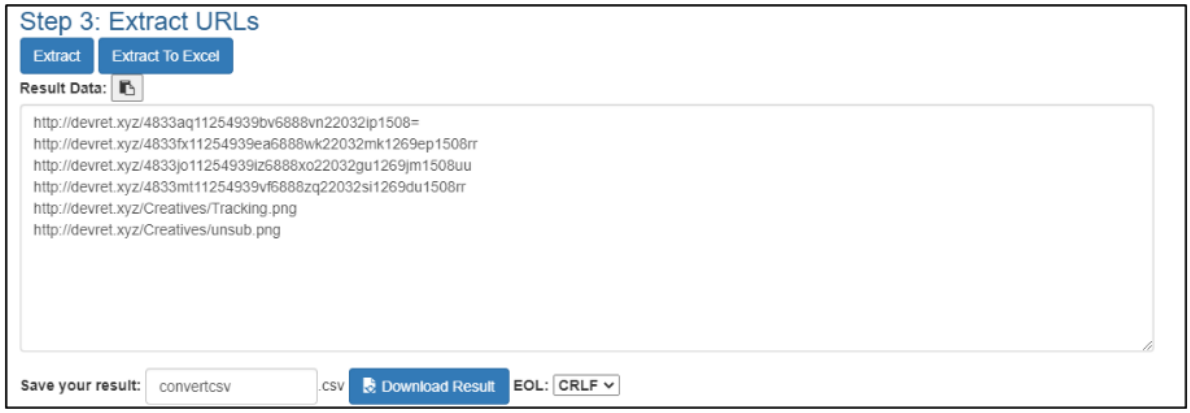
The same can be accomplished with the assistance of a tool. One tool that can aid us with this task is URL Extractor.

URL Extractor: https://www.convertcsv.com/url-extractor.htm

You can copy and paste the raw header into the text box for **Step 1: Select your input**.



The extracted URLs are visible in Step 3.



You may also use **CyberChef** to extract URLs with the Extract URLs recipe.

It's important to note the root domain for the extracted URLs. You will need to perform an analysis on the root domain as well.

After extracting the URLs, the next step is to check the reputation of the URLs and root domain. You can use any of the tools mentioned in the previous task to aid you with this.

If the email has an attachment, you'll need to obtain the attachment safely. Accomplishing this is easy in Thunderbird by using the Save button.

After you have obtained the attachment, you can then get its hash. You can check the file's reputation with the hash to see if it's a known malicious document.

Obtain the file's **SHA256 hash**

user@machine$ sha256sum Double\ Jackpot\ Slots\ Las\ Vegas.dot

c650f397a9193db6a2e1a273577d8d84c5668d03c06ba99b17e4f6617af4ee83 Double Jackpot Slots Las Vegas.dot

There are many tools available to help us with this, but we'll focus on two primarily; they are listed below:

Talos File Reputation: https://talosintelligence.com/talos_file_reputation

VirusTotal - https://www.virustotal.com/gui/home/upload

Another tool/company worth mentioning is https://www.reversinglabs.com/ , which also has a file reputation service.

Answer to the questions of this section-

Copy Link Location

Task 5 Malware Sandbox –

Luckily as Defenders, we don't need to have malware analysis skills to dissect and reverse engineer a malicious attachment to understand the malware better.

There are online tools and services where malicious files can be uploaded and analyzed to better understand what the malware was programmed to do. These services are known as malware sandboxes.

For instance, we can upload an attachment we obtained from a potentially malicious email and see what URLs it attempts to communicate with, what additional payloads are downloaded to the endpoint, persistence mechanisms, Indicators of Compromise (IOCs), etc.

Some of these online malware sandboxes are listed below.

Any.Run: https://app.any.run/

Hybrid Analysis: https://www.hybrid-analysis.com/

Joe Security - https://www.joesecurity.org/

Answer to the questions of this section-

No Answer needed

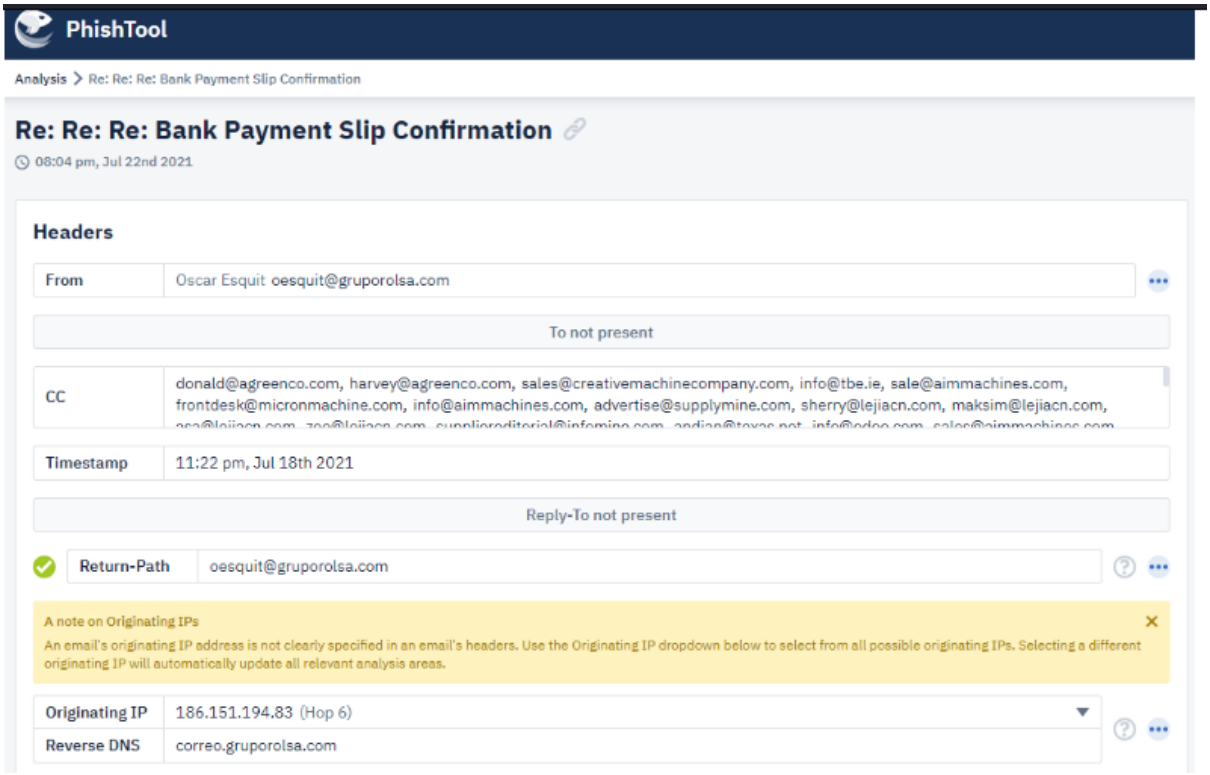
Task 6 PhishTool –

A tool that will help with automated phishing analysis is PhishTool - https://www.phishtool.com/

Note: There is a free community edition you can download and use. :)

I uploaded a malicious email to PhishTool and connected VirusTotal to my account using my community edition API key.

Below are a few screenshots of the malicious email and the PhishTool interface.



From the image above, you can see the PhishTool conveniently grabs all the pertinent information we'll need regarding the email.

1. Email sender
2. Email recipient (in this case, a long list of CCed email addresses)
3. Timestamp
4. Originating IP and Reverse DNS lookup

We can obtain information about the SMTP relays, specific X-header information, and IP info information.

Answer to the questions of this section-

Look at the Strings output. What is the name of the EXE file?

#454326_PDF.exe | Correct Answer

Task 7 Phishing Case 1 –

Scenario: You are a Level 1 SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email for your team to implement the appropriate rules to prevent colleagues from receiving additional spam/phishing emails.

Task: Use the tools discussed throughout this room (or use your own resources) to help you analyze each email header and email body.

Answer to the questions of this section-

What brand was this email tailored to impersonate?

Netflix | Correct Answer

What is the From email address?

N e t f l i x <JGQ47wazXe1xYVBrkeDg-JOg7ODDQwWdR@JOg7ODDQ | Correct Answer

What is the originating IP? Defang the IP address.

209[.]85[.]167[.]226 | Correct Answer | Hint

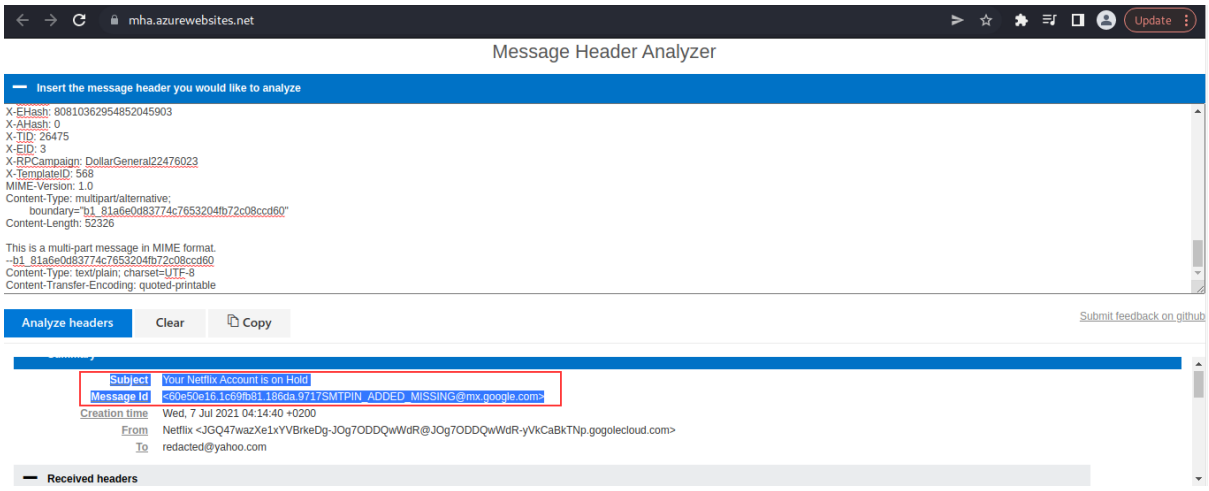
From what you can gather, what do you think will be a domain of interest? Defang the domain.

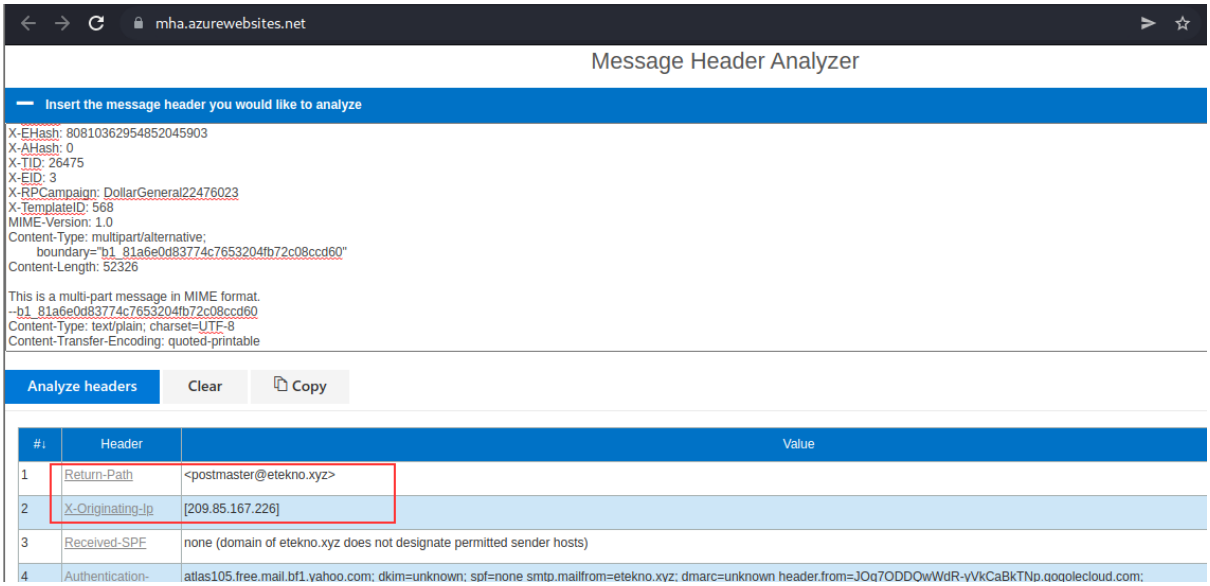
etekno[.]xyz | Correct Answer | Hint

What is the shortened URL? Defang the URL.

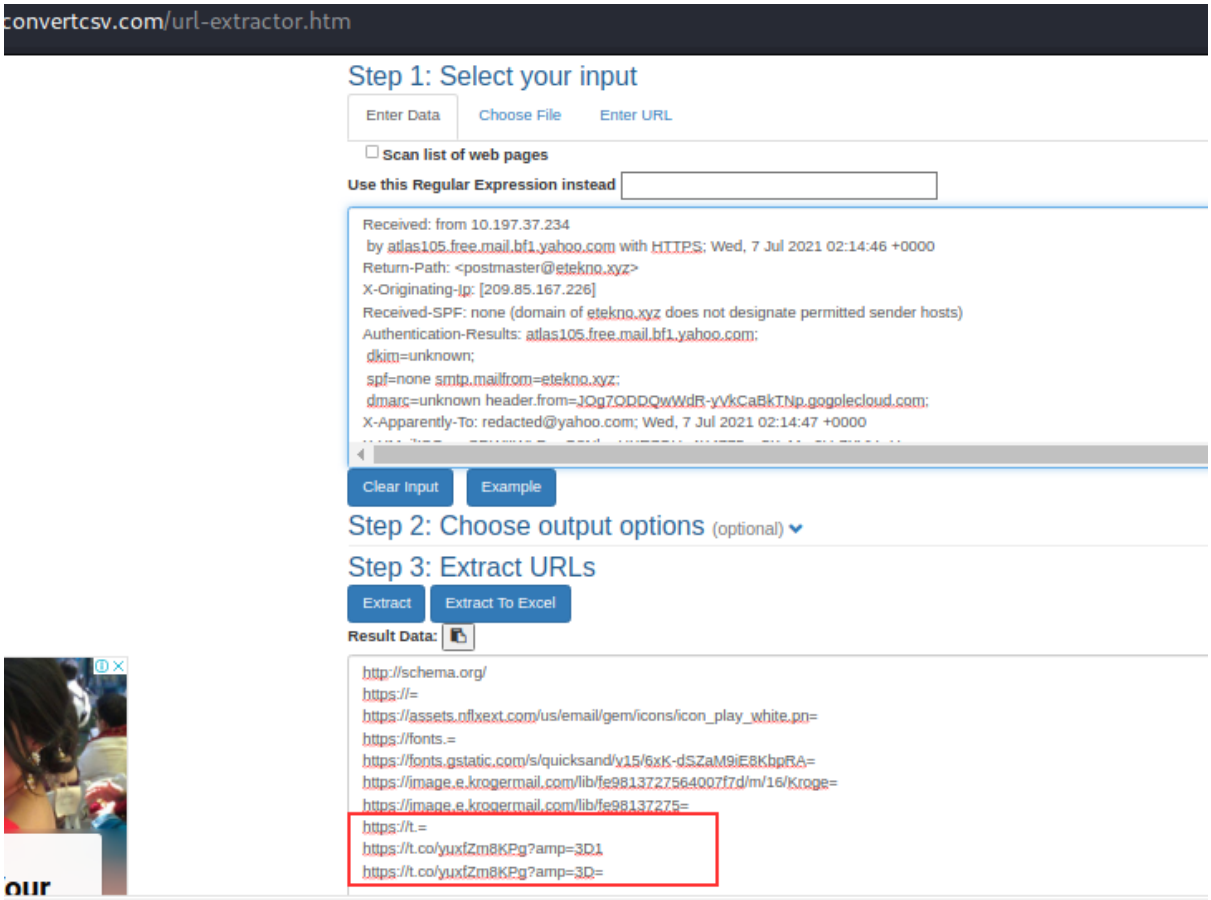
hxxps[://]t[.]co/yuxfZm8KPg?amp==1 | Correct Answer | Hint

For Email Header Analysis is used- https://mha.azurewebsites.net/





For Email Body Analysis I used- https://www.convertcsv.com/url-extractor.htm



Task 8 Phishing Case 2 –

Scenario: You are a Level 1 SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email for your team to implement the appropriate rules to prevent colleagues from receiving additional spam/phishing emails.

A malicious attachment from a phishing email inspected in the previous Phishing Room was uploaded to Any Run for analysis.

Task: Investigate the analysis and answer the questions below.

Link: https://app.any.run/tasks/8bfd4c58-ec0d-4371-bfeb-52a334b69f59

Answer to the questions of this section-

All the answers can be found from here -

https://any.run/report/cc6f1a04b10bcb168aeec8d870b97bd7c20fc161e8310b5bce1af8ed420e2c24/8bfd4c58-ec0d-4371-bfeb-52a334b69f59?_gl=1*3nm857*_ga*Mjc2ODg2NDM1LjE2NjI4ODQ1MzQ.*_ga_53KB74YDZR*MTY2Mjg4NDUzNC4xLjEuMTY2Mjg4NDkwOC4zNS4wLjA.&_ga=2.250087872.752651539.1662884534-276886435.1662884534

Task 9 Phishing Case 3 –

Scenario: You are a Level 1 SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email for your team to implement the appropriate rules to prevent colleagues from receiving additional spam/phishing emails.

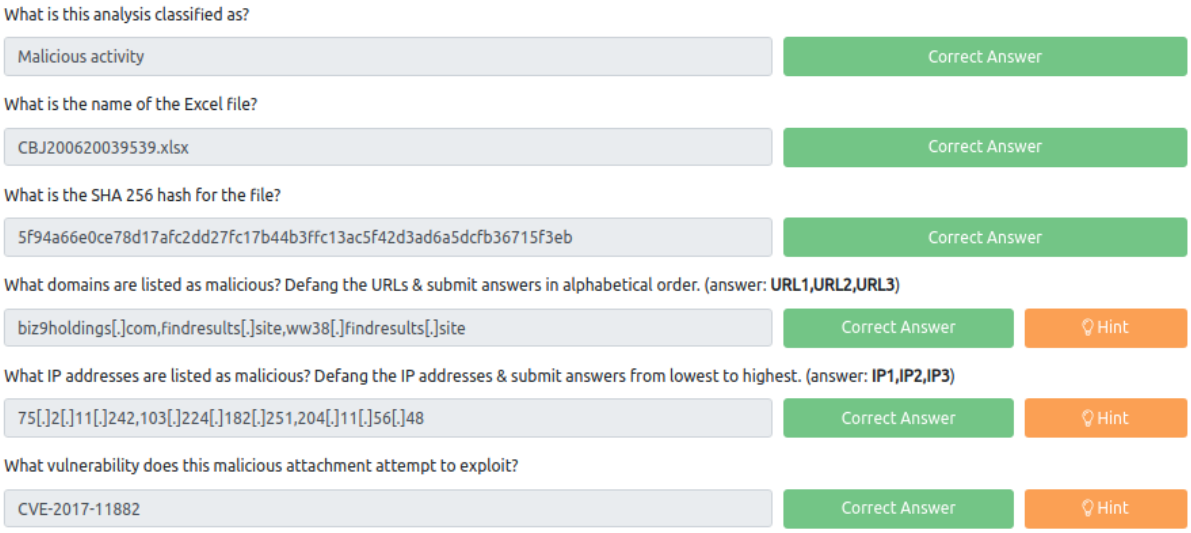
A malicious attachment from a phishing email inspected in the previous Phishing Room was uploaded to Any Run for analysis.

Task: Investigate the analysis and answer the questions below.

Link: https://app.any.run/tasks/82d8adc9-38a0-4f0e-a160-48a5e09a6e83

Answer to the questions of this section-

All the answers can be found from here - https://any.run/report/5f94a66e0ce78d17afc2dd27fc17b44b3ffc13ac5f42d3ad6a5dcfb36715f3eb/82d8adc9-38a0-4f0e-a160-48a5e09a6e83?_gl=1*7s6t7g*_ga*Mjc2ODg2NDM1LjE2NjI4ODQ1MzQ.*_ga_53KB74YDZR*MTY2Mjg4NDUzNC4xLjAuMTY2Mjg4NDU0OC40Ni4wLjA.&_ga=2.6843892.752651539.1662884534-276886435.1662884534



That is all for this Write-up, hoping this will help you in solving the challenges of Phishing Emails 3. Have Fun and Enjoy Hacking! Do visit other rooms and modules on TryHackMe for more learning.

-by Shefali Kumai

For more cyber security learning follow me here-

https://github.com/ctf-time

https://www.youtube.com/channel/UCf-F-eATCUXYaUVk8Xl7OOQ

https://www.instagram.com/cybersecurity.cyber_seek/

https://twitter.com/Shefali37920461