Following is a list of tasks to choose from:

A-- Write a program in a programming language of your choice (preferably in python) to sniff DNS traffic (live capture) and process it to dig out and save the following output to a file whenever an NXdomain packet is found
1- Response Code
2- The query
3- Authoritative name server
4- Transport protocol used and dst port
5- Find if the request is malicious
Also, explain the working of your code and how NXdomain hijacking works.
Output: *Working code, Demonstration*

B-- Analyze the provided pcap(s) and identify the attack type (if any) along with mitigation as per the analysis report template (attached as a separate file):
Output: *Analysis Report as per the given template, Demonstration*

C-- Setup DVWA on an Amazon EC2 instance using Amazon RDS for your database and:
1- Make the EC2 instance accessible only on port 80 and 22
2- Exploit all the 4 levels of at least 1 vulnerability
Output: *Pentest Report, Demonstration*