Initial Pen Testing

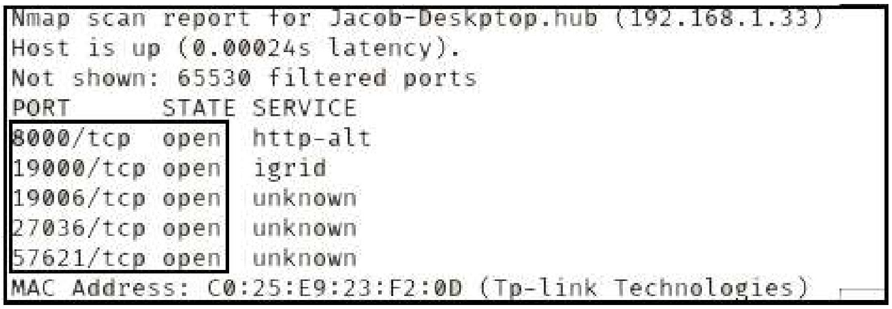
This is the initial pen testing. IP address was 192.168.1.33 during testing when running the server.

There is minimal security leaks with the initial testing done on the server with some basic scans. More scanning is needed to test if it is possible to bypass security measures already in place. Current security level is good.

Open Ports on IP Address

nmap -T4 -p- 192.168.1.33

The above command was used to determine all the open ports found on that IP address. The open ports found were *'8000, 19000,19006, 27063, 57621'*. To find more vulnerabilities on these open ports, more scans need to be done.

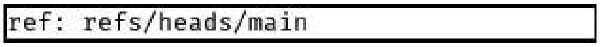


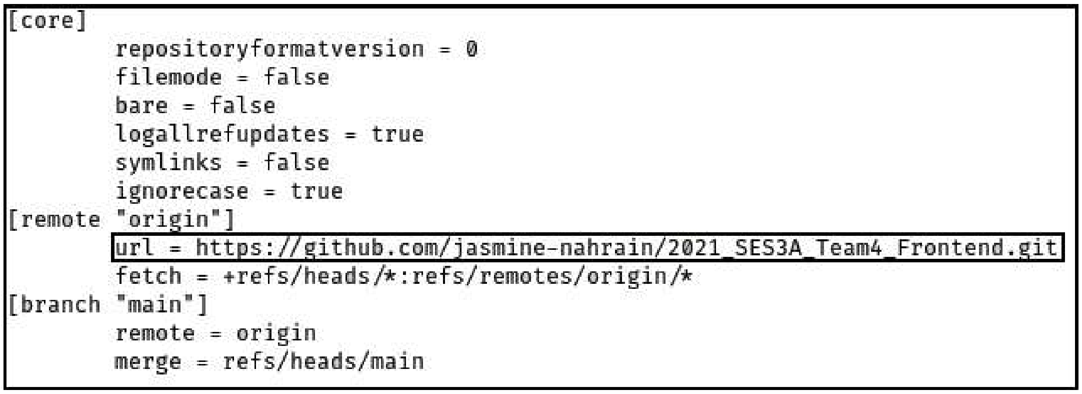
```
Nmap scan report for Jacob-Deskptop.hub (192.168.1.33)
Host is up (0.00024s latency).
Not shown: 65530 filtered ports
PORT      STATE SERVICE
8000/tcp  open  http-alt
19000/tcp open  igrid
19006/tcp open  unknown
27036/tcp open  unknown
57621/tcp open  unknown
MAC Address: C0:25:E9:23:F2:0D (Tp-link Technologies)
```

Files Found

nikto -h 192.168.1.33:19000

Through the above command there were two files found on the port *19000* and are displayed below

- http://192.168.1.33:19000/.git/head
  - 

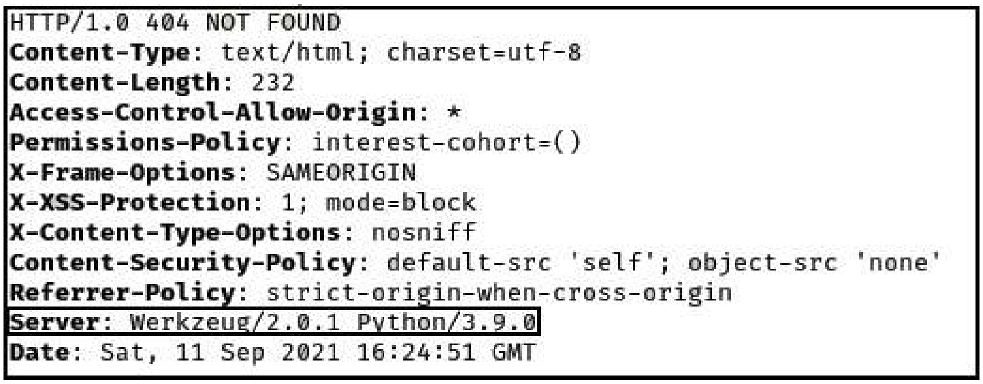
    ```
    ref: refs/heads/main
    ```
  - This file has a potential to show full repo details, however this is all that was found and is not currently an issue.
- http://192.168.1.33:19000/.git/config
  - 

    ```
    [core]
            repositoryformatversion = 0
            filemode = false
            bare = false
            logallrefupdates = true
            symlinks = false
            ignorecase = true
    [remote "origin"]
            url = https://github.com/jasmine-nahrain/2021_SES3A_Team4_Frontend.git
            fetch = +refs/heads/*:refs/remotes/origin/*
    [branch "main"]
            remote = origin
            merge = refs/heads/main
    ```
  - This file has a potential to show details about the repository. Highlighted is a possible issue where the git URL is shown. Securing the URL with authentication will help secure this as well as trying to avoid leaking the URL.

Server Information

curl --head http://192.168.1.33:8000

Using the above command, server information was revealed. This command also can reveal other possible security leaks. Due to the server being up to date there is little risk of exploits being found.



```
HTTP/1.0 404 NOT FOUND
Content-Type: text/html; charset=utf-8
Content-Length: 232
Access-Control-Allow-Origin: *
Permissions-Policy: interest-cohort=()
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; object-src 'none'
Referrer-Policy: strict-origin-when-cross-origin
Server: Werkzeug/2.0.1 Python/3.9.0
Date: Sat, 11 Sep 2021 16:24:51 GMT
```