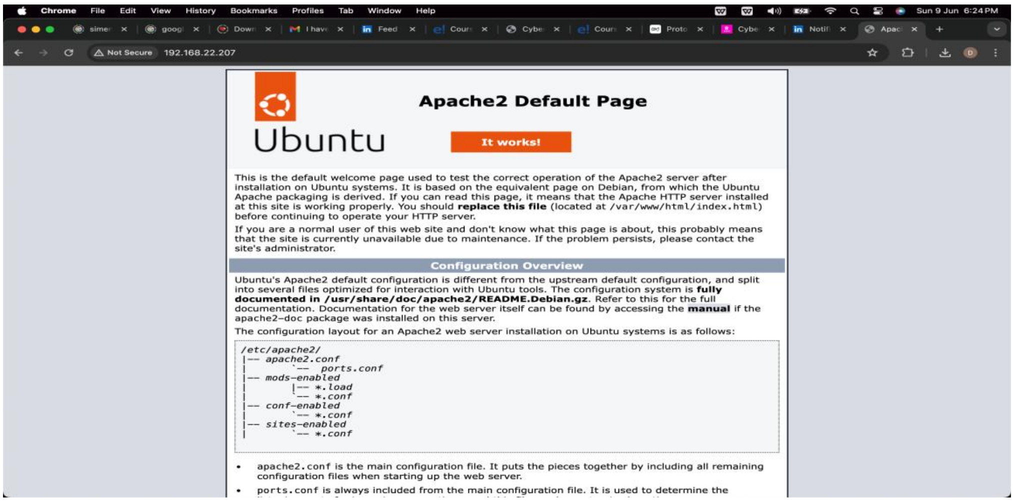
CyberSecurity and Ethical Hacking Certification Project.

Ethically Hacking an E-Commerce Website

Connecting to the javascipt additional requirement and starting the virtual machine and entering into indel page.



Apache2 Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

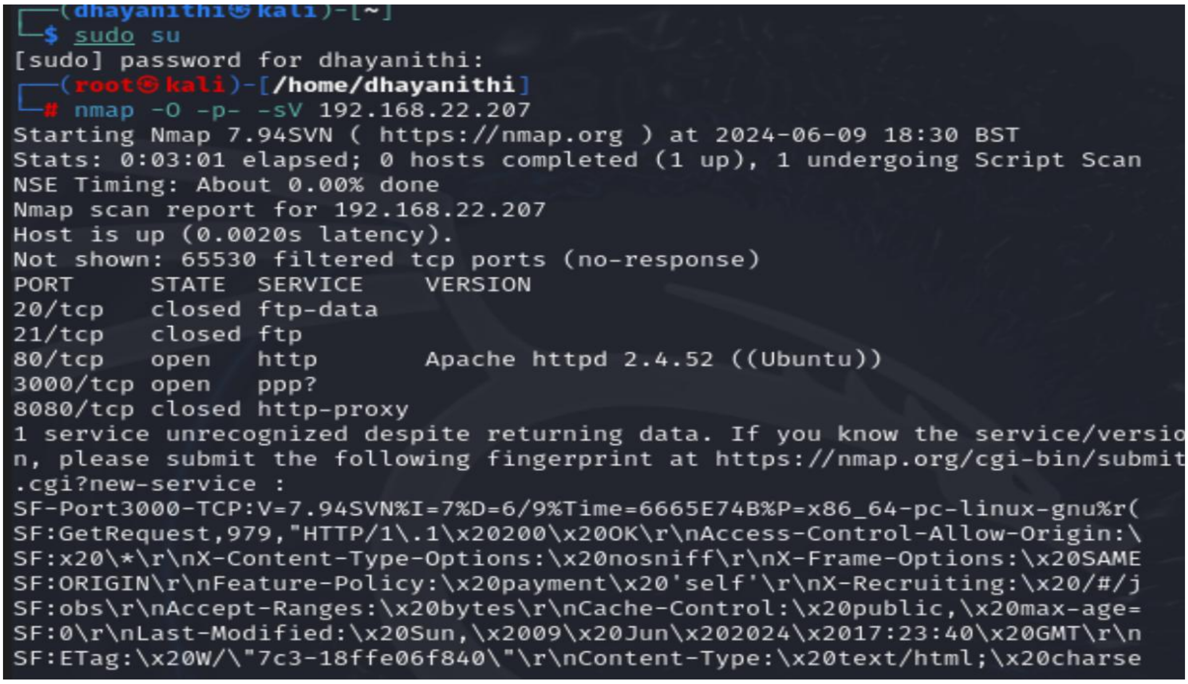
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the

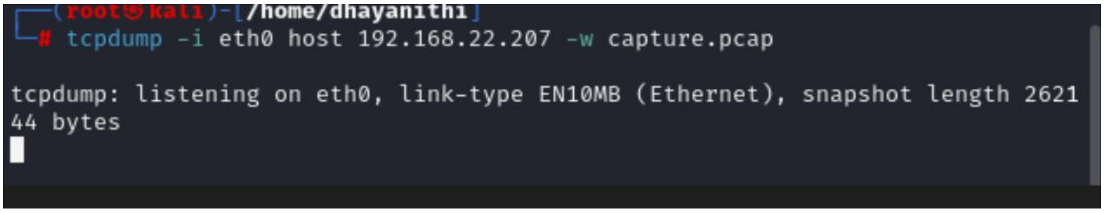
Then starting the Kali linux and scan the network using nmap.

nmap -O -p -sV 192.168.22.207



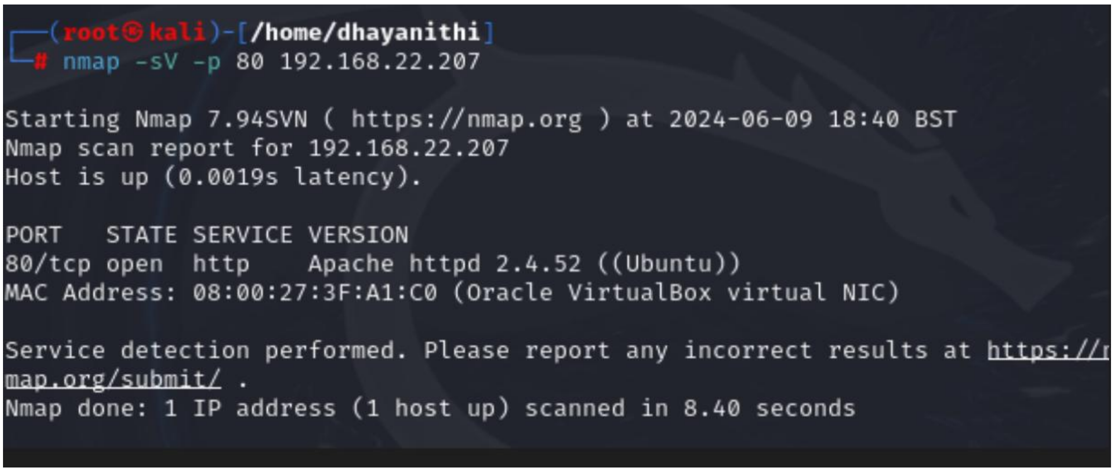
```
┌──(dhayanithi㉿kali)-[~]
└─$ sudo su
[sudo] password for dhayanithi:
┌──(root㉿kali)-[/home/dhayanithi]
└─# nmap -O -p- -sV 192.168.22.207
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-09 18:30 BST
Stats: 0:03:01 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for 192.168.22.207
Host is up (0.0020s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT     STATE  SERVICE    VERSION
20/tcp   closed ftp-data
21/tcp   closed ftp
80/tcp   open   http       Apache httpd 2.4.52 ((Ubuntu))
3000/tcp open   ppp?
8080/tcp closed http-proxy
1 service unrecognized despite returning data. If you know the service/versio
n, please submit the following fingerprint at https://nmap.org/cgi-bin/submit
.cgi?new-service :
SF-Port3000-TCP:V=7.94SVN%I=7%D=6/9%Time=6665E74B%P=x86_64-pc-linux-gnu%r(
SF:GetRequest,979,"HTTP/1\.1\x20200\x20OK\r\nAccess-Control-Allow-Origin:\
SF:x20\*\r\nX-Content-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20SAME
SF:ORIGIN\r\nFeature-Policy:\x20payment\x20'self'\r\nX-Recruiting:\x20/#/j
SF:obs\r\nAccept-Ranges:\x20bytes\r\nCache-Control:\x20public,\x20max-age=
SF:0\r\nLast-Modified:\x20Sun,\x2009\x20Jun\x202024\x2017:23:40\x20GMT\r\n
SF:ETag:\x20W/\"7c3-18ffe06f840\"\r\nContent-Type:\x20text/html;\x20charse
```

To capture the packets used tcp dump.



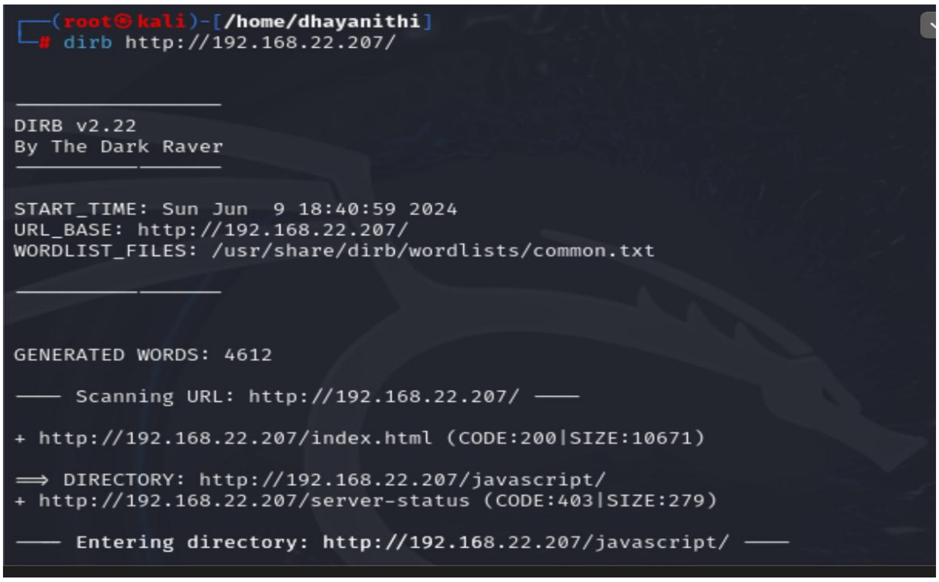
```
┌──(root㉿kali)-[/home/dhayanithi]
└─# tcpdump -i eth0 host 192.168.22.207 -w capture.pcap

tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 2621
44 bytes
█
```

Found the port 80 is open so scanned the port 80 to gather more info



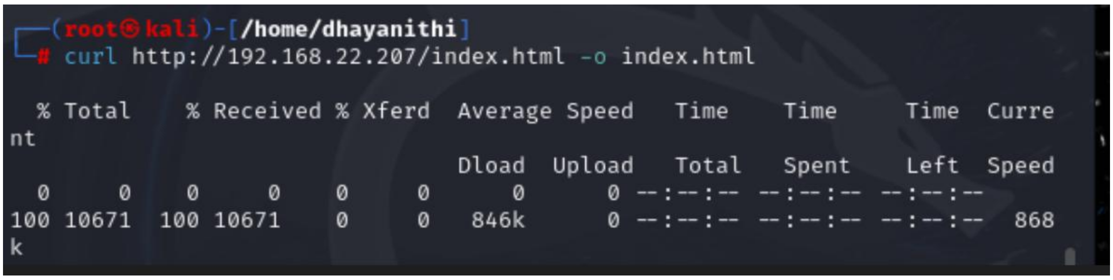
```
┌──(root㉿kali)-[/home/dhayanithi]
└─# nmap -sV -p 80 192.168.22.207

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-09 18:40 BST
Nmap scan report for 192.168.22.207
Host is up (0.0019s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
MAC Address: 08:00:27:3F:A1:C0 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.40 seconds
```

Then we use dirb to scan hidden files in the webpage.



```
┌──(root㉿kali)-[/home/dhayanithi]
└─# dirb http://192.168.22.207/


-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Jun  9 18:40:59 2024
URL_BASE: http://192.168.22.207/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.22.207/ ----

+ http://192.168.22.207/index.html (CODE:200|SIZE:10671)

==> DIRECTORY: http://192.168.22.207/javascript/
+ http://192.168.22.207/server-status (CODE:403|SIZE:279)

---- Entering directory: http://192.168.22.207/javascript/ ----
```

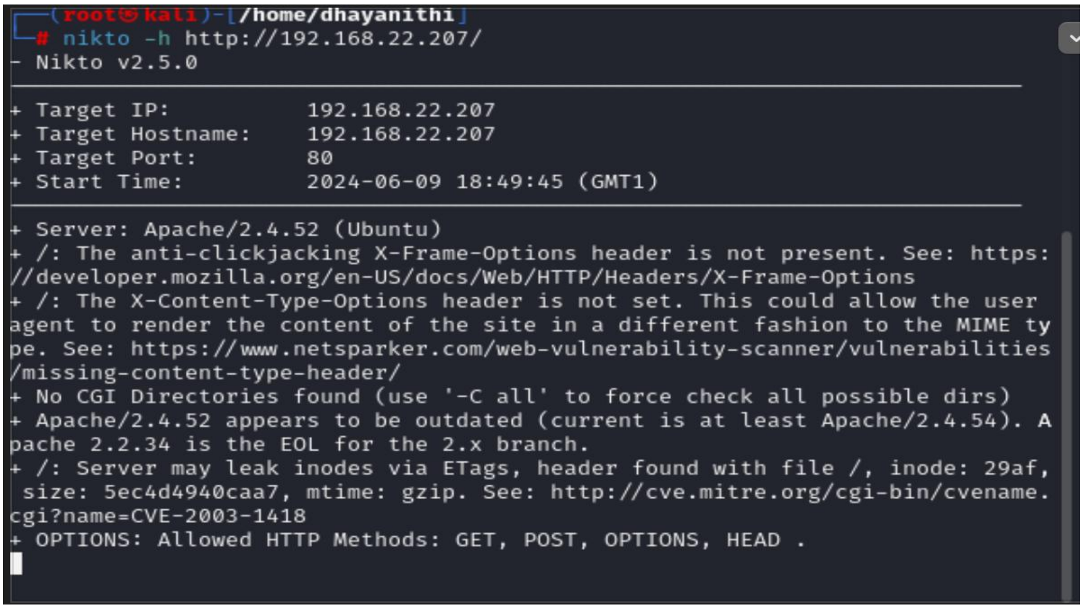
Curl is used to analyse homepage



```
┌──(root㉿kali)-[/home/dhayanithi]
└─# curl http://192.168.22.207/index.html -o index.html

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Curre
nt
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--
100 10671  100 10671    0     0   846k      0 --:--:-- --:--:-- --:--:--   868
k
```

You can use wget to recursively download the contents of the directories for offline analysis.

You can use Nikto to scan the web server for vulnerabilities:



```
┌──(root㉿kali)-[/home/dhayanithi]
└─# nikto -h http://192.168.22.207/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.22.207
+ Target Hostname:    192.168.22.207
+ Target Port:        80
+ Start Time:         2024-06-09 18:49:45 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache/2.4.52 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https:
//developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user
agent to render the content of the site in a different fashion to the MIME ty
pe. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities
/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.52 appears to be outdated (current is at least Apache/2.4.54). A
pache 2.2.34 is the EOL for the 2.x branch.
+ /: Server may leak inodes via ETags, header found with file /, inode: 29af,
 size: 5ec4d4940caa7, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.
cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
```