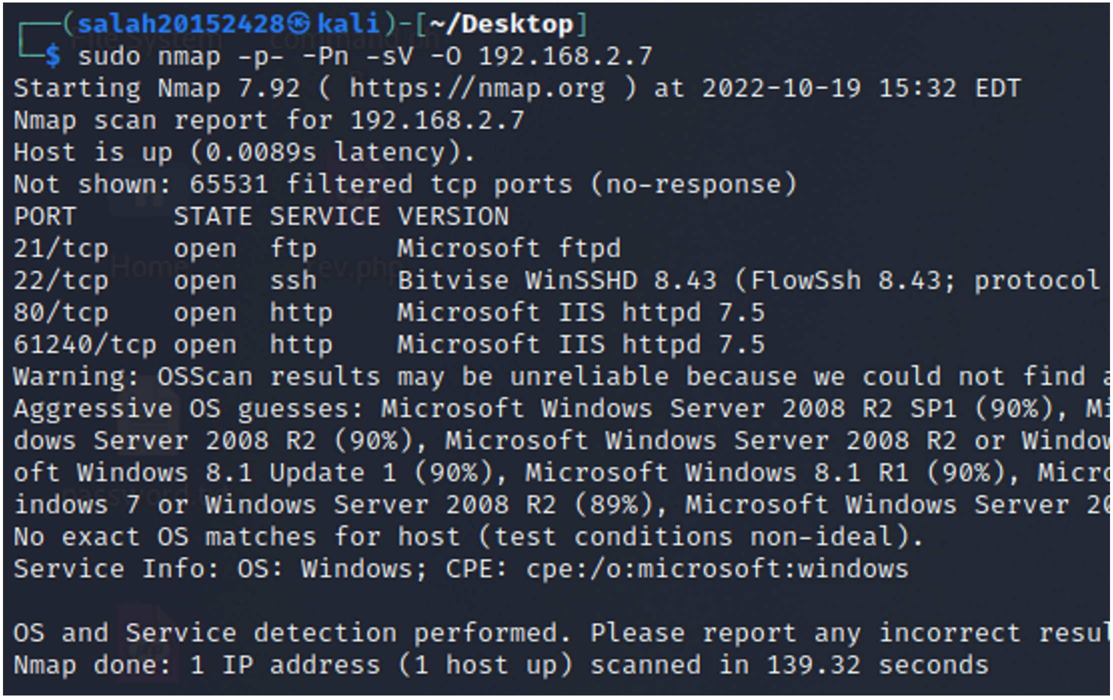
Pelagiad

Wednesday, 12 October 2022 1:15 PM

IP is 192.168.2.7

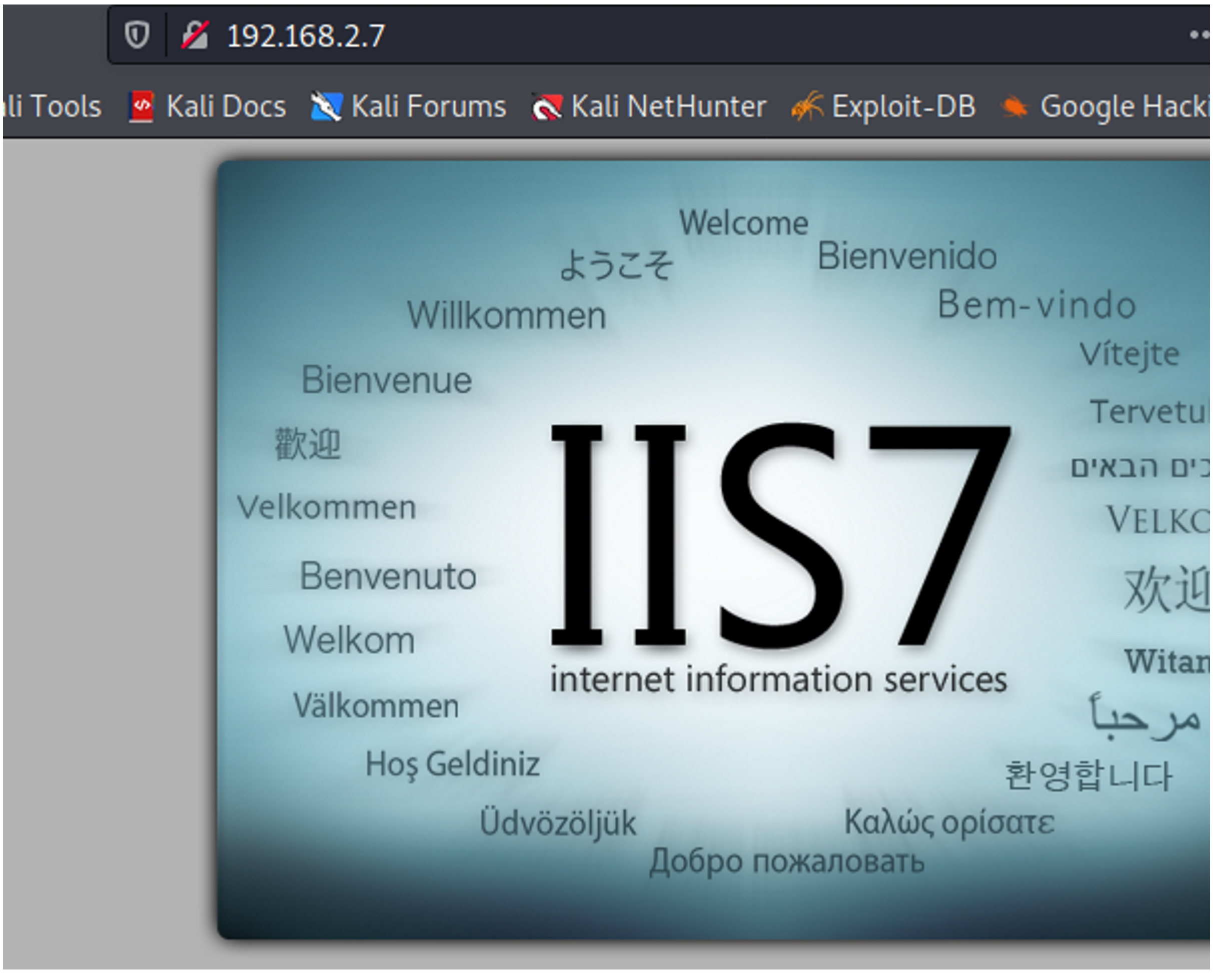
nmap scan



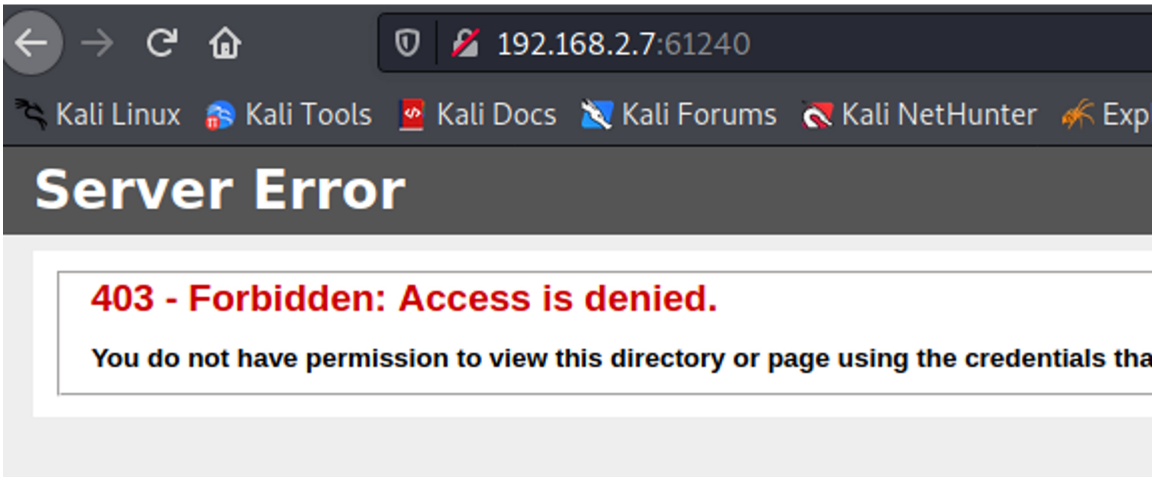
```
┌──(salah20152428㉿kali)-[~/Desktop]
└─$ sudo nmap -p- -Pn -sV -O 192.168.2.7
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-19 15:32 EDT
Nmap scan report for 192.168.2.7
Host is up (0.0089s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     Microsoft ftpd
22/tcp    open  ssh     Bitvise WinSSHD 8.43 (FlowSsh 8.43; protocol
80/tcp    open  http    Microsoft IIS httpd 7.5
61240/tcp open  http    Microsoft IIS httpd 7.5
Warning: OSScan results may be unreliable because we could not find a
Aggressive OS guesses: Microsoft Windows Server 2008 R2 SP1 (90%), Mi
dows Server 2008 R2 (90%), Microsoft Windows Server 2008 R2 or Window
oft Windows 8.1 Update 1 (90%), Microsoft Windows 8.1 R1 (90%), Micro
indows 7 or Windows Server 2008 R2 (89%), Microsoft Windows Server 20
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect resul
Nmap done: 1 IP address (1 host up) scanned in 139.32 seconds
```

Two IIS webservers running

Port 80



Port 61420

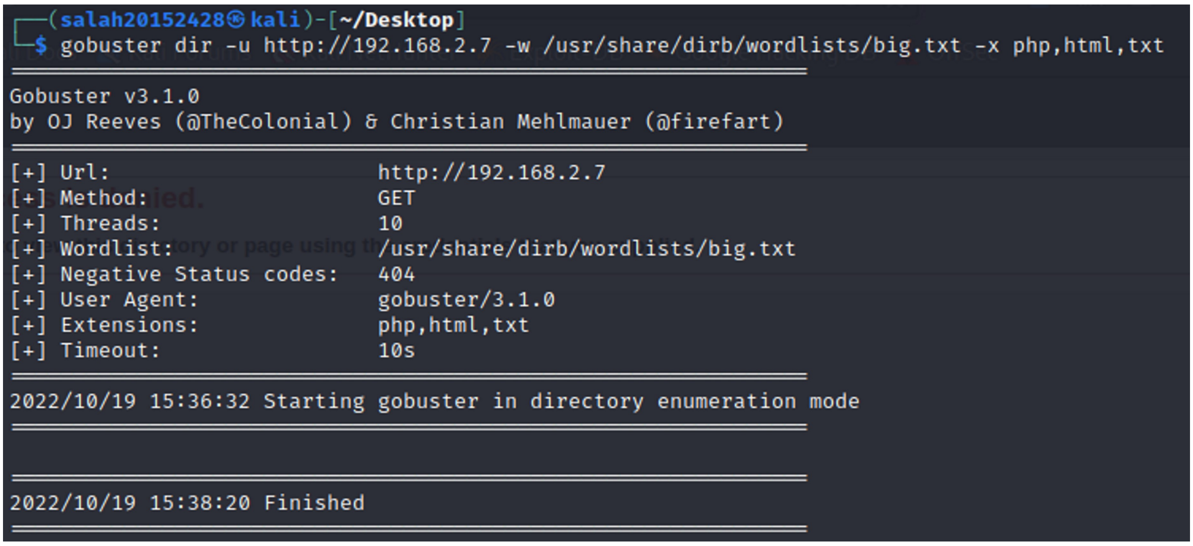


Server Error

403 - Forbidden: Access is denied.

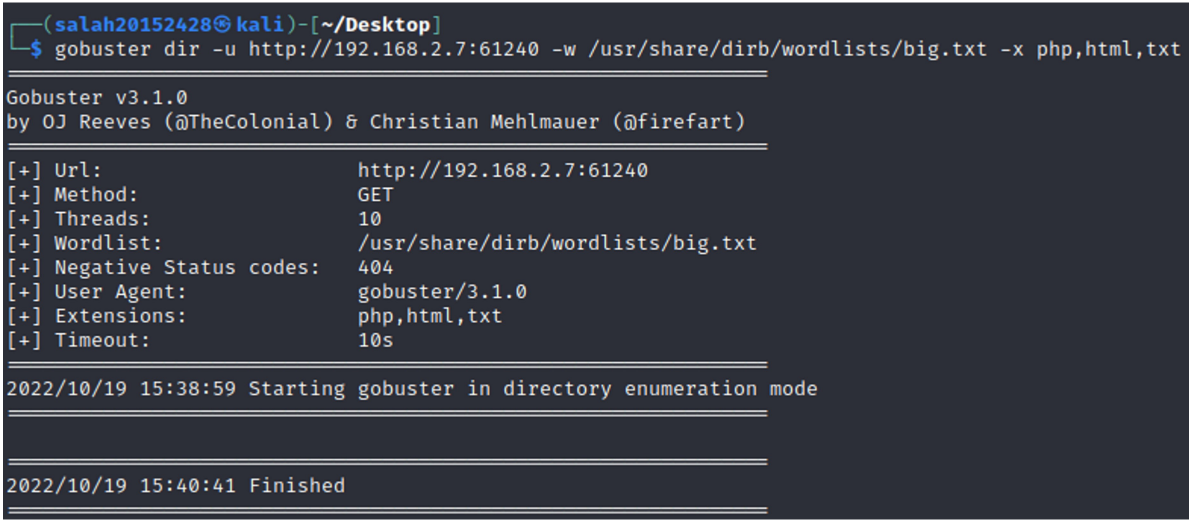
You do not have permission to view this directory or page using the credentials tha

Gobuster scan on port 80



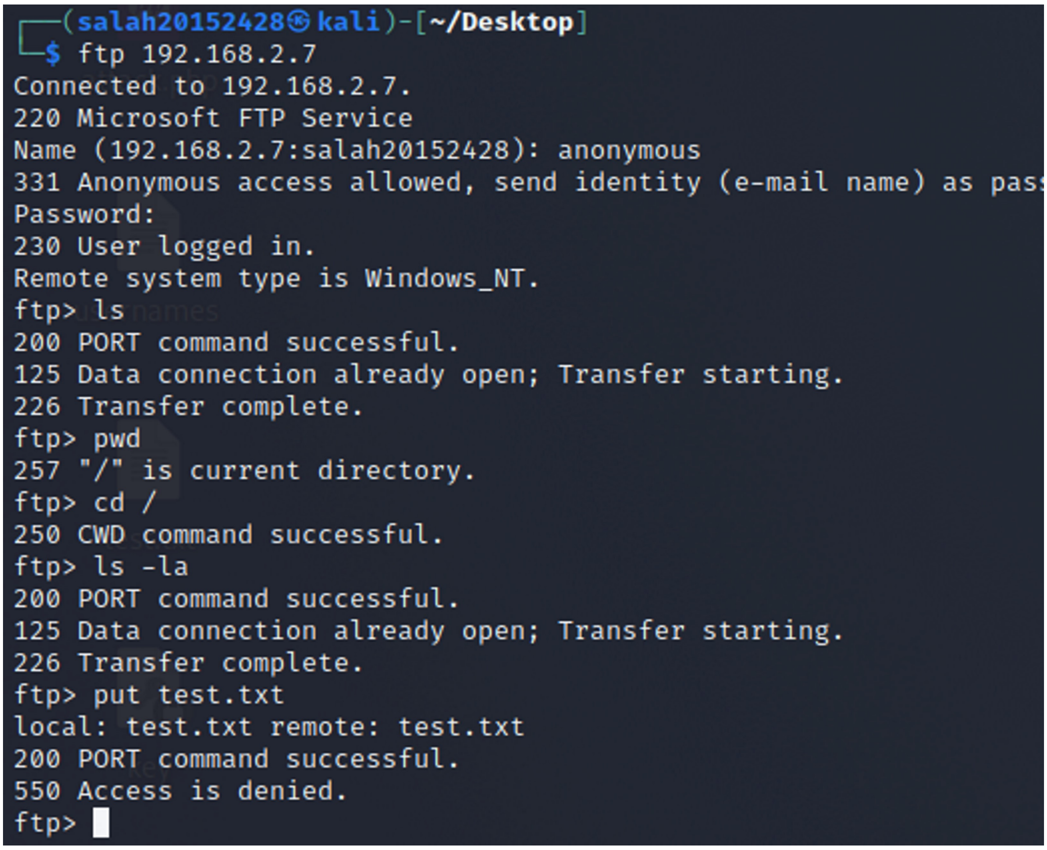
```
┌──(salah20152428㉿kali)-[~/Desktop]
└─$ gobuster dir -u http://192.168.2.7 -w /usr/share/dirb/wordlists/big.txt -x php,html,txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.2.7
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
2022/10/19 15:36:32 Starting gobuster in directory enumeration mode
===============================================================

===============================================================
2022/10/19 15:38:20 Finished
===============================================================
```

Gobuster scan on port 61420



```
┌──(salah20152428㉿kali)-[~/Desktop]
└─$ gobuster dir -u http://192.168.2.7:61240 -w /usr/share/dirb/wordlists/big.txt -x php,html,txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.2.7:61240
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
2022/10/19 15:38:59 Starting gobuster in directory enumeration mode
===============================================================

===============================================================
2022/10/19 15:40:41 Finished
===============================================================
```

Ftp allows anonymous log in but doesn't allow upload
there's nothing to transfer from host either



```
┌──(salah20152428㉿kali)-[~/Desktop]
└─$ ftp 192.168.2.7
Connected to 192.168.2.7.
220 Microsoft FTP Service
Name (192.168.2.7:salah20152428): anonymous
331 Anonymous access allowed, send identity (e-mail name) as pas
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp> pwd
257 "/" is current directory.
ftp> cd /
250 CWD command successful.
ftp> ls -la
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp> put test.txt
local: test.txt remote: test.txt
200 PORT command successful.
550 Access is denied.
ftp> █
```

Those are all the attack vectors and I have concluded that there is no way to gain access to the system