Kiểm thử & đánh giá an toàn hệ thống thông tin

Module 7. Domain Domination

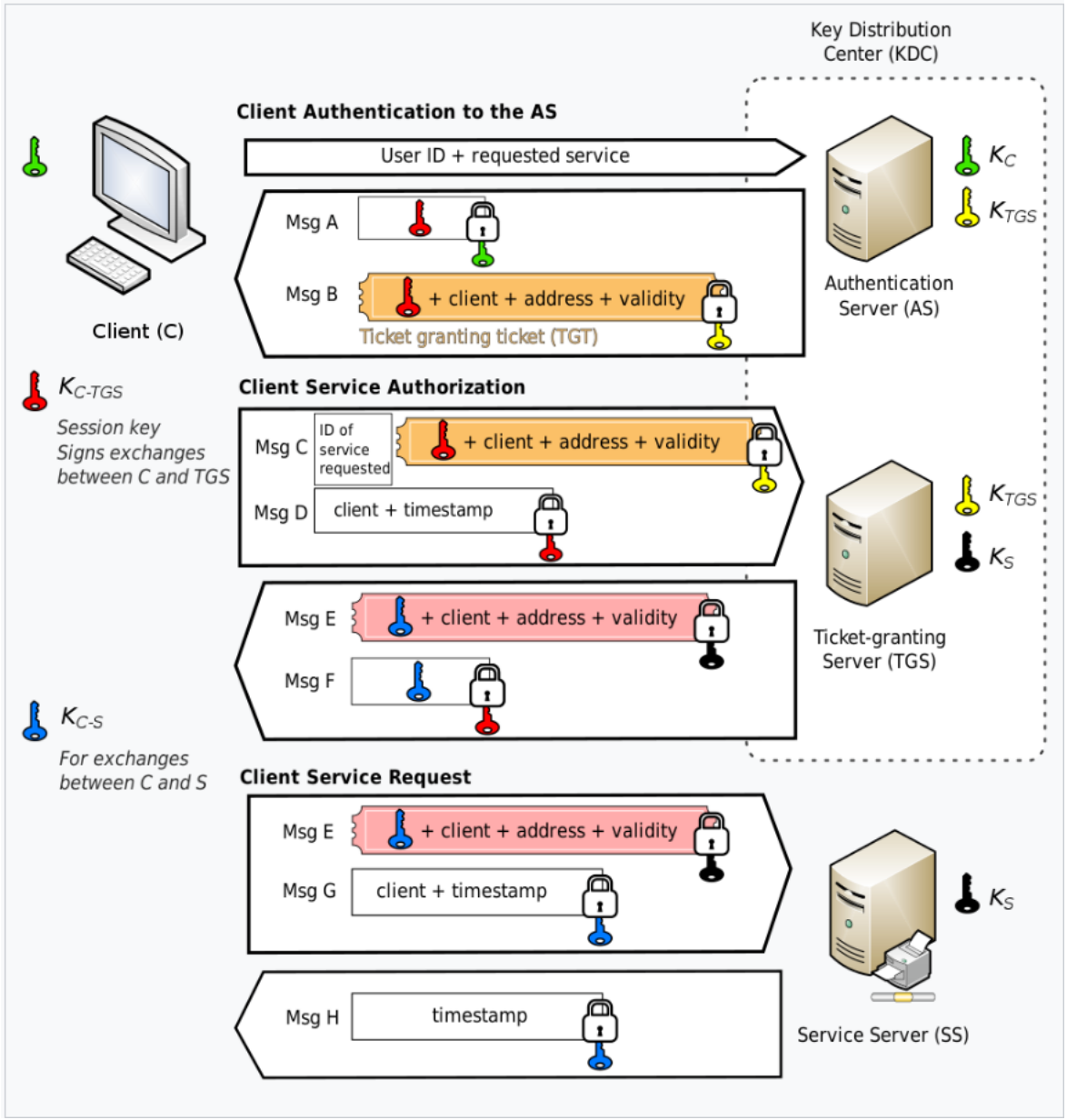
Content

- **Kerberos**
- Kerberoasting
- More Kerberos Attacks
- Domain Dominance
- Silver Ticket
- Golden Ticket
- Domain Privilege Escalation

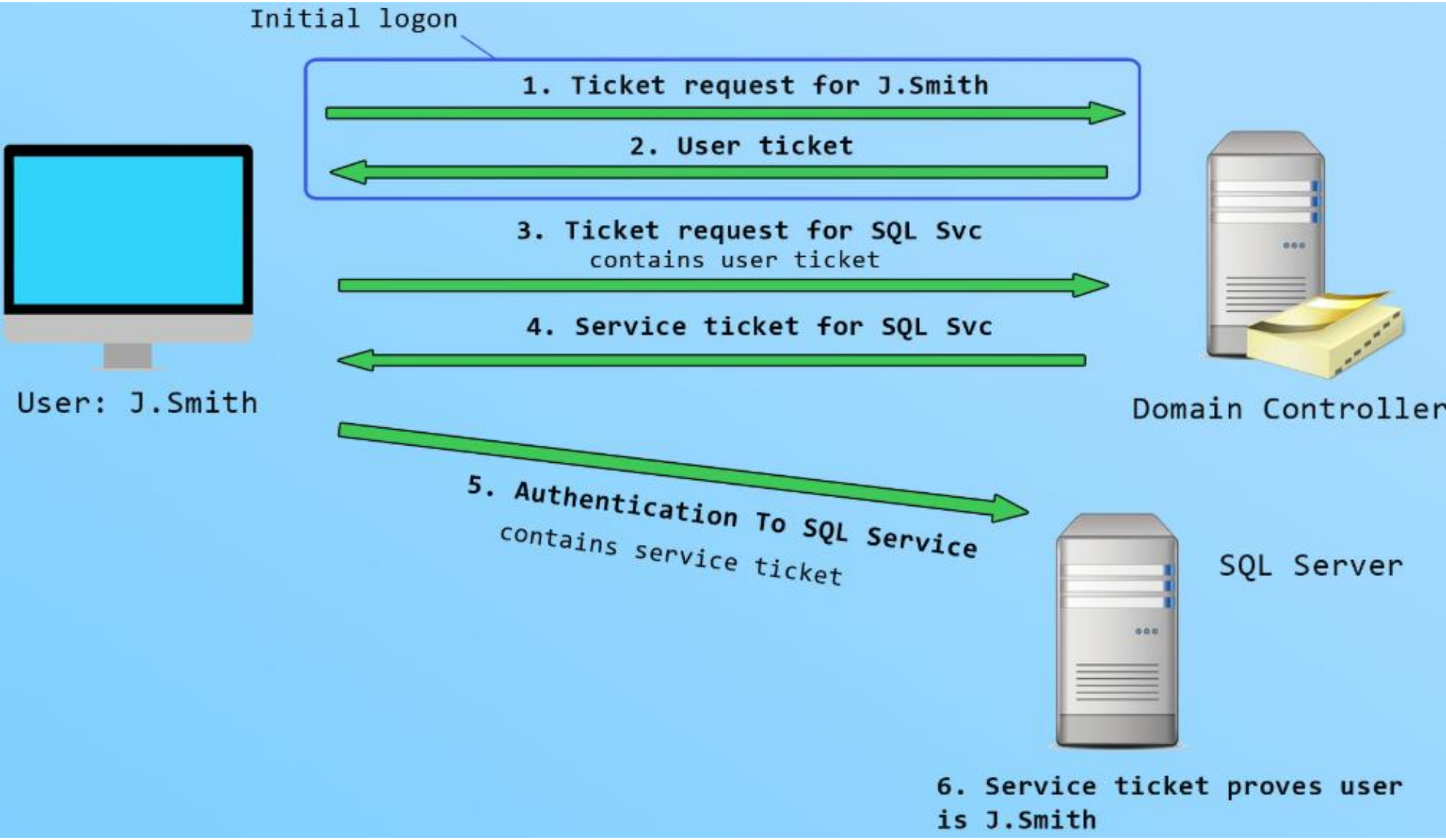
Kerberos: Introduction

- Kerberos là giao thức xác thực chính được sử dụng trong Microsoft Active Directory domain.
  - Kerberos xác thực dựa trên "ticket".
  - Cho phép 2 bên (Client-Server) xác thực nhau thông qua một kênh không an toàn với điều kiện cả 2 bên đều tin tưởng một bên thứ 3 – Key Distribution Center (KDC).
- Nếu Kerberos không thể sử dụng (vì 1 số lý do) thì Windows sẽ quay lại dùng NTLMv1/NTLMv2.

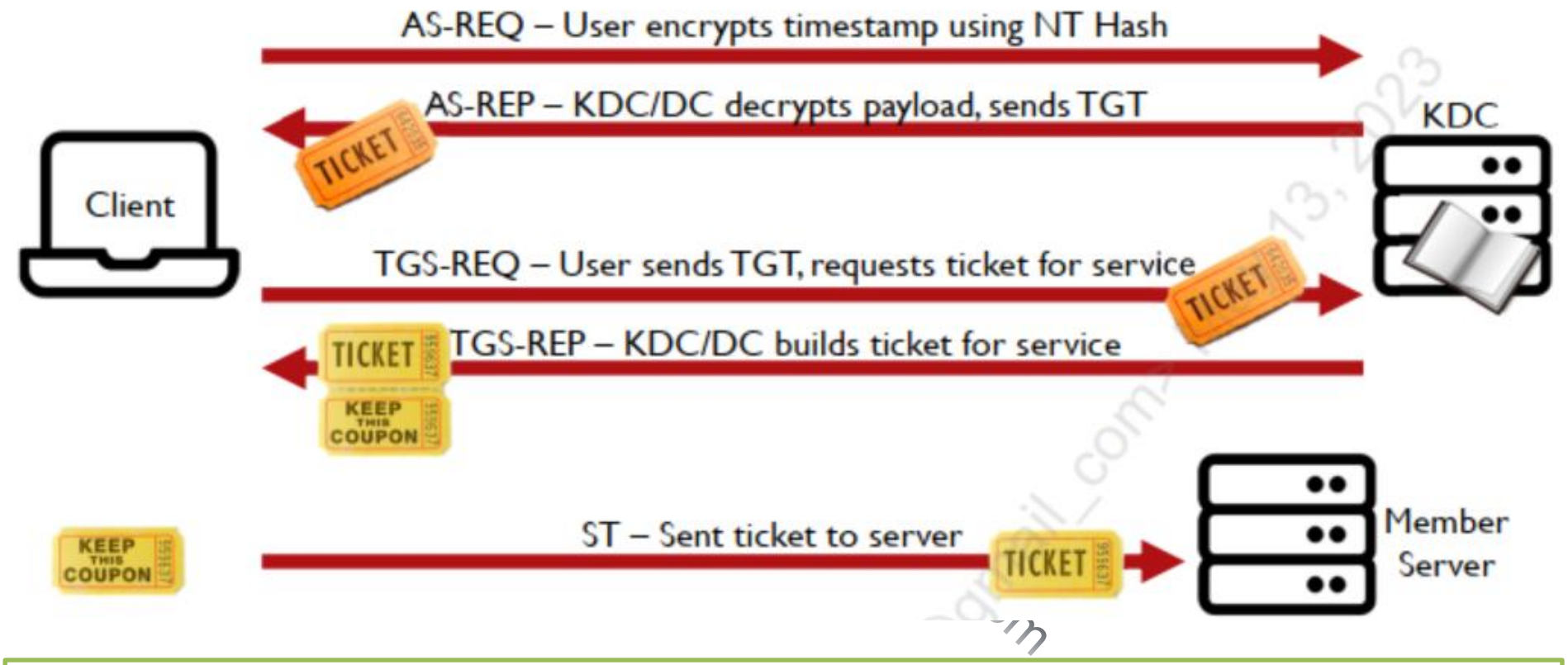
Simple Kerberos: How It Works (1/2)



Simple Kerberos: How It Works (2/2)



Simple Kerberos: Overall Flows



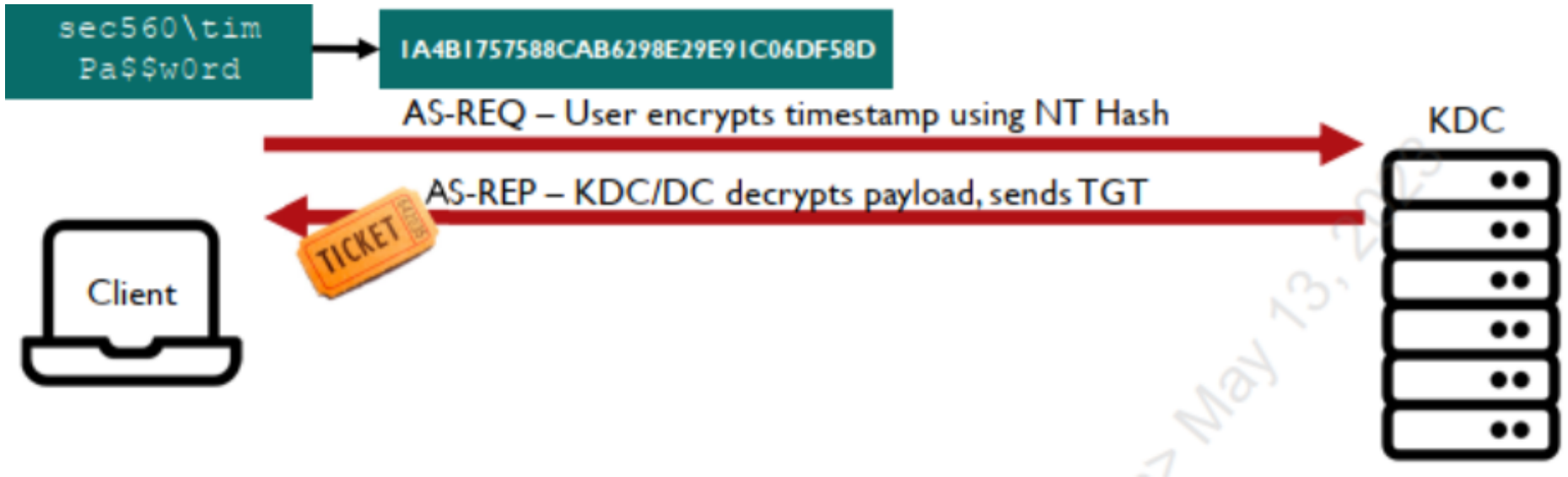
- TGT là "ticket" đầu tiên client nhận được và có thể sử dụng để yêu cầu các "ticket" cho các dịch vụ khác.
  - Có thể coi TGT là "ticket" cho "krbtgt service".
  - Mặc định, TGT có hiệu lực trong 10 tiếng.

Kerberos: Three Long-Term Keys

Long-Term Secret Key	Key (password hash)	Use
KDC	Krbtgt	Encrypt TGT (AS-REP) Sign PAC (AS-REP & TGS-REP)
Client	Client account	Check encrypted timestamp (AS-REQ) Encrypt session key (AS-REP)
Target (Service)	Service account	Encrypt service portion of the ST (TGS-REP) Sign the PAC (TGS-REP)

- Nếu KDC secret key bị thỏa hiệp → "recreate" TGTs và "sign" PAC.
- PAC chứa thông tin về user's authorization và privileges:
  - Với krbtgt hash → làm giả PAC với "đặc quyền" mong muốn.

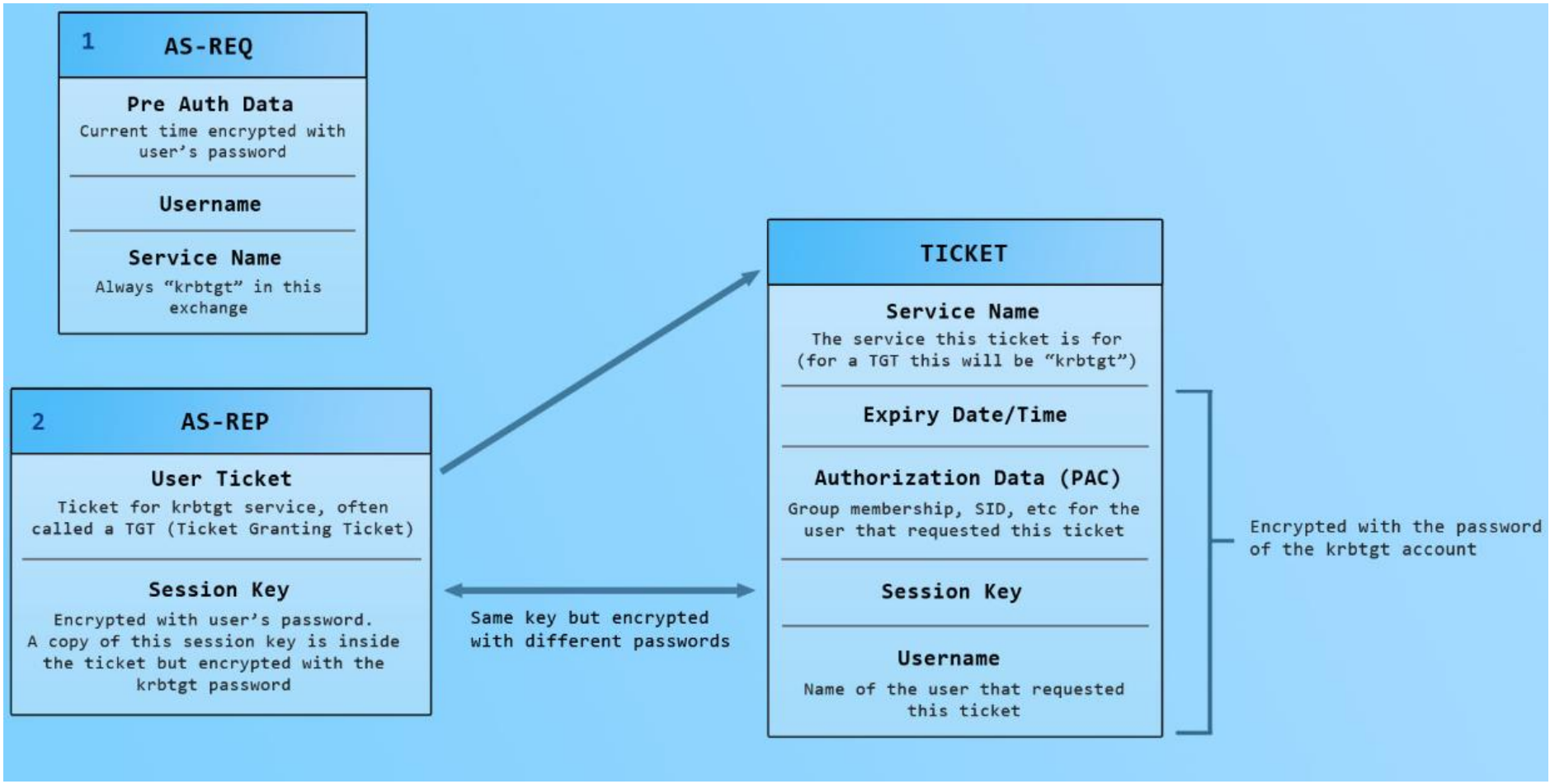
AS-REQ with Pre-Authentication and AS-REP (1/2)



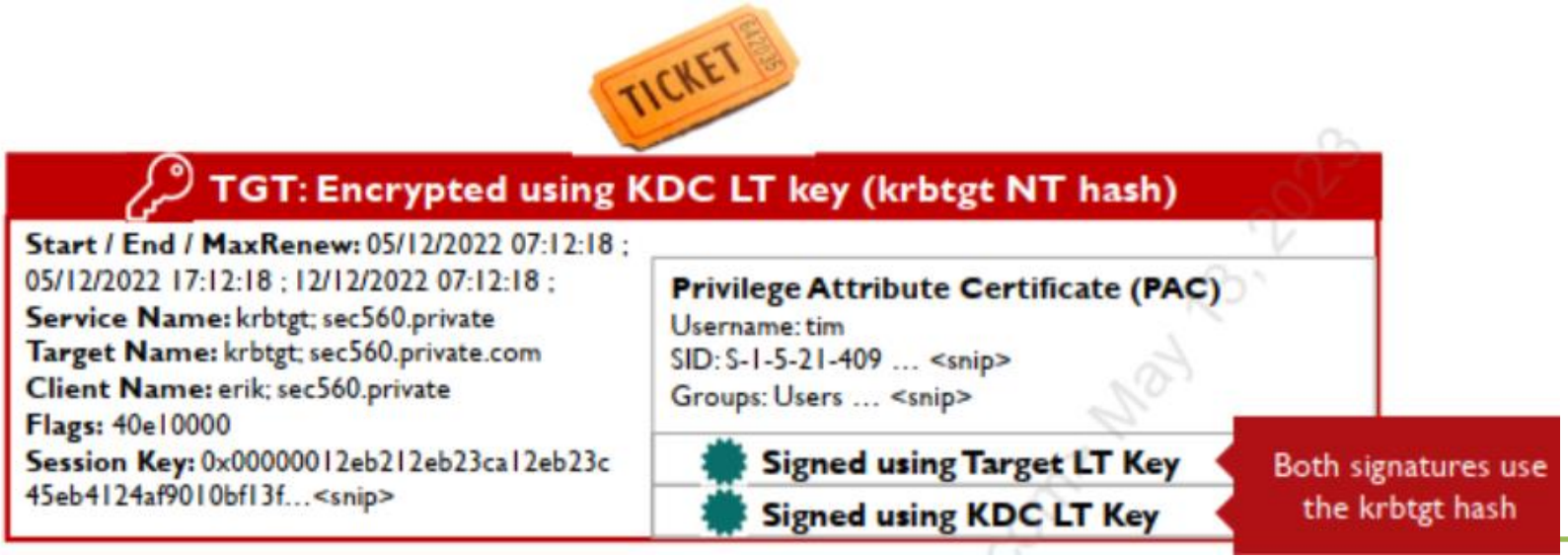
AS-REQ with pre-authentication

- Mã hóa timestamp với user's NT hash và gửi lên AS.
- KDC (AS) giải mã. Nếu giải mã thành công (nghĩa là người dùng hợp lệ) sẽ trả về:
  - TGT (mã hóa với krbtgt NT hash).
  - K_{C-TGS} (mã hóa với user's hash).

AS-REQ with Pre-Authentication and AS-REP (2/2)



TGT (Ticket Granting Ticket) and PAC (1/3)

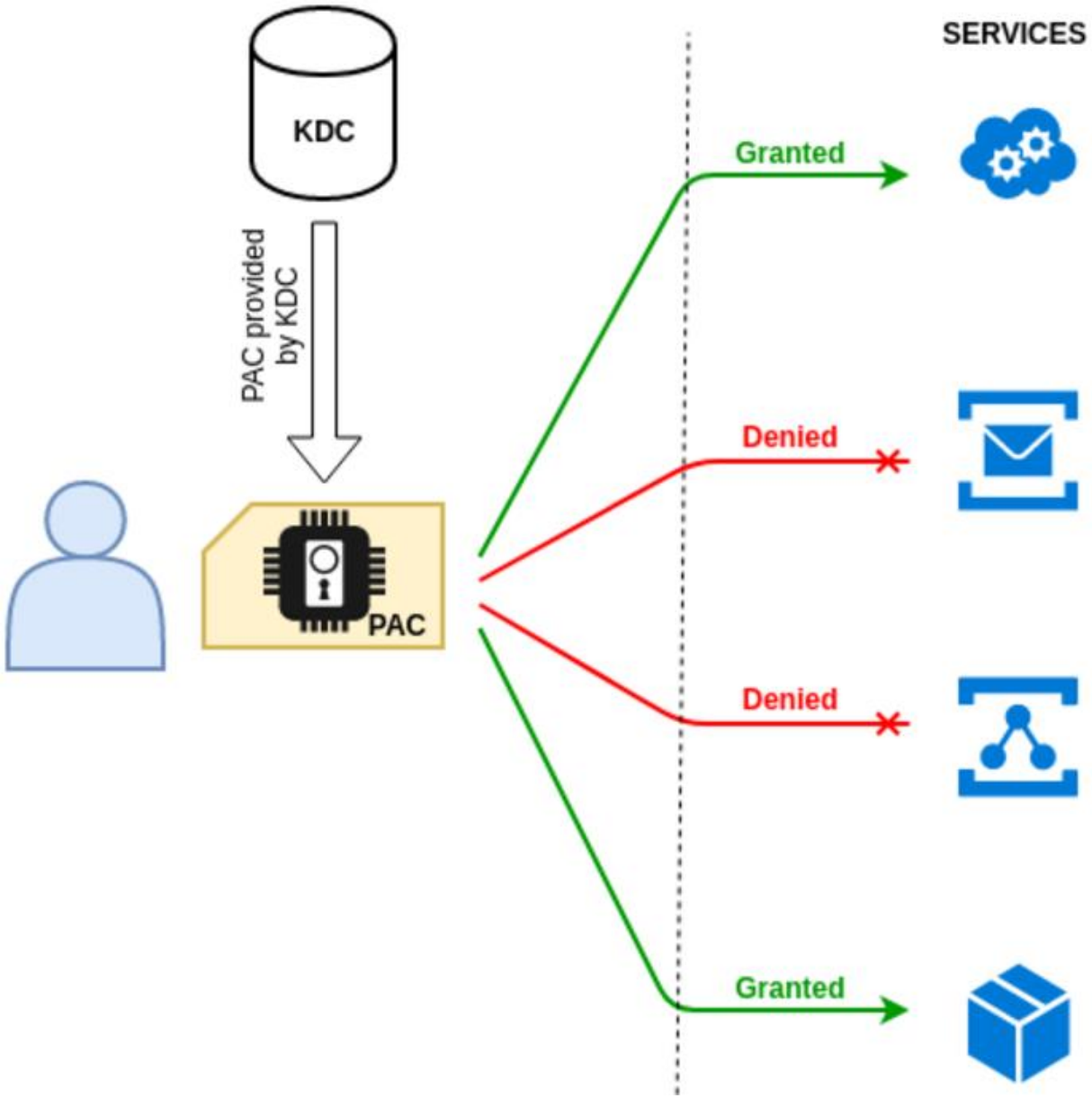


- Kerberos là một "stateless protocol", KDC không nhớ ai có tickets. Tất cả trạng thái được lưu trữ trong tickets.
- PAC được sử dụng để quản lý quyền trong AD.
  - Chỉ có KDC là nắm được tất cả thông tin về mọi đối tượng trong AD do đó KDC cần truyền thông tin này đến cho tất cả các service để những service này có thể tạo ra token phù hợp cho những người dung sử dụng những service này.

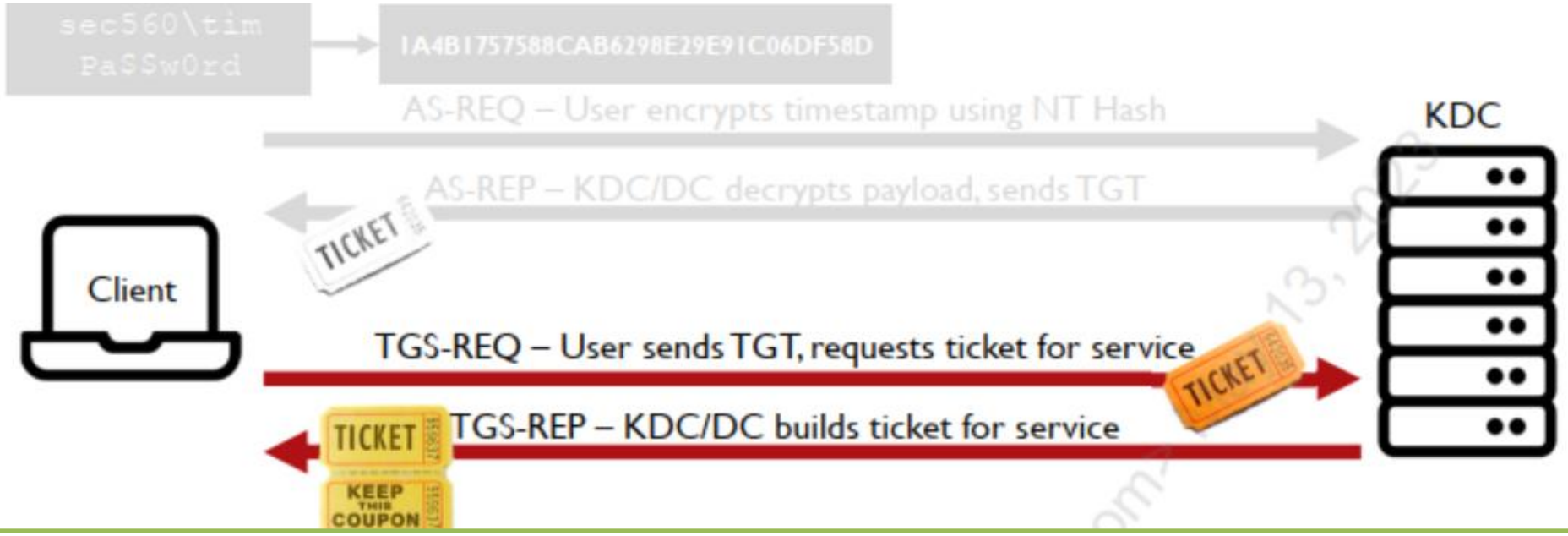
TGT (Ticket Granting Ticket) and PAC (2/3)

- PAC chứa nhiều thông tin về người dùng như username, SID, group membership, security information…
- PAC có trong TGT và ST.
- PAC được ký bởi 2 keys (trong trường hợp này cả 2 key là như nhau).
  - Đầu tiên được ký bởi **Target LT Key** (vì đây là TGT nên "target" là krbtgt account (key là krbtgt NT hash).
  - Sau đó được ký bởi **KDC LT Key** (krbtgt NT hash).
- Do các thông tin trong PAC được mã hóa bởi các key khác nhau (khác với ký số) nên user không có quyền kiểm soát các thông tin trong PAC do đó user **KHÔNG** thể sửa đổi permission, group….của mình.

TGT (Ticket Granting Ticket) and PAC (3/3)

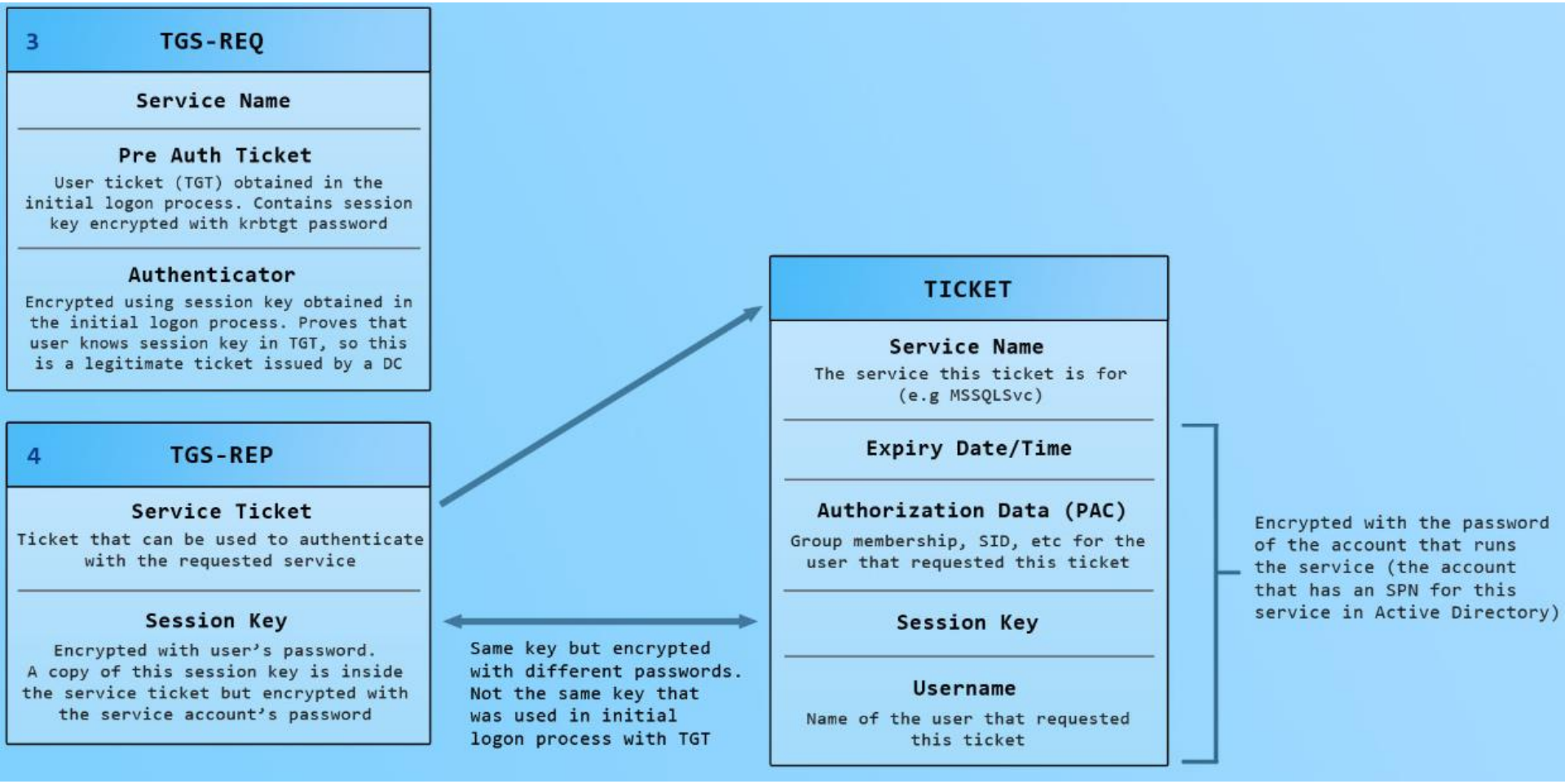


Requesting a Service Ticket (ST) (1/2)



- Client có thể yêu cầu "ticket" cho bất kỳ dịch vụ nào.
- KDC gửi "ticket" (TGS-REP), không quyết định người dùng có quyền truy cập hay không.
  - Việc quyết định user có quyền truy cập hay không do target service dựa trên kiểm tra PAC trong ST.
- ST được mã hóa bởi "target service's password hash".

Requesting a Service Ticket (ST) (2/2)



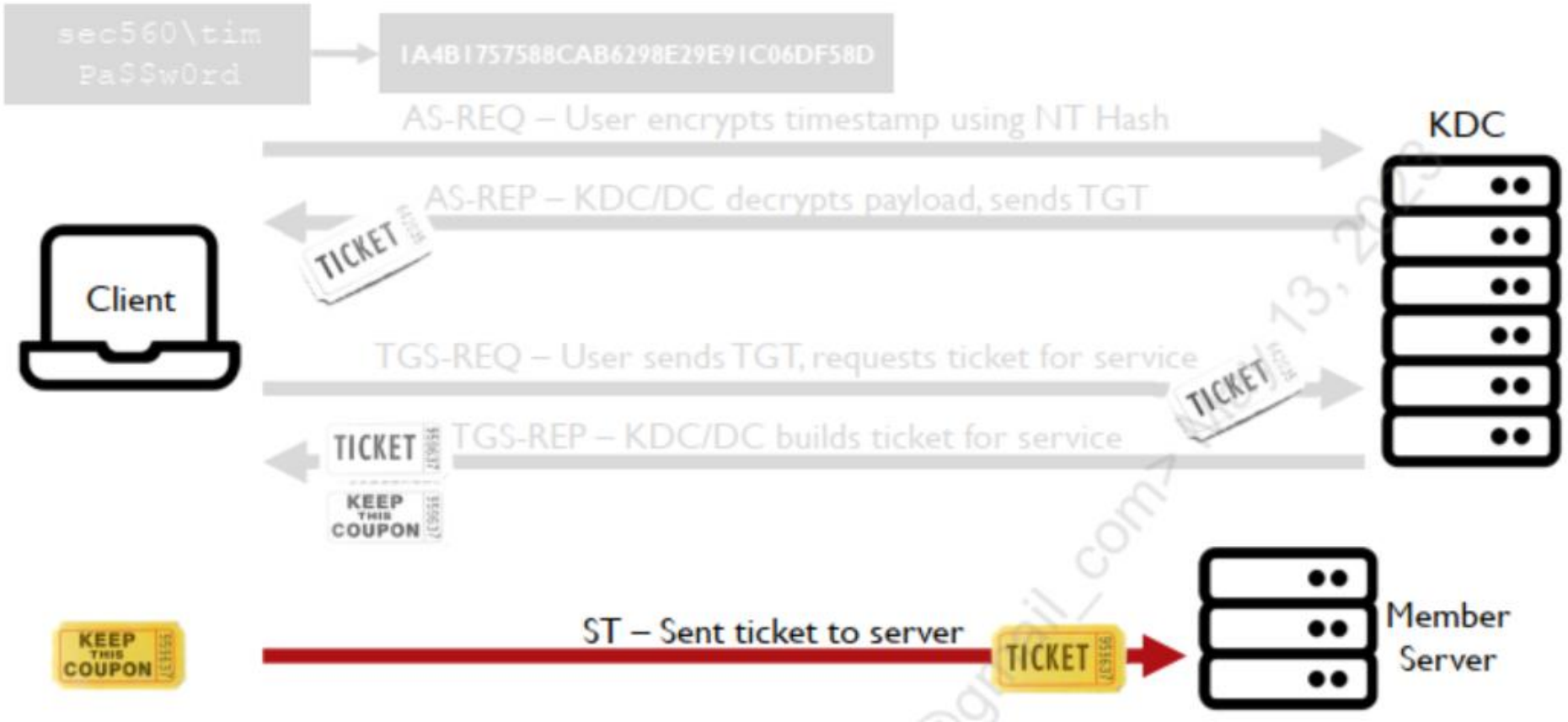
Service Principal Name (1/2)

- Service Principal Name (SPN) – mã định danh (tên dịch vụ) cho 1 dịch vụ được cung cấp bởi máy chủ miền. Mỗi SPN được liên kết với một tài khoản trong AD (có thể là machine hoặc user account).
- SPNs bao gồm 2 thành phần chính:
  - Service Class: Chỉ định loại dịch vụ, chẳng hạn như HTTP cho dịch vụ web, LDAP cho dịch vụ thư mục hoặc MSSQLSvc cho Microsoft SQL Server.
  - Host Name: Xác định máy chủ nơi dịch vụ được lưu trữ.
- SPNs Example:
  - HTTP/webserver.domain.com
  - MSSQLSvc/servername.domain.com:1433

Service Principal Name (2/2)

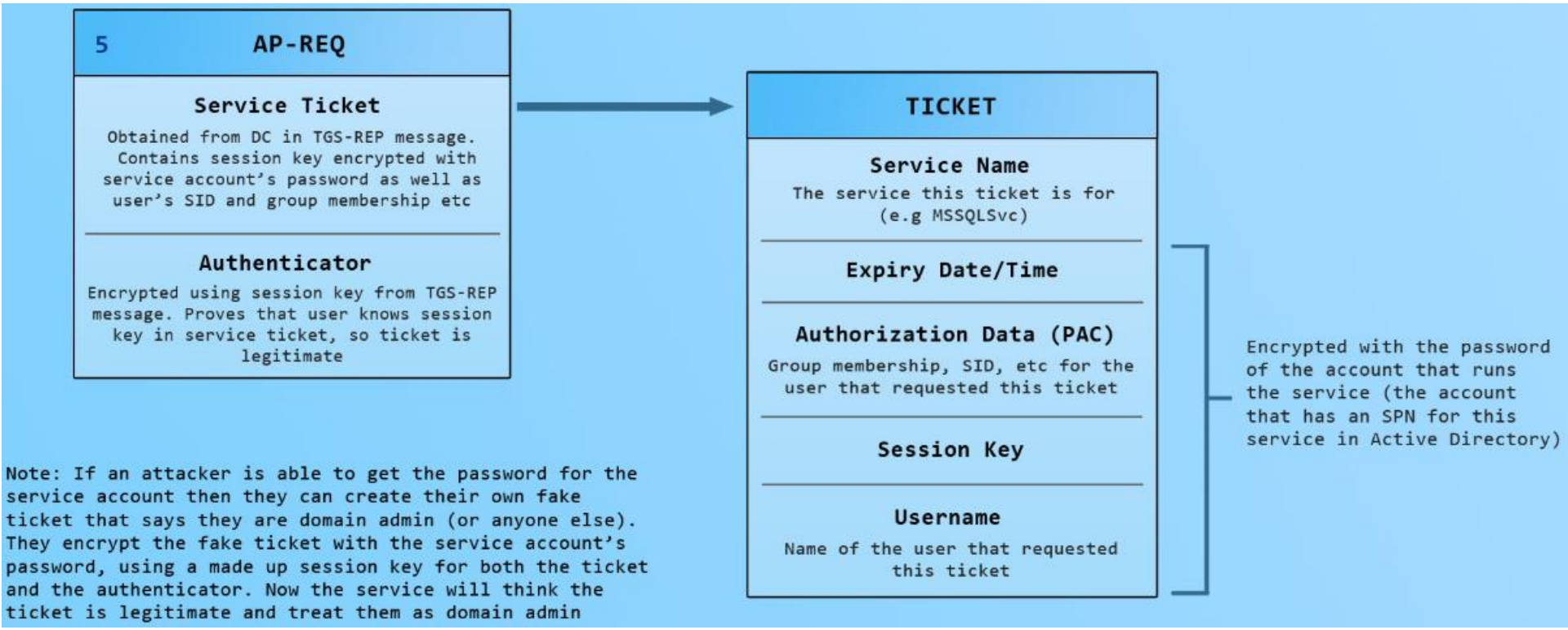
- Ticket được yêu cầu dựa trên tên dịch vụ có dạng serviceclass/host:port.
  - KDC lưu trữ ánh xạ của SPN với tài khoản tương ứng.
  - Example: SMTP/cliff.sec560.local ánh xạ tới tài khoản mailsvc.
  - Ánh xạ được tạo bởi setspn.exe
  - Có thể lấy danh sách SPN với setspn.exe hoặc các công cụ truy vấn LDAP khác (bất kỳ user nào trong miền đều có thể thực hiện truy vấn).

Using a Service Ticket (1/2)



- User gửi ST lên Server.
- Server giải mã ST và quyết định mức độ truy cập của user.

Using a Service Ticket (1/2)



Note: If an attacker is able to get the password for the service account then they can create their own fake ticket that says they are domain admin (or anyone else). They encrypt the fake ticket with the service account's password, using a made up session key for both the ticket and the authenticator. Now the service will think the ticket is legitimate and treat them as domain admin

Service Ticket

Server Portion

- User details (PAC)
- Session Key (same as below)
- Encrypted with the service account's NT Hash

This will be important later (Kerberoasting)

Client Portion

- Validity time
- Session Key (same as above)
- Encrypted with the TGT Session Key

Types of Encryption in the Kerberos Protocol (1/2)

- Để mã hóa Kerberos ticket thì RC4 được sử dụng (mặc định) mặc dù AES (AES128 và AES256) được hỗ trợ từ Windớ 7 và Windows Server 2008.
  - Từ bản cập nhật 11/2022 trên Domain Controller thì AES256 được sử dụng mặc định cho session key nhưng Service Ticket (ST) vẫn sử dụng RC4.
- Microsoft hỗ trợ một số dạng mã hóa (etype)
  - DES-CBC-CRC - etype 0x1 (1)
  - DES-CBC-MD5 - etype 0x3 (3)
  - RC4-HMAC - etype 0x17 (23)
  - AES128-CTS-HMAC-SHA1-96 - etype 0x11 (17)
  - AES256-CTS-HMAC-SHA1-96 - etype 0x12 (18)

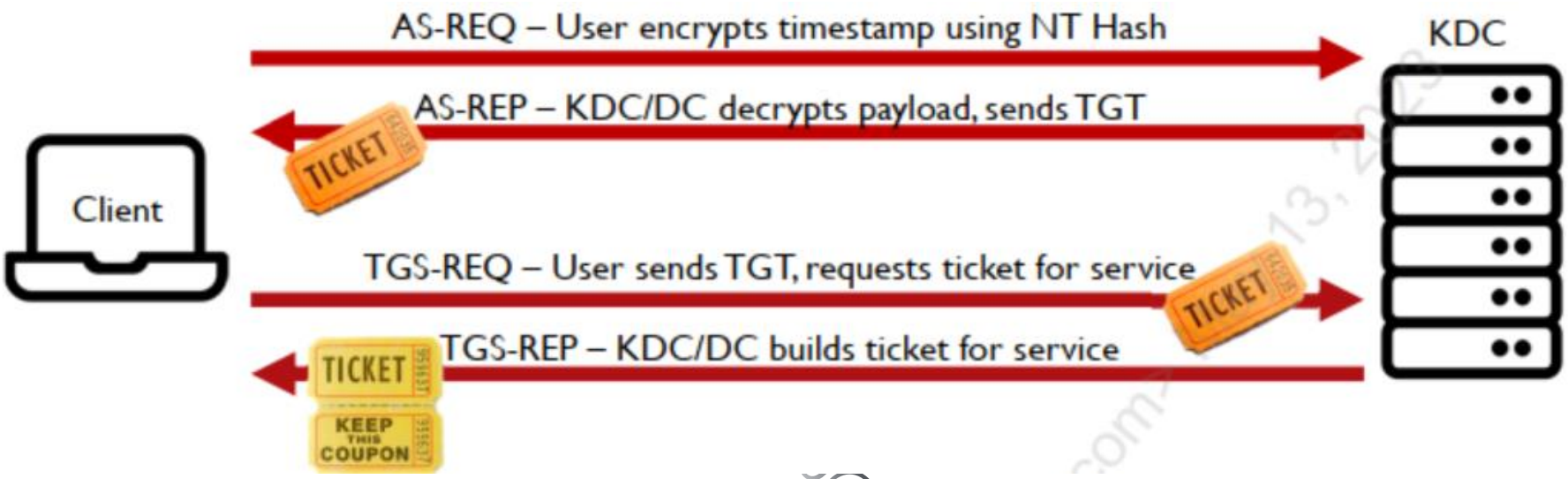
Types of Encryption in the Kerberos Protocol (2/2)

- Trên thực tế, "encryption key" được tạo ra từ "password" sử dụng "hash function".
  - Khi tạo key thì salt thường được thêm vào tuy nhiên trong trường hợp của RC4-HMAC (RFC4757) thì MD4 hash (no salt) được sử dụng → key này giống với NT hash.

Content

- Kerberos
- **Kerberoasting**
- More Kerberos Attacks
- Domain Dominance
- Silver Ticket
- Golden Ticket
- Domain Privilege Escalation

Requesting a Service Ticket (ST) Review



- Client có thể yêu cầu "ticket" cho bất kỳ dịch vụ nào.
- KDC gửi "ticket" (TGS-REP), không quyết định người dùng có quyền truy cập hay không?
- ST được mã hóa bởi "target service's password hash".

Requesting a Ticket

- Client có thể yêu cầu "ticket" cho bất kỳ dịch vụ nào *thậm chí khi:*
  - Client không có quyền sử dụng dịch vụ.
  - Dịch vụ có thể không truy cập được do tường lửa.
  - Dịch vụ có thể bị "tắt" (do crash…).
- Lưu ý: *KDC không quyết định người dùng có quyền truy cập hay không.*
  - Việc quyết định người dùng có quyền truy cập là do target service.

Kerberoasting Attack

- *Kerberoasting is a post-exploitation attack technique that attempts to obtain a password hash of an Active Directory account that has a Service Principal Name ("SPN").*
- Kerberoast attack: Yêu cầu tickets và sau đó "crack"
  - ST được mã hóa bởi "target service account's hash"
  - Chúng ta cần ticket để crack nhưng yêu cầu ticket nào?
- Có 2 loại tài khoản trong domain.
  - Computer accounts: Password hashes được tạo ngẫu nhiên (not crackable).
  - User accounts: Passwords được tạo bởi user/admin.
- Chúng ta cần "SPNs/tickets" gắn liền với "user account".

Setspn.exe

- Setspn.exe được sử dụng để tạo và truy vấn SPNs.
  - Một "domain account" có thể gắn liền với nhiều dịch vụ
  - Sqlservice account được gắn với MSSQLSvc service (class) trên sql01.

```
C:\> setspn -T * -Q */*
CN=sqlservice,CN=Users,DC=mydomain,DC=com
        MSSQLSvc/sql01.mydomain.com
        MSSQLSvc/sql01.mydomain.com:1433
CN=SQL01,CN=Computers,DC=mydomain,DC=com
        WSMAN/sql01
        WSMAN/sql01.mydomain.com
        TERMSRV/SQL01
        TERMSRV/sql01.mydomain.com
        RestrictedKrbHost/SQL01
        HOST/SQL01
        RestrictedKrbHost/sql01.mydomain.com
        HOST/sql01.mydomain.com
```

Obtaining Tickets

- Nhiều công cụ có thể sử dụng để lấy ticket:
  - GetUserSPNs.py (Impacket) – yêu cầu "user SPN tickets", lưu dưới dạng "crackable format" để sử dụng bởi JtR và Hashcat.
  - Invoke-Kerberoast (một phần của PowerSploit and Empire)
  - Một số C2, sử dụng Powershell hoặc trích xuất từ RAM (like mimikatz).

Kerberoast Attack Steps (1/2)

- Domain Authentication.
- Finding a Kerberoastable Target.
  - SPN Scanning.
- TGS Requested.
- Attacker Extracts the TGS Ticket.
- Offline Cracking of Kerberos TGS Ticket.

Kerberoast Attack Steps (2/2)

- Kỹ thuật này được phát hiện bởi Tim Medin vào năm 2014.
  - Truy vấn Active Directory cho "tài khoản gắn với SPN".
  - Yêu cầu "RC4 service tickets" (vẫn hoạt động với AES nhưng chậm hơn) từ DC sử dụng các SPN có giá trị như Domain Account.
  - Trích xuất Service Tickets (ST) nhận được và lưu ra file
  - Sử dụng tấn công vét cạn để bẻ khóa "ticket" và tìm NT hash/password được sử dụng.
- *Tấn công này được sử dụng do mật khẩu tài khoản dịch vụ thường ít được thay đổi.*

AES vs RC4

- Kerberoasting hoạt động trên cả AES và RC4.
- Bẻ khóa RC4 tickets nhanh hơn AES.
- Một số "etype (Encryption types)" phổ biến:
  - 23: RC4.
  - 17: AES128 (chậm hơn ~100 lần so với bẻ khóa RC4).
  - 19: AES256 (chậm hơn ~170 lần so với bẻ khóa RC4).
- Khóa RC4 chỉ dựa trên "account's NT hash".
- AES key dựa trên "account's NT hash và salt (domain và username)".

What Service Accounts are Good Targets?

- Service accounts thường có đặc quyền hoặc có thể truy cập tới dữ liệu nhạy cảm.
  - Nếu chiếm được service account thì có thể dẫn đến chiếm được toàn bộ domain.
- Một số tài khoản thú vị cần lưu ý:
  - AGPMServer: Microsoft Advanced Group Policy Management (thường có toàn quyền quản trị tất cả GPO).
  - MSSQL/MSSQLSvc: SQL server.
  - FIMService: Forefront Identity Manager Service.
- Thực hiện tốt việc liệt kê "account" và "group membership" sẽ hỗ trợ tìm ra các tài khoản thú vị.

Content

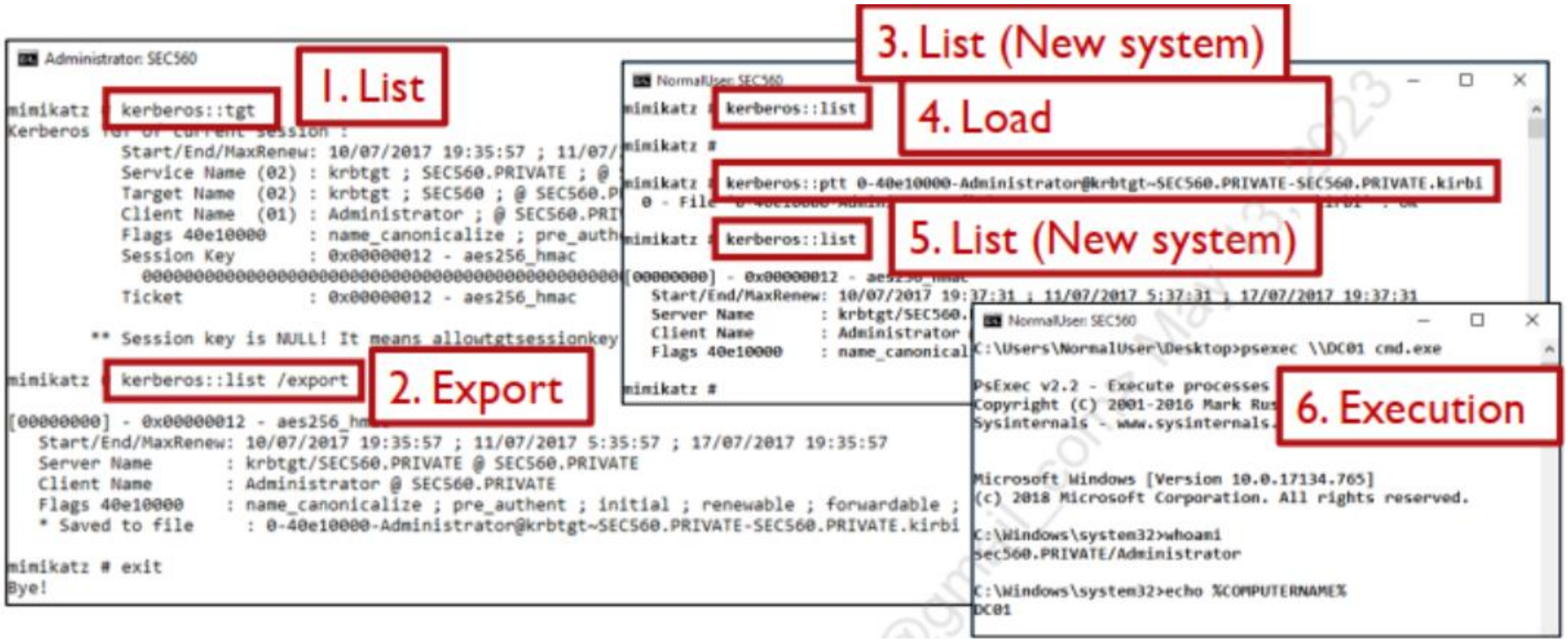
- Kerberos
- Kerberoasting
- **More Kerberos Attacks**
- Domain Dominance
- Silver Ticket
- Golden Ticket
- Domain Privilege Escalation

Pass-the-Ticket

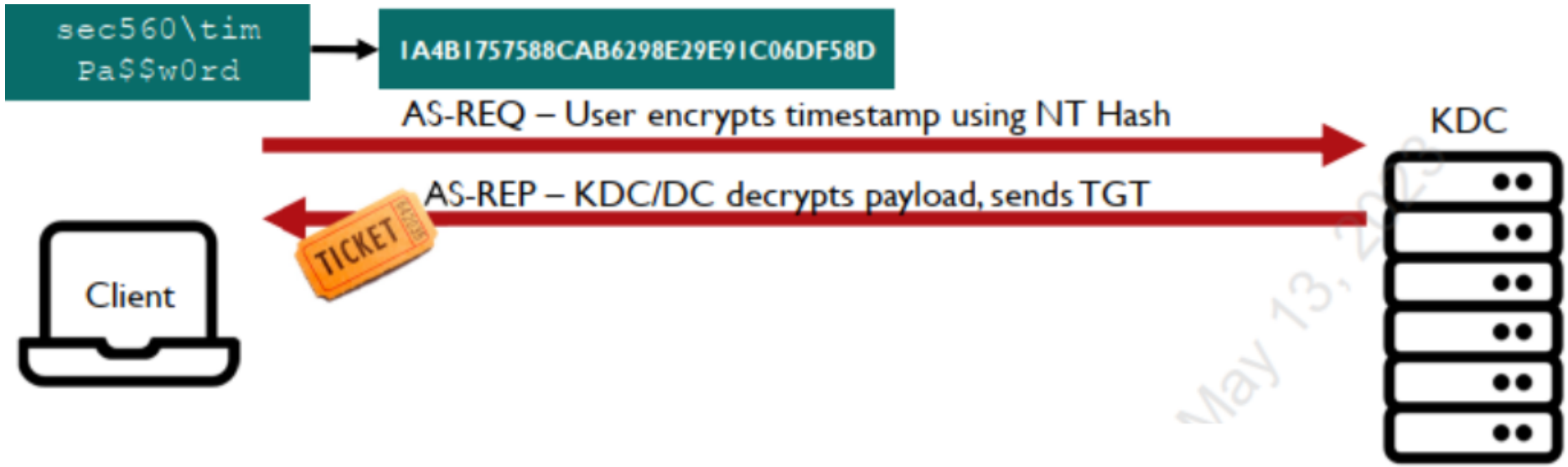
- Kerberos ticket (TGT/ST) bị "trộm" có thể được sử dụng trên hệ thống khác.
- Kỹ thuật đánh cắp thông tin xác thực cho phép truy cập như victim mà không cần biết mật khẩu/hash.
- Ticket có thể được lấy từ hệ thống bất kỳ và sử dụng ở bất kỳ đâu.
  - Chỉ có hiệu lực cho đến khi hết hạn.
  - ST: Chỉ hiệu lực cho "target service".
  - TGT: Có thể sử dụng cho service bất kỳ.
- Để lấy được ticket cần có quyền "local admin" trên máy mà victim đăng nhập.
- Tools: Mimikatz (.kirbi), Rubeus

Pass-the-Ticket: Mimikatz Example

- Export ticket, copy tới hệ thống khác, import



Overpass-the-Hash



- Bước đầu tiên trong xác thực Kerberos là mã hóa timestamp sử dụng "user's hash" và nhận TGT.
- Nếu chúng ta có "user's hash", chúng ta có thể thực hiện AS-REQ/AS-REP và nhận TGT hợp lệ với người dùng tương ứng (Không phải là Leo thang đặc quyền).

Golden Ticket Overview

- Chúng ta có thể làm giả TGT nếu chúng ta có "krbtgt account's hash".
  - TGT được ký và mã hóa bởi "krbtgt account's hash".
  - Ta có thể tạo ra PAC giả mạo với nhiều quyền hơn (như tự biến mình thành "domain admin" - RID 512).
  - Trao đổi về tấn công này ở phần sau.

Content

- Kerberos
- Kerberoasting
- More Kerberos Attacks
- **Domain Dominance**
- Silver Ticket
- Golden Ticket
- Domain Privilege Escalation

Domain Domination and AD Persistence

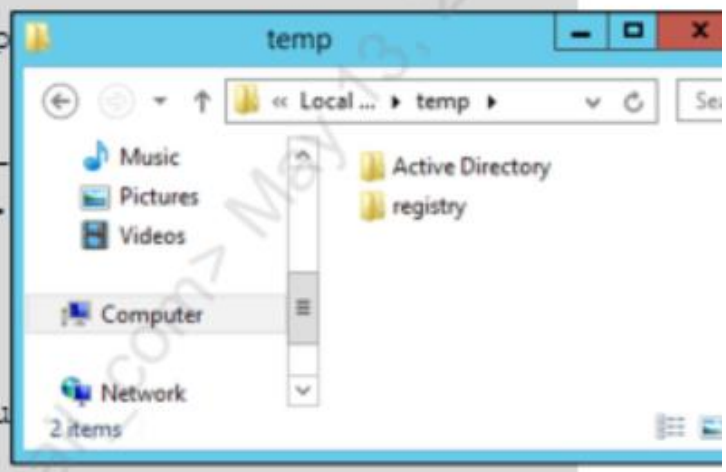
- Một số kỹ thuật thường được sử dụng để củng cố, duy trì quyền truy cập tới AD:
  - Dump NTDS.dit file
  - Tạo tài khoản "domain administrator"
  - Tạo Skeleton Key
  - Sử dụng DCSync hoặc DCShadow
  - Tạo "golden ticket"

Obtaining Access to Back-up NTDS.dit File

- Domain password hashes được lưu trữ trong ntds.dit.
- Ntds.dit yêu cầu đặc quyền để truy cập và bị "khóa" bởi OS khi DC đang chạy.
- ntds.dit được mã hóa bởi system key (lưu trữ trong registry)
- Có nhiều cách để truy cập tới ntds.dit
  - Sử dụng Volume Shadow Copy Service để tạo read-only copy.
  - Sử dụng ntdsutil.exe và tính năng "Install from Media (IFM)".
  - Bản backups được bảo mật không tốt.
- Cần sử dụng công cụ để "giải mã" và trích xuất hash (vd như secretsdump.py trong bộ công cụ Impacket).

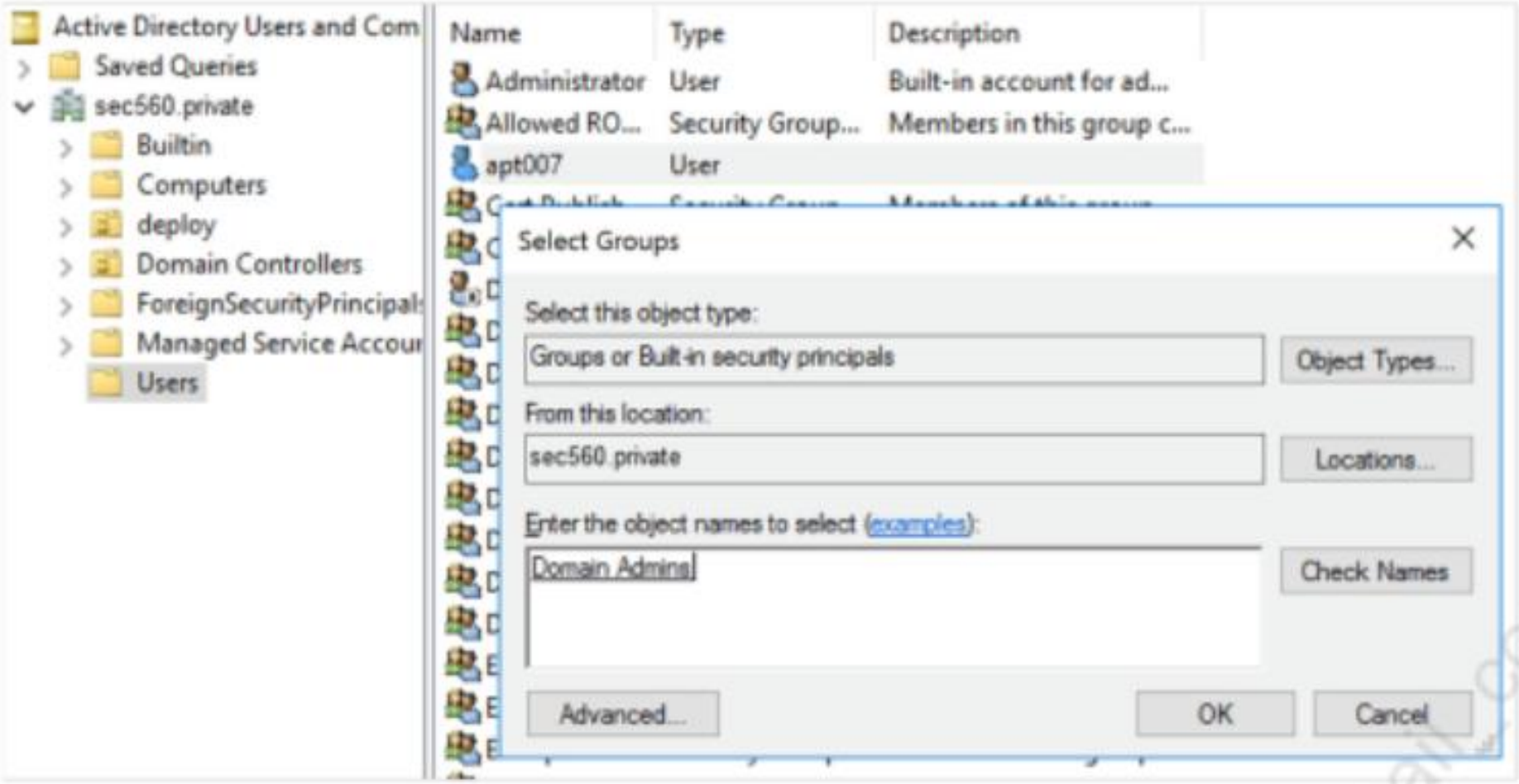
NTDSUtil

```
C:\> ntdsutil.exe
ntdsutil.exe: activate instance ntds
Active instance set to "ntds".
ntdsutil.exe: ifm
ifm: create full c:\temp
Creating snapshot...
...trimmed for brevity...
Initiating DEFRAGMENTATION mode...
     Source Database: C:\$SNAP_202112131421_VOLUMEC$\Windows\NTDS\ntds.dit
     Target Database: c:\temp\Active Directory\ntds.dit

                Defragmentation  Status (% comp

          0    10   20   30   40   50   60   70
          |----|----|----|----|----|----|----|---
          ....................................

Copying registry files...
Copying c:\temp\registry\SYSTEM
Copying c:\temp\registry\SECURITY
Snapshot {c6091d4b-1775-46ab-9158-36cfb2385133} u
IFM media created successfully in c:\temp
ifm: quit
ntdsutil.exe: quit

C:\> ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\temp' q q
```



Oneliner version

Creating a Domain Admin Account



Skeleton Key

- Skeleton key cho phép mở toàn bộ khóa.
- Khi Mimikatz "skeleton key attack" được thực thi, một đoạn mã (backdoor) sẽ được "patch" vào bộ nhớ của tiến trình LSA cho phép đăng nhập tất cả các tài khoản với một mật khẩu đặc biệt "mimikatz".
  - Việc này không loại bỏ mật khẩu cũ, việc đăng nhập vào một tài khoản có thể sử dụng 2 mật khẩu khác nhau (real,fake).
- Skeleton Key chỉ hoạt động với "Kerberos RC4 encryption"
- Do "patch" vào memory nên đơn giản chỉ cần "reboot" lại DC là sẽ loại bỏ được "skeleton key".

Skeleton Key in Action

- Cài đặt Skeleton key với mimikatz.
- Cho phép người dung bất kỳ xác thực với mật khẩu "mimikatz" (không có tùy chọn để thay đổi mật khẩu này trừ khi biên dịch lại mimikatz).

Replicating the Domain: DCSync

- Vì một vài lý do, nhiều ADs sử dụng cùng lúc nhiều DC và thực hiện cập nhật thông qua "AD Replication"
- Mimikatz "dcsync" sẽ mạo danh DC và gửi yêu cầu "replication" tới DC mục tiêu để có được thông tin xác thực được lưu trữ trong AD database
  - Tấn công này yêu cầu quyền Domain Admin hoặc quyền thực hiện "replication"
- Mức độ ảnh hưởng tương tự việc copy tệp tin ntds.dit, cho phép chúng ta lấy được tất cả "password hash"

Replicating the Domain: DCSync Example

```
mimikatz # lsadump::dcsync /user:administrator
[DC] 'sec560.private' will be the domain
[DC] 'WIN-PGF4RHUE40J.sec560.private' will be the DC server
[DC] 'administrator' will be the user account

Object RDN              : Administrator

** SAM ACCOUNT **

SAM Username            : Administrator
Account Type            : 30000000 ( USER_OBJECT )
User Account Control    : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration      : 1/01/1601 2:00:00
Password last change    : 10/07/2017 19:26:57
Object Security ID      : S-1-5-21-1737389956-3911202689-1728583289-500
Object Relative ID      : 500

Credentials:
 Hash NTLM: ae974876d974abd805a989ebead86846
   ntlm- 0: ae974876d974abd805a989ebead86846
   ntlm- 1: e19ccf75ee54e06b06a5907af13cef42
   lm  - 0: b84c6269fc243eefa5a4c667a7ec9656

Supplemental Credentials:
* Primary:NTLM-strong-NTOWF *
    Random Value : 6f537d1aecba5db626dbdfea767a84f3
```

- Yêu cầu hash với lsadump::dcsync /user:[username]
- Yêu cầu krbtgt hash cho phép tạo "Golden ticket"

Becoming a Domain Controller: DCShadow

- Tấn công DCShadow thực hiện qua 4 bước chính sau
  - Phải có quyền "Domain Administrator".
  - Sử dụng mimikatz để đăng ký máy trạm đang sử dụng (workstation) là DC.
  - Kẻ tấn công tạo ra sự thay đổi có lợi (ví dụ: thay đổi password hash của tài khoản nhạy cảm).
  - Sử dụng mimikatz, chúng ta có thể "trigger" việc thực hiện "replication" $\rightarrow$ ép DC hợp lệ phải thực hiện "commit the change".

Becoming a DC: DCShadow in Action

- Thực hiện trong ngữ cảnh "NT AUTHORITY\SYSTEM"

  mimikatz#token::elevate

- Example: thay đổi mô tả của người dung Bob

  mimikatz#lsadump::dcshadow /object: "CN=Bob, OU=Users, DC=domain, DC=com" /attribute: description /value: "DCShadow was here"

- Example: Thêm người dùng vào Domain Admins group

  mimikatz#lsadump::dcshadow /object: "CN=Bob, OU=Users, DC=domain, DC=com" /attribute: primaryGroupID /value: 512

- Push change to the Domain:

  mimikatz#lsadump::dcshadow /push

Abusing Active Directory Certificate Service

- Tại Blackhat 2021, nhóm nghiên cứu SpectreOp chỉ ra rằng lỗi cấu hình (misconfiguration) trong AD CS có thể dẫn tới việc các thông tin xác thực bị đánh cắp, leo thang đặc quyền (local và domain) và duy trì quyền truy cập.
  - https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf

Content

- Kerberos
- Kerberoasting
- More Kerberos Attacks
- Domain Dominance
- **Silver Ticket**
- Golden Ticket
- Domain Privilege Escalation

Overview (1/2)

- Service Ticket (ST) được mã hóa và ký số bởi "service account's hash" điều đó có nghĩa nếu ta có "service account's password/hash" thì ta có thể giả mạo Service Ticket.
- Chúng ta có thể sửa đổi PAC để leo thang đặc quyền.
  - Thay đổi username, thậm chí "username" không tồn tại.
  - Sửa "SID, group membership".
- Silver Ticket là việc "giả mạo Service Ticket", Golden Ticket là việc "giả mạo TGT".

Overview (2/2)

- PAC có 2 signature
  - 1-st signature sử dụng "service's password hash" (chúng ta có -> từ đâu????).
  - 2-nd signature sử dụng "krbtgt's account hash". Nếu chúng ta không có hash này thì chúng ta không thể giả mạo chữ ký số 2. Tuy nhiên krbtgt signature này chỉ được kiểm tra trên một số service.
    - Service account với **SeTcbPrivilege**, account "run as part of OS" (ví dụ SYSTEM account) sẽ không kiểm tra krbtgt signature.
    - CIFS (SMB), HOST, MSSQLSvc (SQL Server), TERMSRV không kiểm tra. Tuy nhiên HTTP với IIS luôn kiểm tra.

Service Ticket and PAC

Service Ticket: Encrypted using target service NT Hash

Start / End / MaxRenew: 05/12/2024 07:12:18 ; 05/12/2024 17:12:18 ; 12/12/2024 07:12:18 ;
Service Name: cifs; file01.hiboxy.com
Target Name: cifs; file01.hiboxy.com
Client Name: bob; hiboxy.com
Flags: 40e10000
Session Key: 0x000000 12eb212eb23ca12eb23c 45eb4124af9010bf13f…<snip>

Privilege Attribute Certificate (PAC)
Username: bob
SID: S-1-5-21-409 … <snip>
Groups: Users … <snip>

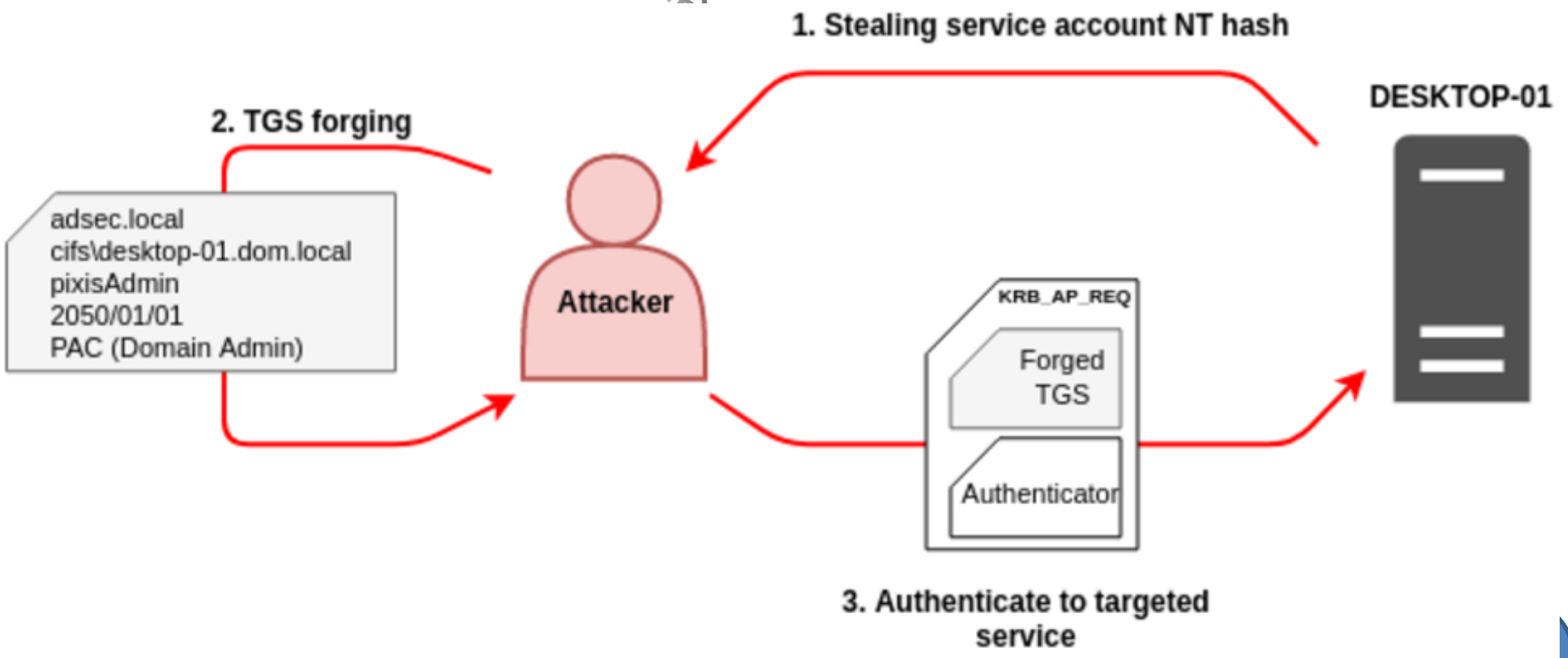
Signed using service's NT hash

Signed using KDC LT Key (krbtgt)

- Kerberos là một giao thức phi trạng thái (stateless protocol). Tất cả thông tin được lưu trữ trong "tickets"
- 2-nd signature (krbtgt) không phải lúc nào cũng được kiểm tra. Điều này cho phép thực hiện tấn công "Silver ticket"

Generating a Silver Ticket with Impacket (1/2)

- Để tạo ra "Silver ticket" chúng ta cần:
  - NT password hash của service account
  - Domain SID (S-1-5-21-XX-YY-ZZ)
  - SPN



Generating a Silver Ticket with Impacket (2/2)

- Sử dụng ticketer.py trong bộ công cụ Impacket

```
ticketer.py –spn SPN –domain-sid SID –nthash NTLM –dc-ip IP_VICTIM –domain DOMAIN USERNAME
```

- Tạo Silver ticket cho người dùng Adminstrator

```
ticketer.py –spn MSSQLSvc/dc1.sec560.local –domain-sid S-1-5-21-721047592-4068106649-2889670365 –nthash b999a16500b87d17ec7f2ea68778f05 –dc-ip dc1.sec560.local –domain sec560.local Administrator
```

Silver Ticket Use

- Linux
  - Thiết lập biến môi trường KRB5CCNAME (để Linux biết sử dụng ticket khi xác thực)

    export KRB5CCNAME=[TGS_ccache_file]
  - Sau đó sử dụng công cụ bất kỳ có khả năng sử dụng xác thực Kerberos

    wmiexec.py [domain]/[user]@[hostname] –k –no-pass
- Windows
  - Sử dụng Mimikatz để tải ticket vào bộ nhớ (Mimikatz cũng có thể tạo "silver ticket"): kerberos::ptt [ticket_file]
  - Sử dụng Rubeus: Rubeus.exe ptt /ticket:[ticket_file]

Content

- Kerberos
- Kerberoasting
- More Kerberos Attacks
- Domain Dominance
- Silver Ticket
- **Golden Ticket**
- Domain Privilege Escalation

Golden Ticket

- "Golden ticket" là một "TGT giả mạo" được tạo ra bởi attacker và ký bởi "krbtgt hash".

TGT: Encrypted using KDC LT key (krbtgt NT hash)

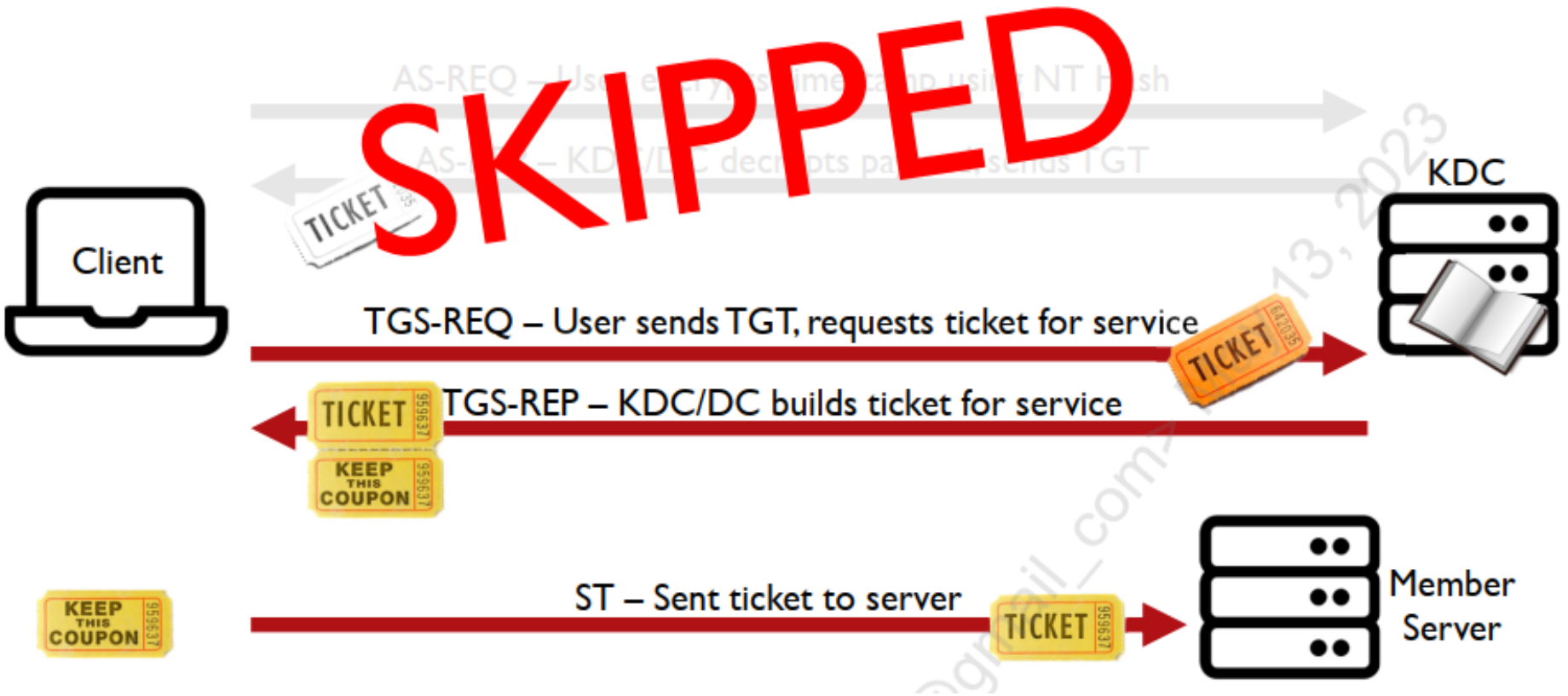
Start / End / MaxRenew: 05/12/2022 07:12:18 ; 05/12/2022 17:12:18 ; 12/12/2022 07:12:18 ;
Service Name: krbtgt; sec560.private
Target Name: krbtgt; sec560.private.com
Client Name: erik; sec560.private
Flags: 40e10000
Session Key: 0x00000012eb212eb23ca12eb23c45eb4124af9010bf13f…<snip>

Privilege Attribute Certificate (PAC)
Username: tim
SID: S-1-5-21-409 … <snip>
Groups: Domain Admins … <snip>

Signed using Target LT Key
Signed using KDC LT Key

Both signatures use the krbtgt hash

Kerberos Flow with Golden Ticket



Golden Ticket Properties

- Golden Ticket được tạo mà không có bất kỳ sự tương tác nào với DC.
  - Điều này là hoàn toàn có thể do Kerberos là "stateless protocol".
  - DC không theo dõi các "TGT" được tạo trước đó.
  - Chúng ta cần "krbtgt hash" để tạo "ticket".
- TGT thường dành cho tài khoản quản trị (RID 500 trong domain hoặc Domain Administrator).
- Nó thường có giá trị trong một khoảng thời gian dài (mặc định 10 năm).

Golden Ticket Tools

- Chúng ta có thể sử dụng nhiều công cụ khác nhau để tạo ra "Golden ticket".
  - Ticketer.py (Impacket); Mimikatz; C2 frameworks
- Để tạo ra "Golden ticket" chúng ta cần:
  - NT password hash của krbtgt account
  - Domain SID (S-1-5-21-XXXXXXXXX-YYYYYYYYY-ZZZZZZZZZ)
  - Full domain name

```
ticketer.py –domain-sid S-1-5-21-721047592-4068106649-2889670365 –domain sec560.local –nthash 5525e655c…e2cc5621fb3 Administrator
```

Content

- Kerberos
- Kerberoasting
- More Kerberos Attacks
- Domain Dominance
- Silver Ticket
- Golden Ticket
- **Domain Privilege Escalation**

PowerView Find-InterestingDomainShareFile

- PowerView Find-InterestingDomainShareFile
- Xác định các file được chia sẻ sau đó:
  - Tìm kiếm các file có thể truy cập được bởi người dùng hiện tại
  - Tìm kiếm các file có chứa: thông tin đăng nhập, mật khẩu, cấu hình, VMDK (*cred*, *password*, *config*, *vmdk*)

PowerView Find-LocalAdminAccess

- PowerView Find-LocalAdminAccess
  - Tìm kiếm các hosts mà người dùng hiện tại có khả năng truy cập dưới quyền "local administrator"

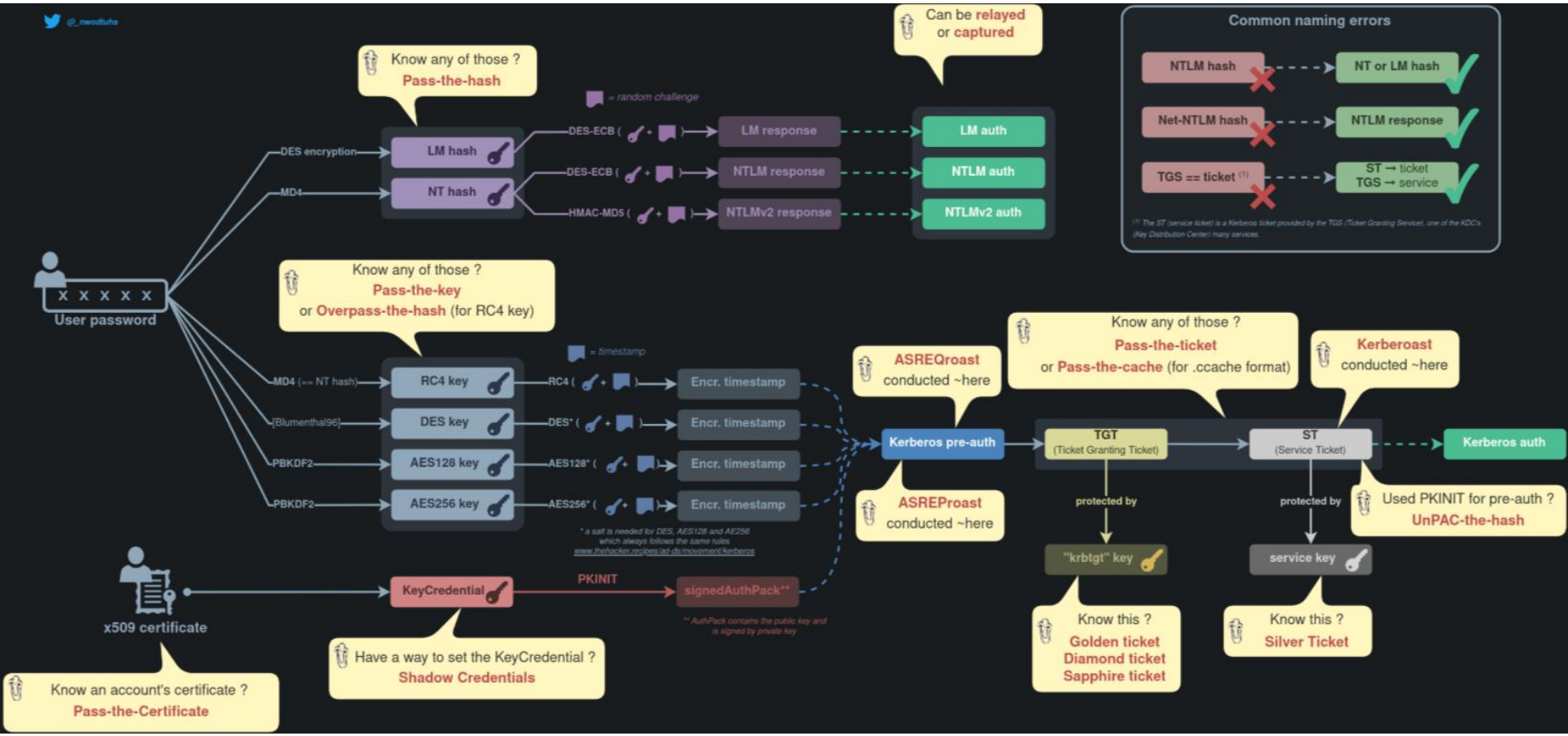
Privilege Escalation (1/2)

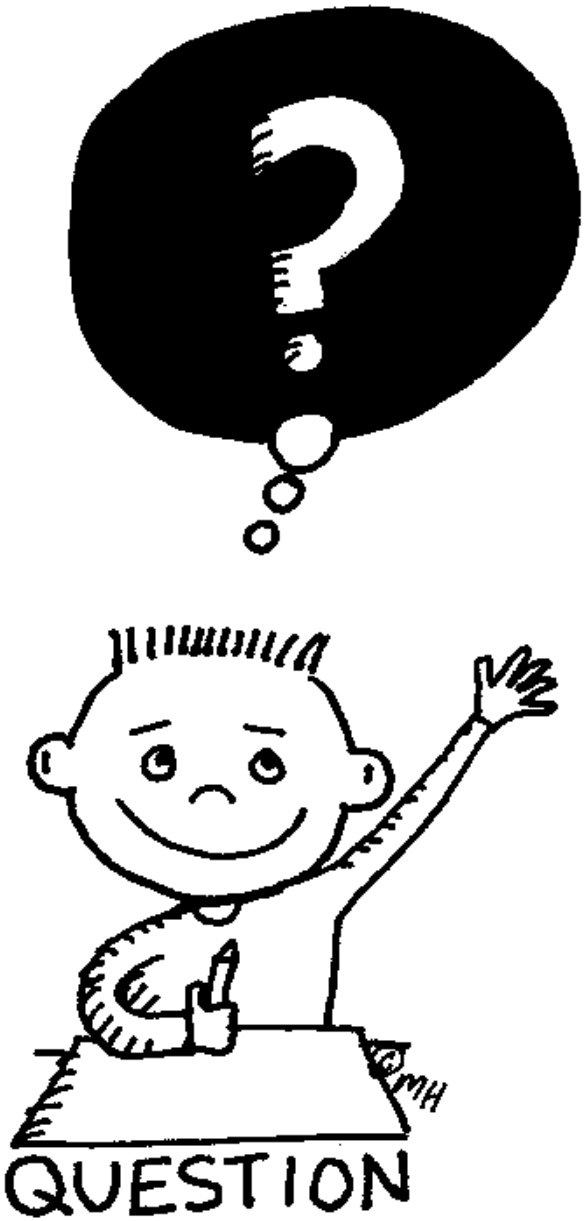
- Process Memory Dumps
  - Yêu cầu "local admin" hoặc "SYSTEM level access"
  - Có thể thu được dưới dạng bản rõ hoặc hash
  - Phương pháp
    - Sysinternals Procdump hoặc Process Explorer
    - Task Manager
    - RunDLL32 with Comsvcs.dll
    - PowerSploit Out-MiniDump
    - Direct System Calls/ Windows API Calls

Privilege Escalation (2/2)

- Một vài kỹ thuật đã thảo luận có thể được sử dụng:
  - Kerberos Attacks
  - Kerberoasting
  - AS-REP Roasting

Kerberos Attack




QUESTION