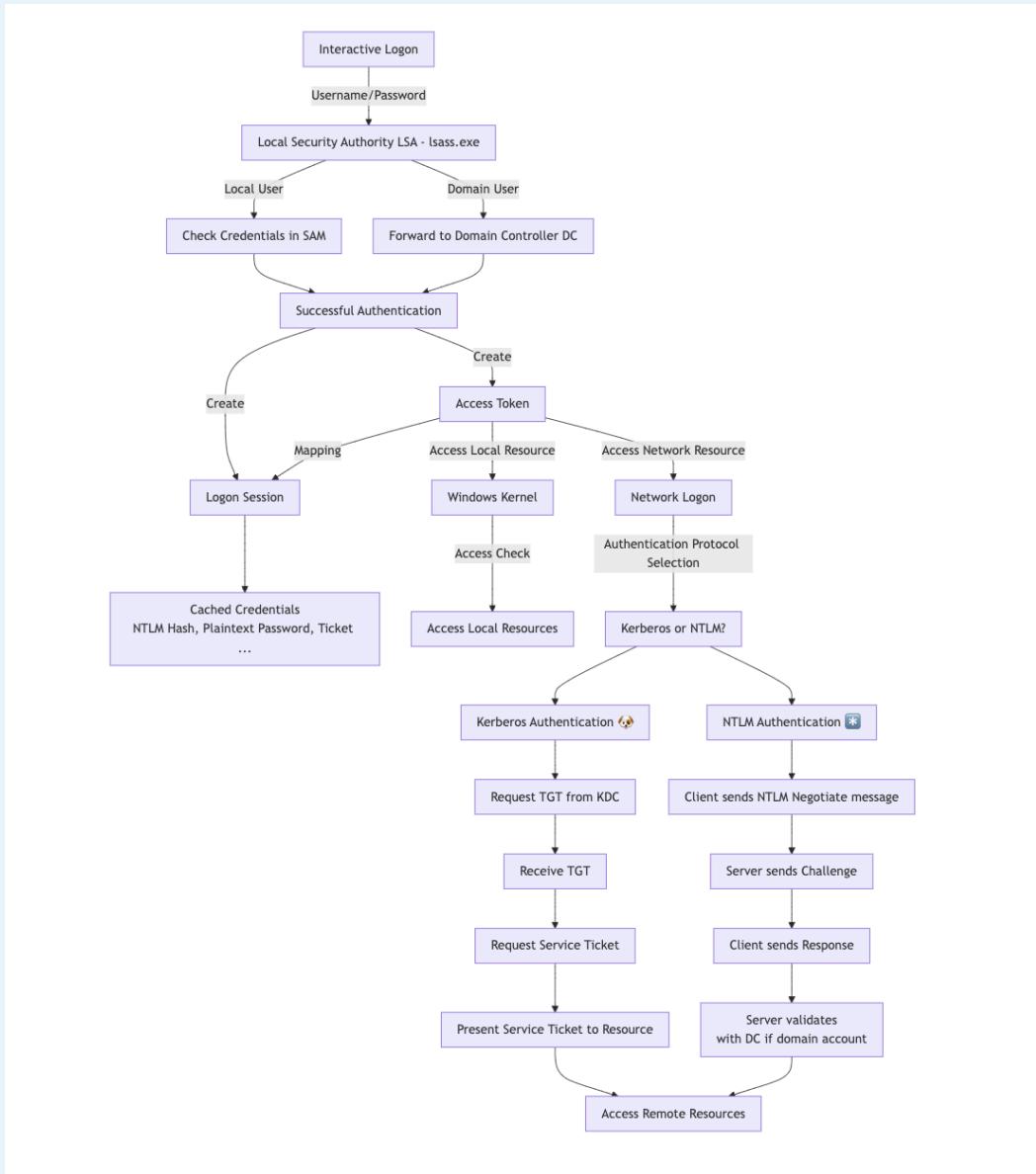




Authentication Attack: Kerberos

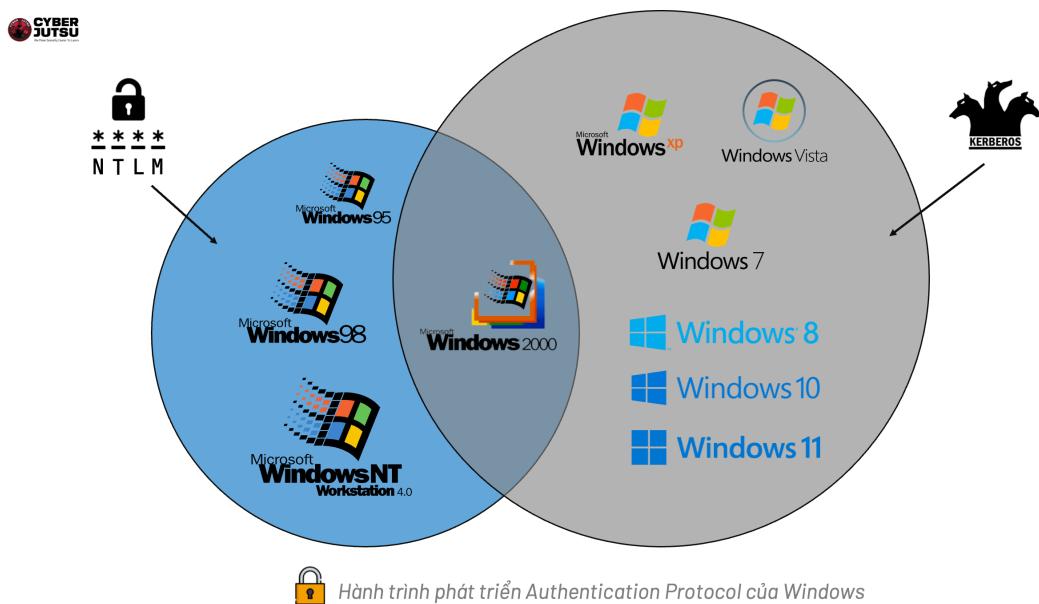
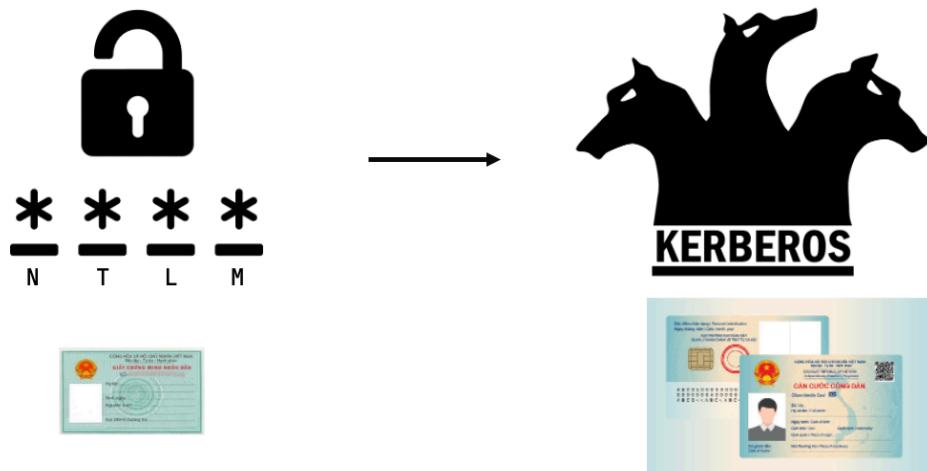
Phiên bản mở rộng của Windows Logon Flow

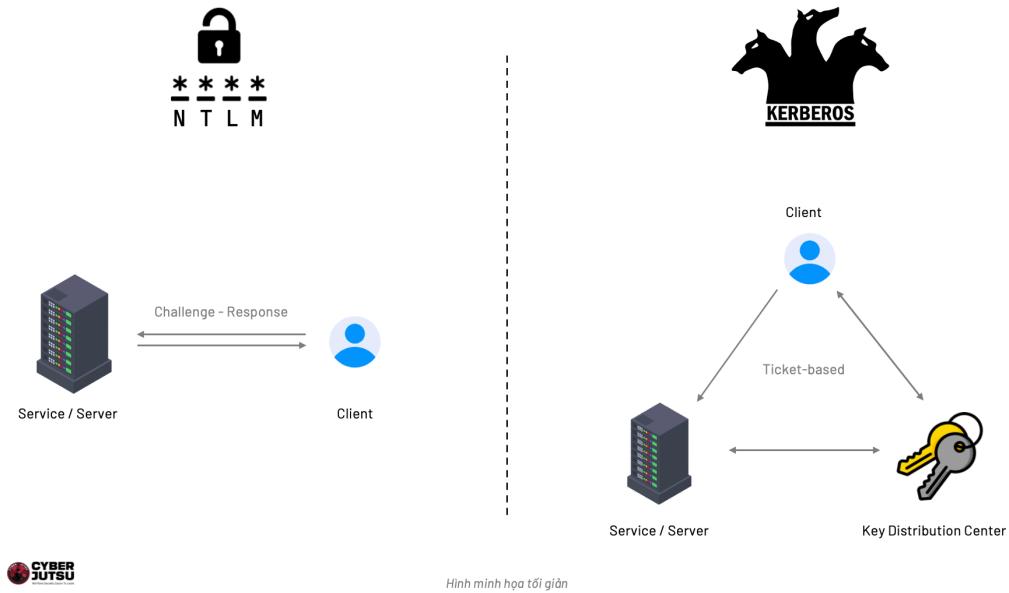


Mermaid live [here](#)

Lý thuyết

- ▼ Sự Cải Tiến của Kerberos so với NTLM: Lý Do Chuyển Đổi





Phải chăng “Kerberos” chó ba đầu ở đây ý nghĩa là: Có thêm vai trò thứ 3 trong quá trình xác thực, để từ đó giải quyết được những nút thắt của giao thức xác thực cũ NTLM.

Việc chuyển đổi từ NTLM sang Kerberos đem lại nhiều lợi ích về security, efficiency và user experience. Mặc dù quá trình chuyển đổi có thể gặp thách thức với các legacy systems, nhưng lợi ích lâu dài về an ninh và hiệu suất là đáng kể. Microsoft đang dần loại bỏ NTLM để ưu tiên Kerberos.

1. Support for Modern Environments:

- NTLM: Hạn chế trong việc hỗ trợ các tính năng bảo mật hiện đại.
- Kerberos: Được thiết kế để hỗ trợ các yêu cầu bảo mật hiện đại và tương lai.

2. Reduced Credential Exposure:

- NTLM: Việc cung cấp thông tin đăng nhập nhiều lần tăng nguy cơ bị đánh cắp.
- Kerberos: Thông tin đăng nhập chỉ được cung cấp một lần trong quá trình xác thực ban đầu.

3. Enhanced Security:

- NTLM: Dễ bị giả mạo do phương pháp xác minh không nhất quán.
- Kerberos: Sử dụng encrypted tickets và timestamps, giảm nguy cơ giả mạo và lạm dụng.

4. Mutual Authentication:

- NTLM: Chỉ xác thực danh tính của người dùng, không xác minh tính hợp lệ của dịch vụ.
- Kerberos: Cung cấp xác thực hai chiều, cả người dùng và dịch vụ đều xác minh lẫn nhau.

5. Single Sign-On (SSO):

- NTLM: Yêu cầu xác thực riêng biệt cho mỗi dịch vụ, gây phiền toái cho người dùng.
- Kerberos: Cho phép người dùng xác thực một lần và truy cập nhiều dịch vụ, cải thiện trải nghiệm người dùng.

6. Centralized Authentication

- NTLM: Mỗi dịch vụ xử lý xác thực độc lập, dẫn đến không nhất quán và kém an toàn.
- Kerberos: Sử dụng Key Distribution Center (KDC) làm trusted third party, đảm bảo tính nhất quán và an ninh.

Kerberos đã trở thành giao thức xác thực ưu tiên trong môi trường Windows, thay thế cho NTLM (NT LAN Manager) cũ hơn. Sự chuyển đổi này được thúc đẩy bởi nhiều cải tiến quan trọng mà Kerberos mang lại:

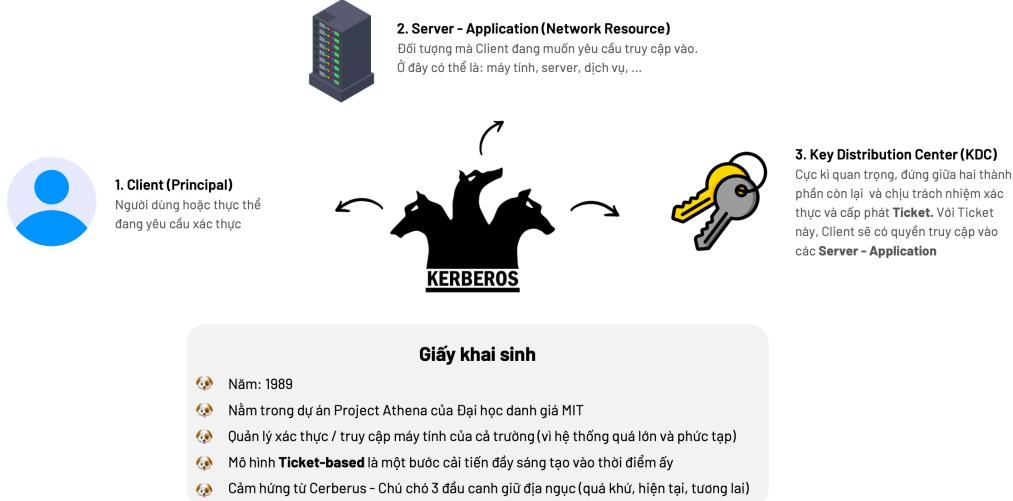
▼ Nguồn gốc và sức mạnh của Kerberos



The Network Authentication Protocol

KERBEROS

nguồn gốc và sức mạnh



- ✓ **Quản lý tập trung**
Mô hình ticket-based khiến cho việc quản lý tập trung dễ hơn, giảm sự phức tạp khi phải quản lý Credentials khắp mạng.
- ✓ **Khả năng scale**
Rất phù hợp cho các tổ chức lớn (giống MIT vào thời bấy giờ).
- ✓ **Security**
Giúp hạn chế các tấn công Relay và tránh lọt Credentials trong mạng so với giao thức cũ là NTLM.
- ✓ **Single Sign-On (SSO)**
Cho phép Client có thể truy cập vào các tài nguyên chỉ bằng một lần nhập Credentials.



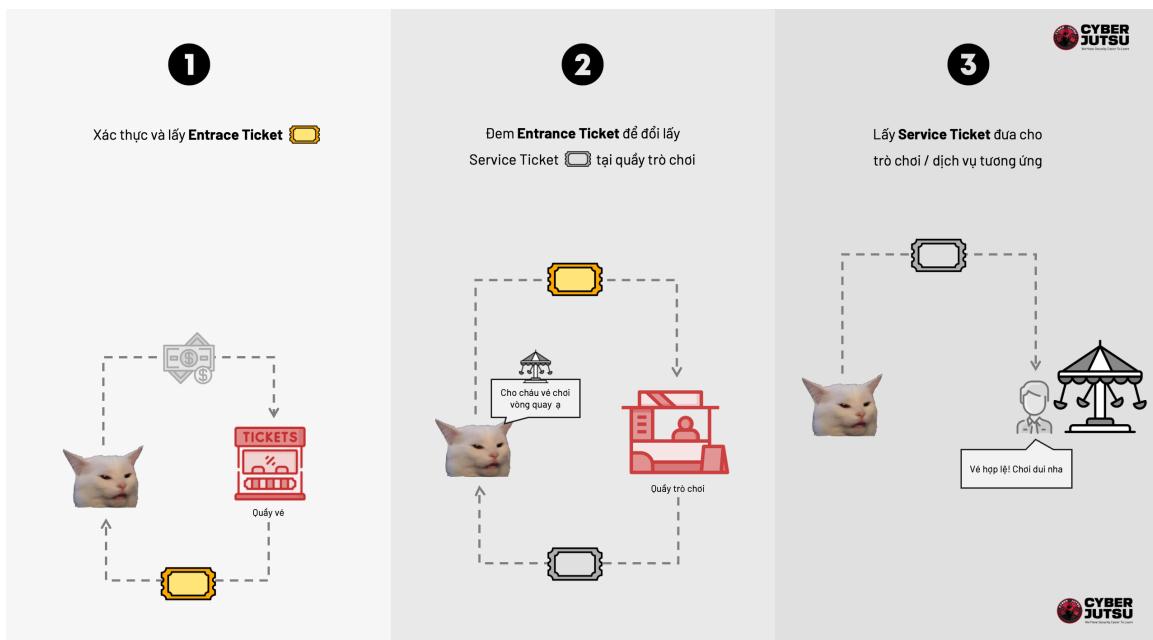
Bản thiết kế vĩ đại...system admin rất yêu

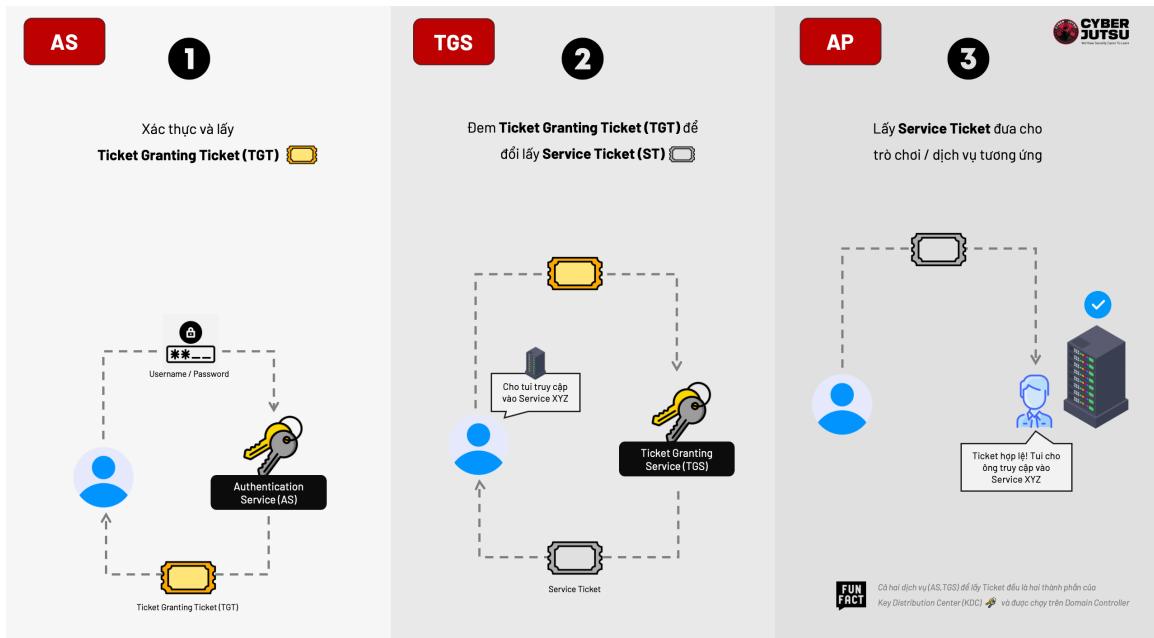
▼ Overview: Kerberos Authentication Flow



KERBEROS == CÔNG VIÊN

Cách Kerberos xác thực cũng khá giống với lúc bạn mua vé ở khu vui chơi

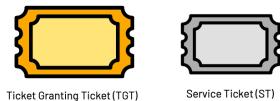




Vé vàng: ý chỉ Ticket Granting Ticket (TGT)

Vé bạc: ý chỉ Service Ticket (ST)

▼ Deep Dive: Kerberos Authentication Flow



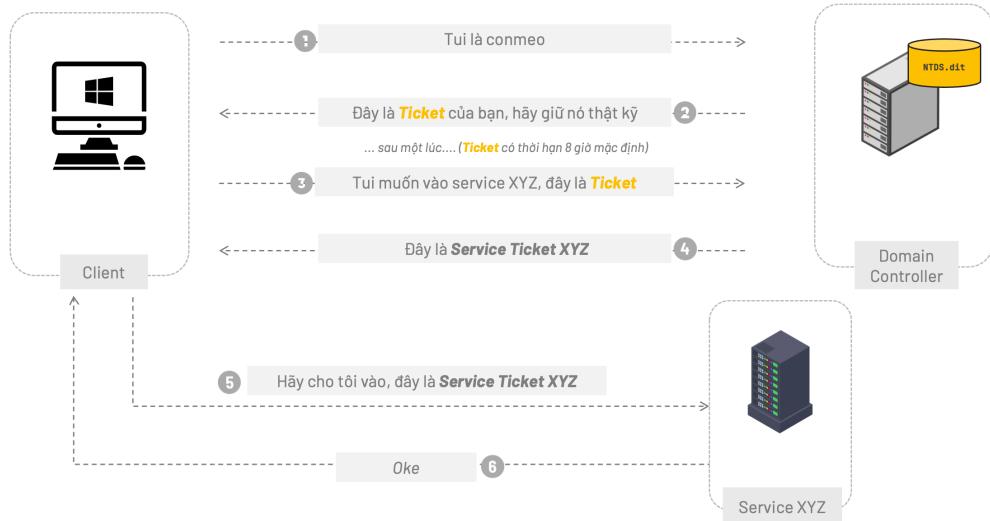
Như thế nào là một ticket hợp lệ?
Cơ chế nào giúp chống giả Ticket?

Để trả lời chỉ có cách chúng ta cùng lặn
sâu vào cách mà Đại học MIT đã thiết kế
ra giao thức này nhé!

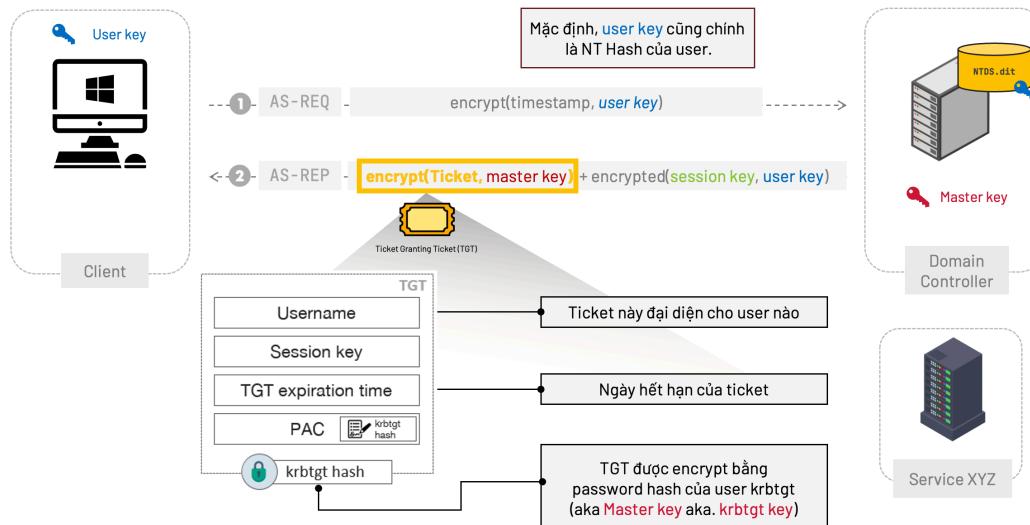




KERBEROS AUTHENTICATION - SIMPLE VERSION

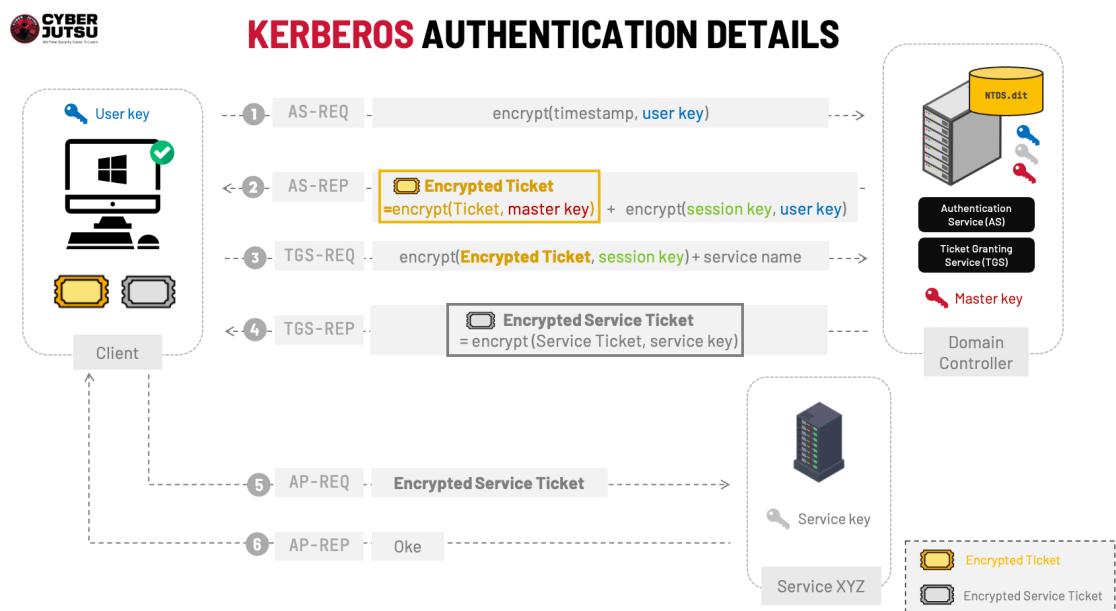


KERBEROS AUTHENTICATION





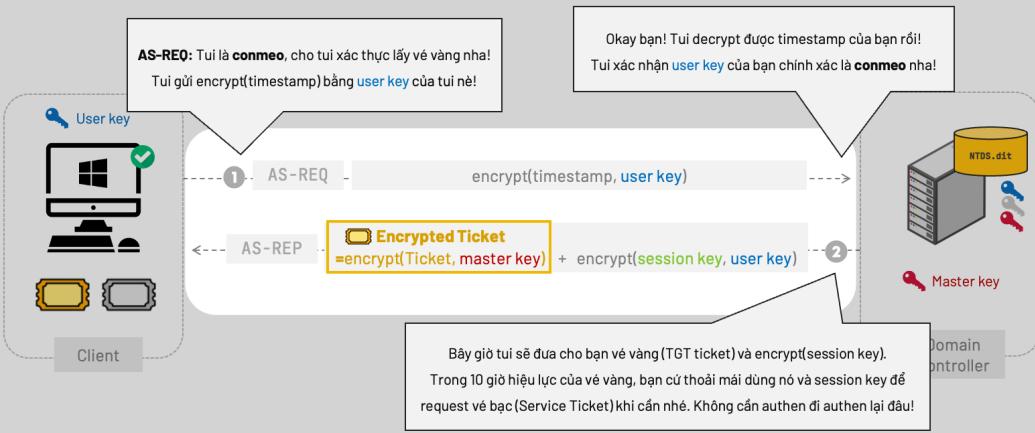
- ☞ Cũng giống như đĩa chơi công viên:
- Vé vàng giúp các quầy trò chơi (service) giảm tải trong việc authen đi authen lại → **Single Sign-On**
 - Bạn không thể mua 1 vé rồi ở đó cả năm luôn đúng không! → **Kiểm soát chặt hơn**
 - Nhỏ vé vàng bị mất hoặc trộm thì chỉ có tác dụng trong 10 giờ thôi → **Hạn chế tấn công Pass-The-Hash, Relay, Force Authen,...**
 - Buộc tất cả mọi người phải quay lại xác thực sau mỗi chu kỳ → **Dễ quản lý và cập nhật hơn**



▼ Ý nghĩa của thiết kế: Kerberos Authentication Flow

Ý NGHĨA CỦA BƯỚC 1-2

User xác thực để lấy vé vàng, vé vàng này sẽ đại diện cho phiên đăng nhập của user trong 10 giờ



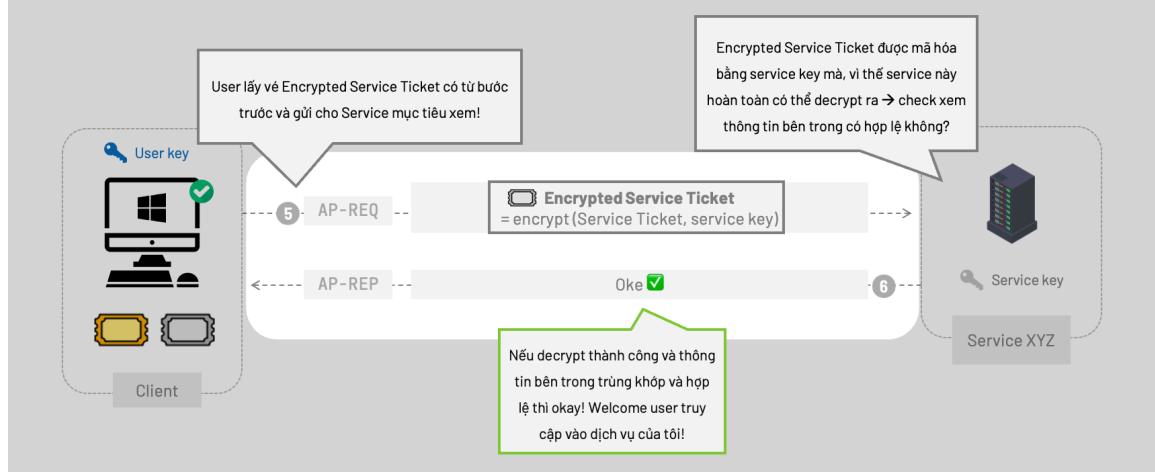
Ý NGHĨA CỦA BƯỚC 3-4

Sau một lúc... user bỗng có nhu cầu truy cập vào một service nào đó



Ý NGHĨA CỦA BƯỚC 5-6

User lấy vé bạc của DC đưa để show cho Service XYZ rằng mình có quyền truy cập

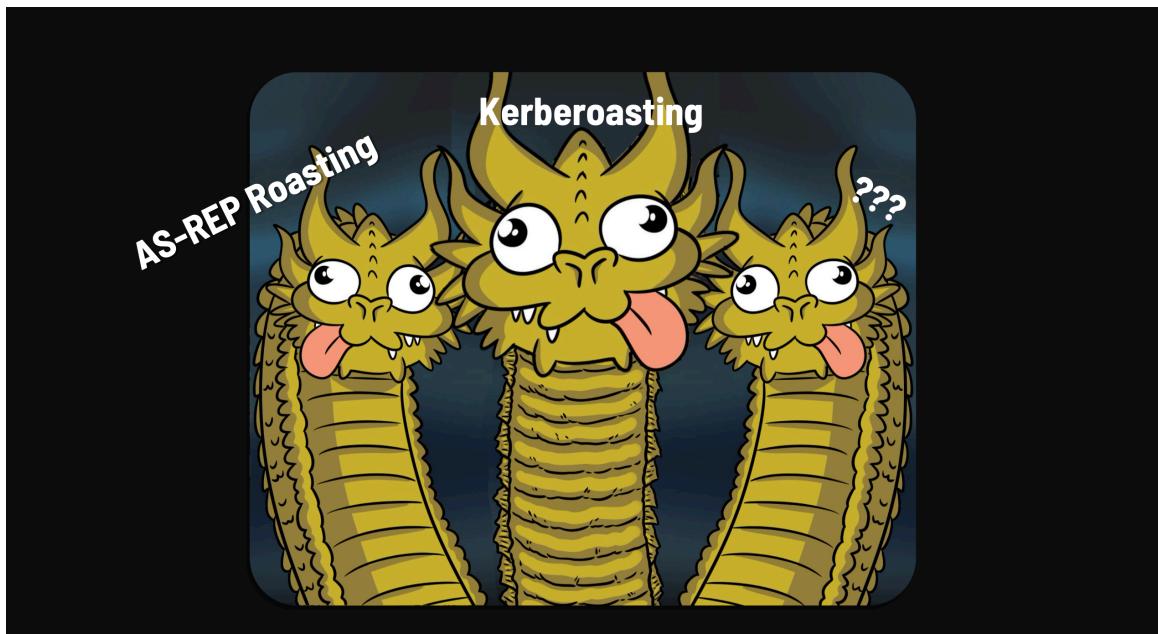


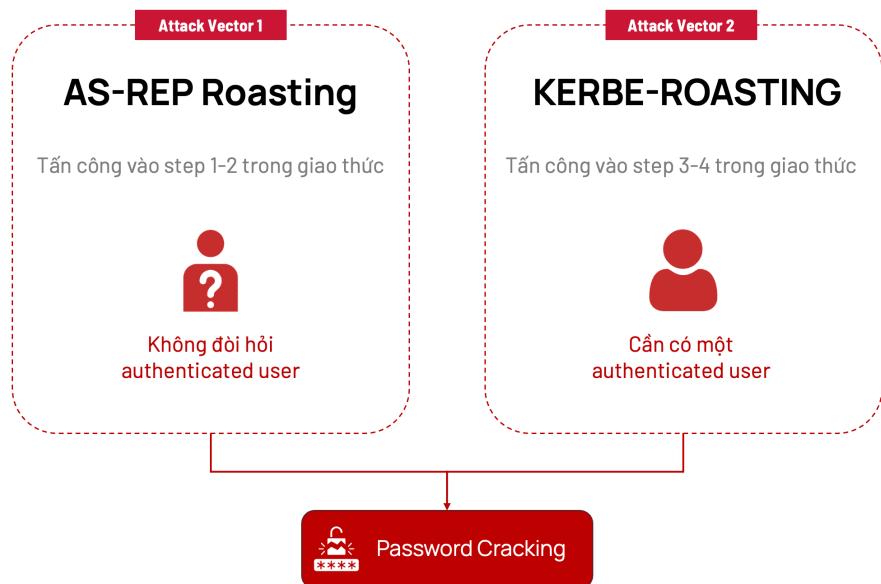
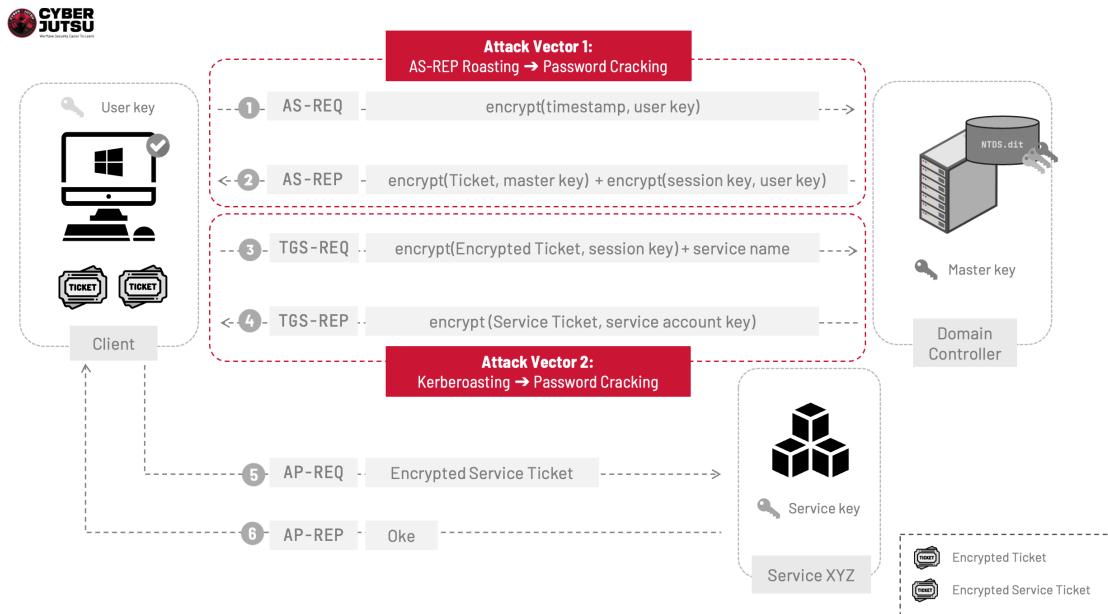
Attack vectors

- ▼ Attack Vector: Overview các cách tấn công



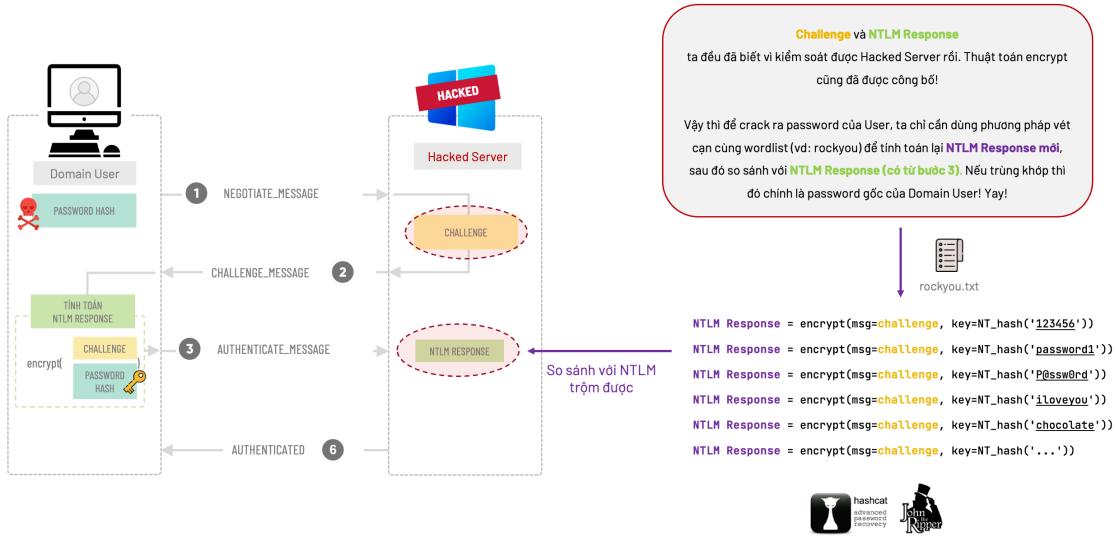
KEBEROS AUTHENTICATION ATTACK VECTOS





▼ Recap: Nguyên lý Password Cracking trong NTLM Response

RECAP: CÁCH PASSWORD HASH CRACKING TRONG NTLM



▼ Attack Vector 1: AS-REP Roasting

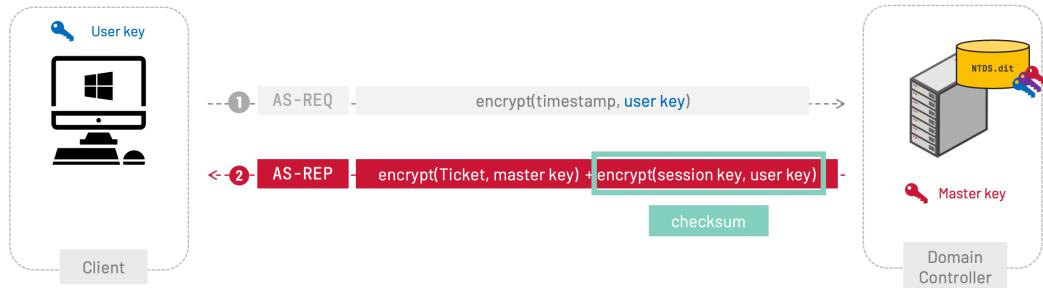


AS-REP Roasting

- Với attack vector này, attacker có thể chiếm được password của bất kì victim user nếu user đó bị misconfiguration.
- Thường được dùng khi chưa chiếm được domain account nào



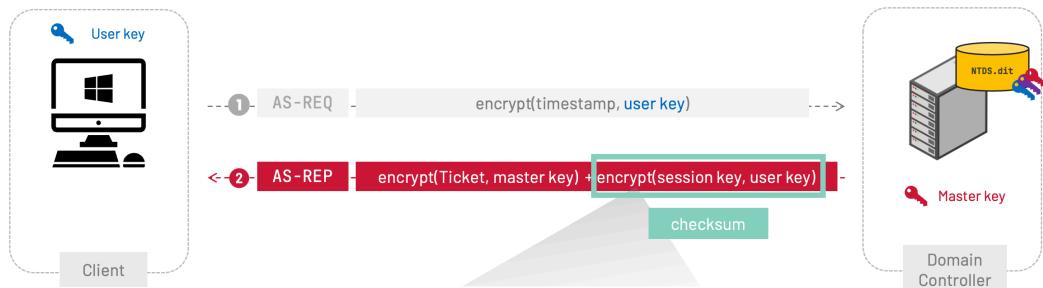
AS-REP ROASTING



Bước ① và ② trong Kerberos được gọi là giai đoạn Pre-auth.

Nghĩa là user phải gửi thông tin xác thực thì Domain Controller mới gửi Ticket về.

AS-REP ROASTING





AS-REP ROASTING

- Admin có thể cấu hình để **tắt** chế độ pre-auth cho một user 😊
- Với tickbox này bật lên cho user nào, thì hacker có thể yêu cầu DC đưa cho Ticket trên danh nghĩa của user đó mà không cần preauthentication
- Sau đó tiến hành crack thành phần bên trong ticket, nếu may mắn sẽ có được mật khẩu của user đấy.
- "Feature" này được dùng để debug và support một số hệ thống cũ (legacy system)!

demo_asrep Properties

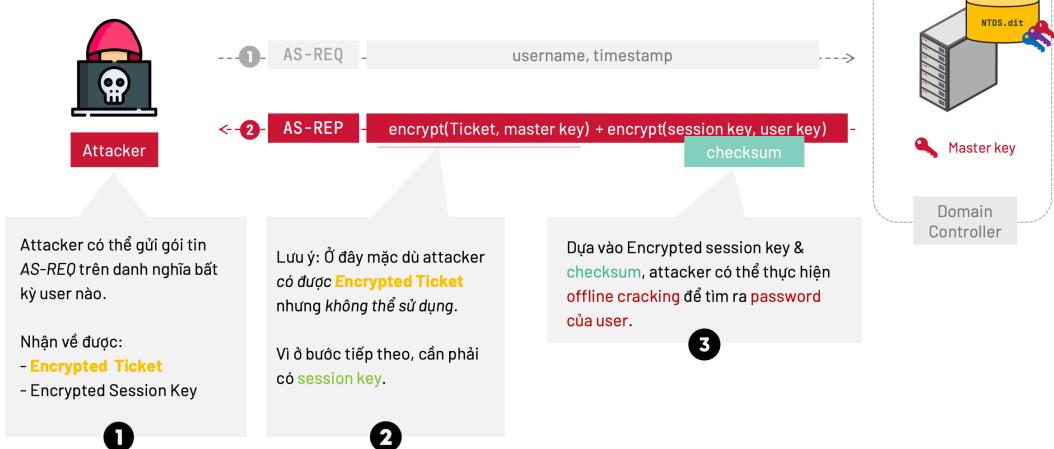
Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile	COM+	
General	Address	Account	Profile
Logon Hours...		Log On To...	
<input type="checkbox"/> Unlock account			
Account options:			
<input type="checkbox"/> Use only Kerberos DES encryption types for this account			
<input type="checkbox"/> This account supports Kerberos AES 128 bit encryption.			
<input type="checkbox"/> This account supports Kerberos AES 256 bit encryption.			
<input checked="" type="checkbox"/> Do not require Kerberos preauthentication			
Account expires			
<input checked="" type="radio"/> Never			
<input type="radio"/> End of: Tuesday , October 15, 2024			

OK Cancel Apply Help

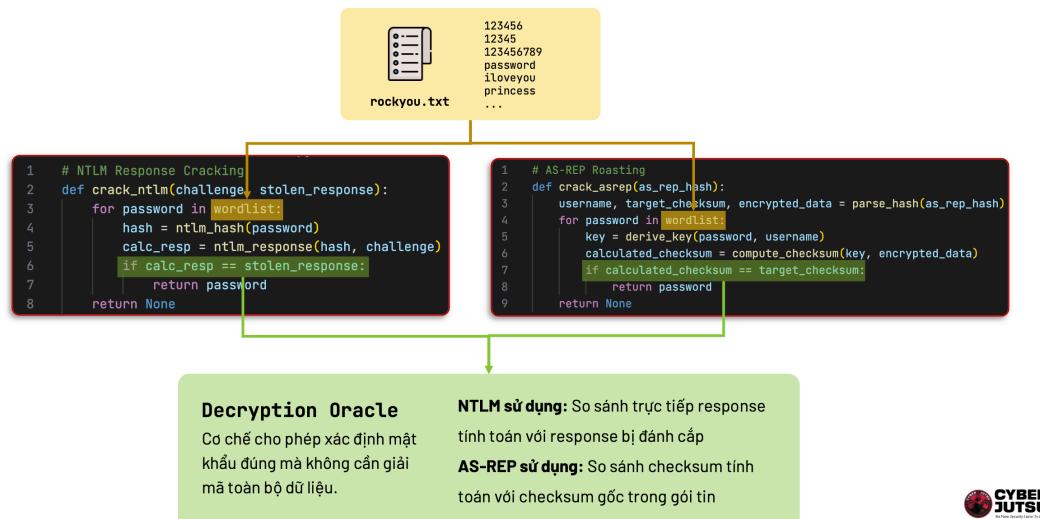


AS-REP ROASTING

Khi không cần Pre-Auth, Kerberos sẽ hoạt động như sau

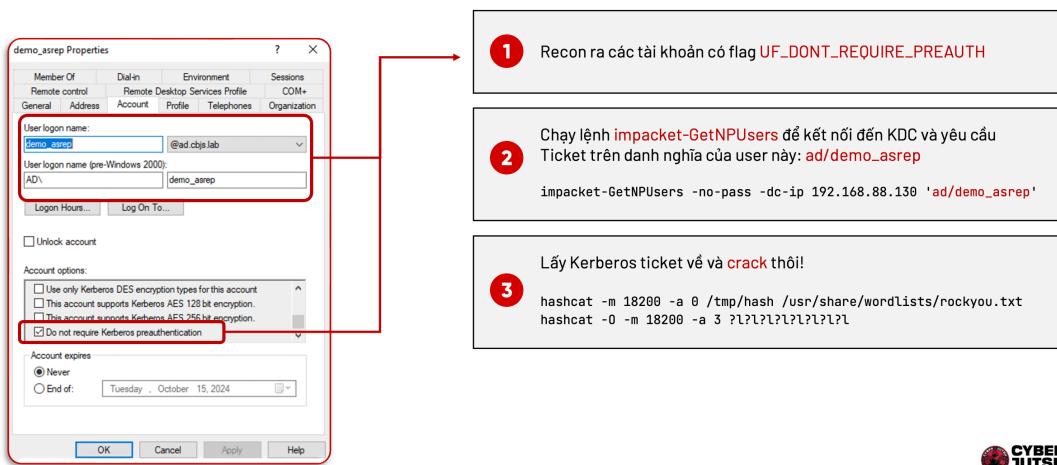


SO SÁNH QUÁ TRÌNH OFFLINE PASSWORD CRACKING: NTLM vs. AS-REP



AS-REP Roasting Attack Flow.

Exploit những tài khoản không có Kerberos preauthentication



- Liên quan đến việc tấn công tài khoản người dùng 
 - Kẻ tấn công yêu cầu dịch vụ **Authentication Service (AS)** của Kerberos tạo một thông báo **AS-REP** cho người dùng có cờ UF_DONT_REQUIRE_PREAUTH
 - **AS-REP** chứa thông tin được mã hóa bằng mật khẩu của người dùng. Kẻ tấn công có thể trích xuất AS-REP và thực hiện brute-force hoặc dictionary attack để crack mật khẩu.
 - Reference code crack:

- <https://github.com/HarmJ0y/ASREPRoast/blob/master/tgscrack.go#L109C8-L109C8>

▼ Attack Vector 2: Kerberoasting 🔒



Kerberoasting

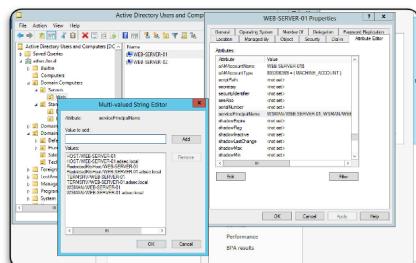
- Tóm lại:
- Thường được dùng sau khi đã chiếm được một user.
- Với attack vector này, attacker có khả năng crack được password của Service Account.
- Tấn công này nhắm vào tài khoản dịch vụ do con người quản lý, không phải tài khoản máy tính (vì tài khoản máy tính password rất random - không thể crack nổi)



Service Account

Khái niệm SPN

- SPN: Service Principal Name
- Một máy chủ có thể có nhiều service chạy cùng lúc → SPN ra đời để định danh chính xác
- SPN được lưu trữ như một thuộc tính của đối tượng trong Active Directory
- Kerberos sử dụng SPNs để cấp đúng ticket cho đúng dịch vụ.



Cấu trúc:

- Định dạng cơ bản: service_class/hostname_or_FQDN
- Có thể thêm port: service_class/hostname_or_FQDN:port

Thành phần:

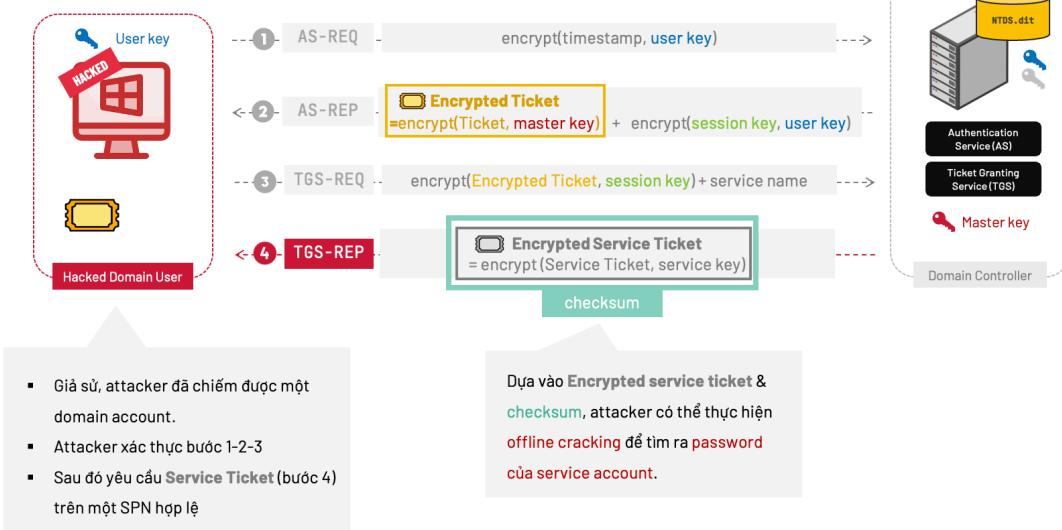
- Service class: Tên chung cho loại dịch vụ (ví dụ: www, SQLServer)
- Hostname: Tên máy chủ hoặc FQDN (Fully Qualified Domain Name)

Ví dụ:

- www/WEB-SERVER-01
- www/WEB-SERVER-01.adsec.local

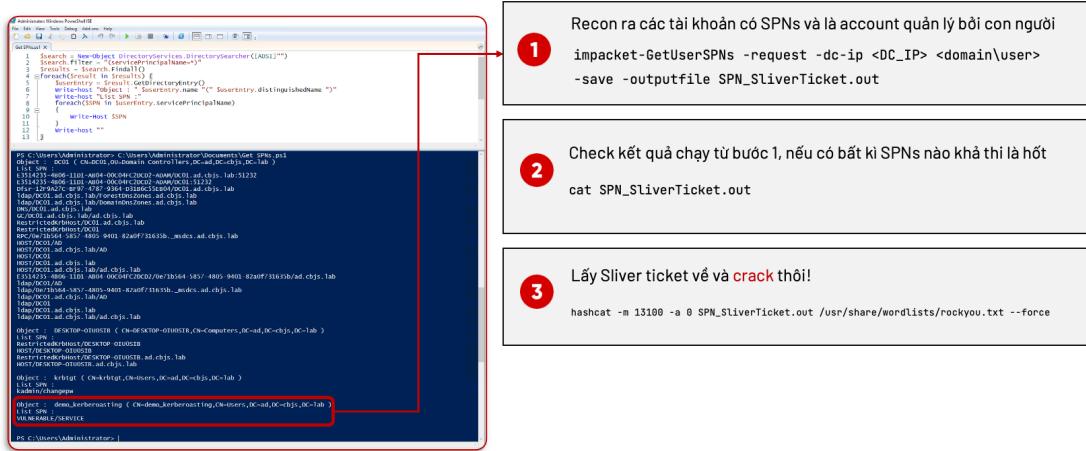


KERBEROASTING



Kerberoasting Attack Flow.

Exploit những tài khoản có SPN

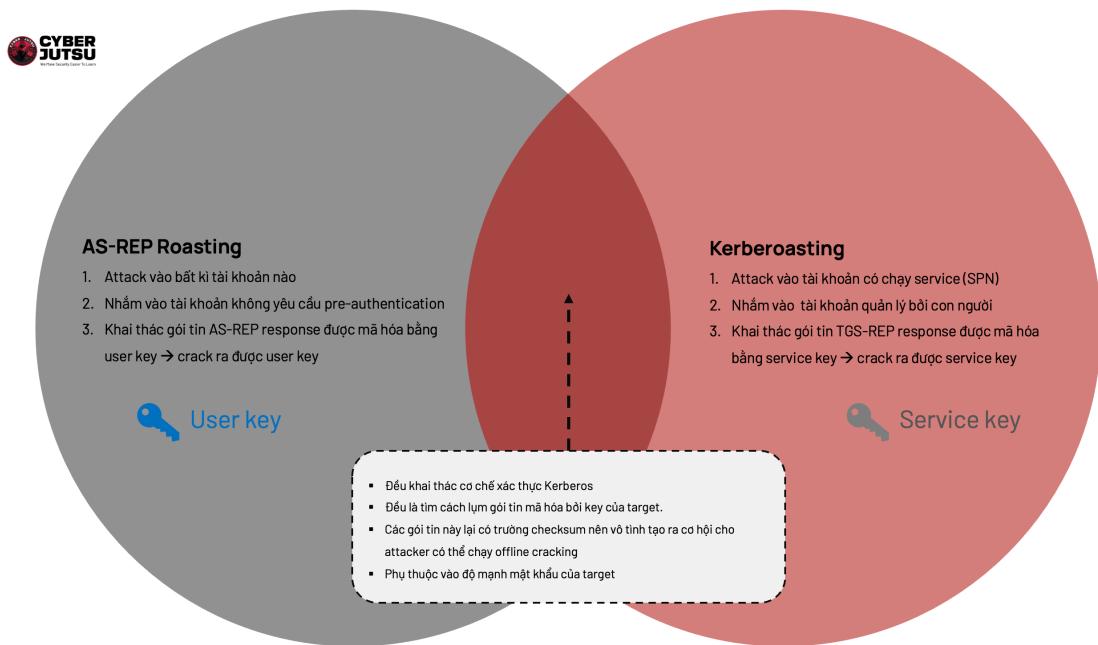


- Nhắm vào tài khoản dịch vụ (Service Accounts) 

- Trong quá trình Kerberos, khi một người dùng yêu cầu để truy cập một dịch vụ, vé dịch vụ (service ticket) sẽ được mã hóa bằng mật khẩu của tài khoản dịch vụ.
 - Kẻ tấn công có thể yêu cầu DC phát hành vé dịch vụ này và lấy được phần vé mã hóa. Sau đó, kẻ tấn công sẽ tiến hành brute-force hoặc dictionary attack để crack mật khẩu của tài khoản dịch vụ bằng việc tính toán và so sánh checksum.
 - Những tài khoản mặc định service có password được tạo ngẫu nhiên rất dài và phức tạp → Tỉ lệ crack được là rất thấp, no hope.

- **Vì thế:** **Kerberoasting** thường tập trung vào tài khoản dịch vụ mà được quản lý bởi con người, thường có mật khẩu yếu hoặc ít được thay đổi, dẫn đến khả năng bẻ khóa cao hơn.
- Đọc thêm:
 - [Service Principal Name \(SPN\) - hackndo](#)
 - <https://en.hackndo.com/kerberoasting/>
 - [GetUserSPNs.py | The Hacker Tools](#)

▼ So sánh: AS-REP Roasting vs. Kerberoasting



Tóm lại:

Cả **AS-REP Roasting** và **Kerberoasting** đều liên quan đến việc **cracking mật khẩu** thông qua quá trình tấn công brute-force hoặc dictionary.

Tuy nhiên, **AS-REP Roasting** nhắm vào tài khoản người dùng không có pre-authentication, còn **Kerberoasting** tập trung vào việc crack mật khẩu tài khoản dịch vụ.

▼ Tìm hiểu thêm các loại attack khác trên Kerberos

- <https://www.thehacker.recipes/ad/movement/kerberos/>

- <https://n1chr0x.medium.com/kerberos-takedown-unleashing-rubeus-and-impacket-for-active-directory-domination-58eeb7b6b6e3>
- <https://labs.lares.com/fear-kerberos-pt1/>
- <https://labs.lares.com/fear-kerberos-pt2/>

Thực hành

▼ rpcclient: Recon thông tin AD

rpcclient là một công cụ dòng lệnh mạnh mẽ được sử dụng để thực hiện các cuộc gọi RPC (Remote Procedure Call) tới máy chủ SMB/CIFS. Nó là một phần của bộ công cụ Samba và có thể được sử dụng để tương tác với các dịch vụ Windows từ xa, đặc biệt hữu ích cho việc liệt kê và thao tác các đối tượng trong môi trường Active Directory.

Reference: [\(¶\) Lateral Movement: Attack vào các Remote Services \(Windows\)](#)

Mặc dù ban đầu được thiết kế để gỡ lỗi và khắc phục sự cố cấu hình Samba Windows, rpcclient đã trở thành một công cụ không thể thiếu đối với các red teamer và penetration tester để thực hiện recon và khai thác các hệ thống Windows.

Các khái niệm chính:

- RPC (Remote Procedure Call): Cho phép một chương trình thực thi thủ tục trên một máy tính từ xa như thể nó là một cuộc gọi cục bộ.
- SMB (Server Message Block): Giao thức mạng được sử dụng để chia sẻ tệp, máy in và giao tiếp giữa các nút trong mạng.
- Active Directory: Dịch vụ thư mục của Microsoft được sử dụng để quản lý tài nguyên mạng.
- SID (Security Identifier): Định danh an ninh duy nhất được sử dụng để xác định một đối tượng bảo mật cụ thể trong Windows.
- RID (Relative Identifier): Phần cuối cùng của SID, xác định đối tượng cụ thể trong một domain.

Kết nối và thông tin cơ bản:

- Kết nối tới máy chủ từ xa:

```
rpcclient -U "username%password" <IP_ADDRESS>
```

```
# Null session
```

```
rpcclient -U "" -N <IP_ADDRESS>
```

- Lấy thông tin máy chủ:

```
srvinfo
```

- Truy vấn thông tin domain:

```
querydominfo
```

Liệt kê người dùng và nhóm:

- Liệt kê tất cả người dùng domain:

```
enumdomusers
```

- Liệt kê tất cả nhóm domain:

```
enumdomgroups
```

- Truy vấn thông tin chi tiết về một người dùng cụ thể:

```
queryuser username
```

- Truy vấn thông tin chi tiết về một nhóm cụ thể:

```
querygroup 0x200
```

Liệt kê đặc quyền và chính sách:

- Liệt kê các đặc quyền của người dùng hiện tại:

```
enumprivs
```

- Lấy thông tin chính sách mật khẩu domain:

```
getdompwinfo
```

▼ Fun fact: Impacket-GetNPUsers

Bạn có biết rằng GetNPUsers có thể tự động thu thập danh sách người dùng thông qua hai cách:

- Phiên RPC null hoặc truy cập LDAP (authenticated)
- Hỗ trợ nhập danh sách người dùng từ file nếu không thể lấy động.

Đọc thêm:

- <https://tools.thehacker.recipes/impacket/examples/getnpusers.py>

```
impacket-GetNPUsers {domain/} -dc-ip {dc_ip} -request
```