

# Breaking into Hades' realm

## an advanced Kerberos exploitation workshop



@rayanlecat



@volker\_carstein

# Slides !



[https://blog.volkercarstein.com/advanced\\_kerberos\\_exploitation\\_workshop\\_slides.pdf](https://blog.volkercarstein.com/advanced_kerberos_exploitation_workshop_slides.pdf)

# Briefing

1. Workshop modalities (timing, goals, etc.)
2. Kerberos 101 and common attacks
3. Let's have some fun ! For each attack:
  - a. Overview
  - b. Lab time
  - c. Solve explanation
4. Conclusion, Q&A




# Story time



# Who are we ?



**Volker Carstein (@volker\_carstein)**

- Pentester / RTO @  **BSECURE**
- Social engineering, OSINT and infosec (with a preference for Active Directory hacking)
- Speaker @ LeHack, Barbhack, Insomni'hack, SecSea, etc

# Who are we ?



## Rayan Bouyaiche (@rayanlecat)

- Pentester @  Quarkslab
- Student @  2600
- 21yo, Active Directory lover
- Certified Big boss (OSCP, OSEP, CRT0, etc...)
- Blog at <https://rayanle.cat/>

# 1. Workshop modalities

- 3-ish hours
- Goals
  - Refresh you on Kerberos and common attacks against it
  - Learn (again) about new and/or niche techniques for Kerberos exploitation
  - Get yourself to practice on a dedicated lab, courtesy of Rayan  
(and Helphy for the hosting 🙏)
  - Have fun!
- 8 flags to grab, go at your own pace (tryharders at the back of the room please!)

# 1. Workshop modalities

1. CVE-2022-33679 (ASREProastable + leak RC4 key)
2. Kerberoasting without preauth
3. RBCD SPN-Less users
4. RBCD to bypass Protected Users
5. Dollar Ticket Attack
6. Spoofing Active Directory users on Linux
7. noPAC / sAMAccountName Spoofing
8. Sapphire Ticket





# 2.1 - Kerberos 101

## Authentication protocol

- Based on tickets that expire in time
- Pre-authentication scheme based on “long term” key
- “Long term” key based on user’s password
- Supports certificates (PKINIT) for pre-auth
- Two types of ticket : Ticket Granting Ticket (**TGT**), Service Ticket (**ST**)

# 2.1 - Kerberos 101

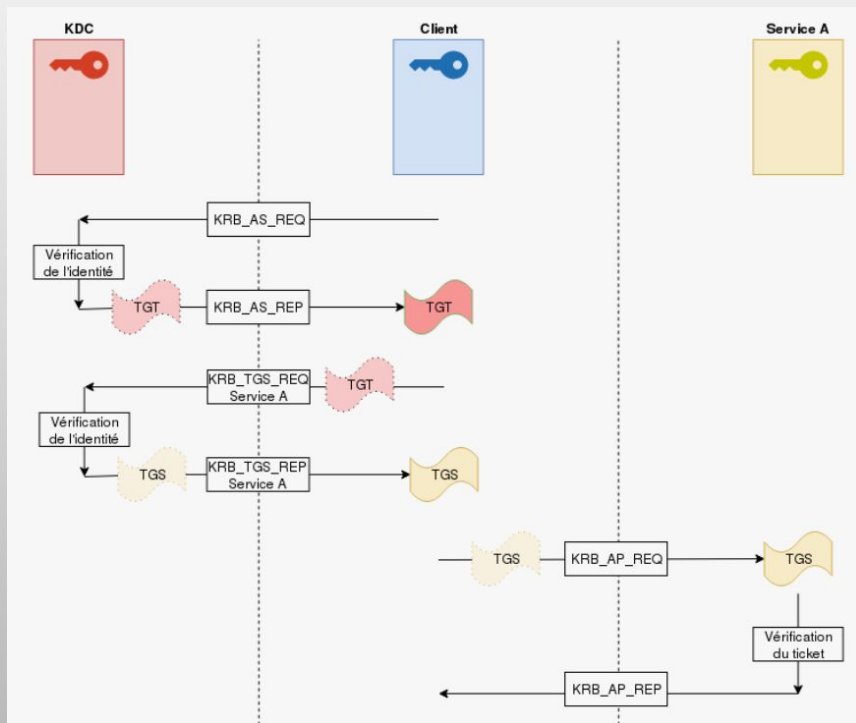
- A ticket contains multiple info : User Name, Service Name, Service Realm, Flags, etc.
- Also, in each ticket is a PAC (Privilege Attribute Certificate), encrypted/signed by the service key
- If service name = krbtgt/domain.local -> It's a TGT ; Else, it's a ST

Impacket v0.13.0.dev0+20241024.220713.de4ad10d - Copyright Fortra, LLC and its affiliated companies

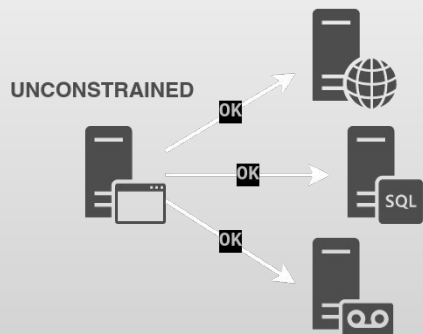
```
[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] Ticket Session Key      : 108ee0a5f6f6b589cd0e35ba35237cf2
[*] User Name               : Administrator
[*] User Realm              : DOMAIN.LOCAL
[*] Service Name            : krbtgt/DOMAIN.LOCAL
[*] Service Realm           : DOMAIN.LOCAL
[*] Start Time              : 11/11/2024 20:18:57 PM
[*] End Time                : 12/11/2024 06:18:57 AM (expired)
[*] RenewTill               : 12/11/2024 20:19:00 PM (expired)
[*] Flags                   : (0x50e10000) forwardable, proxiable, renewable, initial, pre_authent, enc_pa_rep
[*] KeyType                 : rc4_hmac
[*] Base64(key)             : EI7gpfb2tYnNDjW6NSN88g==
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name          : krbtgt/DOMAIN.LOCAL
[*]   Service Realm         : DOMAIN.LOCAL
[*]   Encryption type        : aes256_cts_hmac_sha1_96 (etype 18)
[-] Could not find the correct encryption key! Ticket is encrypted with aes256_cts_hmac_sha1_96 (etype 18), but no keys/creds were supplied
```

# 2.1 - Kerberos 101

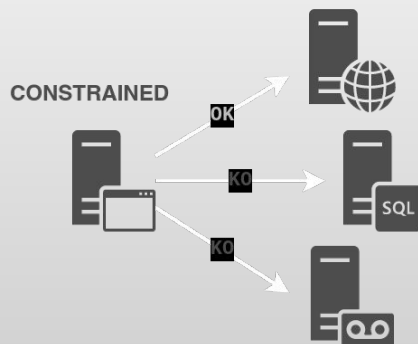
<https://beta.hackndo.com/kerberos/>



# 2.1 - Kerberos 101

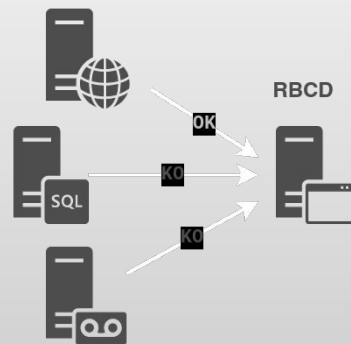


**Kerberos  
Unconstrained  
Delegation**



**Kerberos  
Constrained  
Delegation**

(with or without protocol transition)



**Resource  
Based  
Constrained  
Delegation**

## 2.2 - Kerberos - Common attacks

- **ASREProasting**

- if an account is configured w/o preauth, anybody can ask for a TGT (for this account)
- A TGT contains a session key encrypted with the user secret -> **Offline cracking**

- **Kerberoasting**

- An authenticated attacker can ask for a ST,
- but this ticket contains info encrypted with the service account secret
- If the service account is a user (and not a computer), we can try **Offline cracking**

# 2.2 - Kerberos - Common attacks

- **Silver Ticket**

- Prerequisite : TargetedService LT key (i.e. NT hash or AES key)
- Forge ticket (and PAC) for a specific user/with specific rights
- Use the ticket to access the service

With cifs/TargetedService or host/TargetedService, most dumping operation are allowed.

Works as long as the TargetedService password doesn't change

Stealthier than a Golden Ticket because no KDC is ever contacted during the operation

Problems : PAC must be forged with care to avoid detection, and no KRB\_TGS\_REQ before the ticket's usage

# 2.2 - Kerberos - Common attacks

- **Golden Ticket**
  - Prerequisite : krbtgt LT key (i.e. NT hash or AES key)
  - Forge ticket (and PAC) for a specific user/with specific rights
  - Use the ticket to request any ST

Very powerful as it guarantees full access over everything in the domain as long as the krbtgt password is not changed

Problems : PAC must be forged with care to avoid detection (even with GoldenCopy), especially since the KDC is contacted on every Golden ticket usage. No KRB\_AS\_REQ before the KRB\_TGS\_REQ.

# 3.1 - CVE-2022-33679 - Overview

- Prerequisite
  - knowledge of an ASREProastable account, let's say AccountA
  - RC4 supported
- It is possible to use AccountA to leak the session key and get a service ticket

```
(CVE-2022-33679) [Nov 15, 2024 - 16:51:57 (CET)] exegol-htb (htb) CVE-2022-33679 # python3 CVE-2022-33679.py domain.local/user dc.domain.local
```

<https://googleprojectzero.blogspot.com/2022/10/rc4-is-still-considered-harmful.html>



# 3.1 - CVE-2022-33679 - Lab time



## 3.2 - Kerberoasting without preauth - Overview

- Prerequisite
  - knowledge of an ASREProastable account, let's say AccountA
  - a list of domain accounts
- It is possible to use AccountA to get STs for accounts that have SPNs (aka Kerberoastable accounts)

```
GetUserSPNs.py -no-preauth "AccountA" -usersfile "services.txt" -dc-host "DC_IP_or_HOST" "DOMAIN.LOCAL"/
```

<https://www.thehacker.recipes/ad/movement/kerberos/kerberoast#kerberoast-w-o-pre-authentication>

## 3.2 - Kerberoasting without preauth - Lab time



## 3.3 - RBCD SPN-Less users - Overview

Warning : the used account will be sacrificed

- Obtain a TGT for the SPN-less user allowed to delegate
- Retrieve the TGT session key
- Change the user's password hash and set it to the TGT session key
- S4U2self + U2U so that the SPN-less user can obtain a service ticket to itself, on behalf of another user
- S4U2proxy to obtain a service ticket to the target the user can delegate to on behalf of the other user.
- Access the target as the delegated user with the ticket

<https://www.tiraniddo.dev/2022/05/exploiting-rbcd-using-normal-user.html>

<https://www.thehacker.recipes/ad/movement/kerberos/delegations/rbcd#rbcd-on-spn-less-users>

### 3.3 - RBCD SPN-Less users - Lab time



## 3.4 - RBCD to bypass Protected Users - Overview

- **Protected users :**
  - disable NTLM for users in the Group
  - No DES/RC4 for preauth
  - produce a ticket non-forwardable ticket via S4U2Self (preventing delegation)
  - No ticket renewal beyond the 4h lifetime

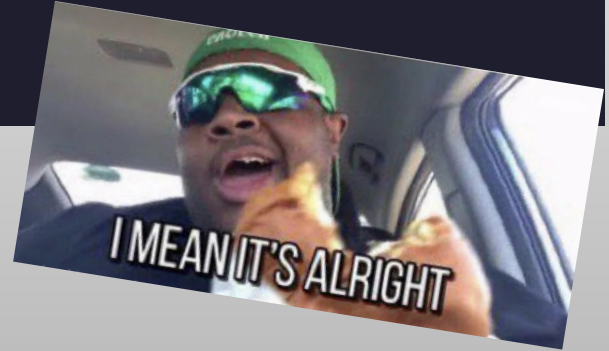
```
[Nov 15, 2024 - 15:28:04 (CET)] exegol-htb (htb) /workspace # nxc smb dc.hades.local -u "Administrator" -p ' ' -d "hades.local"
SMB 10.1.50.10 445 DC [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:hades.local) (signing:True) (SMBv1:False)
SMB 10.1.50.10 445 DC [-] hades.local\Administrator: STATUS_ACCOUNT_RESTRICTION
```

<https://sensepost.com/blog/2023/protected-users-you-thought-you-were-safe-uh/>

## 3.4 - RBCD to bypass Protected Users - Overview

- **But impersonating the default Administrator account works!**
- RBCD delegation like normal, impersonating Administrator account, profit

```
[Nov 15, 2024 - 16:03:21 (CET)] exegol-htb (htb) /workspace # getST.py [REDACTED] /'cat_poc$':'Cat1337!' -impersonate Administrator -spn [REDACTED]  
Impacket v0.13.0.dev0+20241024.220713.de4ad10d - Copyright Fortra, LLC and its affiliated companies  
  
[*] Getting TGT for user  
[*] Impersonating Administrator  
[*] Requesting S4U2self  
[*] Requesting S4U2Proxy  
[*] Saving ticket in Administrator@[REDACTED]
```



<https://sensepost.com/blog/2023/protected-users-you-thought-you-were-safe-uh/>

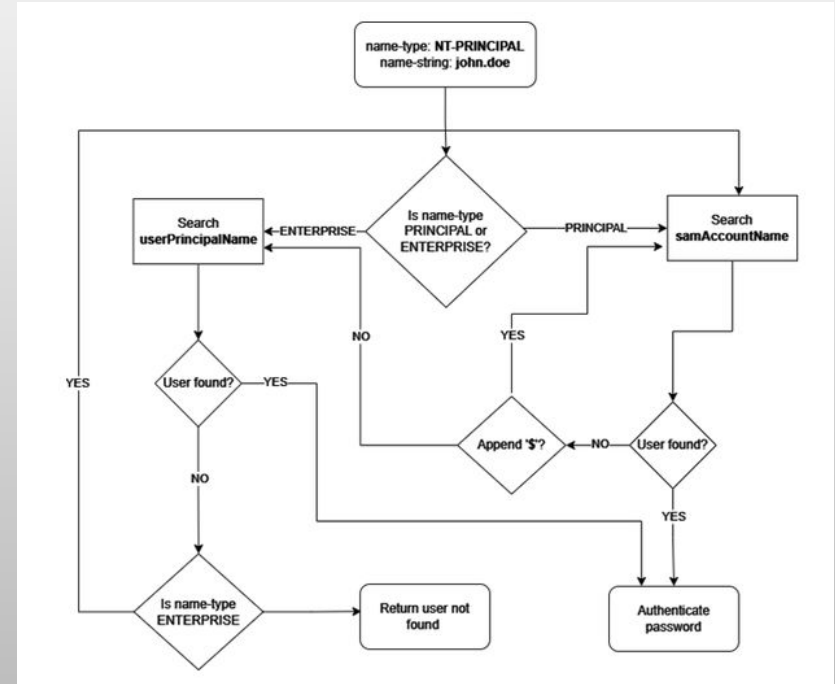
## 3.4 - RBCD to bypass Protected Users - Lab time





# 3.5 - Dollar Ticket attack - Overview

- Prerequisite
  - capability to create machine accounts (MAQ>0) or own already one
  - linux host joined to Active Directory
  - GSSAPI supported on protocol (SSH, PostgreSQL, etc.)



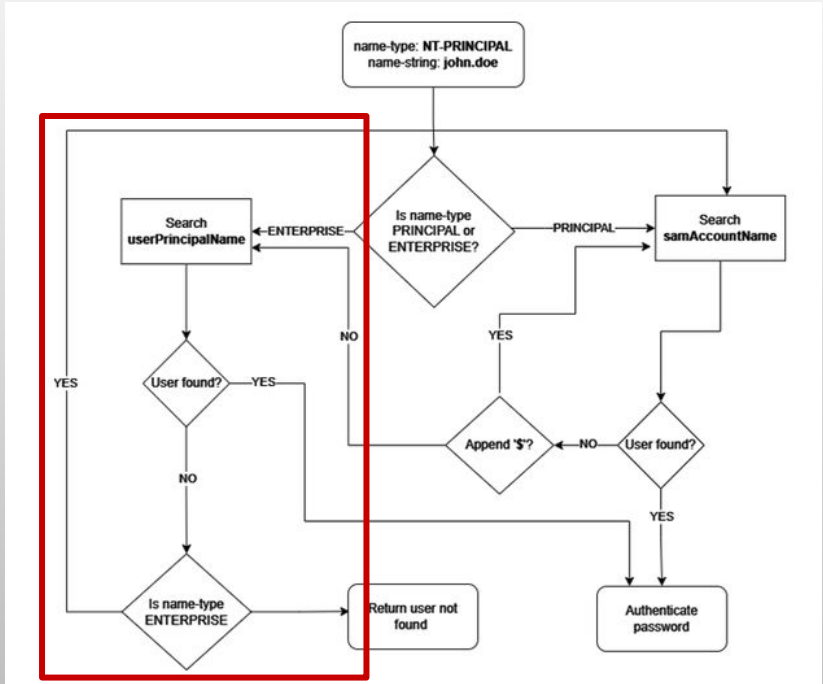
[https://wiki.samba.org/index.php/Security/Dollar Ticket Attack](https://wiki.samba.org/index.php/Security/Dollar_Ticket_Attack)

## 3.5 - Dollar Ticket attack - Lab time



## 3.6 - Spoofing domain users on Linux - Overview

- Prerequisite
  - capability to edit the userPrincipalName of a user
  - linux host joined to Active Directory
  - GSSAPI supported on protocol (SSH, PostgreSQL, etc.)



<https://www.pentestpartners.com/security-blog/a-broken-marriage-abusing-mixed-vendor-kerberos-stacks/>

## 3.6 - Spoofing domain users on Linux - Lab time



## 3.7 - noPAC / sAMAccountName Spoofing - Overview

- **Chaining of two CVEs : CVE-2021-42278 & CVE-2021-42287**

Best to do with a machine account, but possible with a user account

- Clear all SPNs from the controlled account and change the account sAMAccountName to a Domain Controller's name without the trailing \$ (CVE-2021-42278)
- Request a TGT for the controlled account, revert the controlled account sAMAccountName to its old value
- Request a service ticket with S4U2self by presenting the TGT obtained before (CVE-2021-42287), profit !

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

## 3.7 - noPAC / sAMAccountName Spoofing - Lab time



the technique author



## 3.8 - Sapphire Ticket - Overview

**Diamond ticket** : Request legitimate ticket (TGT or ST), decrypt the PAC, modify it to add privileges, recalculate signature and use it legitimately

**Sapphire ticket** : Variation of Diamond ticket, using S4U2self + U2U authentication  
Request legitimate ticket (TGT or ST), replace the PAC with the powerful PAC obtained with S4U2self + U2U, recalculate signature and use the ticket legitimately

Use the ticket to request any ST (GT variant) or use the ticket to access the service (ST variant).  
Same power as Diamond ticket, but stealthier/safer because nothing is rewritten in the PAC

<https://www.thehacker.recipes/ad/movement/kerberos/forged-tickets/#sapphire-ticket>

## 3.8 - Sapphire Ticket - Lab time





# 4. Conclusion, Q&A

- There are many techniques besides ASREProast and Kerberoast
- Delegation are fun, RBCD is a cool gadget
- Kerberos can also be used to impact Linux
- CVEs exploitability is short lived, abuses are better
- Kerberos is complex, implementation is imperfect, many exploit still to be discovered

# Thank you !

