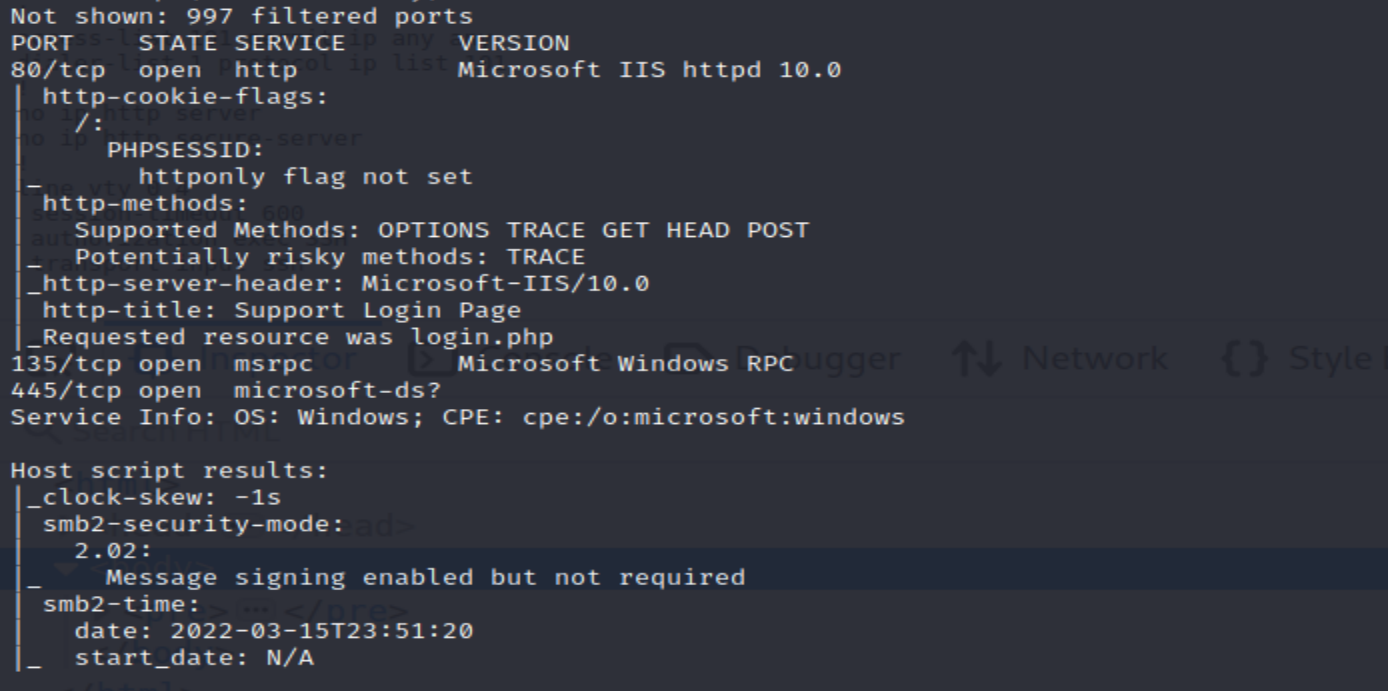
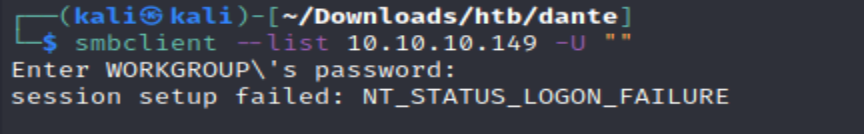
**INTRODUCTION OF DANTE**

**Heist**

Process inspection



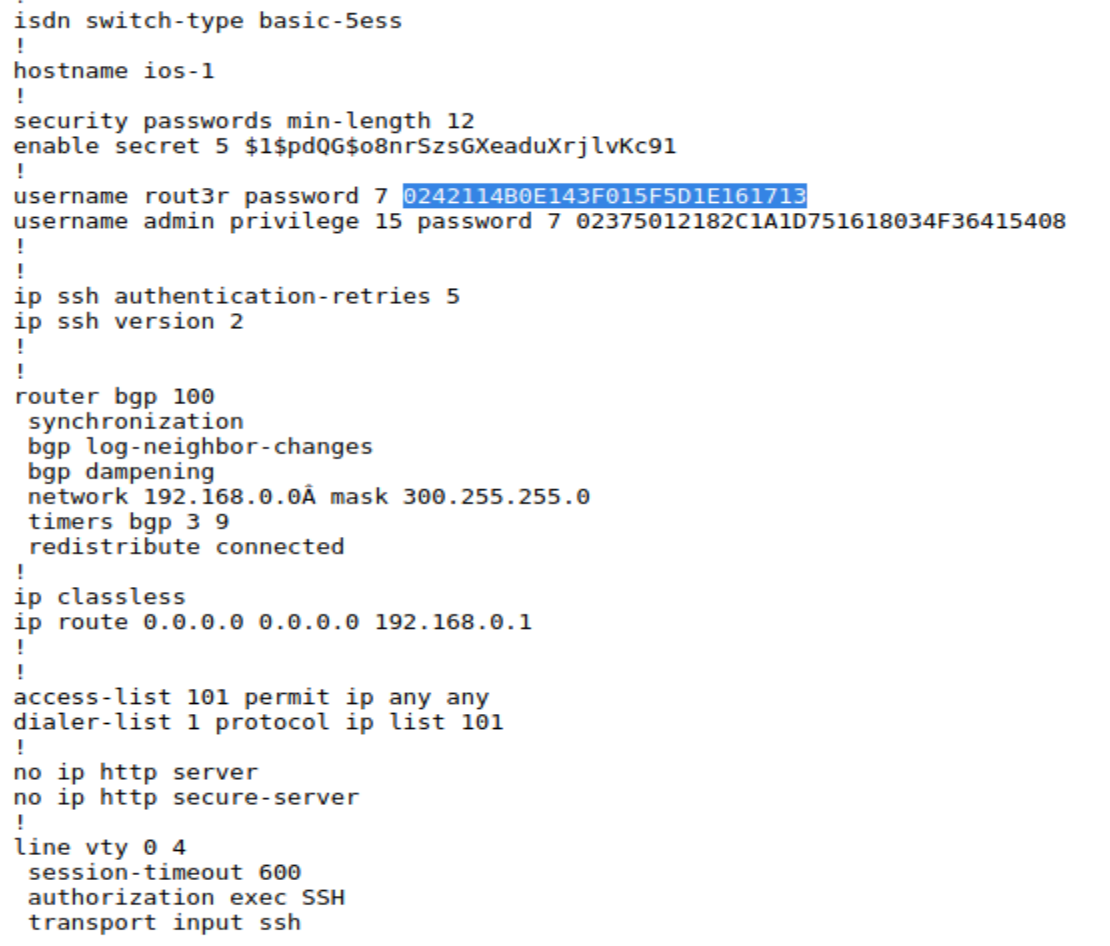
After usual nmap scanning we can find smb client so let focus on anonymous login.

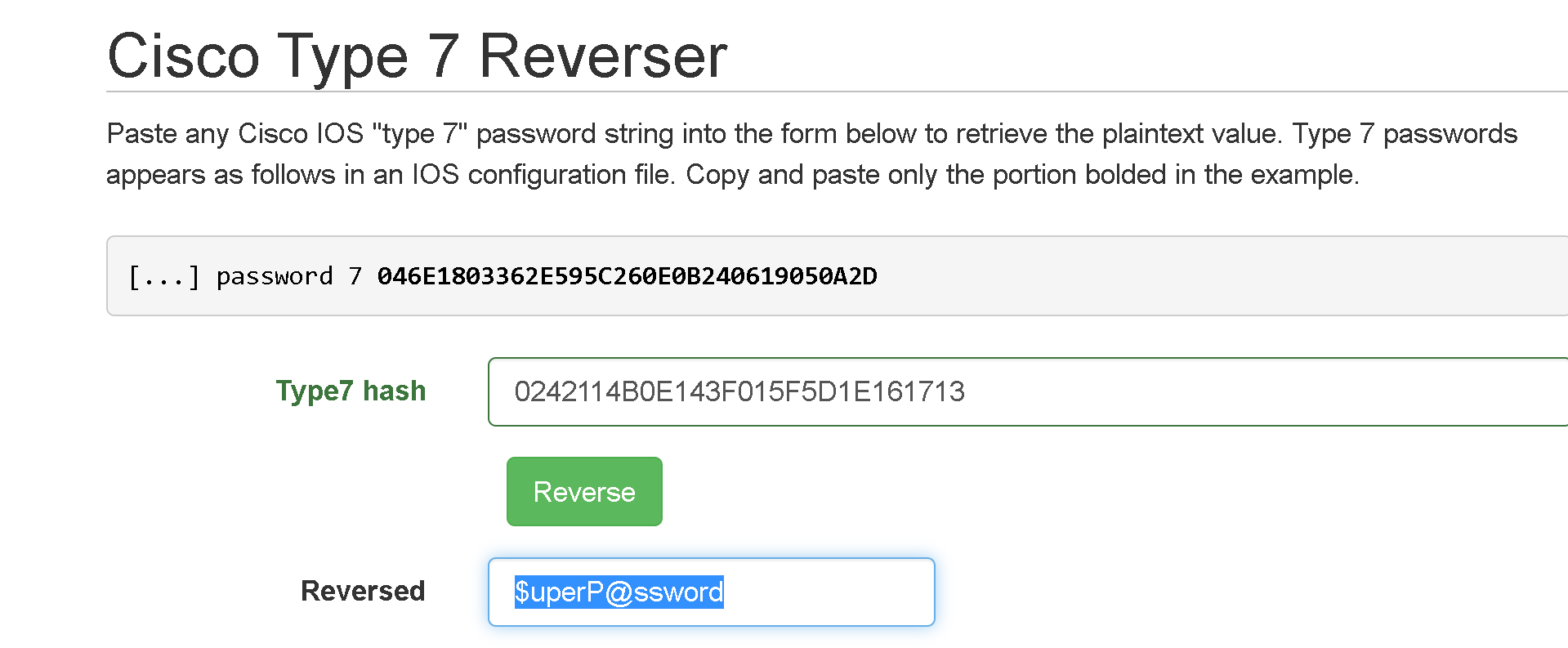


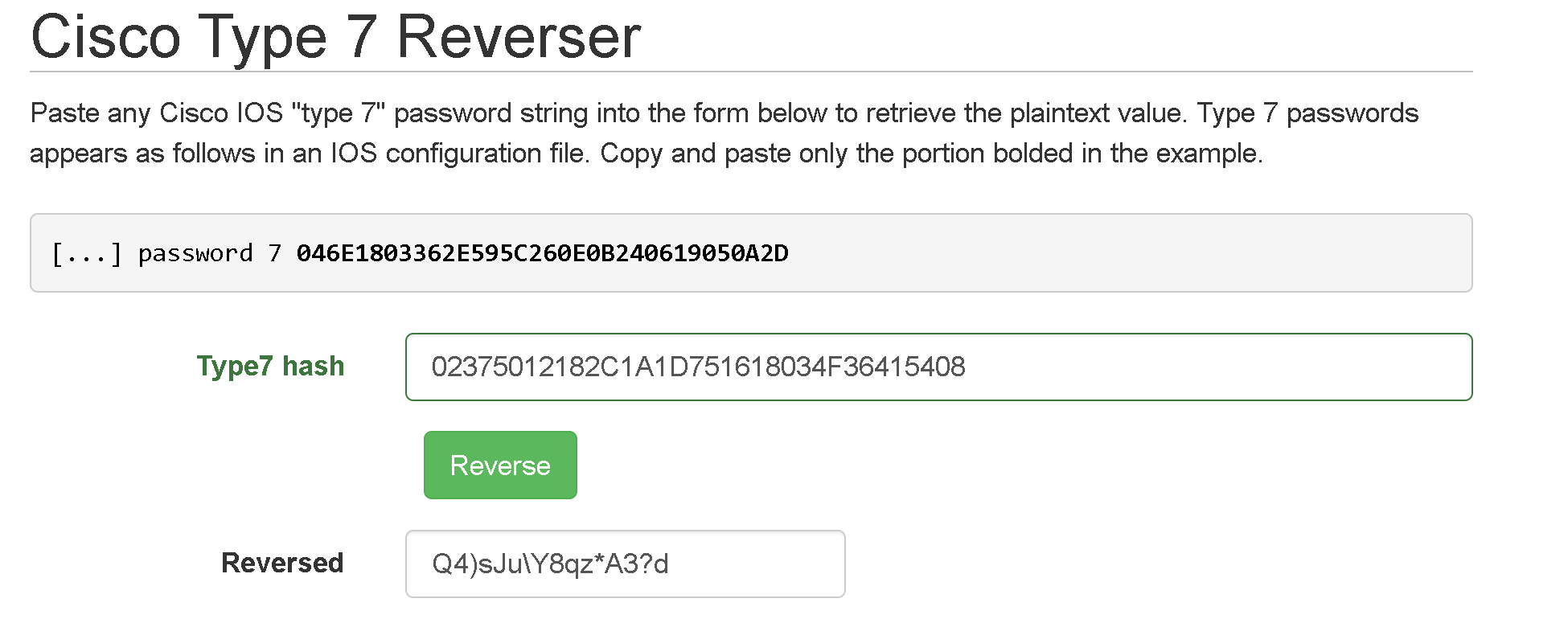
So that’s not possible we require credential, other best way to look for is web enumeration

Web Enumeration

I found a comment by user for cisco configuration issue and have shared the conf file . Initially I thought it to be usual hash password so thought of trying offline cracking .But as always we should first check google dorking and got result that cisco type 7 are just Vigenere cipher so it should be easier. So just using some online tools



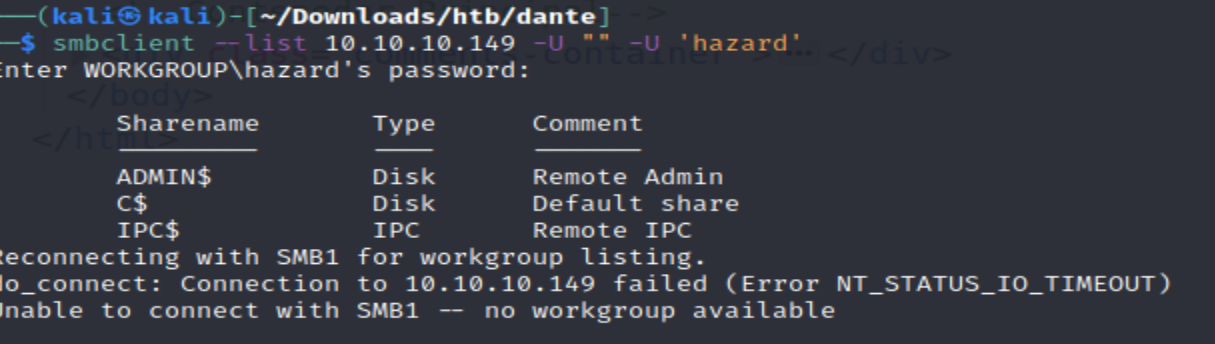




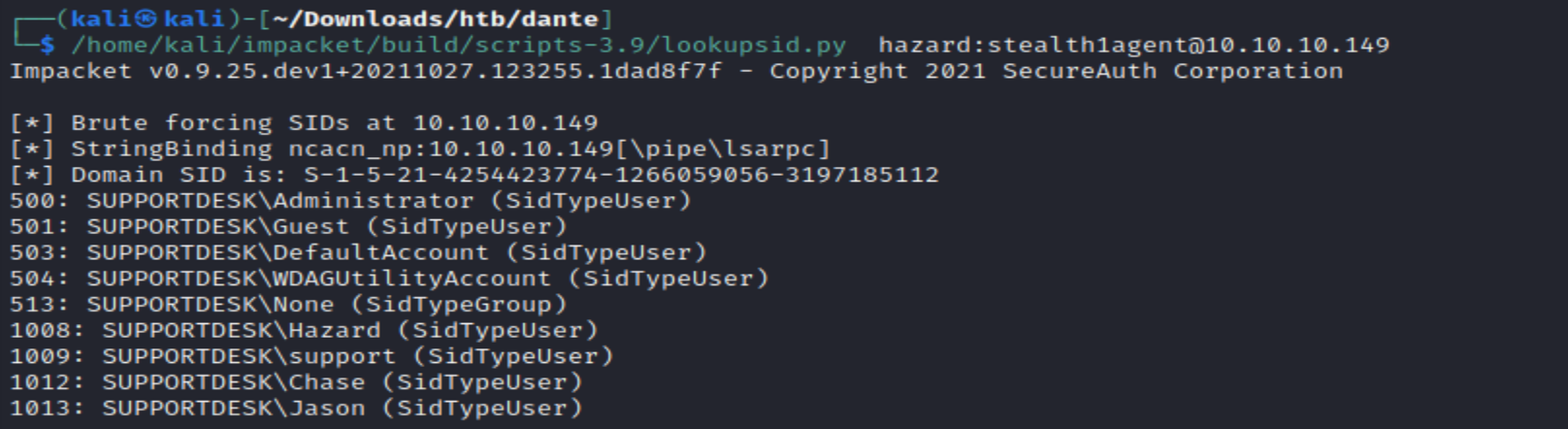
For the user secret hash I used john as it seem to be $1$ it is MD5 .Also its cisco type 5 password

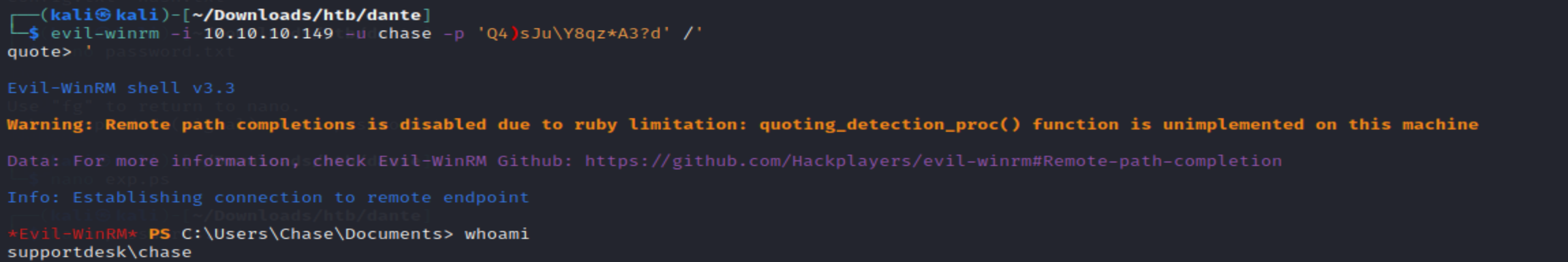
So far we know there is hazard, rout3r, admin as username and password $uperP@ssword and Q4)sJu\Y8qz\*A3?d as password.

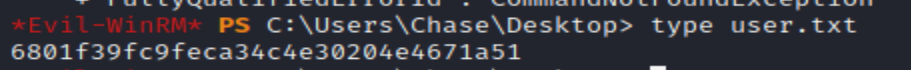
Apart from hazard:stealth1agent none work for useful share or authentication of smbclient

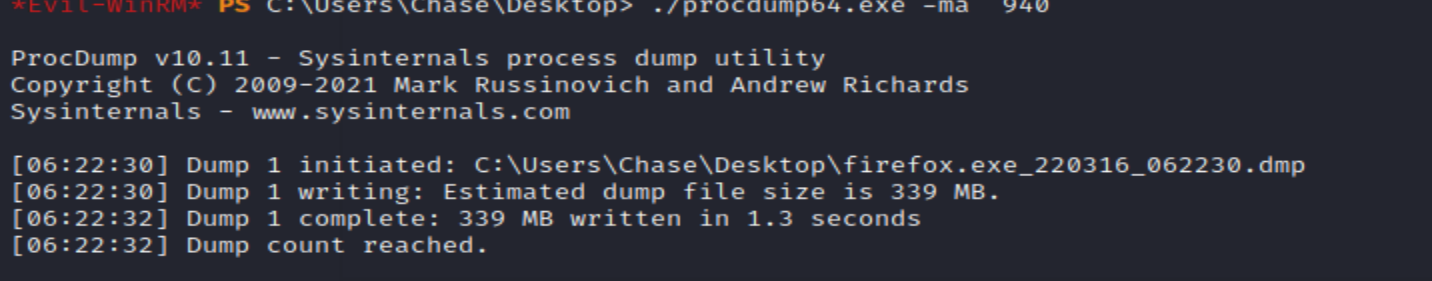


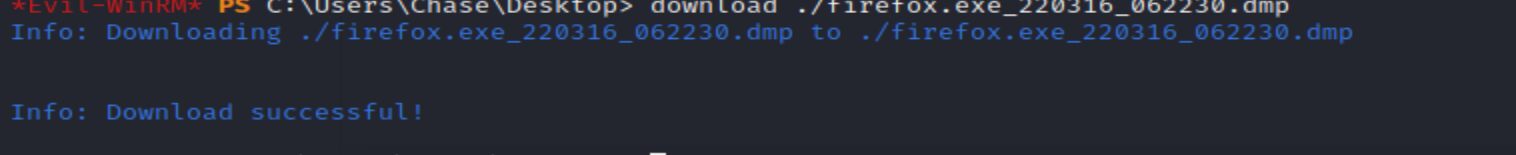
For further enumeration we can use impacket











There using strings by uploading string64.exe ,found password 4dD!5}x/re8]FBuZ

Now have privilege escalation for root access , focus on

https://bond-o.medium.com/htb-heist-390c079a20e5