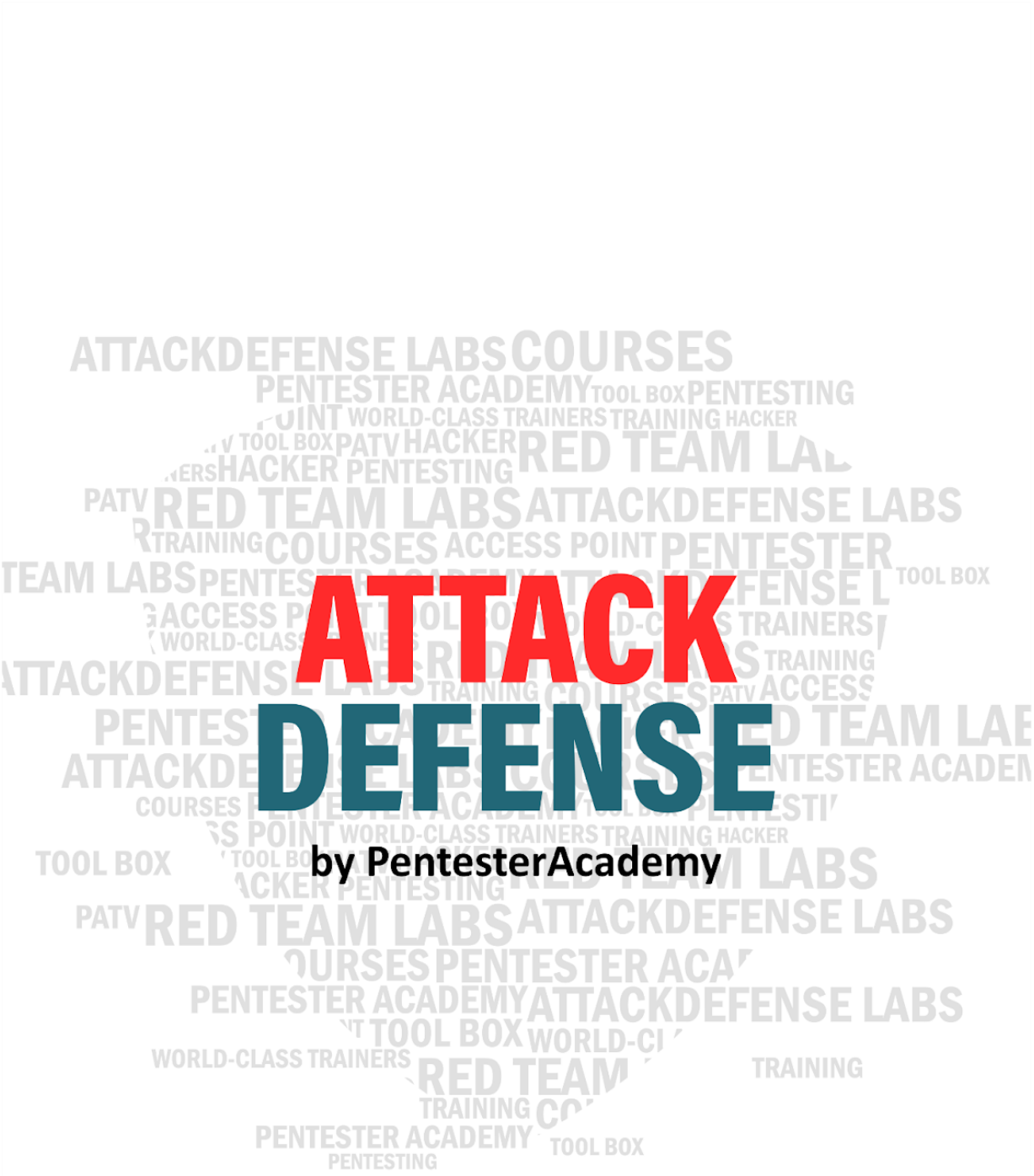

ATTACK
DEFENSE
by PentesterAcademy

Name	WinRM: PowerShell Remoting from Linux
URL	https://attackdefense.com/challengedetails?cid=2025
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 10.0.0.201

```
root@attackdefense:~# nmap --top-ports 7000 10.0.0.201
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-02 01:11 IST
Nmap scan report for ip-10-0-0-201.ap-southeast-1.compute.internal (10.0.0.201)
Host is up (0.0031s 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 15.96 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 have the credentials to access the remote server, 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 3: Store target server credentials in creds variable.

Command: $cred = Get-Credential

Also, enter the target server credentials for the connection. administrator:password_001

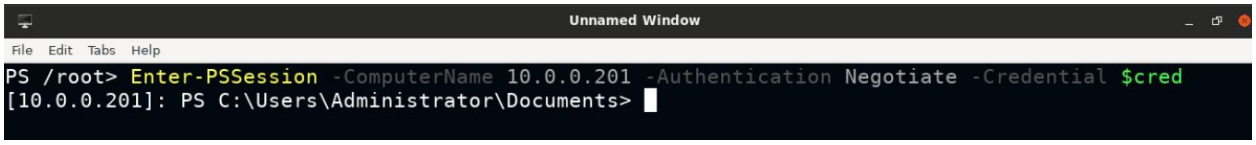
```
PS /root> $cred = Get-Credential

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 10.0.0.201 -Authentication Negotiate -Credential $cred



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

Step 4: Check the IP configuration information on the remote server.

Command: ipconfig /all

```
[10.0.0.201]: PS C:\Users\Administrator\Documents> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : server
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : ap-southeast-1.ec2-utilities.amazonaws.com
                                       ap-southeast-1.compute.internal

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal
   Description . . . . . . . . . . . : AWS PV Network Device #0
   Physical Address. . . . . . . . . : 06-FF-16-CB-D4-DE
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c97d:f1cc:8e08:6fb5%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.0.0.201(Preferred)
```

Step 5: Checking all the running processes.

Command: Get-Process

```
[10.0.0.201]: PS C:\Users\Administrator\Documents> Get-Process

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
    126       9    13356      13868       0.06   1908   0 amazon-ssm-agent
    151       9     6692      12548       0.11   2636   0 conhost
    302      13     2192       4612       0.45    532   0 csrss
    227      11     1756       4364       0.11    604   1 csrss
    352      15     3360      13928       0.08   2900   1 ctfmon
    591      28    18872      43840       0.34    108   1 dwm
   1466      56    22960      75148       1.02   2528   1 explorer
     49       6     1420       3344       0.02    868   0 fontdrvhost
```

We can notice, we have received all the running processes.

Step 6: Checking the system information.

Command: systeminfo

```
[10.0.0.201]: PS C:\Users\Administrator\Documents> systeminfo

Host Name:                 SERVER
OS Name:                   Microsoft Windows Server 2019 Datacenter
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          EC2
Registered Organization:   Amazon.com
Product ID:                00430-00000-00000-AA947
Original Install Date:     10/1/2020, 2:03:49 PM
System Boot Time:          10/1/2020, 7:35:38 PM
System Manufacturer:       Xen
System Model:              HVM domU
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 63 Stepping 2 GenuineIntel ~2400 Mhz
BIOS Version:              Xen 4.2.amazon, 8/24/2006
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
```

We can notice that the target is running Windows Server 2019 also we have received all the CPU, Bios, RAM etc information.

Step 7: Find the flag.
'

Command: cd /
dir

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


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        11/14/2018   6:56 AM                EFI
d-----         5/13/2020   5:58 PM                PerfLogs
d-r---        11/14/2018   4:10 PM                Program Files
d-----         10/1/2020   2:39 PM                Program Files (x86)
d-r---         10/1/2020   2:04 PM                Users
d-----         10/1/2020   2:02 PM                Windows
-a----         10/1/2020   2:36 PM             32 flag.txt


[10.0.0.201]: PS C:\> cat flag.txt
8c3f19547629da63b6d5f8132c6f5ab2
[10.0.0.201]: PS C:\>
```

We have discovered the flag.

Flag: 8c3f19547629da63b6d5f8132c6f5ab2

References

1. Powershell on Linux (https://docs.microsoft.com/en-us/powershell/scripting/install/installing-powershell-core-on-linux?view=powershell-7)