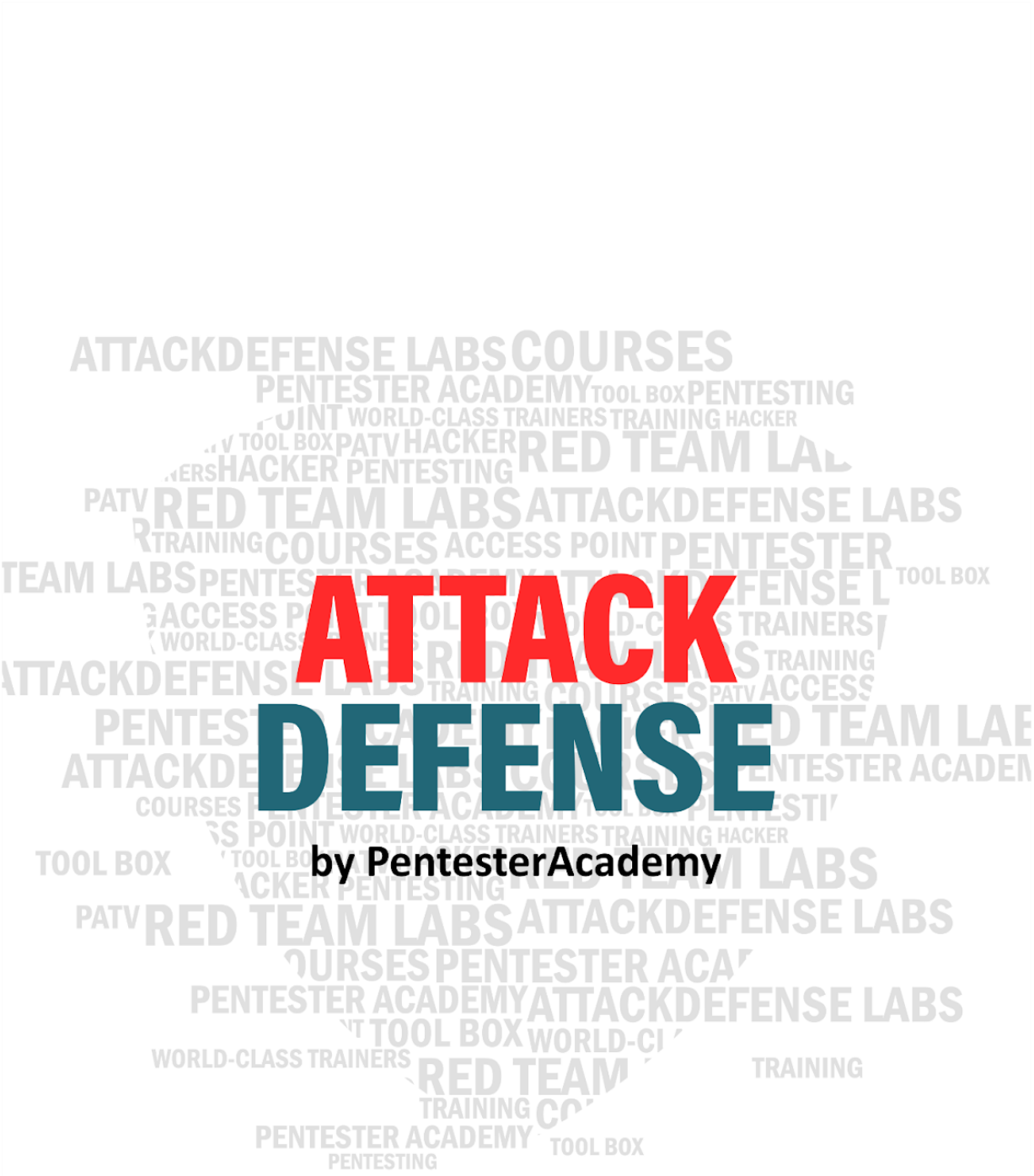

ATTACK
DEFENSE
by PentesterAcademy

Name	Apache Recon: Basics
URL	https://www.attackdefense.com/challengedetails?cid=538
Type	Network Recon : Webservers

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. Which web server software is running on the target server and also find out the version using nmap.

Answer: Apache 2.4.18

Command: nmap -sV -script banner 192.30.247.3

```
root@attackdefense:~# nmap -sV -script banner 192.30.247.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-24 06:21 UTC
Nmap scan report for g9qydq0llxvhwuom6w84o69su.temp-network_a-30-247 (192.30.247.3)
Host is up (0.000026s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 02:42:C0:1E:F7:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 21.84 seconds
root@attackdefense:~#
```

Q2. Which web server software is running on the target server and also find out the version using suitable metasploit module.

Answer: Apache 2.4.18

Commands: msfconsole
use auxiliary/scanner/http/http_version
set RHOSTS 192.30.247.3
exploit

```
msf5 > use auxiliary/scanner/http/http_version
msf5 auxiliary(scanner/http/http_version) > set RHOSTS 192.30.247.3
RHOSTS => 192.30.247.3
msf5 auxiliary(scanner/http/http_version) > exploit

[+] 192.30.247.3:80 Apache/2.4.18 (Ubuntu)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/http_version) >
```

Q3. Check what web app is hosted on the web server using curl command.

Answer: Apache default page

Command: curl http://192.30.247.3/

```
root@attackdefense:~# curl http://192.30.247.3

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <!--
    Modified from the Debian original for Ubuntu
    Last updated: 2014-03-19
    See: https://launchpad.net/bugs/1288690
  -->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Ubuntu Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }
```

```
  </head>
  <body>
    <div class="main_page">
      <div class="page_header floating_element">
        <img src="/icons/ubuntu-logo.png" alt="Ubuntu Logo" class="floating_element"/>
        <span class="floating_element">
          Apache2 Ubuntu Default Page
        </span>
      </div>
<!--      <div class="table_of_contents floating_element">
        <div class="section_header section_header_grey">
          TABLE OF CONTENTS
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#about">About</a>
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#changes">Changes</a>
        </div>
        <div class="table_of_contents_item floating_element">
```

Q4.Check what web app is hosted on the web server using wget command.

Answer: Apache default page

Command: wget “http://192.30.247.3/index”

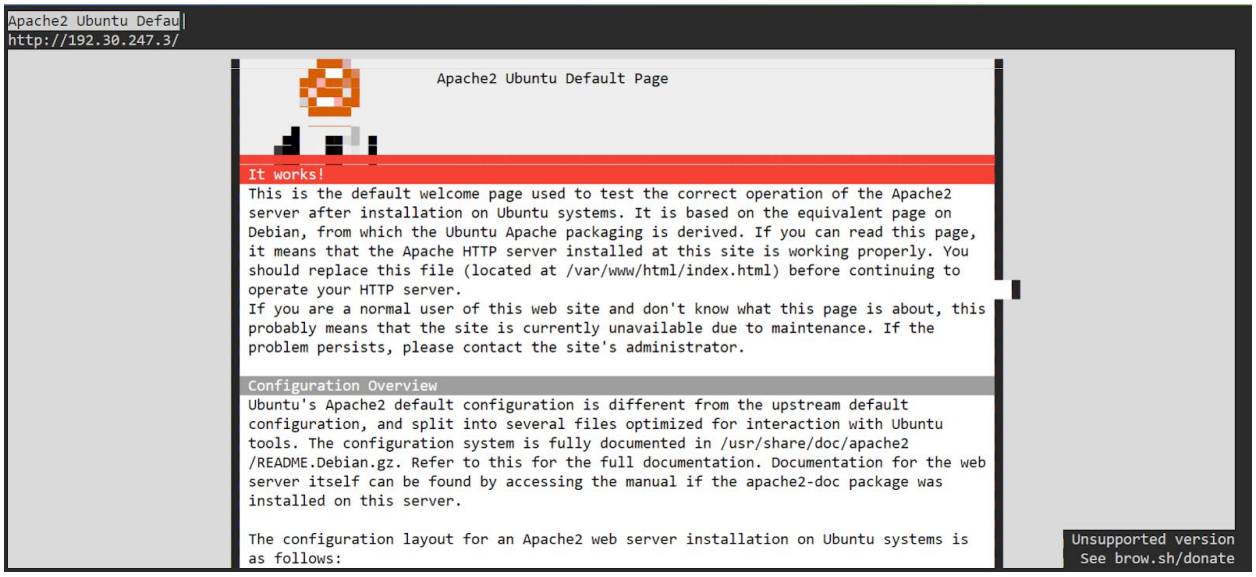
```
root@attackdefense:~#
root@attackdefense:~# wget http://192.30.247.3/index
--2018-11-24 06:28:08--  http://192.30.247.3/index
Connecting to 192.30.247.3:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11321 (11K) [text/html]
Saving to: 'index'

index                         100%[=============================================================>]  11.06K

2018-11-24 06:28:08 (127 MB/s) - 'index' saved [11321/11321]

root@attackdefense:~#
```

Q5. Check what web app is hosted on the web server using browsh CLI based browser.

Answer: Apache default page

Command: browsh --startup-url 192.30.247.3

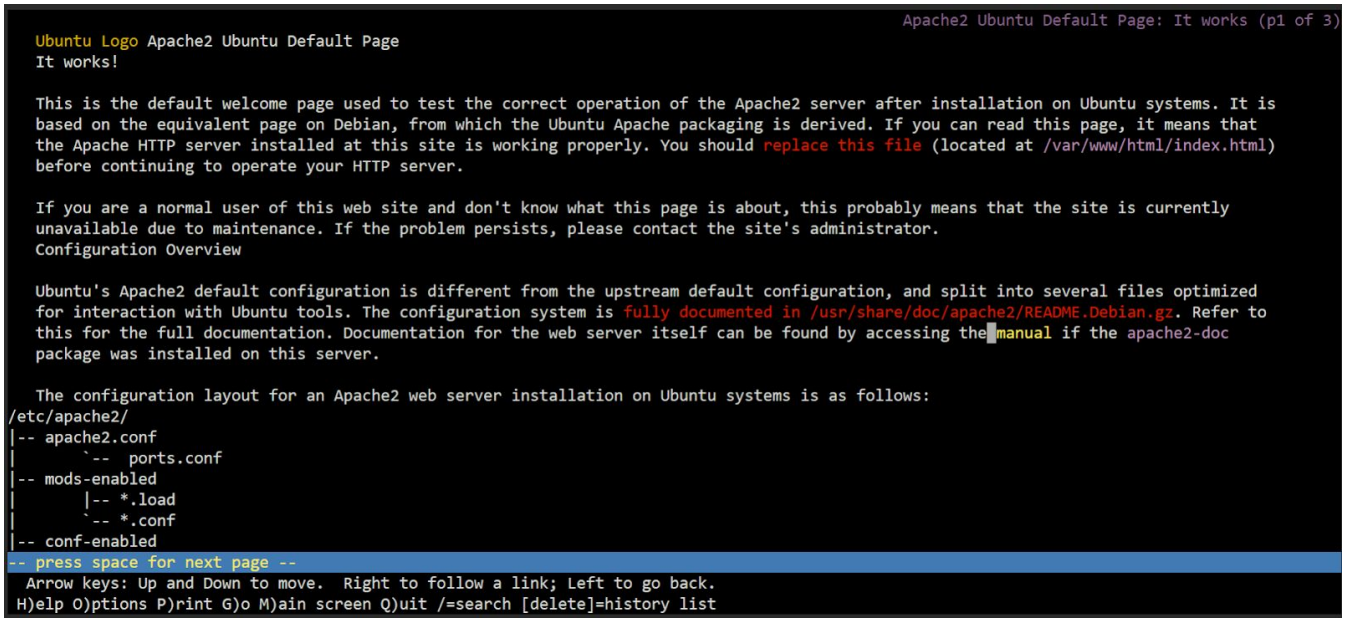
```
root@attackdefense:~# browsh -h
Usage of browsh:
      --debug                  Log to ./debug.log
      --firefox.path string    Path to Firefox executable (default "firefox")
      --firefox.use-existing   Whether Browsh should launch Firefox or not
      --firefox.with-gui       Don't use headless Firefox
      --http-server-mode       Run as an HTTP service
      --startup-url string     URL to launch at startup (default "https://www.brow.sh")
      --time-limit int         Kill Browsh after the specified number of seconds
      --version                Output current Browsh version
pflag: help requested
root@attackdefense:~#
```



Q6. Check what web app is hosted on the web server using lynx CLI based browser.

Answer: Apache default page

Command: lynx http://192.30.247.3



Q7. Perform bruteforce on webserver directories and list the names of directories found. Use brute_dirs metasploit module.

Answer: dir, src

Commands:
use auxiliary/scanner/http/brute_dirs
set RHOSTS 192.30.247.3
exploit

```
msf5 auxiliary(scanner/http/http_version) >
msf5 auxiliary(scanner/http/http_version) > use auxiliary/scanner/http/brute_dirs
msf5 auxiliary(scanner/http/brute_dirs) > set RHOSTS 192.30.247.3
RHOSTS => 192.30.247.3
msf5 auxiliary(scanner/http/brute_dirs) > exploit

[*] Using code '404' as not found.
[+] Found http://192.30.247.3:80/dir/ 200
[+] Found http://192.30.247.3:80/src/ 200
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/brute_dirs) >
```

Q8. Use the directory buster (dirb) with tool/usr/share/metasploit-framework/data/wordlists/directory.txt dictionary to check if any directory is present in the root folder of the web server. List the names of found directories.

Answer: data, dir

Commands: dirb http://192.30.247.3 /usr/share/metasploit-framework/data/wordlists/directory.txt

```
root@attackdefense:~# dirb http://192.30.247.3 /usr/share/metasploit-framework/data/wordlists/directory.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Nov  24 07:23:56 2018
URL_BASE: http://192.30.247.3/
WORDLIST_FILES: /usr/share/metasploit-framework/data/wordlists/directory.txt

-----------------

GENERATED WORDS: 24

---- Scanning URL: http://192.30.247.3/ ----
+ http://192.30.247.3//data (CODE:301|SIZE:313)
+ http://192.30.247.3//dir (CODE:301|SIZE:312)

-----------------
END_TIME: Fri Nov  24 07:23:56 2018
DOWNLOADED: 24 - FOUND: 2
root@attackdefense:~#
```

Q9. Which bot is specifically banned from accessing a specific directory?

Answer: BadBot

Commands: use auxiliary/scanner/http/robots_txt
set RHOSTS 192.30.247.3
run

```
msf5 auxiliary(scanner/http/brute_dirs) > use auxiliary/scanner/http/robots_txt
msf5 auxiliary(scanner/http/robots_txt) > set RHOSTS 192.30.247.3
RHOSTS => 192.30.247.3
msf5 auxiliary(scanner/http/robots_txt) > exploit

[*] [192.30.247.3] /robots.txt found
[+] Contents of Robots.txt:
User-agent: *
Disallow: /cgi-bin/
Disallow: Disallow: /junk/

User-agent: BadBot
Disallow: /no-badbot-dir/

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/robots_txt) > _
```

References:

1. Apache Web Server (https://httpd.apache.org/)
2. Browsh (https://www.brow.sh/)
3. Lynx (https://lynx.invisible-island.net/)
4. Metasploit Module: HTTP Version Detection (https://www.rapid7.com/db/modules/auxiliary/scanner//http/http_version)
5. Metasploit Module: HTTP Directory Brute Force Scanner (https://www.rapid7.com/db/modules/auxiliary/scanner//http/brute_dirs)
6. Metasploit Module: HTTP Robots.txt Content Scanner (https://www.rapid7.com/db/modules/auxiliary/scanner/http/robots_txt)