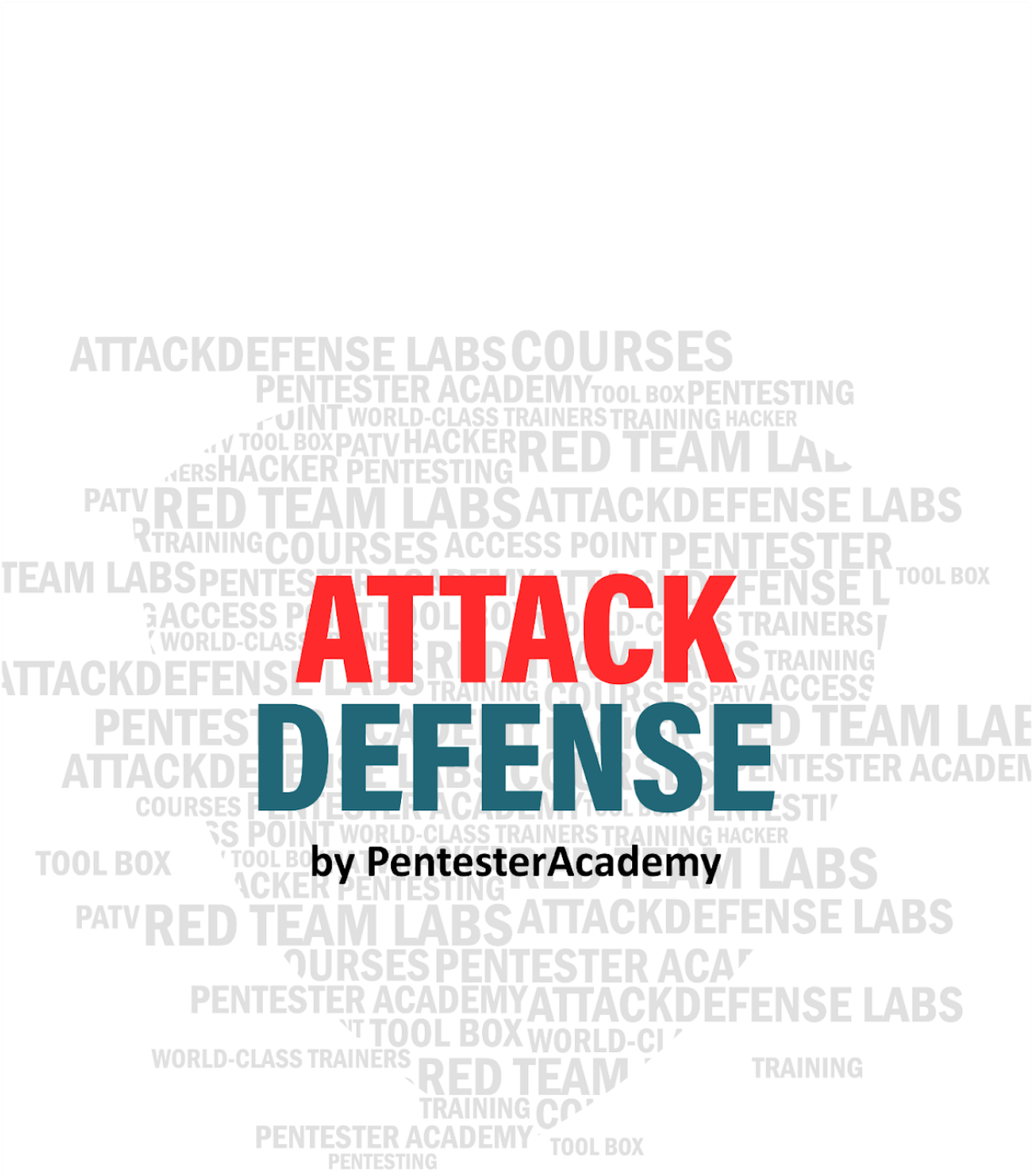
ATTACK
DEFENSE
by PentesterAcademy

Name	Nginx Recon: Basics
URL	https://www.attackdefense.com/challengedetails?cid=537
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. What is the version of Nginx server?

Answer: 1.14.2

Command: nmap -sV 192.152.43.3

```
root@attackdefense:~# nmap -sV 192.152.43.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-09 04:51 UTC
Nmap scan report for target-1 (192.152.43.3)
Host is up (0.000014s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.14.2
MAC Address: 02:42:C0:98:2B: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 6.66 seconds
root@attackdefense:~#
```

Q2. How many directory can you find in root folder of web server using brute_dirs metasploit module (with default dictionary)?

Answer: 3

Commands:
msfconsole
use auxiliary/scanner/http/brute_dirs
set RHOSTS 192.152.43.3
exploit

```
msf5 > use auxiliary/scanner/http/brute_dirs
msf5 auxiliary(scanner/http/brute_dirs) > set RHOSTS 192.152.43.3
RHOSTS => 192.152.43.3
msf5 auxiliary(scanner/http/brute_dirs) > exploit

[*] Using code '404' as not found.
[+] Found http://192.152.43.3:80/dir/ 403
[+] Found http://192.152.43.3:80/poc/ 403
[+] Found http://192.152.43.3:80/pro/ 403
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/brute_dirs) >
```

Q3. How many of the directories from list /usr/share/metasploit-framework/data/wordlists/directory.txt are present in the root folder of a web server? List the names.

Answer: 8

Command: dirb http://192.152.43.3 /usr/share/metasploit-framework/data/wordlists/directory.txt

```
root@attackdefense:~# dirb http://192.152.43.3 /usr/share/metasploit-framework/data/wordlists/directory.txt

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

START_TIME: Sat May  9 04:52:40 2020
URL_BASE: http://192.152.43.3/
WORDLIST_FILES: /usr/share/metasploit-framework/data/wordlists/directory.txt

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

GENERATED WORDS: 24

---- Scanning URL: http://192.152.43.3/ ----
+ http://192.152.43.3//pro (CODE:301|SIZE:185)
+ http://192.152.43.3//poc (CODE:301|SIZE:185)
+ http://192.152.43.3//dir (CODE:301|SIZE:185)
+ http://192.152.43.3//Benefits (CODE:301|SIZE:185)
+ http://192.152.43.3//Data (CODE:301|SIZE:185)
+ http://192.152.43.3//Invitation (CODE:301|SIZE:185)
+ http://192.152.43.3//Office (CODE:301|SIZE:185)
+ http://192.152.43.3//Site (CODE:301|SIZE:185)

-----------------
END_TIME: Sat May  9 04:52:40 2020
DOWNLOADED: 24 - FOUND: 8
root@attackdefense:~#
```

Q4. Which directories are allowed & disallowed for the web crawlers?

Answer:
Allowed: /Benefits, /Invitation
Disallowed: /Admin, /Office

Commands:
use auxiliary/scanner/http/robots_txt
set RHOSTS 192.152.43.3
exploit

```
msf5 > use auxiliary/scanner/http/robots_txt
msf5 auxiliary(scanner/http/robots_txt) > set RHOSTS 192.152.43.3
RHOSTS => 192.152.43.3
msf5 auxiliary(scanner/http/robots_txt) > exploit

[*] [192.152.43.3] /robots.txt found
[+] Contents of Robots.txt:
User-agent: *
Allow: /Benefits
Allow: /Invitation
Disallow: /Admin
Disallow: /Office


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

Q5. Which folder is protected with HTTP basic authentication?

Answer: Admin

Solution:

Send HTTP GET request to each discovered directory and check the request headers

Command: curl -I http://192.152.43.3/Admin

```
root@attackdefense:~# curl -I http://192.152.43.3/Admin
HTTP/1.1 401 Unauthorized
Server: nginx/1.14.2
Date: Sat, 09 May 2020 04:54:04 GMT
Content-Type: text/html
Content-Length: 195
Connection: keep-alive
WWW-Authenticate: Basic realm="FLAG: 9CDFB439C7876E703E307864C9167A15"

root@attackdefense:~#
```

Q6. Which directory present in root directory of web server is writable? Use http_put metasploit module with default dictionary.

Answer: Data

Solution:

Scanning each discovered directory with nikto.

Command: nikto -h http://192.152.43.3/Data

```
root@attackdefense:~# nikto -h http://192.152.43.3/Data
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.152.43.3
+ Target Hostname:    192.152.43.3
+ Target Port:        80
+ Start Time:         2020-05-09 04:54:55 (GMT0)
---------------------------------------------------------------------------
+ Server: nginx/1.14.2
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different
MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-397: HTTP method 'PUT' allows clients to save files on the web server.
+ 7917 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2020-05-09 04:55:12 (GMT0) (17 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Verifying by using the metasploit module to put file on the web server.

Commands:
msfconsole
use auxiliary/scanner/http/http_put
set RHOSTS 192.152.43.3
set PATH /Data
exploit

```
msf5 > use auxiliary/scanner/http/http_put
msf5 auxiliary(scanner/http/http_put) > set RHOSTS 192.152.43.3
RHOSTS => 192.152.43.3
msf5 auxiliary(scanner/http/http_put) > set PATH /Data
PATH => /Data
msf5 auxiliary(scanner/http/http_put) > exploit

[+] File uploaded: http://192.152.43.3:80/Data/msf_http_put_test.txt
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/http_put) >
```

Deleting uploaded file

Commands:
set ACTION DELETE
exploit

```
msf5 auxiliary(scanner/http/http_put) > set ACTION DELETE
ACTION => DELETE
msf5 auxiliary(scanner/http/http_put) > exploit

[+] File deleted: http://192.152.43.3:80/Data/msf_http_put_test.txt
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/http_put) >
```

Q7. Which directory present in root directory of web server, allows directory/file listing?

Answer: Office

Solution:

Send HTTP GET request to each discovered directory and checking for 200 OK status

Command: curl -I -L 192.152.43.3/Office

```
root@attackdefense:~# curl -I -L 192.152.43.3/Office
HTTP/1.1 301 Moved Permanently
Server: nginx/1.14.2
Date: Sat, 09 May 2020 04:57:06 GMT
Content-Type: text/html
Content-Length: 185
Location: http://192.152.43.3/Office/
Connection: keep-alive

HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Sat, 09 May 2020 04:57:06 GMT
Content-Type: text/html
Connection: keep-alive

root@attackdefense:~#
```

Q8. We have hidden a flag on the server. It is hidden in the response headers of a particular directory. Retrieve the flag.

Answer: 9CDFB439C7876E703E307864C9167A15

Commands:

use auxiliary/scanner/http/http_header
set RHOSTS 192.152.43.3
set TARGETURI /Admin/
set HTTP_METHOD GET
exploit

```
msf5 > use auxiliary/scanner/http/http_header
msf5 auxiliary(scanner/http/http_header) > set RHOSTS 192.152.43.3
RHOSTS => 192.152.43.3
msf5 auxiliary(scanner/http/http_header) > set TARGETURI /Admin/
TARGETURI => /Admin/
msf5 auxiliary(scanner/http/http_header) > set HTTP_METHOD GET
HTTP_METHOD => GET
msf5 auxiliary(scanner/http/http_header) > exploit

[+] 192.152.43.3:80       : CONTENT-TYPE: text/html
[+] 192.152.43.3:80       : SERVER: nginx/1.14.2
[+] 192.152.43.3:80       : WWW-AUTHENTICATE: Basic realm="FLAG: 9CDFB439C7876E703E307864C9167A15"
[+] 192.152.43.3:80       : detected 3 headers
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/http_header) >
```

References

1. Nginx (https://www.nginx.com/)
2. Dirb (https://tools.kali.org/web-applications/dirb)
3. Metasploit Module: HTTP Directory Brute Force Scanner (https://www.rapid7.com/db/modules/auxiliary/scanner//http/brute_dirs)
4. Metasploit Module: HTTP Header Detection (https://www.rapid7.com/db/modules/auxiliary/scanner/http/http_header)
5. Metasploit Module: HTTP Writable Path PUT/DELETE File Access (https://www.rapid7.com/db/modules/auxiliary/scanner/http/http_put)