

[Home](#) [About](#) [Category](#) [Contact](#)

Chapter 6. Enumerating Target

INFORMATION GATHERING – Enumerating Target

Enumeration is defined as the process of extracting user names, machine names, network resources, shares and services from a system. In this phase, the attacker creates an active connection to the system and performs directed queries to gain more information about the target. The gathered information is used to identify the vulnerabilities or weak points in system security and tries to exploit in the System gaining phase.

Recent Posts

- [IS – Chapter 1](#)
- [Ethical Hacking & Penetration](#)
- [HCI – Construct 2](#)
- [Database Proposal](#)

Recent Comments

Archives

- [October 2019](#)
- [April 2019](#)
- [November 2018](#)

November 2019

Note

This is processes performed by intruders or hackers to system network resources, users and groups, web servers and installed applications etc.

Techniques for Enumeration

- Extracting user names using email ID's
- Extract information using the default password
- Brute Force Active Directory
- Extract user names using SNMP
- Extract user groups from Windows
- Extract information using DNS Zone transfer

Enumerating Tools

There are a lot of tools available to perform enumerating scanning. Some of the most popular tools are nmap, zenmap, nikto2 and WPScan.

- [Nmap](#) is a powerful network security tool written by Gordon Lyon. It was released almost 20 years ago (in 1997) and has since become the de facto standard for network mapping and port scanning, allowing network administrators to discover hosts and services on a computer network, and create a map of the network.
- [Zenmap](#) is the official Nmap Security Scanner GUI. It performs the same functions as that of nmap. The only difference is that you get to see everything graphically instead on the console logs provided by nmap.
- [Nikto](#) is an Open Source ([GPL](#)) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers.

M	T	W	T	F	S	S
					1	2
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

« Oct

- [WPScan](#) is a black box WordPress vulnerability scanner that can be used to scan remote WordPress installations to find security issues.

In the previous post, we have discussed about nmap and zenmap and also performed some information gathering technique using the tools. In this post, we will use Nikto and WPScan to target the same domain for possible information sourcing. Both tools provides additional options for different target. See `–help` for more information.

Nikto Tools

- Using Nikto to perform scanning on a secure or hidden domain IP might result to no information found result. We have performed multiple scanning on the same

```
root@user: ~
root@user: ~ 80x24
root@user:~# nikto -h team1.pentest.id
- Nikto v2.1.6
-----
+ Target IP: 104.28.31.3
+ Target Hostname: team1.pentest.id
+ Target Port: 80
+ Start Time: 2019-06-19 13:32:23 (GMT-4)
-----
+ Server: cloudflare
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'cf-ray' found, with contents: 4e973def5d67c33b-SIN
+ 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 fashion to the MIME type
+ All CGI directories 'found', use '-C none' to test none
+ 26151 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time: 2019-06-19 13:45:36 (GMT-4) (793 seconds)
-----
+ 1 host(s) tested
```

- After using [Censys](#) to reveal the real IP of **team1.pentest.id** domain, we performed the same process again and we were able to gather information about the target. The web server, Operating System, database or the server and it's version.

```
root@user: ~
root@user: ~ 80x24
^Croot@user:~# nikto -h 178.128.108.247
- Nikto v2.1.6
-----
+ Target IP:      178.128.108.247
+ Target Hostname: 178.128.108.247
+ Target Port:    80
+ Start Time:     2019-06-19 13:57:34 (GMT-4)
-----
+ Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
+ Retrieved x-powered-by header: PHP/5.4.16
+ 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
+ Uncommon header 'link' found, with contents: <https://team1.pentest.id/wp-json/>; rel="https://api.w.org/"
+ 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 fashion to the MIME type
+ Uncommon header 'x-redirect-by' found, with contents: WordPress
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x3e 0x5890bef9235c5
+ Entry '/wp-login.php' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/password.lst' in robots.txt returned a non-forbidden or redirect HTTP code (200)
```

```
root@user: ~
root@user: ~ 80x24
trings.
+ OSVDB-3092: /download/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /aw/: This might be interesting... potential country code (Aruba)
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ /wp-app.log: Wordpress' wp-app.log may leak application/system details.
+ /wordpress/: A Wordpress installation was found.
+ /wp-admin/wp-login.php: Wordpress login found
+ /blog/wp-login.php: Wordpress login found
+ 8347 requests: 0 error(s) and 26 item(s) reported on remote host
+ End Time: 2019-06-19 14:35:46 (GMT-4) (2292 seconds)
-----
+ 1 host(s) tested

*****
Portions of the server's headers (OpenSSL/1.0.2k-fips) are not in
the Nikto database or are newer than the known string. Would you like
to submit this information (*no server specific data*) to CIRT.net
for a Nikto update (or you may email to sullo@cirt.net) (y/n)? n

root@user:~#
```

WPScan Tools

- Performing wpscan -url team1.pentest.id --enumerate u, we are able to gather information about the target.

The host server, database version and some entry points

“/wp-login.php and /password.lst”

```
root@user: ~
root@user: ~ 80x24

root@user:~# wpscan --url team1.pentest.id --enumerate u

  _____
 /            \
|  WPSCAN  |
|_____|_____|

WordPress Security Scanner by the WPScan Team
      Version 3.4.3
    Sponsored by Sucuri - https://sucuri.net
@_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]Y
[i] Updating the Database ...
[i] Update completed.

[+] URL: http://team1.pentest.id/
[+] Started: Wed Jun 19 13:35:20 2019
```

```
root@user: ~
root@user: ~ 80x24
[i] Updating the Database ...
[i] Update completed.

[+] URL: http://team1.pentest.id/
[+] Started: Wed Jun 19 13:35:20 2019

Interesting Finding(s):

[+] http://team1.pentest.id/
| Interesting Entries:
|   - X-Powered-By: PHP/5.4.16
|   - Server: cloudflare
|   - CF-RAY: 4e9741962cdfd9b4-SIN
| Found By: Headers (Passive Detection)
| Confidence: 100%

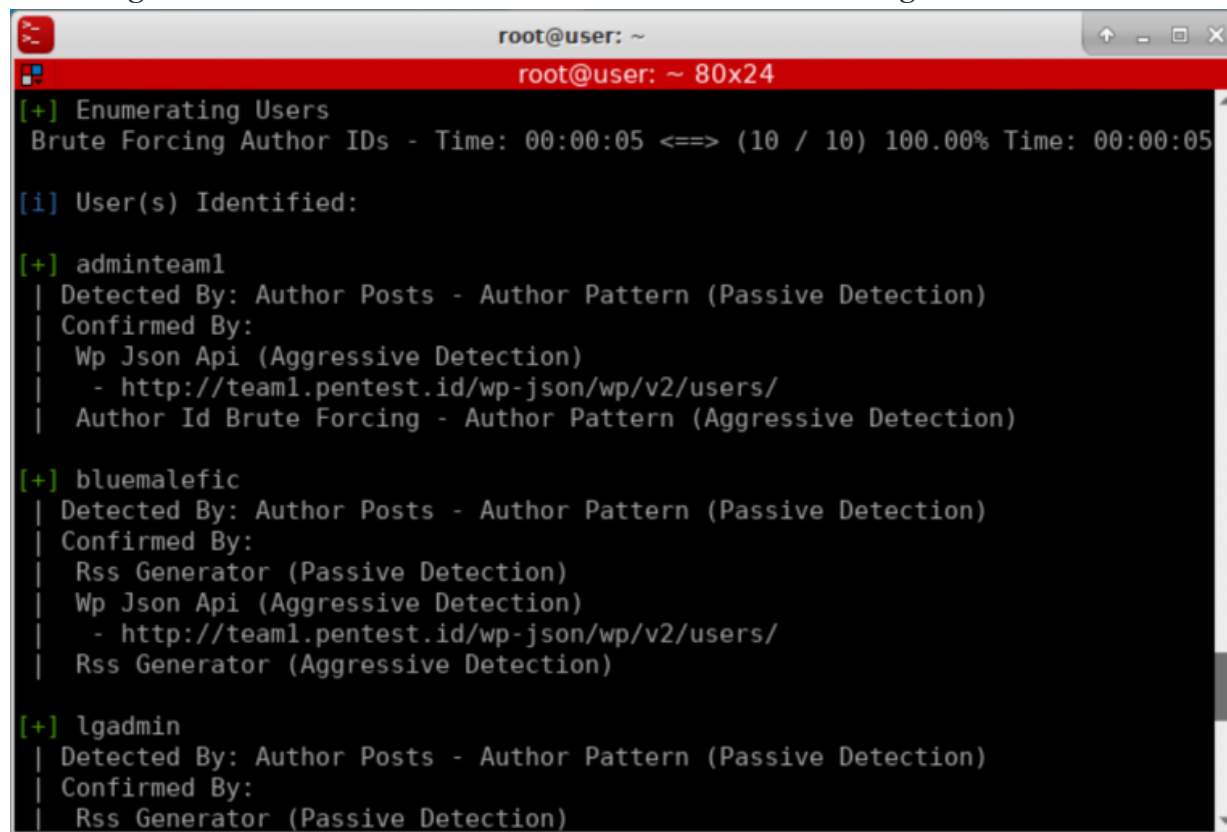
[+] http://team1.pentest.id/robots.txt
| Interesting Entries:
|   - /wp-login.php
|   - /password.lst
| Found By: Robots Txt (Aggressive Detection)
| Confidence: 100%

[+] http://team1.pentest.id/xmlrpc.php
```


- We are also able to gather information about some of the plugins installed.

```
root@user: ~  
root@user: ~ 80x24  
[+] WordPress theme in use: twentynineteen  
| Location: http://team1.pentest.id/wp-content/themes/twentynineteen/  
| Latest Version: 1.4 (up to date)  
| Last Updated: 2019-05-07T00:00:00.000Z  
| Readme: http://team1.pentest.id/wp-content/themes/twentynineteen/readme.txt  
| Style URL: http://team1.pentest.id/wp-content/themes/twentynineteen/style.css  
?ver=1.4  
| Style Name: Twenty Nineteen  
| Style URI: https://wordpress.org/themes/twentynineteen/  
| Description: Our 2019 default theme is designed to show off the power of the  
block editor. It features custom sty...  
| Author: the WordPress team  
| Author URI: https://wordpress.org/  
|  
| Detected By: Css Style (Passive Detection)  
|  
| Version: 1.4 (80% confidence)  
| Detected By: Style (Passive Detection)  
| - http://team1.pentest.id/wp-content/themes/twentynineteen/style.css?ver=1.4  
, Match: 'Version: 1.4'  
[+] Enumerating Users  
Brute Forcing Author IDs - Time: 00:00:05 <==> (10 / 10) 100.00% Time: 00:00:05
```

- We also gather information about the users available on the target database.



```
root@user: ~
root@user: ~ 80x24
[+] Enumerating Users
Brute Forcing Author IDs - Time: 00:00:05 <==> (10 / 10) 100.00% Time: 00:00:05

[i] User(s) Identified:

[+] adminteam1
| Detected By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
|   Wp Json Api (Aggressive Detection)
|     - http://team1.pentest.id/wp-json/wp/v2/users/
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] bluemalefic
| Detected By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
|   Rss Generator (Passive Detection)
|   Wp Json Api (Aggressive Detection)
|     - http://team1.pentest.id/wp-json/wp/v2/users/
|   Rss Generator (Aggressive Detection)

[+] lgadmin
| Detected By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
|   Rss Generator (Passive Detection)
```

References

- [Nikto2 – defination](#)
- [Nmap – defination](#)
- [WPScan – defination](#)
- [Zenmap – defination](#)

[Previous Chapter](#) | [Next Chapter](#)

Meta

- [Register](#)
- [Log in](#)
- [Entries RSS](#)
- [Comments RSS](#)
- [WordPress.org](#)

Lamin BIU

 Proudly powered by WordPress.