National College of Ireland

Configuration Manual

MSc Research Project
MSc in Cybersecurity

Deepti Gupta
Student ID: x21135193

School of Computing
National College of Ireland

Supervisor: Mr. Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Deepti Gupta
Student ID:	X21135193
Programme:	MSc in Cybersecurity
Year:	2022
Module:	MSc Internship
Supervisor:	Mr. Vikas Sahni
Submission Due Date:	06/01/2023
Project Title:	Configuration Manual
Word Count:	2170
Page Count:	18

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ……Deepti Gupta……..……..……

Date: ……05/01/2023……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Deepti Gupta
X21135193

1 Introduction

DeepRecon is a python tool designed for automating recon and information gathering tasks for WordPress websites mainly, but it works on other CMS and web applications as well. It is developed by Deepti Gupta and is intended for use by cybersecurity professionals and researchers interested in collecting and analyzing information about a target website and people that are worried about the security of their application infrastructure.

The tool is designed to perform a variety of tasks on small to medium scope targets, including collecting live subdomains and sub-subdomains, spidering and analyzing archived versions of the target website, extracting JavaScript files, conducting content discovery, performing port scans, and vulnerable links etc. It also includes features for scanning for subdomain vulnerabilities, scanning links for Common Vulnerabilities and Exposures (CVEs), analyzing security headers, and identifying misconfigurations and vulnerabilities on the target website.

2 Applied Software

1.1 Python

Python is a popular, high-level programming language known for its simplicity, readability, and flexibility. It is widely used in a variety of fields, including web development, data analysis, artificial intelligence, scientific computing, and more (Peta, October 2022International). Some key features of Python include a large standard library that supports many common programming tasks, such as connecting to web servers, reading and writing files, and handling data, a simple and consistent syntax, which makes it easy to learn and use, dynamically-typed, which means that there is no need to specify the data type of a variable when declaring it, object-oriented, which means that objects and methods to represent real-world entities and actions can be created (Peta, October 2022).

1.2 Bash (Shell)

Shell script is a type of script written for the shell, or command line interpreter, of an operating system (Yiwen Dong, April 2022). It is typically used to automate tasks that are performed on the command line, such as setting up environments, running commands, and manipulating files. Shell script is commonly used in Unix-like operating systems, such as Linux and macOS (Yiwen Dong, April 2022).

[1] Python: https://www.python.org/
[2] Bash: https://www.gnu.org/software/bash/

2 Configuration

2.1 Hardware Configuration

- A processor that supports the tools and languages used in the script
- At least 1 GB of RAM
- Enough storage to hold the script and its output files
- A Unix-like operating system, such as Linux or macOS
- Python 3 installed on the system
- The packages installed on the system are : git, golang, python3, python3-pip, ruby, and screen.

2.2 Software Configuration

In order to use DeepRecon, following packages are required:

- termcolor
- optparse
- requests

Packages can be installed using pip

```
o    pip install termcolor
o    pip install optparse
o    pip install requests
```

Packages Used in Python

The following is the list of packages that are required in order for the code to run.

termcolor: This package provides functions for printing text in different colors and styles to the terminal.

optparse: This package provides a way to parse command-line options and arguments. It is used to get the target URL from the user as an input.

requests: This is a Python library that allows to send HTTP requests using Python.

Extra Tools Being Used in DeepRecon:

Subfinder is a subdomain discovery tool that uses passive sources to find subdomains of a target domain.

Assetfinder is a tool that discovers assets such as subdomains, IP addresses, and S3 buckets by using several passive sources.

Altdns is a tool that generates permutations, alterations, and mutations of subdomains and then resolves them. It is used for discovering subdomains that are not easily detectable using regular techniques.

Dirsearch is a command-line tool that performs brute-force attacks on web servers to discover directories and files.

Httpx is a tool that concurrently makes HTTP requests to a list of URLs and prints the response details.

Waybackurls is a tool that extracts URLs from the Wayback Machine (a digital archive of the World Wide Web) for a given domain.

Gau (GooglE Analytics URLs) is a tool that extracts Google Analytics tracking IDs (also known as property IDs) from a given list of URLs.

Naabu is a tool that performs port scanning and IP discovery.

Gf (Grep for) is a command-line tool that allows to search for strings in files and streams. It can be used to search for vulnerabilities in web applications.

Gf-templates is a collection of pre-defined search patterns (templates) that can be used with the gf tool to search for vulnerabilities in web applications.

Nuclei is a tool that uses pre-defined templates to scan for vulnerabilities in web applications and infrastructure.

Nuclei-templates is a collection of pre-defined templates that can be used with the nuclei tool to scan for vulnerabilities in web applications and infrastructure.

Subjack is a tool that allows to detect subdomain takeovers by checking if the DNS records of a subdomain point to an IP address that is not owned by the target organization.

[3] Subfinder: https://github.com/projectdiscovery/subfinder
[4] Assetfinder: https://github.com/tomnomnom/assetfinder
[5] Altdns: https://github.com/infosec-au/altdns
[6] Dirsearch: https://github.com/maurosoria/dirsearch
[7] Httpx: https://github.com/projectdiscovery/httpx
[8] Waybackurls: https://github.com/tomnomnom/waybackurls
[9] Gau: https://github.com/lc/gau
[10] Naabu: https://github.com/projectdiscovery/naabu
[11] Gf: https://github.com/tomnomnom/gf
[12] Gf-templates: https://github.com/1ndianl33t/Gf-Patterns
[13] Nuclei: https://github.com/projectdiscovery/nuclei
[14] Nuclei-templates: https://github.com/projectdiscovery/nuclei-templates
[15] Subjack: https://github.com/haccer/subjack

3 Installation

3.1 Python

Generally, on latest version of Windows (Windows 10) python is pre-installed in the system. But for the GUI version of the software, it has to be manually installed it. The latest version can be easily download from the internet and run to install on the system. For installing the above extra packages in Python, the following code with the package name should run in the terminal of the windows (cmd).

```
Microsoft Windows [Version 10.0.186362.267]
(c) 2022 Microsoft Corporation. All rights reserved.
C:\Windows: pip install <package_name>
```

Figure 1: Code to install packages of Python in Windows

4 Extraction

Extract the rar files from the zip (Program code) and paste all the files in the python folder.

- Create two folders in python folders - dataset and result
- Copy all the files from the zip and paste in the main folder of python installed.
- The cover images should be in the same folder as the the code is saved in.
- Copy the watermark(copyright.png) in the dataset folder created before.

5 Working

For this experiment to work, a python code file and two shell script files are needed only.

5.1 Implementing DeepRecon.py

DeepRecon.py is a script that performs recon and information gathering tasks on a given target URL. It is written in Python and uses the termcolor and optparse packages.

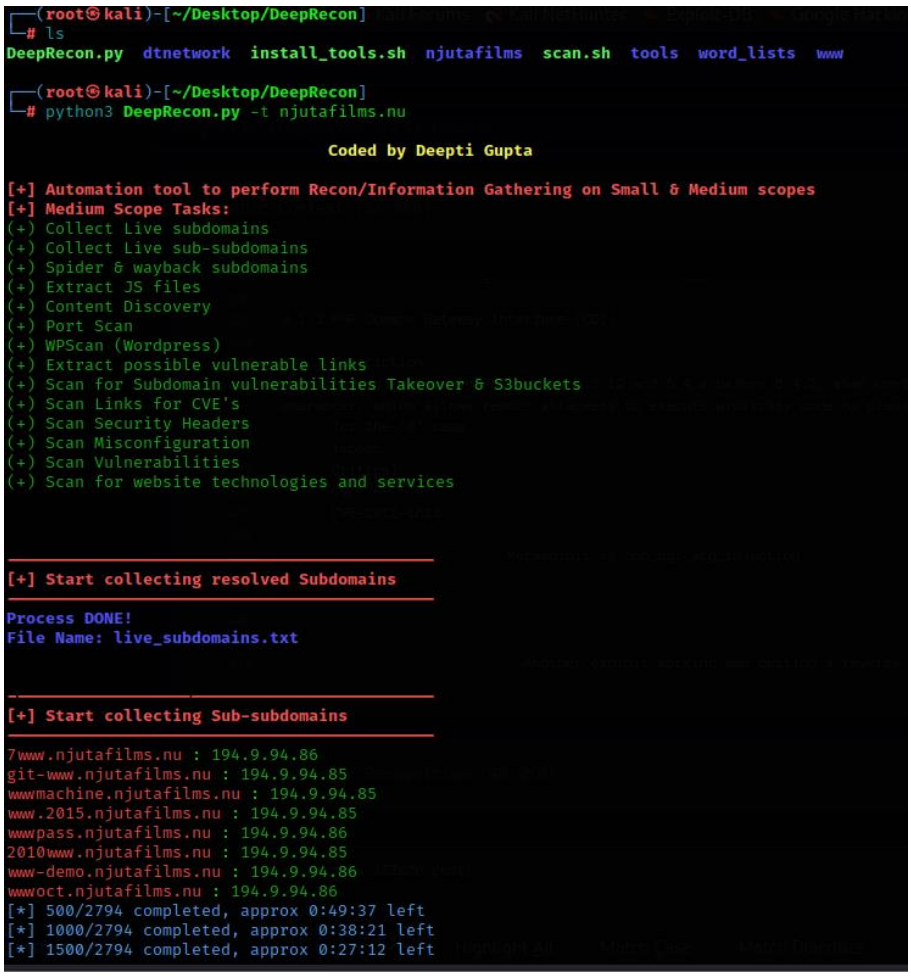


Figure 2: Running Code

1. This code contains the scanners for testing along with their commands to scan and create reports at the end in a decent way.
2. The script starts by printing a banner and a list of tasks that it can perform.

- The script then gets the target URL from the user as an input using the optparse package. If no target URL is provided, the script displays an error message and exits. Recovering of watermark is done after filters are applied.

3. After getting the target URL, the script performs the following tasks:

    - Extracts possible vulnerable links using gau
    - Scans links for CVE's using nuclei
    - Scans security headers using gau
    - Scans for misconfigurations and vulnerabilities using nuclei
    - Scans for website technologies and services using amass

The script then saves the results of the tasks in a directory called "output".

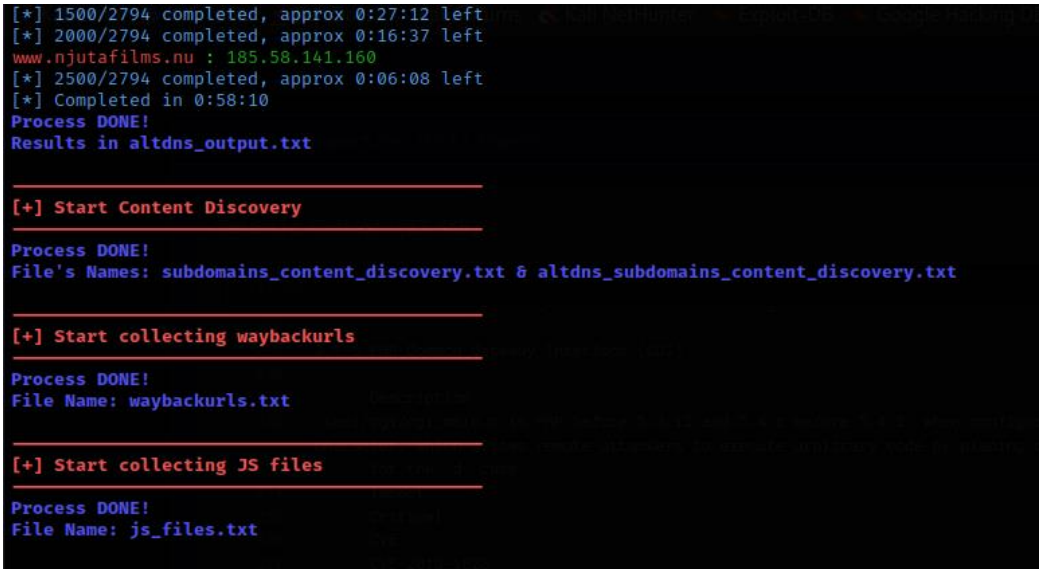


Figure 3: Reconnaissance using DeepRecon

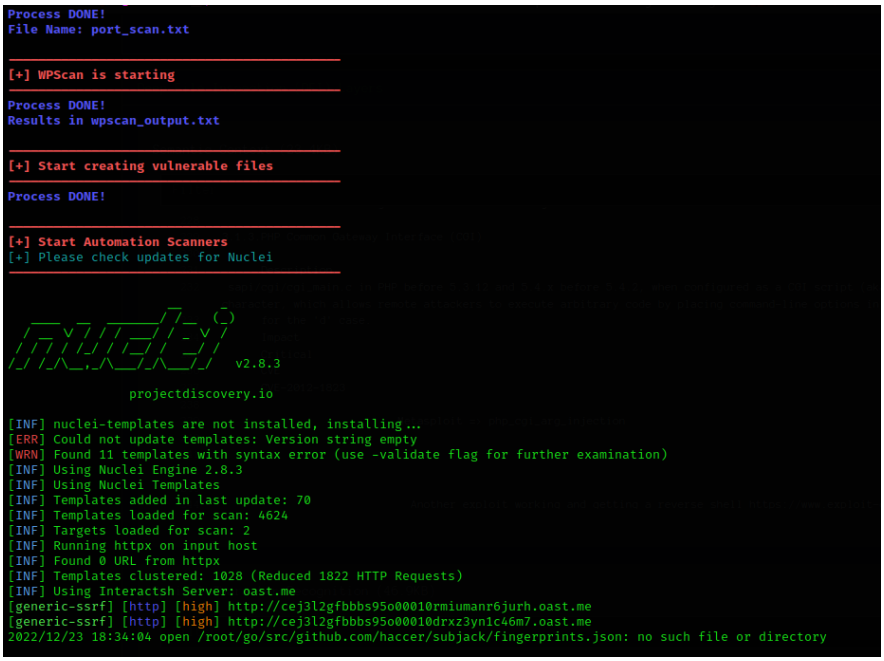


Figure 4: Automated Scanners in DeepRecon

Here is some code snippets from the script that show how to use the optparse library to parse command-line arguments:

```
import optparse

#get user input
def get_user_input():
# Create an OptionParser object to parse the command-line arguments
parser = optparse.OptionParser()

# Add an option to the parser
parser.add_option("-t", "--target_url", dest="target_url", help="\tTarget URL
(google.com, microsoft.com)")

# Parse the command-line arguments
(options, arguments) = parser.parse_args()

# If the target_url option is not provided, print an error message and exit
if not options.target_url:
print(colored("\n\n[-] Target url doesn't exist, see --help for more info", 'blue',
attrs=['bold']))
print(colored('[+] Usage: python DeepRecon.py -t target.com', 'blue',
attrs=['bold']))
print(" ")
raise SystemExit
else:
# Return the value of the target_url option
return options.target_url

# Get the value of the target_url option
user_input = get_user_input()
target = user_input
```

The optparse library provides a way to define command-line options and parse them from the command line. In the code above, the add_option() method is used to add a command-line option -t or --target_url to the parser object. The dest argument specifies the name of the attribute that will be added to the options object, which will contain the value of the option. The help argument specifies the help text that will be displayed when the --help option is used.

The parse_args() method is used to parse the command-line arguments. It returns a tuple containing the options object and a list of positional arguments. The options object is an instance of the Values class, which is a subclass of dict. The value of the target_url option can be accessed using the target_url attribute of the options object.

5.2 Implementing install.sh

Install.sh is a shell script that installs various tools and languages for recon and information gathering tasks. The script is designed to be run on a Unix-like operating system, such as Linux or macOS

5.2.1 The script starts by installing the following packages using apt-get:

- golang
- python3
- python3-pip

- ruby
- screen
- git

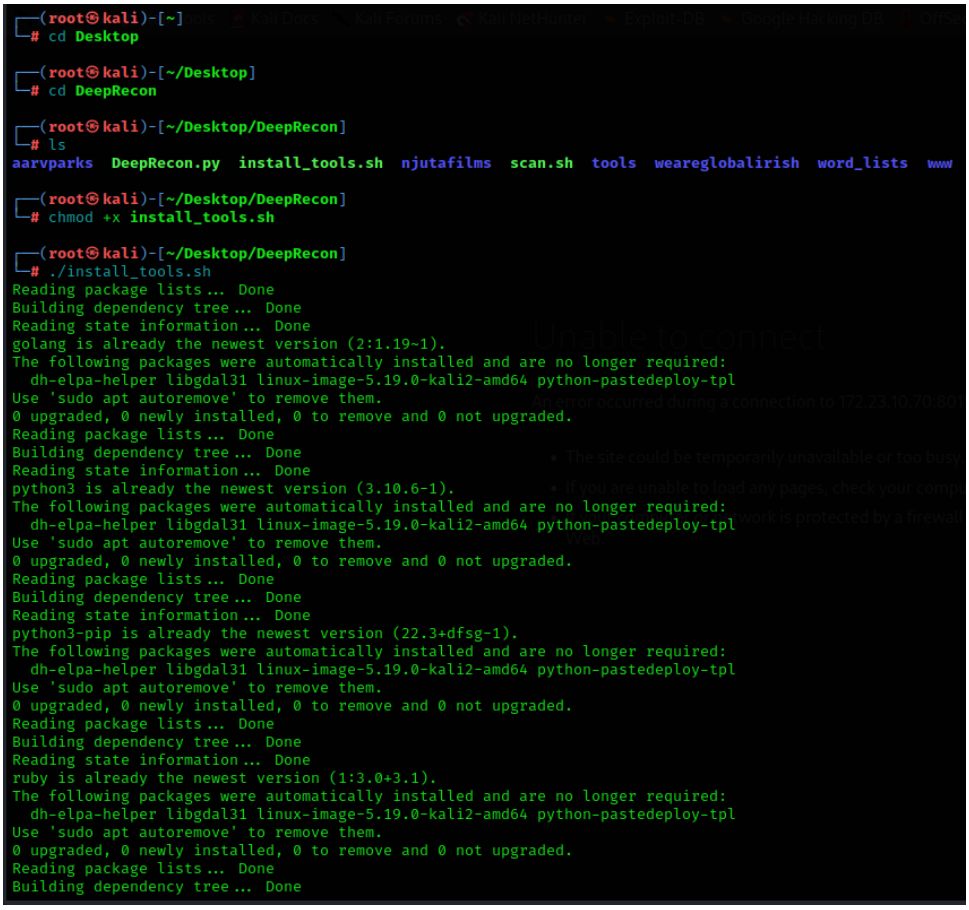


Figure 5: Running install.sh

5.2.2 Then it starts the installation of the requests package using pip3.

5.2.3 Additionally, the script then installs the following tools:

- subfinder
- httpx
- nuclei
- assetfinder
- waybackurls
- port_scanner (a script called scan.sh)
- subjack
- gau
- nuclei-templates

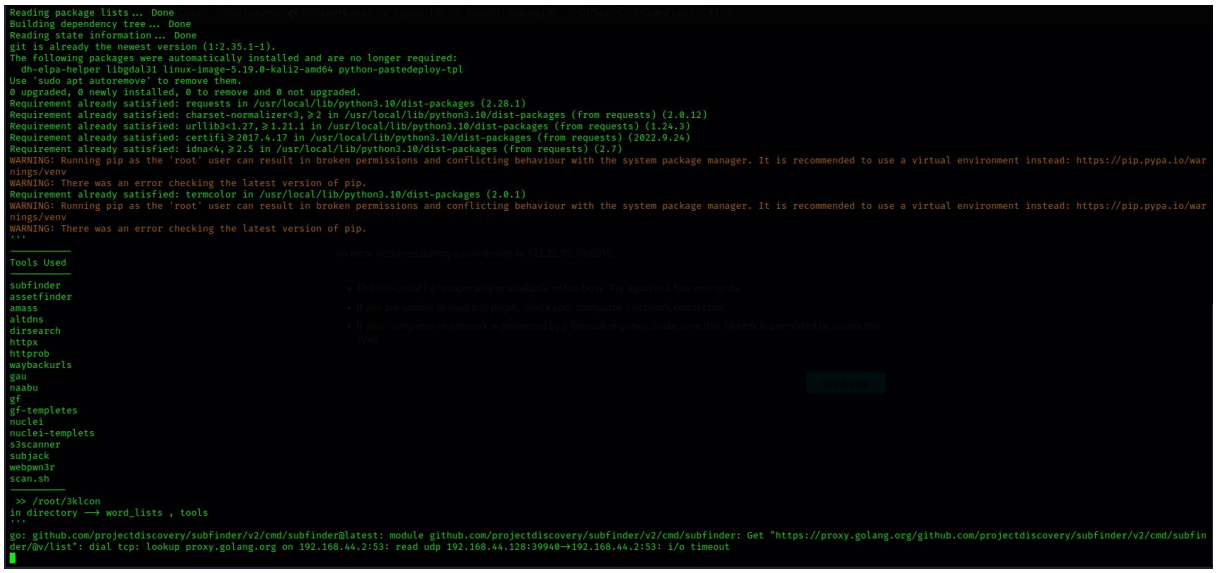


Figure 6: Installing all required tools

4. The script then installs amass & naabu.
5. Next step, it initializes the scan.sh file to perform IP Port Scan.
6. Finally, the script displays a message listing the tools and languages that were installed.

6 Full Tool Installation

1. Before any installation instruction: User must be the ROOT user
    - $ sudo su

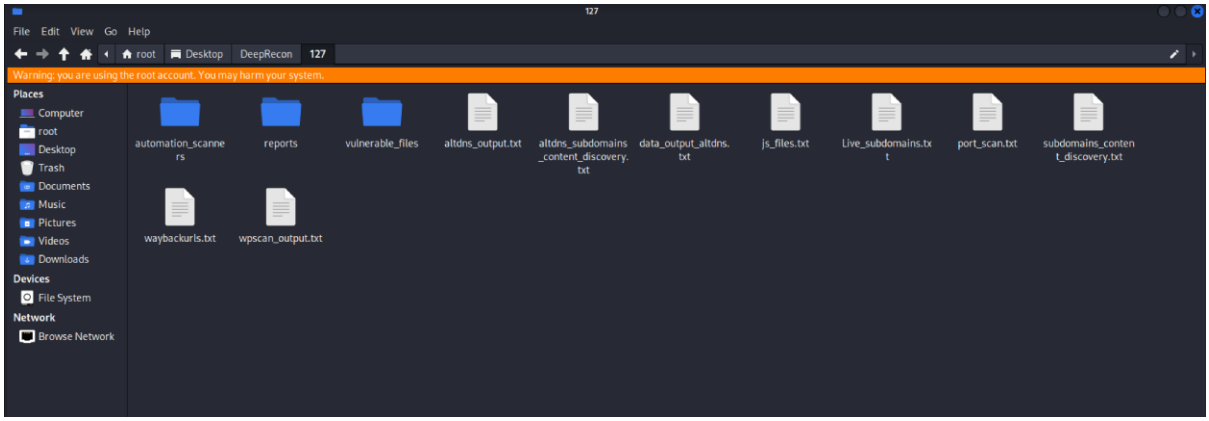
   (Because some of tools and dependencies will need the root permission)
2. Install required tools (It should must run even if tools are already installed)
    - chmod +x install_tools.sh
    - ./install_tools.sh
3. Running tool (Preferred to use python2 not python3)
4. Run this quey: python DeepRecon.py -t target.com
5. Check that the latest version of GO is installed because some tools require to be updated!
6. If any problem arises at the installation process, check that:
    - Logged in user is ROOT user not a normal user
    - Check that GO language is installed, and this path exist /root/go/bin

Note:

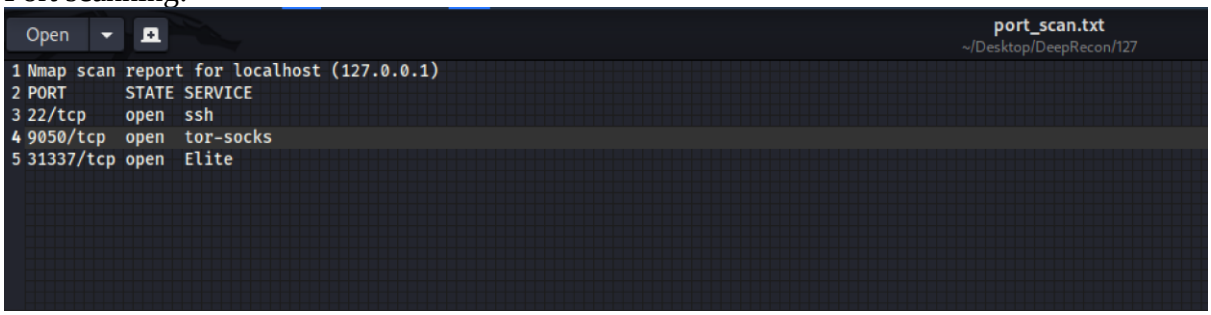
- It will take almost 5 to 6 hours running if the target is a medium. So, be Patient or use VPS (Virtual Private Server) and sleep while running :)
- It will collect all the result into one directory with the target name.

7 Results

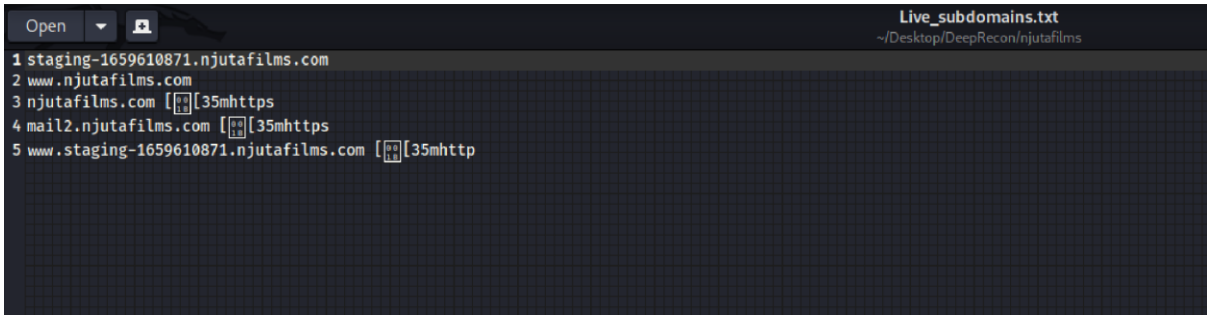
Folder structure after running the DeepRecon file:



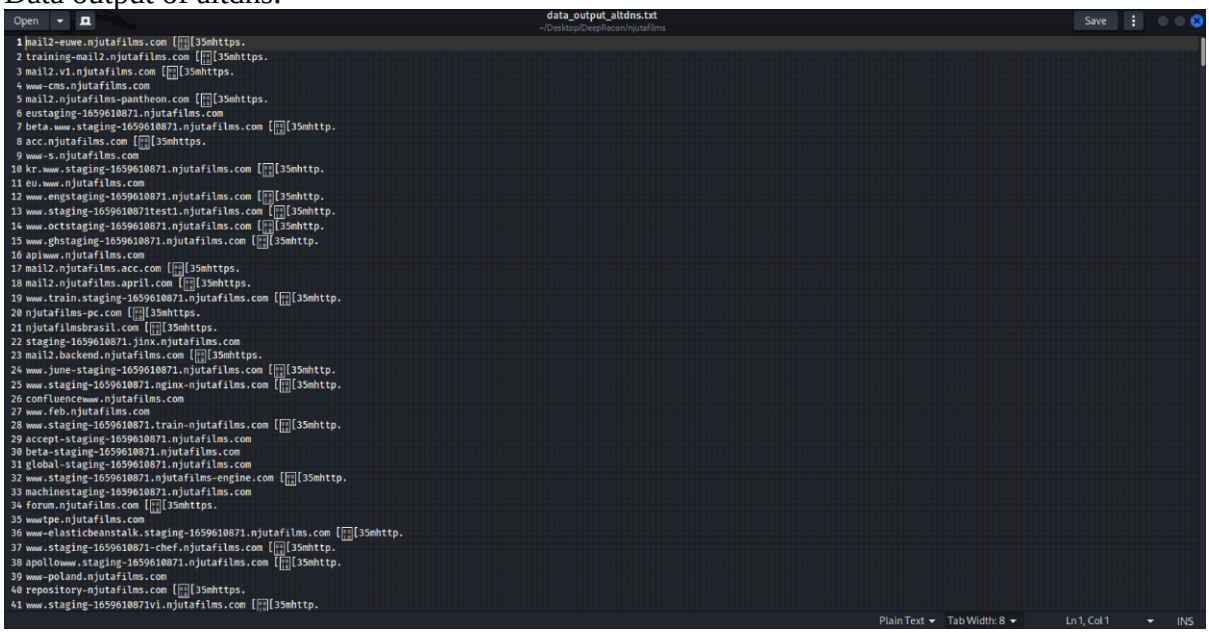
Port scanning:



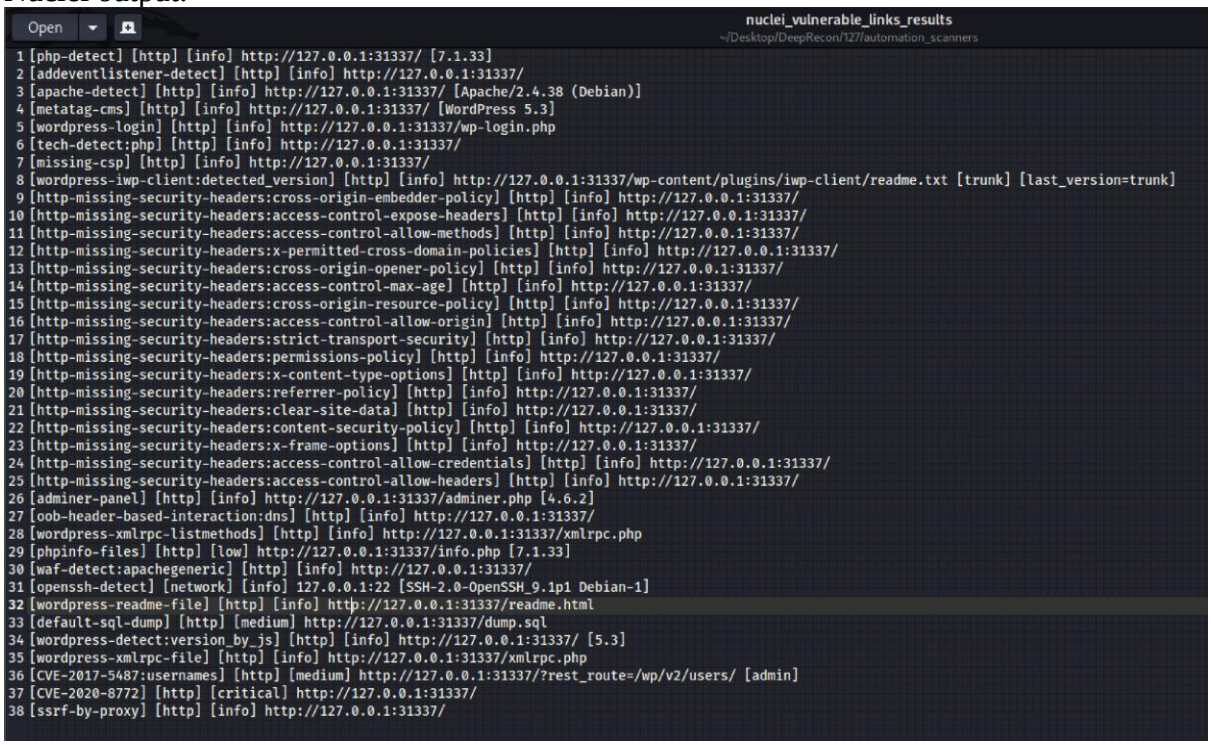
Live subdomains



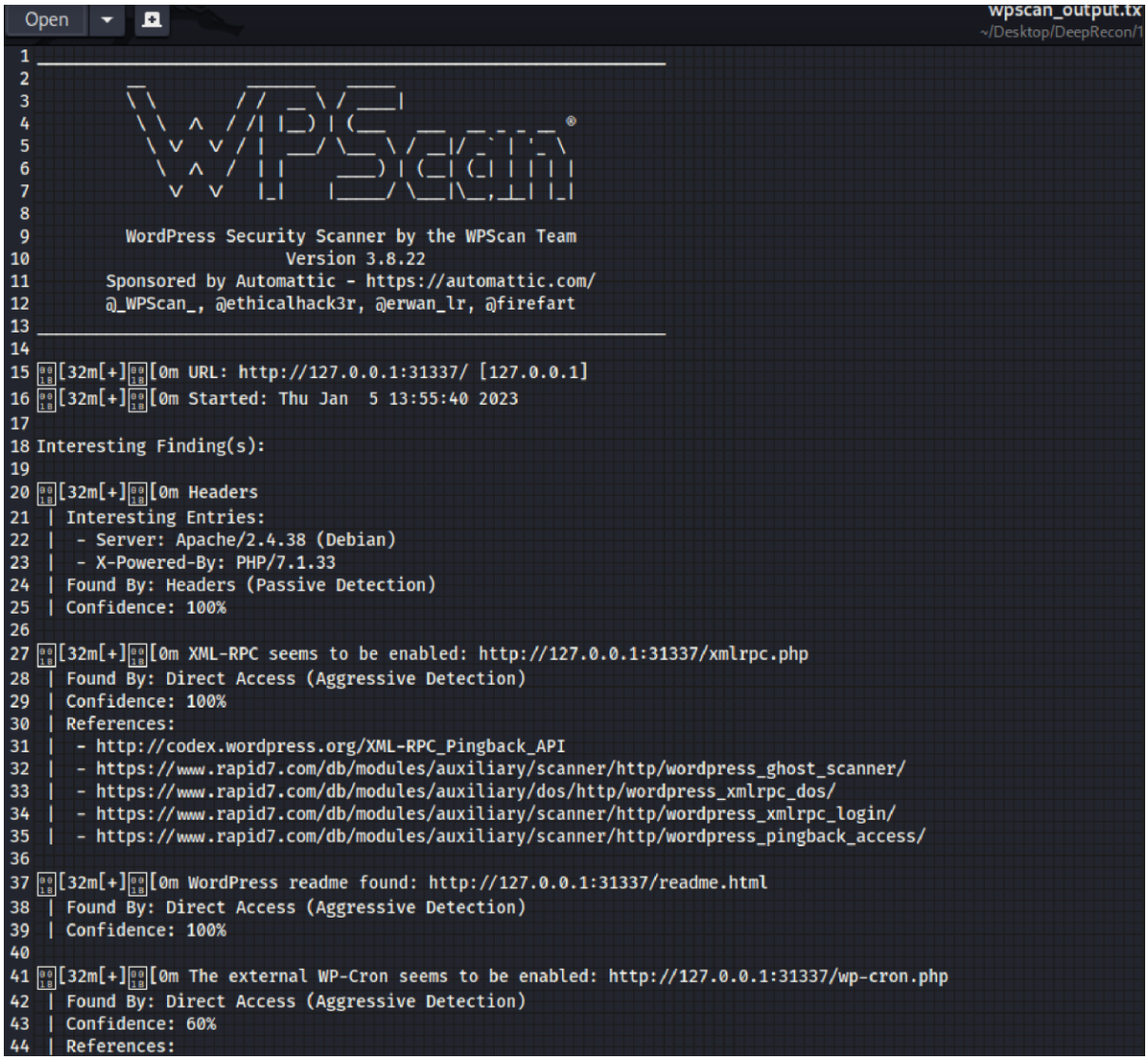
Data output of altdns:

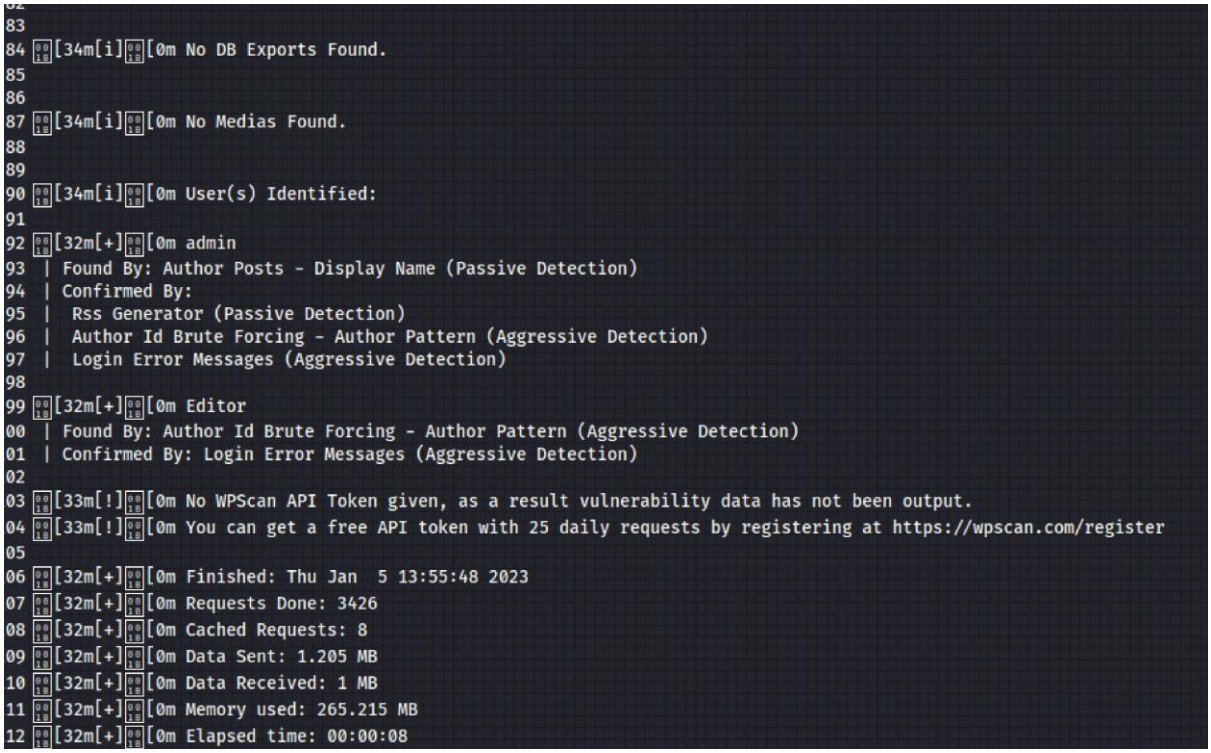


Nuclei output:



WPScan:


Open
wpscan_output.tx
~/Desktop/DeepRecon/1
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://127.0.0.1:31337/ [127.0.0.1]
[+] Started: Thu Jan 5 13:55:40 2023
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.38 (Debian)
| - X-Powered-By: PHP/7.1.33
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://127.0.0.1:31337/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_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
[+] WordPress readme found: http://127.0.0.1:31337/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://127.0.0.1:31337/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:



8 References

Peta, S. (October 2022International). Python- An Appetite for the Software Industry. *International Journal of Programming Languages and Applications 12(4):1-14*.

Yiwen Dong, Z. L. (April 2022). Bash in the Wild: Language Usage, Code Smells, and Bugs. *ACM Transactions on Software Engineering and Methodology*.

Appendix:

Monthly Internship Activity Report – Oct 2022

Student Name: Deepti Gupta Student number: x21135193

Company: ALT Digital Technologies Month Commencing: October -2022

1. Studied and analysed the current manual and automation penetration testing tools for WordPress.
2. Communicated the research updates with project manager and project mentor.
3. Learned about different vulnerabilities that are mostly found in WordPress site and were the component of OWASP.
4. Did research on the existing issues and identify the pros and cons for the proposed tool.
5. Documented the relevant research study.

Employer comments

Deepti Gupta is a great team player, and she was a big help during the new transition. She has diligently and successfully completed all the internship responsibilities listed above.

Student Signature: Deepti Gupta Date: 30th Oct 2022

Industry Supervisor Signature: Vikas Goyal Date: 04th Nov 2022

Monthly Internship Activity Report – Nov 2022

Student Name: Deepti Gupta Student number: x21135193

Company: ALT Digital Technologies Month Commencing: November -2022

1. Brainstorm methodology and finalized the methodology.
2. Completed account setup, trainings and choice of tools selection.
3. Run the Nessus tool and shared the list of vulnerabilities with the team.
4. Worked on the framework design and identify the product feasibility in terms of technical, operational, economical, legal & ethical.
5. Documented above mentioned in research report.

Employer comments

I have observed that you've been taking on increasingly challenging tasks lately. Thank you for sharing the monthly scan reports and the developers are working on it. Also, I'm pleased that you shared your ideas at our team meetings. If there is anything more you would need to know in order to contribute more successfully, do let me know.

Student Signature: Deepti Gupta Date: 30th Nov 2022

Industry Supervisor Signature: Vikas Goyal Date: 2nd Dec 2022

Monthly Internship Activity Report – Dec 2022

Student Name: Deepti Gupta Student number: x21135193

Company: ALT Digital Technologies Month Commencing: Decembere-2022

1. Developed a tool named DeepRecon, based on framework.
2. Run the tool and evaluate the results.
3. Creation of research report using the relevant data obtained via the industrial internship and the implementation of the research.

Employer comments

Deepti completed the tasks assigned to her promptly and diligently.
Deepti has already established herself as a crucial member of the team, completing all responsibilities to a quality that exceeds what was first anticipated. If there is anything I can do to help you, do let me know. Continue your wonderful work!

Student Signature: Deepti Gupta Date: 31st Dec 2022

Industry Supervisor Signature: Vikas Goyal Date: 3rd Jan 2023