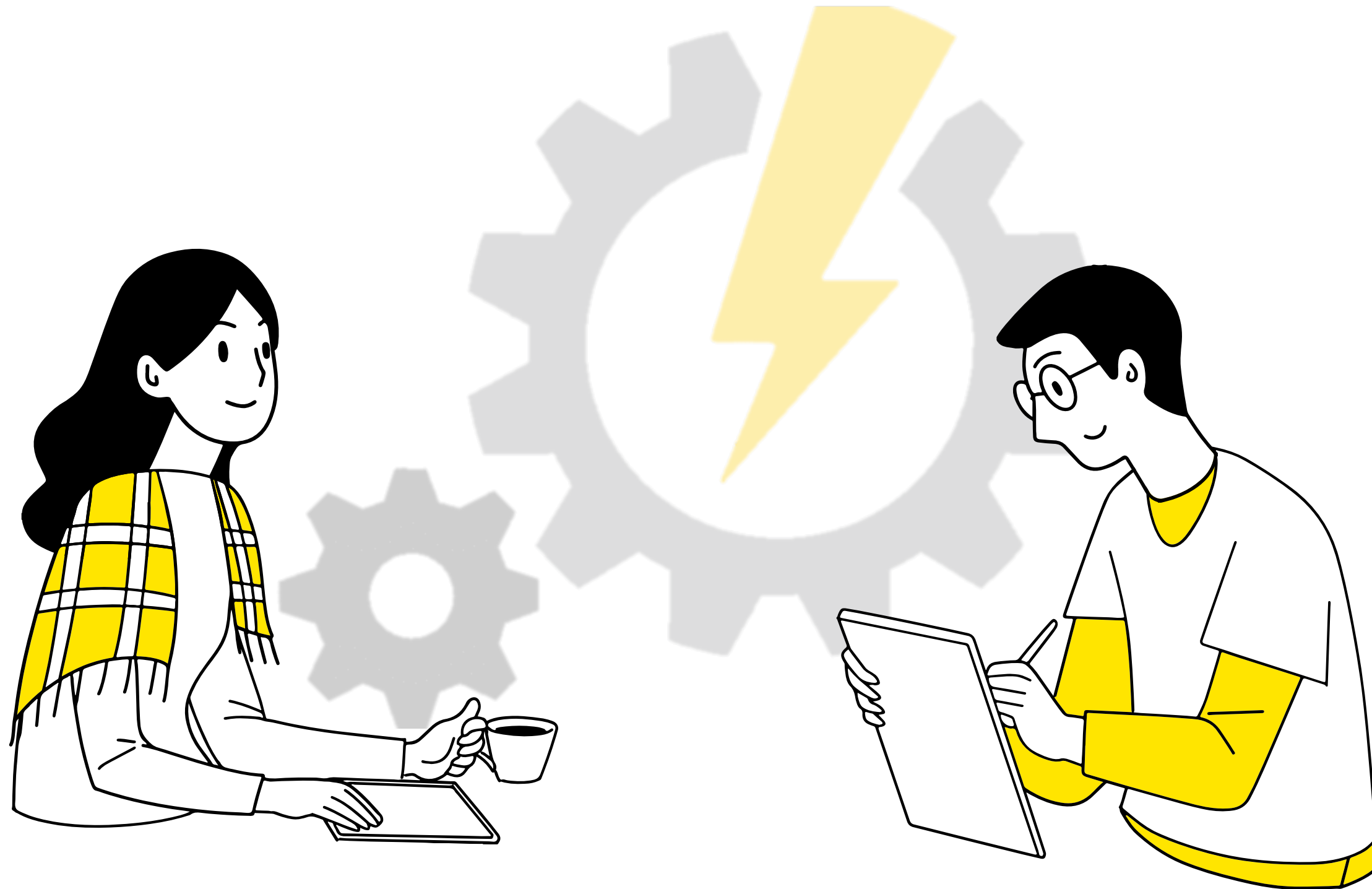


Bug Bounty Automation



Objectives

- It is the collection of pentesting tools. It's scan the target and generates the reports in text format.

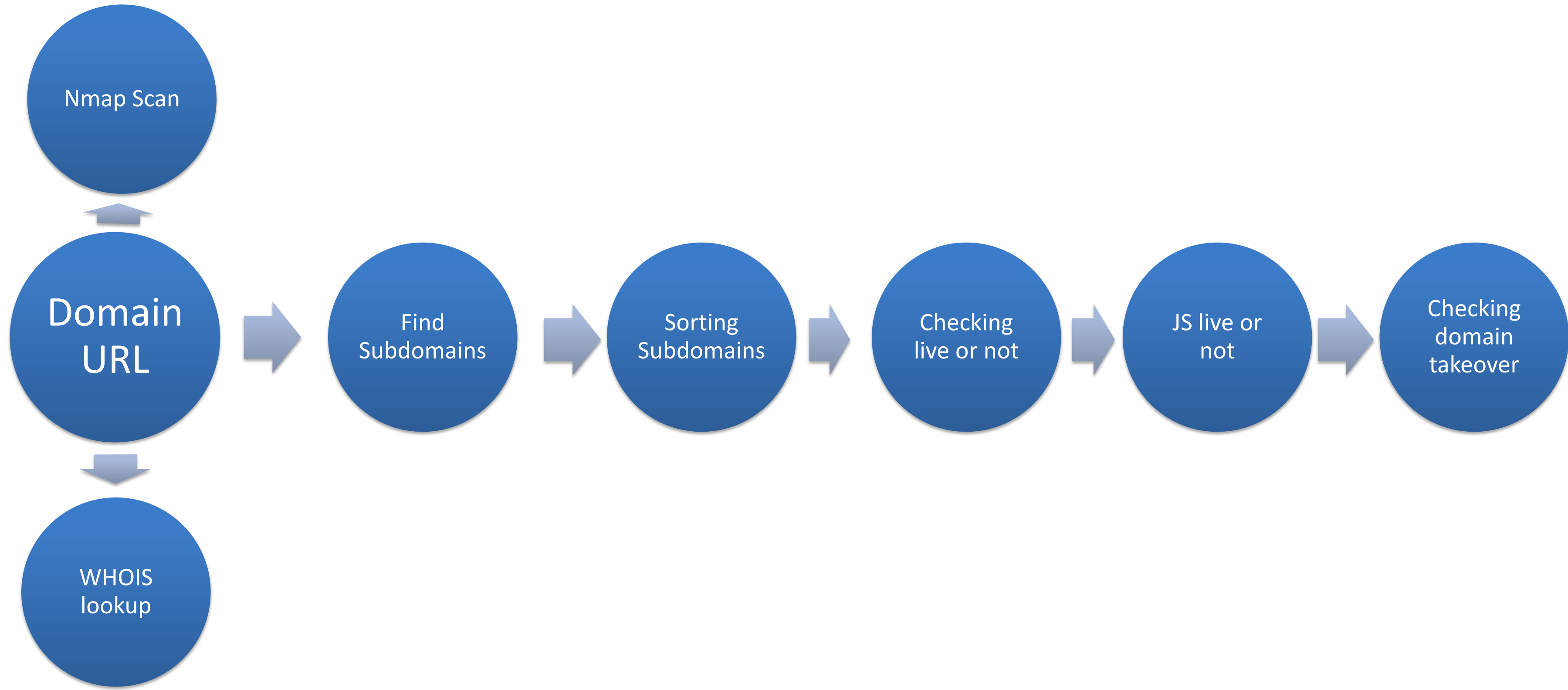
Benefits

- Easily identify low-hanging vulnerabilities.
- Continuous recon to capture changing environments.
- Maximize time and profit by automating repetitive tasks.

Data Sharing Agreement (Domain URL)

- Data Folder Name: **Domain_Name**
- Number of Files: **8+ (Depends on number of Subdomains)**
- Number of Folder: **<User Defined>**
- Files Name: NmapScan_\$url.txt, Subdomains.txt, SubdomainsSorted.txt, Whois_\$url.com, aliveSubdomains.txt , JsAliveSubdomains.txt, DomainsTakeover.txt
- File type: **.TXT format**

Architecture



Download Tool from GitHub

Step 1: Copy the HTTPS Link

The screenshot shows the GitHub interface for the repository 'sahsisunny/xProBBA'. The 'Code' button is clicked, opening a dropdown menu. The 'HTTPS' option is selected, and the URL 'https://github.com/sahsisunny/xProBBA.git' is highlighted with a yellow box. A yellow arrow points to the copy icon next to the URL.

Browser address bar: `https://github.com/sahsisunny/xProBBA`

Repository: **sahsisunny / xProBBA** (Public)

Navigation: Code (selected), Issues, Pull requests, Actions, Projects, Wiki, Security, Insights

Repository details: main (1 branch), 1 tag

Clone dropdown menu:

- Clone (icon)
- HTTPS (selected)
- GitHub CLI
- `https://github.com/sahsisunny/xProBBA.git` (highlighted)
- Use Git or checkout with SVN using the web URL.
- Open with GitHub Desktop
- Download ZIP

Repository files:

- src: Update banner.png
- wordlist: add wordlist directory
- README.md: remove Resuscan module from all
- setup.sh: remove Resuscan module from all
- xprobbas.sh: Update xprobbas.sh

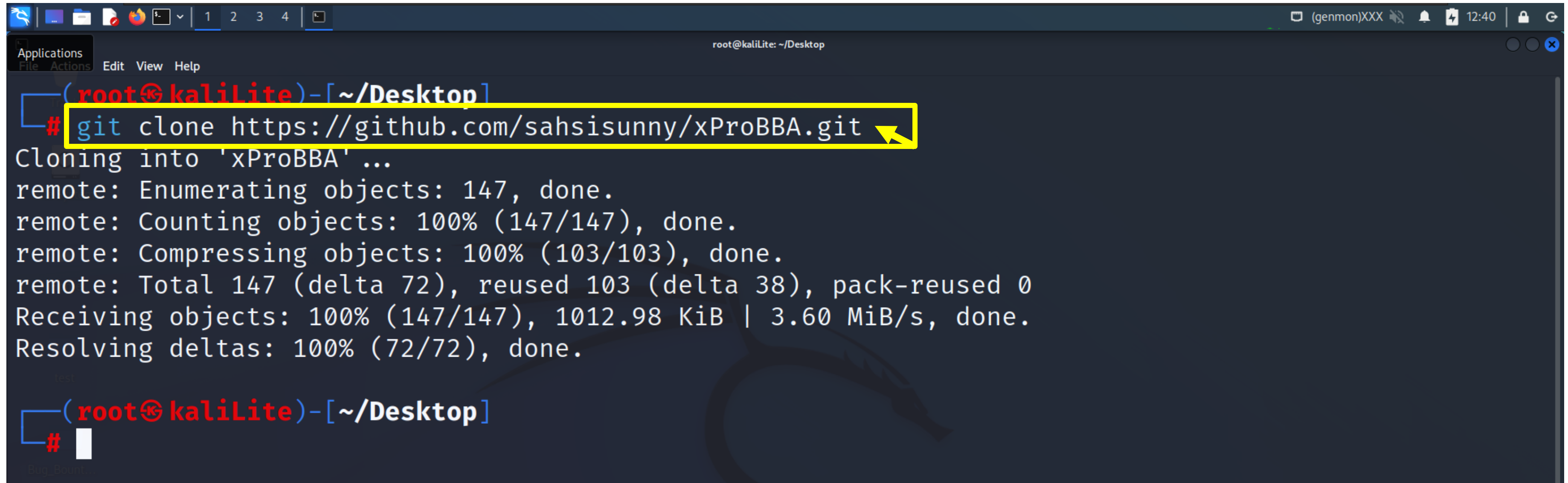
About section:

It is the collection of pentesting tools. It's scan the target and generates the reports in text format. root user is necessary to used this tool.

Tags: bash, nmap, bugbounty, bugbountyautomation

Stats: Readme, 0 stars, 1 watching, 0 forks

Step 2: Clone on Kali Linux Machine



A terminal window on a Kali Linux machine. The window title is "root@kaliLite: ~/Desktop". The terminal shows the command `git clone https://github.com/sahsisunny/xProBBA.git` being executed. The output shows the cloning progress, including enumerating, counting, and compressing objects, and receiving the data. The prompt then returns to the shell.

```
(root@kaliLite)-[~/Desktop]
# git clone https://github.com/sahsisunny/xProBBA.git
Cloning into 'xProBBA' ...
remote: Enumerating objects: 147, done.
remote: Counting objects: 100% (147/147), done.
remote: Compressing objects: 100% (103/103), done.
remote: Total 147 (delta 72), reused 103 (delta 38), pack-reused 0
Receiving objects: 100% (147/147), 1012.98 KiB | 3.60 MiB/s, done.
Resolving deltas: 100% (72/72), done.

(root@kaliLite)-[~/Desktop]
#
```

Step 3: Give executable permission to the files

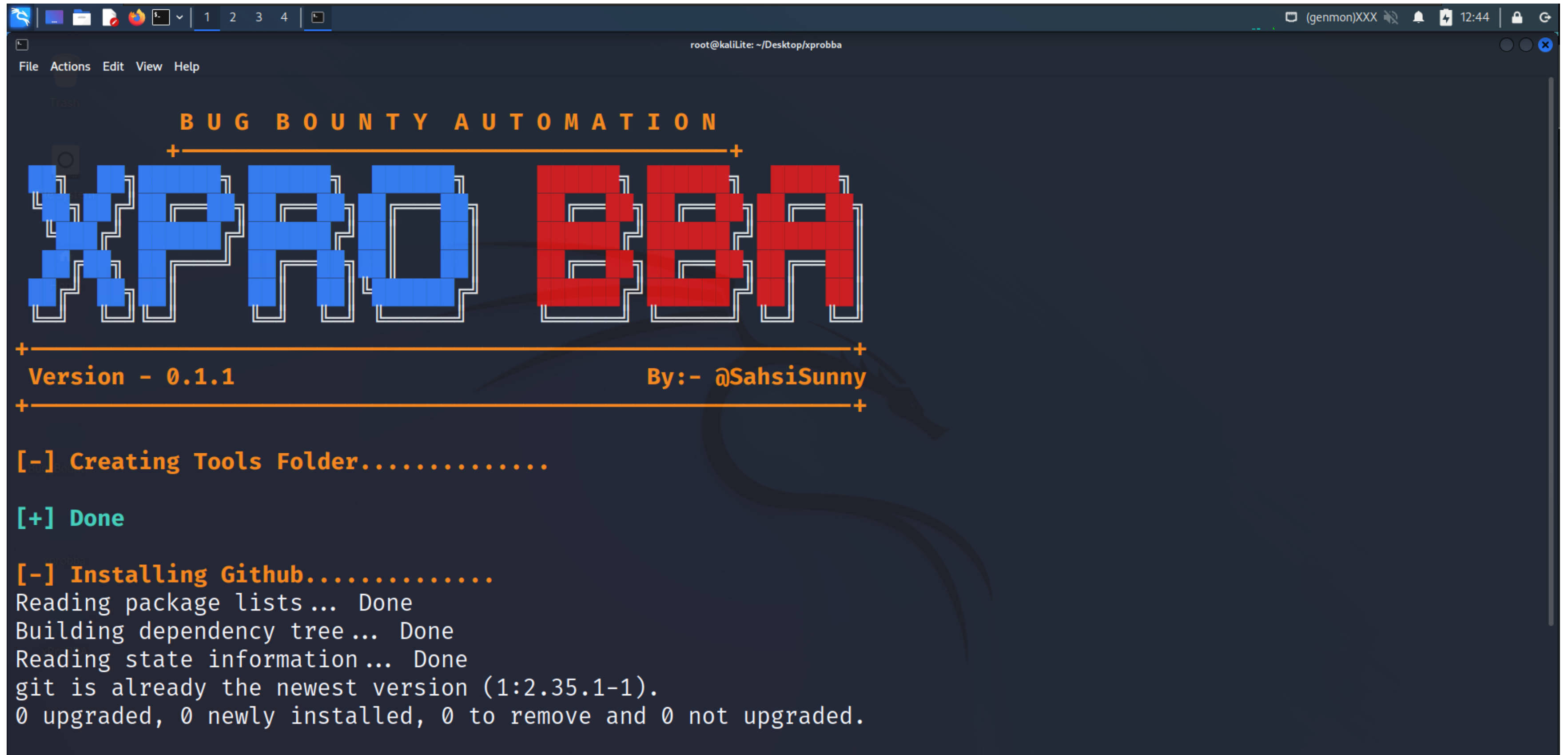
```
(root@kaliLite)-[~/Desktop]
# cd xprobba

(root@kaliLite)-[~/Desktop/xprobba]
# chmod 777 *

(root@kaliLite)-[~/Desktop/xprobba]
# ls -al
total 48
drwxr-xr-x 6 root root 4096 Jun 26 12:05 .
drwxr-xr-x 6 root root 4096 Jun 26 12:39 ..
drwxr-xr-x 8 root root 4096 Jun 26 12:04 .git
-rwxrwxrwx 1 root root 1903 Jun 26 12:04 README.md
-rwxrwxrwx 1 root root 6188 Jun 26 12:04 setup.sh
drwxrwxrwx 2 root root 4096 Jun 26 12:04 src
drwxrwxrwx 2 root root 4096 Jun 26 12:38 vulnweb.com
drwxrwxrwx 2 root root 4096 Jun 26 12:04 wordlist
-rwxrwxrwx 1 root root 8416 Jun 26 12:04 xprobba.sh

(root@kaliLite)-[~/Desktop/xprobba]
```


Step 4: Run “setup.sh” file



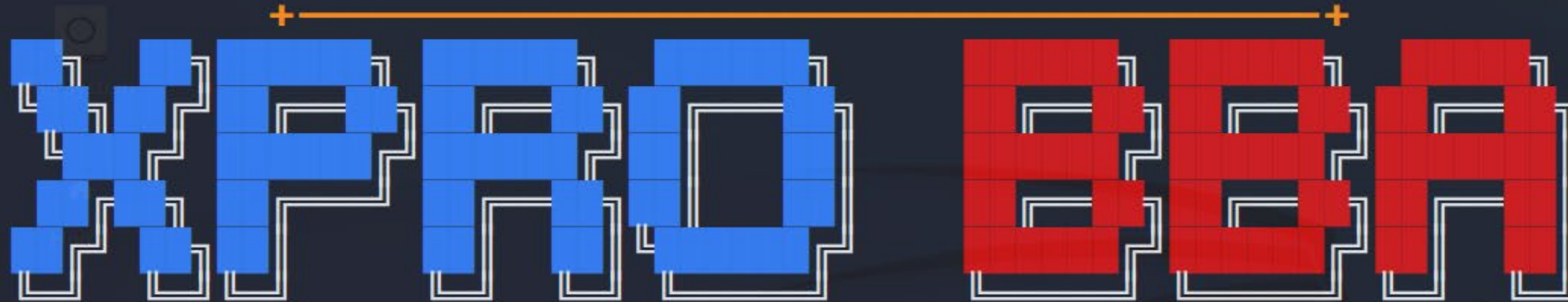
The image shows a terminal window titled "root@kaliLite: ~/Desktop/xprobba". The terminal displays the output of a script, including a large ASCII art logo for "WPFOGBA" and a progress report. The logo consists of the letters "WPFOGBA" in a stylized, blocky font. The letters "W", "P", "F", "O", and "B" are blue, while "G", "A", and "A" are red. Above the logo is the text "BUG BOUNTY AUTOMATION" in orange. Below the logo is the text "Version - 0.1.1" and "By:- @SahsiSunny" in orange. The progress report shows the following steps:

```
[+] Done
[-] Installing Github.....
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (1:2.35.1-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Step 5: Run “xprobba.sh” script for BBA

```
(root@kaliLite)-[~/Desktop/xprobba]  
# ./xprobba.sh vulnweb.com
```

BUG BOUNTY AUTOMATION

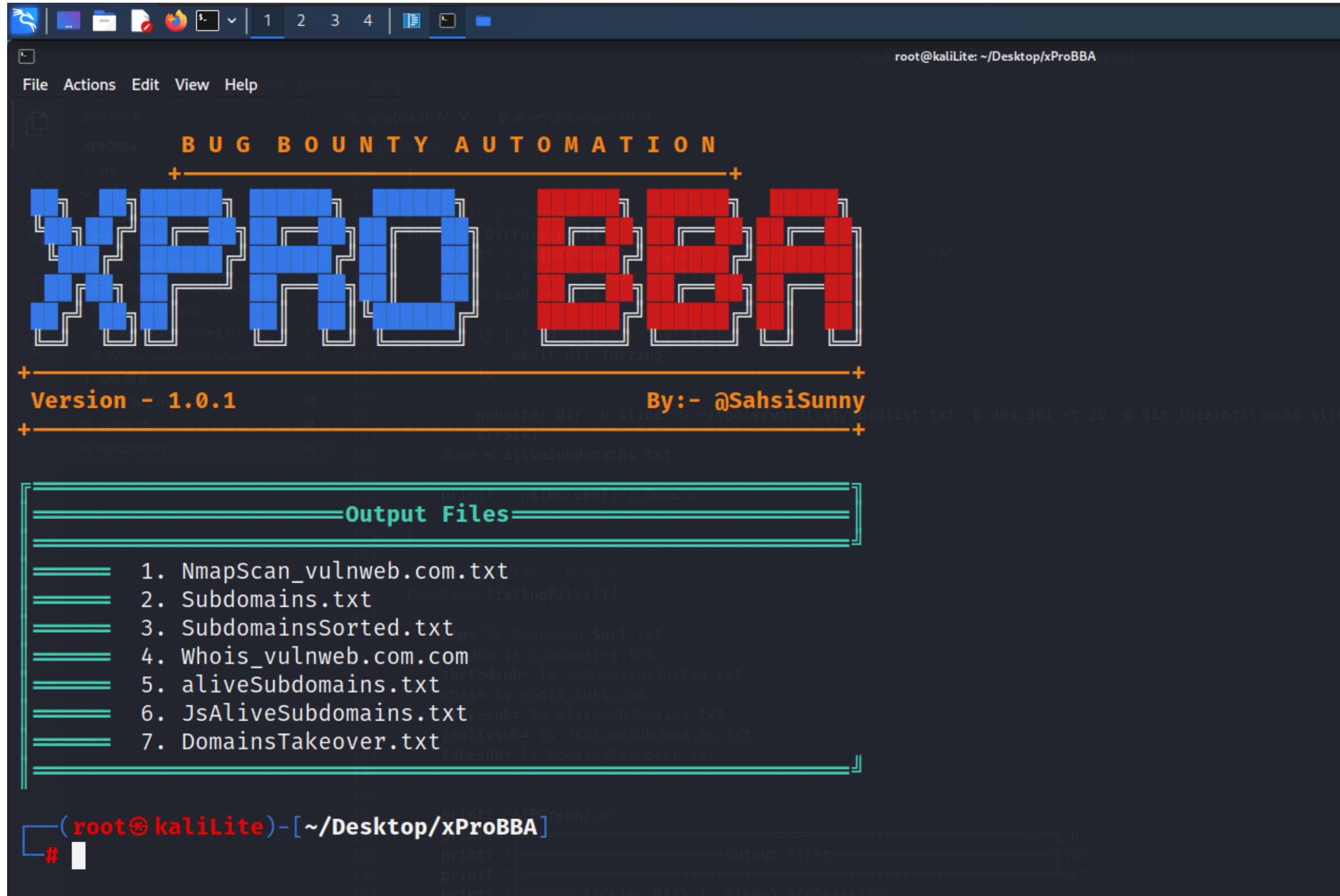


Version - 1.0.1

By:- @SahsiSunny

[-] Aggressive Scanning through Nmap.....

Step 6: Output Data Saved files



```
root@kaliLite: ~/Desktop/xProBBA
File Actions Edit View Help
BUG BOUNTY AUTOMATION
+-----+
xProBBA
+-----+
Version - 1.0.1
By:- @SahsiSunny
+-----+
Output Files
=====
1. NmapScan_vulnweb.com.txt
2. Subdomains.txt
3. SubdomainsSorted.txt
4. Whois_vulnweb.com.com
5. aliveSubdomains.txt
6. JsAliveSubdomains.txt
7. DomainsTakeover.txt
=====
(root@kaliLite)-[~/Desktop/xProBBA]
#
```

Steps to Deploy and Use

- `git clone https://github.com/sahsisunny/xProBBA.git`
- `cd xProBBA`
- `chmod 777 *`
- `./setup.sh`
- `./xprobba.sh {DOMAIN_URL}`