1. System & Language Installation

Python 3

```
sudo apt-get update -y
sudo apt-get dist-upgrade -y
sudo apt install -y python3
sudo apt install -y python3-pip
sudo apt install python3.12-venv
python3 --version
pip3 --version
```

Golang

```
sudo apt-get update -y
sudo apt-get dist-upgrade -y
wget https://go.dev/dl/go1.23.3.linux-amd64.tar.gz
rm -rf /usr/local/go
sudo tar -C /usr/local -xzf go1.23.3.linux-amd64.tar.gz
echo $SHELL
echo 'export PATH=$PATH:/usr/local/go/bin' >> ~/.zshrc
echo 'export PATH=$PATH:/usr/local/go/bin' >> ~/.bashrc
echo 'export PATH=$PATH:~/go/bin' >> ~/.zshrc
echo 'export PATH=$PATH:~/go/bin' >> ~/.bashrc
source ~/.zshrc
source ~/.bashrc
go version
rm -rf go1.23.3.linux-amd64.tar.gz
```

C-Make

```
sudo apt-get update -y
sudo apt-get dist-upgrade -y
sudo apt install cmake -y
```

Rust

```
sudo apt-get update -y
sudo apt-get dist-upgrade -y
curl --proto '=https' --tlsv1.2 -sSf https://sh.rustup.rs | sh
source $HOME/.cargo/env
rustc --version
```

2. Tool Installation

urldedupe

```
git clone https://github.com/ameraman/urldedupe.git
cd urldedupe
cmake CMakeLists.txt
make
sudo cp urldedupe /usr/local/bin/
cd ../
urldedupe -h
```

Arjun

```
git clone https://github.com/s0md3w/Arjun.git
python3 -m venv arjun-env
source arjun-env/bin/activate
cd Arjun
pip3 install .
sudo cp ~/arjun-env/bin/arjun /usr/local/bin/
deactivate
cd ../
arjun -h
```

Waymore

```
git clone https://github.com/xnl-h4ck3r/waymore.git
python3 -m venv waymore-env
source waymore-env/bin/activate
cd waymore
pip3 install .
pip3 install -r requirements.txt
sudo cp ~/waymore-env/bin/waymore /usr/local/bin/
deactivate
cd ../
waymore -h
```

Sublist3r

```
git clone https://github.com/aboul3la/Sublist3r.git
python3 -m venv sublist3r-env
source sublist3r-env/bin/activate
cd Sublist3r
pip3 install .
pip3 install -r requirements.txt
```

```
sudo cp ~/sublist3r-env/bin/sublist3r /usr/local/bin/
deactivate
cd ../
sublist3r -h
```

Dirsearch

```
git clone https://github.com/maurosoria/dirsearch.git --depth 1
python3 -m venv dirsearch-env
source dirsearch-env/bin/activate
cd dirsearch
pip3 install .
pip3 install -r requirements.txt
sudo cp ~/dirsearch-env/bin/dirsearch /usr/local/bin/
deactivate
cd ../
dirsearch -h
```

subExtreme

```
sudo apt-get update -y
sudo apt-get dist-upgrade -y
sudo apt install pkg-config -y
sudo apt install libssl-dev -y
git clone https://github.com/ahmedkhlief/subextreme.git
cd subextreme
cargo build --release
sudo cp target/release/subextreme /usr/local/bin/
sudo chmod +x /usr/local/bin/subextreme
subextreme -h
cd ../
```

Httpx

```
sudo rm -f /usr/bin/httpx
sudo apt remove httpx -y
go install -v github.com/projectdiscovery/httpx/cmd/httpx@latest
httpx -h
```

Crawley

```
mkdir crawley
cd crawley
wget
https://github.com/s8rg/crawley/releases/download/v1.7.18/crawley_v1.7.19_linux_x86_64.tar.gz
tar -xvzf crawley_v1.7.19_linux_x86_64.tar.gz
```

```
sudo cp crawley /usr/local/bin/
cd ../
crawley -h
```

PassURLs

```
git clone https://github.com/ahmedkhlief/passurls.git
python3 -m venv passurls-env
source passurls-env/bin/activate
cd passurls
pip3 install .
pip3 install -r requirements.txt
sudo cp ~/passurls-env/bin/passurls /usr/local/bin/
deactivate
cd ../
passurls -h
```

Dalfox

```
go install github.com/hahwul/dalfox/v2@latest
dalfox -h
```

Seelists

```
git clone https://github.com/danielmiessler/Seelists.git
```

3. Utility Configuration

Import Burp Suite Certificate

Export certificate from Burp Suite as a .der file to your home directory.

```
openssl x509 -inform DER -in ~/burp.der -out ~/burp-ca.crt
sudo cp ~/burp-ca.crt /usr/local/share/ca-certificates/
sudo update-ca-certificates
```

4. Reconnaissance Workflow Commands

Initial Setup

```
mkdir bugbounty
cd bugbounty
mkdir target
cd target
```

Subdomain Enumeration

```
sublist3r -d example.com -b -t 50 -v -o sublist3r.txt
subextreme -w ~/SecLists/Discovery/DNS/subdomains.txt -d example.com -c 100 -o subextreme.txt
cat sublist3r.txt subextreme.txt | urldedupe -s > subdomains.txt
```

URL Discovery (Waymore)

```
waymore -i subdomains.txt -o waymore_urls.txt
cat waymore_urls.txt | urldedupe > unique_urls.txt
```

Proxy URLs through Burp Suite

```
passurls -p 127.0.0.1:8080 -i unique_urls.txt
```

Deep Crawling (Through Proxy)

```
export http_proxy="http://127.0.0.1:8080"
export https_proxy="http://127.0.0.1:8080"
export ALL_PROXY="http://127.0.0.1:8080"
crawley --headless --delay 30ms --depth -1 --subdomains --all --timeout 30s --user-agent "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36" https://example.com/ | tee crawley.txt
```