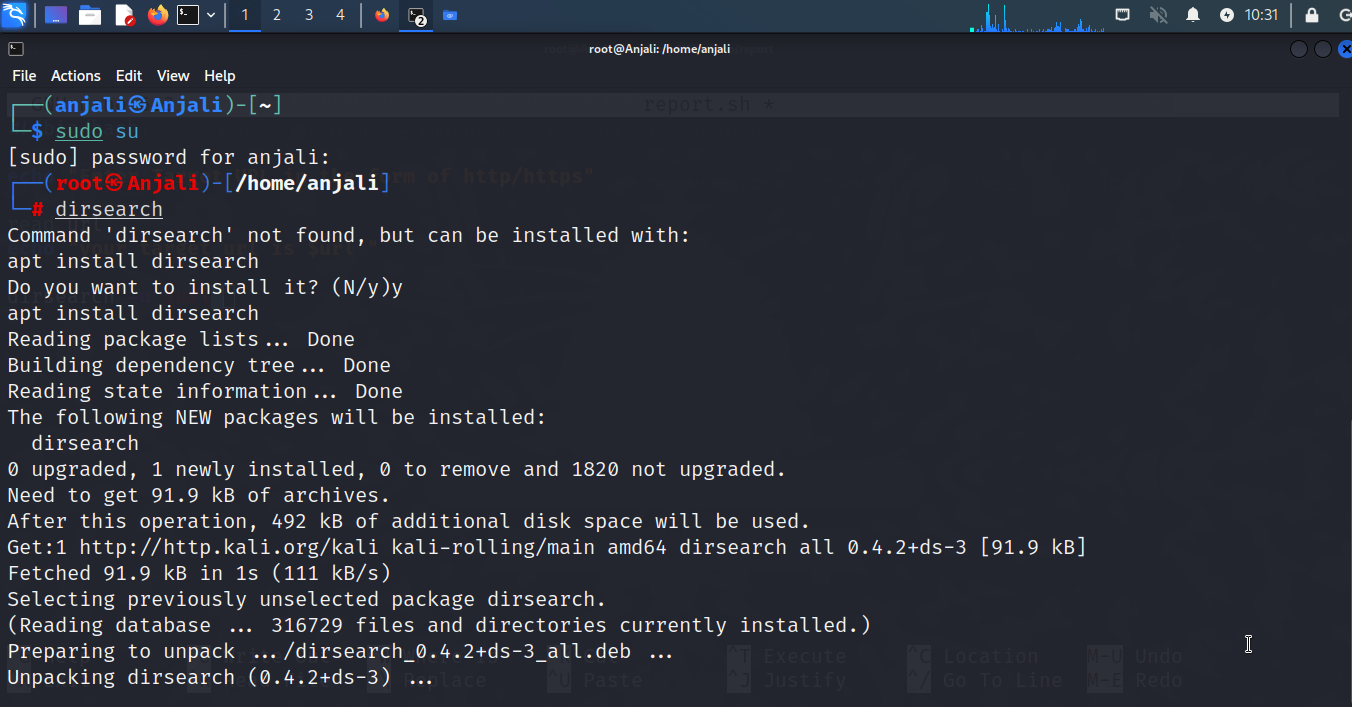
* **Dependences**

**Tools :**

1. **whois**
2. **dmitry**
3. **assetfinder**
4. **subfinder**

* if above mentioned tools are not download then just right the tool name and then enter. E.g: assetfinder

****

* **SOURCE CODE**

#!/bin/bash

#some font color's for better interface.

Red=`tput setaf 1 bold`

White=`tput setaf 7`

Green=`tput setaf 2 bold`

echo "=================================================="

echo "${Red}Enter Target Domain name e,g google.com"

echo "${White}"

# target domain input.

read domain

echo "${Green}your target url is https://$domain/ "

echo " exicuting whois on $domain "

echo "------------------------------------------------"

echo "${White}"

#collection some information with the whois tool.

whois $domain > whois.txt

#grep some important and common stuff.

cat whois.txt | grep -n [0-9]

echo "======================================================================="

echo "${Red}what type of information you want about your target -p indicate passive information gathering -sb indicate subdomain info:P/sb "

echo "${White}"

# taking input for scan.

read scantype

if [ $scantype == p ] || [ $scantype == "sb" ]

then

if [ $scantype == p ]

then

echo "${Green}you select for passive information gattering "

echo " scanning done by dmitry tool..."

echo "${White}"

echo "${white}------------------------------------"

# run the passive information gattering tool i.e. dmitry.

dmitry $domain

else

echo "${Green}you select for sub domains finding"

echo "subdomain finding done by diffrent tools like assetfinder , subfinder..."

echo "======================"

echo "it's may take long time plz wait"

echo "----------------------"

echo "${White}"

# Run Assetfinder and save the output

assetfinder --subs-only "$domain" > assetfinder.txt

# Run Subfinder and save the output

subfinder -d "$domain" > subfinder.txt

# Consolidate and sort the results

cat assetfinder.txt subfinder.txt | sort -u > subdomanoutput.txt

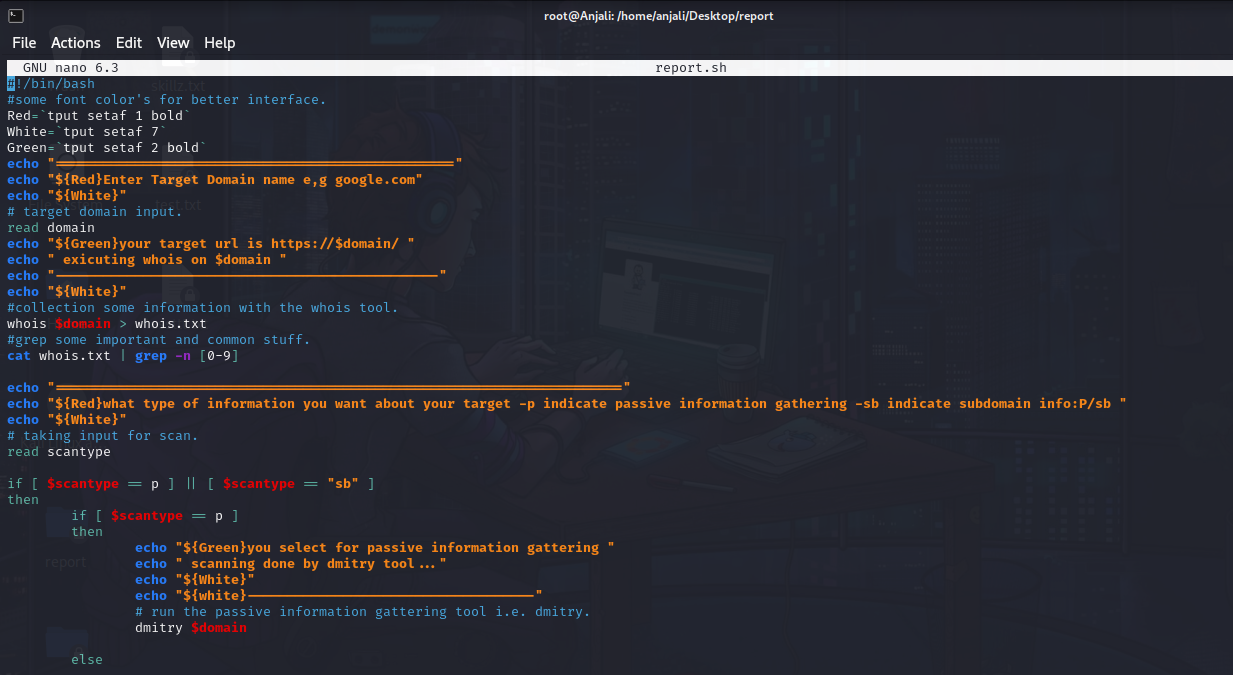
cat subdomanoutput.txt

fi

else

echo "plz enter p or sb"

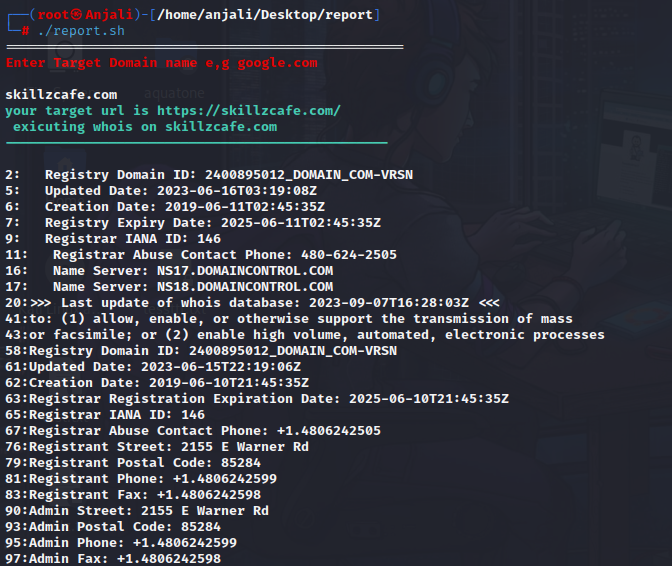
fi

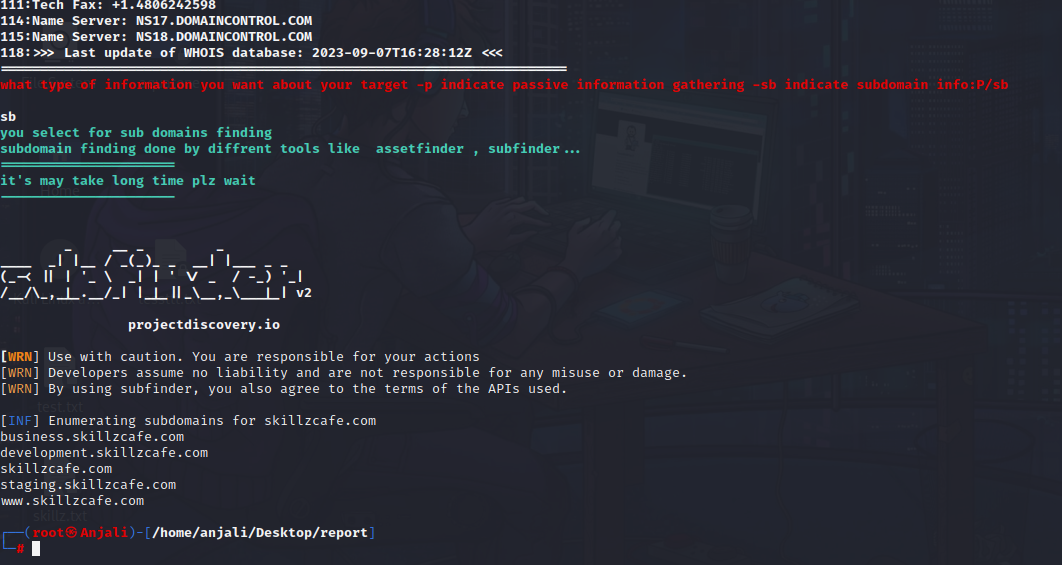




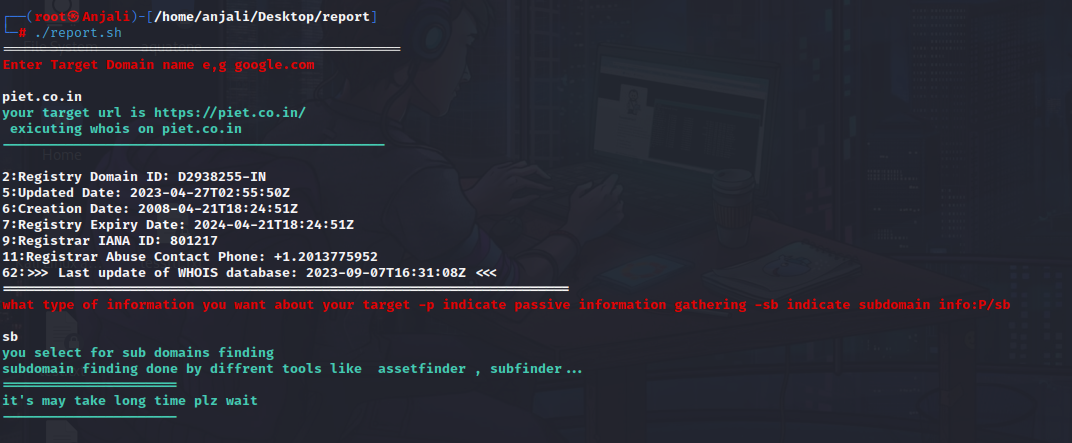
* **OUTPUT**

**🡺Testing on slillzcafe.com**

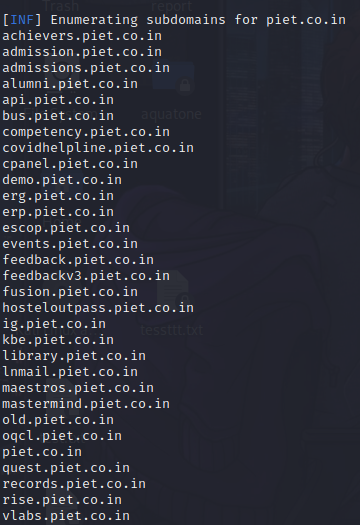




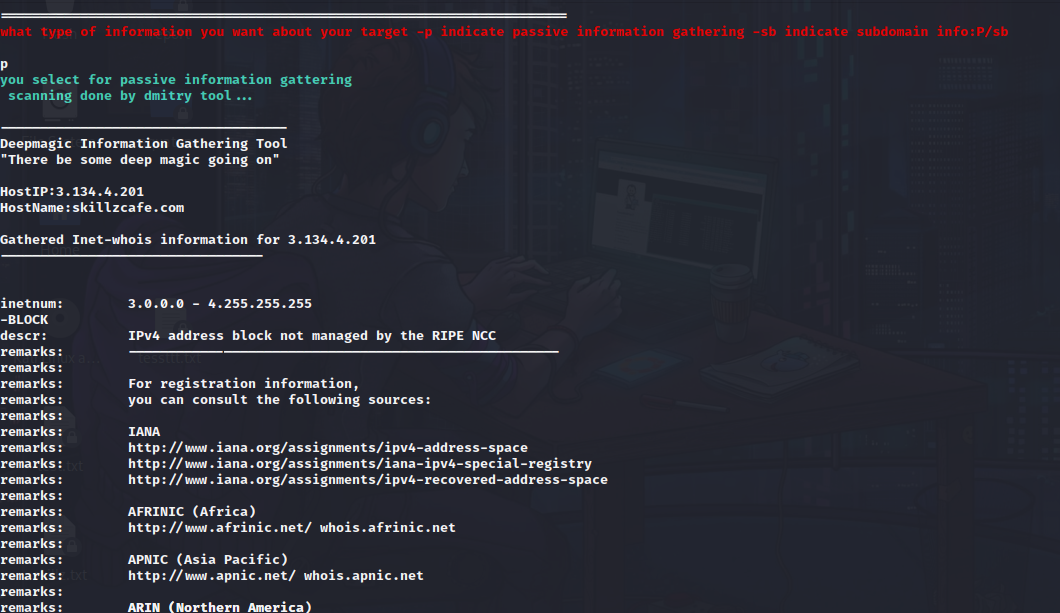
🡺**Testing on piet.co.in**



* Sub-domains



* Passive information



* **DFD**

