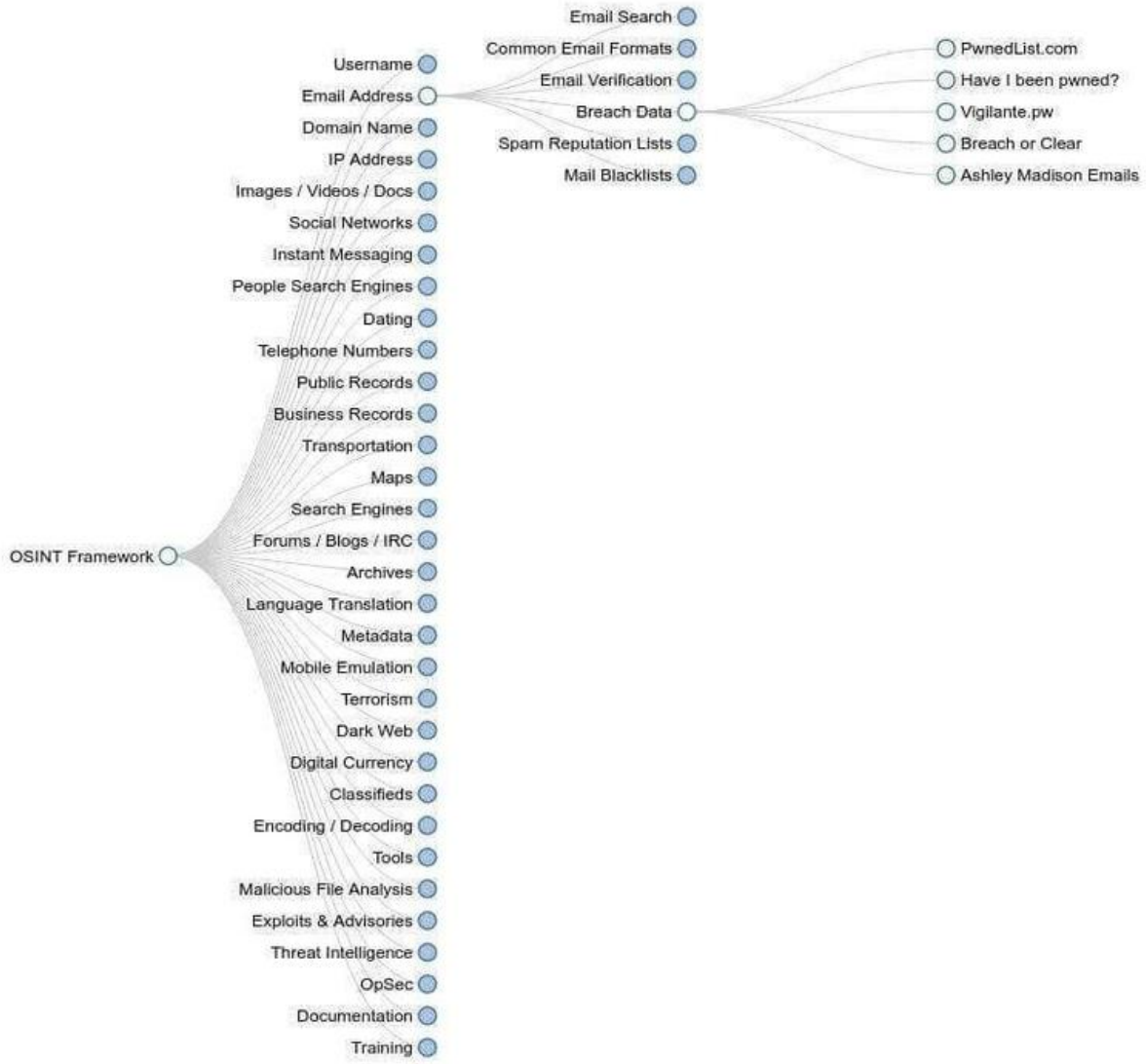
Task – 7

Name : C DEVAKI NANDAN REDDY

Select a website do footprinting and reconnaissance like collect information about website us e like Nslookup Osint framework



What Is footprinting

Footprinting is one of the most convenient ways for hackers to collect information about targets such as computer systems, devices, and networks. Using this method, hackers can unravel information on open ports of the target system, services running, and remote access probabilities.

Types of footprinting:

- Who is footprinting
- Network footprinting
- DNS footprinting
- Competitive intelligence
- Email footprinting
- Website footprinting
- Social Engineering
- Google Hacking

CheckUserNames

CheckUserNames is an online OSINT tool that can help you to find usernames across over 170 social networks. This is especially useful if you are running an investigation to determine the usage of the same username on different social networks.

It can be also used to check for brand company names, not only individuals.

3. HaveIbeenPwned

HaveIbeenPwned can help you to check if your account has been compromised in the past. This site was developed by Troy Hunt, one of the most respected IT security professionals of this market, and it's been serving accurate reports since years.

If you suspect your account has been compromised, or want to verify for 3rd party compromises on external accounts, this is the perfect tool. It can track down web compromise from many sources like Gmail, Hotmail, Yahoo accounts, as well as LastFM, Kickstarter, Wordpress.com, Linkedin and many other popular websites.

Once you introduce your email address, the results will be displayed, showing something like:

4. SecurityTrails API

The SecurityTrails API allows you instant access to current DNS and historical records, domain details, and associated domains, IP information, as well as WHOIS data so you can integrate it within your own applications for asset discovery, threat intelligence, risk scoring, and much more. The best part is that you only need an HTTP request to retrieve the data, such as:

```
curl --request GET \
--url https://api.securitytrails.com/v1/history/netflix.com/dns/a \
--header 'apikey: >'
```

5. Censys

Censys is a wonderful search engine used to get the latest and most accurate information about any device connected to the internet, it can be servers or domain names.

You will be able to find full geographic and technical details about 80 and 443 ports running on any server, as well as HTTP/S body content & GET response of the target website, Chrome TLS Handshake, full SSL Certificate Chain information, and WHOIS information.

6. Wappalyzer

Wappalyzer is a highly useful service that allows security researchers to quickly identify technologies on websites. With it, you can find a complete list of details

for any technology stack running on any website. It also allows you to build lists of websites that use certain technologies, letting you add phone numbers and email addresses as well.

Their free plan includes instant results and up to 50 free monthly lookups. It’s perfect for tracking website technologies, discovering old/vulnerable software, finding organic data about your competitors, and last but not least, can be quickly triggered from the web browser with their Chrome/Firefox extensions.

If that isn’t enough, they also offer a handy API to automate technology lookups, and you can even set up website alerts to monitor your competition.

7. Google Dorks

While investigating people or companies, a lot of IT security newbies forget the importance of using traditional search engines for recon and intel gathering.

In this case, Google Dorks can be your best friend. They have been there since 2002 and can help you a lot in your intel reconnaissance.

Google Dorks are simply ways to query Google against certain information that may be useful for your security investigation.

Search engines index a lot of information about almost anything on the internet, including individual, companies, and their data.

Some popular operators used to perform Google Dorking:

- Filetype: you can use this dork to find any kind of filetypes.
- Ext: can help you to find files with specific extensions (eg. .txt, .log, etc).
- Intext: can perform queries helps to search for specific text inside any page.
- Intitle: it will search for any specific words inside the page title.
- Inurl: will look out for mentioned words inside the URL of any website.

Log files aren't supposed to be indexed by search engines, however, they do, and you can get valuable information from these Google Dorks, as you see below:

Now let's focus on other more practical tools used by the most respected InfoSec professionals:

8. Maltego

Is an amazing tool to track down footprints of any target you need to match. This piece of software has been developed by Paterva, and it's part of the Kali Linux distribution.

Using Maltego will allow you to launch reconnaissance tests against specific targets.

One of the best things this software includes is what they call 'transforms'. Transforms are available for free in some cases, and on others, you will find commercial versions only. They will help you to run a different kind of tests and data integration with external applications.

In order to use Maltego you need to open a free account on their website, after that, you can launch a new machine or run transforms on the target from an existing one. Once you have chosen your transforms, Maltego app will start running all the transforms from Maltego servers.

Finally, Maltego will show you the results for the specified target, like IP, domains, AS numbers, and much more.

If you need to explore more Kali Linux utilities, check out this article: Top 25 Kali Linux Tools

---

9. Recon-Ng

Recon-ng comes already built in the Kali Linux distribution and is another great tool used to perform quickly and thoroughly reconnaissance on remote targets.

This web reconnaissance framework was written in Python and includes many modules, convenience functions and interactive help to guide you on how to use it properly.

The simple command-based interface allows you to run common operations like interacting with a database, run web requests, manage API keys or standardizing output content.

Fetching information about any target is pretty easy and can be done within seconds after installing. It includes interesting modules like google_site_web and

bing_domain_web that can be used to find valuable information about the target domains.

While some recon-ng modules are pretty passive as they never hit the target network, others can launch interesting stuff right against the remote host.