

## TASK-3

# INFORMATION GATHERING



## OVER VIEW

1. TYPES OF INFORMATION GATHERING

2. CATEGORIES OF INFORMATION GATHERING

3. METHODOLOGIES OF INFORMATION GATHERING

# INFORMATION GATHERING:

### Information Gathering means gathering different kinds of information about the target. It is basically, the first step or the beginning stage of Ethical Hacking, where the penetration testers or hackers (both black hat or white hat) tries to gather all the information about the target, in order to use it for Hacking.

## #TYPES OF INFORMATION GATHERING:

INFORMATION GATHERING IS OF MAINLY DIVIDED INTO 2 TYPES THEY ARE

- 1.ACTIVE INFORMATION GATHERING
- 2.PASSIVE INFORMATION GATHERING

## ACTIVE INFORMATION GATHERING:

\*This refers to the collecting of information by interacting with the target physically.

\*It is illegal to do this without authentication

Ex: OS fingerprinting, social engineering etc

\*It involves between the pen tester and actual target



# PASSIVE INFORMATION GATHERING:

\*This refers to the collecting of information by not interacting with the target physically.

\*It can involve the internet resources to find out target.

Ex: sniffing

## #CATEGORIES OF INFORMATION GATHERING:

The information gathering can be categorized into three ways

- 1.information gathering on organisations.
- 2.information gathering on systems
- 3.information gathering on networks

## #METHODOLOGIES OF INFORMATION GATHERING:

### **INFORMATION GATHERING USING SOCIAL MEDIA:**

Social media data is any type of data that can be gathered through social media only.

- 1.It makes to understand the identification of target.
- 2.By using this, we can know some of personals like
  - a. name
  - b. date of birth
  - c. phone number
  - d. address.

**3.**Based on all these we can attack the target.

Social media data is any type of data that can be gathered through social media. In general, the term refers to social media metrics and demographics collected through analytics tools on social platforms. Social media data can also refer to data collected from content people post publicly on social media.





## **INFORMATION GATHERING USING GROUPS OR NETWORKS OR BLOGS:**

By using groups, channels and so on we can collect the information and attack the target

### **1.WHATSAPP GROUPS**

- Remote Projects TechxPert:
- PMP CISCO AWS CERTIFICATI:
- WELCOME TO Cyber Security:
- Development.Environment:
- CyberThreat.in Updates:
- Hub of IT Certifications:
- Aws solution architect:
- Security:
- Excel Trngs & Trainers 2:
- Cyber Security Online:
- Microsoft Azure and AWS:
- Azure & AWS Training:
- GETHELPWORLDWIDE:

### **2.TWITTER ACCOUNTS**

"<https://www.appknox.com/blog/top-cybersecurity-influencers>"

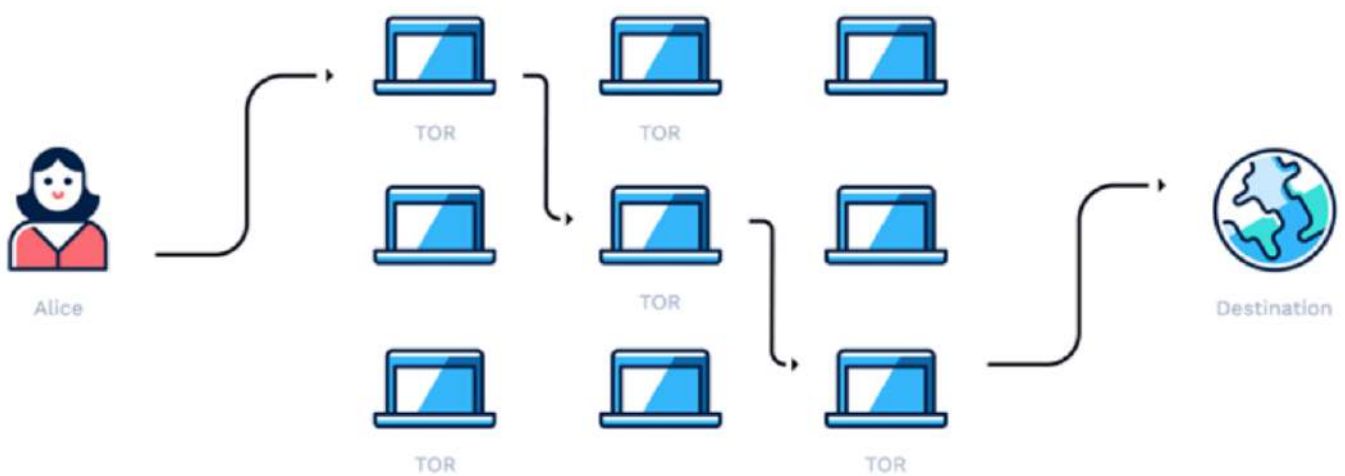
### **3.INSTAGRAM ACCOUNTS**

"<https://www.balbix.com/insights/top-cybersecurity-influencers/>"

## INFORMATION GATHERING USING SEARCH ENGINES:

Search engines are nothing but using the engines related to the internet

1. Some of them are Google, Yahoo, TOR etc.
2. By using the GITTUB PLATFORM, we can find out the code, comments, and so on.
3. The code contains the sensitive information.
4. By using GOOGLE DORKS, we can find some private information.
5. TOR is the best example for google dorks
6. Unauthorized persons cannot access tor without security pin.
7. By using brave browser we can use tor
8. This was discover to perform leagal activities.



## INFORMATION GATHERING USING WAPPALYZER:

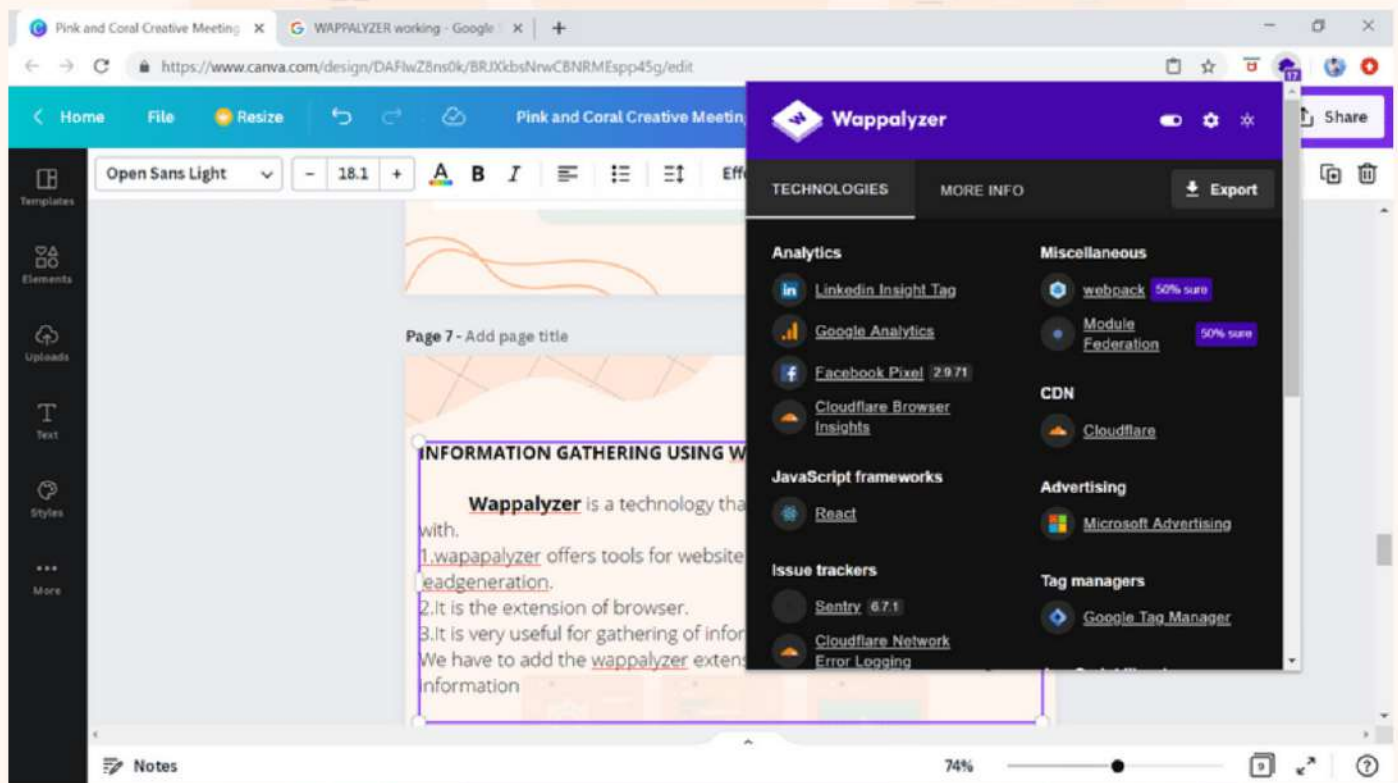
**Wappalyzer** is a technology that shows us what websites are built with.

1.wapapalyzer offers tools for website profiling ,market research and leadgeneration.

2.It is the extension of browser.

3.It is very useful for gathering of information related to the target.

We have to add the wappalyzer extension to the chrome and can gather information





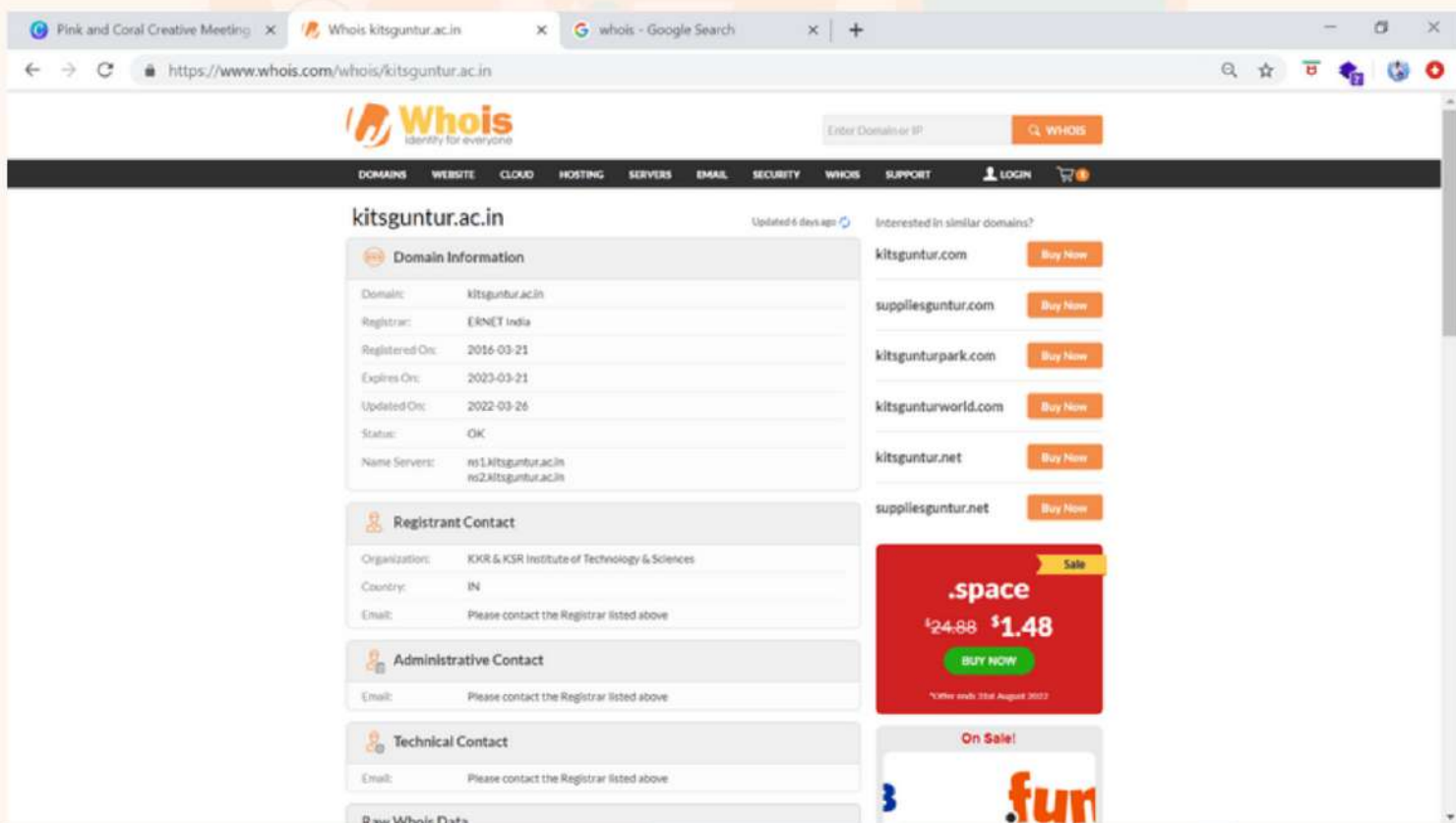
## INFORMATION GATHERING USING WHOIS:

A whois is a record contains all of the information associated with the persons, groups and company.

àwhois a kali linux command used to find the part of information in linux systems.

àwhois shows the ip addresses of domains.

àThrough them we can find the complete details including names, phone numbers, emails, of the registrant.



The screenshot displays the Whois website interface for the domain kitsguntur.ac.in. The page is titled "Whois" with the tagline "Identity for everyone". The domain information is as follows:

Domain Information	
Domain:	kitsguntur.ac.in
Registrar:	IKNET India
Registered On:	2016-03-21
Expires On:	2023-03-21
Updated On:	2022-03-26
Status:	OK
Name Servers:	ns1.kitsguntur.ac.in ns2.kitsguntur.ac.in

The Registrant Contact information is as follows:

Registrant Contact	
Organization:	KKR & KSR Institute of Technology & Sciences
Country:	IN
Email:	Please contact the Registrar listed above

The Administrative Contact information is as follows:

Administrative Contact	
Email:	Please contact the Registrar listed above

The Technical Contact information is as follows:

Technical Contact	
Email:	Please contact the Registrar listed above

Raw Whois Data

Interested in similar domains?

Domain	Buy Now
kitsguntur.com	Buy Now
suppliesguntur.com	Buy Now
kitsgunturpark.com	Buy Now
kitsgunturworld.com	Buy Now
kitsguntur.net	Buy Now
suppliesguntur.net	Buy Now

**.space** Sale  
\$24.88 **\$1.48**  
BUY NOW  
\*Offer ends 28th August 2023

**On Sale!**  
**.fun**



## INFORMATION GATHERING USING METADATA ANALYZER:

Metadata extraction is the retrieval of any embedded metadata that may be present in a given file.

By using this we can find the information which is in the form of audio, video, pictures etc

It gives the complete details of data regarding when ,  
Where, how.

The complete information of the file will be known.



## INFORMATION GATHERING USING SUB DOMAINS:

By using these sub domains ,we can find the details of that particular domain.

1.to get the details of a domain we use “WWW” url to get the ip address and details.

2.By this the target information is collected.

By using virus total we can scan the pdf and get the information related to that domain

3.The personal information can be hided by the company if they are privatized.



## INFORMATION GATHERING USING GEO LOCATOR:

Ip geo locator is used to find the ip address of the target .

- 1.it contains many domains and we search for our required target
- 2.It will show if any bugs are available and we can perform attack there.
- 3.EDEX -UI is one of the geo locator .





# THE END

