**DAY-5**

Methods to gather the information from websites:

1. Manually opening the websites

2. Web crawling techniques

3. Grab the contact details from the target website

We can use **web data extractor pro**

4. Finding the technologies the website is built with known as technology lookup

We can use tools like **wappalyzer**

**5. Footprinting using emails**

We can use hunter.io web tool to search publicly available emails

**6. Footprinting using who is lookup**

To gather:

-Organisation registered the domain

-who registered the domain

-IP address

-Expire and creation dates

-contact details of registrar

-address details of registrar

We can use **whois.domaintools.com**

**7. Footprinting using DNS**

-DNS maintains records like:

IPv4 (A record)

IPv6 (AAAA)

Name Server addresses (NS)

Mail Server addresses (MX)

Domain owner email id (SOA start of authority)

Hostname/redirection to ip address (PTR)

Some description (TXT records)

Canonical name (CNAME)