1. **Web Vulnerabilities**

1. SQL injection (Union, Error, Blind Time, Blind Boolean, Double Query)
2. Bypass WAF
3. Broken Authentication & Session Hijacking
4. IDOR
5. File Upload Vulnerability - RFI/LFI
6. XSS (Persistent, Non-persistent, DOM)
7. CSRF

2. **Tools**

1. Nmap
2. Wireshark
3. Metasploit
4. John the Ripper
5. Burp Suite
6. Nessus
7. Netsparker
8. Findomain
9. Httpx
10. Aircrack
11. Bettercap
12. Wfuzz
13. Sqlmap
14. Dirb
15. Wafw00f
16. Wappalyzer
17. Dnsenum
18. Nikto

3. **Black Box Testing**

A type of Penetration testing where the pentester does not have any knowledge regarding the website (Target), He must start his testing procedure from scratch. Hence This consumes more time when compared to other testing techniques.

The Ultimate goal is to simulate an external hacking.

Eg:

1. *Say there's a website (www.example.com).*
2. *With the help of OSINT and google dorks try to find any relevant data about the website.*
3. *Scan the ip with nmap scanner and search for any open ports.*

4. *If found, Exploit the open ports using the required payloads and methods.*
5. *Else keep on exploiting it based on the Owasp top 10 vulnerabilities.*
   (Try to Follow the phases of hacking)

4. Tools to find information about person / email id / phone number

1. **“Google Dorks”** is the best method to search and find information about a particular person - (username) / email id / phone number.
2. Personally, “**hunter.io”** is one of the best websites to search information about certain organizations' email id.
3. **“Phoneinfoga”** is another tool which is very helpful to find information about phone numbers.
4. **“Profil3r”** is another such tool, used to find information about people's profiles on social networks and also their email addresses.

There are many such OSINT Tools which could be very helpful to gather as much information about the target (Reconnaissance Phase).

5. Cyber Security

According to me, Cyber Security is a concept of protecting electronic systems from different types of cyber attacks.
Cyber Security - (Root domain)
Cloud Security, Network Security, Application Security - all come under cyber security - (subdomains under cyber security)
These days in the world, there are more devices than the users of those devices and attacking procedures are becoming smarter.