CTF Categories:
**Web Exploitation**
**Cryptography**
**Forensics - Steganography, Digital Forensics**
**Reverse Engineering**
**OSINT**
**Networking**
**Web exploitation**

**Forensic Tools:**

1. **File format identification (and "magic bytes")**
2. All of Eric Zimmermann Tools (Digital Forensics)
   **FTK Imager** - It allows us to create perfect copies (or images) of computer disks for analysis, preserving the integrity of the evidence. It also lets us view and analyze the contents of data storage devices without altering the data.
   **Autopsy** - Open-source digital forensics platform used for analyzing disk images, file systems, and various artifacts to uncover evidence in investigations.
   **Volatility** - Advanced memory forensics framework for analyzing volatile memory (RAM) dumps to extract information about running processes, network connections, and other system activities.
   **KAPE** - Command-line tool designed for automating the collection and parsing of digital forensic artifacts from Windows systems, aiding in rapid evidence collection and analysis.
   **Velociraptor** - Open-source endpoint visibility and digital forensics platform designed for monitoring and collecting detailed information from endpoints in enterprise environments, enabling threat hunting, incident response, and security monitoring at scale.
   **MFT Explorer**: A tool used in digital forensics to analyze the Master File Table (MFT) of a Windows NTFS file system, providing insights into file metadata, directory structure, and file system usage for investigative purposes.
   **Active Disk Editor** It is used for viewing & editing raw data (sectors) on Physical Disks including Volumes, Partitions & Files.
   **Amcache Parser** is a specialized tool used in digital forensics to analyze the Amcache.hve registry hive on Windows systems. It extracts information about program execution, including details such as executed binaries, timestamps, and file paths
   **Scalpel** is an open-source forensic tool used for file carving, which is the process of extracting files from disk images or other storage media without relying on file system metadata.
   **TimeLine Explorer**- Used to read CSV files generated from KAPE output.

**Registry Explorer** is a digital forensics tool used to navigate and analyze the Windows Registry, assisting in uncovering evidence of malicious activities and system configurations by examining registry entries and tracking changes over time.

3. Command Line utility - Command-line utility for parsing and analyzing **Windows Event Log files (EVTX)**, allowing forensic investigators and security analysts to extract valuable information such as system events, user activities, and security-related events for incident response and threat hunting purposes.
   **RegRipper** - Command line tool to analyze registry hives
   **PECmd (Program Execution)** is a command-line tool commonly utilized in digital forensics and incident response to analyze program execution artifacts on Windows systems. It aids investigators in extracting valuable information regarding executed programs, their associated metadata, timestamps, and execution paths.
   **DeepBlueCLI** It enables cybersecurity professionals to efficiently manage security policies, monitor threat detection, orchestrate incident responses, and perform various security operations directly from the command line interface

4. **Binwalk**- Binwalk is a command-line tool used for analyzing, extracting, and identifying embedded files within binary data, commonly employed in digital forensics and reverse engineering tasks.
5. **Sleuthkit** - The SleuthKit is a collection of command-line tools used for analyzing disk images and performing forensic investigations on digital media.
6. Jsteg - https://wiki.bi0s.in/steganography/jsteg/
7. Foremost - Extract particular kind of files using headers
8. Audacity - Analyze sound files (mp3, m4a, whatever)

**Cryptography:**

1) Cipher Identifier - to identify the cipher
2) Code chef - see “Magic” option
3) ROT Cipher/ Caesar Cipher
4) https://crackstation.net/ - Hash decrypter
5) John the ripper- John the Ripper is utilized as a tool to find the passwd for dictionary attacks, brute force attacks
   https://www.freecodecamp.org/news/crack-passwords-using-john-the-ripper-pentesting-tutorial/
6) Hash cat - to find the password
7) Hash Identifier - to find what type of hash
8) Xor tool - A tool to analyze multi-byte xor cipher
9) RSA tools - To solve RSA cipher
10) RSActf tool
    {https://stackoverflow.com/questions/49878381/rsa-decryption-using-only-n-e-and-c}
11) https://github.com/X-Vector/X-RSA

**Web exploitation:**

**https://github.com/riramar/Web-Attack-Cheat-Sheet**

BurpSuite – A graphical tool for testing website security.
Commix – Automated All-in-One OS Command Injection and Exploitation Tool.
Hackbar – Firefox addon for easy web exploitation
OWASP ZAP – Intercepting proxy to replay, debug, and fuzz HTTP requests and responses
Postman – Add on for chrome for debugging network requests
SQLMap – Automatic SQL injection and database takeover tool
W3af – Web Application Attack and Audit Framework.
XSSer – Automated XSS tester

**OSINT:**

**https://epieos.com/ - Helps in searching a persons details based on email id or phone number**
**https://intelx.io/ - Used for searching a domain, URL, email, Bitcoin address**
**https://whatsmyname.app/ -Used for searching and gathering social links of a person**
**https://haveibeenpwned.com/ - Used for checking if an email ID has been breached**
**https://urlscan.io/ - Used for knowing details about a URL**
**https://osintframework.com/ - Used for knowing about the OSINT approach of a target**
**https://www.whois.com/ - Used for knowing about IP address, domain name**
**https://builtwith.com/ - Used for knowing about the tech stack used for a website**
**http://web.archive.org/ - Used for checking if any archives of a URL is present**
**https://www.exploit-db.com/ - Used for knowing about the vulnerabilities along with the CVE ID**
**https://www.wappalyzer.com/ - Used for finding technology of a website**
**https://www.crunchbase.com/ - Used for finding details about an organization and its employees**
**https://viewdns.info/reversewhois/ - Used for finding DNS Info about a domain**
**https://justgetmydata.com/ - Used for finding maximum possible details about in different websites**
**https://cybdetective.com/osintmap/ - An OSINT Global Map for finding Governmental Details**
**https://namechk.com/ - For checking a Name in over 30 domains and 90 social media accounts**

**https://checkusernames.com/ - Used for checking a username or brand over 160 social media accounts**

**https://www.thelawpages.com/court-cases/court-case-search.php?mode=1 - Law Records of the UK Government**

**https://blackbird-osint.herokuapp.com/ - Used for finding out social media accounts with username**

**https://www.meertens.knaw.nl/nvb/naam/is/Giancarlo -Dutch Name Database**

**https://scb.se/hitta-statistik/sverige-i-siffror/namnsok/ - Sweden Name Database**

**https://emailrep.io/ - Website for checking reputation of a email address**

**https://sur.ly/o/numberway.com/AA000014 - Reverse Phone Number Lookup**

**http://www.192.com/ - Used for searching people, business and places in the UK**

**https://personlookup.co.za/ - South Africa People & Phone Number Database**

**http://fastpeoplesearch.com/ - Database of people in USA**

**Reverse Engineering:**

**Ghidra** - Ghidra is a free and open source reverse engineering tool

**Androguard** - It is a full python tool to play with android files

**Apktool** - It is another reverse engineering tool to decompile Android APKs.

**BinUtils** - The GNU Binary Utilities, or Binutils, are a set of programming tools for creating and managing binary programs, object files, libraries, profile data, and assembly source code.

**GDB** - GDB, the GNU Project debugger, allows you to see what is going on 'inside' another program while it executes

IDA Pro - IDA is a Windows, Linux or Mac OS X hosted multi-processor disassembler and debugger that offers so many features.

**Detox** - Detox is the most popular JS malware analysis tool which works on most Linux distributions. The development is currently done on Linux with the latest chrome browser.

**Networking :**

**Wireshark** is a popular open-source network protocol analyzer

Nmap Nmap is a network scanning tool

Shodan Shodan is a search engine designed to map and gather information about internet-connected devices and systems.

Zmap ZMap is a free, open-source network scanner that can be used for information security research.

DNS lookup to look up about domain names and their history

Who is to find about history of some Ip address or domain name