🛠 TOOLS & METHODS USED IN CYBERCRIME

*Quick Exam Notes - Cybercrime Unit (**3**)*
*Brought to you by **ZenYukti***

1. Introduction

- Cybercriminals use a wide range of tools and techniques to attack systems, steal data, and cause disruption
- Tools range from simple scripts to sophisticated automated attack frameworks
- Understanding these tools is key to building effective defences

Category	Examples
Network Attacks	DoS, DDoS, MitM, Rogue AP
Malware	Virus, Worm, Trojan, Spyware, Keylogger, Ransomware
Credential Attacks	Phishing, Password Cracking, Keylogging
Anonymity Tools	Proxy Servers, Anonymizers, Tor, VPN (abused)
Web Attacks	SQL Injection, Buffer Overflow, XSS
Concealment Tools	Steganography, Backdoors, Rootkits

2. Proxy Servers and Anonymizers

- **Proxy Server:** Intermediate server between user and the internet — forwards requests on behalf of user
  - Hides real IP address of the attacker
  - Can bypass geo-restrictions and content filters
  - Attackers chain multiple proxies to make tracing nearly impossible
- **Anonymizer:** Tool/service that strips identifying info from internet traffic — hides identity online
  - Examples: Tor (The Onion Router), VPN, Anonymous proxies, I2P

- **Tor Network:** Routes traffic through multiple volunteer nodes (onion routing), encrypting at each layer
  - Exit node sends the final request — cannot be traced back to origin
  - Used legitimately for privacy; abused by cybercriminals on dark web
- **Proxy Chaining:** Using multiple proxies in sequence — each only knows adjacent proxy, not origin

Tool	How It Works	Attacker Use
Web Proxy	Browser routes through proxy server	Hide IP, bypass filters
SOCKS Proxy	Lower-level proxy — works for any traffic	Hide C&C communication
Tor	Multi-hop onion routing with encryption	Dark web access, anonymity
VPN (abused)	Encrypted tunnel to VPN server	Mask location, bypass blocks
I2P	Invisible Internet Project — private network layer	Anonymous communication

◐ *Defence: Log all outbound traffic, detect Tor/proxy usage via Deep Packet Inspection (DPI)*

3. Phishing

- **Phishing:** Fraudulent attempt to steal sensitive info (credentials, card details) by disguising as a trusted entity
- Primarily via email, but also SMS (Smishing), voice (Vishing), and social media

Type	Description
Standard Phishing	Mass fake emails pretending to be bank/service — targets everyone
Spear Phishing	Targeted phishing — customized for a specific person using their personal info

Whaling	Spear phishing targeting executives (CEO, CFO, CTO)
Clone Phishing	Copy of a legitimate email with malicious link replacing the original
Smishing	Phishing via SMS — fake OTP requests, delivery notifications
Vishing	Voice call phishing — fake bank/IT support calls
Pharming	Redirect users from real website to fake one (via DNS poisoning)
Evil Twin	Fake Wi-Fi hotspot mimicking a legitimate network

How a Phishing Attack Works

- Attacker creates fake website/email mimicking a trusted brand
- Sends mass emails with urgent message ('Your account will be suspended!')
- Victim clicks link → lands on fake login page
- Victim enters credentials → attacker captures them
- Attacker uses stolen credentials for account takeover / financial fraud

Indicators of Phishing

- Sender email domain is slightly misspelled (paypa1.com, amaz0n.com)
- Urgency/fear tactics ('Act now or lose access')
- Generic greeting ('Dear Customer' instead of your name)
- Suspicious attachments or links (hover to see actual URL)
- Poor grammar and spelling

◐ *Defence: Check sender domain carefully, use email filters, enable 2FA, verify via official website*

4. Password Cracking

- **Password Cracking:** Process of recovering passwords from stored/transmitted data using various techniques
- Attackers target password hashes stored in databases after a breach

Technique	How It Works	Defence
Brute Force	Try every possible combination systematically	Long complex passwords; account lockout
Dictionary Attack	Try words from a wordlist/dictionary	Avoid real words; use passphrases
Rainbow Table	Pre-computed hash-to-password lookup table	Salt hashes (add random data before hashing)
Hybrid Attack	Dictionary + brute force (e.g., password1, P@ssword)	Avoid predictable substitutions
Credential Stuffing	Use leaked username/password pairs from other breaches	Use unique passwords per site
Shoulder Surfing	Physically observe someone typing password	Privacy screen, be aware of surroundings
Password Spraying	Try a few common passwords against many accounts	Block accounts after few failed attempts

- **Common Tools:** John the Ripper, Hashcat, Hydra, Aircrack-ng (for Wi-Fi), Ophcrack
- **Salting:** Adding random data to password before hashing — defeats rainbow tables

◐ *Defence: Long passwords (12+ chars), MFA, hashed+salted storage, account lockout policies*

5. Keyloggers and Spyware

Keyloggers

- **Keylogger:** Records every keystroke typed on a device — captures passwords, messages, card numbers

Type	Description
Software Keylogger	Installed as program/malware — runs in background, logs keys to file
Hardware Keylogger	Physical device plugged between keyboard and PC — stores keystrokes internally
Kernel-based	Operates at OS kernel level — very hard to detect
Form Grabber	Intercepts data submitted in web forms before it's encrypted
Acoustic Keylogger	Records sound of keystrokes — analyzes to determine keys pressed

Spyware

- **Spyware:** Malware that secretly monitors and collects user data without consent
- Collects: browsing history, login credentials, banking info, location, screen captures, contacts
- Often bundled with free software (freeware, shareware)
- **Adware:** Displays unwanted ads; lighter form of spyware
- **Stalkerware:** Spyware used for personal surveillance (e.g., by abusive partners)
- **RAT (Remote Access Trojan):** Full remote control + spying capabilities

- **Common Spyware:** FinFisher, Pegasus (nation-state), Emotet, DarkComet
  Defence: Antivirus/anti-spyware, avoid free software from untrusted sources, regular scans, check running processes

6. Virus and Worms

Computer Virus

- **Virus:** Self-replicating malicious code that attaches to legitimate programs/files — needs human action to spread
- Requires host file; activates when infected file is executed

Virus Type	Description
File Infector	Attaches to executable files (.exe, .com)
Boot Sector Virus	Infects MBR — activates before OS loads
Macro Virus	Embeds in documents (Word, Excel macros) — spread via file sharing
Polymorphic Virus	Changes its code signature each time to evade AV detection
Metamorphic Virus	Completely rewrites itself each generation — hardest to detect
Multipartite Virus	Infects both boot sector and files simultaneously
Stealth Virus	Hides itself from antivirus by intercepting system calls

Computer Worm

- **Worm:** Self-replicating malware that spreads autonomously over networks — NO host file needed
- Spreads by exploiting network vulnerabilities, email, shared drives
- Main damage: network congestion, bandwidth consumption, payload delivery

Feature	Virus	Worm
Needs host file?	YES — attaches to file/program	NO — standalone program
Spreads via	Human action (running infected file)	Network, automatically
Speed of spread	Slower	Very fast (self-propagating)
Example	ILOVEYOU, Melissa	WannaCry, CodeRed, Slammer

Defence: Antivirus with real-time protection, email filters, patch vulnerabilities, disable macros

7. Trojan Horses and Backdoors

Trojan Horse

- **Trojan:** Malware disguised as legitimate software — user willingly installs it
- Does NOT self-replicate (unlike virus/worm)
- Named after Greek Trojan Horse — appears useful, hides malicious intent

Trojan Type	Purpose
Remote Access Trojan (RAT)	Give attacker full remote control of victim's system
Downloader Trojan	Download and install additional malware on infected system
Banker Trojan	Steal online banking credentials (e.g., Zeus, TrickBot)
DDoS Trojan	Use victim's machine to launch DDoS attacks
Ransomware Trojan	Encrypt files and demand ransom (e.g., CryptoLocker)
Rootkit Trojan	Hide malware presence deep in the OS
Backdoor Trojan	Open hidden access channel for future attacks

Backdoors

- **Backdoor:** Hidden entry point into a system that bypasses normal authentication
- Can be installed by Trojans, worms, or even legitimate software developers
  - Gives attacker persistent access even after password changes
  - Often installed after initial exploitation to maintain access
- **Rootkit:** Set of tools that hide malware/backdoor presence by modifying OS — very hard to detect
- **Examples:** Back Orifice, NetBus, SubSeven (old RATs), modern APT backdoors

  ◐ *Defence: Download only from official sources, scan downloads, use application whitelisting, monitor network connections*

8. Steganography

- **Steganography:** Art of hiding secret data INSIDE ordinary-looking files (images, audio, video, text) — data is hidden, not encrypted
- Different from cryptography: Crypto hides the CONTENT; Stego hides the EXISTENCE of the message

Type	How Data is Hidden
Image Steganography	Hidden in LSB (Least Significant Bits) of image pixels — image looks unchanged
Audio Steganography	Hidden in audio file noise floor or frequency ranges
Video Steganography	Hidden in video frames — vast capacity due to large file size
Text Steganography	Hidden via whitespace, word spacing, or invisible characters
Network Steganography	Hidden in network packet headers (unused fields)

- Cybercrime Uses:
  - Transmit malware commands hidden inside images (evades firewalls)
  - Exfiltrate stolen data hidden in innocent-looking files
  - Covert communication between criminals — chat hidden in images
  - Watermarking (legitimate) — proving ownership of digital content
- **Steganalysis:** Detecting steganography — statistical analysis of files for anomalies
- **Tools:** Steghide, OpenStego, SilentEye, DeepSound (audio)

  ◐ *Defence: Monitor unusual large outbound file transfers; use steganalysis tools at network borders*

9. DoS and DDoS Attacks

- **DoS (Denial of Service):** Overwhelm a system/service with traffic so it becomes unavailable to legitimate users — single source
- **DDoS (Distributed DoS):** Same goal but using thousands/millions of sources (botnet) — much harder to block

Types of DoS/DDoS Attacks

Attack Type	How It Works
Volume-based (Flood)	Flood target with massive traffic — saturate bandwidth (UDP flood, ICMP flood)
SYN Flood	Send thousands of TCP SYN packets without completing handshake — exhaust server connections
HTTP Flood	Thousands of bots send legitimate-looking HTTP GET/POST requests — exhaust web server
Ping of Death	Send malformed/oversized ICMP packets — crash older systems
Smurf Attack	Spoof victim's IP, send broadcast ICMP — all machines reply to victim
Slowloris	Keep many HTTP connections open with partial requests — starve server connections
DNS Amplification	Small query → large DNS response → reflected to victim (amplification)
Application Layer (Layer 7)	Target specific app functions (login page, search) — resource exhaustion

- **Botnet Role:** Attacker commands botnet (thousands of zombies) to simultaneously attack — traffic from many IPs makes blocking hard
- **Amplification Factor:** DNS amplification can amplify attack traffic 70x — small input, massive output

Mitigation

- Rate limiting — limit requests per IP per second
- CDN / Traffic scrubbing services (Cloudflare, Akamai)
- Blackhole routing — null-route attack traffic
- Firewall rules — block known attack patterns
- CAPTCHA for application layer attacks

DDoS protection must be at network level — cannot be stopped by the victim server alone

10. SQL Injection (SQLi)

- **SQL Injection:** Inserting malicious SQL code into input fields to manipulate the backend database
- One of the most common and dangerous web application vulnerabilities — OWASP Top 10
- Exploits poor input validation in web applications

How It Works

- Application takes user input and embeds it directly in SQL query
- Attacker enters SQL code as input instead of normal data
- Database executes the injected code — unintended results

- **Classic Example:** Login form with query: SELECT * FROM users WHERE user='{input}' AND pass='{input}'
  - Attacker enters username: admin'-- (comment out password check)
  - Query becomes: SELECT * FROM users WHERE user='admin'--' AND pass='anything'
  - Result: Logged in as admin without knowing password

SQLi Type	Description
In-band SQLi	Result returned directly in same channel (classic, most common)
Error-based	Force DB errors that reveal database structure info

Union-based	Use UNION to combine results from other tables
Blind SQLi	No visible output — infer data from true/false responses or timing
Time-based Blind	Use SQL SLEEP() — if response delayed, condition is true
Out-of-band SQLi	Data exfiltrated via different channel (DNS, HTTP request)
Stored SQLi	Malicious SQL stored in DB (e.g., in profile) — executes when viewed

Impact

- Bypass authentication, extract entire database, modify/delete data
- Execute OS commands (in some DBs), read/write files

- **Tools:** sqlmap (automated SQLi tool), Havij, Burp Suite

Defence: Prepared statements / parameterized queries, input validation, WAF, least privilege DB accounts

11. Buffer Overflow

- **Buffer:** Temporary storage area in memory to hold data
- **Buffer Overflow:** Writing more data into a buffer than it can hold — excess data overwrites adjacent memory
- Can overwrite return addresses → redirect execution to attacker's malicious code
- Primarily affects programs written in C/C++ (no automatic bounds checking)

How It Works

- Program allocates fixed-size buffer (e.g., 100 bytes for username)
- Attacker sends 200 bytes — extra 100 bytes overflow into adjacent memory
- Overwrites return address on stack with address of malicious code
- When function returns → executes attacker's shellcode instead

Type	Description
Stack Overflow	Overflows stack buffer — overwrites return address (most common)
Heap Overflow	Overflows heap-allocated buffer — corrupts heap metadata
Integer Overflow	Arithmetic overflow causes wrong buffer size calculation
Format String	Exploit format string functions (%s, %n) to read/write memory

- **Shellcode:** Attacker-supplied machine code injected via overflow — typically opens a shell/command prompt
- **NOP Sled:** Series of NOP (no-operation) instructions before shellcode — increases hit probability

Defences

- ASLR (Address Space Layout Randomization) — randomize memory addresses
- Stack Canaries — place sentinel value before return address; check before return
- DEP/NX (Data Execution Prevention / No-Execute) — mark memory regions as non-executable
- Safe languages (Java, Python) — automatic bounds checking
- Code auditing and static analysis tools

Defence: Use modern compilers with stack protection flags (-fstack-protector), enable ASLR/DEP at OS level

12. Attacks on Wireless Networks

Attack	Description
Eavesdropping / Sniffing	Capture unencrypted Wi-Fi packets using tools like Wireshark, Aircrack-ng
Rogue Access Point	Set up fake Wi-Fi hotspot — users connect, attacker intercepts all traffic
Evil Twin	Fake AP with same SSID as legitimate network — users auto-connect

WEP Cracking	WEP encryption is weak — cracked in minutes using statistical attacks
WPA/WPA2 Cracking	Capture 4-way handshake → offline dictionary/brute force attack
KRACK Attack	Key Reinstallation Attack — vulnerability in WPA2 handshake process
Deauth Attack	Send fake deauthentication frames — disconnect users (DoS)
Wardriving	Driving around scanning for vulnerable/open Wi-Fi networks
WPS Attack (Pixie Dust)	Exploit Wi-Fi Protected Setup PIN vulnerability — recover WPA key
Bluetooth Attacks	Bluejacking, Bluesnarfing, Bluebugging via open Bluetooth
Man-in-the-Middle	Position between client and AP — intercept and manipulate traffic
Jamming	Transmit interference signals to disrupt wireless communication

Wireless Security Standards — Weakest to Strongest

Protocol	Security Level	Notes
WEP	✗ Broken	Never use — cracked in minutes
WPA	⚠ Weak	Deprecated — TKIP encryption has flaws
WPA2 (TKIP)	⚠ Moderate	TKIP weak — use AES instead
WPA2 (AES/CCMP)	☑ Good	Current standard — use this
WPA3	☑☑ Best	Strongest — SAE handshake, forward secrecy

◐ Defence: Use WPA3/WPA2-AES, strong passphrase, disable WPS, hide SSID, MAC filtering, use VPN on public Wi-Fi

13. Phishing and Identity Theft

Introduction to Phishing (Detailed)

- **Phishing:** Deceptive attempt to acquire sensitive information by masquerading as a trustworthy entity in digital communication
- Phishing lifecycle:
  - Plan → Set up fake infrastructure (domain, website, email)
  - Attack → Send phishing emails/messages to targets
  - Collect → Harvest submitted credentials/data
  - Monetize → Use stolen data for fraud or sell on dark web

Identity Theft (ID Theft)

- **Identity Theft:** Fraudulently obtaining and using someone's personal information (name, SSN, Aadhaar, card details) without their consent — for financial gain or other crimes

Type of ID Theft	Description
Financial ID Theft	Use stolen identity to open bank accounts, take loans, make purchases
Medical ID Theft	Use someone's identity to claim medical insurance or get prescriptions
Criminal ID Theft	Give victim's identity when arrested — criminal record appears on victim
Tax ID Theft	File fraudulent tax returns using victim's info to claim refunds
Child ID Theft	Use minor's clean SSN/Aadhaar — often undetected for years
Synthetic ID Theft	Combine real and fake info to create new fake identity

Account Takeover	Gain control of existing bank/email/social media account

How Identity is Stolen

- Phishing emails / fake websites
- Data breaches — stolen from company databases
- Social engineering — tricks victim into revealing info
- Physical theft — stolen wallet, mail, documents
- Dumpster diving — search trash for bills, bank statements
- Shoulder surfing — observe entering PIN or credentials
- Malware/spyware on device
- Dark web purchase — data from previous breaches

Signs You Are a Victim of ID Theft

- Unexplained charges on bank/credit card statements
- Loan rejection despite good credit history
- Unknown accounts appearing on credit report
- Bills for services you didn't use
- IRS/tax notices for returns you didn't file

Prevention of Identity Theft

- Shred documents with personal info before disposal
- Monitor bank statements and credit reports regularly
- Use strong unique passwords + MFA on all accounts
- Freeze credit when not applying for loans
- Never share Aadhaar/PAN/SSN unless absolutely necessary
- Be cautious on social media — don't overshare personal details

- **India:** Report to Cyber Crime Portal (cybercrime.gov.in), file FIR, alert bank immediately

⚠ *Identity theft can take years to fully recover from — prevention is far easier than recovery*

14. QUICK RECAP — ALL KEY TERMS

Tool / Attack	One-Line Definition
Proxy Server	Intermediate server hiding user's real IP address
Tor	Multi-hop onion routing for anonymity — used on dark web
Anonymizer	Strips identifying info from internet traffic
Phishing	Fake emails/sites to steal credentials — mass targeted
Spear Phishing	Targeted phishing using victim's personal info
Whaling	Phishing aimed at C-level executives
Pharming	Redirect to fake site via DNS poisoning
Brute Force	Try all password combinations until correct one found
Rainbow Table	Pre-computed hash lookup — defeated by salting
Credential Stuffing	Use leaked username/password pairs from other breaches
Keylogger	Records every keystroke — hardware or software
Spyware	Secretly collects user data without consent
Virus	Self-replicating, needs host file, spreads via human action
Worm	Self-replicating, no host needed, spreads automatically via network
Trojan	Disguised as legitimate software — hides malicious payload

Backdoor	Hidden access channel bypassing normal authentication
Rootkit	Hides malware presence by modifying OS
Steganography	Hides secret data inside ordinary files (images, audio)
DoS	Single-source attack flooding target to deny service
DDoS	Multi-source (botnet) flooding attack — much harder to stop
SYN Flood	Incomplete TCP handshakes exhaust server connection table
SQL Injection	Malicious SQL in input fields manipulates database
Buffer Overflow	Overflow memory buffer to overwrite return address → execute shellcode
ASLR	Randomize memory addresses — defend against buffer overflow
Stack Canary	Sentinel value detects stack overflow before execution
Wardriving	Scanning for vulnerable Wi-Fi networks from a moving vehicle
WEP	Broken Wi-Fi encryption — never use
WPA3	Strongest current Wi-Fi security standard
KRACK	Key Reinstallation Attack — WPA2 vulnerability
Deauth Attack	Send fake deauth frames to disconnect Wi-Fi users
Identity Theft	Steal and misuse someone's personal identity for fraud
Synthetic ID Theft	Combine real + fake info to create new fake identity

END OF NOTES