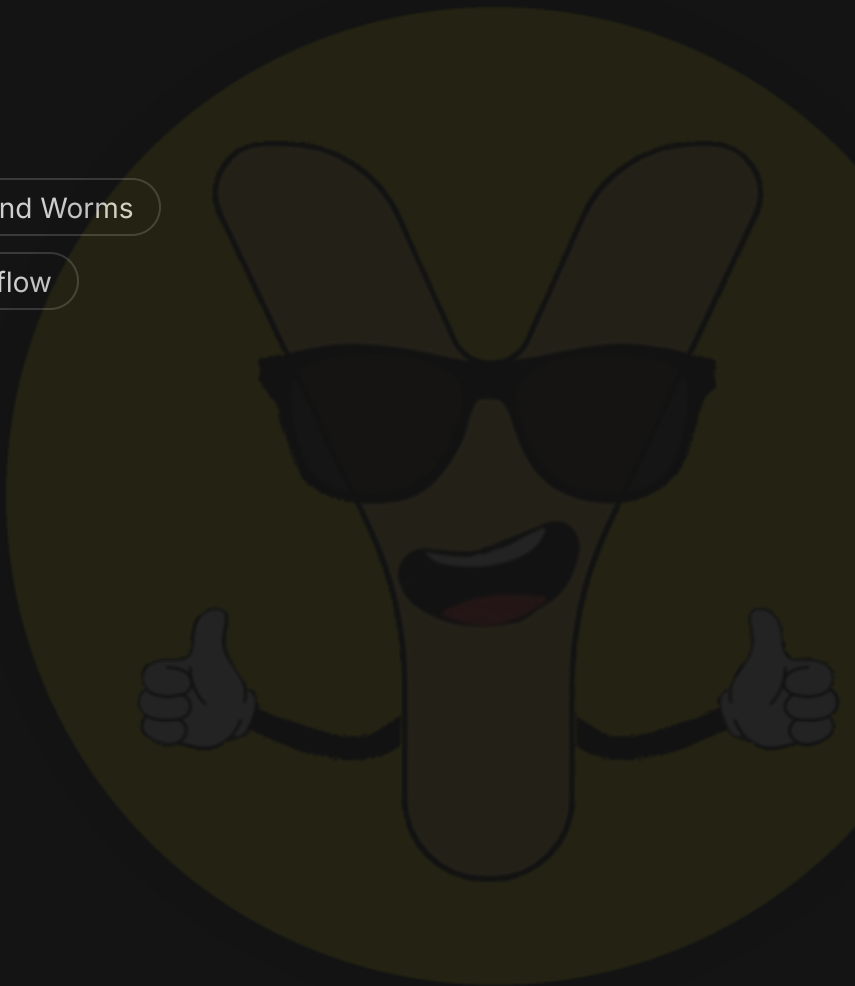
AKTU · 2ND YEAR · BCC301 / BCC401

Cyber Security

Unit 3 — Tools and Methods Used in Cybercrime

- Proxy Servers and Anonymizers
- Phishing
- Password Cracking
- Keyloggers and Spywares
- Virus and Worms
- Trojan Horses and Backdoors
- Steganography
- DoD and DDoS Attacks
- SQL Injection
- Buffer Overflow
- Attacks on Wireless Networks



DECODED BY

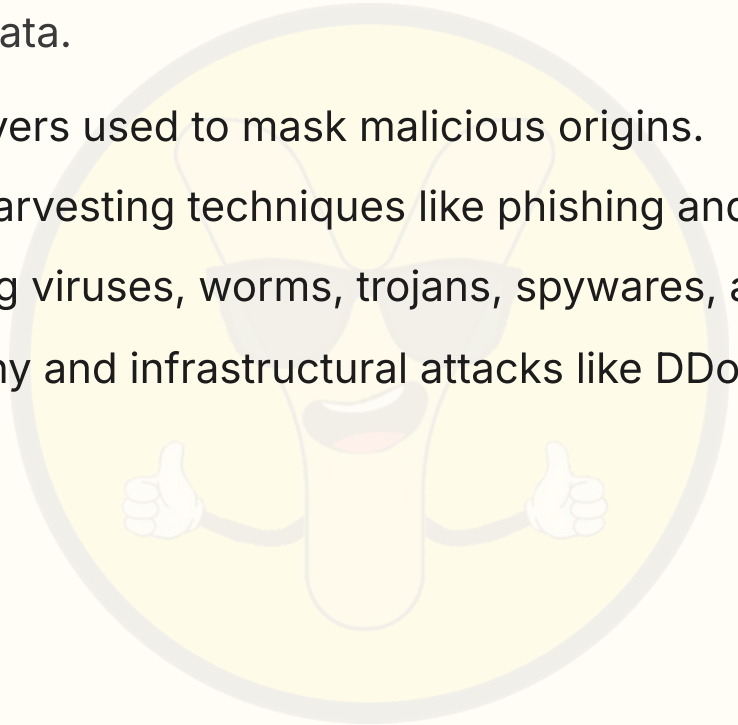
Chirag Jain

Founder, Ycotes · Gold Medalist in Artificial Intelligence, IIT Madras · taught 10,000+ students

Unit 3 Overview: Tools and Methods Used in Cybercrime

This unit covers the technical vectors, software tools, and methodologies utilized by attackers to compromise systems, networks, and data.

- Anonymity networks and proxy servers used to mask malicious origins.
- Social engineering and credential harvesting techniques like phishing and password cracking.
- Malicious software classes including viruses, worms, trojans, spywares, and keyloggers.
- Data concealment via steganography and infrastructural attacks like DDoS and SQL injection.



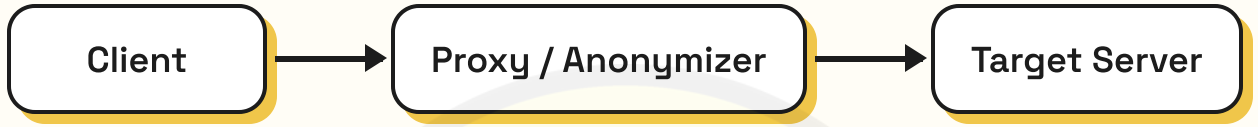
Proxy Servers and Anonymizers

PROXY SERVER

An intermediary server between a client application and a destination server, forwarding requests and hiding the true client IP address.

- Acts as a gateway, providing caching, filtering, and basic source IP masking.
- Anonymizers take this a step further by stripping headers and routing traffic through multi-hop circuits (e.g., Tor network).

Proxy and Anonymizer Routing Architecture



The client sends a request to the proxy, which strips identity markers and forwards it to the target server, hiding the original source.

Phishing

PHISHING ATTACK

A social engineering attack consisting of fraudulent communications disguised as reputable sources to steal sensitive user data.

- Commonly executed via deceptive emails containing malicious links or attachments.
- Spear phishing targets specific individuals or organizations; whaling targets high-profile executives.
- Goal is credential theft, financial fraud, or malware installation.

Password Cracking Methods

Techniques used by attackers to recover passwords from stored hashes or intercept authentication flows.

- Brute-Force Attack
  - Systematic trial of every possible combination of characters until the correct password is found.
  - Computationally intensive and time-consuming for long passwords.
- Dictionary Attack
  - Tests a precompiled list of common words, phrases, and previous breaches against target hashes.
  - Much faster than brute-force because human password habits are predictable.
- Rainbow Table Attack
  - Uses precomputed tables of all possible plaintext passwords and their corresponding cryptographic hashes.
  - Trades storage space for execution speed, bypassing runtime hashing.

Keyloggers and Spywares

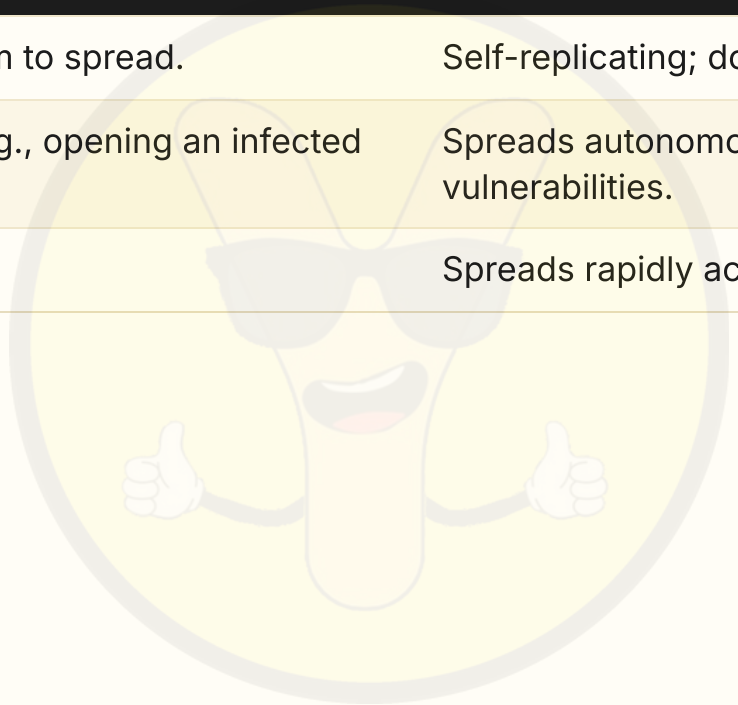
SPYWARE

Malicious software installed on a device without consent to gather user information, activity logs, and credentials.

- Keyloggers specifically record keystrokes made on a keyboard, capturing passwords, chats, and banking details.
- Can be implemented at the kernel level, API level, or via hardware physical implants.

Virus vs Worm

Feature	Virus	Worm
Propagation	Requires a host file or program to spread.	Self-replicating; does not need a host program.
User Action	Needs human intervention (e.g., opening an infected file).	Spreads autonomously across networks by exploiting vulnerabilities.
Speed	Spreads relatively slower.	Spreads rapidly across connected networks.

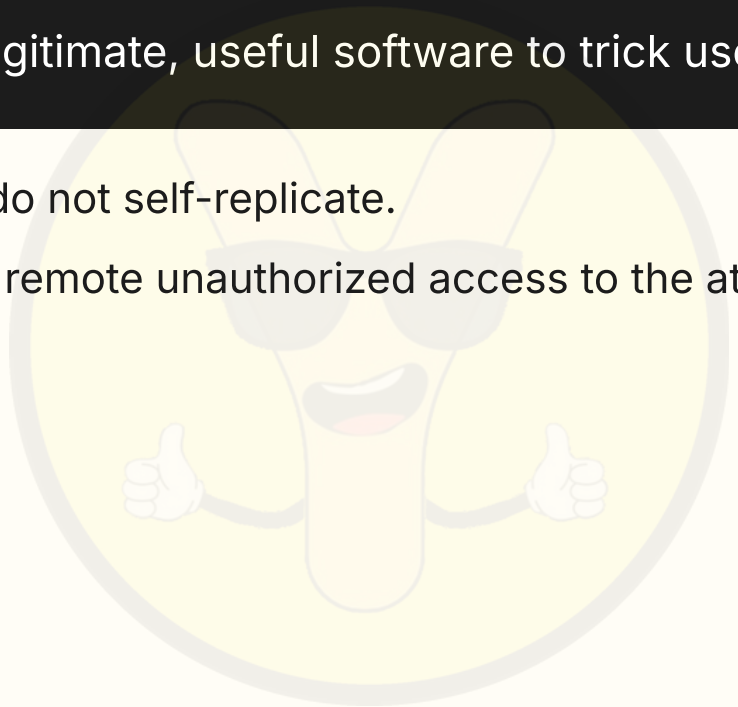


Trojan Horses and Backdoors

TROJAN HORSE

Malicious software disguised as legitimate, useful software to trick users into executing it.

- Unlike viruses and worms, Trojans do not self-replicate.
- Often installs a backdoor, providing remote unauthorized access to the attacker while bypassing standard authentication mechanisms.

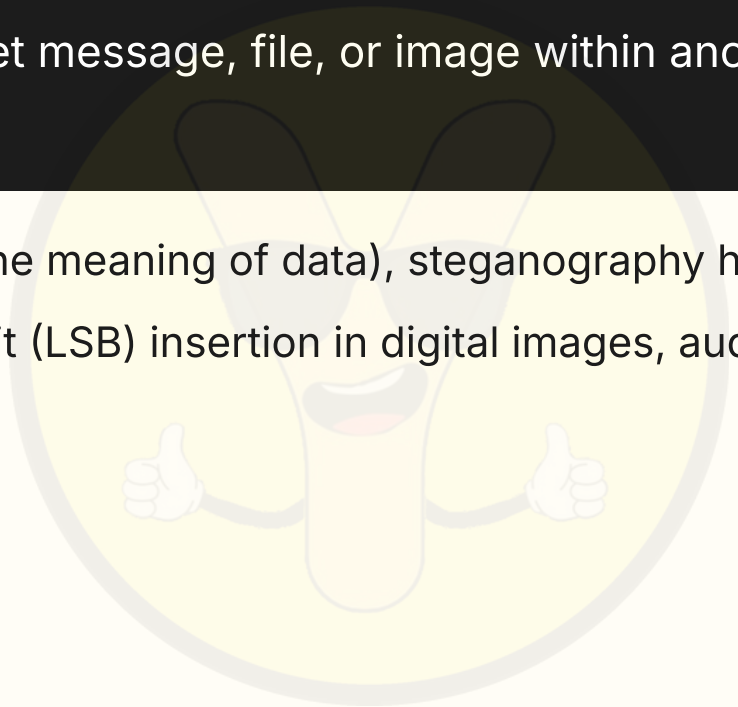


Steganography

STEGANOGRAPHY

The practice of concealing a secret message, file, or image within another ordinary, non-secret file or medium.

- Unlike cryptography (which hides the meaning of data), steganography hides the existence of data.
- Commonly uses Least Significant Bit (LSB) insertion in digital images, audio, or video files.



DoD and DDoS Attacks

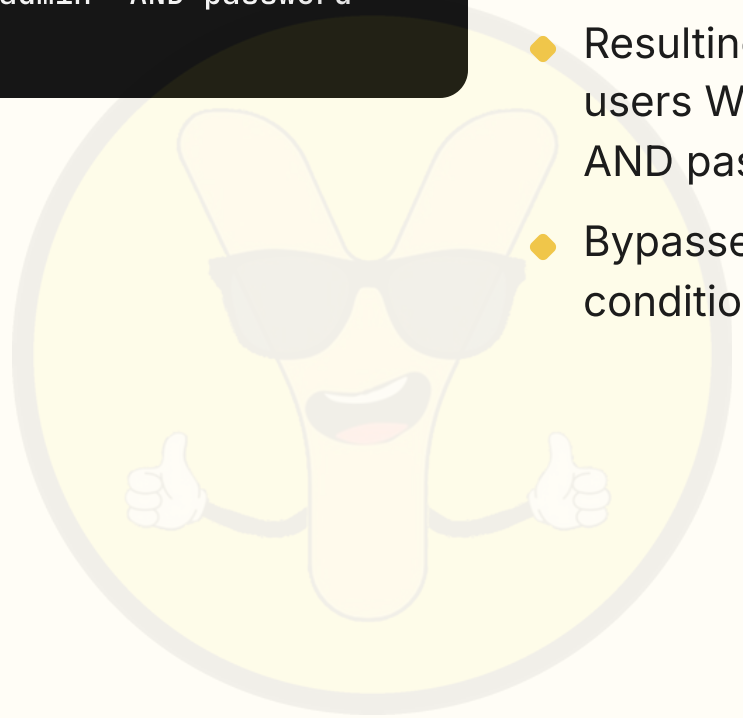
DISTRIBUTED DENIAL OF SERVICE (DDOS)

An attack where multiple compromised systems (a botnet) flood the bandwidth or resources of a targeted system, rendering it unavailable.

- DoS uses a single source; DDoS uses distributed sources, making mitigation difficult.
- Common types: Volumetric attacks, Protocol attacks, and Application layer attacks.

SQL Injection (SQLi) Vulnerability Example

```
SELECT * FROM users WHERE username = 'admin' AND password =
'password';
```



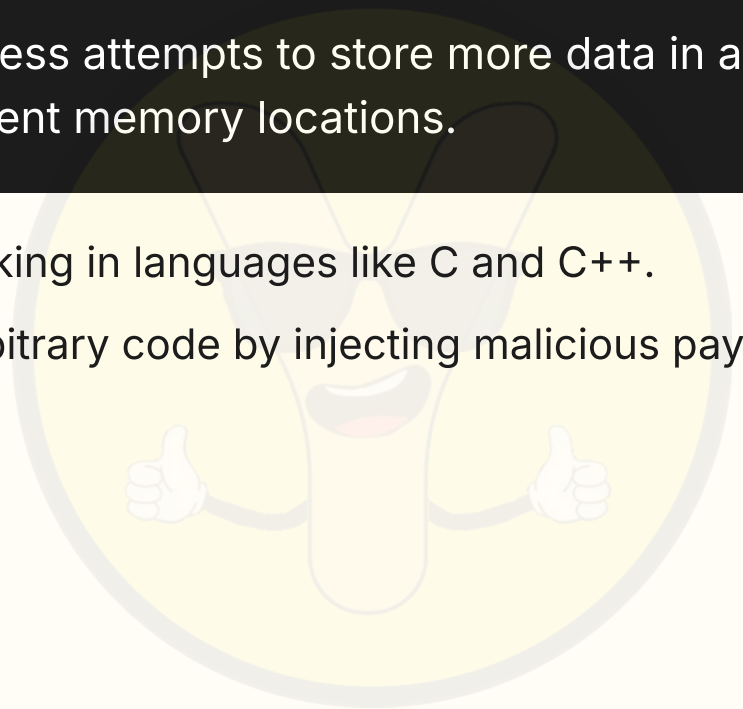
- Vulnerable input: admin' OR '1'='1
- Resulting query becomes: SELECT * FROM users WHERE username = 'admin' OR '1'='1' AND password = '';
- Bypasses authentication because the boolean condition '1'='1' is always true.

Buffer Overflow

BUFFER OVERFLOW VULNERABILITY

A programming flaw where a process attempts to store more data in a fixed-length memory buffer than it can hold, overwriting adjacent memory locations.

- Occurs due to lack of bounds checking in languages like C and C++.
- Attackers exploit this to execute arbitrary code by injecting malicious payloads into the stack or heap.



Attacks on Wireless Networks

Wireless networks are vulnerable to interception and compromise due to the broadcast nature of radio waves.

- Eavesdropping
  - Monitoring wireless traffic passively to capture sensitive unencrypted data packets.
- Rogue Access Points
  - Unauthorised access points set up by attackers to mimic legitimate corporate networks and harvest credentials.
- Evil Twin Attack
  - A fraudulent Wi-Fi access point that mimics a legitimate hotspot to intercept traffic from connected users.
- MAC Spoofing
  - Faking the Media Access Control address of a legitimate device to bypass MAC-filtering security.

Exam corner

- **Q1** Explain the working mechanism of a Proxy Server and how anonymity is maintained.
- **Q2** Differentiate clearly between a Virus, a Worm, and a Trojan Horse with examples.
- **Q3** What is a Buffer Overflow attack? Explain how attackers exploit memory mismanagement.
- **Q4** Discuss SQL Injection vulnerabilities with a suitable query example and prevention methods.
- **Q5** Explain the concept of Steganography and compare it with traditional Cryptography.
- **Q6** What is a DDoS attack? Discuss various types of DDoS attack vectors.
- **Q7** Describe the different methods used for Password Cracking in cybercrime.

Unit 3 done. You are exam-ready.

Revise the Exam corner once more, then open Unit 4 on theycotes.com. Every AKTU subject, unit by unit, free. Notes by Chirag Jain, Ycotes.

