Sure! Here's a one-liner for each type of scan:

- ACK Scan: Sends TCP packets with only the ACK flag set to check firewall rules and determine if ports are filtered or unfiltered.

- FIN Scan: Sends TCP packets with only the FIN flag to identify open ports based on lack of response.

- NULL Scan: Sends TCP packets with no flags set to detect open ports by exploiting how some systems handle unexpected packets.

- XMAS Scan: Sends TCP packets with FIN, PSH, and URG flags set (like a lit Christmas tree) to probe for open ports through unusual responses.

Let me know if you'd like diagrams or examples!

Here’s a simple one-liner for each:

- Dictionary Attack: A password-cracking method that tries a list of likely passwords (a "dictionary") to guess a user's password.

- RC4: A fast and simple stream cipher used in encryption, now considered insecure due to multiple vulnerabilities.

Let me know if you want a short example or diagram for either!

- Encryption: The process of converting plain data into a coded format to prevent unauthorized access.

- Decryption: The process of converting encrypted data back into its original, readable format.

Here are one-liners for each:

- ifconfig: A command used to view or configure network interfaces on Unix/Linux systems.

- ping: A network tool that checks if a host is reachable and measures round-trip time.

- netstat: Displays network connections, routing tables, interface stats, and more.

- traceroute: Shows the path packets take to reach a destination across a network.

Reconnaissance is the process of gathering information about a target system or network to identify potential vulnerabilities before launching an attack.

Keylogger is a type of software or hardware that records every keystrokes made on keyboard, often used to steal sensitive information like password.

Cain and Abel is a password recovery tool for Windows that can crack passwords using methods like dictionary attacks, brute-force, and sniffing network traffic.

Nmap (Network Mapper) is a powerful open-source tool used for network discovery and security auditing by scanning hosts, ports, and services.

- \*\*Cross-Site Scripting (XSS) Attack\*\*: A security vulnerability where an attacker injects malicious scripts into web pages viewed by other users, potentially stealing sensitive information like cookies or session tokens.

- \*\*Session Cookies\*\*: Small pieces of data stored in a user's browser that track the user's session state, such as login status, while navigating a website.

- \*\*SQL Injection\*\*: A type of attack where an attacker manipulates SQL queries by injecting malicious code into input fields, potentially gaining unauthorized access to a database.

- \*\*WHOIS\*\*: A protocol used to query databases to retrieve information about domain names, IP addresses, and the entities that own or manage them.