Ransomware is malicious software that encrypts your system and demands payment for the decryption key, effectively encrypting your files and holding them hostage until the ransom is paid.

Rainbow Table: A collection of precomputed password hashes that allows for quick password hash cracking during cybersecurity attacks.

Reconnaissance is the process of gathering information about a target through methods such as Google searches, social media analysis, and other publicly available data in order to assess potential vulnerabilities.

Reverse engineering is the process of analyzing and reconstructing a piece of software in order to understand its functions, which is frequently done in order to discover vulnerabilities or modify the software's behavior.

Role-Based Access: Assigning specific permissions to roles rather than individual users, such as "Managers" and "Developers."

Rootkit: Malware that gives unauthorized users administrative access to a system, allowing them to control and manipulate it. Keyloggers and password sniffers are examples of rootkits.

Scanning: The process of probing a system by sending packets to gather information about the target, which frequently involves the 3-way handshake in network communication.

Secure Shell (SSH): A protocol that creates an encrypted communication channel between a client and a server, which is commonly used for secure remote server administration.

Session: The time that a communication channel between a client and a server is open, such as the time spent logged into a website.

Session Hijacking: Illegally taking control of another person's session, usually by stealing cookies and session tokens and performing actions on the victim's behalf.

Social engineering is the manipulation of individuals to reveal sensitive information or perform actions against their own interests, such as tricking someone over the phone into revealing a password.

SHA (Secure Hashing Algorithm):
A popular family of encryption algorithms, such as SHA256, which is highly secure and operates as a one-way function, making it suitable for password hashing.

Sniffing: Attacking networks as a man-in-the-middle, intercepting and analyzing data, often in wired or wireless environments.

Spam: Unwanted digital communication, such as email and social media messages, that typically attempts to entice recipients to engage in malicious activities.

Syslog: A system logging protocol that administrators use to capture and store all server activity, which is critical for monitoring and forensic analysis during security incidents.

SecureSockets Layer (SSL): A method of establishing an encrypted tunnel between a client and server in order to protect data during transmission, which is commonly used in secure online transactions.

Snort is a lightweight open-source Intrusion Detection System (IDS) for Windows and Linux that aids in the detection and response to network threats.

SQL Injection: A type of cyber attack on web applications that exploits SQL database vulnerabilities when user input is not properly validated, allowing unauthorized data access.