- **CRIME Attack:** Compression Ratio Info-Leak Made Easy (CRIME) is a client-side attack that exploits the vulnerabilities present in the data compression feature of protocols, such as SSL/TLS, SPDY, and HTTPS.
- **Circuit-Level Gateway Firewall:** Circuit-level gateways monitor requests to create sessions and determine if those sessions will be allowed.
- **Cross-Site Scripting (XSS) Attacks:** Cross-site scripting ('XSS' or 'CSS') attacks exploit vulnerabilities in dynamically generated web pages, enabling malicious attackers to inject client-side scripts into web pages viewed by other users.
- **Cross-Site Request Forgery (CSRF) Attack:** Cross-Site Request Forgery (CSRF) attacks exploit web page vulnerabilities that allow an attacker to force an unsuspecting user's browser to send malicious requests they did not intend.
- **Clickjacking Attack:** Attackers perform clickjacking attacks by tricking the victim into clicking on any malicious web page element that is placed transparently on the top of any trusted web page.
- **Cookie Poisoning:** It is a type of parameter tampering attack in which the attacker modifies the cookie contents to draw unauthorized information about a user and thus perform identity theft.
- **Cookie Sniffing:** It is a technique in which an attacker sniffs a cookie containing the session ID of the victim who has logged in to a target website and uses the cookie to bypass the authentication process and log in to the victim's account.
- **Cookie Replay:** It is a technique used to impersonate a legitimate user by replaying the session/cookie that contains the session ID of that user (as long as he/she remains logged in).
- **Camfecting Attack:** A camfecting attack is a webcam capturing attack that is performed to gain access to the camera of a target's computer or mobile device.
- **Critical Infrastructure:** A collection of physical or logical systems and assets that the failure or destruction of which will severely impact the security, safety, economy, or public health.
- **Cloud Computing:** Cloud computing is an on-demand delivery of IT capabilities where IT infrastructure and applications are provided to subscribers as a metered service over a network.
- **Container-as-a-Service (CaaS):** It provides services such as virtualization of container engines, management of containers, applications, and clusters through a web portal, or an API.
- **Community Cloud:** It is a multi-tenant infrastructure shared among organizations from a specific community with common computing concerns, such as security, regulatory compliance, performance requirements, and jurisdiction.
- **Cloud Consumer:** A person or organization that uses cloud computing services.
- **Cloud Provider:** A person or organization providing services to interested parties.
- **Cloud Carrier:** An intermediary for providing connectivity and transport services between cloud consumers and providers.
- **Cloud Auditor:** A party for making independent assessments of cloud service controls and taking an opinion thereon.
- **Cloud Broker:** An entity that manages cloud services in terms of use, performance, and delivery, and maintains the relationship between cloud providers and consumers.
- **Container:** A container is a package of an application/software including all its dependencies such as library files, configuration files, binaries, and other resources that run independently of other processes in the cloud environment.
- **Container Orchestration:** Container orchestration is an automated process of managing the lifecycles of software containers and their dynamic environments.

Printed by: shikridat@gmail.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

- **Cluster:** A cluster refers to a set of two or more connected nodes that run parallelly to complete a task.
- **Cloud Cryptojacking:** Cryptojacking is the unauthorized use of the victim's computer to stealthily mine digital currency.
- **Cloudborne Attack:** Cloudborne is a vulnerability residing in a bare-metal cloud server that enables the attackers to implant a malicious backdoor in its firmware.
- **Cache Poisoned Denial of Service (CPDoS):** In CPDoS, attackers create malformed or oversized HTTP requests to trick the origin web server into responding with malicious or error content, which is cached at the CDN servers.
- **Cloud Snooper Attack:** Cloud snooper attacks are triggered at AWS security groups (SGs) to compromise the target server and extract sensitive data stealthily.
- **Cloud Application Security:** It is a set of rules, processes, policies, controls, and techniques used to administer all the data exchange between collaborative cloud platforms.
- **Cloud Integration:** Cloud integration is the process of grouping multiple cloud environments together in the form of a public or hybrid cloud.
- **Cloud Auditing:** Cloud auditing is the process of analyzing the services offered by cloud providers and verifying the conformity to requirements for privacy, security, etc.
- **Cloud Security Alliance (CSA):** CSA is a nonprofit global organization that provides rising awareness and promotes best practices and security policies to help and secure the cloud environment.
- **CASB:** Cloud Access Security Brokers (CASBs) are on-premise or cloud-hosted solutions responsible for enforcing security, compliance, and governance policies for the cloud applications.
- **Cryptography:** Cryptography is the conversion of data into a scrambled code that is encrypted and sent across a private or public network.
- **CAST-128:** CAST-128, also called CAST5, is a symmetric-key block cipher having a classical 12- or 16-round Feistel network with a block size of 64 bits.
- **Camellia:** Camellia is a symmetric-key block cipher having either 18 rounds (for 128-bit keys) or 24 rounds (for 256-bit keys).
- **Cryptanalysis:** Cryptanalysis is the study of ciphers, ciphertext, or cryptosystems with the ability to identify vulnerabilities in them and thus extract plaintext from ciphertext even if the cryptographic key or algorithm used to encrypt the plaintext is unknown.

D

- **Distribution Attacks:** Distribution attacks occur when attackers tamper with hardware or software prior to installation.
- **Defense-in-Depth:** Defense-in-depth is a security strategy in which several protection layers are placed throughout an information system.
- **Diamond Model:** The Diamond Model offers a framework for identifying the clusters of events that are correlated on any of the systems in an organization.
- **Deep web:** It consists of web pages and contents that are hidden and unindexed and cannot be located using traditional web browsers and search engines.
- **Dark Web or Darknet:** It is the subset of the deep web that enables anyone to navigate anonymously without being traced.
- **Dumpster Diving:** This uncouth technique, also known as trashing, involves the attacker rummaging for information in garbage bins.