- **Reflector Antennas:** Reflector antennas are used to concentrate EM energy that is radiated or received at a focal point.
- **Reverse Engineering:** Reverse engineering is the process of analyzing and extracting the source code of a software or application, and if needed, regenerating it with required modifications.
- **RC4:** RC4 is a variable key-size symmetric-key stream cipher with byte-oriented operations, and it is based on the use of a random permutation.
- **RC5:** RC5 is a fast symmetric-key block cipher designed by Ronald Rivest for RSA Data Security (now RSA Security).
- **RC6:** RC6 is a symmetric-key block cipher derived from RC5. It is a parameterized algorithm with a variable block size, key size, and number of rounds.
- **Rivest Shamir Adleman (RSA):** Ron Rivest, Adi Shamir, and Leonard Adleman formulated RSA, a public-key cryptosystem for Internet encryption and authentication.
- **RIPEMD-160:** RACE Integrity Primitives Evaluation Message Digest (RIPEMD) is a 160-bit hash algorithm developed by Hans Dobbertin, Antoon Bosselaers, and Bart Preneel.
- **Rainbow Table Attack:** A rainbow table attack is a type of cryptography attack where an attacker uses a rainbow table to reverse cryptographic hash functions.
- **Related-Key Attack:** An attacker launch a related key attack by exploiting the mathematical relationship between keys in a cipher to gain access over encryption and decryption functions.

S

- **Suicide Hackers:** Suicide hackers are individuals who aim to bring down critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment.
- **Script Kiddies:** Script kiddies are unskilled hackers who compromise systems by running scripts, tools, and software developed by real hackers.
- **State-Sponsored Hackers:** State-sponsored hackers are individuals employed by the government to penetrate, gain top-secret information from, and damage the information systems of other governments.
- **Scanning:** Scanning refers to the pre-attack phase when the attacker scans the network for specific information based on information gathered during reconnaissance.
- **Supervised Learning:** Supervised learning uses algorithms that input a set of labeled training data to attempt to learn the differences between the given labels.
- **Sarbanes Oxley Act (SOX):** Enacted in 2002, the Sarbanes-Oxley Act aims to protect the public and investors by increasing the accuracy and reliability of corporate disclosures.
- **Shoulder Surfing:** In the shoulder surfing technique, an attacker stands behind the victim and secretly observes the victim's activities on the computer, such as keystrokes while entering usernames, passwords, and so on.
- **Stealth Scan (Half-open Scan):** Stealth scanning involves abruptly resetting the TCP connection between the client and server before the completion of three-way handshake signals, thus leaving the connection half-open.
- **SCTP INIT Scanning:** Attackers send an INIT chunk to the target host, and an INIT+ACK chunk response implies that the port is open, whereas an ABORT Chunk response means that the port is closed.
- **SCTP COOKIE ECHO Scanning:** Attackers send a COOKIE ECHO chunk to the target host, and no response implies that the port is open, whereas an ABORT Chunk response means that the port is closed.
- **Source Routing:** Source routing refers to sending a packet to the intended destination with a partially or completely specified route (without firewall-/IDS-configured routers) in order to evade an IDS or firewall.

- **Source Port Manipulation:** Source port manipulation refers to manipulating actual port numbers with common port numbers in order to evade an IDS or firewall.
- **SNMP Enumeration:** SNMP enumeration is the process of enumerating user accounts and devices on a target system using SNMP.
- **Spyware:** Spyware is a stealthy program that records the user's interaction with the computer and the Internet without the user's knowledge and sends the information to the remote attackers.
- **Steganography:** Steganography is a technique of hiding a secret message within an ordinary message and extracting it at the destination to maintain confidentiality of data.
- **Spam/Email Steganography:** Spam/email steganography refers to the technique of sending secret messages by hiding them in spam/email messages.
- **Steganalysis:** Steganalysis is the art of discovering and rendering covert messages using steganography.
- **Skeleton Key Attack:** A skeleton key is a form of malware that attackers use to inject false credentials into domain controllers (DCs) to create a backdoor password.
- **Silver Ticket Attack**: A silver ticket attack is a post-exploitation technique implemented by an attacker to steal legitimate users' credentials and create a fake Kerberos Ticket Granting Service (TGS) ticket.
- **Sheep Dip Computer:** Sheep dipping refers to the analysis of suspect files, incoming messages, etc. for malware.
- **Static Malware Analysis:** It involves going through the executable binary code without executing it to have a better understanding of the malware and its purpose.
- **System Baselining:** Baselining refers to the process of capturing the system state (taking a snapshot of the system) when the malware analysis begins, which can be compared with the system's state after executing the malware file.
- **SPAN Port:** A SPAN port is a port that is configured to receive a copy of every packet that passes through a switch.
- **STP Attack:** Attackers connect a rogue switch into the network to change the operations of the STP protocol and sniff all the network traffic.
- **SAD DNS Attack:** SAD DNS is a new variant of DNS cache poisoning, in which an attacker injects harmful DNS records into a DNS cache to divert all traffic toward their own servers.
- **Social Engineering:** Social engineering is the art of convincing people to reveal confidential information.
- **Spam Email:** Irrelevant, unwanted, and unsolicited emails that attempt to collect financial information, social security numbers, and network information.
- **Scareware:** Malware that tricks computer users into visiting malware infested websites, or downloading/buying potentially malicious software.
- **Spear Phishing:** Attackers send spear phishing to send a message with specialized, social engineering content directed at a specific person, or a small group of people.
- **Spimming:** A variant of spam that exploits Instant Messaging platforms to flood spam across the networks.
- **SMiShing:** SMiShing (SMS phishing) is the act of using SMS text messaging system of cellular phones or other mobile devices to lure users into instant action, such as downloading malware, visiting a malicious webpage, or calling a fraudulent phone number.
- **Smurf Attack:** In a Smurf attack, the attacker spoofs the source IP address with the victim's IP address and sends a large number of ICMP ECHO request packets to an IP broadcast network.