- **Packet Filtering Firewall:** In a packet filtering firewall, each packet is compared to a set of criteria before it is forwarded.
- **Pure Honeypots:** Pure honeypots emulate the real production network of a target organization.
- **Production Honeypots:** Production honeypots are deployed inside the production network of the organization along with other production servers.
- **Port Scanning:** Port scanning is used to identify open ports and the services running on these ports.
- **Patch:** A patch is a small piece of software designed to fix problems, security vulnerabilities, and bugs and improve the performance of a computer program or its supporting data.
- **Patch Management:** Patch management is a process used to fix known vulnerabilities by ensuring that the appropriate patches are installed on a system.
- **Pass-the-Cookie Attack:** The pass-the-cookie attack occurs when attackers obtain a clone of a cookie from the user's browser and uses the cookie to establish a session with the target web server.
- **Parabolic Grid Antenna:** A parabolic grid antenna uses the same principle as a satellite dish, but it does not have a solid dish. It consists of a semi-dish in the form of a grid consisting of aluminum wires.
- **Purdue Model:** The Purdue model is derived from the Purdue Enterprise Reference Architecture (PERA) model, which is a widely used to describe internal connections and dependencies of important components in the ICS networks.
- **Programmable Logic Controller (PLC):** A programmable logic controller (PLC) is a small solid-state control computer where instructions can be customized to perform a specific task.
- **Platform-as-a-Service (PaaS):** This offers development tools, configuration management, and deployment platforms on-demand, which can be used by subscribers to develop custom applications.
- **Public Cloud:** In this model, the provider makes services such as applications, servers, and data storage available to the public over the Internet.
- **Private Cloud:** A private cloud, also known as the internal or corporate cloud, is a cloud infrastructure operated by a single organization and implemented within a corporate firewall.
- **Post-quantum Cryptography:** Post-quantum cryptography is an advanced cryptographic algorithm designed to protect security systems from attacks initiated on both conventional and quantum computers.
- **Public Key Infrastructure (PKI):** PKI is a set of hardware, software, people, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates.
- **Pretty Good Privacy (PGP):** It is often used for data compression, digital signing, encryption and decryption of messages, emails, files, and directories, and to enhance the privacy of email communications.
- **Padding Oracle Attack:** In a padding oracle attack (also known as a Vaudenay attack), attackers exploit the padding validation of an encrypted message to decipher the ciphertext.

Q

- **Quantum Cryptography:** This cryptography is processed based on quantum mechanics, such as quantum key distribution (QKD), using photons instead of mathematics as a part of encryption.
- **Quantum Cryptanalysis:** Quantum cryptanalysis is the process of cracking cryptographic algorithms using a quantum computer.

R

- **Reconnaissance:** Reconnaissance refers to the preparatory phase where an attacker seeks to gather information about a target prior to launching an attack.

- **Risk:** Risk refers to the degree of uncertainty or expectation that an adverse event may cause damage to the system.
- **Risk Management:** Risk management is the process of reducing and maintaining risk at an acceptable level by means of a well-defined and actively employed security program.
- **Risk Identification:** Identifies the sources, causes, consequences, and other details of the internal and external risks affecting the security of the organization.
- **Risk Assessment:** Assesses the organization's risk and provides an estimate of the likelihood and impact of the risk.
- **Risk Treatment:** Selects and implements appropriate controls for the identified risks.
- **Risk Tracking:** Ensures appropriate controls are implemented to handle known risks and calculates the chances of a new risk occurring.
- **Risk Review:** Evaluates the performance of the implemented risk management strategies.
- **Return-Oriented Programming (ROP) Attack:** Return-oriented programming is an exploitation technique used by attackers to execute arbitrary malicious code in the presence of security protections such as code signing and executable space protection.
- **RPC:** Remote Procedure Call (RPC) allows clients and servers to communicate in distributed client/server programs.
- **Resource Exhaustion:** A resource exhaustion attack damages the server by sending multiple resource requests from different locations to exploit software bugs or errors, thereby hanging the system and server or causing a system crash.
- **Race Condition:** A race condition is an undesirable incident that occurs when a software or system program depends on the execution of processes in a sequence and on the timing of the programs.
- **Replay Attack:** In a replay attack, packets and authentication tokens are captured using a sniffer. After the relevant information is extracted, the tokens are placed back on the network to gain access.
- **Rainbow Table:** A rainbow table is a precomputed table that contains word lists like dictionary files, brute force lists, and their hash values.
- **Rootkits:** Rootkits are programs that hide their presence as well as attacker's malicious activities, granting them full access to the server or host at that time, and in the future.
- **Rich Text Format (RTF) Injection:** RTF injection involves exploiting features of Microsoft Office such as RTF template files that are stored locally or in a remote machine.
- **Ransomware:** Ransomware is a type of malware that restricts access to the computer system's files and folders and demands an online ransom payment to the malware creator(s) to remove the restrictions.
- **Rogue DHCP Server Attack:** The attacker sets up a rogue DHCP server on the network and responds to DHCP requests with bogus IP addresses resulting in compromised network access.
- **Reverse Social Engineering:** The attacker presents him/herself as an authority and the target seeks his or her advice before or after offering the information that the attacker needs.
- **RST Hijacking:** RST hijacking involves injecting an authentic-looking reset (RST) packet using a spoofed source address and predicting the acknowledgment number.
- **Research Honeypots:** Research honeypots are high-interaction honeypots primarily deployed by research institutes, governments, or military organizations to gain detailed knowledge about the actions of intruders.
- **RASP:** Runtime application self protection (RASP) provides security to web and non-web application running on a server.