Null-Byte Injection:
An attacker attempts to exploit a web server by injecting null bytes (%00 or 0x00) into URLs. This manipulation causes the server to return unintended data.

Network Interface Card (NIC):
A computer is equipped with a NIC, allowing it to connect to a local area network (LAN) or the internet.

Network Address Translation (NAT):
A home network employs NAT to convert local IP addresses (for example, 192.168.1.20) to global IP addresses.

Nmap:
A cybersecurity professional uses Nmap to scan a network too look for open ports, active services, and operating system details.

Netcat:
An administrator employs Netcat to view and record data transmitted over TCP or UDP connections.

Nikto:
A security analyst uses Nikto to scan a web app for vulnerabilities

Nessus:
A security expert uses Nessus Essentials to hunt for vulnerabilities in the company's software and report it to the appropriate team

Packet:
Data transmitted between systems is encapsulated into packets.

Password Cracking:
A security professional or hacker attempts to crack an encrypted password using tools like John the Ripper

Password Sniffing:
A hacker launches a man-in-the-middle attack using tools like BurpSuite to intercept and analyze network traffic.

Patch:
A vendor releases a patch to address a bug or vulnerability in their software system.

Phishing:
Fake websites resembling like legitimate ones, such as instagram.com, inorder to deceive users into providing sensitive information.

Ping Sweep:
Sending ping requests to multiple IPs to identify if the hosts are active.

Public Key Cryptography:
Messages encrypted with the public key can only be decrypted using the corresponding private key using algorithms such as RSA

Public Key Infrastructure (PKI):
Digital certificates can be generated, stored, and distributed via a PKI system.

Personally Identifiable Information (PII):
PII includes any information that can identify an individual, such as their address or phone number.

Payload:
A malicious payload is a piece of code that, when executed, accomplishes a particular task. An example of one would be a keylogger.

PCI-DSS:
Companies that process credit cards for customers are required to follow the Payment Card Industry Data Security Standard (PCI-DSS).