**Glossary terms from module 2**

**Terms and definitions from Course 6, Module 2**

**Command and control (C2):** The techniques used by malicious actors to maintain communications with compromised systems

**Command-line interface (CLI):** A text-based user interface that uses commands to interact with the computer

**Data exfiltration:** Unauthorized transmission of data from a system

**Data packet:** A basic unit of information that travels from one device to another within a network

**Indicators of compromise (IoC):** Observable evidence that suggests signs of a potential security incident

**Internet Protocol (IP):** A set of standards used for routing and addressing data packets as they travel between devices on a network

**Intrusion detection systems (IDS):** An application that monitors system activity and alerts on possible intrusions

**Media Access Control (MAC) Address:** A unique alphanumeric identifier that is assigned to each physical device on a network

**National Institute of Standards and Technology (NIST) Incident Response Lifecycle:** A framework for incident response consisting of four phases: Preparation; Detection and Analysis; Containment, Eradication and Recovery; and Post-incident activity

**Network data:** The data that’s transmitted between devices on a network

**Network protocol analyzer (packet sniffer):** A tool designed to capture and analyze data traffic within a network

**Network traffic:** The amount of data that moves across a network

**Network Interface Card (NIC):** Hardware that connects computers to a network

**Packet capture (p-cap):** A file containing data packets intercepted from an interface or network

**Packet sniffing:** The practice of capturing and inspecting data packets across a network

**Playbook:** A manual that provides details about any operational action

**Root user (or superuser)**:A user with elevated privileges to modify the system

**Sudo:** A command that temporarily grants elevated permissions to specific users

**tcpdump:** A command-line network protocol analyzer

**Wireshark:** An open-source network protocol analyzer