# Glossary

# Intro to IT & Cybersecurity

**Created By: Adolfo Alarcon, Teaching Assistant**

Provide the term in **Bold** and then provide the explanation after it separated by a hyphen. These can be organized alphabetically, by module, etc.

### Module 1: Introduction

**1. System Administration -** Responsible for a system or specific components of a system.

a. Install, configure, and maintain hardware and software
b. Adhere to and enforce policies and procedures
c. Provide technical support to users
d. Perform regular backups and data recovery as needed.

**2. Network Engineering -** Responsible for building, maintaining, and protecting networks

a. Analyze design and requirement documents from different departments and then make appropriate changes to network topology.
b. Operate network services and systems, to include hardware and virtual environments.

**3. Incident Response & Forensics -** Responsible for identifying and responding to incidents.

a. Follow a standard process to analyze data to determine if an incident occurred, the severity of the incident, mitigation of the incident, and assess the effectiveness of solutions.
b. Use forensic tools to harvest data for civil, administrative, and criminal investigations.

**4. Offensive Security & Pentesting** - Responsible for identifying security gaps and vulnerabilities by emulating threat actors.

a. Perform security analysis against the networks of anything from small nonprofits to multinational corporations.

b. Use a combination of technical and social approaches to find weaknesses in the target organization, then document and provide remediation options for those weaknesses.

## Module 2: System Administration

**1. System Administrator Duties:**

a. Determine technical needs
b. Install, maintain, upgrade, and repair hardware and software
c. Evaluate and optimize performance, security, and survivability
    i. CIANA:
        1. Confidentiality
        2. Integrity
        3. Authentication
        4. Non-Repudiation
        5. Availability
d. Create, manage, and train users
e. Follow and enforce policies and regulations
f. Solve problems related to the items listed above

**2. Sysinternals** - A suite of troubleshooting tools

**3. Powershell** - Built on top of the Windows command prompt, offers some Linux commands, improved scripting, and a whole pair of quality of life upgrades.

**4. Wireshark** - The gold standard in packet-capture tools.

**5. Packet-Capturing** - Monitoring your network for communications that are happening on your network.

**6. Microsoft Management Console (MMC)** - The one-stop for all Microsoft built-ins, takes all Microsoft profiles (user, network and computer management) and makes them accessible in one location.

## Module 3: Network Engineering

**1. Network Engineer Duties:**

a. Determine network topology
b. Configure, operate, and maintain network equipment
c. Evaluate network traffic and performance
d. Backups

i. Incremental - Backup from the last change
ii. Differential - Backup everything from last full backup
iii. Full - Backup everything

e. Regulations and Policies
f. Security
g. Troubleshooting

## Module 4: Incident Response & Forensics

**1. Security Operations Center (SOC) Analyst Duties:**

a. Monitor critical systems for security threats
b. Analyze logs and reports to provide threat intelligence
c. Perform incident Response and triage
d. Investigate security threats and breaches

**2. Incident Response Sequence:**

a. Preparation
b. Detection and Analysis
c. Containment
d. Eradication and Recovery
e. Post-Incident Activity

**3. Hash** - An algorithm that is fed the bits of a file (0s and 1s) into a set of rules that process them into a string that matches to a set of bits.

## Module 5: Offensive Security & Penetration Testing

**1. Pentester Duties:**

a. Emulate threat actors in order to identify and remediate security gaps
b. Establish physical, social, and technological approaches to defeating security, then design solutions to those attacks.
c. Maintain awareness of new vulnerabilities and mitigations.

**2. Threat Emulation -** Emulating a threat actor

a. Organizational Weaknesses
b. Physical Weaknesses
c. Technological Weaknesses

**3. Pentesting Model:**

a. Reconnaissance
b. Scanning
c. Gaining Access
d. Maintaining Access
e. Covering Tracks