**Methods to Performing Intrusion Analysis, Intrusion Kill Chain**

Performing intrusion analysis involves following a systematic approach to investigate and understand the attack. One common framework used in intrusion analysis is the Intrusion Kill Chain. The Kill Chain is a model that describes the stages of a cyberattack. Here are the steps involved in performing intrusion analysis using the Kill Chain framework:

1. Reconnaissance: The attacker gathers information about the target, such as identifying potential vulnerabilities, network architecture, or employee details. In intrusion analysis, analysts examine network logs, traffic patterns, and external threat intelligence to identify any reconnaissance activities.
2. Weaponization: In this phase, the attacker develops or acquires the necessary tools or malware to exploit the identified vulnerabilities. Analysts focus on identifying indicators of weaponization, such as malicious code or exploit attempts, through analysis of email attachments, network traffic, or system artifacts.
3. Delivery: The attacker delivers the weaponized payload to the target system. Analysts investigate email headers, web logs, or network traffic to identify the delivery method, such as phishing emails, drive-by downloads, or watering hole attacks.
4. Exploitation: The attacker gains unauthorized access or compromises the target system. Intrusion analysts analyze network logs, intrusion detection/prevention system (IDS/IPS) alerts, and system logs to identify signs of exploitation, such as unusual network connections, system vulnerabilities, or successful brute force attempts.
5. Installation: After successful exploitation, the attacker installs malware or establishes a foothold within the compromised system. Analysts examine system artifacts, memory dumps, or file analysis to identify the presence of malicious code, backdoors, or unauthorized accounts.
6. Command and Control (C2): The attacker establishes communication channels with the compromised system to maintain control and issue commands. Intrusion analysts investigate network traffic, DNS logs, or firewall logs to detect any communication with suspicious or malicious domains or IP addresses.
7. Actions on Objective: The attacker achieves their intended goal, which could be data exfiltration, unauthorized access, or further lateral movement within the network. Analysts examine network traffic, log files, or system activity to identify any unauthorized or suspicious actions, such as data transfers, privilege escalation attempts, or lateral movement.

By following the Intrusion Kill Chain framework, intrusion analysts can systematically identify and analyze each stage of the attack, understand the attacker's techniques and intentions, and develop effective mitigation strategies. It allows for a comprehensive investigation of the incident, aids in identifying vulnerabilities, and provides insights to enhance security measures and prevent future attacks.