Things to Know About Attackers

Understanding attacker tactics, techniques, and procedures (TTPs) is crucial for defending against cyber threats. Attackers often use various methods to evade detection, confuse security systems, and hide their true identity. Here are some key things to know about attackers:

1. Slow Attacks Are Harder to Detect:

- **Slow and Low**: Attackers often use slow attacks (sometimes called low-and-slow attacks) to avoid triggering security alerts. Rather than launching a rapid, high-volume attack that might quickly be flagged by intrusion detection systems (IDS) or firewalls, the attacker sends a small number of malicious packets or makes subtle changes over a long period of time.
    - Example: A slow brute-force attack where the attacker attempts one or two login attempts every few minutes to avoid being noticed by systems designed to detect rapid login failures.
- **Evasion**: By spreading their activities over a longer timeframe, attackers evade threshold-based detection systems, which are more likely to miss low-volume traffic that doesn't cross alert thresholds.

2. Attackers Can Spoof Packets to Create Noise:

- **Noise Generation**: Attackers can spoof packets that mimic other types of attacks, deliberately creating a lot of noise in the network. This tactic is meant to distract or overwhelm the defenders, forcing them to deal with large amounts of fake or decoy traffic while the real attack is conducted quietly elsewhere.
    - Example: The attacker floods the network with thousands of spoofed SYN packets that simulate a Distributed Denial-of-Service (DDoS) attack. While security teams are busy mitigating the DDoS attack, the attacker is attempting a more targeted and stealthy attack, like privilege escalation or data exfiltration.
- **False Positives**: This tactic can cause false positives in security systems, making it more challenging for defenders to separate real threats from fake ones. It can exhaust the resources of security analysts or automated systems.

3. Attackers Can Spoof IP Addresses:

- **IP Spoofing**: Attackers can spoof (forge) the source IP address of packets to hide their real identity and make it look like the traffic is coming from a different device or location. This can be used to avoid detection, complicate attribution, or trigger attacks that appear to come from trusted sources.
    - Example: In a DDoS attack, the attacker may spoof the source IP addresses to make it appear as if the traffic is coming from hundreds or thousands of different systems, even though it is being orchestrated from one location.
- **Detecting IP Spoofing**:
    - TTL (Time to Live): One way to detect spoofed IP addresses is **by analyzing the TTL value in packet headers**. The TTL indicates the number of hops a packet can take before it is discarded. Comparing the TTL of the incoming packet with the TTL value obtained from a reverse lookup (the response packet) can help identify discrepancies.
        - Example: If the TTL value of a packet seems inconsistent with what is expected based on its source, it might indicate that the packet's source address has been spoofed.

    - Limitations of IP Spoofing: While IP spoofing can make attacks harder to trace, **it doesn't allow the attacker to receive responses from the spoofed packets, as the responses would be sent to the spoofed address**. This makes spoofing more useful in specific scenarios, like DDoS attacks, but less practical for attacks that require interaction.

4. Correlating IPs with Physical Location Is Difficult:

- Geolocation Challenges: Attempting to **correlate an IP address with a physical location is difficult and often inaccurate**. Attackers may use techniques such as proxy servers, VPNs, or Tor to hide their real IP address and location, making it nearly impossible to pinpoint where an attack is truly coming from.
    - IP Address Databases: Geolocation services that map IP addresses to physical locations (such as cities or countries) often use IP address databases. However, these databases are not always up-to-date, and in many cases, **IP addresses may be incorrectly associated with a location**.
    - Dynamic IPs and NAT: Some networks use NAT (Network Address Translation) or dynamic IP addressing, meaning that multiple devices share a single public IP address, or the IP address changes periodically, making it hard to tie an attack to a specific device or location.
- Proxy and VPN Evasion: Attackers frequently **route their traffic through proxies, VPNs, or anonymizing services like Tor to further obscure their location**. This can make it appear as though the attack is originating from a completely different country or region than where the attacker is truly located.

Summary:

1. **Slow Attacks Are Harder to Detect**: Attackers can use slow, subtle attacks to stay under the radar of detection systems.
2. Attackers Can **Spoof Packets**: By spoofing packets, attackers can create noise, simulate false attacks, and distract defenders from the real threat.
3. Attackers Can **Spoof IP** Addresses: Attackers can hide their true location by using spoofed IP addresses, but TTL analysis and reverse lookups can help detect discrepancies.
4. **Correlating IPs to Physical Locations Is Difficult**: Mapping IP addresses to physical locations is often inaccurate, and attackers can use VPNs, proxies, and other methods to obscure their true origin.

> Understanding these tactics helps defenders design better detection methods, mitigate threats effectively, and improve the accuracy of their response efforts.