# Detecting Port Scanning Activities in Network Environments

**Student Name:** Jeremie, Mihai, Bilel
**Coaches:** Mathias, Sananda

---

## 1. Introduction

Port scanning is a common reconnaissance technique used by attackers to identify open ports and services on a target machine or network. By identifying these entry points, malicious actors can tailor their attacks to exploit specific vulnerabilities. While port scanning itself is not necessarily malicious, it is often a precursor to more serious threats. Therefore, detecting port scanning activity is a critical step in proactive network defense.

---

## 2. Understanding Port Scanning

Port scanning involves systematically sending packets to a range of ports on a host to determine which ones are open, closed, or filtered. The most common types of port scans include:

- **TCP Connect Scan**
- **SYN Scan (Half-open Scan)**

Each scanning method attempts to evade detection by security tools, making it essential for defenders to employ a variety of detection strategies.

---

## 3. Detection Techniques

Several techniques can be employed to detect port scanning activities. These methods typically rely on identifying unusual traffic patterns, connection attempts, or packet signatures.

### 3.1. Signature-Based Detection

Signature-based Intrusion Detection Systems (IDS) such as Snort or Suricata can detect known port scanning tools and behaviors by comparing traffic against predefined rules or signatures.

- Example: Snort rules that detect excessive SYN packets from a single source IP over a short period.
- Limitation: May fail to detect new or modified scanning tools.

### 3.2. Anomaly-Based Detection

Anomaly detection involves monitoring network behavior for deviations from the baseline. If an IP suddenly attempts to access hundreds of ports across many IPs, this behavior is flagged.

- Tools: Zeek (formerly Bro), custom scripts using NetFlow data.
- Limitation: Can result in false positives if legitimate scanning occurs (e.g., vulnerability scans by internal teams).

### 3.3. Connection Rate Monitoring

Tracking the rate at which a single IP address attempts connections to different ports or IPs can reveal scanning activity.

- Indicators: High rate of failed connections, multiple connection attempts to sequential ports.
- Implementation: Network flow analysis tools like Cisco NetFlow or sFlow.

### 3.4. Firewall and IDS/IPS Logging

Modern firewalls and Intrusion Prevention Systems (IPS) log connection attempts and can be configured to alert or block suspected scanners.

- Example: Configuring iptables with `--limit` and `--recent` modules to detect and block repeated connection attempts.

### 3.5. Honeypots

Honeypots are decoy systems designed to attract attackers. Any unsolicited connection attempts to a honeypot can be assumed to be malicious or scanning activity.

- Example Tools: Cowrie (SSH honeypot), Honeyd (general-purpose).

- Advantage: High accuracy in detecting unauthorized activity.

## 4. Challenges in Detection

- **Low and Slow Scans:** Scanners that distribute scans over a long time period evade rate-based detection.
- **False Positives:** Legitimate applications may perform behavior similar to scanning (e.g., monitoring services).
- **Encrypted Traffic:** Makes it harder to inspect packet payloads for malicious intent.

## 5. Conclusion

Detecting port scanning is an essential aspect of network security. By employing a combination of signature-based tools, anomaly detection, and strategic monitoring, network defenders can identify and respond to scanning attempts before more serious intrusions occur. While no method is foolproof, layering these techniques increases overall security posture and reduces the window of opportunity for attackers.