**Network Security Analysis Report**

**1. Introduction** This report provides a comprehensive analysis of the network at IP address **10.48.221.92** through practical testing and enumeration of network services. Various security assessments, network mapping, access point identification, and traffic analysis have been performed to assess potential vulnerabilities and provide recommendations.

**2. Methodology** The following tools and techniques were used for network scanning and analysis:

- **Nmap** for service enumeration and vulnerability detection.
- **Zenmap** for network visualization.
- **Wireshark** and **tcpdump** for traffic analysis.
- **Airport (MacOS)** for detecting access points.

**3. Findings**

## 3.1 Service Enumeration

A detailed Nmap scan of **10.48.221.92** revealed the following open ports:

| Port | State | Service | Version |
|---|---|---|---|
| 1433/tcp | Open | ms-sql-s | Microsoft SQL Server 2019 15.00.2000 |
| 3000/tcp | Open | ppp | Unknown |
| 64189/tcp | Open | Unknown | - |
| 64640/tcp | Open | Unknown | - |

**Security Risks**

- **SQL Server (Port 1433)**: If weak authentication is enabled, attackers may exploit brute-force attacks.
- **Unidentified Services (Ports 64189, 64640)**: Potential security threats if services are misconfigured.

**Further Testing**

- Brute-force testing using ms-sql-brute for weak credentials.
- SQL connection test via sqlcmd.

## 3.2 Network Mapping

- A **network discovery scan** (nmap -sn 10.48.221.0/24) was conducted to identify other active hosts.
- The topology was visualized using **Zenmap**, revealing key network relationships and dependencies.

## 3.3 Access Points Identification

- Nearby access points were detected using airport -s (MacOS Wi-Fi scanning tool).
- The default gateway was scanned using nmap -p 1-65535 <router_ip> to identify exposed router services.
- Security risks such as weak encryption and open SSIDs were assessed.

### 3.4 Traffic Analysis

- **Wireshark** and **tcpdump** were used to capture network packets.
- SQL Server traffic was filtered (tcp.port == 1433) to analyze authentication attempts and possible plaintext credentials.
- Findings:
  - No unencrypted credentials were detected.
  - Several connection attempts were logged, suggesting possible brute-force attempts.

#### 4. Security Recommendations

- **Enforce Strong Authentication**: Ensure SQL Server and other services require complex passwords.
- **Restrict Network Access**: Limit open ports to authorized IPs only.
- **Secure Access Points**: Use WPA2/WPA3 encryption and disable SSID broadcasting.
- **Monitor Traffic Regularly**: Set up intrusion detection systems (IDS) to log unauthorized access attempts.

**5. Conclusion** The analysis of **10.48.221.92** revealed potential security concerns, primarily in SQL Server exposure and unidentified open services. Implementing stronger authentication, restricting network access, and monitoring traffic are critical steps in improving network security. Further testing with penetration tools is recommended to identify additional vulnerabilities.