Source of Information: ChatGPT

Network Analysis Report

1. Identified IP Addresses and Open Ports

This section details the IP addresses found on the network and the services running on their open ports.

IP Address	Open Ports (Service)
192.168.31.1	53 (domain), 80 (http), 443 (https), 7443 (oracleas-https), 8080 (http-proxy), 8443 (https-alt)
192.168.31.36	2869 (icslap)
[redacted]	135 (msrpc), 139 (netbios-ssn), 445 (microsoft-ds), 8000 (http-alt), 8089 (unknown)

2. Packet Capture Analysis with Wireshark (Optional)

Using Wireshark to capture network traffic can provide deeper insights into the services and communications occurring on the network. Specific areas of interest for analysis include:

- **DNS requests:** Traffic on port 53, originating from 192.168.31.1.
- **HTTP/HTTPS traffic:** Communications on ports 80 and 443, also originating from 192.168.31.1.
- **NetBIOS and SMB traffic:** Activity on ports 139 and 445, primarily from [redacted].
- **Unusual or unexpected traffic:** Any communications on non-standard ports such as 7443, 8089, or others.

3. Common Services Running on Those Ports

This table provides a description of the common services associated with the identified open ports.

Port	Common Service / Description
53	DNS (Domain Name System)

80	HTTP (Web Server)
443	HTTPS (Secure Web Server)
7443	Oracle Application Server HTTPS
8080	HTTP Proxy / Alternate Web Port
8443	HTTPS Alternate
2869	ICS (Internet Connection Sharing / UPnP)
135	Microsoft RPC (Remote Procedure Call)
139	NetBIOS Session Service (Windows file sharing)
445	Microsoft-DS / SMB (Windows file sharing)
8000	HTTP Alternate
8089	Unknown (could be custom application service)

4. Potential Security Risks from Open Ports

Open ports can present various security vulnerabilities if not properly secured or monitored.

- **DNS (Port 53):** If exposed externally, it could be exploited for DNS amplification attacks, leading to denial of service.
- **HTTP / HTTPS (Ports 80, 443, 8080, 8443, 8000):** Web servers can be targets for a range of attacks, including:
    - Outdated software vulnerabilities
    - SQL injection
    - Cross-site scripting (XSS)
    - Brute-force attacks
- **Oracle HTTPS (Port 7443):** This specific service could be a target for Oracle-specific exploits if the application server is not patched or configured securely.
- **UPnP / ICS (Port 2869):** Universal Plug and Play (UPnP) and Internet Connection Sharing (ICS) services are frequently exploited by malware and can allow remote attackers to gain control or access the network.

- **MSRPC / NetBIOS / SMB (Ports 135, 139, 445):** These Windows-centric services are highly targeted by malware (e.g., WannaCry) and can lead to:
    - Remote code execution
    - File sharing exploitation
    - Credential theft
    - Lateral movement within the network
- **Unknown ports (e.g., 8089):** Any service running on an unknown or non-standard port poses a risk if it is not identified, monitored, or kept updated. It could be a custom application with undocumented vulnerabilities.