Below is an example of a **Professional Reconnaissance & Information Gathering Report** that references your Wireshark screenshot and includes mock data in place of actual sensitive details. You can adapt or expand this template as needed for your specific environment and findings.

Professional Reconnaissance & Information Gathering Report

---

1. Introduction

1.1 Purpose and Scope

The purpose of this report is to document the methodology, tools, and findings from passive reconnaissance, active enumeration, and asset discovery conducted against the target environment. The scope of this engagement includes:

- Passive OSINT gathering using publicly available information and services.
- Network enumeration using approved scanning and discovery tools.
- Documentation of all identified systems, services, and potential vulnerabilities.
- Ethical and compliant reconnaissance adhering to relevant guidelines and legal requirements.

1.2 Objectives

1. Identify and document external information about the target (e.g., domain names, IP addresses, publicly available services).
2. Enumerate the internal network where authorized, identifying systems, open ports, services, and potential entry points.
3. Provide a comprehensive report with recommendations for further testing or mitigation.

---

2. Methodology

2.1 Passive Reconnaissance (OSINT)

Passive reconnaissance was performed to gather information about the target without directly interacting with its systems in a manner that might be detected. The OSINT sources and techniques used included:

1. **Search Engines**: Google, Bing, DuckDuckGo, etc.
2. **Social Media Platforms**: LinkedIn, Twitter, GitHub for identifying potential employees, technologies in use, etc.
3. **Domain & DNS Tools**: WHOIS lookups, DNS enumeration (Zone transfers, subdomain lookups, etc.).
4. **Public Data Archives**: Pastebin, public breach data repositories.
5. **Shodan**: For finding exposed services and devices associated with the target IP space.

Sample (Mock) Findings from OSINT

- **Domain Registration**: Target domain `examplecorp.com` registered to ExampleCorp, Inc. with contact details publicly available.
- **Subdomains Discovered**:
  - `mail.examplecorp.com`
  - `vpn.examplecorp.com`
  - `test.examplecorp.com`
- **Potential Employee Identifiers**: Several LinkedIn profiles listing job roles such as “Network Engineer,” “Security Analyst,” and “DevOps Engineer.”
- **Technology Stack**: Apache HTTP Server 2.4, Tomcat 9, WordPress 5.x on some subdomains.

2.2 Network Enumeration

Upon authorization, active scanning and network enumeration were conducted against internal IP ranges provided by the client. Tools used included:

- **Nmap** (Network Mapper)
- **Wireshark**
- **masscan** (for high-speed scanning)
- **Netdiscover** (for ARP-based host discovery on local segments)

Example Nmap Commands

1. `nmap -sS -p1-65535 -T4 -A 192.168.1.0/24`
2. `nmap -sU -p 53,123,161,162 -T4 192.168.1.0/24`

Example Network Segments Scanned (Mock)

- **192.168.1.0/24** (Corporate LAN)
- **10.10.10.0/24** (Development Network)
- **172.16.5.0/24** (DMZ)

---

3. Asset Discovery

During the enumeration phase, multiple hosts and services were identified. All discovered assets have been cataloged in the table below (using mock data). Each entry includes an assigned Host ID, IP address, hostname (if resolved), open ports, and identified services.

Host ID	IP Address	Hostname	Open Ports	Services/Version
H1	192.168.1.10	corp-ws01.examplecorp	22, 80, 443	SSH 7.6, Apache 2.4, SSL/TLS
H2	192.168.1.15	corp-ws02.examplecorp	135, 139, 445	Windows RPC, SMB (v3)
H3	192.168.1.20	corp-sql01.examplecorp	1433, 3389	MSSQL 2019, RDP
H4	10.10.10.50	dev-app01.examplecorp	8080, 8443	Tomcat 9.0
H5	172.16.5.100	dmz-web01.examplecorp	80, 443	Apache 2.4, SSL/TLS

---

4. Wireshark Analysis

4.1 Overview of Captured Traffic

A Wireshark capture was performed to observe network traffic on the internal subnet **192.168.1.0/24**. The screenshot below shows a sample of DNS and mDNS queries within the local environment:

> *Note: This is a placeholder link. In your final report, you would replace this with the actual screenshot you provided or embed it if possible.*

From the highlighted packets:

- **Source**: Local IP addresses making DNS or mDNS queries (e.g., `224.0.0.251` for mDNS).
- **Destination**: DNS servers or broadcast/multicast addresses used for name resolution.
- **Protocol**: Primarily DNS or mDNS.
- **Queries**: Various PTR (Pointer) queries, including `_companion-link._tcp.local` and other local service advertisements.

These entries indicate typical local service discovery traffic. The presence of `mDNS` suggests that devices on the network are using Apple's Bonjour or similar zero-configuration networking services to discover local hosts and services.

4.2 Findings and Observations

- **mDNS Traffic**: Normal in many modern networks for device and service discovery.
- **PTR Records**: Indicate that local devices are publishing or requesting service records.
- **Potential Misconfigurations**: If mDNS is not intended to be used in this environment, the broadcast traffic might be exposing more information than necessary.
- **Security Considerations**: Attackers can leverage mDNS or DNS queries to map out device names and potential services. Filtering or restricting multicast traffic might reduce the attack surface.

---

5. Potential Vulnerabilities and Areas of Concern

Based on the reconnaissance and enumeration, the following (mock) vulnerabilities or concerns were identified:

1. **Exposed SMB Services (Port 445)**: On Host `192.168.1.15`, SMBv1 might be enabled, which is insecure and susceptible to EternalBlue or similar exploits.
2. **Default Tomcat Credentials**: Host `10.10.10.50` might be using default Tomcat credentials (`tomcat:tomcat`).
3. **Open RDP Port (3389)**: Host `192.168.1.20` with RDP accessible internally could be a lateral movement vector if credentials are compromised.
4. **DNS & mDNS Traffic**: The broadcast of local services might allow an attacker to enumerate hostnames and services.

---

6. Recommendations

1. **Disable or Restrict SMBv1**: Ensure SMBv1 is disabled across all Windows hosts and SMB services.

2. **Harden Tomcat Server**: Change default credentials, implement strong password policies, and restrict administrative interfaces to trusted IP ranges.
3. **Segment RDP Services**: Restrict RDP to a dedicated management VLAN or use a jump box for secure access.
4. **Review mDNS Usage**: If not required for business operations, consider disabling mDNS or limiting it to necessary hosts.
5. **Regularly Update and Patch**: Ensure all operating systems, applications, and frameworks are up to date to mitigate known vulnerabilities.

---

7. Conclusion

This reconnaissance engagement identified various systems and services within the target network. The passive OSINT revealed publicly accessible information and potential subdomains. Active enumeration uncovered multiple hosts running services that could be exploited if not properly secured.

Key takeaways include:

- Comprehensive OSINT is critical for mapping external exposure.
- Network enumeration with tools like Nmap and Wireshark provided valuable insights into open ports, protocols, and potential vulnerabilities.
- mDNS and DNS traffic can reveal a significant amount of network topology and service information.

Next Steps:

- Implement the recommended security measures.
- Conduct further in-depth vulnerability assessments or penetration testing on critical systems.
- Continuously monitor and audit the network to maintain a secure environment.

---

8. References

- Nmap Security Scanner
- Wireshark Network Analyzer
- Shodan
- OWASP Testing Guide

Appendices

Appendix A: Detailed Nmap Output (Sample)

```
# Nmap 7.91 scan initiated Fri Mar 3 10:00:00 2025
nmap -sS -p1-65535 -A -T4 192.168.1.0/24

Host: 192.168.1.10
Open ports:
22/tcp   SSH
80/tcp   HTTP
443/tcp  HTTPS
...
```

Appendix B: Wireshark Filter Examples

1. **DNS Traffic**: `udp.port == 53 or tcp.port == 53`
2. **mDNS Traffic**: `udp.port == 5353`
3. **Filter by IP**: `ip.addr == 192.168.1.10`

Report Summary

This report demonstrates a structured approach to passive reconnaissance, active network enumeration, and asset discovery. The findings, while based on mock data, illustrate common issues and misconfigurations observed in many corporate networks. By following the recommendations, the target environment can reduce its attack surface and enhance overall security posture.

End of Report