# Network Traffic Analysis - Student Worksheet

**Name:** **\_\_\_\_** **Date:** **\_\_\_\_**

**Lab Partner:** **\_\_\_\_** **Section:** **\_\_\_\_**

## 🔧 Pre-Exercise Setup Verification

**Before starting network analysis, verify your environment is ready:**

### Step 1: Check Docker Environment

# Verify containers are running:  
cd docker && docker-compose ps

**Container Status Check:**

* ☐ cybersec\_sandbox - State: Up
* ☐ vulnerable\_web\_app - State: Up

### Step 2: Test Network Analysis Tools

# Test Network Analysis CLI:  
python src/analyzer/network\_cli.py --help  
  
# Test basic network tools:  
nmap --version  
netstat --version

**Network Tools Check:**

* ☐ Network Analysis CLI available ✅
* ☐ Nmap available ✅
* ☐ Netstat available ✅

### Step 3: Verify Network Scenarios

# Check sample network scenarios:  
ls samples/network-scenarios/  
python samples/network-scenarios/basic\_network\_activity.py --help

**Network Scenarios Check:**

* ☐ Network scenario scripts accessible ✅
* ☐ Basic network activity script executable ✅

### Step 4: Test Target Applications (Network Monitoring Targets)

# Test network monitoring targets:  
curl -s http://localhost:5000 | head -2  
curl -s http://localhost:9090 | head -2

**Monitoring Targets Check:**

* ☐ Flask App accessible for monitoring ✅
* ☐ PWA App accessible for monitoring ✅

### Step 5: Basic Network Connectivity Test

# Test basic network monitoring:  
python src/analyzer/network\_cli.py --monitor-connections --duration 10

**Network Monitoring Test:**

* ☐ Network monitoring produces output ✅
* ☐ No connection errors ✅

### Troubleshooting:

**If any verification fails:**

1. Restart containers: cd docker && docker-compose down && docker-compose up -d
2. Wait 30 seconds for network services to initialize
3. Re-run verification commands
4. **Notify instructor if network tools don’t work - networking issues require administrator assistance**

**⚠️ Complete ALL verification steps before proceeding with network analysis exercises.**

## 🎯 Learning Objectives

By completing this worksheet, I will:

* ☐ Understand what network traffic analysis is and how it differs from SAST, DAST, and Sandbox analysis
* ☐ Practice monitoring network connections and identifying suspicious activity
* ☐ Learn to use network scanning tools to discover services and assess security
* ☐ Analyze network traffic patterns for indicators of compromise
* ☐ Generate professional network security reports with evidence

## 📚 Pre-Exercise Knowledge Check

### 1. Security Analysis Methods Comparison

Fill in the comparison table:

| Method | What it analyzes | When it runs | Real-time capability |
| --- | --- | --- | --- |
| SAST | **\_\_\_\_**\_**\_\_\_\_** | **\_\_\_\_**\_**\_\_\_\_** | **\_\_\_\_**\_\_\_\_\*\* |
| DAST | **\_\_\_\_**\_**\_\_\_\_** | **\_\_\_\_**\_**\_\_\_\_** | **\_\_\_\_**\_\_\_\_\*\* |
| Sandbox | **\_\_\_\_**\_**\_\_\_\_** | **\_\_\_\_**\_**\_\_\_\_** | **\_\_\_\_**\_\_\_\_\*\* |
| Network | **\_\_\_\_**\_**\_\_\_\_** | **\_\_\_\_**\_**\_\_\_\_** | **\_\_\_\_**\_\_\_\_\*\* |

### 2. Network Security Scenarios

**Scenario**: You notice that multiple computers in your network are making connections to an external IP address on port 4444, and there’s been unusual DNS query activity.

**Question**: What type of security incident might this indicate?

**Question**: How could network traffic analysis help you investigate this situation?

## 🌐 Exercise 1: Network Connection Monitoring

### Setup Phase

**Task**: Monitor active network connections to establish a baseline

1. **Check current network connections**:

* Command to run: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Use our network analysis tool**:

* Command to run: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Record baseline connections** (manual observation):

* Command to run: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Baseline Observations**:

How many active connections do you see? **\_\_\_\_** What are the most common ports being used? **\_\_\_\_**\_\_\_\_\*\*

Do you see any external IP addresses? **\_\_\_\_**\_\_\_\_\*\*

### Analysis Phase

1. **Run comprehensive connection monitoring**:

* Command to run: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Look for suspicious ports**:

* Command to run: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Connection Analysis Findings**:

List any connections you found on these suspicious ports:

* Port 4444: **\_\_\_\_**\_**\_\*\*\_\_**\*\*
* Port 6666: **\_\_\_\_**\_**\_\*\*\_\_**\*\*
* Port 1337: **\_\_\_\_**\_**\_\*\*\_\_**\*\*
* Port 31337: **\_\_\_\_**\_\_\_\_\*\*

**External Communication Analysis**: What external IP addresses is your system communicating with?

Are any of these concerning? Why? **\_\_\_\_**\_\_\_\_\*\*

### Risk Assessment

**Question**: Based on your analysis, are there any suspicious network connections? Explain:

**Question**: What additional investigation would you recommend?

## 🔍 Exercise 2: Network Service Discovery

### Discovery Phase

**Task**: Discover and analyze network services

1. **Scan localhost for services**:

* Command to run: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Check what services are listening**:

* Command to run: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Service Discovery Results**: Fill in the services you discovered:

| Port | Service Name | Protocol | Security Risk Level | Notes |
| --- | --- | --- | --- | --- |
| **\_** | **\_\_\_\_**\_\_\_\_\*\* | **\_\_\_\_** | **\_\_\_\_**\_\_\_\_\*\* | **\_\_** |
| **\_** | **\_\_\_\_**\_\_\_\_\*\* | **\_\_\_\_** | **\_\_\_\_**\_\_\_\_\*\* | **\_\_** |
| **\_** | **\_\_\_\_**\_\_\_\_\*\* | **\_\_\_\_** | **\_\_\_\_**\_\_\_\_\*\* | **\_\_** |
| **\_** | **\_\_\_\_**\_\_\_\_\*\* | **\_\_\_\_** | **\_\_\_\_**\_\_\_\_\*\* | **\_\_** |
| **\_** | **\_\_\_\_**\_\_\_\_\*\* | **\_\_\_\_** | **\_\_\_\_**\_\_\_\_\*\* | **\_\_** |

### Security Assessment

1. **Generate detailed service analysis**:

* Command to run: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**High-Risk Services Identified**:

List any high-risk services you found:

* Service: **\_\_\_\_**\_**\_\_\_\_** Port: **\_\_** Risk: **\_\_\_\_**
* Service: **\_\_\_\_**\_**\_\_\_\_** Port: **\_\_** Risk: **\_\_\_\_**
* Service: **\_\_\_\_**\_**\_\_\_\_** Port: **\_\_** Risk: **\_\_\_\_**

**Security Recommendations**: For each high-risk service, what would you recommend?

### Service Research

**Research Task**: Pick one service you discovered and research it:

**Service Name**: **\_\_\_\_**\_**\_\*\*\_\_**\*\* **Purpose**: **\_\_\_\_**\_\_\_\_\*\*

**Common Vulnerabilities**: **\_\_\_\_**\_**\_\*\*\_\_**\*\*

**Security Best Practices**: **\_\_\_\_**\_\_\_\_\*\*

## 📡 Exercise 3: Traffic Pattern Analysis

### Baseline Traffic Analysis

**Task**: Analyze network traffic patterns for suspicious activity

1. **Start traffic monitoring**:

* Command to run: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Generate some network activity** (in another terminal):

* Commands to run:  
  - curl http://httpbin.org/get  
  - ping -c 5 8.8.8.8  
  - nslookup google.com

### Traffic Analysis Results

**Protocol Analysis**: Record the traffic patterns you observed:

| Protocol | Number of Connections | Percentage | Normal/Suspicious |
| --- | --- | --- | --- |
| TCP | **\_\_** | **\_\_**% | **\_\_\_\_**\_**\_\_\_\_** |
| UDP | **\_\_** | **\_\_**% | **\_\_\_\_**\_**\_\_\_\_** |
| ICMP | **\_\_** | **\_\_**% | **\_\_\_\_**\_**\_\_\_\_** |
| Other | **\_\_** | **\_\_**% | **\_\_\_\_**\_**\_\_\_\_** |

**Destination Analysis**: What external destinations did you communicate with?

**Suspicious Activity Detection**: Did you observe any suspicious network patterns?

### Advanced Traffic Analysis

1. **Run extended traffic capture**:

* Command to run: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Advanced Findings**: What additional patterns did the extended analysis reveal?

**Failed Connections**: Were there any failed connection attempts? If so, list them:

## 🔍 Exercise 4: DNS Traffic Analysis

### DNS Monitoring Setup

**Task**: Monitor DNS queries for suspicious patterns

1. **Start DNS monitoring**:

* Command to run: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Generate DNS queries**:

* Commands to run:  
  - nslookup google.com  
  - nslookup github.com  
  - dig stackoverflow.com

### DNS Analysis Results

**DNS Query Patterns**: Record your DNS analysis results:

| Domain Queried | Query Type | Response Time | Suspicious (Y/N) | Reason |
| --- | --- | --- | --- | --- |
| **\_\_\_\_** | **\_\_\_\_\*\*\_\_**\*\* | **\_\_\_\_**\_**\_\_\_\_** | **\_\_\_\_** | **\_\_** |
| **\_\_\_\_** | **\_\_\_\_\*\*\_\_**\*\* | **\_\_\_\_**\_**\_\_\_\_** | **\_\_\_\_** | **\_\_** |
| **\_\_\_\_** | **\_\_\_\_\*\*\_\_**\*\* | **\_\_\_\_**\_**\_\_\_\_** | **\_\_\_\_** | **\_\_** |
| **\_\_\_\_** | **\_\_\_\_\*\*\_\_**\*\* | **\_\_\_\_**\_**\_\_\_\_** | **\_\_\_\_** | **\_\_** |

**Suspicious DNS Indicators**: Look for these patterns and check if you found any:

* ☐ Unusually long subdomain names (potential DNS tunneling)
* ☐ Queries to suspicious top-level domains (.tk, .ml, etc.)
* ☐ High frequency of queries to the same domain
* ☐ Failed DNS resolutions to suspicious domains

### DNS Security Assessment

**Question**: Based on your DNS analysis, are there any security concerns?

**Question**: What DNS security measures would you recommend?

## 📊 Synthesis and Network Security Report

### Comprehensive Threat Assessment

Complete your network security assessment:

| Analysis Area | Findings Summary | Risk Level | Evidence | Recommended Actions |
| --- | --- | --- | --- | --- |
| Connection Monitoring | **\_\_\_\_**\_\_\_\_\*\* | **\_\_\_\_\*\*\_\_**\*\* | **\_\_\_\_** | **\_\_\_\_**\_**\_\_\_\_** |
| Service Discovery | **\_\_\_\_**\_\_\_\_\*\* | **\_\_\_\_\*\*\_\_**\*\* | **\_\_\_\_** | **\_\_\_\_**\_**\_\_\_\_** |
| Traffic Patterns | **\_\_\_\_**\_\_\_\_\*\* | **\_\_\_\_\*\*\_\_**\*\* | **\_\_\_\_** | **\_\_\_\_**\_**\_\_\_\_** |
| DNS Analysis | **\_\_\_\_**\_\_\_\_\*\* | **\_\_\_\_\*\*\_\_**\*\* | **\_\_\_\_** | **\_\_\_\_**\_**\_\_\_\_** |

### Critical Thinking Questions

1. **Detection Capabilities**: What types of attacks would network traffic analysis be most effective at detecting?
2. **Limitations**: What are the limitations of network traffic analysis? What might it miss?
3. **Real-World Application**: How would you implement continuous network monitoring in an organization?
4. **Integration**: How does network analysis complement SAST, DAST, and sandbox analysis?

### Tool Mastery Checklist

Check off the tools and techniques you’ve successfully used:

**Network Monitoring Tools**:

* ☐ network\_cli.py - Educational network analysis tool
* ☐ netstat - Network connection display
* ☐ ss - Socket statistics
* ☐ nslookup / dig - DNS query tools

**Analysis Techniques**:

* ☐ Connection pattern analysis
* ☐ Service discovery and risk assessment
* ☐ Traffic flow analysis
* ☐ DNS query pattern analysis

**Security Concepts**:

* ☐ Suspicious port identification
* ☐ Protocol analysis and assessment
* ☐ External communication monitoring
* ☐ Network-based threat detection

## 🏆 Challenge Questions (Optional)

### Advanced Network Analysis

**Challenge 1**: Research a real network-based attack (e.g., APT, botnet, data exfiltration). How would network traffic analysis help detect and investigate this attack?

**Challenge 2**: Design a network monitoring strategy for a small business. What tools and techniques would you implement?

### Career Connection

**Challenge 3**: Research the role of a “Network Security Analyst” or “SOC Analyst.” How do they use network traffic analysis in their daily work?

**Challenge 4**: What certifications or skills would be valuable for a career in network security monitoring?

## 📝 Self-Assessment

Rate your confidence level (1-5, where 5 = very confident):

* Understanding network traffic analysis concepts: **\_**/5
* Using network monitoring tools effectively: **\_**/5
* Identifying suspicious network patterns: **\_**/5
* Analyzing network services and risks: **\_**/5
* Generating professional network security reports: **\_**/5

**What was the most challenging part of this exercise?**

**What was the most interesting discovery you made?**

**How does network analysis complement the other security testing methods you’ve learned?**

**What would you like to learn more about in network security?**

## ⚖️ Legal and Ethical Considerations

### Professional Responsibility in Network Analysis

**1. Employment Impact:** How could network security incidents affect IT and security staff careers?

**2. Privacy Rights:** What privacy concerns arise when monitoring network traffic and user communications?

**3. Intellectual Property:** How could network vulnerabilities expose proprietary data or trade secrets?

### Regulatory and Legal Compliance

**4. Network Monitoring Laws:** What legal restrictions apply to network traffic monitoring in your jurisdiction?

**5. Data Protection Compliance:** How do network security gaps violate Privacy Act,1988 (Privacy Act) or industry regulations?

### Ethical Network Security

**6. Authorized Monitoring:** Why is it critical to only monitor networks you own or have explicit permission to analyze?

**7. Incident Reporting:** What are your ethical obligations when discovering network security incidents?

## 🔐 Cryptography and Network Security

### Network Cryptographic Assessment

**1. Encryption in Transit:** What issues did you find with data encryption over the network?

**2. Certificate Management:** Did you identify any problems with SSL/TLS certificates or PKI infrastructure?

**3. VPN and Tunnel Security:** How would you assess the cryptographic strength of network tunnels?

**4. Network Cryptography Recommendations:** What cryptographic improvements would strengthen network security?

## 💼 Business Impact Assessment

### Enterprise Network Security Impact

**1. Business Continuity:** How would network security incidents affect critical business operations?

**2. Financial Impact:** Estimate the potential costs of network security breaches:

* **Downtime Costs:** **\_\_\_\_\_\*\*\_\_**\*\*
* **Data Breach Costs:** **\_\_\_\_**\_\_\_\_\*\*
* **Regulatory Fines:** **\_\_\_\_**\_\_\_\_\*\*
* **Recovery Costs:** **\_\_\_\_\_\*\*\_\_**\*\*

**3. Reputation Management:** How could network security failures damage organizational reputation?

**4. Customer Impact:** How would network security incidents affect customer trust and business relationships?

**Completed by**: **\_\_\_\_**\_**\_\*\*** Date**: \*\*\_\_\_\_\_\_**  
**Instructor Review**: **\_\_\_\_**\_**\_\*\*** Grade**: \*\*\_\_**\*\*