Network Traffic Analysis & Threat Detection – Nmap & Wireshark Investigation

Environment: Simulated Enterprise LAN (10.168.27.0/24 Subnet)

Overview

This project involved analyzing network traffic and performing vulnerability assessment on a simulated enterprise environment. Using Nmap and Wireshark, I identified exposed services, insecure protocols, and suspicious network behavior indicative of potential attack activity.

The goal was to detect security weaknesses, analyze network anomalies, and assess the risk of exploitation in a real-world environment.

Objective

- Identify active hosts, services, and open ports
- Detect vulnerabilities in network protocols and configurations
- Analyze packet-level data for suspicious activity
- Assess potential attack vectors and security risks

Methodology

The investigation combined active scanning (Nmap) and packet analysis (Wireshark) to gain full visibility into the network.

Key steps included:

- Performed network scanning to identify hosts and services
- Enumerated open ports and mapped services to potential risks
- Captured and analyzed network traffic using Wireshark
- Investigated anomalies including unusual traffic patterns and malformed packets

Key Findings

Insecure Protocols Exposing Sensitive Data

- FTP (port 21) transmitted credentials in plaintext
- HTTP (port 80) lacked encryption for sensitive communications

Risk:

- Credentials and data vulnerable to Man-in-the-Middle (MITM) attacks
- Potential for session hijacking and unauthorized access

Critical Vulnerability – Outdated Windows Server

- Identified Windows Server 2012 system (end-of-life)
- Vulnerable to EternalBlue exploit (CVE-2017-0144)

Risk:

- Remote code execution
- Ransomware attacks (e.g., WannaCry)
- Lateral movement across the network

Network Exposure & Service Enumeration

Multiple hosts exposed services including:

- SMB (445)
- FTP (21)
- HTTP (80)
- SSH (22)

Risk:

- Expanded attack surface
- Increased likelihood of exploitation through exposed services

Suspicious Network Activity (Anomaly Detection)

1. Port Scanning Behavior

- Detected unusual TCP packets with FIN, PSH, URG flags
- Activity targeted multiple critical ports

Indicates:

- Reconnaissance activity by a potential attacker

2. Malformed DNS Queries

- Observed failed DNS PTR lookups
- Possible indication of DNS tunneling or misconfiguration

Risk:

- Data exfiltration through covert DNS channels

3. Abnormal TCP Reset (RST) Traffic

- High volume of TCP reset packets detected

Indicates:

- Possible intrusion attempts or denial-of-service behavior
- Disruption of legitimate connections

Security Impact

If left unaddressed, these vulnerabilities could result in:

- Credential theft and unauthorized access
- Data interception and exfiltration
- Remote system compromise
- Network-wide attacks through lateral movement

Recommendations

- Replace FTP with secure alternatives (SFTP / FTPS)
- Enforce HTTPS with TLS encryption
- Upgrade or patch outdated systems (eliminate SMBv1)
- Deploy IDS/IPS solutions (e.g., Snort, Suricata)
- Implement network segmentation and access controls

SOC / Detection Relevance

This project demonstrates hands-on experience in:

- Network traffic analysis and packet inspection
- Identifying vulnerabilities and attack vectors
- Detecting reconnaissance and anomalous behavior
- Correlating network activity with potential threats

In a SOC environment, this directly applies to:

- Monitoring alerts from IDS/IPS systems
- Investigating suspicious traffic patterns
- Identifying early-stage attack activity (reconnaissance)

Tools & Technologies

- Nmap / Zenmap
- Wireshark
- TCP/IP Protocol Analysis
- Vulnerability Assessment Techniques