Network Reconnaissance & SOC Automation

Automated Nmap Reporting Toolkit

Overview

This project documents the design and use of a Python-based network reconnaissance toolkit that automates Nmap scanning, parses scan output, and generates analyst-ready reports.
The goal is to standardize reconnaissance output for SOC investigations, reduce manual analysis time, and support escalation and risk assessment workflows.

Why This Project Matters to SOC Teams

- Automates repetitive reconnaissance tasks during investigations
- Produces consistent, structured outputs for analyst review
- Enables rapid identification of exposed services and attack surface
- Supports validation, escalation, and enrichment workflows
- Preserves raw evidence for follow-on analysis and correlation

Environment

- **Operating Systems:** Linux, macOS, Windows
- **Scanning Tool:** Nmap
- **Scripting Language:** Python 3.8+
- **Output Formats:** HTML, CSV, XML
- **Framework Alignment:** SOC investigation workflow

Data Collected / Artifacts

- Active host identification
- Open TCP/UDP ports

- Running services and versions
- Service banners and fingerprints
- Raw Nmap XML scan data
- Parsed HTML and CSV reports

Analysis Workflow

- Executed automated Nmap scans using predefined profiles
- Collected raw scan output in XML format
- Parsed results using a custom Python script
- Extracted ports, services, versions, and protocol data
- Generated structured HTML reports for analyst review
- Exported CSV files for tracking, comparison, and enrichment

Findings

- Identified active hosts and exposed services across target networks
- Detected SSH and HTTP services with version disclosure
- Observed additional open ports requiring further validation
- Successfully generated readable, analyst-ready HTML reports
- Produced CSV outputs suitable for SOC tooling and SIEM ingestion

Outcome

- Automated reconnaissance workflow validated
- Standardized reporting reduced manual triage effort
- Evidence preserved in multiple formats for correlation
- Output suitable for SOC escalation and documentation

Evidence

- HTML network reconnaissance report
- CSV scan summary

- Raw Nmap XML scan data

Skills Demonstrated

- Network reconnaissance and service enumeration
- Python automation for SOC workflows
- Nmap scan profiling and analysis
- Evidence handling and structured reporting
- SOC-oriented documentation and escalation readiness