



Summer 2025 Senior Design Project

Frozen Network Reporting (FNR)

Team members: Marek Ferfecky, Kevin Ocana, Anthony Torres, Elizabeth Luzardo
Instructor/Faculty: *Masoud Sadjadi* Florida International University

Problem

Networks are constantly targeted by malicious actors aiming to exploit vulnerabilities and compromise security. Vulnerabilities such as open ports, outdated software, and misconfigured services are common in many environments, which could lead to unauthorized access, data breaches, service disruptions, or even full system compromise.

Solution

To address the complexity and inaccessibility of existing network scanning tools, we developed a Network Vulnerability Scanner with a simple web interface. This tool enables users to input a target IP or domain, select specific ports, and receive scan results showing open ports, protocols, and vulnerabilities.

Requirements

Software: Python, Nmap, HTML



System Design

A Flask web app allows users to scan IPs using Nmap and then checks for known vulnerabilities via the CVE API.

It includes:

- scanner.py: Runs Nmap scans
- cve_lookup.py: Finds CVEs by service/version
- Flask + HTML: Handles input and displays results

Flow: User → Flask → Nmap → CVE API → Results
Secure, lightweight, and user-friendly.



Implementation

```
import socket
import nmap

def port_scan(target_ip, ports):
    open_ports = []
    for port in ports:
        try:
            sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
            sock.settimeout(1) # Timeout to avoid hanging
            result = sock.connect_ex((target_ip, port))
            if result == 0:
                open_ports.append(port)
            sock.close()
        except Exception as e:
            print(f"Error scanning port {port}: {e}")
    return open_ports
```

Team Timeline



Summary

This project introduces a Python-based tool that scans for and identifies basic network vulnerabilities in a user friendly web interface. Built with accessibility and clarity in mind, the scanner helps to understand network exposure in real-time