Self-Hosted Workflow Automation For AI-Based Cybersecurity Operations

By: Hareign Casaclang, Bianca Ionescu, Dr. Yoohwan Kim, and Dr. Ju-Yeon Jo

UNLV

Introduction

- Cyber tasks are repetitive and tedious.
- What's the solution? Automated workflows.
- What platform? n8n, but locally hosted.
- Why n8n? Low Code/No Code (LCNC) platform that's accessible for most any user.

Workflow Automation Tools Comparison

n8n

- Open-source, self-hostable
- External AI model(s) setup
- Free OR Paid Subscription
- Flexible

SOAR

- Purpose-built for SOCs
- Increasing AI for enrichment
- Enterprise licensing
- Scalable, compliance-ready

Power Automate

- LCNC for Microsoft ecosystem
- Azure AI, Copilot
- Enterprise bundle
- Limited custom security workflows

Opal AI

- Experimental LCNC
- Google Gemini integrated
- No standard pricing
- Accessible, but lacks governance & resilience

n8n

- Open-source, low-code/no-code platform for workflow automation
- Enables drag-and-drop creation of triggers, nodes, and AI agents
- Supports self-hosting for data control and security
- Integrates with 400+ tools and major AI models (ChatGPT, Gemini, Ollama)

Dataset

- Masscan scan from a Google Cloud VM running Debian 10
- Ran from April 26, 2021 - April 30, 2021
- **43,050,668** IPs scanned
- **64,790,266** open ports
- 9.92 GB JSON file containing:
  - IP address
  - Port Number
  - Status

kaggle

DATASET DETAILS

Port Number	Service
21	FTP
22	SSH
23	Telnet
80	HTTP
443	HTTPS
3389	Remote Desktop Protocol(RDP)
4444	Metasploit default listener
5601	Kibana
8000	HTTP Alternative

UNLV

Environment

Windows 11 Pro: 24H2

n8n: v1.109.2

Docker Engine: v28.3.3 build 980b856
Docker Compose: v2.39.2-desktop.1

Lubuntu: v25.04

VMWare Workstation Pro: v17.6.3

Large Language Models(LLMs) Used

Ollama 3.5

ChatGPT 4o-mini

Gemini 2.5-flash

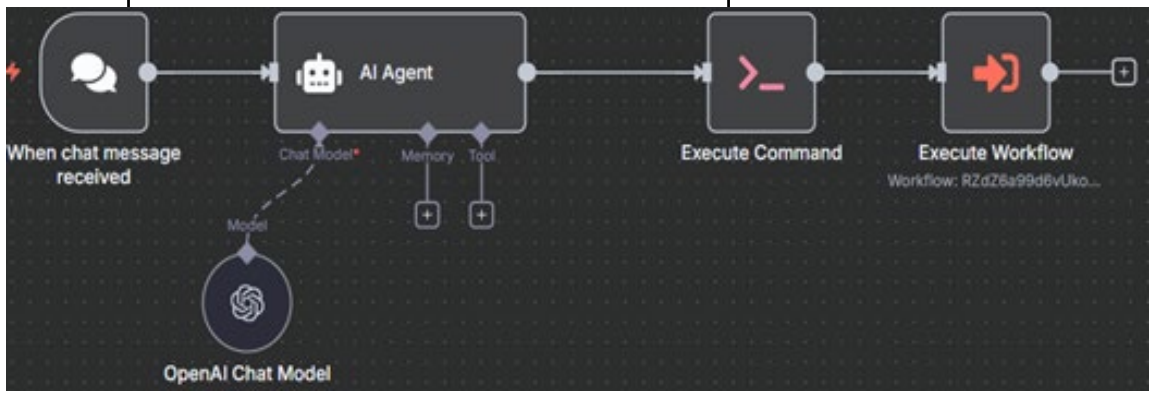
Methodology

- Compared the performance, accuracy, and practicality of using automated workflows driven by different LLMs
- Evaluation of the experiments considered three areas:
  1. Efficiency
  2. Accuracy
  3. Consistency

Nmap Creation

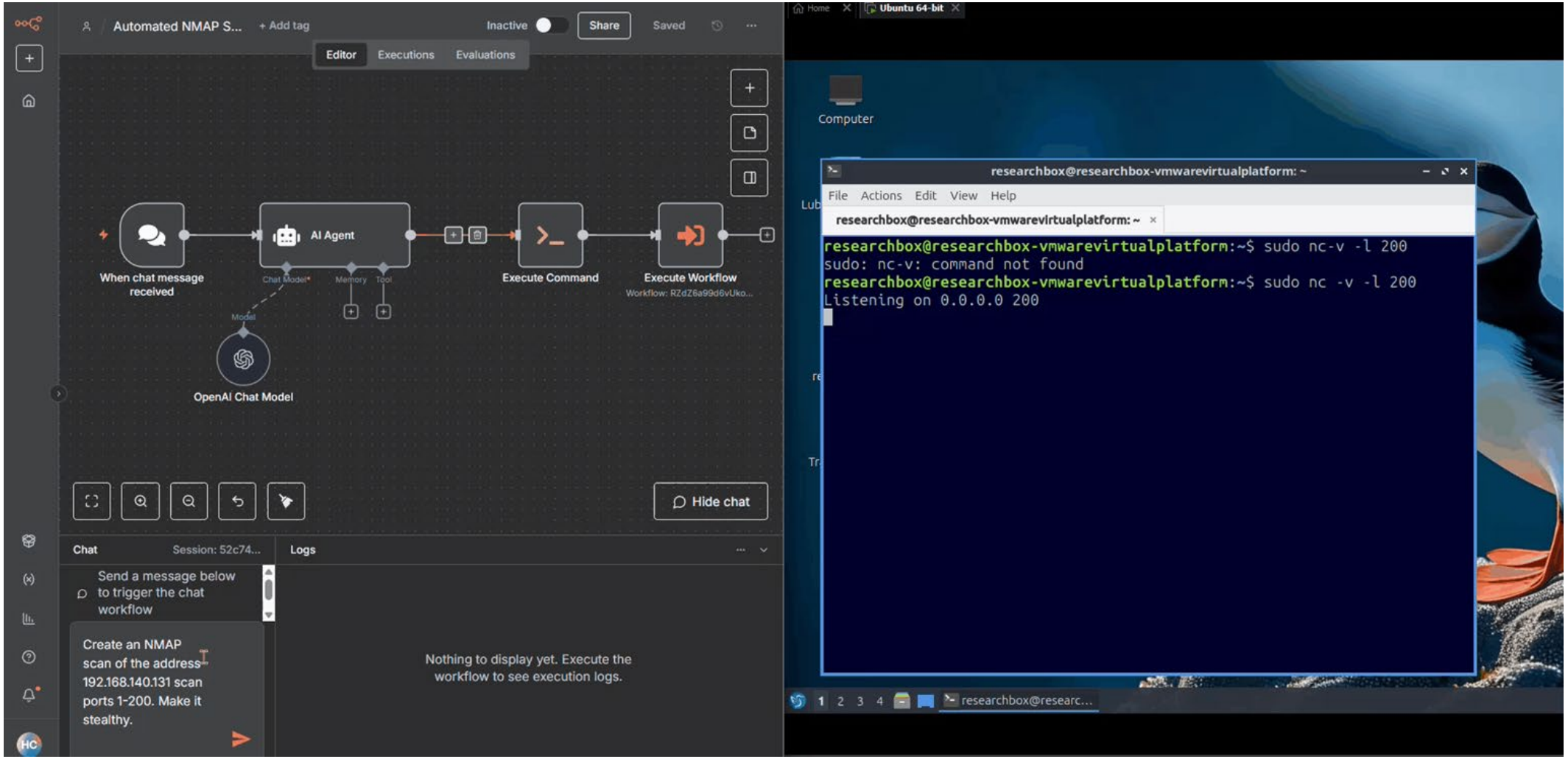
- Generates an Nmap scan from natural language with specific parameters
- Example Output:

```
nmap -sS -sV -T4 -p 1-100 example.com
```

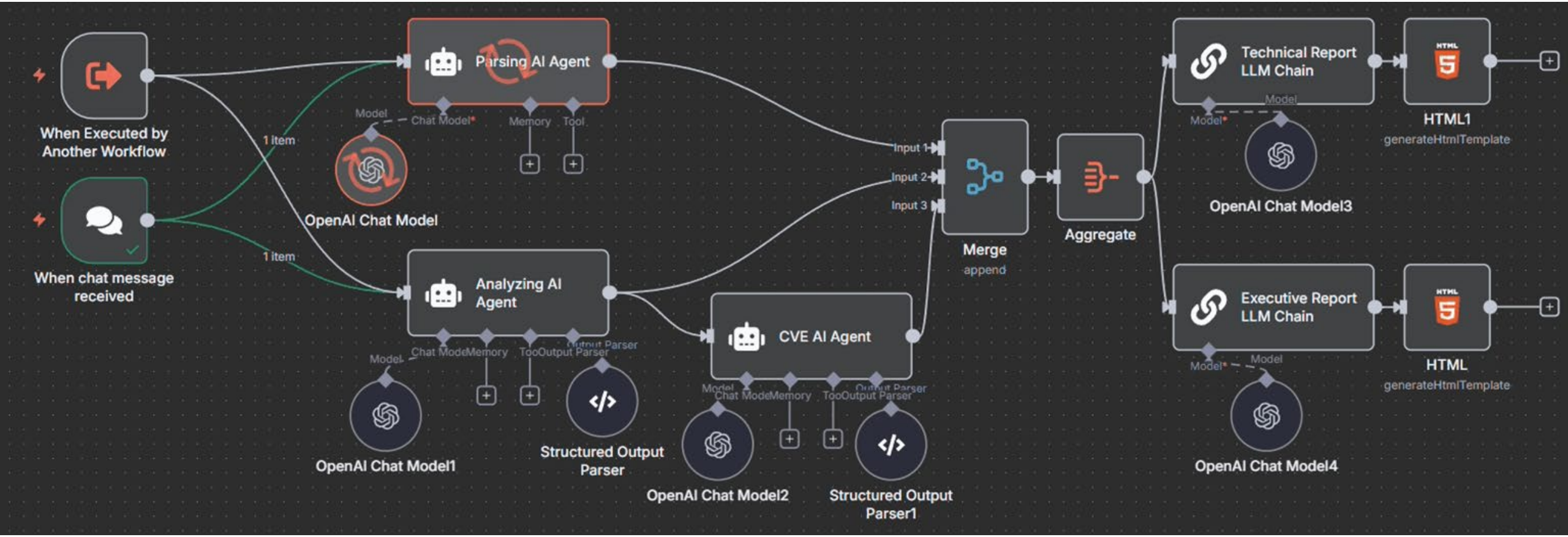


Automated Nmap Creation and Execution Workflow

Nmap Creation

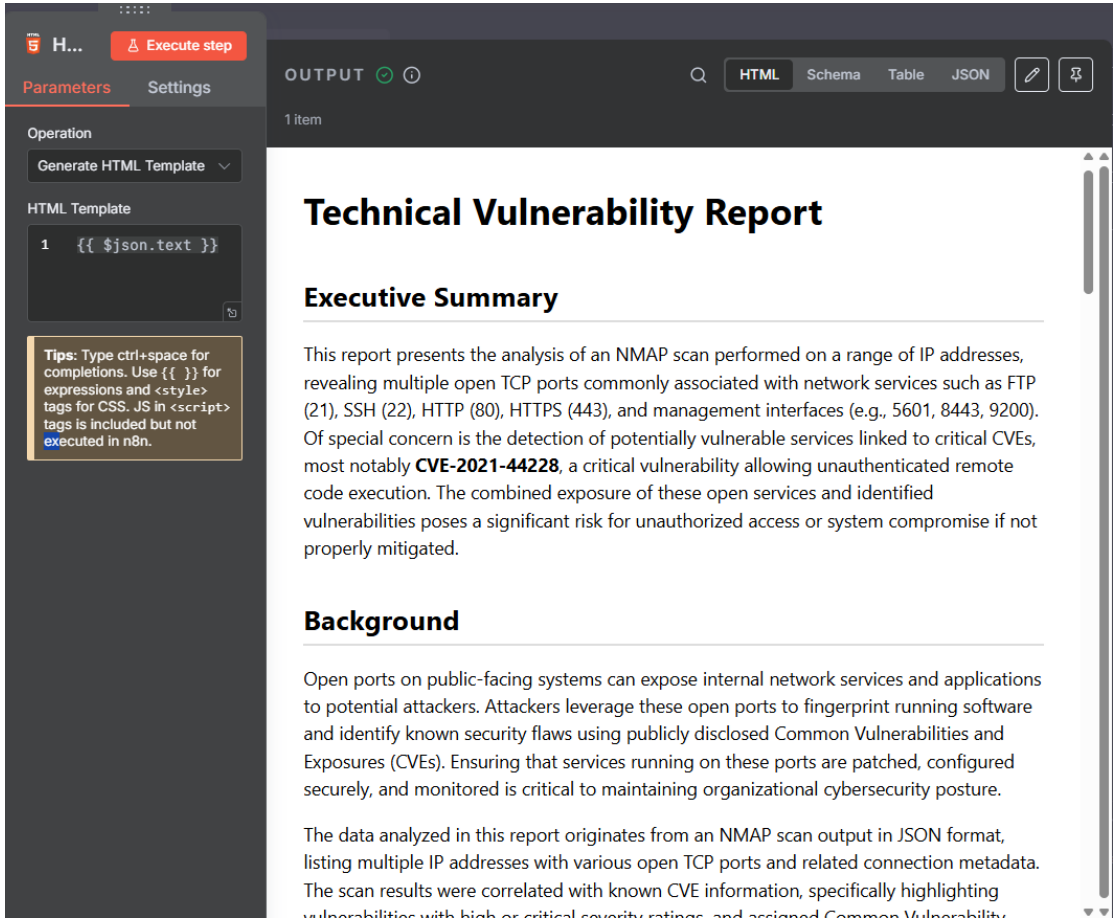


Analysis and Report Creation Workflow



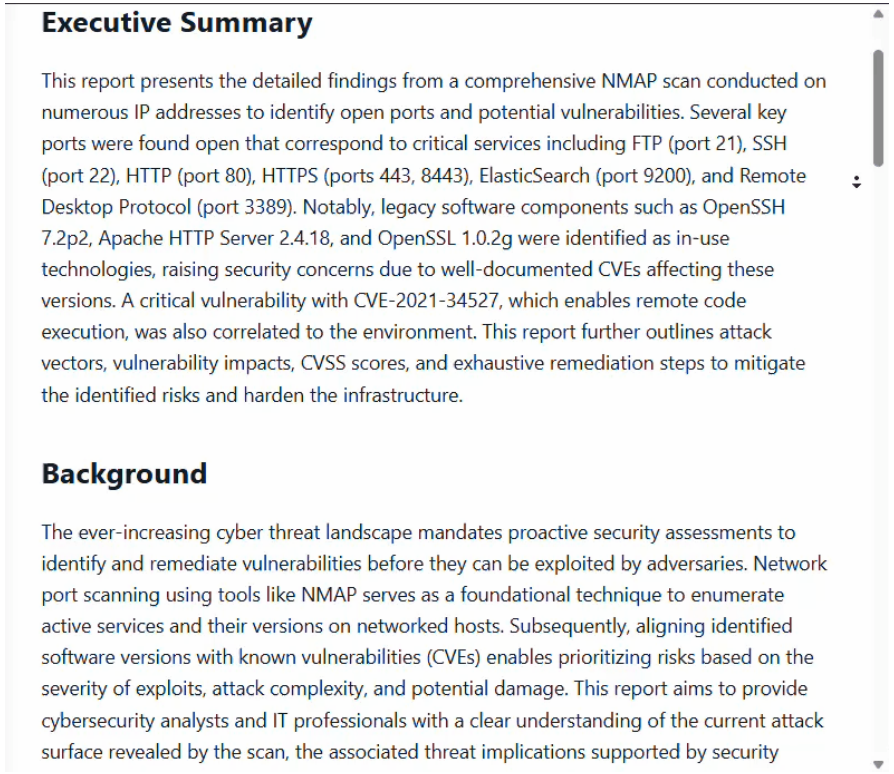
Output

- Automatically generates two reports:
  - Technical
  - Executive
- Used a consistent and standardized structure between all workflows



Automated Analysis and Report Creation Ollama Workflow

Output



Executive Summary

This report presents the detailed findings from a comprehensive NMAP scan conducted on numerous IP addresses to identify open ports and potential vulnerabilities. Several key ports were found open that correspond to critical services including FTP (port 21), SSH (port 22), HTTP (port 80), HTTPS (ports 443, 8443), ElasticSearch (port 9200), and Remote Desktop Protocol (port 3389). Notably, legacy software components such as OpenSSH 7.2p2, Apache HTTP Server 2.4.18, and OpenSSL 1.0.2g were identified as in-use technologies, raising security concerns due to well-documented CVEs affecting these versions. A critical vulnerability with CVE-2021-34527, which enables remote code execution, was also correlated to the environment. This report further outlines attack vectors, vulnerability impacts, CVSS scores, and exhaustive remediation steps to mitigate the identified risks and harden the infrastructure.

Background

The ever-increasing cyber threat landscape mandates proactive security assessments to identify and remediate vulnerabilities before they can be exploited by adversaries. Network port scanning using tools like NMAP serves as a foundational technique to enumerate active services and their versions on networked hosts. Subsequently, aligning identified software versions with known vulnerabilities (CVEs) enables prioritizing risks based on the severity of exploits, attack complexity, and potential damage. This report aims to provide cybersecurity analysts and IT professionals with a clear understanding of the current attack surface revealed by the scan, the associated threat implications supported by security

Technical Report (ChatGPT)

Cybersecurity Assessment Report

2024-06-10

Table of Contents

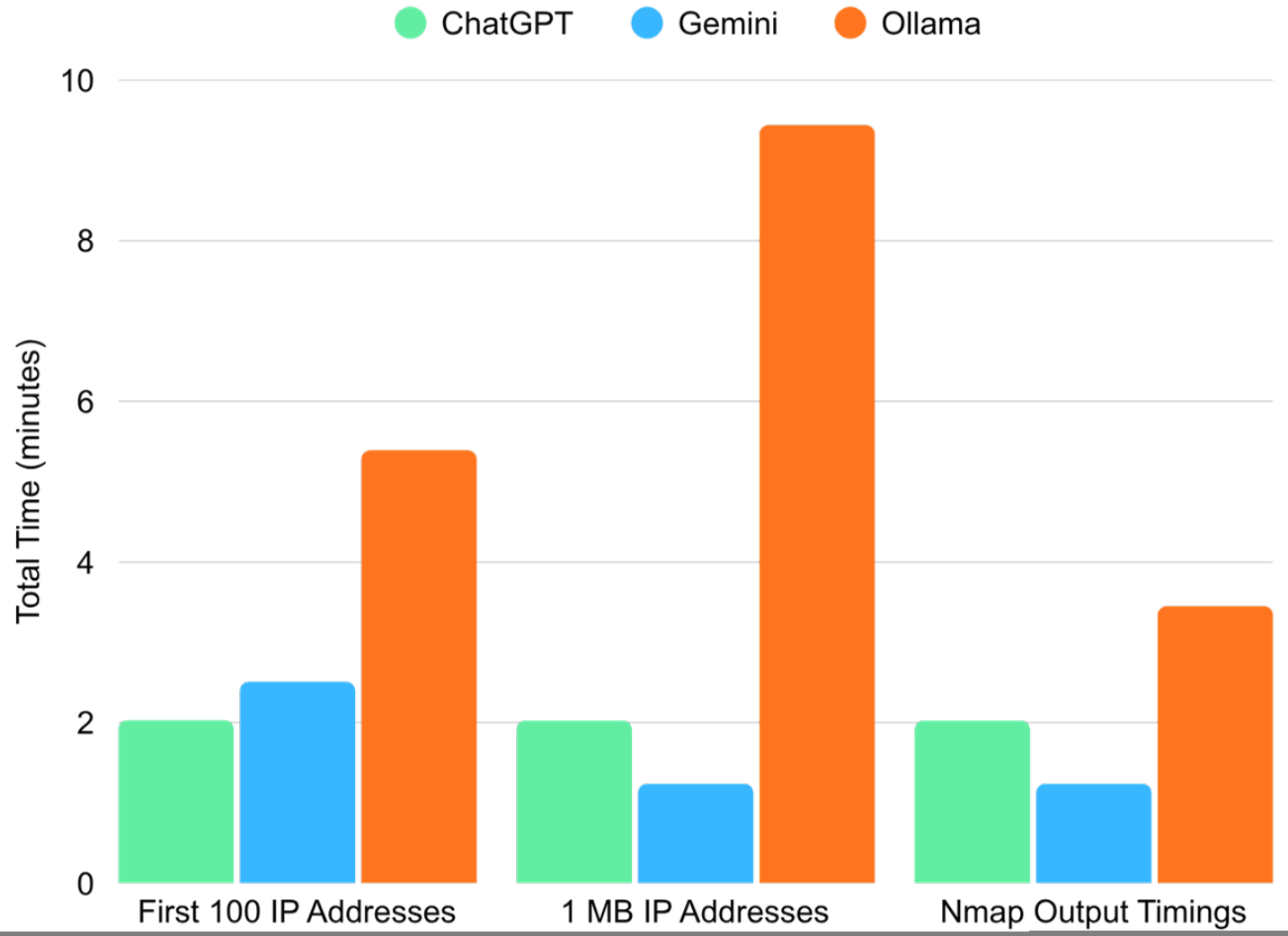
1. Executive Summary
2. Background
3. Overview of Risks
4. Affected Assets
5. Business Impact
6. Recommendations
7. Acronym List

Executive Summary

Our recent network assessment identified numerous open ports and associated services across multiple IP addresses in our environment. Critical vulnerabilities, notably CVE-2021-34527 with a CVSS score of 9.8, pose significant risks including remote code execution and privilege escalation. These weaknesses could lead to substantial

Executive Report (ChatGPT)

Timing Results



Limitations

- Steep learning curve
- AI execution failures
- API credential linking
- Restrictions in the no-cost version

Applications & Implications

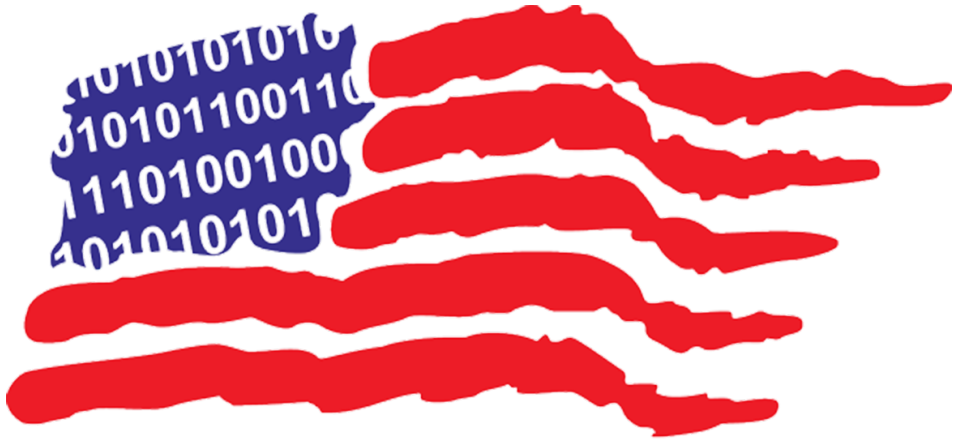
- Good for scheduling vulnerability scans, recurring log analysis, report generation, and after-action reviews
- Students can experiment and gain experience in automation
- A lightweight and open-source alternative that can fill a critical niche for smaller organizations

Conclusion

- n8n is a flexible and low-cost alternative
- Capable of integrating LLMs to automate processes
- Despite constraints, n8n remains a valuable tool for:
  - Smaller organizations
  - Academic environments
  - Automation in structured cybersecurity tasks

Acknowledgement

➢ This work supported by the National Science Foundation grant **no. 2336539**



CyberCorps®

Defending America's Cyberspace

UNLV