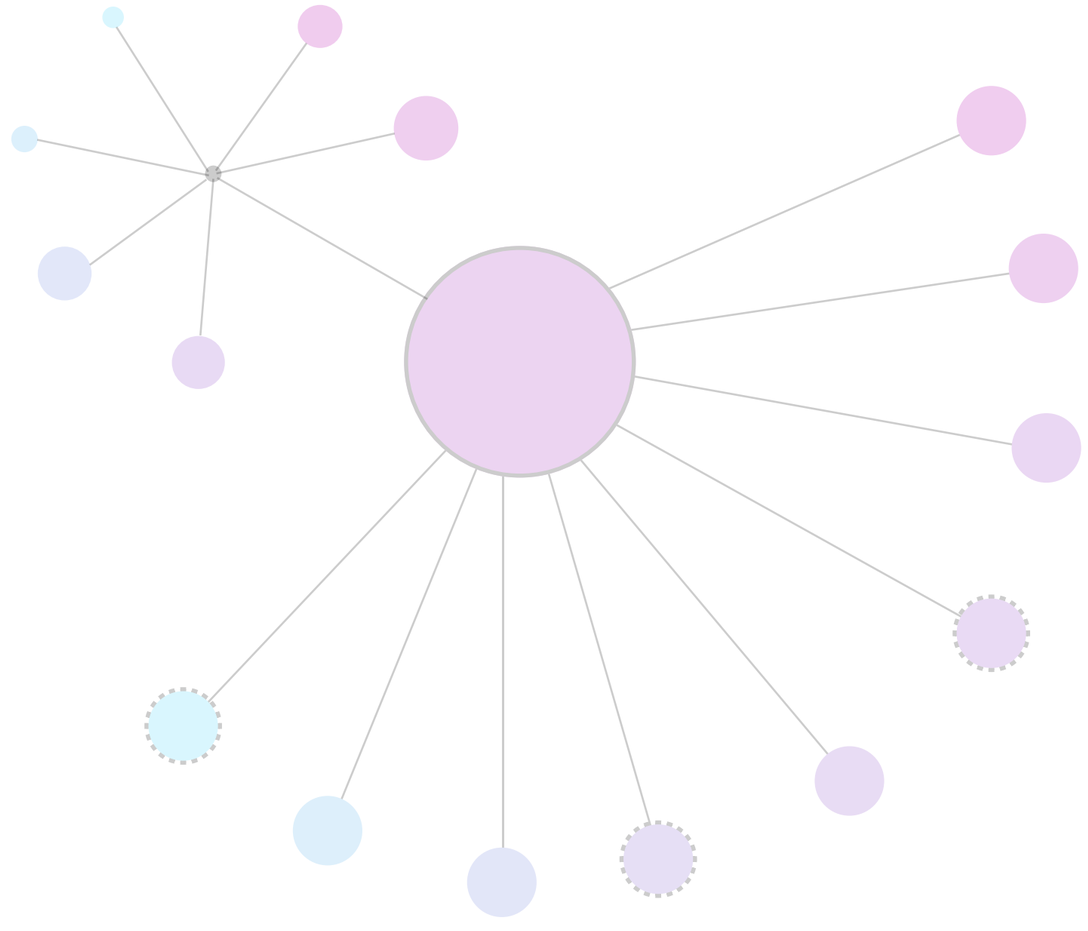
VIBE

Visual Insight for Breach Exploration (VIBE) is a tool designed to make vulnerability scans visually engaging. The goal is to help pen testers or security assessors easily identify, analyze, and prioritize targets to attack on an assessment. By using graph theory, VIBE streamlines and better portrays how pen testers work.

VIBE uses D3.js to create interactive visuals that show potential vulnerabilities and their connections in a more useful and visually appealing way. You can zoom, pan, and click on nodes to get more information about specific vulnerabilities to help prioritization. The tool uses color coding to communicate the vibe of the network's attack surface.

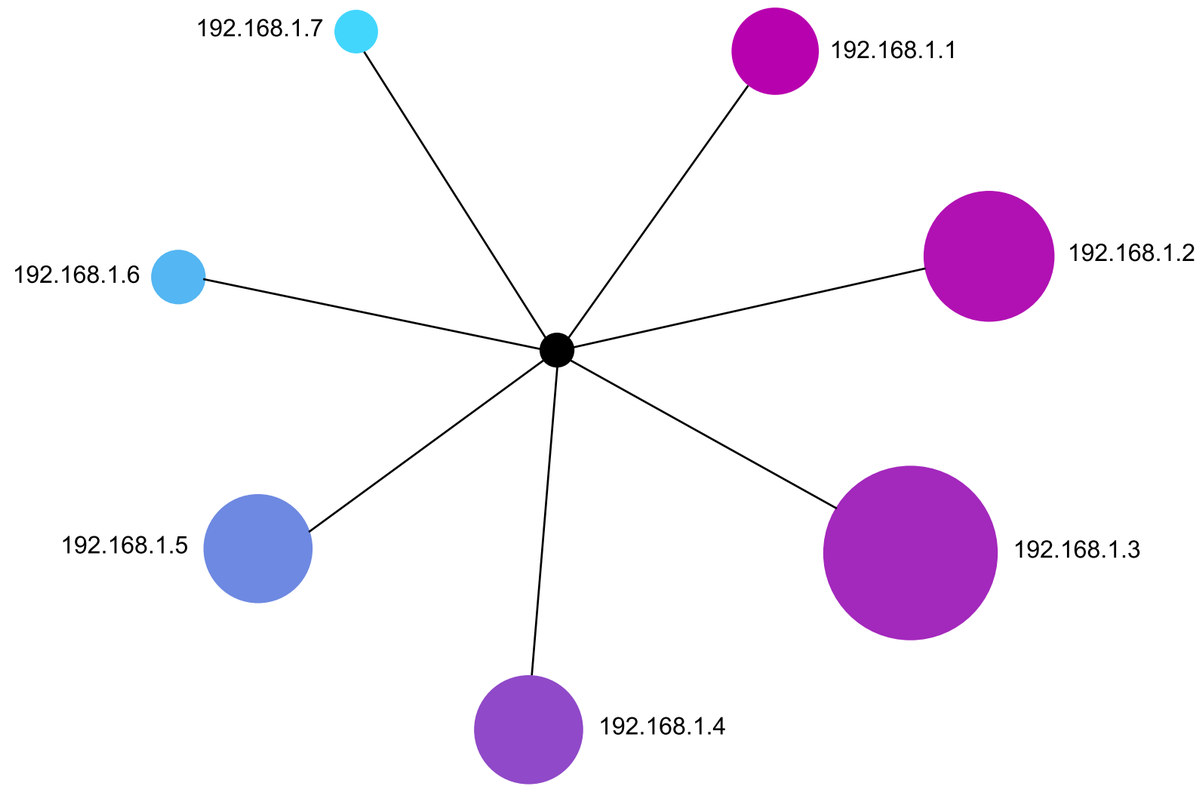
VIBE scores are done through a RAG (Retrieval-Augmented Generation) language model that calculates the VIBE check, providing context aware assessments of surface area and possible vulnerabilities. The goal is to use AI to prioritize the more vulnerable paths an attacker can take without taking itself too seriously.



Created by:
Red Teamer: Rambo Anderson-You
Visualization Developer: Amanda Anderson-You

Status: On XML initial connection

- Nodes show targets on network
- Color coded and ordered (clockwise) by VIBE score



Port Status:

Open Filtered Selected

VIBE Scale:

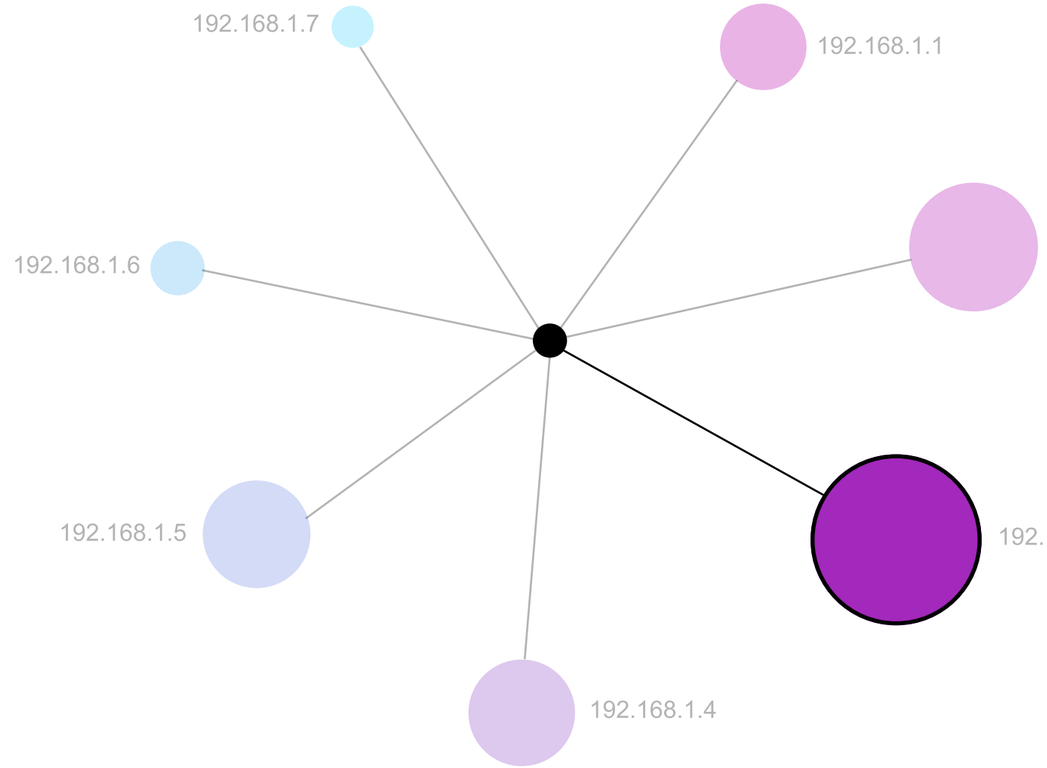
Secure Vulnerable

VIBE Rating:

Low: 🤓 Medium: 😉 High: 🥴 Critical: 😈

Status: Hover over target

- Mouse over target to have tooltip show
  - Displays vibe rating and message
- Non-selected target elements become transparent



Target address: 192.168.1.3

VIBE: 😉

The target host has a high VIBE score due to several high-severity vulnerabilities, including an outdated web server with known vulnerabilities and multiple open ports exposing sensitive services. Additionally, weak password policies and unpatched software further increase the risk of exploitation.

- **CVE-2021-3449**: The host is running an outdated version of OpenSSL, which is vulnerable to a denial-of-service attack.
- **ExploitDB ID:** 49749

- **CVE-2020-0601**: The host has an unpatched Windows CryptoAPI, making it susceptible to spoofing attacks.
- **ExploitDB ID:** 47999

Port Status:

Open Filtered Selected

VIBE Scale:

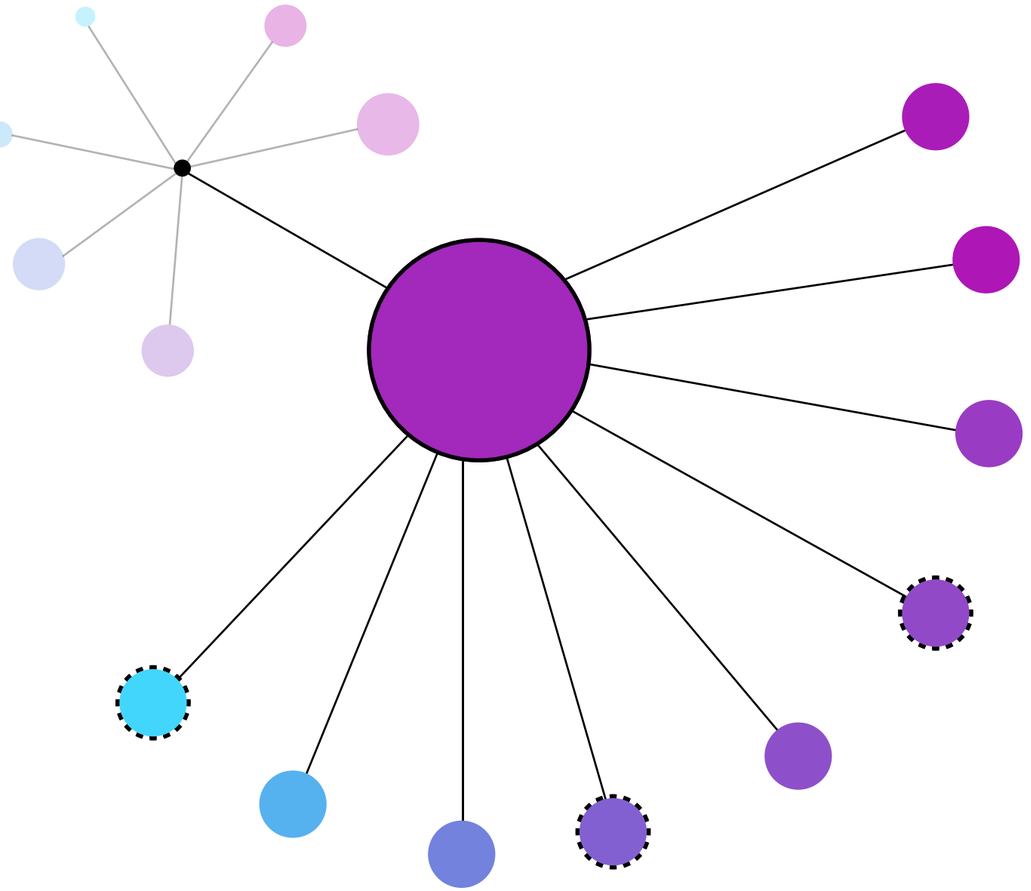
Secure — Vulnerable

VIBE Rating:

Low: 🤓 Medium: 😉 High: 😕 Critical: 😈

Status: Click on selected target

- Click on target to expand port network
  - Zooms into selected target view and remaining targets become transparent
- Ports color coded and ordered by VIBE score
- Filtered ports have dotted outline, open ports have no outline



Port Status:

Open Filtered Selected

VIBE Scale:

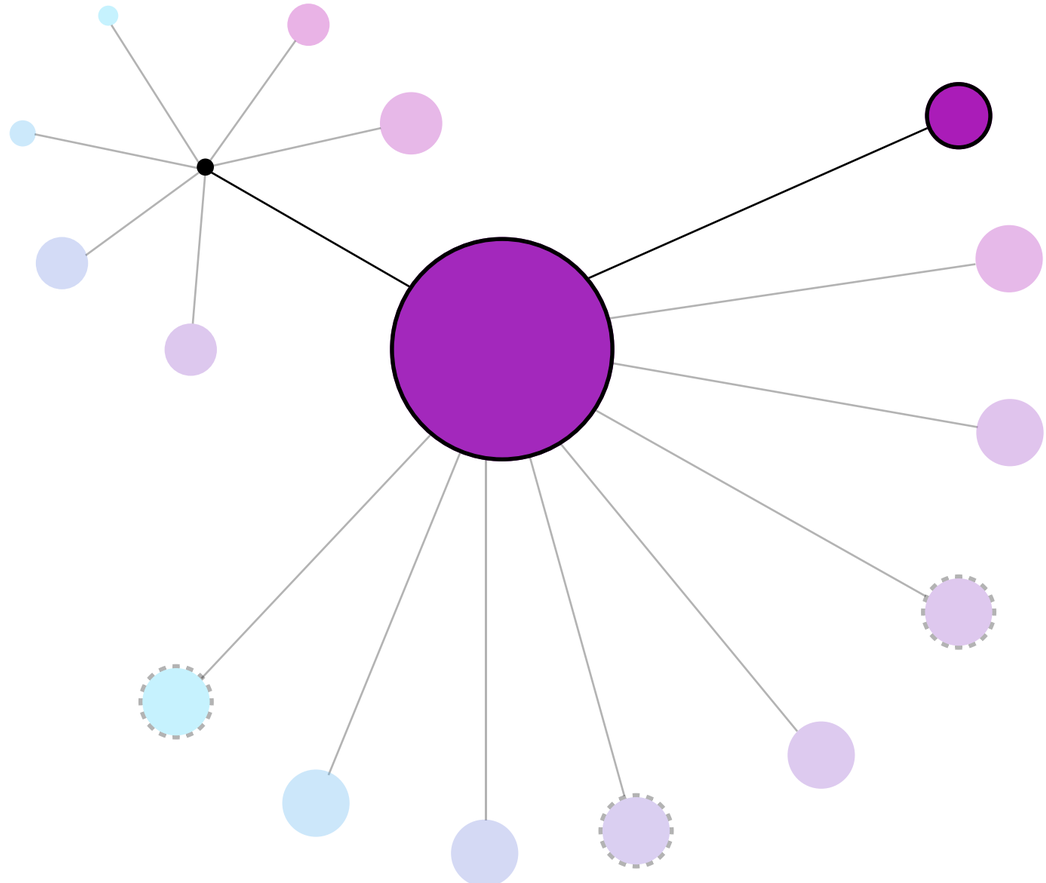
Secure Vulnerable

VIBE Rating:

Low: 🤓 Medium: 😏 High: 🥴 Critical: 😈

Status: Hover or click on port

- Click or hover on port to show port tooltip displaying VIBE score and notes
- Click again on selected port to go back to full port map



Port ID: 139 **Version:** SMBv1

VIBE: 😈

SMBv1 vulnerability exploited by WannaCry ransomware, allowing remote code execution. Affects older Windows versions and is highly dangerous.

- **CVE:** CVE-2017-0144
- **ExploitDB ID:** 42391

Port Status:

Open Filtered Selected

VIBE Scale:

Secure Vulnerable

VIBE Rating:

Low: 🤓 Medium: 😏 High: 🥴 Critical: 😈