SDEV220\_Final\_Project\_Group1

Bloodhound is a lightweight, GUI-based cybersecurity tool for ethical network reconnaissance. Built with Python and Tkinter, it features live packet sniffing, port scanning, and alert mechanisms for suspicious services — all wrapped in a hacker-style console interface.

Language: Python 3.x

Libraries:

tkinter – GUI framework

scapy – Packet sniffing

socket – Port scanning

threading – Parallel scanning/sniffing

playsound – Sound feedback

🛠️ Installation

Clone or download this repo.

Install dependencies:

pip install scapy playsound

Run the application:

python "BloodhounSDEV220Final.py"

🧪 How to Use:

\*\*\*⚠️ Note: Running packet sniffing requires admin/root privileges.\*\*\*

Start App: Launch the Python script.

Set Target: Use “Enter Target IP” to define your scan destination.

Scan Ports: Run a scan across a specified range. – This will give you information for open and closed ports

Sniff Packets: Start/stop packet capture to log live traffic. – You will be able to view live packet traffic

View Results: See console-style logs and suspicious port alerts.

Save Summary: Export protocol stats after sniffing stops.

🔐 Ethical Disclaimer

This tool is intended for educational and ethical use only. Unauthorized scanning or sniffing of networks you do not own or have explicit permission to test may violate laws and policies.

👩‍💻 Author

Project Manager: Tyler Hall

GUI/ Front-End Dev: Nelson Marte

Packet Sniffing: Juvens & Doniana

Port Scanning: Kezrae

Securrity & Documentation: Clayton and Kavon