**Spirit Bomb**

**Introduction:**

The Spirit Bomb, known as "Genki Dama" in Japanese, The Spirit Bomb involves Hero raising his hands to the sky to gather energy from all living beings and the environment, including plants, animals, and the sun. This collected energy forms a large, blue sphere above Hero's head. The Spirit Bomb is designed to harness the collective energy and spirit of all living beings, creating a massive, powerful attack. Once enough energy is gathered, Hero hurls the Spirit Bomb at his target. The technique is immensely potent and has been crucial in defeating several major villains in the series.

This tool will help us gather all the information from the frames that are moving around us. This tool is super easy to use as compare to other tools.

**Tool Functionality:**

1. Scan all the available wifi device around you.
2. Scan all the available smart devices which are connected all those wifi devices that is around you
3. Scan all the hidden devices like spy microphone, spy camera, IP cameras etc.
4. De-authentication attack
5. Capturing authentication 4-way handshake
6. Decrypting GTK

**Requirements**

Open your Terminal and enter/copy past the below command.

sudo apt update && sudo apt install -y aircrack-ng && pip install wifi pywifi scapy netifaces pycryptodome cryptography pycrypto

**Required Documents:**

After downloading this tool you will found two things in zip file. The first is the spiritbomb.sh script and the second one is OUI.txt file. You have to put both file in same directory. If don’t find any device vender name then you can download any oui file and change its name like abc\_oui.txt to oui.txt then script will automatically fetch the data from the oui file.

**Version:**

This is the v1 of SPIRIT BOMB. I will only launch its THREE version. So this is a Beta version.

**Step by Step Guide:**

**Step 1:** First of all you need to open your Linux terminal. Then you have to use write “**ifconfig**” in your terminal for checking all the available network interface like eth0,wlan etc. So, here we are going to use wlan

**Step 2**: sudo airmon-ng check kill

The command "sudo airmon-ng check kill" is used to ensure that no processes interfere with the monitoring mode setup on a wireless interface. It identifies and stops any running processes that might hinder the functionality of tools like Wireshark or aircrack-ng, which require exclusive access to the wireless interface. This command is crucial before enabling monitor mode because it prevents conflicts and ensures that the interface is clear for monitoring or capturing wireless traffic. By killing conflicting processes, it optimizes the reliability and effectiveness of monitoring activities, allowing users to perform detailed analysis and testing without interruptions.

Step 3: sudo airmon-ng start wlan0

The command "sudo airmon-ng start wlan0" initiates monitor mode on the wireless interface wlan0. Monitor mode enables the interface to capture and analyze all wireless traffic within its range, including packets not addressed to the device. This mode is essential for tasks such as network monitoring, troubleshooting, and security analysis, as it provides access to raw wireless data for tools like Wireshark or aircrack-ng. Starting monitor mode with this command allows users to conduct in-depth examinations of network activity, detect unauthorized access points, analyze protocols, and identify potential security vulnerabilities by observing all wireless transmissions within the vicinity of the interface.

Step 4: iwconfig

Use above command to make sure your desire interface is convert in monitor mode or not

Step 5: cd Download/spiritbomb

Go to the Downlaod dir and then you will find spirtbomb dir then change dir to spiritbomb. Then you will find spiritbomb and oui file there.

Step 6: sudo ./spiritbomb

The above command will start the spiritbomb tool.

Step 7: sudo airmon-ng stop wlan0mon

Use above command for converting the interface from monitor mode to manage mode

Step 8: sudo systemctl start NetworkManager

The command "sudo systemctl start NetworkManager" is used to manually start the NetworkManager service on a Linux system. NetworkManager is a daemon that manages network connections, including wired, wireless, and VPN connections. By starting this service, administrators can initiate network management functionalities, enabling automatic detection, configuration, and connection to available networks. This command is particularly useful after system boot or when troubleshooting network connectivity issues, ensuring that NetworkManager actively monitors and manages network interfaces. It facilitates seamless switching between networks, handling network settings, and maintaining connectivity stability, making it essential for efficient network administration and user connectivity on Linux platforms.

Step 9: sudo systemctl start wpa\_supplicant

The command "sudo systemctl start wpa\_supplicant" initiates the wpa\_supplicant service on a Linux system. wpa\_supplicant is essential for managing wireless connections, handling authentication, and encryption protocols like WPA and WPA2. Starting this service enables devices to establish secure connections to Wi-Fi networks, authenticate users or devices, and manage encryption keys dynamically. It ensures that wireless interfaces can scan for available networks, negotiate security parameters, and establish connections based on configured settings. This command is crucial for enabling Wi-Fi functionality, allowing devices to connect securely to wireless networks and providing essential capabilities for network access and communication in diverse environments.

**Disclaimer:**

This tool is provided for educational and informational purposes only. The developer of this tool is not responsible for any misuse or illegal use of the tool. Users are solely responsible for ensuring that their use of the tool complies with all applicable laws and regulations. By using this tool, you agree that you will not use it for any unlawful or malicious purposes. The developer disclaims all liability for any damages or consequences resulting from improper or unauthorized use of the tool.