**PROBLEM STATEMENT**

The most common form of authentication is the combination of a username and a password or passphrase. If both match values stored within a locally stored table, the user is authenticated for a connection. Password strength is a measure of the difficulty involved in guessing or breaking the password through cryptographic techniques or library-based automated testing of alternate values.

Work with an Emulator that uses information about the user to create a password list that can be used against him.

**SOLUTION**

A weak password might be very short or only use alphanumeric characters, making decryption simple. A weak password can also be one that is easily guessed by someone profiling the user, such as a birthday, nickname, address, name of a pet or relative, or a common word such as God, love, money or password.

**TECHNOLOGY USED**

CUPP:

Cupp stands for **Common User Passwords Profiler** and this tool can be used in many circumstances like license penetration tests or forensic crime investigations, CUPP is a cross-platform and written in Python and it’s functioning is simple but with very powerful results. This application is a social engineer’s best friend when it comes to creating targeted password dictionaries which are tailored to an individual.

Cupp takes vectors from the profiling done for an individual, such as their nickname, pets name, child’s birthdate, etc. It works on the principle that a password is, more often, a combination of things known to an individual. These known things are often personal details that are very close to a person’s heart.

In cases when a person might use special notations in place of alphabets (e.g.: leet can be written as 133t) Cupp has you covered.

Aircrack-ng:

Aircrack-ng is a complete suite of tools to assess WiFi network security.

It focuses on different areas of WiFi security:

* Monitoring: Packet capture and export of data to text files for further processing by third party tools
* Attacking: Replay attacks, deauthentication, fake access points and others via packet injection
* Testing: Checking WiFi cards and driver capabilities (capture and injection)
* Cracking: WEP and WPA PSK (WPA 1 and 2)

All tools are command line which allows for heavy scripting. A lot of GUIs have taken advantage of this feature. It works primarily on Linux but also Windows, macOS, FreeBSD, OpenBSD, NetBSD, as well as Solaris and even eComStation 2.

Which can be used along with CUPP to crack the victims password with the help of personalized dictionary of generated passwords and usernames.

**WORKING PROCESS**

**Optional Arguments (CUPP):**

**-i**      Interactive questions for user password profiling

**-w FILENAME**      Use this option to profile an existing dictionary,

**-l**      Download huge wordlists from a repository

**-a**      Parse default usernames and passwords directly from Alecto DB.

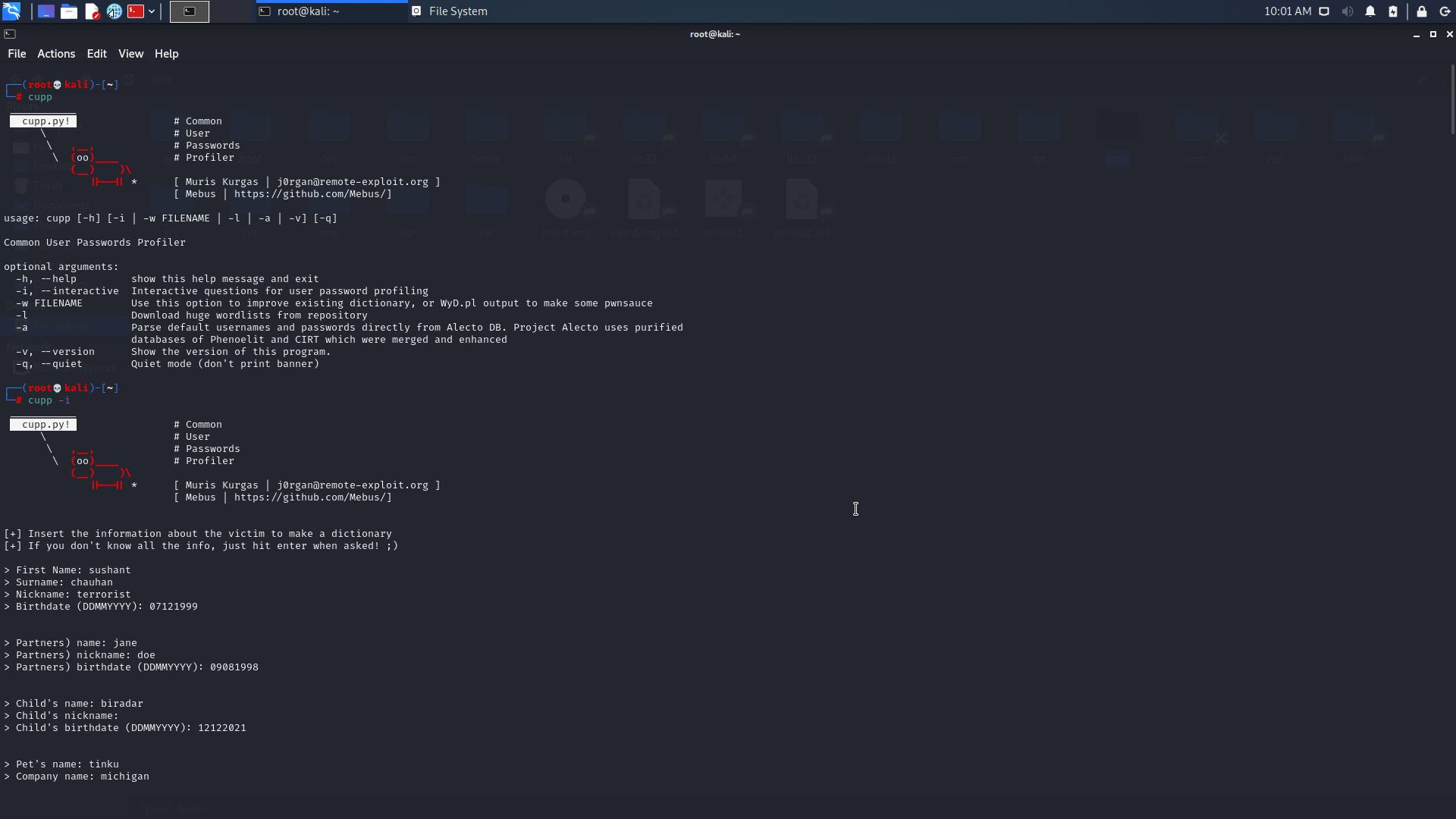
Project Alecto uses purified databases of Phenoelit and CIRT which merged and enhanced.

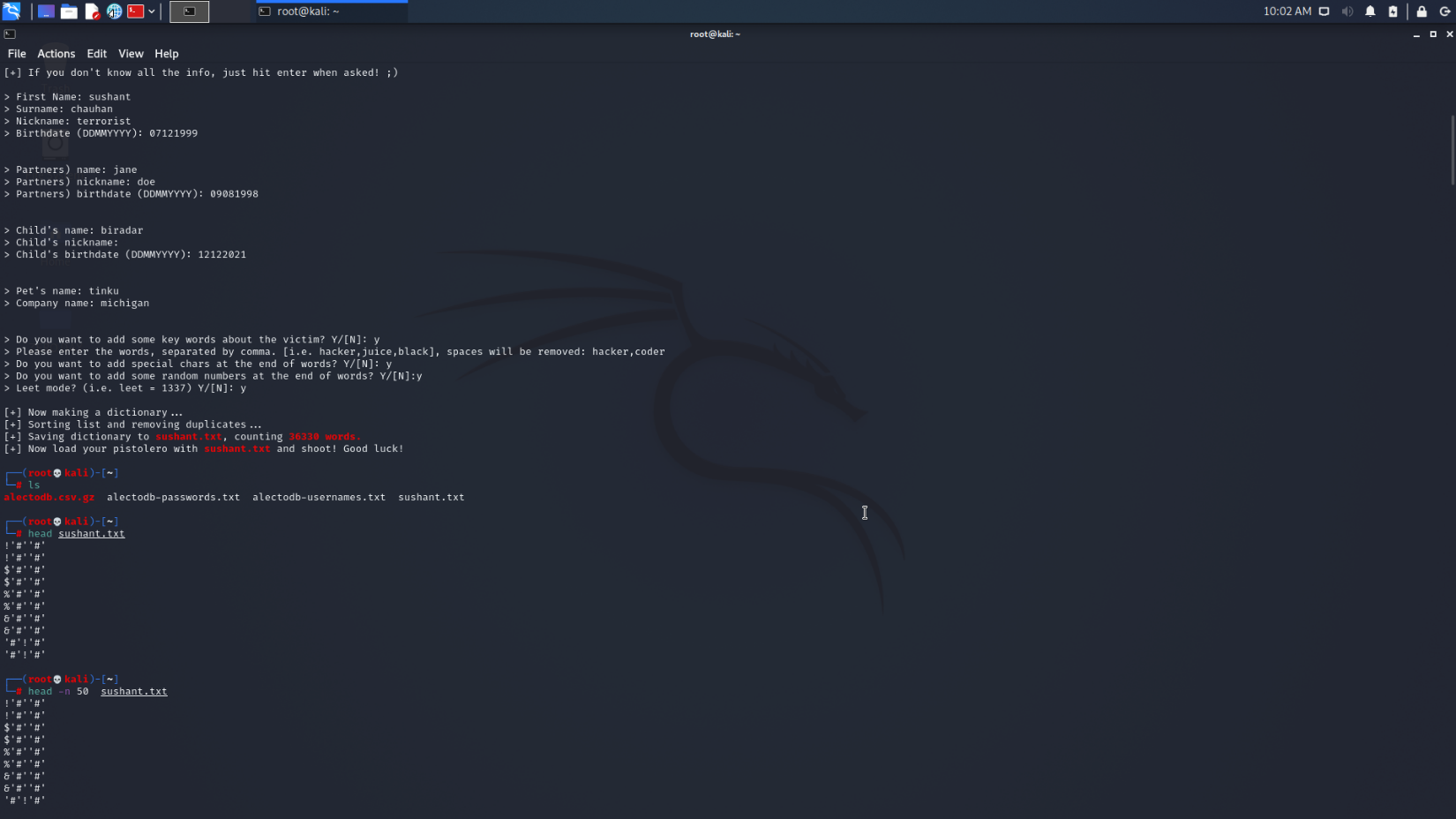
**-v**      Version of the program

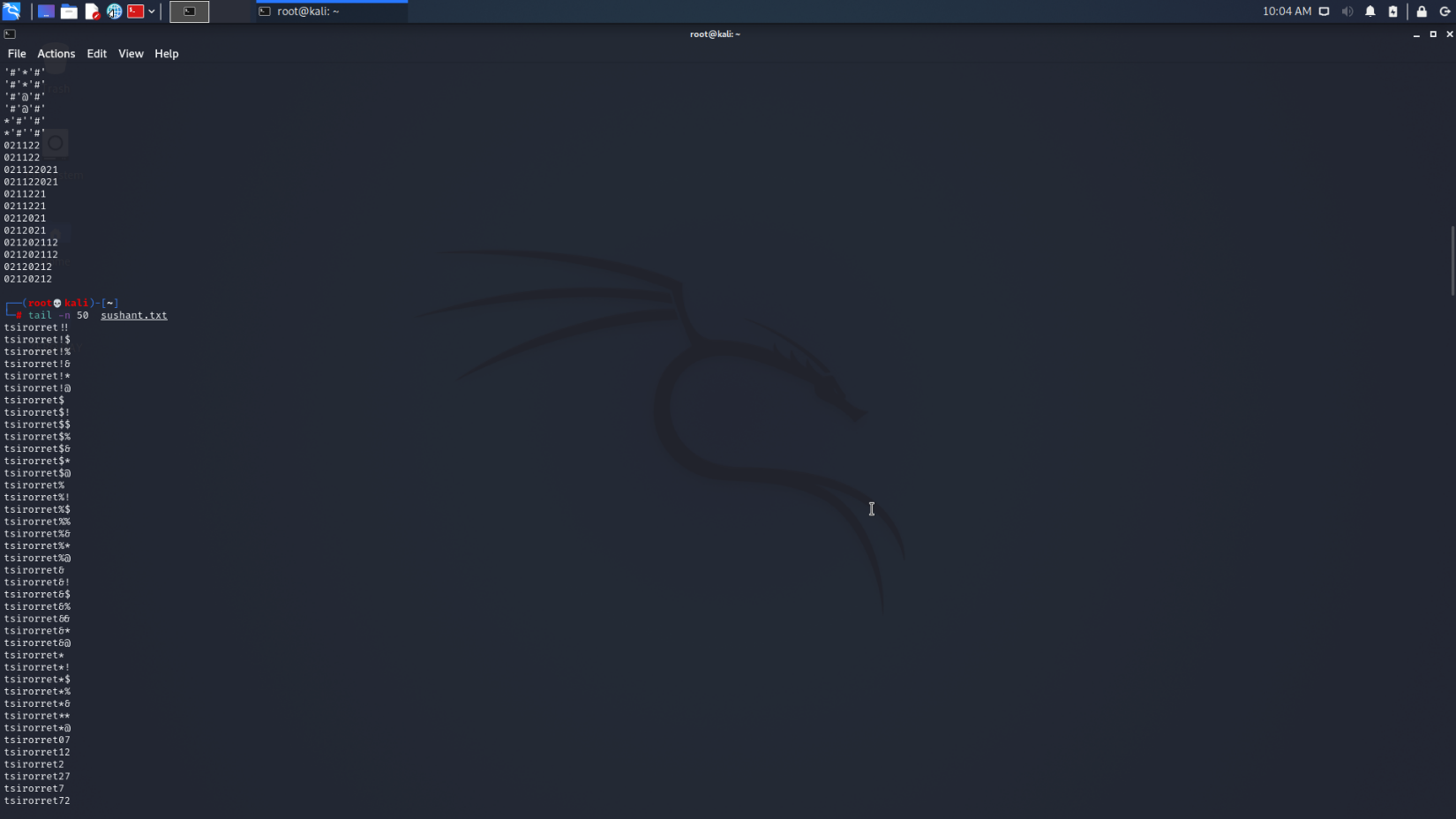
**Generating Custom Dictionary:**

We will be using the interactive option to generate the custom dictionary. You will see that we have the option to input options such **as pet’s name, child’s name, partners nickname,** etc. All these things are highly personal and very common to find these things in a password, one way or another.

There’s also an option to add any specific keywords, special characters, and random numbers. Apart from all this, there’s the option to activate Leet mode, this will make the generated dictionary extremely effective.



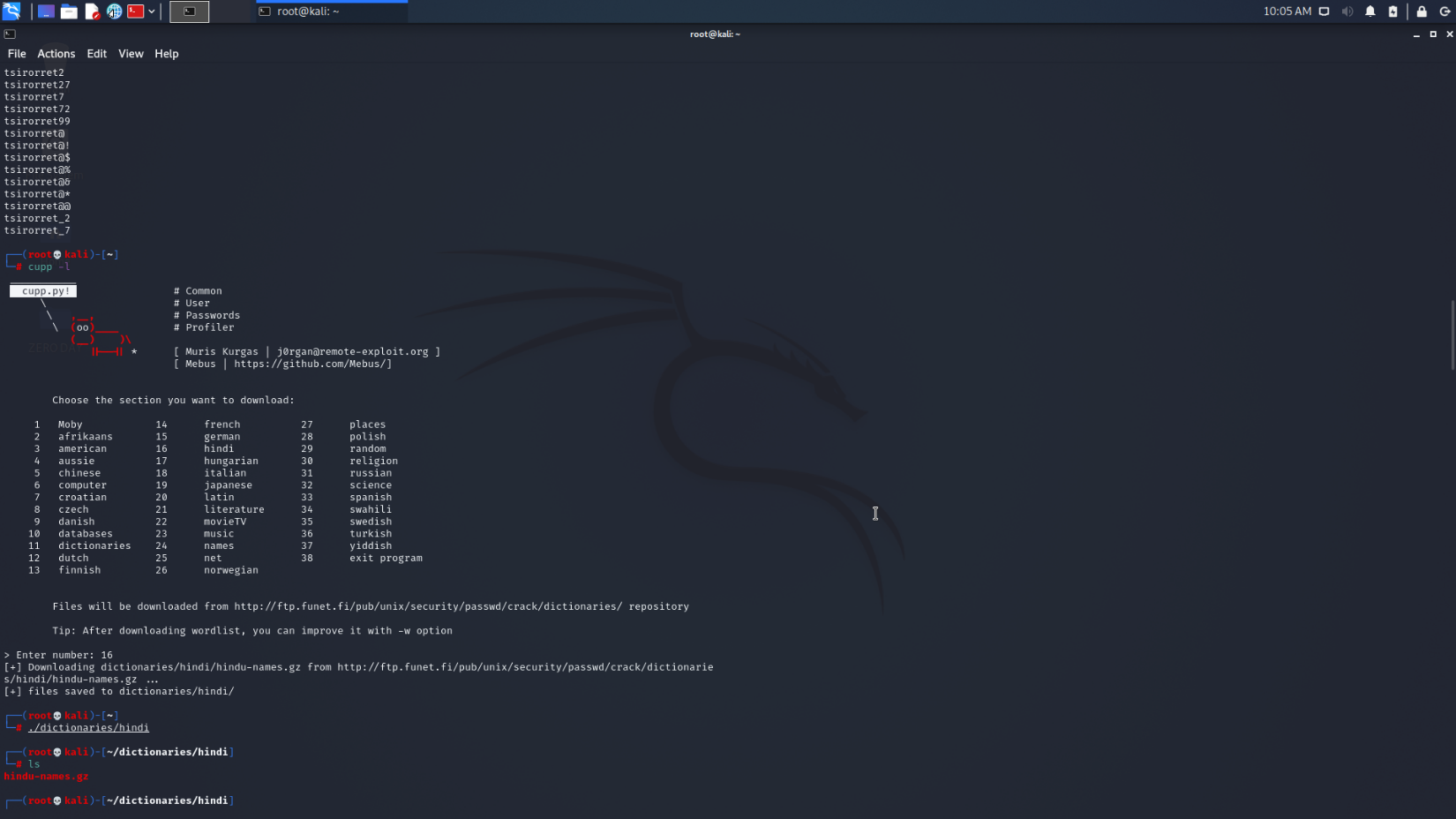




**Downloading Dictionaries from Cupp Repository:**

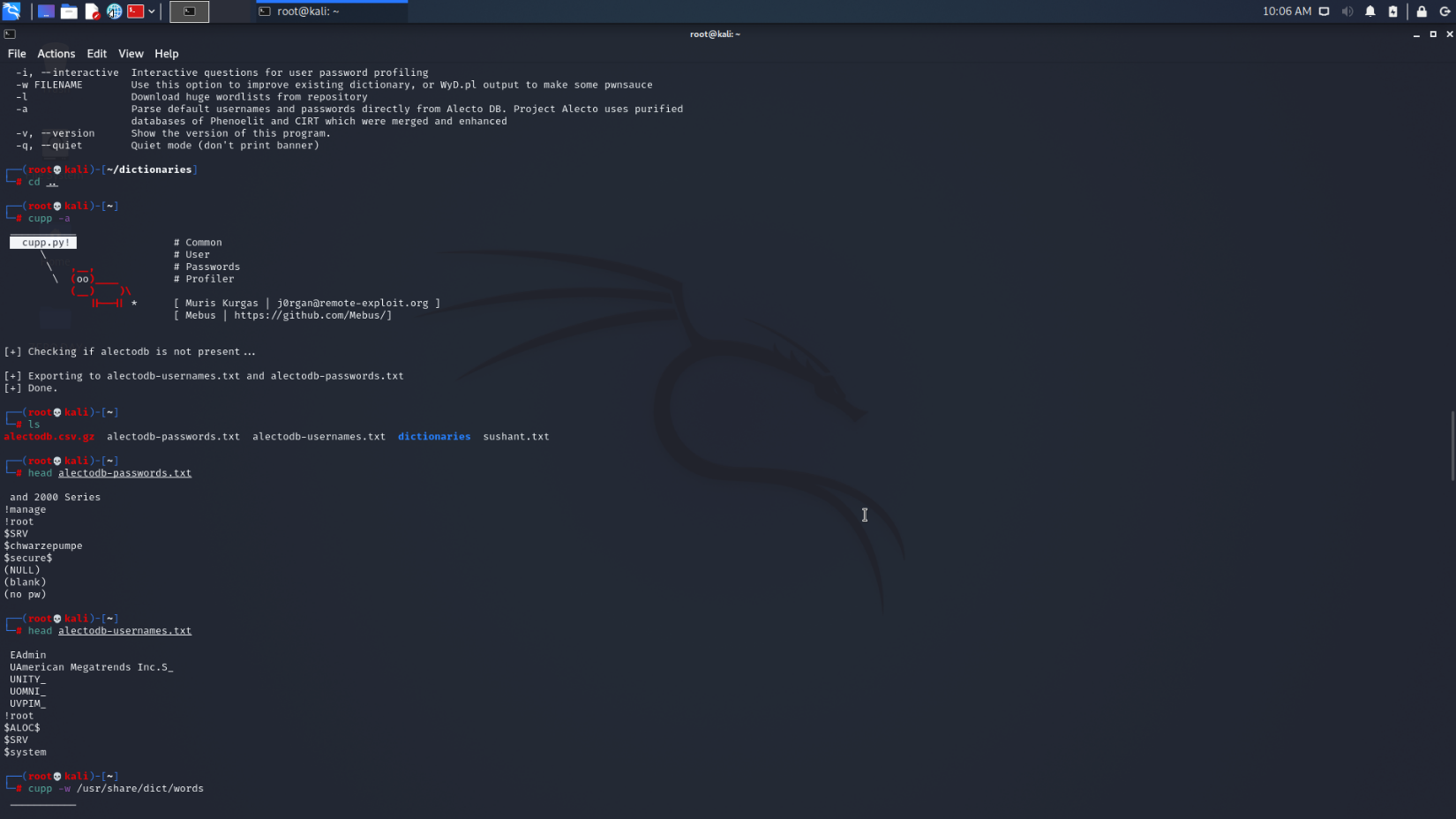
Cupp has its own repositories of dictionaries which are pre-classified. These dictionaries can be downloaded and used. The downloaded files are compressed and have to be uncompressed to be viewed.

Enter the number to choose a name to select the dictionary you want to download; we have **pressed 16** and downloaded to view a dictionary of Hindi names.



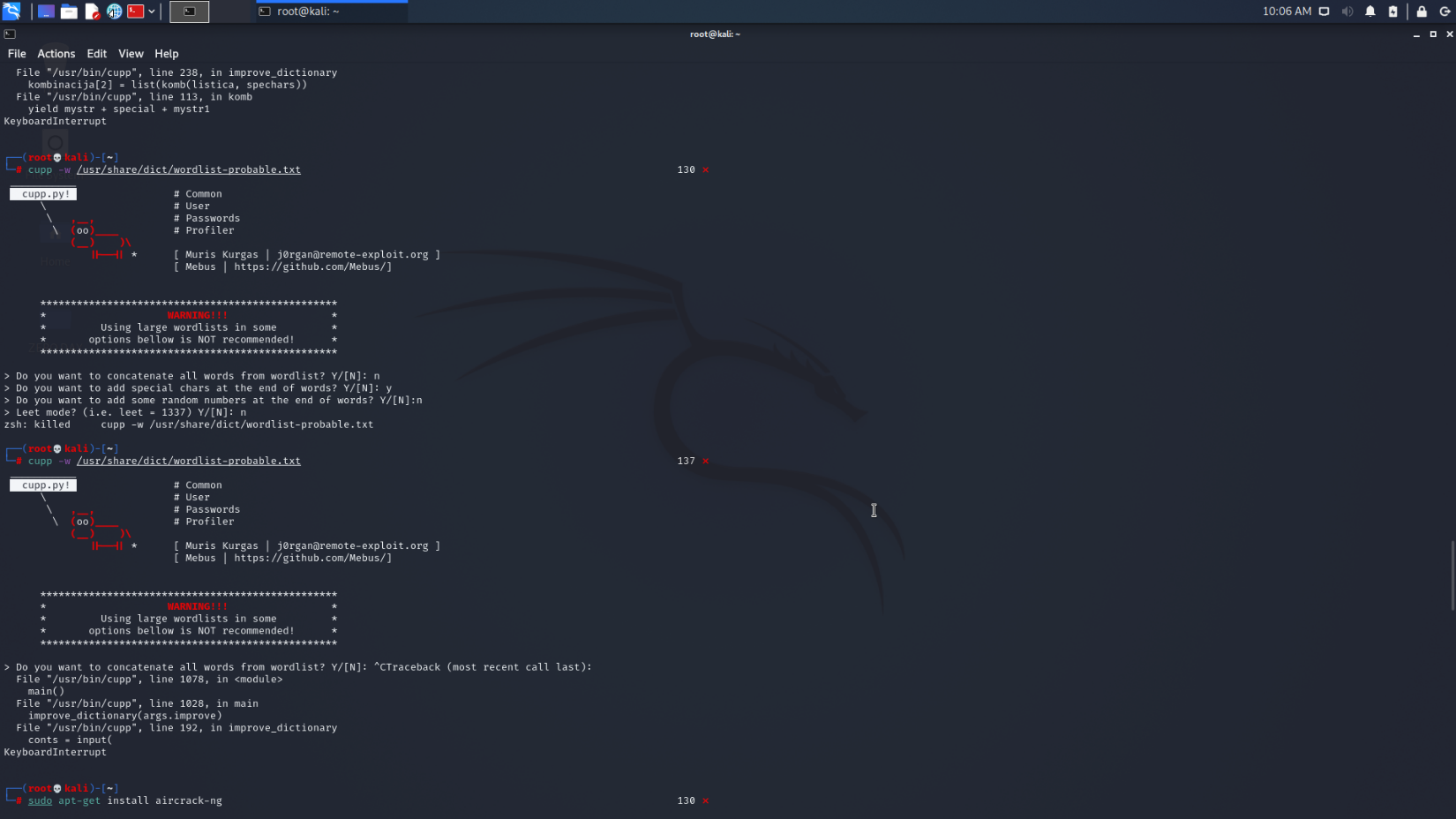
**Downloading Default Usernames and Passwords:**

Cupp can download premade dictionaries holding the most common usernames and passwords from the project Alecto database for usage.

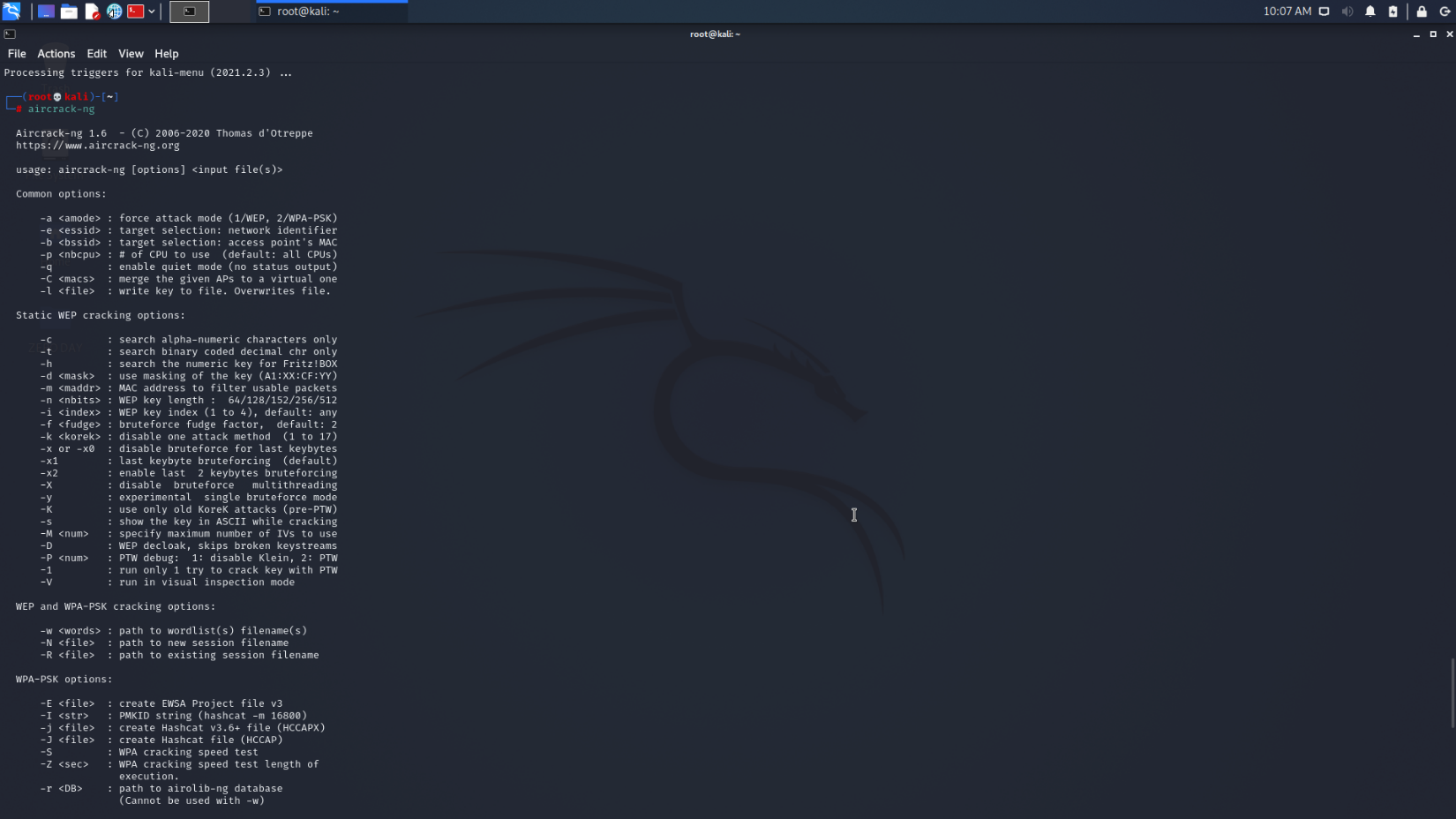


**Adding to Custom Dictionary:**

Cupp gives us the option to add more words to our created dictionary. We can customize the kind of words we would like to add by using the provided options.



**Aircrack-ng:**



**Quiet Mode:**

Quiet mode is for running Cupp in a more hush-hush way. If you’re the kind of person who does not want a big banner on their screen showing everyone what you’re doing, you’ll like this option. This basically makes for a cleaner screen while cupp is carrying out the commands you’re giving it, without the funny cow popping up on top.

**cupp -a -q**

**GitHub Link:** <https://github.com/vishalpoonacha/Zero-Day-Cybersec.git>

**Video Link:** [**https://drive.google.com/drive/folders/1RpUJiPt-\_VbGknrx-jw0HoPsyv2WFI6l?usp=sharing**](https://drive.google.com/drive/folders/1RpUJiPt-_VbGknrx-jw0HoPsyv2WFI6l?usp=sharing)