**NAME-KOYEL GHOSH**

**PROJECT-1~~~~SYSTEM HACKING**

PASSWORD ATTACK

* **ABSTRACT**

Passwords play an important role in our daily life style. We use it in many fields such as like ATM machines, desktop/mobile phones, login different internet web browser etc. In this project we are going to observe about different methods of password cracking like Hydra, auxiliary module, NSE Scripts, John the ripper, Crunch.

* **OBJECTIVE**

The main object of this project that to generate a password. If anyone has forgotten the password, they can follow this way to get their passwords. It is utilized to increase the access to digital evidence like who are involved in System administrator priviledges they can access that .

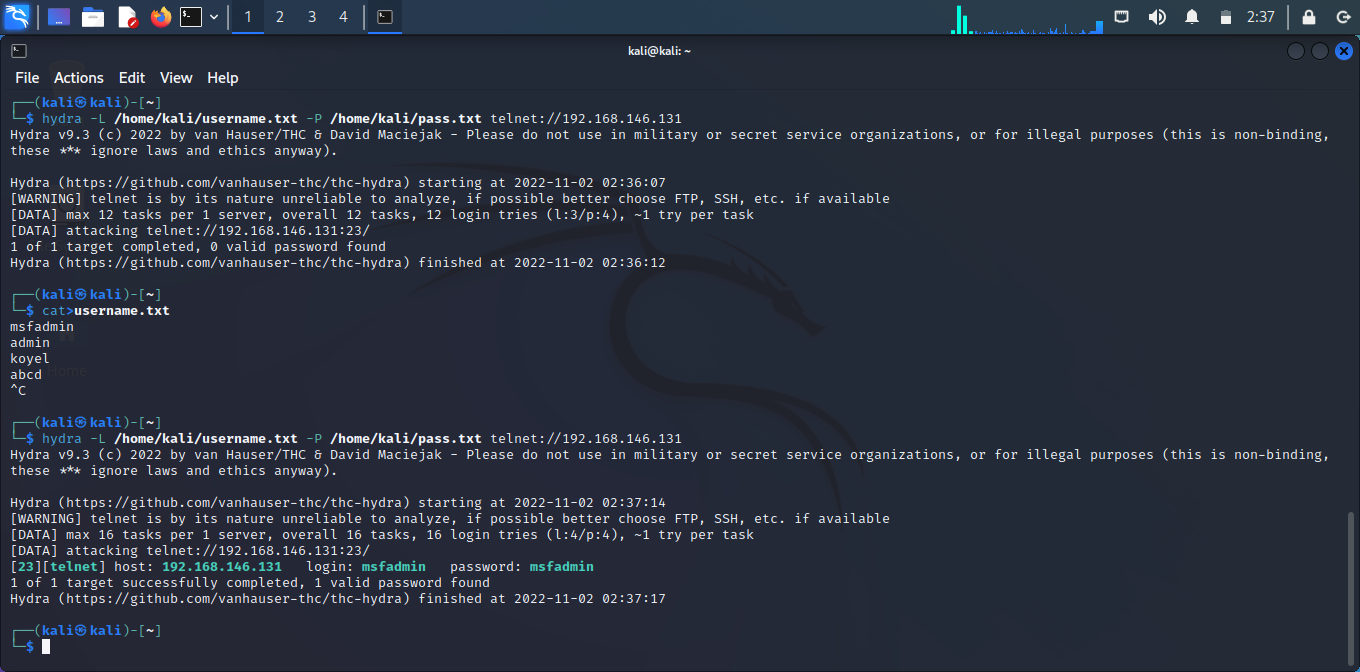
* **INTRODUCTION**

Password attacks involve exploiting a broken authorization vulnerability in the system combined with automatic password attack tools that speed up the guessing and cracking passwords. The username-password combination is one of the oldest known account authentication techniques, so adversaries have had time to craft multiple methods of obtaining guessable passwords. Password attacks have far-reaching consequences since malicious users only require unauthorized access to a single privileged account or a few users accounts to compromise the web application.

* **METHODOLOGY**

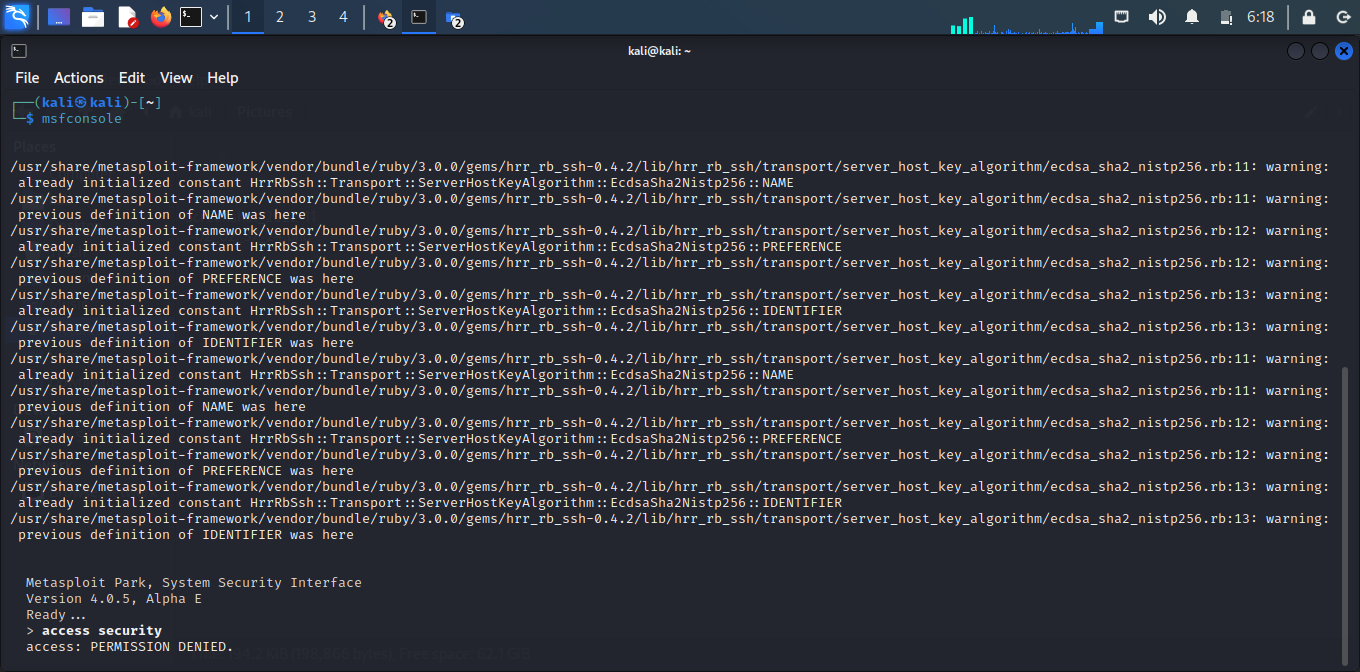
1. **Hydra**

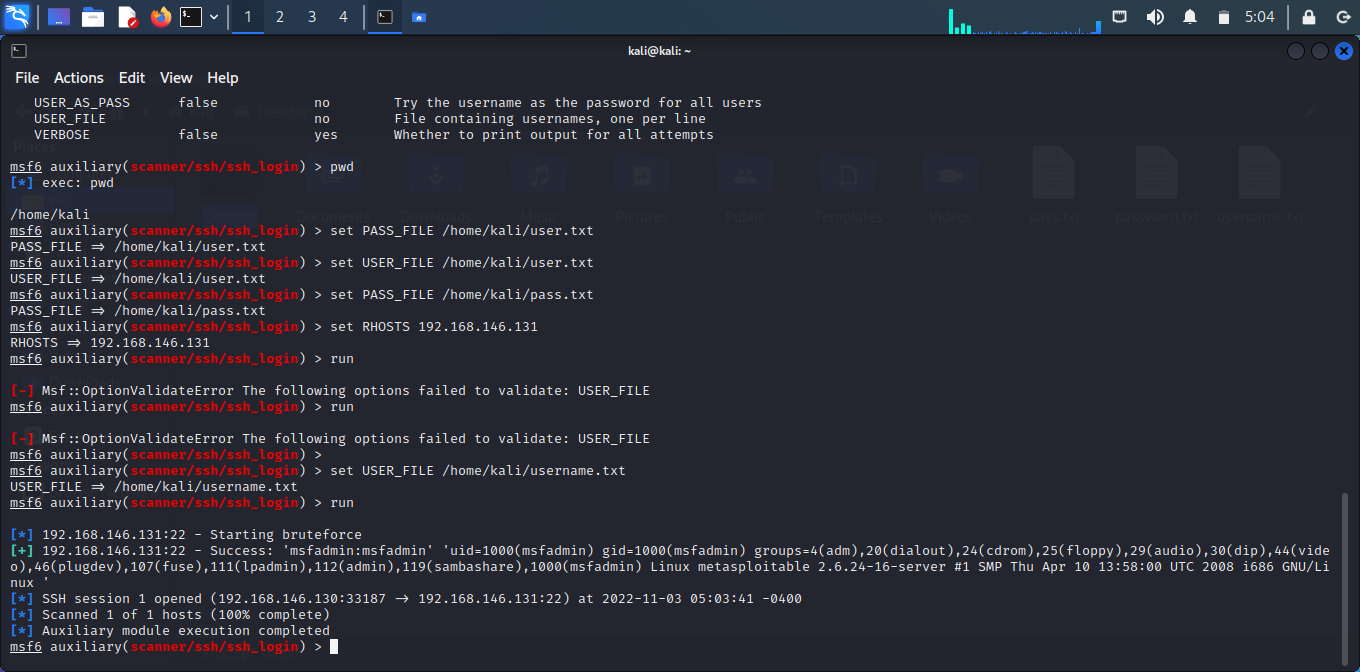
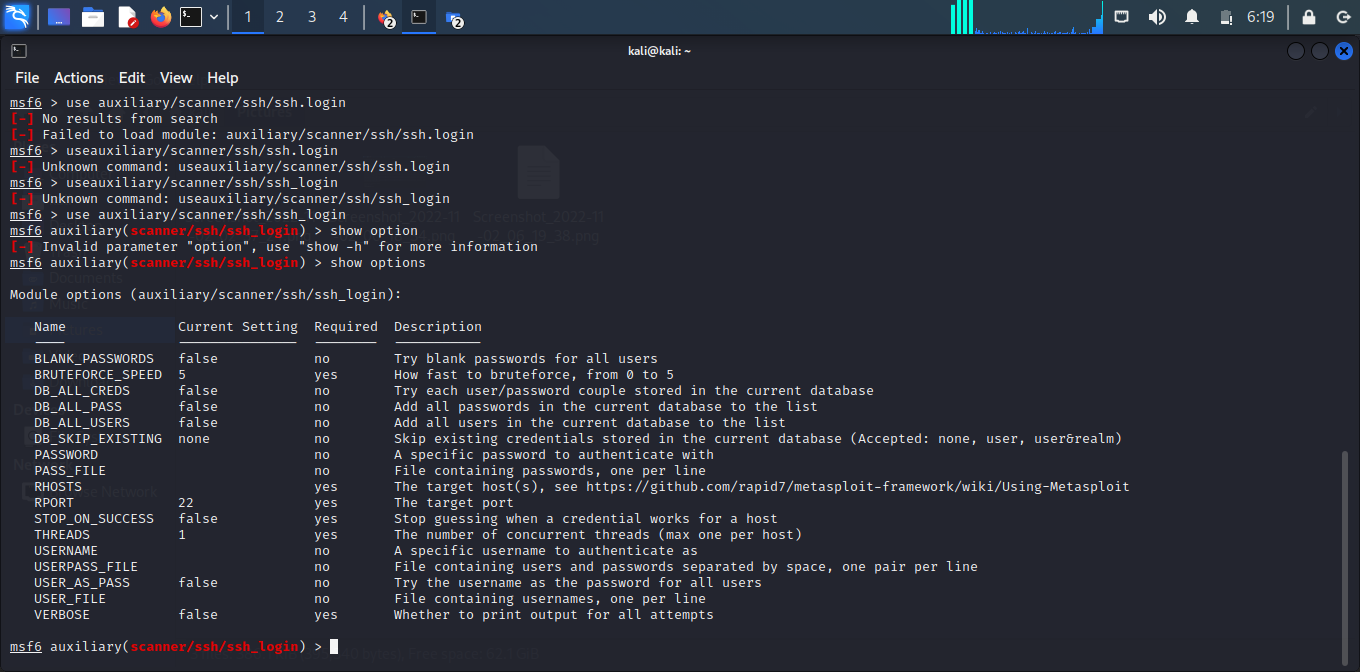
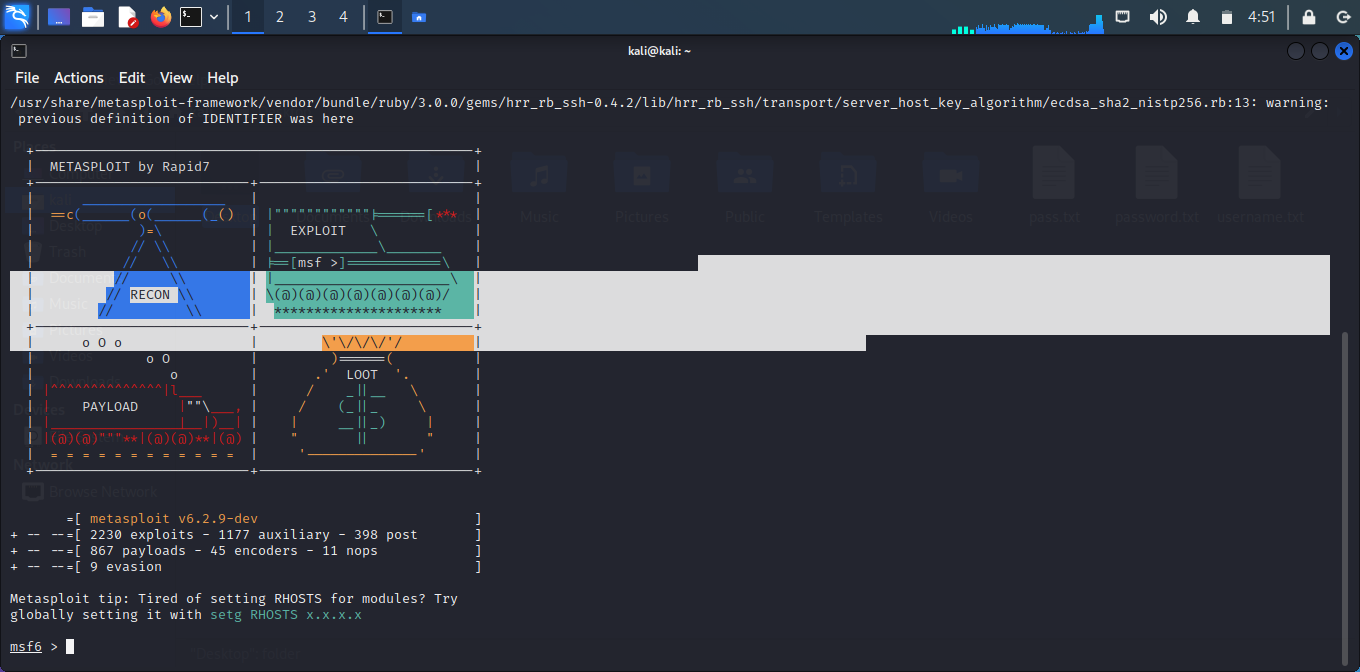
Hydra is a parallelized password attack system type cracker which is used to built in different Operating System . It works by using different approaches to perform brute-force attacks in order to guess the right username and password combination



**2. Auxiliary Module**

After scanning the Metasploitable machine with NMAP, we know what services are running on it. The services are FTP, SSH, mysql, http, and Telnet. To perform a brute-force attack on these services, we will use **auxiliaries** of each service. Auxiliaries are small scripts used in Metasploit which don’t create a shell in the victim machine; they just provide access to the machine if the brute-force attack is successful. Let’s see how to use auxiliaries. Here, we have created a dictionary list at the root of Kali distribution machine

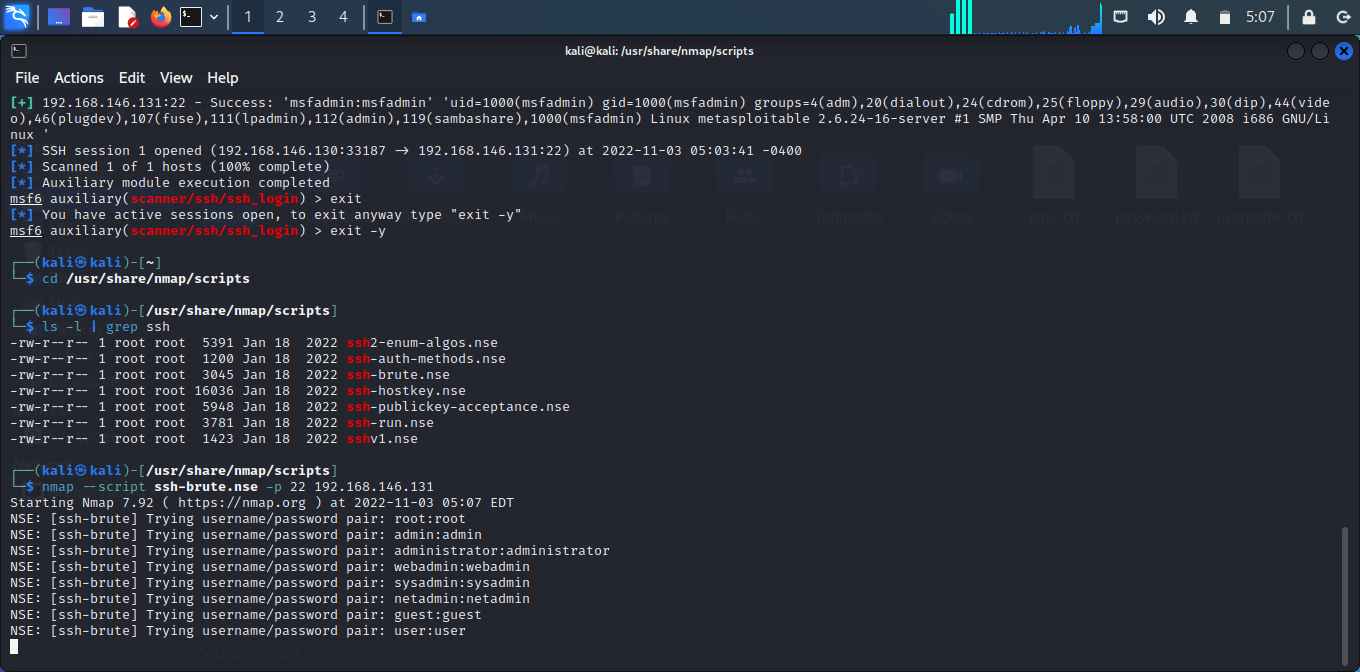




**3. NSE Scripts**

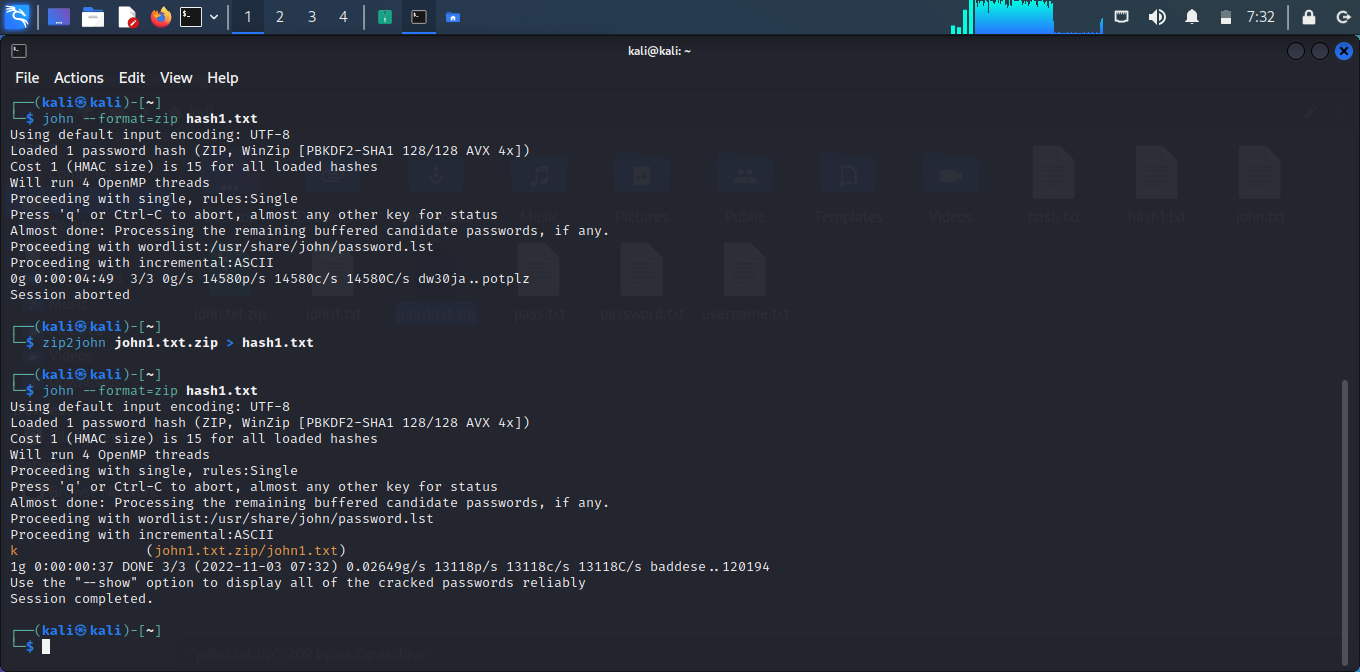
We will process the showcase for Nmap Brute NSE Script for dictionary attack in this article since Nmap is such a large tool that it can’t be covered in one post. If you’re wondering whether or not a brute-force assault using Nmap is doable.Performs brute force password auditing against http basic, digest and ntlm authentication.

This script uses the unpwdb and brute libraries to perform password guessing. Any successful guesses are stored in the nmap registry, using the creds library, for other scripts to use.



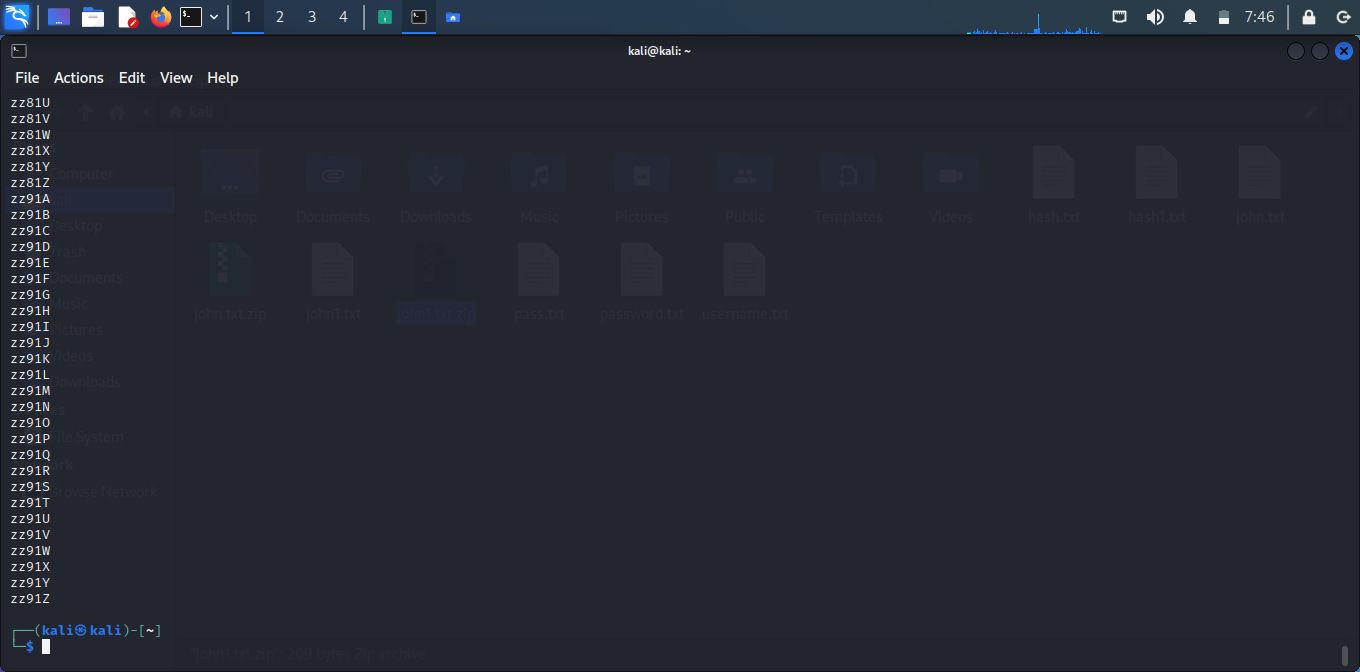
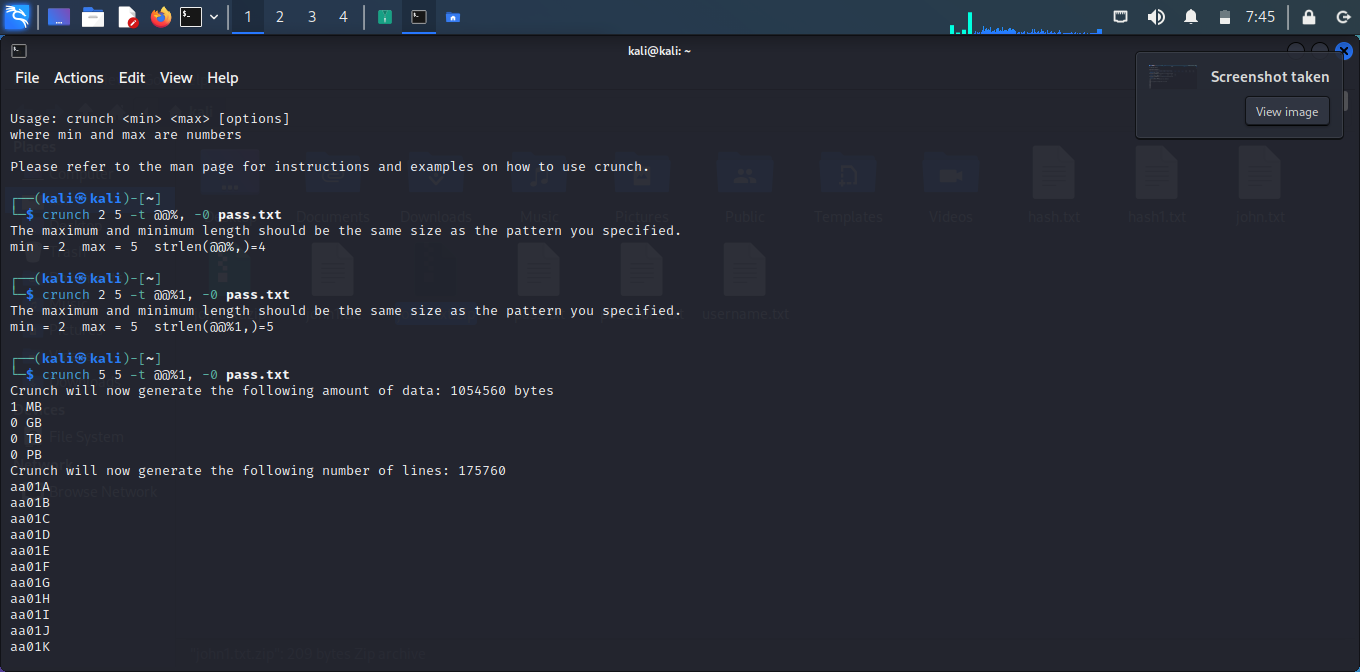
**4. John the ripper**

John the Ripper uses a combination of brute force attacks and dictionary attacks to crack passwords. First, however, penetration testers can use the single-crack mode to determine a password based on other factors in the credential file, like username or the users’ full name. Then, it runs through other common passwords on its wordlist. If neither of those methods works, it moves onto the brute force and dictionary attack options.



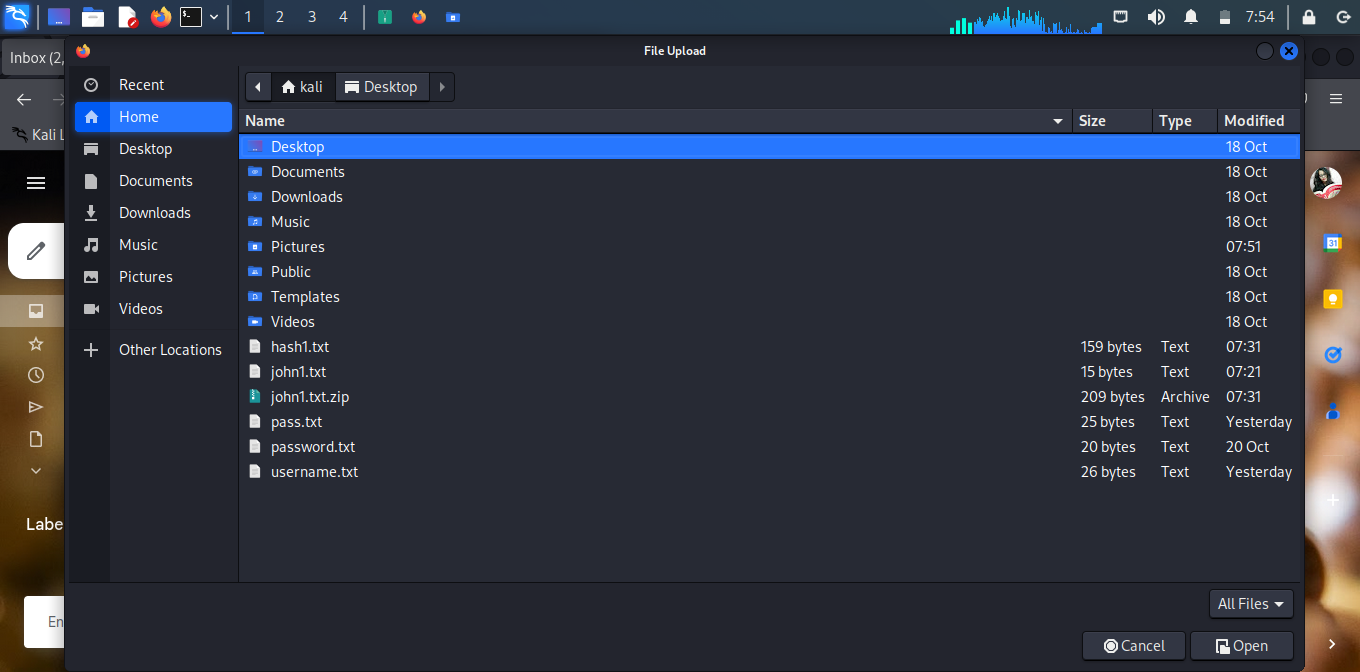
**5. Crunch**

crunch is a wordlist generating tool that comes pre-installed with Kali Linux. It is used to generate custom keywords based on wordlists. It generates a wordlist with permutation and combination. We could use some specific patterns and symbols to generate a wordlist.



* **CONCLUSION**

After all the work in our kali we can see such things.



Passwords are already a weak form of authentication. If a user is using a password so weak that it can be recovered by a slow, online attack, that’s a real problem! But even “strong” passwords, if they have been recovered from a breach such as the RockYou! hack, are still vulnerable to cracking. The best defense against an online attack is to lock out the attacked account after a handful of unsuccessful login attempts. Not only can this stop an Online Password Cracking attack dead in its tracks, it can also alert an administrator that such an attack is being carried out.