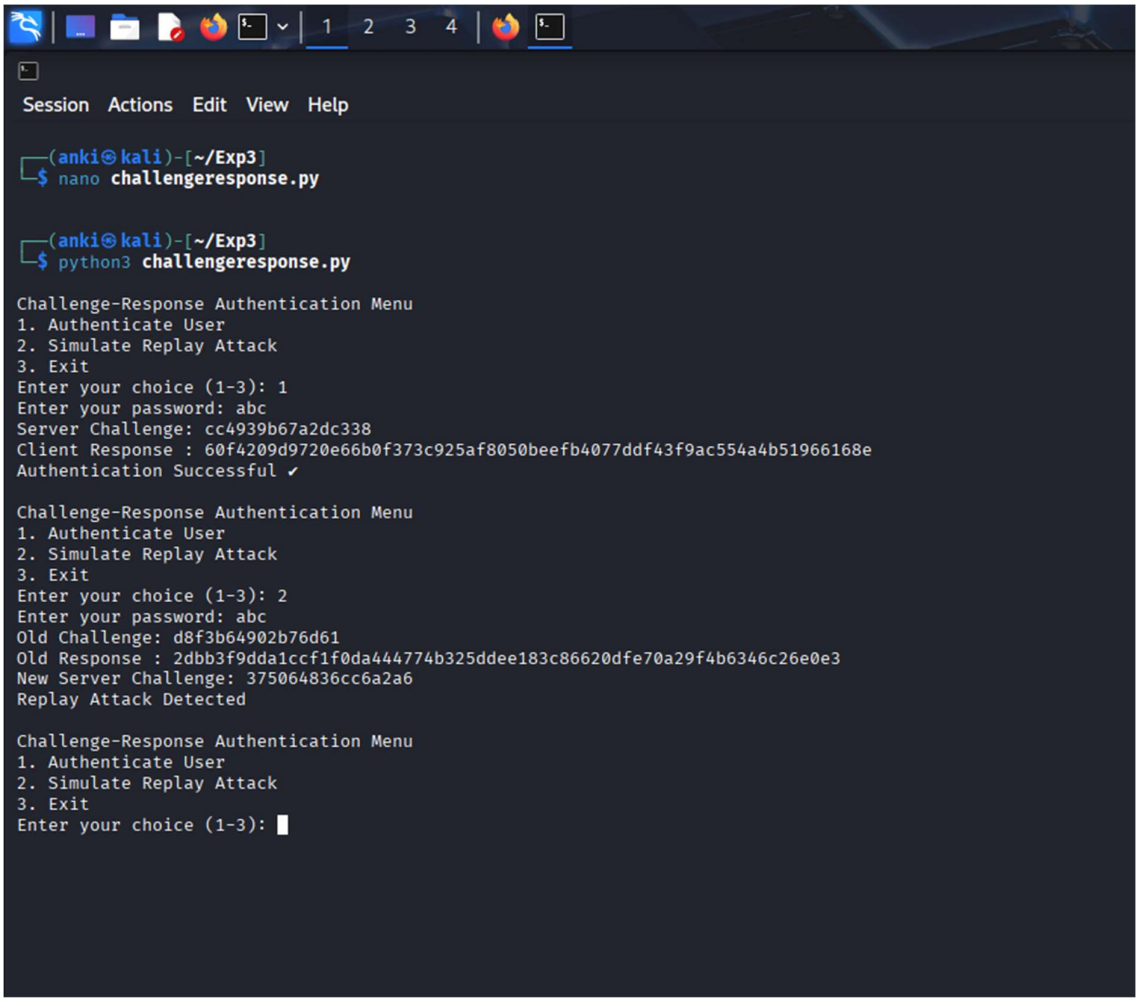
1 2 3 4
Session Actions Edit View Help
(anki㉿kali)-[~/Exp3]
$ nano challengeresponse.py
(anki㉿kali)-[~/Exp3]
$ python3 challengeresponse.py
Challenge-Response Authentication Menu
1. Authenticate User
2. Simulate Replay Attack
3. Exit
Enter your choice (1-3): 1
Enter your password: abc
Server Challenge: cc4939b67a2dc338
Client Response : 60f4209d9720e66b0f373c925af8050beefb4077ddf43f9ac554a4b51966168e
Authentication Successful ✔
Challenge-Response Authentication Menu
1. Authenticate User
2. Simulate Replay Attack
3. Exit
Enter your choice (1-3): 2
Enter your password: abc
Old Challenge: d8f3b64902b76d61
Old Response : 2dbb3f9dda1ccf1f0da444774b325ddee183c86620dfe70a29f4b6346c26e0e3
New Server Challenge: 375064836cc6a2a6
Replay Attack Detected
Challenge-Response Authentication Menu
1. Authenticate User
2. Simulate Replay Attack
3. Exit
Enter your choice (1-3):

Session Actions Edit View Help

GNU nano 8.7

```
import os
import hashlib

def generate_challenge():
    return os.urandom(8).hex()

def compute_response(challenge, password):
    return hashlib.sha256((challenge + password).encode()).hexdigest()

while True:
    print("\nChallenge-Response Authentication Menu")
    print("1. Authenticate User")
    print("2. Simulate Replay Attack")
    print("3. Exit")

    choice = input("Enter your choice (1-3): ")

    if choice == "1":
        password = input("Enter your password: ")

        challenge = generate_challenge()
        print("Server Challenge:", challenge)

        response = compute_response(challenge, password)
        print("Client Response :", response)

        expected = compute_response(challenge, password)

        if response == expected:
            print("Authentication Successful ✓")
        else:
            print("Authentication Failed ")

    elif choice == "2":
        password = input("Enter your password: ")

        old_challenge = generate_challenge()
        old_response = compute_response(old_challenge, password)

        print("Old Challenge:", old_challenge)
        print("Old Response :", old_response)

        new_challenge = generate_challenge()
        print("New Server Challenge:", new_challenge)

        expected_new = compute_response(new_challenge, password)

        if old_response == expected_new:
            print("Replay Attack Successful ")
        else:
            print("Replay Attack Detected ")

    elif choice == "3":
        print("Exiting...")
        break

    else:
        print("Invalid choice.")
```

^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/