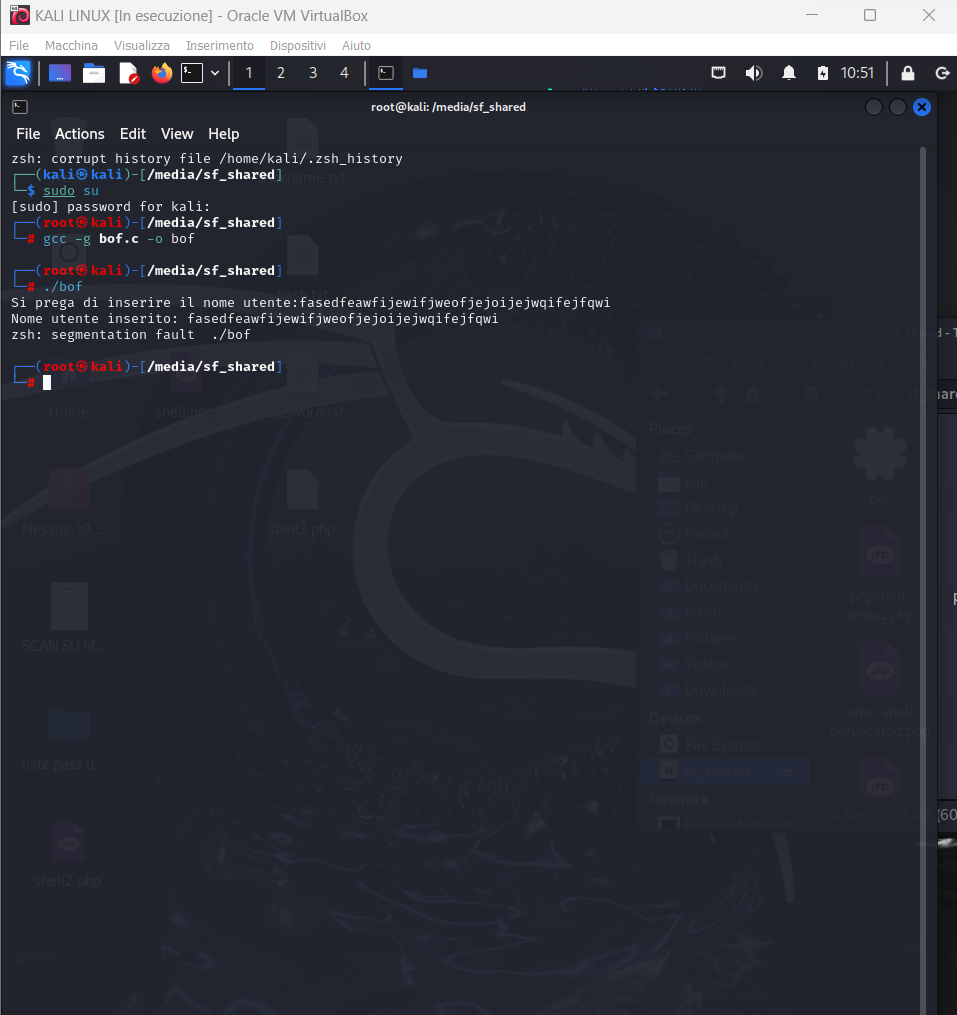
**“ESERCIZIO S7L4”**

**TRACCIA**

**Immagine che contiene testo, schermata, software, Pagina Web

Descrizione generata automaticamente**

**“RISOLUZIONE”**

****

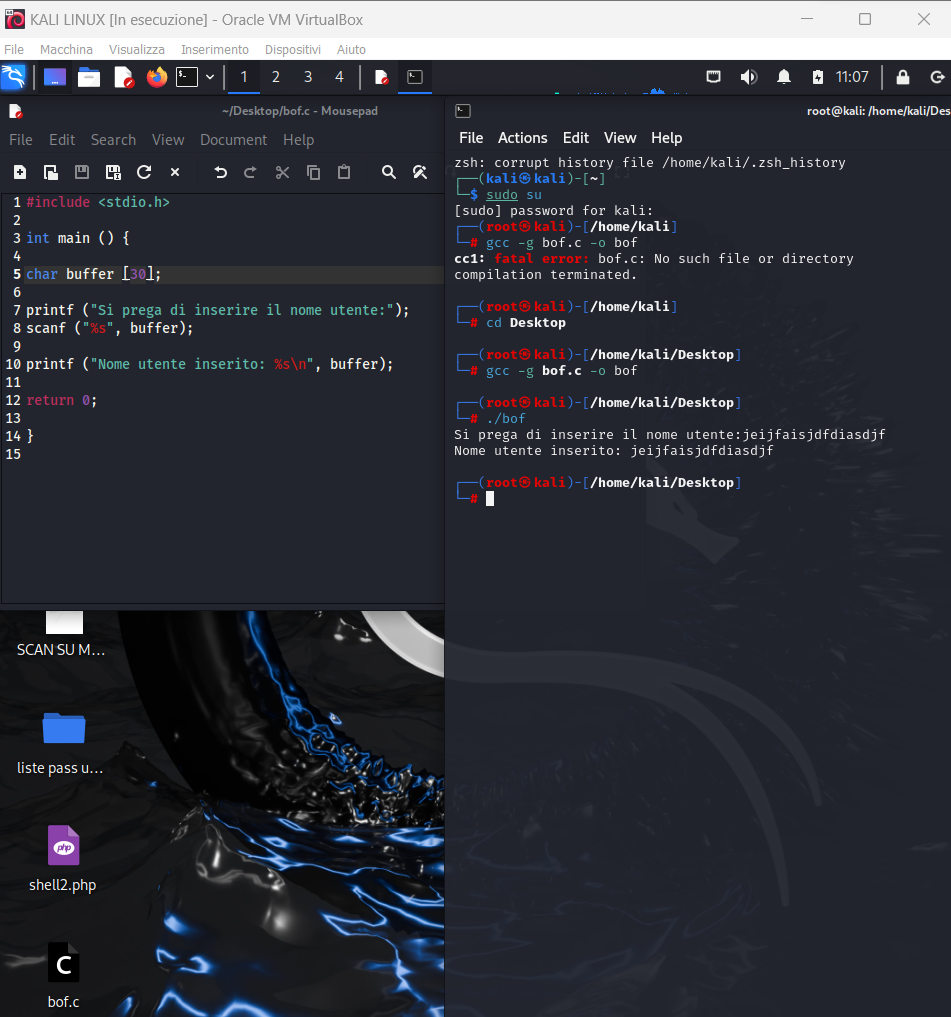
**COME POSSIAMO VEDERE IN FIGURA SOVRASTANTE ABBIAMO UN ERRORE DI BUFFER OVERFLOW SOVRASCRIVENDO PIU’ CAMPI DI MEMORIA DEL POSSIBILE.**

**IN QUESTO MODO UN ATTACCANTE POTREBBE SFRUTTARE QUESTA VULNERABILITA’ PER IMMETTERE CODICE MALEVOLO NEL CICLO DI RIAVVIO.**

**INOLTRE QUESTA VULNERABILITA’ ATTRAVERSO LE APERTURE DI UNA SHELL POTREBBE PORTARE UN ATTACCANTE AD AVERE PIENO POSSESSO DELLA MACCHINA “TARGET”.**

* **UN POSSIBILE RIMEDIO E AUMENTARE LA CAPIENZA DI CARATTERI (“QUINDI DI MEMORIA PRE ALLOCATA”)**

**ECCO UN ESEMPIO CON MODIFICA DEL CODICE :**

****

**COME POSSIAMO EVINCERE ABBIAMO AUMENTATO LA TRINGA DEL BUFFER A 30 CARATTARI .**