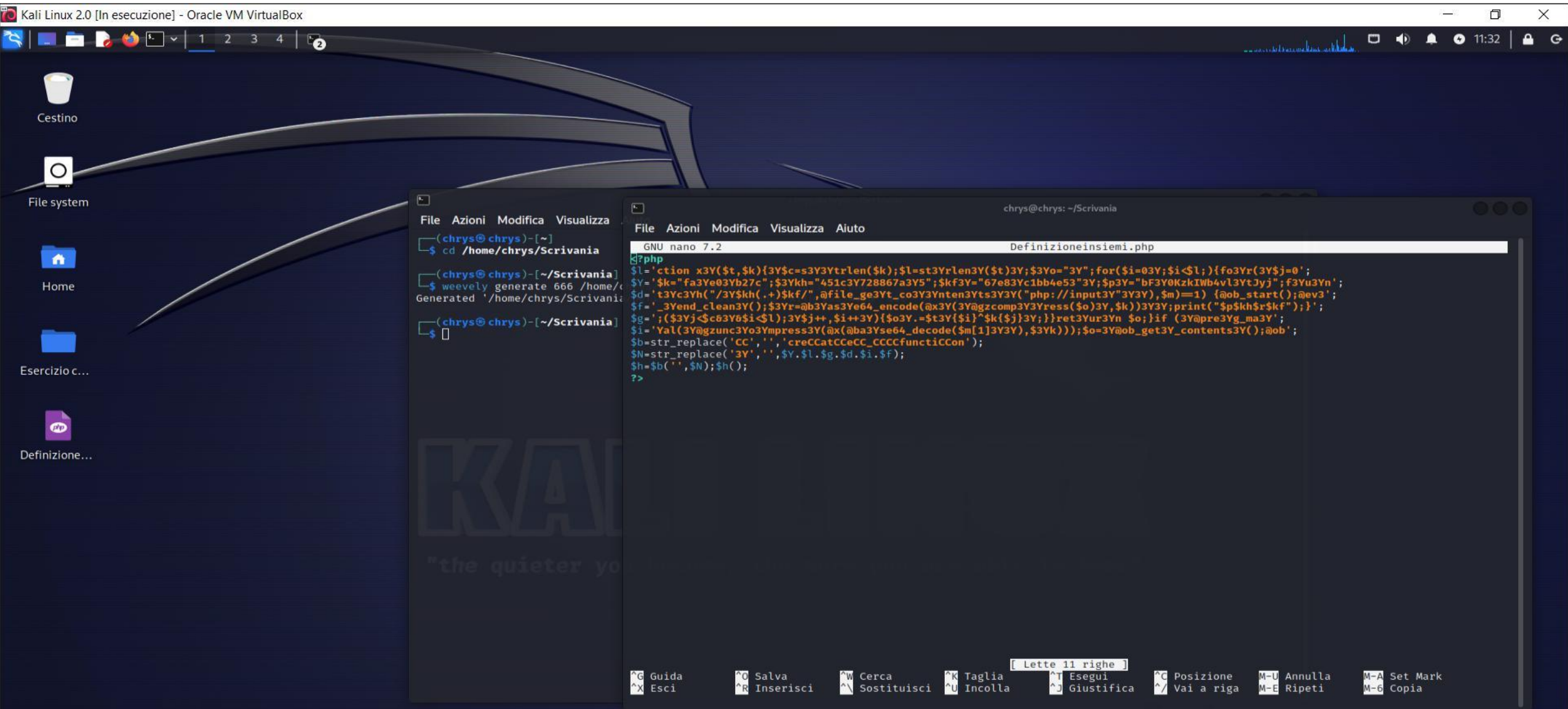


Creazione di una "Backdoor.php" attraverso l'utilizzo del tool Weeveily presente su Kali.



Carichiamo la Backdoor precedentemente creata e richiamiamola attraverso il campo URL del nostro browser.

The image displays three side-by-side windows of a Kali Linux virtual machine, each running Burp Suite. The leftmost window shows the DVWA (Damn Vulnerable Web App) interface at the 'Vulnerability: File Upload' page. A message indicates a successful upload: '.../hackable/uploads/Definizioneinsiemi.php successfully uploaded!'. The middle window shows the Burp Suite 'Proxy' tab with a list of HTTP history. The selected request is a POST to '/dwa/vulnerabilities/upload/'. The rightmost window shows the Burp Suite 'Proxy' tab with a list of HTTP history. The selected request is a GET to '/dwa/hackable/uploads/Definizioneinsiemi.php'. The Burp Suite interface includes a dashboard, target, proxy, intruder, repeater, collaborator, sequencer, decoder, comparer, and logger. The HTTP history table lists requests with columns for #, Host, Method, URL, Params, Edited, Status, Length, MIME type, and Extensions. The request details pane shows the raw HTTP request and response, including headers, cookies, and body content.

Richiamo della Backdoor da terminale per connetterci all'indirizzo target.

