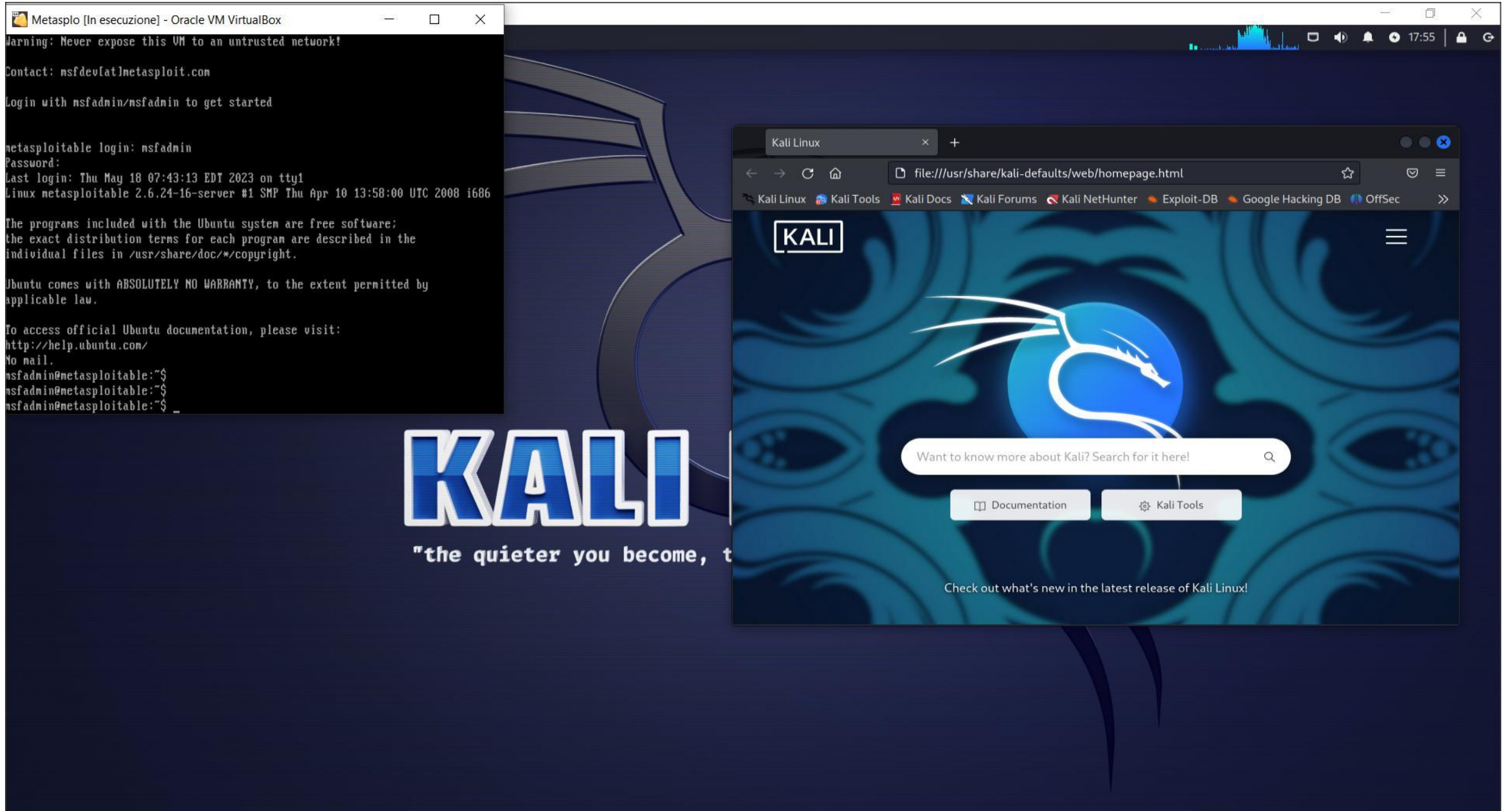
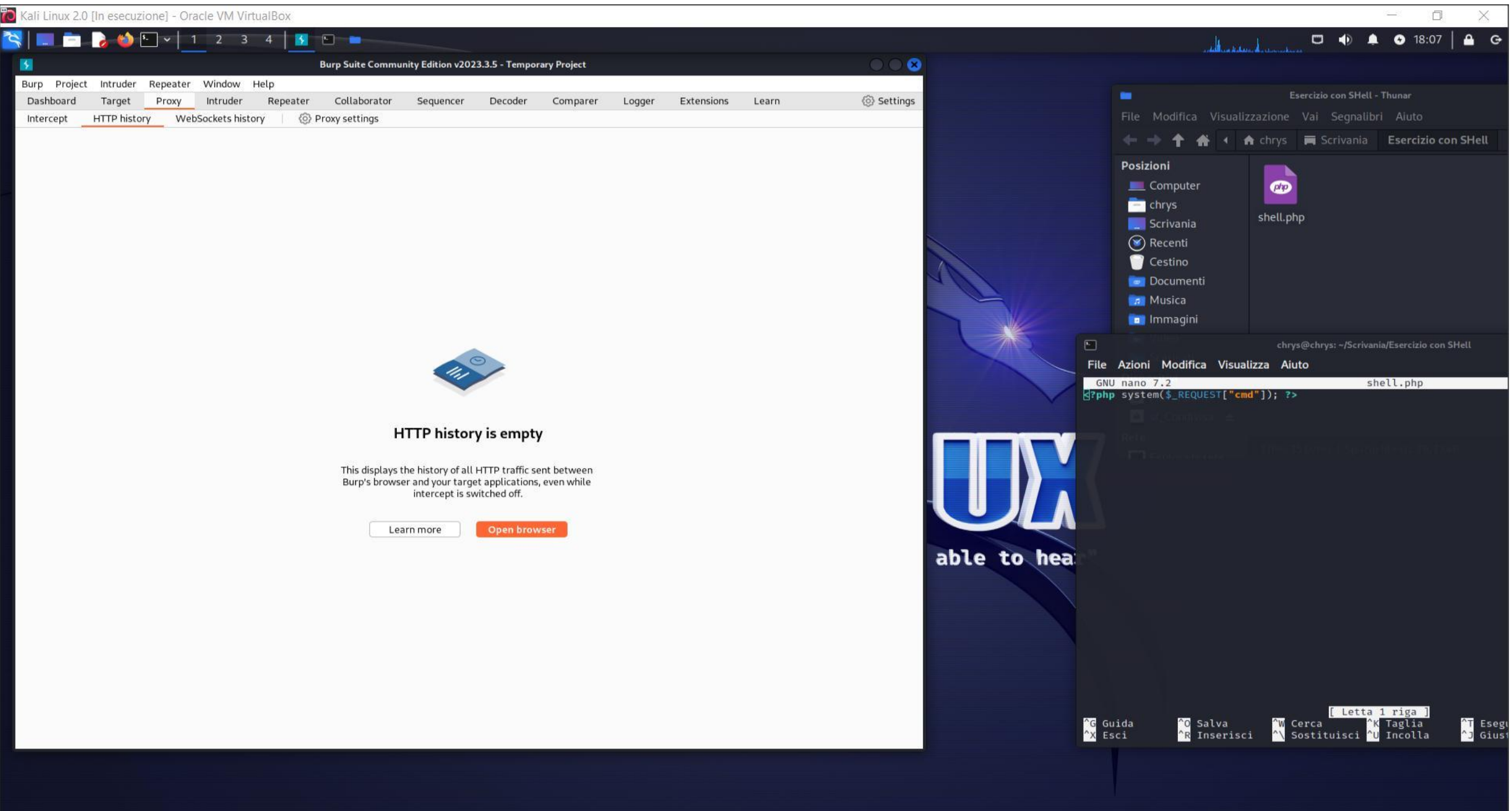


## Avvio Delle macchine virtuali Kali e Metasploit.



## Configurazione Tool Burpsuit e creazione di una Shell Base in formato " PHP".



The image shows a Kali Linux 2.0 virtual machine running on Oracle VM VirtualBox. The desktop environment includes a web browser with a single tab titled 'Damn Vulnerable Web Ap' and a Burp Suite Community Edition v2023.3.5 window. The browser displays the DVWA 'Vulnerability: File Upload' page, which has a sidebar with navigation links like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, and Upload (which is highlighted). The main content area shows a file upload form with a 'Choose an image to upload:' label, a file selection button, and an 'Upload' button. Below the form, there is a 'More info' section with links to external resources. The Burp Suite window is in the 'Intercept' tab, showing a request to 'http://192.168.50.100:80'. The request is a POST to '/dvwa/vulnerabilities/upload/' with a content length of 434. The request body is a multipart form-data containing a file named 'shell.php' and a 'MAX\_FILE\_SIZE' parameter. The 'Inspector' panel on the right shows the request attributes, query parameters, body parameters, cookies, and headers. The status bar at the bottom of Burp Suite indicates '0 matches'.



# Utilizzo del link del caricamento del file per vedere cosa ci mostra l'url di indirizzamento.

