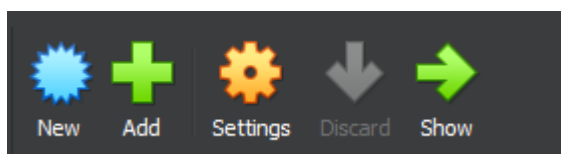


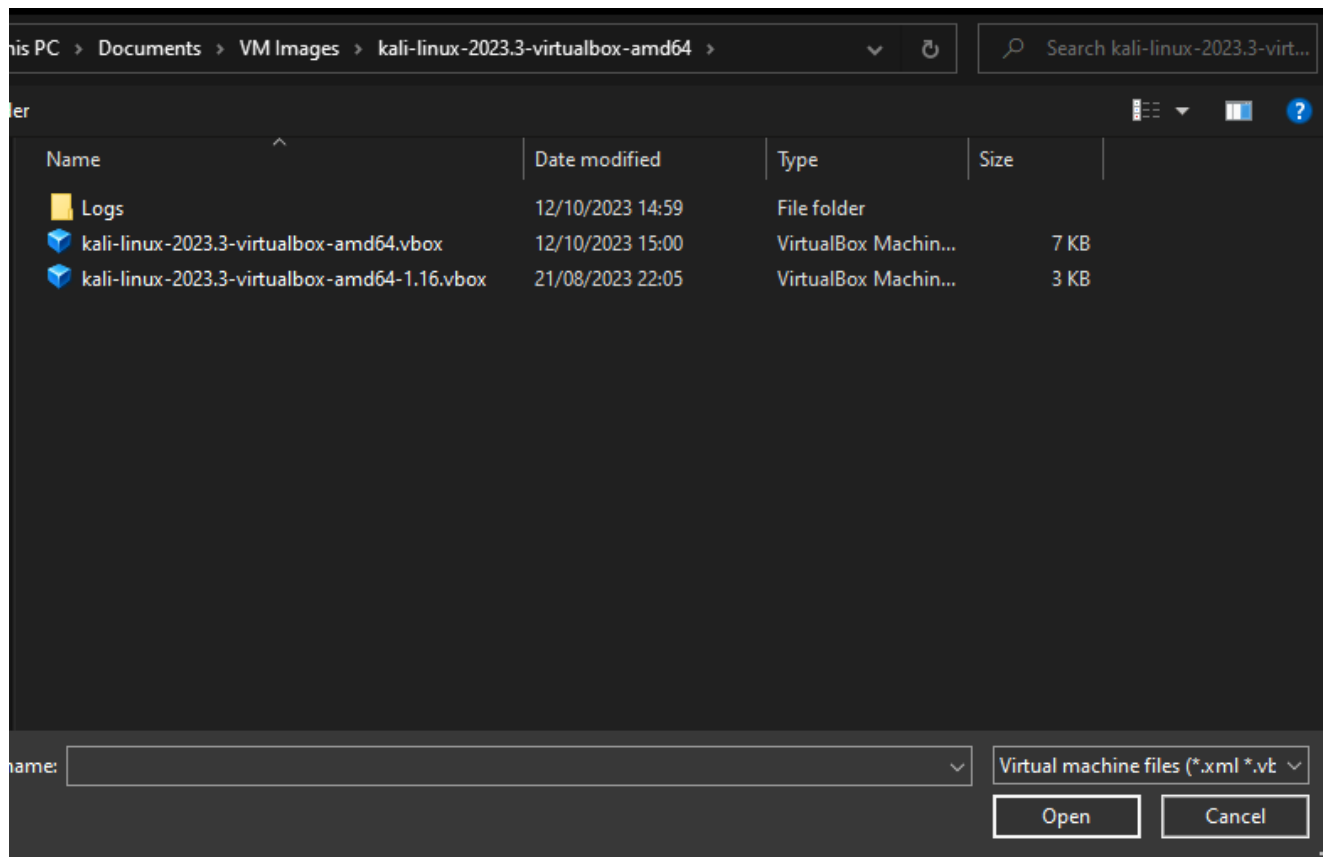
Install Kali

[Kali-0VA](#) runterladen



in VBox hinzufügen



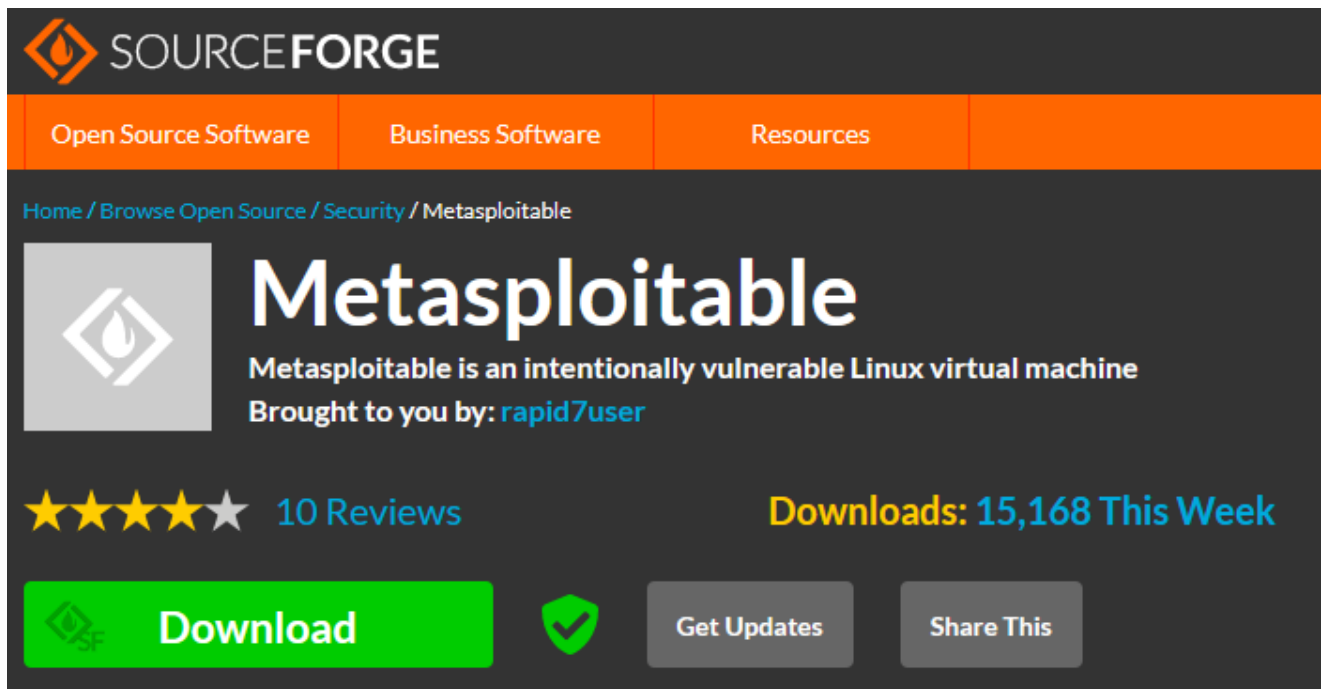


und starten



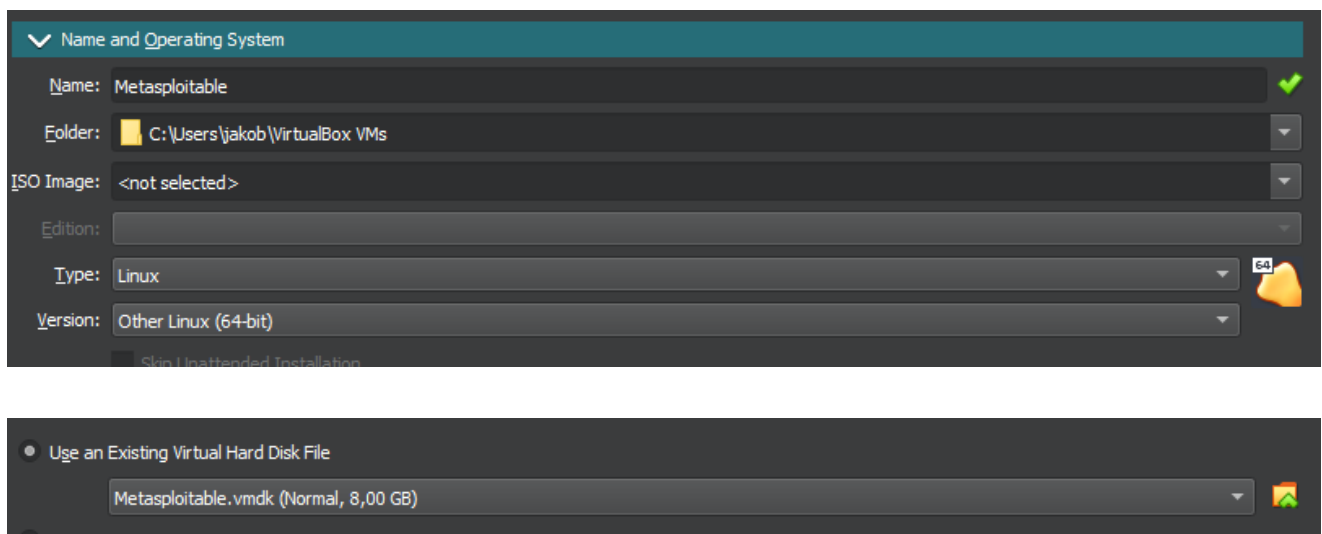
Metasploitable

[Metasploitable](#) von SourceForge runterladen



The image shows the SourceForge project page for Metasploitable. At the top is the SourceForge logo and navigation tabs for Open Source Software, Business Software, and Resources. The breadcrumb trail reads: Home / Browse Open Source / Security / Metasploitable. The main header features the Metasploitable logo (a diamond with a flame) and the title "Metasploitable". Below the title, it states: "Metasploitable is an intentionally vulnerable Linux virtual machine" and "Brought to you by: rapid7user". The page shows a rating of 4 stars from 10 reviews and "Downloads: 15,168 This Week". At the bottom, there are three buttons: a green "Download" button with the SourceForge logo, a green shield icon, and a grey "Get Updates" button, followed by a grey "Share This" button.

eine neue Virtual Machine in VBox mit dem Metasploitable-Disk File anlegen



The image shows the "Name and Operating System" step of the Virtual Machine creation wizard in Oracle VM VirtualBox. The "Name" field is set to "Metasploitable" with a green checkmark. The "Folder" is set to "C:\Users\jakob\VirtualBox VMs". The "ISO Image" is set to "<not selected>". The "Edition" is set to "Linux". The "Type" is set to "Linux" and the "Version" is set to "Other Linux (64-bit)". There is a small orange icon next to the version dropdown. Below this section, there is a radio button for "Use an Existing Virtual Hard Disk File" which is selected. The dropdown menu for this option shows "Metasploitable.vmdk (Normal, 8,00 GB)" with a green checkmark.

OWASP Juice Shop