VIT UNIVERSITY
SCHOOL OF COMPUTER SCIENCE ENGINEERING

UNIT 02
Pen Testing with Metasploit

By
Dr. Ravi Verma

Output of this Presentation

- Students will be able to Install various tools and software like VMware, Kali Linux to perform Pen Testing .
- This session will brings the concept of realizing how to conduct pen testing on Metasploit.

Contents To Be Discuss Cont

Today's Agenda

- Introduction To Metasploit
- History Of Metasploit
- Prepare The Metasploit Lab Environment
- Metasploit Architecture
- Metasploit Modules

Introduction to metasploit

- Metasploit is a popular penetration testing tool
- A tool for developing and executing exploit code against a remote target machine
- Offer a broad platform for pen-testing and exploit development

Msfconsole

- The msfconsole is the most popular interface to the Metasploit Framework (MSF)
- Execution of external commands in msfconsole is possible

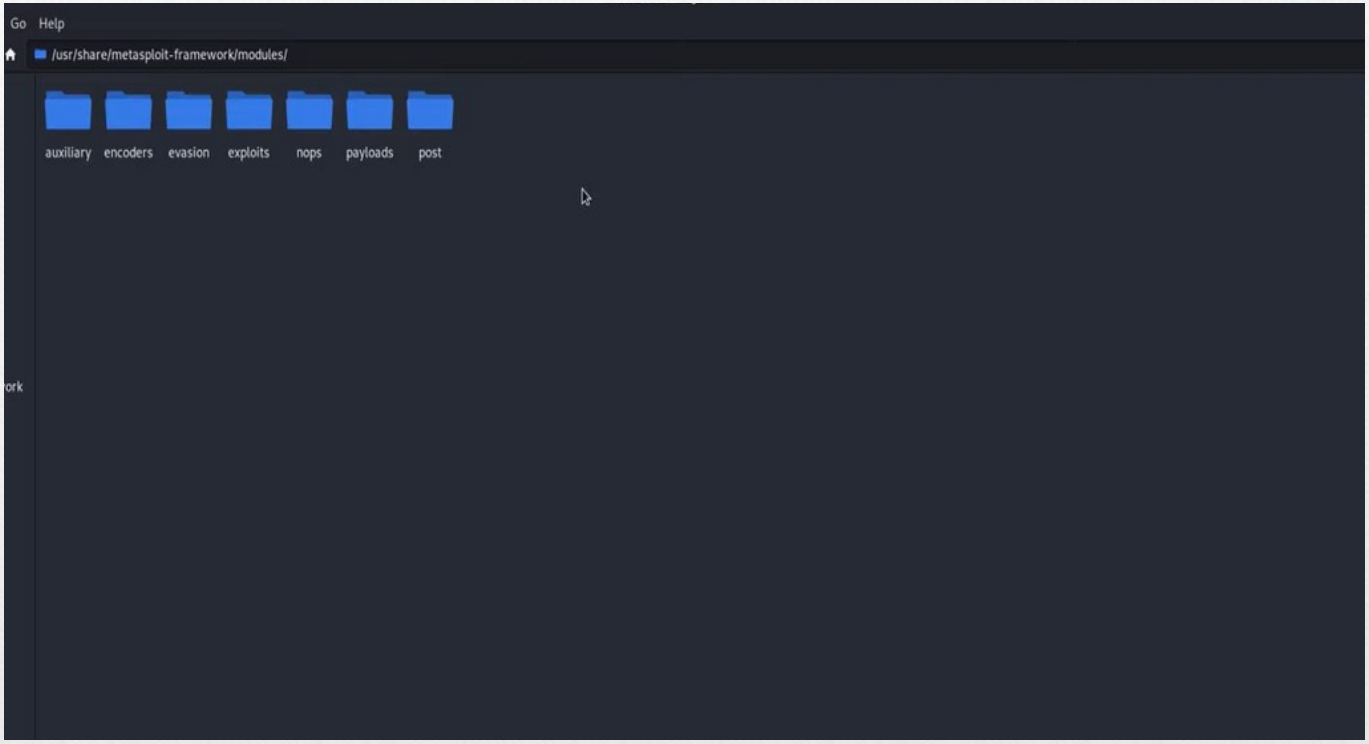
History of metasploit

- Undertaken in 2003 by H.D. Moore
- Perl-based portable network tool
- Later rewritten in Ruby by 2007
- Rapid7 purchased the Metasploit Project in 2009

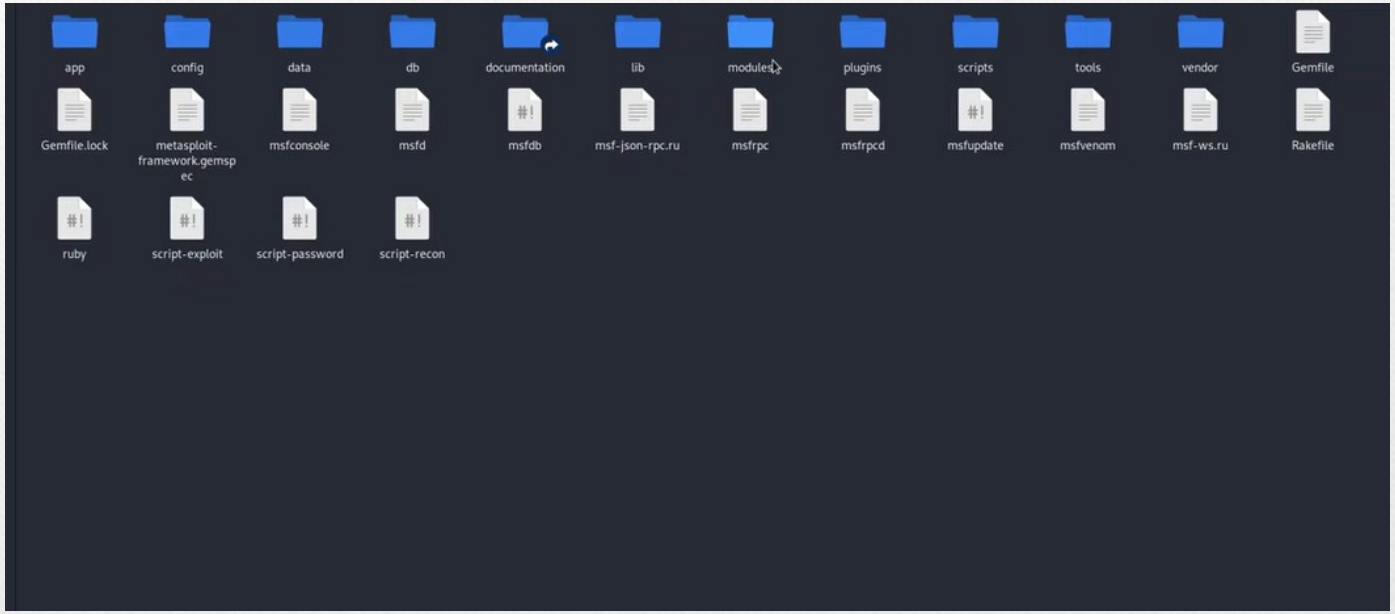
Prepare the metasploit lab

- Vmware
- Kali Linux
- Metasploitable
- Windows

Architecture of Metasploit



Architecture of Metasploit Cont..



Metasploit Modules

- A module is a piece of software that the Metasploit Framework uses to perform a task, such as exploiting or scanning a target.
  - Exploits
  - Auxiliary
  - Payloads
  - Encoders
  - Nops
  - Evasion
  - Post

Metasploit Modules

- Exploits
  - An exploit executes a sequence of commands that target a specific vulnerability found in a system
- Auxiliary
  - Auxiliary modules include port scanners, fuzzers, sniffers, and more
- Payloads
  - Payloads consist of code that runs remotely

Metasploit Modules

- Encoders
  - Encoders ensure that payloads make it to their destination intact
- Nops
  - Nops keep the payload sizes consistent across exploit attempts
- Evasion
  - These new modules are designed to help you create payloads that can evade anti-virus (AV) on the target system

Metasploit Modules

- Post
  - Post-exploitation modules that can be run on compromised targets to gather evidence, pivot deeper into a target network, and much more.

Conclusion

- Presentation brings various modules used in Metasploit platform to conduct a Pen Testing for Network and other Computing Devices.

Question ?

Download Extrapolatable as second machine for

download metasploitable vmware

All | Videos | News | Images | Shopping | More

About 32,100 results (0.39 seconds)

https://sourceforge.net › ... › Security

Metasploitable download | SourceForge.net

19-Aug-2019 — **Metasploitable** is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and ...

★★★★½ Rating: 4.3 · 6 votes · Free · Security

Browse /Metasploitable2 · Metasploitable · Files · 6 Reviews

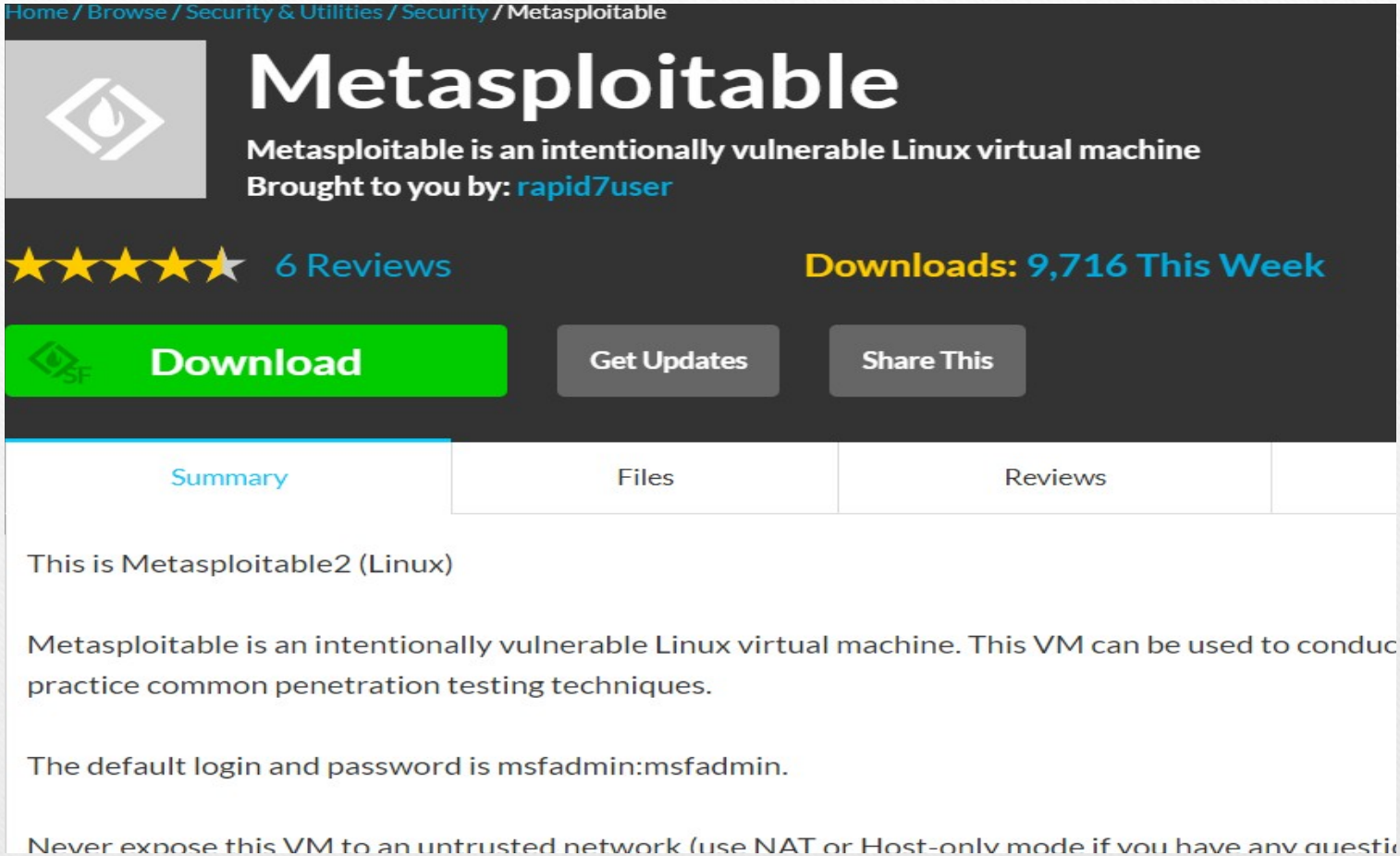
People also ask

Where can I download Metasploitable?

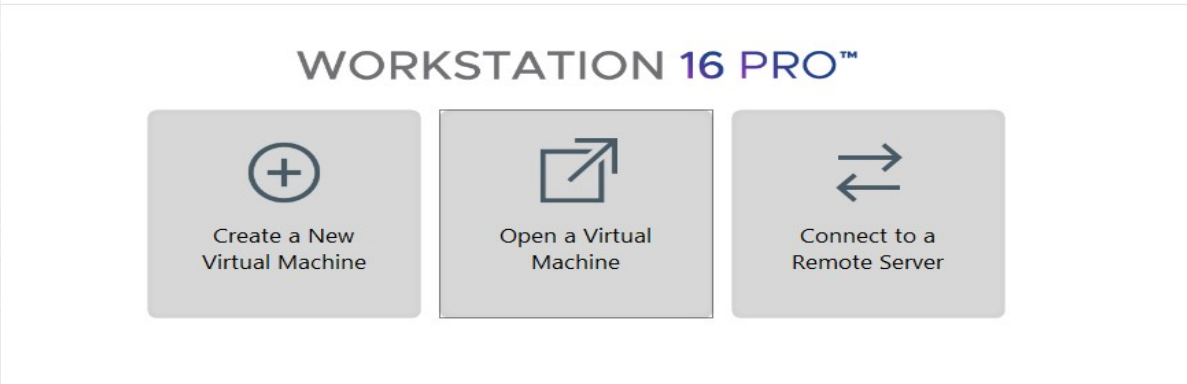
Where can I download Metasploitable 2?

What is Metasploitable virtual machine?

How much RAM does Metasploitable need?



- Metasploitable download | SourceForge.net

Installation

- After downgliding file need to extract it .
- Now open VMware workstation and choose Open virtual machine option. Then select file from extracted folder.