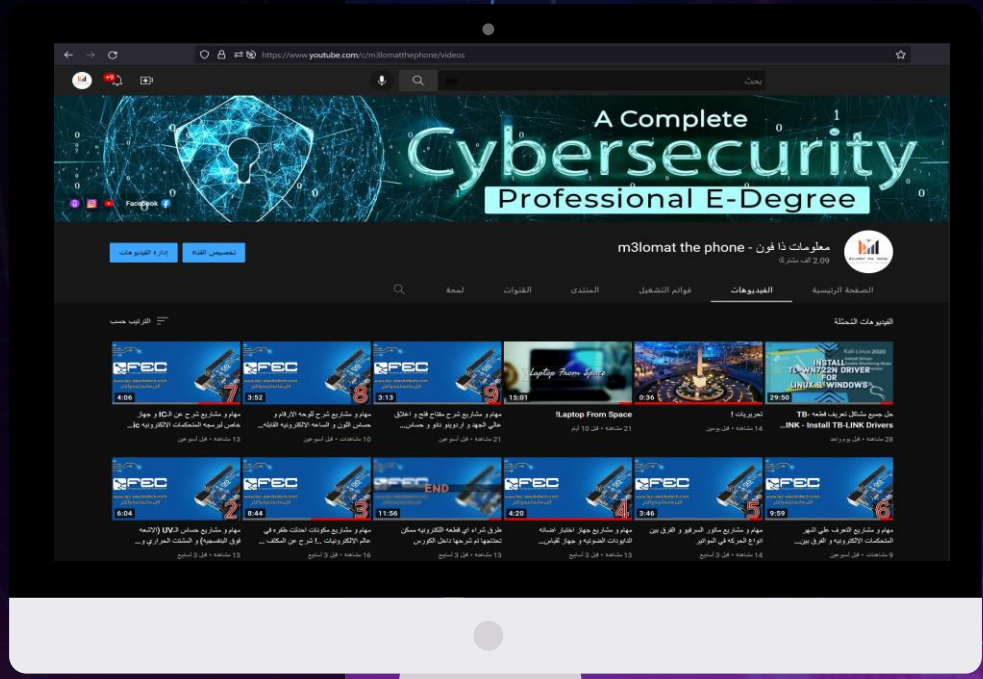
METASPLOIT

MSFCONSOLE

Eng. Mina Magdy
<sscp,oscp,crtp,pts>

Installation material

- Download Course Material
- Download VirtualBox
- Install Kali linux
- Install Windows 7
- Install metasploitable



Introduction

- The Metasploit Framework (MSF) is far more than just a collection of exploits–it is also a solid foundation that you can build upon and easily customize to meet your needs. This allows you to concentrate on your unique target environment and not have to reinvent the wheel. We consider the MSF to be one of the single most useful security auditing tools freely available to security professionals today. From a wide array of commercial grade exploits and an extensive exploit development environment, all the way to network information gathering tools and web vulnerability plugins, the Metasploit Framework provides a truly impressive work environment.

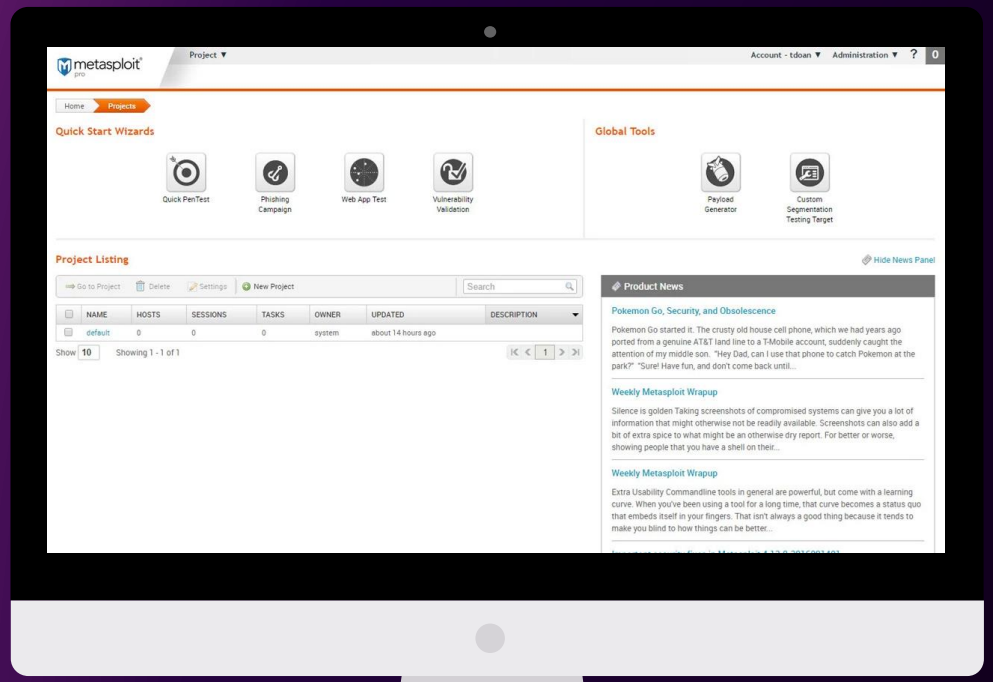
HOW IT RUN ....

How To Open & update MSF

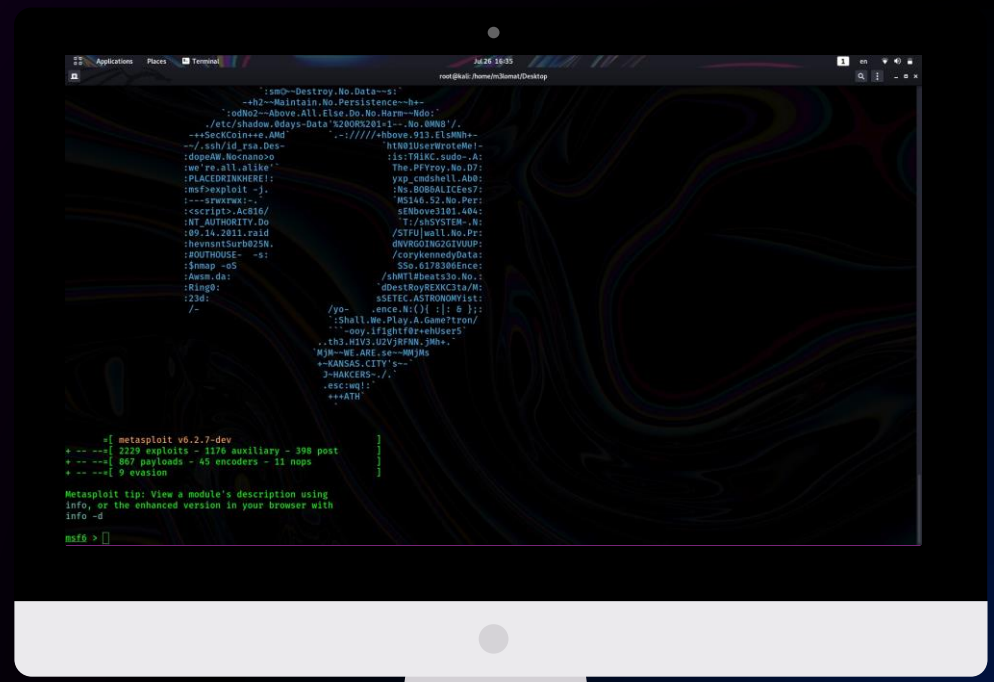
1) sudo apt update && sudo apt upgrade –y
2) sudo apt update ; apt install metasploit-framework (if uninstalled)
3) sudo msfupdate
4) sudo msfconsole

MSF INTERFACES

GUI
Graphical User Interface



Console



Information Gathering

Scan

Exploit

An exploit executes a sequence of commands that target a specific vulnerability found in a system or application to provide the attacker with access to the system. Exploits include buffer overflow, code injection, and web application exploits.

The Metasploit Framework includes hundreds of auxiliary modules that perform scanning, fuzzing, sniffing, and much more. Although these modules will not give you a shell, they are extremely valuable when conducting a penetration test.

Post-exploitation refers to any actions taken after a session is opened. A session is an open shell from a successful exploit or bruteforce attack. A shell can be a standard shell or Meterpreter. To learn more about the difference between each, see Manage Meterpreter and Shell Sessions.

Exploits

Auxiliary

Post

Payloads

Encoders

Nops

Evasion

Exploit

Auxiliary

Post

Payloads

Encoders

Nops

Evasion

6-


Placeholder
Placeholder
Placeholder
Placeholder
Placeholder
Placeholder
06
01
05
02
04
03


6-Item Hexagonal Diagram Slide Template
Placeholder
This is a sample text. Insert your desired text here.
06
01
Placeholder
This is a sample text. Insert your desired text here.
Placeholder
This is a sample text. Insert your desired text here.
05
02
Placeholder
This is a sample text. Insert your desired text here.
Placeholder
This is a sample text. Insert your desired text here.
04
03
Placeholder
This is a sample text. Insert your desired text here.

6-Item Hexagonal Diagram Slide Template

Placeholder

This is a sample text. Insert your desired text here.

Placeholder

This is a sample text. Insert your desired text here.

Placeholder

This is a sample text. Insert your desired text here.

Placeholder

This is a sample text. Insert your desired text here.

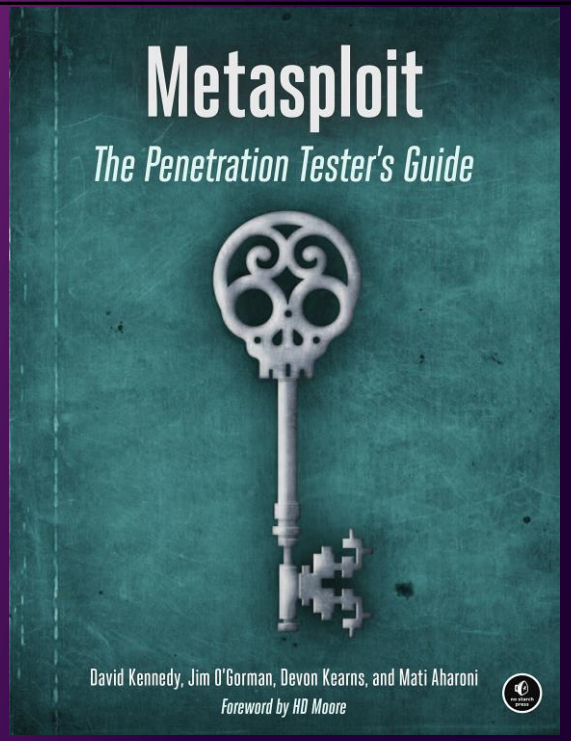
Placeholder

This is a sample text. Insert your desired text here.

Placeholder

This is a sample text. Insert your desired text here.

Books You Can Read About Metasploit



You can Ask Me ON ?

Facebook : https://www.facebook.com/m3lomatthephone

My YouTube Chanel : https://www.youtube.com/c/m3lomatthephone

M3lomat the phone 2 : https://www.youtube.com/channel/UCixopZbFBzdYKk2qsZLsRCA

M3lomat_Electric : https://www.youtube.com/channel/UCGnXhX2E_MaGYOY8kyOowbQ

Instagram : https://instagram.com/mena.m.rushdy?igshid=1xg5sxvjtek7i

LinkedIn : https://www.linkedin.com/in/mina-magdy-38362b1b6/

Facebook Group : https://www.facebook.com/groups/391033085092937