Introduction to Metasploit

SoftUni Team

Technical Trainers

Software University

SoftUni

Software University

https://softuni.bg

Have a Questions?

Software University

sli.do

#Cyber_Security

Table of Contents

What is Metasploit?

Metasploit in a Nutshell

Software University

- Metasploit is automatic **exploitation framework**
- The exploited inside are precompiled with **ruby** and **already imported**
- The whole framework is based on ruby and works **only** with **ruby** exploits
- Everyone can create **msf exploit**
- Before using exploit, a little configuration must be made

Metasploit in a Nutshell

- Exploits in **Metasploit** are based on **real** vulnerabilities
- There is a paid version of the product, having extended functionalities
- Everyone can **create msf exploit**
- Before using exploit, a little configuration must be made

Metasploit in a Nutshell

- Beside exploits, **Metasploit** have predefined payloads and auxiliary modules, for either post exploitation or scanning
- Metasploit is really loud! If the goal of the engagement is to **stay stealthy**, avoid it!
- Now let's get to practical examples

How to Work With Metasploit?

How to Search for Everything?

- Metasploit supports the term "**search**"
- It is used for searching for all modules, independent of it's core (exploit / auxiliary / payload / misc)
  - For example: "**search wordpress**" will output all modules containing wordpress inside
- Searchsploit also have support for Metasploit
- If you see (**Metasploit**) at the end of an exploit, it can be imported to Metasploit if it is missing

How to Trigger Exploit?

- To use an exploit, invoke "**use**" command with the full path of the module
  - For example: use **exploit** / **multi** / **handler**

How to Config the Exploit?

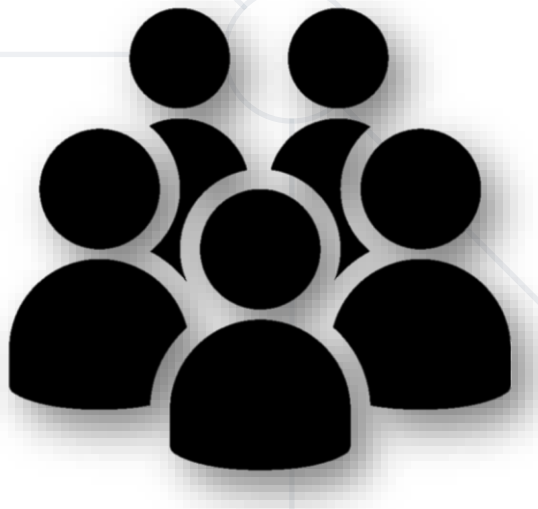
- To specify configuration to any module, use "**set**" keyword
- Example:
  - **set payload windows/x64/shell/reverse_tcp**
  - **set LHOST eth0**
  - **set LPORT 443**
- Start the exploit with "**exploit**" keyword
  - To start an exploit on the background use "**exploit –j**" keyword

Exploit Worked, Now What?

- After successful exploitation, you should see opened session
- To list all sessions use the keyword "**sessions**"
- To interact with specific session use the keyword "**sessions -i ID**"
- After engaging with a session, depending on the payload, you would have extended functionalities (**meterpreter payload**) or standard reverse shell (**reverse_tcp**) payload

How to Manage Multiple Sessions?

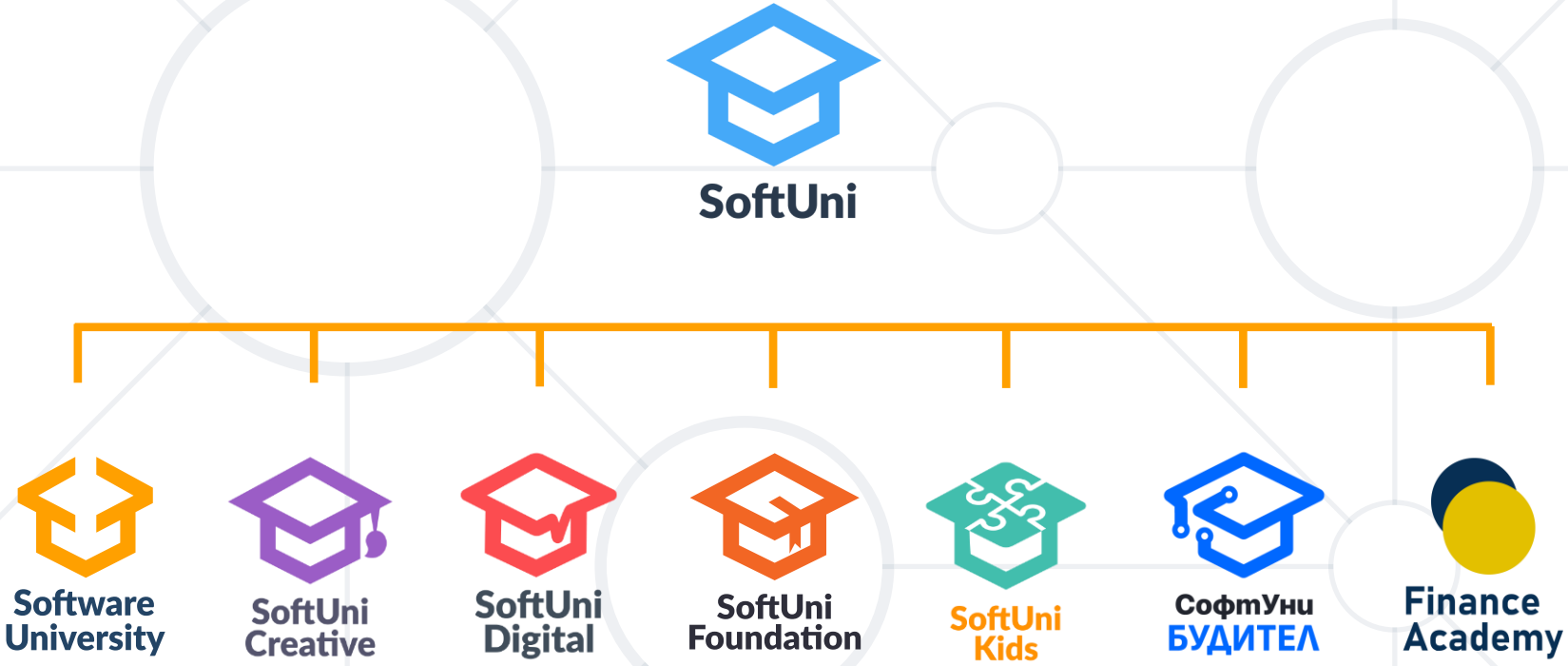
- While being engaged in session, type "**bg**" for moving it to background
- To open it again, use the same syntax "**sessions -i ID**"
- Now let's showcase that!



Summary

- Metasploit in a nutshell
- Search for everything
- Trigger exploit
- Config the exploit
- Manage multiple sessions

Questions?



SoftUni Diamond Partners

Software University

SmartIT

Coca-Cola HBC Bulgaria

SUPER HOSTING .BG

createX

Postbank

Решения за твоето утре

DRAFT KINGS

THE CROWN IS YOURS

VIVACOM

AMBITIONED

INDEAVR

Serving the high achievers

PHAR VISION

Trainings @ Software University (SoftUni)

- Software University – High-Quality Education, Profession and Job for Software Developers
  - softuni.bg, about.softuni.bg
- Software University Foundation
  - softuni.foundation
- Software University @ Facebook
  - facebook.com/SoftwareUniversity

License

- This course (slides, examples, demos, exercises, homework, documents, videos and other assets) is **copyrighted content**
- Unauthorized copy, reproduction or use is illegal
- © SoftUni – https://about.softuni.bg/
- © Software University – https://softuni.bg