LEARN METASPLOIT

Djebbar yehya
Mletta mohammed Mouncif

Supervised By:
DR.niar leila

RAPID7

CONTENT

0001

1 What is pentesting?

blackdragons@root:~$ answer

Penetration testing allows you to answer the question, “How can someone with malicious intent mess with my network?” Using pen-testing tools

2 What can i pentest?

```
blackdragons@root:~$  answer -show pentest-list
```

```
blackdragons@root:~$
-> clouds
-> web applications
-> mobile applications
-> internal network (Ethernet | WIFI)
-> iot
-> operating systems
```

0100

3 What's metasploit?

```
blackdragons@root:~$ msfconsole -define
```

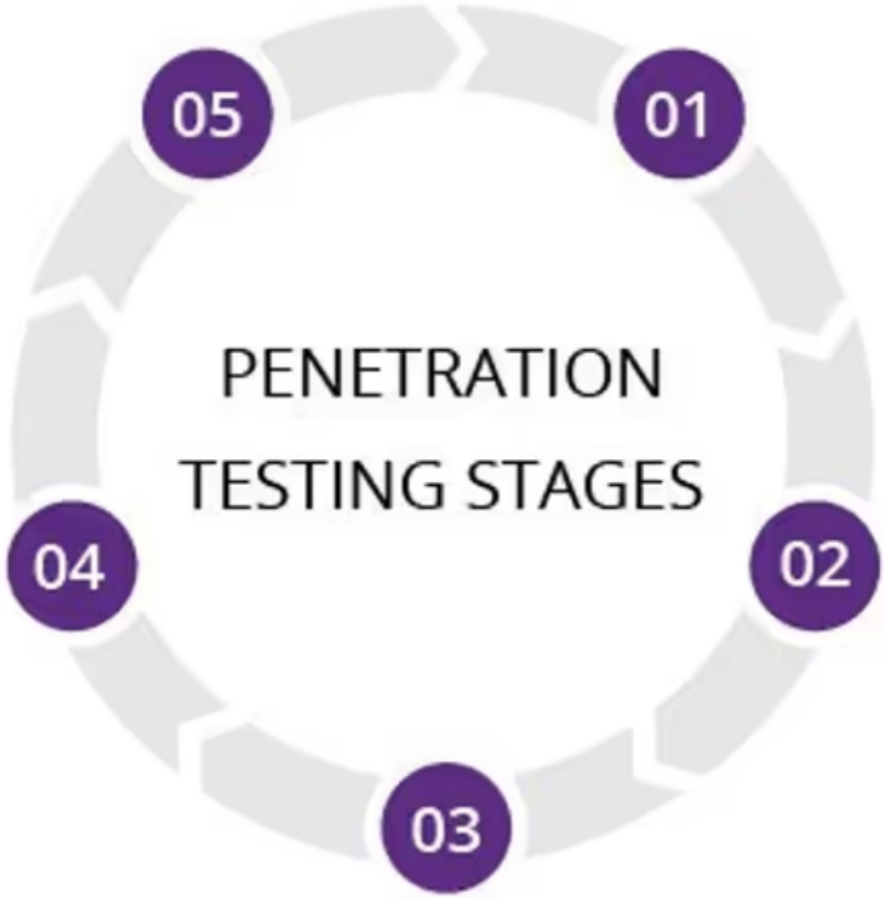
0101

3 What's metasploit?

The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it’s an open-source framework, it can be easily customized and used with most operating systems.

0110

PENETRATION TESTING STAGES



01

Planning and reconnaissance

Test goals are defined and intelligence is gathered.

02

Scanning

Scanning tools are used to understand how a target responds to intrusions.

03

Gaining access

Web application attacks are staged to uncover a target's vulnerabilities.

04

Maintaining access

APTs are imitated to see if a vulnerability can be used to maintain access.

05

Analysis and WAF configuration

Results are used to configure WAF settings before testing is run again.

4 Brief history

```
blackdragons@root:~$ msfconsole -useless --inf
```

0111

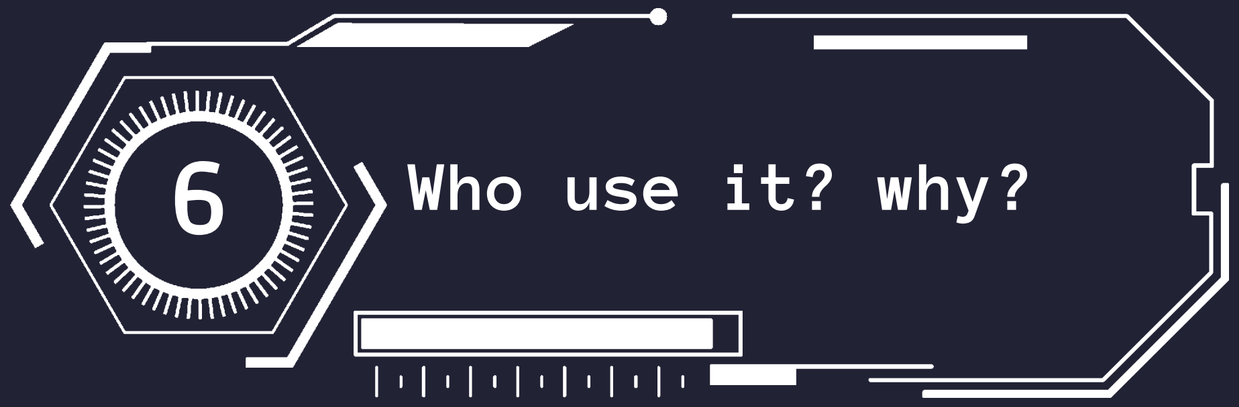
4 Brief history

The Metasploit Project was undertaken in 2003 by H.D. Moore for use as a Perl-based portable network tool, with assistance from core developer Matt Miller. It was fully converted to Ruby by 2007, and the license was acquired by Rapid7 in 2009, where it remains as part of the Boston-based company’s repertoire of IDS signature development and targeted remote exploit, fuzzing, anti-forensic, and evasion tools.

1000


```
blackdragons@root:~$ msfconsole -i -os=linux
› https://linuxhint.com/metasploit_usage_examples/
blackdragons@root:~$ msfconsole -i -os=windows
› https://docs.rapid7.com/metasploit/installing-the-metasploit-framework/
```

1001

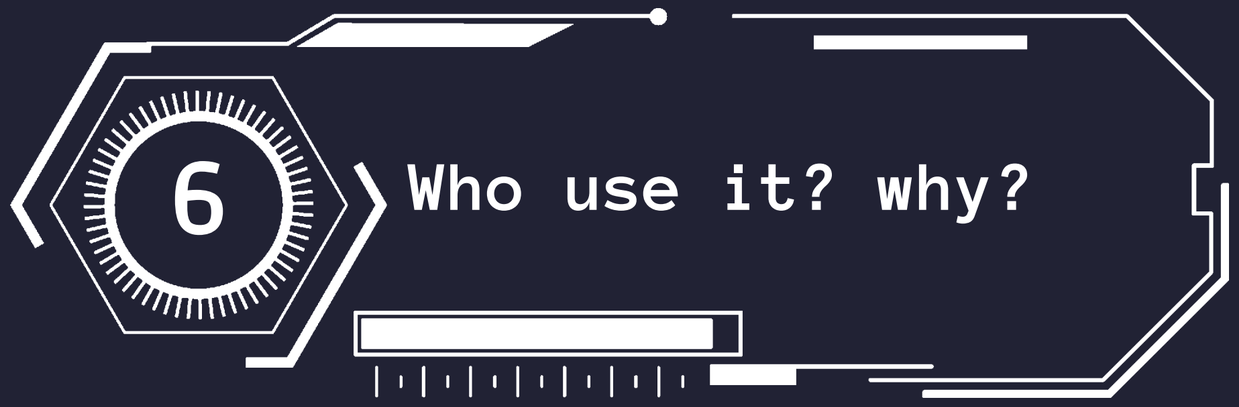


Due to its wide range of applications and open-source availability, Metasploit is used by everyone from the evolving field of DevSecOps pros to hackers.

1010

6 Who use it? why?

It’s helpful to anyone who needs an easy to install.



reliable tool that gets the job done regardless of which platform or language is used.

6 Who use it? why?

The software is popular with hackers and widely available.

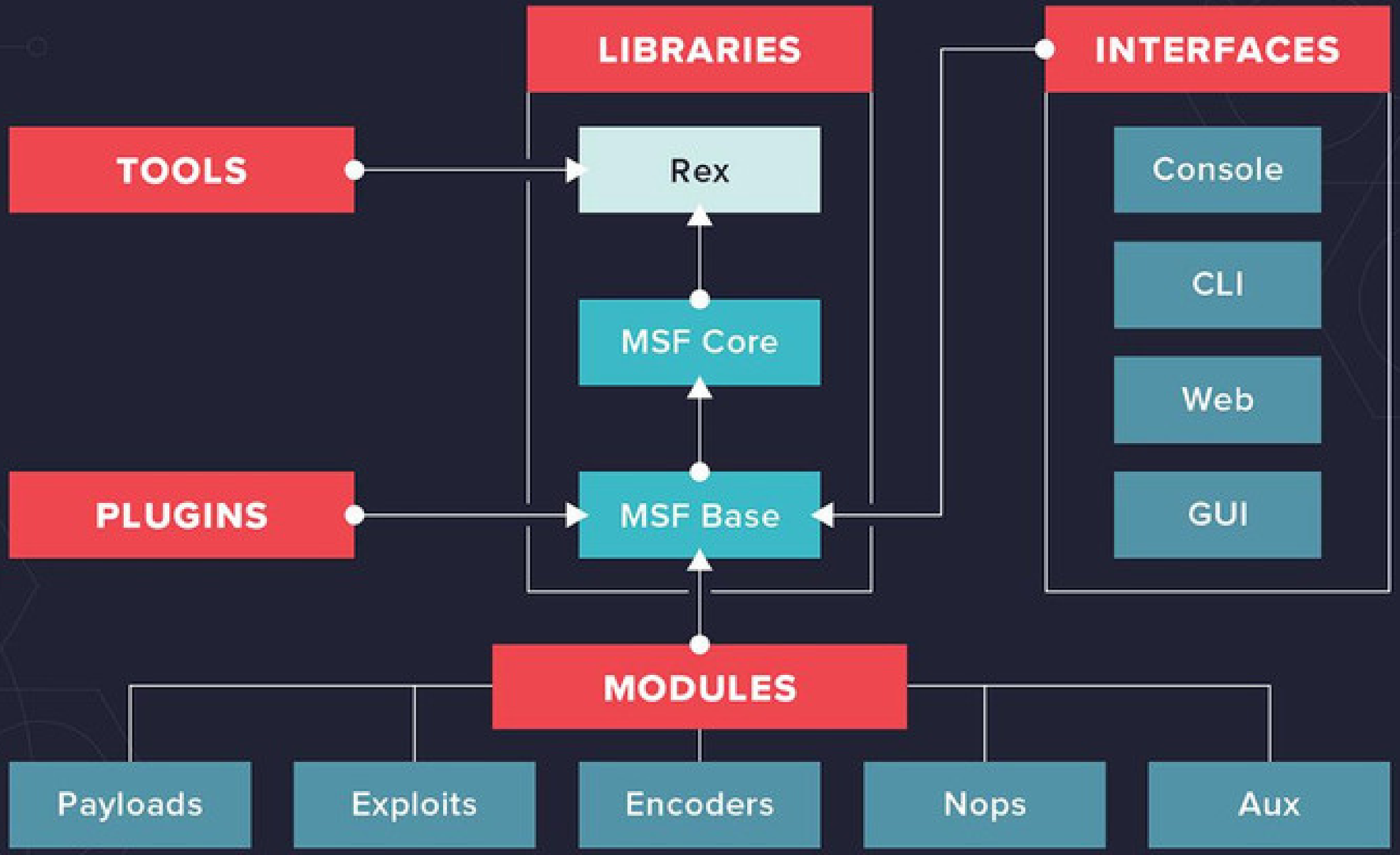

```
blackdragons@root:~$ msfconsole -show -modules
› exploits, payloads, encoders, listeners, shellcode
› post-exploitation code, nov
```

RAPID7

- **Exploits**: Tool used to take advantage of system weaknesses
- **Payloads:** Sets of malicious code Auxiliary furaccioaLi
  Supplementary tools and commands
- **Encoders:** Used to convert code or information
- **Listeners:** Malicious software that hides in order to gain access
- **Shellcode:** Code that is programmed to activate once inside the target.
- **Post-exploitation code:** Helps test deeper penetration once inside
- **Nov:** An instruction to keep the payload from crashing


```
blackdragons@root:~$ msfconsole -show -architecture
[##########] - 100%
› Libraries, Interface, tools, modules, plugins
```

10000



CREATED BY
BLACK DRAGONS

RESOURCES

- name: location
- WHAT CAN I PENTEST ?
- WHAT IS METASPLOIT ?
- BRIEF HISTORY
- INSTALLATION
- WHO USE IT ? AND WHY ?
- METASPLOIT MODULES
- METASPLOIT ARCHITECTURE

THANK YOU.