Metasploit

Metasploit is the most widely used framework in exploitation. It is a powerful tool that can support all phases of penetration testing engagements, from information gathering to post-exploitation.

2 main versions:
Metasploit pro: Commercial version, facilitates automation, and management of the tasks. Also has a GUI.
Matasploit framework: Open source free version, works from the command line.

Main components:

- **Msfconsole:** Main command line interface
- **Modules:** Supporting modules such as exploits, scanners and payloads
- **Tools:** Stand alone tools that help vulnerability research, assessment or penetration testing. Some tools for example could be pattern recognition.

Main Components:

msfconsole - **command.** Will allow us to interact with the different modules of metasploit. Modules are small components within that allow us to perform specific tasks, such as exploiting vulnerabilities, scanning a target or performing brute force attacks.

Auxiliary:
Supporting module for scanners, crawlers and fuzzers.

Encoders:
Allow you to encode, exploit and payload in the hope that signature antivirus solutions may miss them.

Evasion:
Encoders encode the payload, they should not be considered a direct attempt to evade. The evasion tool will try that with more or less success.

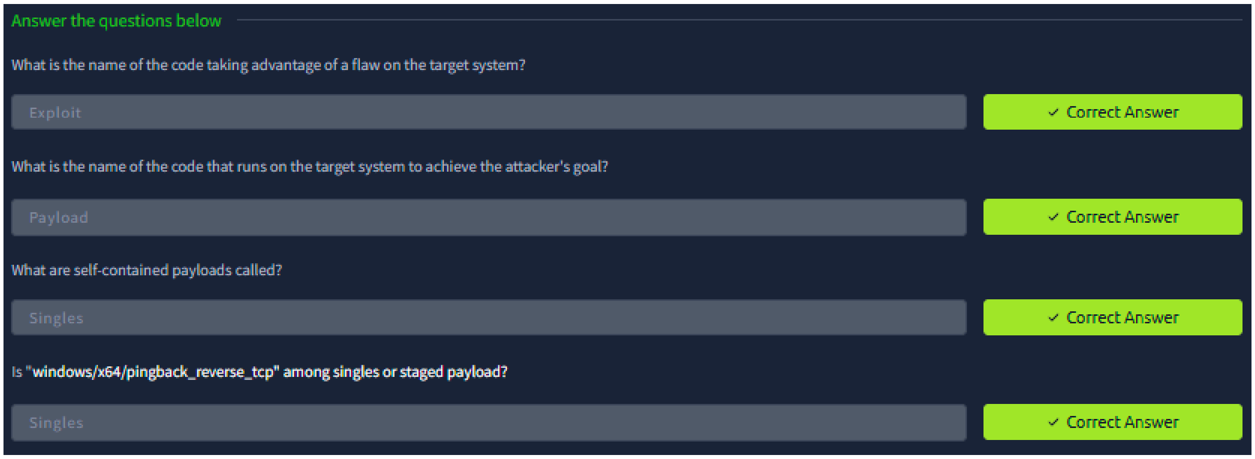
Exploits:
Neatly organise the target system.

NOPs:
No Operation do nothing. Represent the intel x86 cpu family. Do nothing for one cycle.

Payloads:
Codes that will run on the target system. Exploits leverage a vulnerability on a target system but to achieve the desired result we need a payload.
There are 4 different directories under payload and they are:

- **Adapters:** Wraps single payloads to convert them into different formats.
- **Singles:** Self-contained payloads (add user, launch notepad.exe etc) do not need additional components to run.
- **Stagers:** Responsible for setting up a connection channel between Matasploit and the target system. Useful with staged payloads.
- **Stages:** Downloaded by the stager, this will allow you to use larger payloads.

Post:
Post modules will be useful on the final stage of the penetration testing process.



Answer the questions below

What is the name of the code taking advantage of a flaw on the target system?

Exploit

What is the name of the code that runs on the target system to achieve the attacker's goal?

Payload

What are self-contained payloads called?

Singles

Is "windows/x64/pingback_reverse_tcp" among singles or staged payload?

Singles

Msfconsole:
Doing this command opens the console on the command prompt.
ls = Lists contents

If we ping 8.8.8.8 which is googles IP address we would do
Ping -c 8.8.8.8

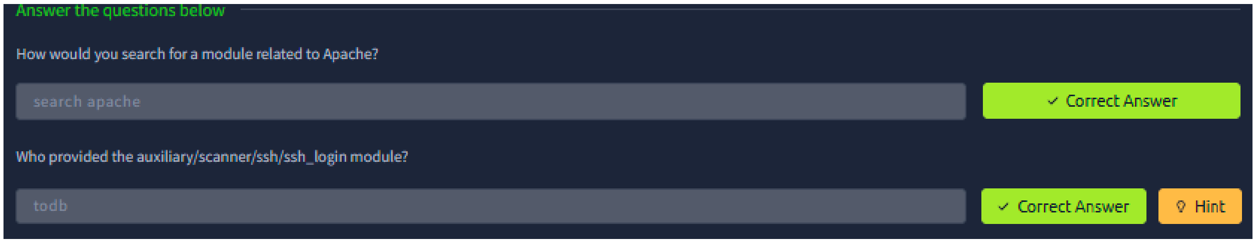
Metasploit will **support most linux commands.** Including clear - which clears the terminal.
History = Shows history commands you have typed earlier
Help = Lists commands / description

Command:
use exploit/windows/smb/ms17_10_eternalblue = Exploit mode

Use = Followed by the number at the beginning of the search result line.

Show options = Variety of option to choose from
Eg, Payload, Module etc.

Show = Variety of show options eg show payloads.
Back = Command that allows you to go back
Info = More context
Search = Manually search the metasploit framework



Answer the questions below

How would you search for a module related to Apache?

search apache

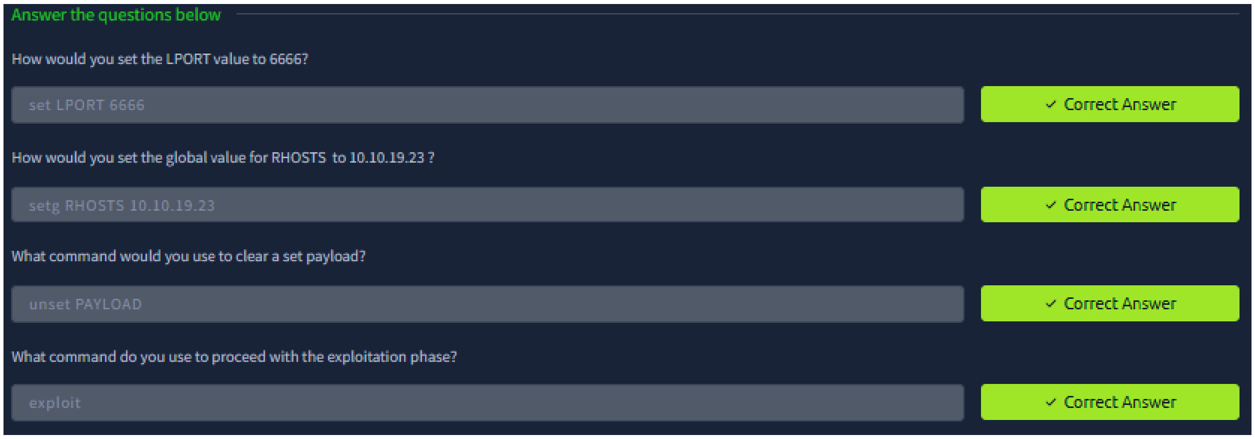
Who provided the auxiliary/scanner/ssh/ssh_login module?

todb

Show option - Module options
Eg setting rhosts:
Set rhosts 10.10.165.39
Show options to check command was done correctly
Rhosts - Remote host the IP address of the target system. A single IP address or a network range can be set. Support **Classless inter domain routing**.
Rport - Remote port
Payload - Payload
Lhost - Local host
Lport - Local port
Session - Each connection established to the target system using metasploit

Override using
Unset: Clears selected parameter
Unset all: Clears all set parameters

Setg: Set values for all modules.
Set: Set value using for selected module.



Answer the questions below

How would you set the LPORT value to 6666?

set LPORT 6666

How would you set the global value for RHOSTS to 10.10.19.23 ?

setg RHOSTS 10.10.19.23

What command would you use to clear a set payload?

unset PAYLOAD

What command do you use to proceed with the exploitation phase?

exploit