1) Attacking from kali to windows -

① start VM < kali
window

② VM → windows → cmd → ipconfig → Note it down
(for windows - ipconfig
kali - ifconfig)

③ VM → kali → cmd →

nmap -sS <ip>
nmap -sT/sU/sV/sP
nmap - O
init 0

- sudo su
- password - kali
- type all commands.
(we hv to use IP of windows to execute all commands).

kali (attacker)
windows (victim)

2) phishing → attackers trick ppl into revealing sensitive info like password e.g fake email to get password...

- to see installatn of socialphish → refer manual.
- ① VM → kali → firefox/chrome → socialphish.github (go on this site)
→ take url/code → paste it in kali (cmd) →

every thing on kali

ⓐ cd socialphish
ⓑ ./socialphish.sh
ⓒ choose option from - Instagram (enter it's code)
ⓓ link generate (open link)
ⓔ enter fake email/Id & Pass.

[psudo su
[pass - kali
} helps you to get in root folder. (you can use it after step ⓐ or ⓑ if error occur).

3) DDOS -

① open Metaspoitable — username & password : msfadmin

② ifconfig - to get ip address (Note it down).

③ Outside VMware → chrome → slowloris (github) →
copy the code(url:
① git clone <url code>

④ open kali → cmd → ② cd slowloris
② python3 slowloris.py <ip & meta>

⑤ VM → windows / kali → Chrome → enter <ip & meta>

you can see → Site will not load.

4) Keylogger - (See manual for pitures)

① setting → virus & Threat protectn → Turn of all protectn.

② (outside vm) browser → spyrix.app → download (free one) [spyrix free logger]
→ go to download →
install (sfk-setup) which we install →

③ more info → run anyway.

④ select language → email → email & pass → next →

⑤ Brower → spyrix.com → my account →
Login with Same email & pass →
select screenshot tab to see recent screenshots.

Now you will be able to monitor victim's Device.

5) zap -(do from manual)

- instead of juice-shop link u can use "testphp" also.

① open zap → cut comment box → Automated scan → paste url of testphp → attack → Alerts (vulnerabilities) → Generate report.

* disable - antivirus / firewall

6) MBSA (from manual)

① disable antivirus / firewall

② open MBSA → scan a computer → computer name (dropdown to automatically get hostname) → start scan → report generated

7) wireshark

① open wireshark →

② double click on wifi

③ "testphp site" → username - test, pass - test → login

④ search "http" in filter → in wireshark.

⑤ double click on → userinfo.php.

⑥ search your username & pass i.e. test in it (scroll down)

all 3 do outside vmware on app

security.org (password)
nordpass (secure password)