1. Jarraitu hurrengo gida, testing ingurune bat sortzeko:

https://www.elladodelmal.com/2018/09/como-montar-un-entorno-de-pentesting.html

2. [Opzionala]: Sortu docker-compose fitxategi bat pentesting laboratorioarekin
3. Frogatu nmap eskaneo motak aurkitzeko makina vulnerableak kalitik [[Nmap eta eskaneatze motak]]
4. Frogatu nmap eskeneo motak aurkitzeko portu irekiak makina hauetan

---

Honaino eginda klasen

---

1. Dockerren interfaze grafikorik erabili nahi ez dugunez. Zeren honek, pisutzuagoa egingo luke ingurunea eta bere deskarga/instalazio prosezua. Aurkitu moduren bat Wireshark interfazea erabiltzeko.
2. Nikto, web zerbitzariak aztertzen dituen eskaner bat da. Ikusi ahal duzuenez, gure kali irudia sortzerakoan instalatu egiten dugu. Aurkitu moduren bat Niktoren analisia gordetzeko eta beste nonbaiten zabaltzeko.

Nikto ulertzen, Nikto vs Nmap vs Nessus

Makinga gehiago: https://shamsher-khan-404.medium.com/docker-images-for-penetration-testing-security-7362519985b8

https://github.com/vulhub/vulhub/tree/master/imagemagick/imagetragick