**Ethical hacker**

**-white hat**

**-легални хакери**

**-пентестъри**

Oсигуряват непрекъсната сигурност на цялата организация и на нейните приложения. Много организации го използват, за да гарантират спазването на регулаторни стандарти, например, PCI-DSS или HIPAA, заедно с техники за отбрана като Static Application Security Testing (SAST). Tе правят по-висококачествен анализ на риска, чрез експлоатация на реално откритите уязвимости.

**Resources**

- OWASP https://wiki.owasp.org/index.php/Testing\_Guide\_Introduction

- toolswatch(top 125 tools)

http://www.toolswatch.org/

- SecTools.Org : Top 125 Network Security Tools

**Practicing defence and attack**

**(capture the flag sites)**

- OWASP Broken Web Applications

https://resources.infosecinstitute.com/owasp-practice-learn-play-scratch-2/

- Vulnhub

https://www.vulnhub.com/

- CTFtime

https://ctftime.org/

**10 famous and free hacking tools**

- Metasploit

Metasploit е фреймуърк за експлоатация на различни системи, използвайки конкретни уязвимости. Поддържа голяма база от експлойти, в комбинация с различни payload-и и непрекъснато се развива.

https://www.metasploit.com/

- Armitage

Проектиран като по-удобна за потребителя графична версия на Metasploit, Armitage бързо стана много популярен и се превърна в един от най-предпочитаните фреймуърк за пенетрейшън тестване на мрежи и IT инфраструктури.

http://www.fastandeasyhacking.com/

- NMap

Nmap, съкратено от Network Mapper, е друг безплатен инструмент с отворен код, който служи за сканиране за отворени портове и за картиране на мрежата, които след това ще анализирате. NMap е включен в още много други инструменти.

https://nmap.org/

- WireShark

WireShark е още един индустриален стандарт, който служи за прихващане на мрежовия трафик и анализ в реално време. Инструментът позволява на етичните хакери да проникнат дълбоко в мрежовия трафик и проучат индивидуалните пакети, като предлага на начинаещите добро въведение в TCP/IP.

https://www.wireshark.org/

- Faraday

Тестовата среда Faraday наскоро беше класирала на 6 място в класацията на инструменти за сигурност в ToolsWatch.org. Тя предлага нов начин за извършване на пенетрейшън тест - в IDE. Инструментът е създаден за анализ, индексиране и разпространение на данните.

https://www.faradaysec.com/#integreated-pentest-environment

- IronWASP

Създаден с пакет от интегрирани модули за сигурност, IronWASP е система за сканиране на уеб приложения, която открива над 25 често срещани уязвимости, с възможност за добавяне на персонализирани инструменти за сканиране според вашите собствени нужди за тестване на сигурността. Това е чудесен инструмент за начинаещи.

https://ironwasp.org/download.html

- Drozer

Приложенията за Android стават все по-масово използвани и все повече организации изграждат приложения за Android. Drozer може да помогне на етичните хакери да намерят уязвимостите в приложенията за Android.

https://labs.mwrinfosecurity.com/tools/drozer/

- Clutch

Приложенията за Android са известни с уязвимостите си, но и в тези на Apple също има достатъчно проблеми. Използвайте Clutch, за да декриптирате приложенията за iOS и да проверите дали имат уязвимости в сигурността си.

https://github.com/KJCracks/Clutch

- BeEF (The Browser Exploitation Framework)

Това е пентест инструмент, създаден специално за експлоатация на XSS уязвимости в уеб браузъра, включително такива в мобилната среда. BeEF е създаден за експлоатиране на атакуваните среди чрез вектори на атака от страна на клиента.

http://beefproject.com/

**Tool for social engineering**

Eтичните хакери тестват не само мрежи, системи и приложения, но и знанията за сигурността на служителите.

Social Engineering Toolkit, или накратко SET, е инструмент с множество вектори на атака, специално проектирани за социално инженерство. Възможните начини за употребата му включват разпространяване на фишинг, злонамерен USB код, различни видове атаки срещу уеб приложения – целта им е да открият слабите места на служителите ви. SET дори се интегрира с Metasploit за още по-широк спектър от функционалности.

https://github.com/trustedsec/social-engineer-toolkit

http://beefproject.com/