**Acceptance clause:** by completing this project the student accepts that he/she is responsible for what he/she will do and that he/she will not use these tools outside the virtual one created for that purpose. The student also accepts the legal repercussions that some of these actions may be subject to if these actions are carried out on external sites.

# Project 1: Information Gathering (source of information)[1]

**Level: 0**

**Difficulty: easy**

**Objective: Install and analyze the indicated tools obtaining information.**

**Environment: Windows, MacOs, Linux or mobile environments can be used.**

**Task: The student will have to collect information about the tools, install and use to obtain general information about tools & sites.**

There are a large number of sources of information and tools for ethical hacking, such as:

- Kali distribution (https://www.kali.org/ ): Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering. This distribution has the indicated tools installed
- Awesome Hacking (https://github.com/Hack-with-Github/Awesome-Hacking): A collection of awesome lists for hackers, pentesters & security researchers.
- SecTools.org (https://sectools.org/): Top 125 Network Security Tools
- Top 10 Most Popular Ethical Hacking Tools (2022 Rankings, https://www.softwaretestinghelp.com/ethical-hacking-tools/)
- Top 15+ Most Popular Web Service Testing Tools in 2022 (https://www.softwaretestinghelp.com/web-services-testing-tools/)
- Hackthissite.org (http://www.hackthissite.org/pages/index/index.php): This site is a free, safe and legal training ground for hackers to test and expand their skills. There is a large community with a list of projects in development and a vast selection of hacking articles to read along with a forum for commenting and discussing hacking and network security. An account must be created and the terms and conditions read before entering the site fully and afterwards you are free to join any of the missions that are currently in progress.
- Ethical hacking Courses & Tutorials:
  https://www.tutorialspoint.com/ethical_hacking/index.htm
  https://www.mygreatlearning.com/ethical-hacking/free-courses

1 Some parts are based on: https://www.w3schools.in/ethical-hacking

Penetration Testing, Incident Response and Forensics
https://portal.offensive-security.com/library/all

## DarkNet, Deep Web,

In today's world, the Internet has become the most indispensable part of human life, connecting the entire globe. But there is some mysteriously hidden internet area which many people don't familiar with. That is called the "Deep Web" or the "Darknet" that users can't usually find using regular or manual search and is stay hidden from most web surfers. "Darknet" or "Dark Net" is a lamination of a specific type of network which can only be retrieved by appropriate software, techniques, authorization, or configurations. It is often accessed using non-standard protocols and ports.

It is also called the 'hidden web' or 'invisible web.' Here all information can't be indexed using general searching mechanisms or search engines. The term 'Search Engine' defines a program and a website that searches for documents with specific keywords or phrases and results in a list of search documents and articles where the keyword matches on the Internet. The search engine uses 'spider' - a program to fetch as many web pages as possible. The spider program of a search engine cannot find everything, and those things which are not available using the keyword search technique resides as a part of the Darknet.

Most web pages are not indexed on the Internet via search engines. Experts estimate that 75% of the entire Internet is on 'invisible Web' content. The Deep Web is the majority of online content, and it is estimated to be 400-550 times greater than the surface web. Here, most contents are not readily accessible using standard means. For example - web pages regarding private user's accounts reside in the deep Web, i.e., the private information.

It was originated in the 1970s' for security and privacy purpose isolated from ARPANET (Advanced Research Project Agency Network). Darknet user's addresses did not appear in the network list and did not ping to others' inquiries.

**Characteristics of Darknet Webpages:**

- Web pages with no HTML codes or HTML texts for which the spider program cannot understand.
- Web pages with secured anonymize registration form.
- Dynamically generated web pages.
- Password protected web pages.
- Web pages with real-time content.
- No further links are there on the web pages, generally called 'disconnected pages'.

There different layers of Web starting ( 5 levels is most frequently used but there are some authors that indicates 6 or 8 levels). These are (most common):

- Level-0 Web:e. The common Web which maximum people use for browsing and downloading. It is accessible in any nation that does not block internet access.

- Level-1 Web: Also called the Surface Web or Clearnet - which is the reciprocal term for encrypted Darknet, which contains foreign social networking sites, Reddit, dig, Temp Email services, Web-hosting, human Intel Tasks, pirated media, free p-o-r-n-o-graphy, etc. This layer is blocked in some nations. One example of this level is the torrent sites, usually blocked by some ISP's, though it can be accessed using proxy servers.
- Level-2 Web: termed as Bergie Web requires one or two proxies or Tor browser to get the hidden content. It is the beginning stage of the deep Web. It contains links and access to FTP servers, Google locked results, existing honey-pots, loaded web servers, jailbait p-o-r-n videos, stream videos, etc. It also contains archived web pages, web sites that don't renew their domain names, and articles. The government, business, and college research articles are also available.
- Level-3 Web: This is the next stage of Deepweb, which requires a proxy or two or Tor Browser to take access to this part of the Internet. It contains massive jailbait videos, celebrity scandals, VIP gossip, hackers and script kiddies, latest virus information and their source codes, raid information, Microsoft's Data Secure networks, and XSS worm scripting, and various other leaked information.
- Level-4 Web: This is called the chartered Dark Web, which contains hacking groups, head and bounty hunters, illegal game hunters, paid murderers and hackers, illegal trading sites, etc. Advanced covert government researches are sometimes available here but need proxies, VPNs, and Tor browsers to take malicious access to these sites and links. Most of the Internet's black market, which runs on bitcoin, is found in this Web stage.

Another Levels of Web is the lowest level of Deep Web - called the Level 6 (acts as an intermediary between Marianas Web and therefore the Level 7 called THE FOG/VIRUS SOUP). Marianas Web is part of the Darknet is tough to access or browse. It is considered the safest part of the Internet because of its acute privacy.

**Uses of deep web (many of the services or products offered are illegal or crimes in many countries):**

- There is a large amount of information, which focuses on a precise subject.
- Holds a large amount of information that is not available on the visible Web.
- It allows users to find a specific date and time-based web pages and websites.
- Allows finding precise result or answer to a particular question.
- Improve the security and privacy rights of citizens by mass surveillance.
- Obtain whistleblowing and news leaks.
- Sale of restricted products on dark-markets.

**Ethical users of the DarkNet:**

- If users can dig deep and browse deeper, there is exciting information regarding past and present experiments and research.
- Some organizations and security researchers claim that 'Deep Web' has higher quality and in-depth articles on different topics than Surface Web. Search engines like IPL2, Duckduckgo, Infomine are used to find them.
- Ethical hackers and security researchers use these dark sites to learn about how to create viruses and information related to hacking, find a community of hackers from elite hackers to script kiddies, and learn from them via chat-rooms and discussions.

**How Access to the DarkNet safely:**

- Use Proxy servers or programs (such as Tor Browse project https://www.torproject.org/ ).
- Turn off all plug-ins before taking access to the Dark Web.
- Vertical and Split searching.
- Keep distance from links and things that seems remotely criminal or suggestive.
- If your computer is connected through a webcam, disconnect it, obstruct it, or shut down that webcam.
- Use safe, private network connections to gain access to these sites.

**Accessing the Deep Web:**

- .onion: is a domain host suffix which designates an anonymous hidden service which can be accessed via Tor. The purpose of using such a system is to make information more difficult to detect, whether by one another, by an intermediate network host, or by an outsider.
- -.onion addresses are 16-character non-mnemonics hashes comprised of characters and numeric strings.
- Tor Browser: This protects deep web browsing users by bouncing the communication and the IP address around a distributed network? It also prevents tracking the physical location of the user. Using this Tor browser, go to google.com and search for 'Hidden Wiki' and press enter. You'll see the 1st few links. Opening those single links will lead users to a list of links that lay on the dark Web.

**References:** Ethical Hacking, Cibersecurity, TutorialsPoint, MygreatLearning, Coursera, Portal-Offensive.

misuse of the information in this document can result in criminal charges brought against the persons in question. The authors will not be held responsible in the event any criminal charges be brought against any individuals misusing the information in this document/tools to break the law.

The examples, tools, tests or any other activity shown or suggested in this document should NEVER be carried out outside the private network created for this purpose, since criminal and/or punishable responsibility may be incurred.