Exercise 2 - Open Source Intelligence

For each exercise (except the setup Exercise 2.1), you have to prepare a summary report of your activities. This summary report should include:

1. What tools did you use with which options.
2. How did you connect different tools to achieve specific goals.
3. A summary of your findings.

Exercise 2.1 Setup of your environment:

1. Download and install a current version of VMware Player `https://www.vmware.com/de/products/workstation-player.html`. As there are known problems with Ethernet on Virtual Box, it is recommended to use VMware Player.
2. Download a current version of Kali Linux from `https://www.kali.org/` for VMware.
3. Update or install fierce on your Kali Linux VM.
4. Update or install recon-ng on your Kali Linux VM.
5. Update or install metagoofil on your Kali Linux VM.
6. Register (free) accounts at `https://shodan.io` and `https://intelx.io`.
7. You have to add API keys to at least recon-ng for some of the modules.

Hint: There might be other search engines which you might need to register for or tools that you could to install.

Exercise 2.2 Public network enumeration:

1. Use the tools and search engines available to you to make a list of hosts of the University Albstadt-Sigmaringen. The list should include at least:
   a) domain names
   b) IP addresses
   c) open ports
   d) operating system, if the information is available
   e) running services at the open ports, including their version, if that information is available
   f) known vulnerabilities, if any
2. For each IP address you should try to find out if the host is operated by the University Albstadt-Sigmaringen or a third party.
3. If you used a search engine (e.g., shodan.io) for querying hosts, check if the information is still valid or if it is outdated. (Note: Limit your nmap activity to just a few hosts, do NOT scan all found hosts).

Hint: You should combine different tools (fierce, different recon-ng modules, etc.), data sources (DNS, whois, etc.) and search engines (google, bing, shodan.io, etc.).

Exercise 2.3 Account, email and password searching (do NOT include full email addresses, passwords, etc. in your report):

1. Login to intelx.io, then try to figure out, if a password for one of your personal email addresses has been leaked. If you are logged in to intelx.io, it might also be possible that some of your passwords is available without even being hashed!
2. Make a list of mail addresses of the University (or your favorite company) (there are specific search engines for that, e.g., `https://phonebook.cz/`) and check for leaked passwords on intelx.io.
3. Try to figure out the real name behind one or two of the email addresses and connect social network or other profiles to the person (Facebook, Linkedin, Instagram, github etc.).

Exercise 2.4 Metadata analysis:

1. Use the tools metagoofil and exiftool to seach and download for specific types of documents (JPGs, PDFs, PPT, etc.) and search for interesting information (e.g., again on the Universitys domain hs-albsig.de). Especially useful information might be, but is not limited to:
   a) Tool versions (and creation dates)
   b) User names
   c) Geo locations
2. For each category of information, specify, why you think that information would be usefule (Example: specific tool versions might reveal known vulnerabilities).