**Assignment 1 (Due Date 07 August)**

**Description**

Create a tool in Python that can automate the "Information Gathering" stage by using different python modules together.

Given a domain "company.com" your tool should do the following:

* use the WHOIS module to get domain information (<https://pypi.org/project/python-whois/>)
* Use dnspython to run DNS queries to get the (A, MX, NS DNS records ) (<https://www.dnspython.org/>)
* Use the requests library to bruteforce subdomains.
* Use the requests library to do directory bruteforcing

Use the python argparse to receive the user arguments from the CLI. The user should input a domain and a wordlist to be used for bruteforcing.

**Deliverables**:

* Working Code with documentation for each function, classes.
* The criteria for the grading will depend on code functionality, readability, documentation.

**Assignment 2 (Due Date 14 August)**

**Description**:

Choose from one of the TryHackMe challenges below:

* BasicPentesting
* RootMe
* AgentSudo
* SimpleCTF

**Deliverables**:

Submit a full report after solving the challenge using the report sample from hackthebox

<https://www.hackthebox.com/storage/press/samplereport/sample-penetration-testing-report-template.pdf>

Make sure to include an Executive Summary, use screenshots and document your findings. Remember to show your work.

If you wish to do another challenge, please submit it to me and I will review it.

The challenge must be a CTF and not a walkthrough.

**Assignment 3 (Due Date 20 August)**

Go on root-me or any website, pick 3 reverse engineering challenges and solve them.

The 3 challenges have to come from the exact same website.

Document the solution in a PDF and send it (text + screenshot).

Demonstrate the cracking of at least one of them using x64dbg and IDA.

Techniques:

1. patch the file on disk
2. patch the process in memory:
   1. changing the EFLAGS (ZF, ...)
   2. changing the value of the register (e.g EAX)
   3. changing the instruction
3. keygen or find the right answer.