CS 410: Web Security
A0: Labs

For these exercises, you only need to provide what is asked in the description. (There is no need to describe a vulnerability, the exploit, and prevention techniques)

**Indirect reconaissance**
- Run https://www.pdx.edu and https://oregonctf.org/ through the sites below
  - [https://observatory.mozilla.org/](https://observatory.mozilla.org/)
  - [https://builtwith.com/](https://builtwith.com/)
- Answer the questions below
  - How do the two sites differ in what they find out about each site?
  - Provide a screenshot of the [https://www.pdx.edu](https://www.pdx.edu) output

**Direct reconaissance**
- Set up pentest-vm
  - Log into console.cloud.google.com
  - Create a new project labeled (cs410fall17)
  - On Menu, find “Cloud Launcher” and “Compute Engine” and pin them to the top
  - Click on “Compute Engine” and wait for it to be enabled
  - Click on “Create”
  - Create a new instance
    - Name: pentest-vm
    - Zone: us-west1-b
    - Machine type: micro
    - Boot disk: Ubuntu 17.04
  - Click on “Create” and wait
  - `ssh` into new instance and perform the following
sudo apt-get update
sudo apt-get install wfuzz nmap -y

- Use Google Cloud Launcher to set up several web server VMs
  - Zone: us-west1-b
  - Machine type: micro
  - Deselect “Allow HTTPS traffic”
  - Visit the landing page for each VM to ensure it has been deployed properly
  - Note the “Internal IP address” of each instance
  - VMs to bring up
  - ssh into each instance
    - Find where each server pulls its configuration from via a “ps -ef | grep apache” or “ps -ef | egrep nginx”
      - apache2 will use httpd.conf
      - nginx will use nginx.conf => bitnami.conf
    - From the conf files, identify where the DocumentRoot (apache2) or / (nginx) folder resides and cd into it
    - On the lampstack and nginxstack VMs, create directories named secret, files, admin (via sudo mkdir).

- Use Google Compute Engine, bring up a web server on a Windows Server 2012 R2 instance
  - [https://cloud.google.com/compute/docs/quickstart-windows](https://cloud.google.com/compute/docs/quickstart-windows)
  - To connect to your instance, use an RDP client
    - remmina on linuxlab machines
- Google Chrome’s RDP for Google Cloud Platform extension (does not seem to work on Chromium)
  - Skip the clean-up step
  - Connect to your Windows Server 2012 instance and install the IIS component
    - [https://cloud.google.com/compute/docs/tutorials/basic-webserver-iis](https://cloud.google.com/compute/docs/tutorials/basic-webserver-iis)
    - Note: Windows PowerShell can be accessed in the upper right corner under “Tools”

![PowerShell Menu]

- Within PowerShell, change directories into the webroot folder (cd)
- Create directories named secret, files, admin using mkdir
  - Note that you may need to do “sudo mkdir …” to be able to make the directory
- Create directories of your own using words of your choice
• Use wfuzz and nmap to automatically scan directories on each of the 4 web servers using their Internal IP address
  ○ wfuzz -c -z file,wordlist/general/common.txt
      --hc 404 http://w.x.y.z/FUZZ
  ○ nmap --script http-enum w.x.y.z
  ○ Answer the following questions
    ■ Do the nmap and wfuzz tools get similar results for each site?
    ■ Provide screenshots of each tool’s output on the Windows web server VM
• Stop all VM instances when complete