MUNI

FI

Introduction to Penetration Testing Practice Seminar

PA211 Advanced Topics of Cyber Security

October 11, 2022

Ádám Ruman, Jan Vykopal

Goals of this seminar

- Become **acquainted** with:
  - **System under test** (target) in the pentesting sandbox.
  - **Your teammates.**

Pentesting Sandbox

Pentesting sandbox – Preparation

1. Run `pa211_setup` command – only on school computers (nymfe).
2. Clone a new repository with the target (pentesting sandbox):

   https://gitlab.fi.muni.cz/cybersec/pa211/pentesting.git
3. Change directory to `pentesting`. This directory contains `Vagrantfile`.
4. Run `vagrant up`.

Pentesting sandbox – Description

- **Two hosts** in the same LAN 10.1.26.0/24.
- **Kali Linux** (`attacker` machine) is here for you (pentester).
- Server machine runs the **target system**.
- You can access the target (server) from Kali (attacker) via **CLI** (SSH) or **GUI** (VirtualBox) console.
- You can also access **web applications at the target** using SSH port forwarding (see next slide).

Pentesting sandbox – Local browser access

1. Set up port forwarding to be able to use your browser at the host to access the target:

   ```
   vagrant ssh server -- -ND 9050
   ```

   Let it run in the background.

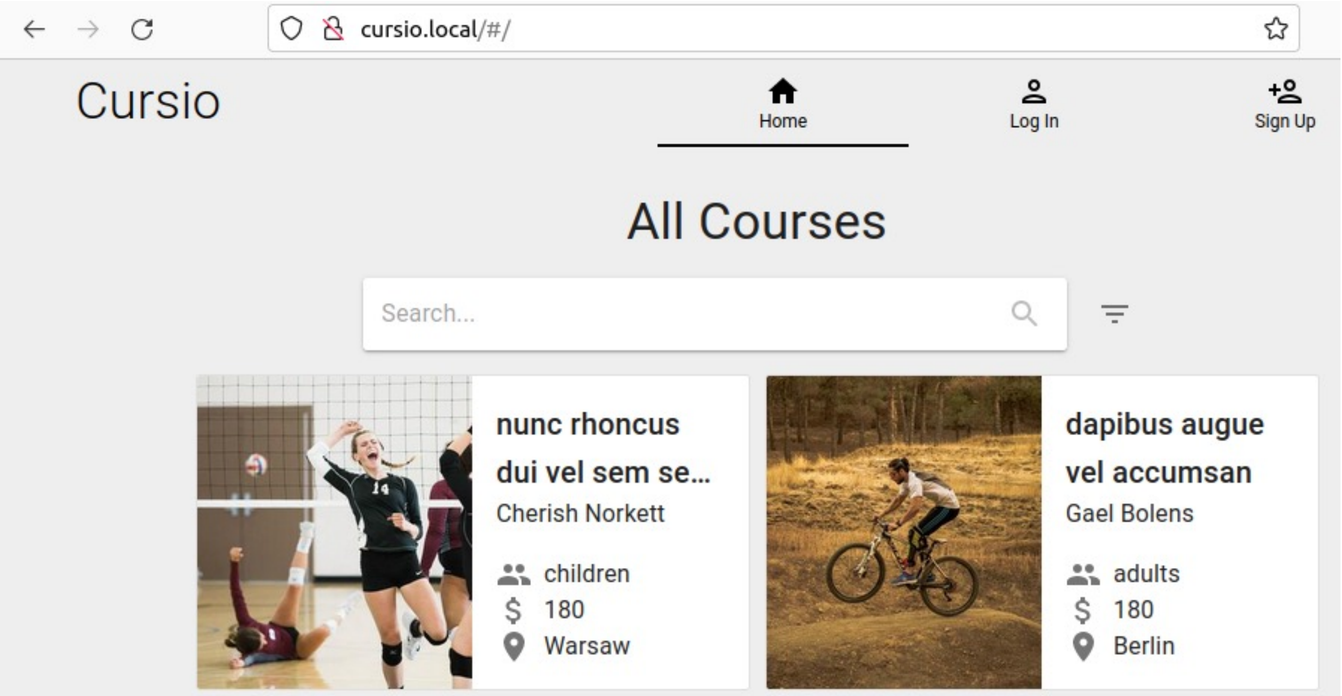
2. Set up Firefox **at your host** (nymfe) steps in README.md.

   If you cannot connect to Cursio, check you have set the SOCKS proxy in Firefox according to the screenshot in the README.

Pentesting sandbox – Check the target app

Verify that you can **access the target** at http://cursio.local using Firefox at your attacker or your local host.

1. Open GUI console and log in the Kali using `kali` as username and password. Open Firefox at Kali and visit Cursio.
2. Or, if you use local browser access: open Firefox at your local and visit Cursio.



Pentesting sandbox – Check networking

- Kali Linux has IP 10.1.26.23.
- The target has IP 10.1.26.9.
- Check whether you can ping *cursio.local* from the attacker:

```
vagrant ssh attacker
```

```
ping cursio.local
```

Troubleshooting

- **Destroy** and (re)**create** a virtual machine:

  -
    ```
    vagrant destroy <machine_name> -f
    ```

  -
    ```
    vagrant up <machine_name>
    ```
- If Ansible provisioning **fails**, **rerun** tasks with:

  -
    ```
    vagrant provision <machine_name>
    ```
- List **open ports** the on server:

  -
    ```
    sudo netstat -tulpn
    ```

The target

Cursio application – I

- Cursio is a **web portal** for offering and searching various **courses and free-time activities**.
- **Users** can create and manage their user accounts, including changing their e-mail or password and editing their profile picture and user description.
- **Registered users** can create courses and sign up for courses created by other users.

Cursio application – II

- Each course is classified by target age group, location, and general type.
- Courses are filtered by their categories or by using a full-text search feature.
- The **front-end application with the API server** provides the most significant **attack surface** of the sandbox.

Scope of the pentest

- The server machine hosting Cursio.
- IP address 10.1.26.9 within the pentesting sandbox.

Rules of engagement

- Each of you is provided with a testing instance (this will NOT happen in practice).
- Using social engineering is forbidden.
- If you break your sandbox, feel free to recreate it using `vagrant destroy` and `vagrant up`.
- Do not share your findings with other teams.
- Do not share the sandbox outside the class.
- Contact person: Ádám Ruman <469068@muni.cz>

Your task for today

- **Familiarize yourselves with the pentesting sandbox.**
- You are expected to **interact with the application** and **observe** various **features, API calls**, and **user roles**.
- Note the sandbox contains **more targets than the web portal.**
- Remember, you are a team. **Work in a team, and share what you find with other team members.**
- Next week: actual pentesting (using tools at Kali).

Recommendation for teamwork

- Create a shared document for your findings
- Establish a secure communication channel for your team:
  - MS Teams, Keybase, …
- Agree on a time window for working outside the class (will be necessary next week)

How was it today?

Please fill in an **anonymous** exit ticket:

https://muni.cz/go/pa211-22-05

MUNI

FI