Bootcamp Intro PPT

Session 1.1 Security 101 I

Tuesday September 1, 2020 / 6:30-9:30 PM
Zoom Link: https://zoom.us/j/2246200754
Zoom Password: 508637

Introduction

- **Krishana Anderson**
  - **Office Hours:** 12-5 PM / **M-Th**
  - No more than **8 absences**.
  - No more than **2 missed or incomplete assignments**.
  - Hold at least a **70% average** on homeworks and pojects.
  - Participate in all projects.
  - Balance paid in full.
  - Academic Honesty.
  - **Drop Period** is the first week of class (including transferring section).
  - **Drop Deadline** is **Tuesday, September 8, 2020**.
  - Speak with Erin and Robert about any homework issues.
  - **CompTIA**: (Weeks 10-13)
    - Access to CompTIA CertMaster Practice Practice for Security+.
    - CompTIA Security+ Exam Voucher. (Good for 12 months.)
  - **Ways to get support**:
    - Speak up, reach out, and **attend office hours**.
    - There are 30 minutes of office hours after class.
    - Form study groups.
    - Use a **support ticket** in Bootcamp Spot to **request a tutor**. (1 hr/week)
  - Access to career services.
- **Erin, Robert, Siddartha, and Srividhyaa (Instructors)**
  - Assignments will be made available by the 2nd session of each weekly topic.
  - Assignments open until the end of the consecutive weekly topic.
  - Grade deductions for late homework.
  - Locked homework require tutoring fo submission.

    - Surprise Quiz Games, "Cold Calls".
    - Extra Credit Assignment.
    - Assignment exmpansion.
    - Hints. (Coughs when something is important.)
    - Ask good questions, take good notes.
    - Utilize resources.
    - Have a good attitude. (Be persistant.)
    - Teamwork. (Grades are shared - weakest link is the highest grade mark.)
    - Respect.
    - Class Goals
- **Why security and cyber-skills is important/relevant today.**
    - Explosive growth in dependence on IT
    - More user on conencted devices.
    - Better tools, bigger damage.
    - Significant investment by bad actors.
    - Dire shortage of skilled professionals.
- **Defining Cybersecurity**:
    - Assessment of threats and migitation of risks.
    - Example hack: Stuxnet, 2009. Malware worm distributed on USBs.
    - **Castle Model** vs **layers of security** (that assume a breach) to protect an **asset**, typically **data**.
- **Course Overview**:
    - **Goals**
        - Threat assesment.
        - Risk mitigation.
    - **Daily Routine**
        - Set objectives.
        - Brief background lecture.
        - Instructor demonstrations.
        - Thought exercises.
        - In-class skill builder.
        - Project work.
- **Tips**:
    - Curiosity.
    - Embrace being a beginner.
    - Find your community now.
    - Put in the hours.
- **Attacking the Wall Activity:**
    - Users and Admin **<-->** Web Login **<-->** Server **<-->** Data
- **Defining Attack Strategies:**
    - Social engineering.

    - Phishing.
    - Credential reuse.
    - Malware.
    - Man-in-the-middle-attack.
    - Sniffing packets.
    - Stolen hardware.
- **Website Attacks:**
    - Brute force strategy.
    - Code-injection.
    - Faulty session management.
- **Server Attacks:**
    - Malicious software.
    - OS exploits.
- **Database Attacks:**
    - Unpatched database.
    - Lack of segregation.