Introduction to Computer Security

Final Project

Contents

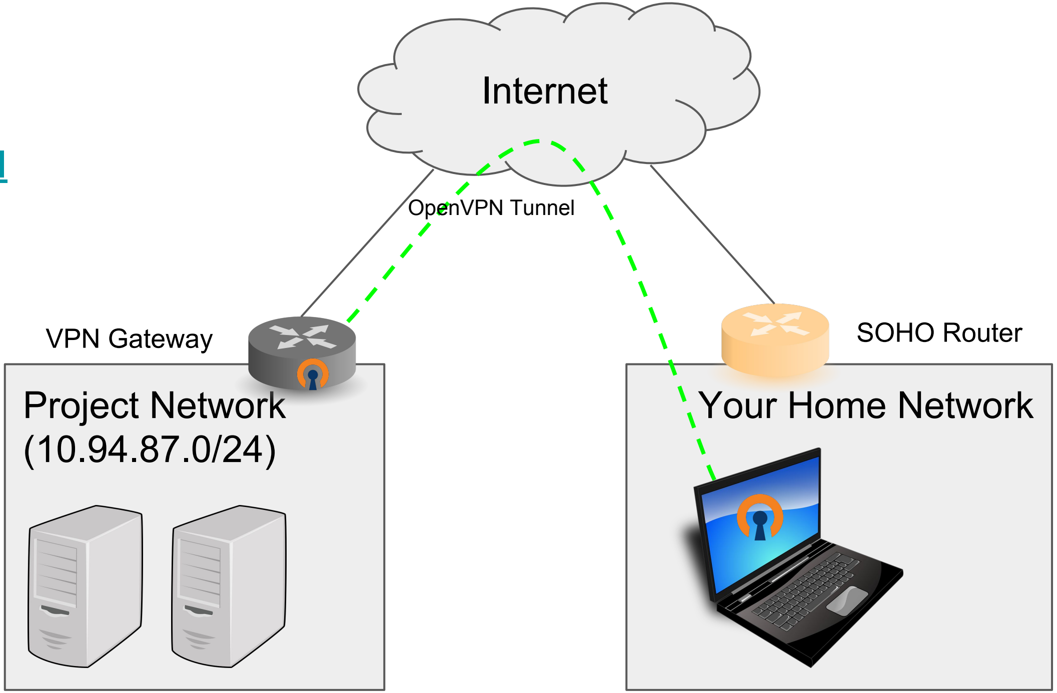
- Introduction
- Project Environment
  - VPN Tunnel Setup
- Two Challenges
  - Web Challenge
  - Wireless Forensics Challenge
- Grading
- Schedule

Introduction

- Two challenges to test your ability to hack a system
- Gather the tokens when you’ve successfully exploited the system
  - 12 tokens in total, 6 for each challenges
- All the activities are contained in a private network
  - **DO NOT** try to exploit the system outside the private network
- The rankings and additional announcements (including additional hints) will be shown on the dashboard
- Keep notes and take screen dumps of the steps you take during the process
  - You’ll need them for the write-up
- **DO NOT try to DDoS the server, or you’ll get BANNED**

Project Environment (1/3)

- All of the hosts and targets reside in a private network
  - 10.94.87.0/24
- Tools
  - OpenVPN (2.4 up)
    For Win x64: https://url.fit/ZHQeI
    For Win i386: https://url.fit/ZQttj
- Configuration
  - Download

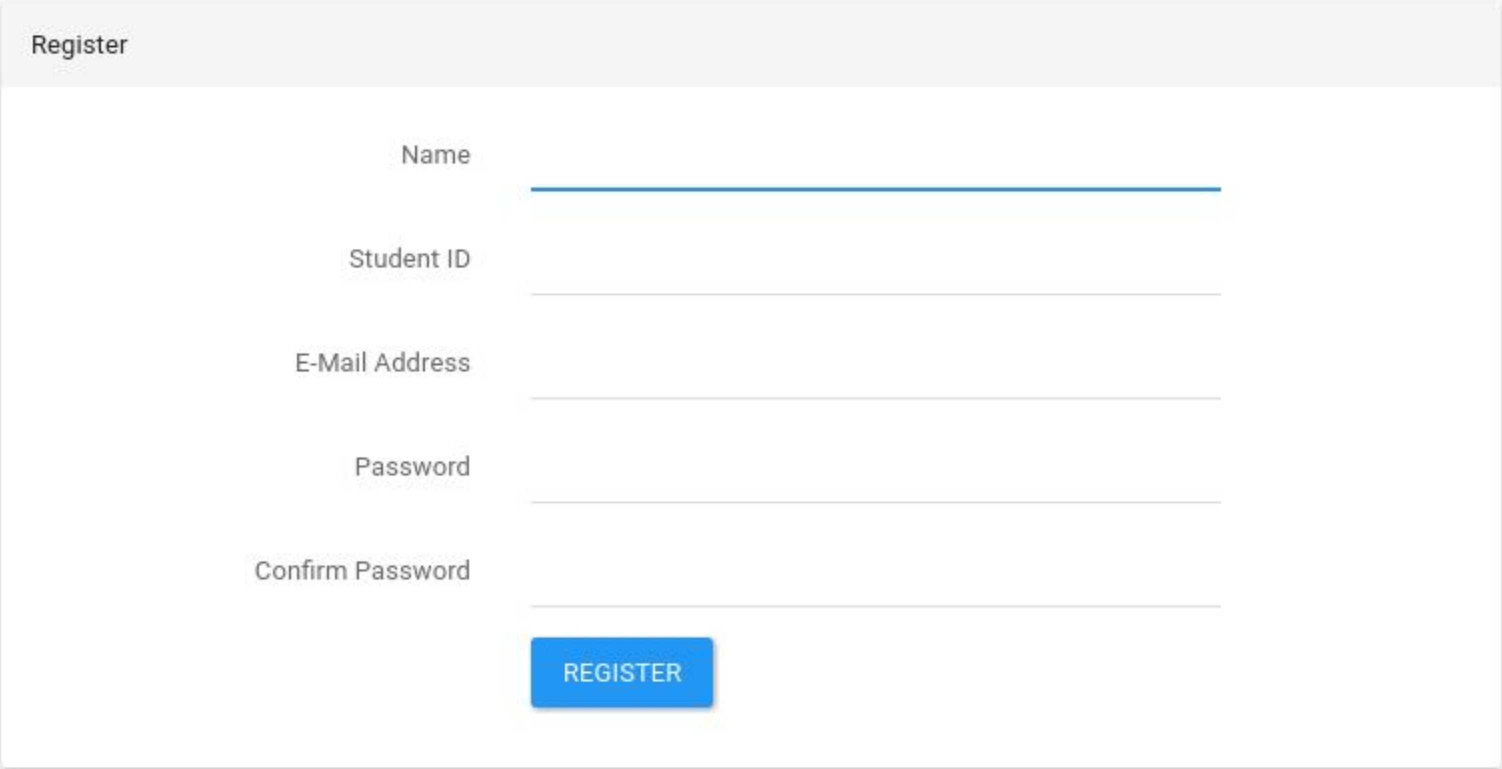


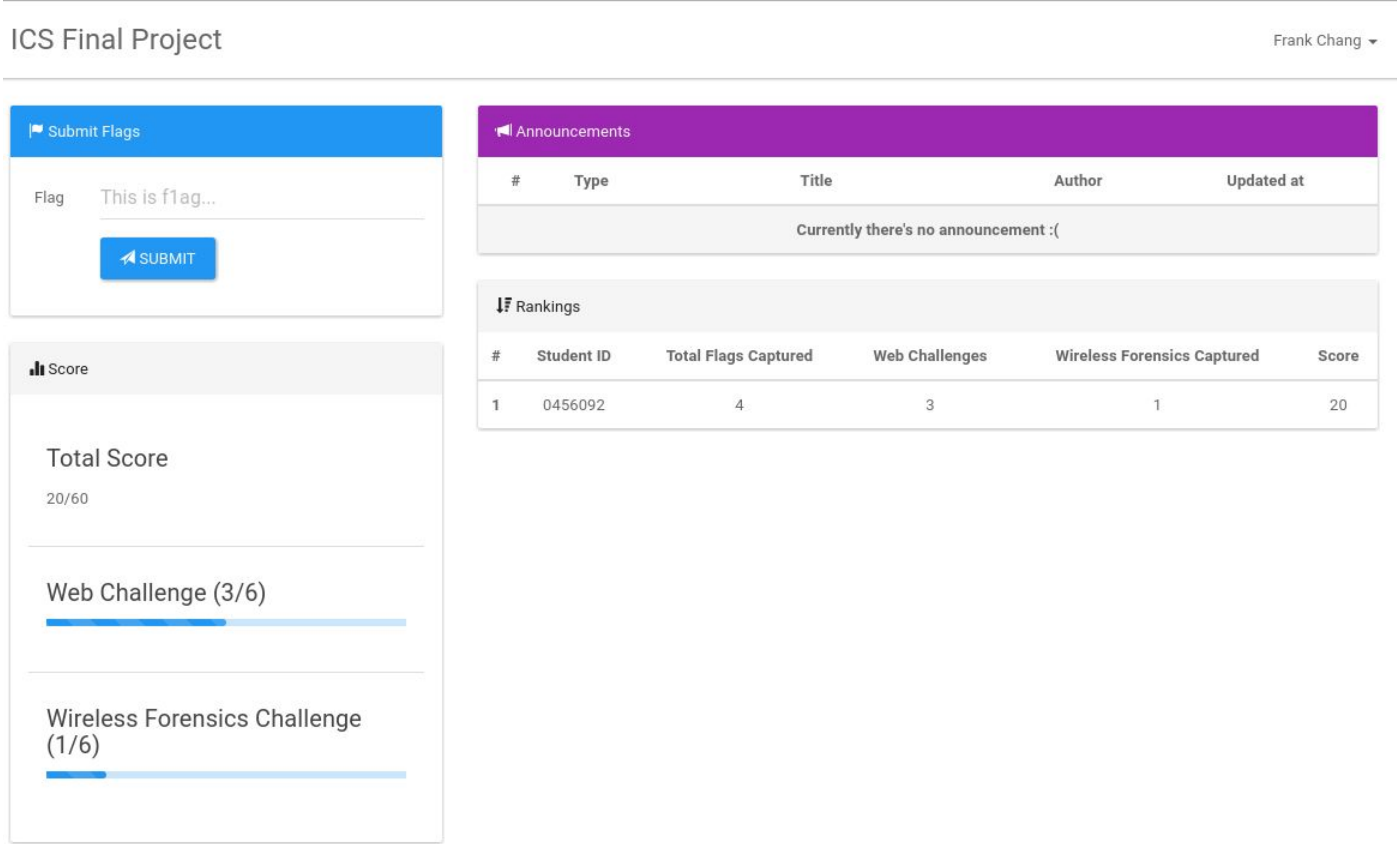
Project Environment (2/3)

- VPN Tunnel Setup Instruction
  1. Download and Install OpenVPN
     - apt install -y openvpn (Debian-based)
     - yum install openvpn (RedHat)
     - pacman -Sy (archlinux)
  2. Download Configuration
  3. Start the VPN tunnel
     - sudo openvpn --config <path to conf. file> --daemon
  4. DNS Settings
     - Modify /etc/resolv.conf
     - nameserver 10.94.87.1
  5. Check the connectivity
     - ping dash.board

Project Environment (3/3)

- Dashboard
    - Located at https://dash.board
        - It’s only reacheable when you’re connected to the private network
    - Your Score
    - Rankings
    - Token Submission
    - Problem Report
    - **Announcements**
        - Additional hints are released from time to time


Register
Name
Student ID
E-Mail Address
Password
Confirm Password
REGISTER



Submit Flags

Flag: This is f1ag...

Announcements

#	Type	Title	Author	Updated at
Currently there's no announcement :(				

Rankings

#	Student ID	Total Flags Captured	Web Challenges	Wireless Forensics Captured	Score
1	0456092	4	3	1	20

Score

Total Score

20/60

Web Challenge (3/6)

Wireless Forensics Challenge (1/6)

Project 1. Web Challenge (1/2)

In project 1, you'll be given instructions on how to find out the potential target and use tools to exploit the flaws in a web application

- Tools for reference
  - nmap
  - sqlmap
  - hydra
  - firefox (or any browser you like)
    - hackbar
    - temper data
    - header modifiers (you may choose any one you want)

Project 1. Web Challenge (2/2)

- Initial Instructions and Hints
    1. Find out where the potential targets reside (Hint: nmap)
    2. Gather system information about the potential targets
    3. What people do to avoid search engine crawler from crawling importand information
    4. Discover SQL injection flaw and exploit manually or with tools
    5. Find out possible management portal and try to login

Project 2. Wireless Forensics Challenge (1/2)

In the wireless forensics challenge, you'll be given a packet trace captured from a cyber cafe with a wireless dongle, try to analyze and crack it

- Tools for reference
  - Aircrack-ng suite
  - Wireshark
  - GnuPG
  - fcrackzip
- Files (Accessible from the dashboard)
  - trace.pcap

Project 2. Wireless Forensics Challenge (2/2)

- Initial Instructions and Hints
    1. The wireless traffic is encrypted
    2. Analyze the decrypted traffic, find out the application protocols used
    3. Try to extract login credentials and files from the traffic
    4. Decrypt the encrypted text with the PGP key you found

Grading

- Tokens Gathered (60%)
  - 12 tokens, 5 points each
  - Do not share the tokens with your classmates
- Write-up (40%)
  - Write as detail as possible
    - How did you retrieve the flag?
    - What is the cause of the vulnerability?
  - Provide screen dumps on critical steps
  - Submit your write-up to E3 with filename **final_writeup_${student id}.pdf**

Schedule

- Practice
  - 2018/05/22 (Tue) ~ 2018/05/28 (Mon)
- Q & A
  - 2018/05/28 (Mon) @ 10:10
- Time of start
  - 2018/05/28 (Mon)
- End of token submission
  - **2018/06/04 (Mon) @ 23:59**
- End of write-up submission
  - **2018/06/04 (Mon) @ 23:59**

Any Questions?