Capture-The-Flag Hacking Contest

•••

June 9, 2018
tbl

WHOAMI

- Senior Security Consultant at SCHUTZWERK GmbH
  - Technical and Conceptual Security Assessments
  - Organisation of CTF Hacking Contests

- Lecturer Hochschule Aalen
  - “Penetration Testing und Computerforensik”

- Contact
  - tblaesing@schutzwerk.com
    FFF2 800A 8959 7356 C896 6E16 8E47 0724 75FE 5EDE

Agenda

- Introduction
- Overview
- Rules

Introduction (or “Capture the whaaat?”)

- Capture The Flag (short CTF) is a traditional (military) outdoor game where the objective is to capture an other team's flag (or marker)

- In IT security field, CTF contests are usually designed to serve as an educational exercise to raise experience in attacking and securing a virtual machine, application or embedded device

- Widely used kinds
  - Attack/Defense
  - Jeopardy
  - Mixed

Attack/Defense-Style Contests

- Each team is given a virtual machine, connected to an isolated network

- There are different (self-written) services running on each machine
    - Game Bot stores flag into service (e.g. web forum)
    - Game Bot comes back at a later time and tries to retrieve the flag again
    - When the flag is still there and not already sent by another team to the game bot you’ll get a defense point for the services
    - If you captured a flag from another team’s service and submit it to the game bot you’ll get an attacking point for the service

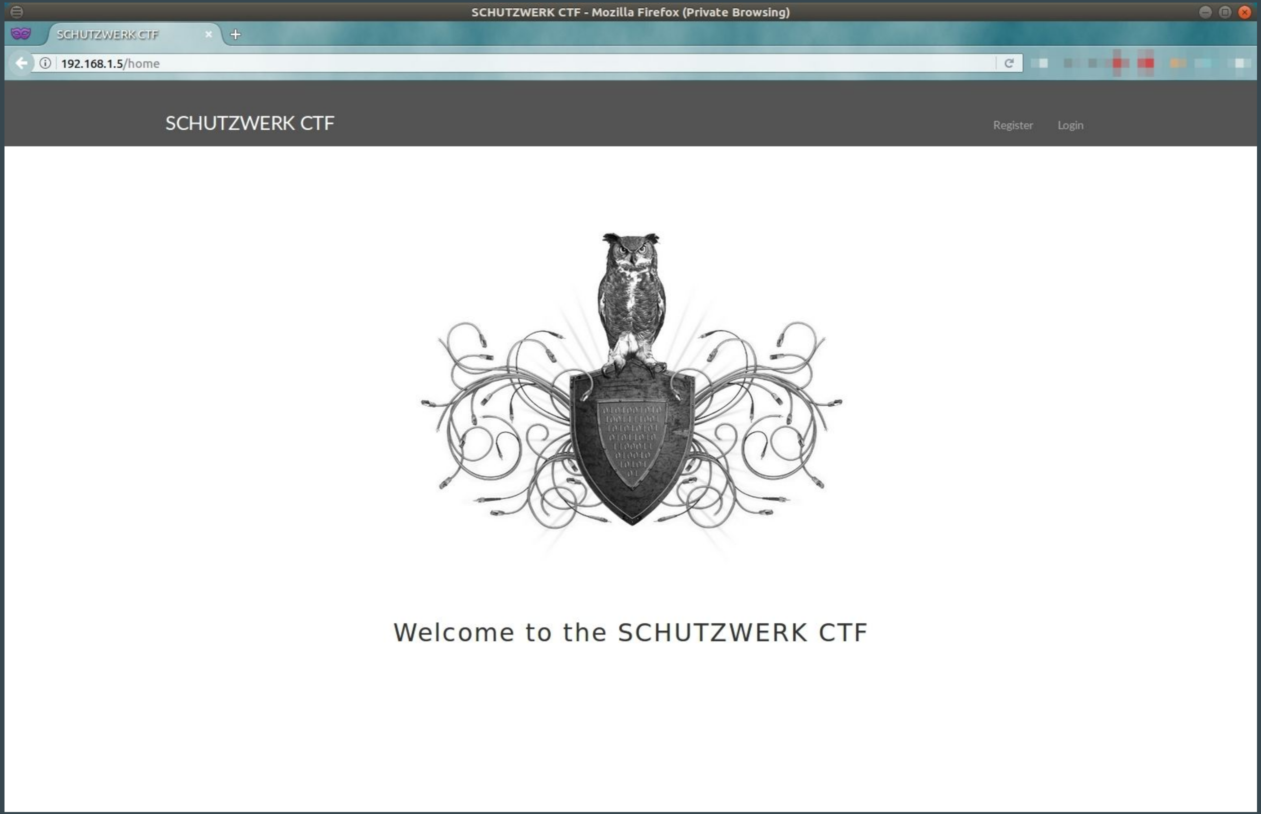
Jeopardy-Style Contests

- Questions based competition where the answers are simple strings (Flags)
- Multiple categories each of which contain several questions and challenges
- Usually there are different amount of points for different difficulties

Contest Overview

Start Screen

- Open a browser, navigate to https://192.168.1.5

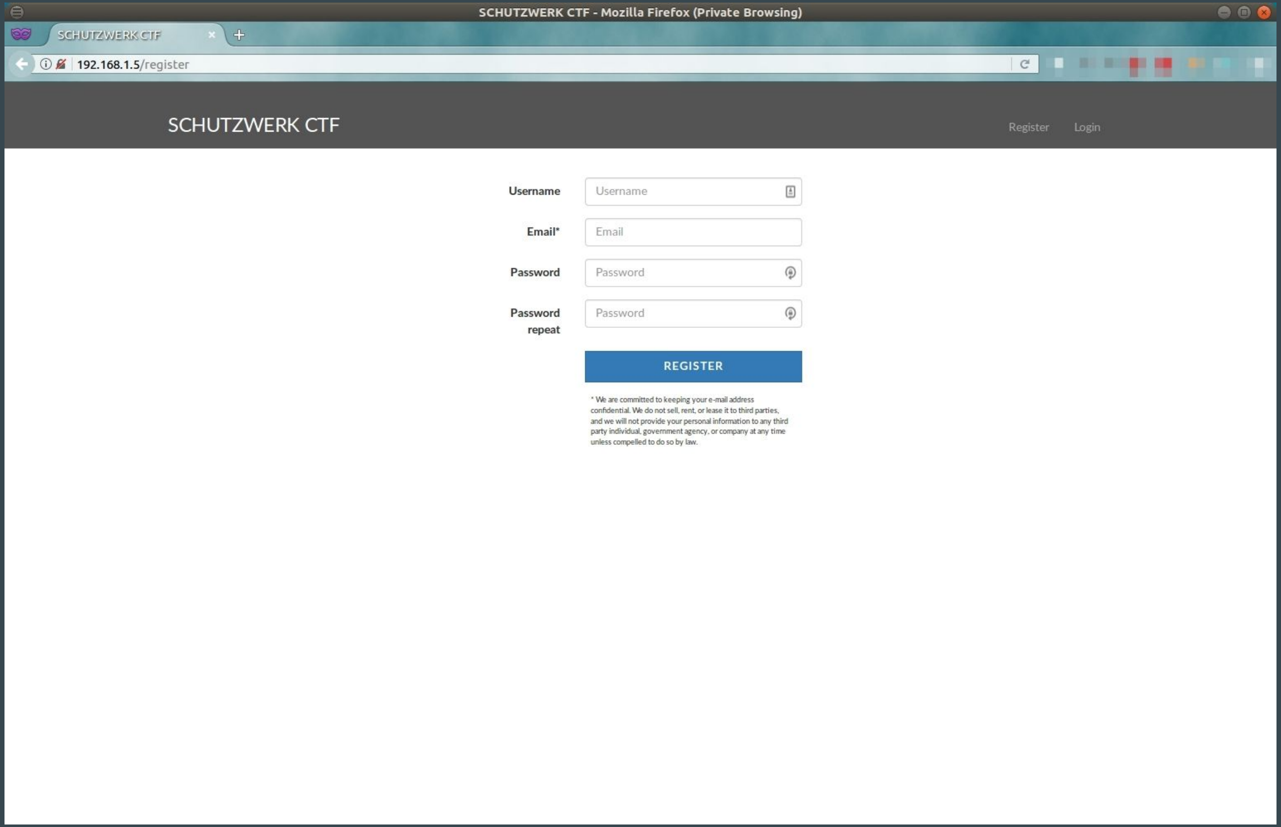


SCHUTZWERK CTF - Mozilla Firefox (Private Browsing)

Welcome to the SCHUTZWERK CTF

Register Screen

- Use valid
  - Username
  - E-Mail
  - Password

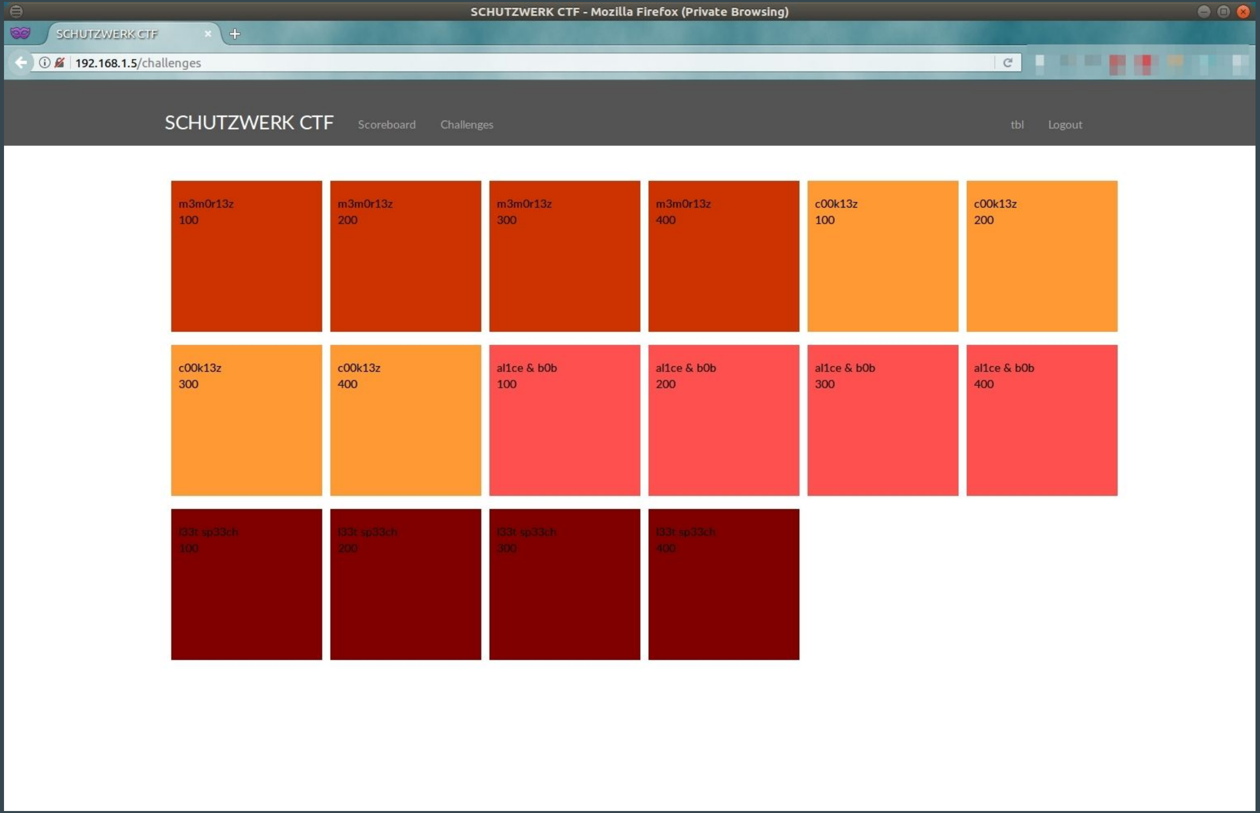


Username	Username
Email*	Email
Password	Password
Password repeat	Password

* We are committed to keeping your e-mail address confidential. We do not sell, rent, or lease it to third parties, and we will not provide your personal information to any third party individual, government agency, or company at any time unless compelled to do so by law.

Challenge Screen

- Once registered you can login to the CTF platform and start solving challenges :)



m3m0r13z
100

m3m0r13z
200

m3m0r13z
300

m3m0r13z
400

c00k13z
100

c00k13z
200

c00k13z
300

c00k13z
400

al1ce & b0b
100

al1ce & b0b
200

al1ce & b0b
300

al1ce & b0b
400

l33t sp33ch
100

l33t sp33ch
200

l33t sp33ch
300

l33t sp33ch
400

Rules

Rules I

- This is a non-public Jeopardy-Style CTF Hacking Contest
  - Please don't create write-ups or publish any solution
  - The CTF network is isolated from all other networks
- There will be four challenges in each category
  - Security Knowledge (H0m3w0rk)
  - Cryptography (Al1c3 & B0b)
  - Coding (L33t Sp33ch)
  - Forensics (m3m0r13z)
- Each flag follows the following pattern:

  SW{[a-zA-Z0-9]+}
- Peoples are ranked by score
  - First three in list get rewarded

Rules II

- All challenges are designed to be solved manually/without automated tools
- There's no need to use automated and aggressive tools, such as
  - Sqlmap, Acunetix, Nikto, Nessus, etc pp
  - If you are being detected using such tools, you will be banned and disclosed from contest

- People that show inappropriate behavior will be disqualified immediately
  Do not ...
  - ... attack the CTF infrastructure. All targets are explicitly outlined.
  - ... attack other People.
  - ... create duplicate accounts.
  - ... share hints or solutions during the event.
  - ... play unfair in any way.

Have Fun!

PDF of the slides: https://goo.gl/vGUvp3