SANReN
South African National Research Network

CSIRT
Information Security

Cyber Security Challenge

csc@sanren.ac.za

cybersecuritychallenge.ac.za/

science & technology
Department:
Science and Technology
REPUBLIC OF SOUTH AFRICA

6th SIG-ISM Workshop: 12 February 2018

CSIR
our future through science

Where it began…

- Annual CHPC conference student cluster competition – building mini-HPC clusters – came 1st every year bar one since 2013
- SANReN track @ 2017 conference > can we do something similar?
- How about a “hot & sexy” infosec contest?
- A dream since 2009…

Objective

- To provide a safe environment for information security enthusiasts to test their skills
- Test both offensive and defensive skills
- Validate understanding of core information security concepts
- Attract interest and funding
- Human capacity development – identify talent

Preparation

- Research…
- EU Cyber Security Challenge
- Reach out to other NRENs?

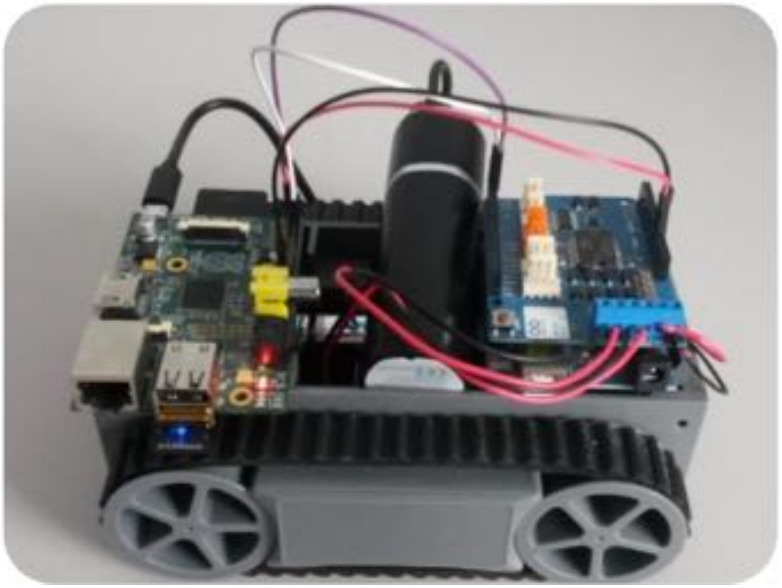
The European Cyber Security Challenge gives young talents an opportunity to pitch their IT security prowess against their peers in a friendly competition. Their skills are urgently needed, if we want to tackle the digital revolution.

CTF ARCHITECTURE

"Every team had their own server with certain vulnerabilities placed by the Hacking-Lab staff. On the one hand everyone had to defend their own server and services against attacks from the opposing teams and on the other hand the teams had to patch vulnerabilities, decipher hidden messages and solve difficult hacking challenges."

7 Jeopardy Challenge: Reverse Engineering

9 Jeopardy Challenge: Robot Fun Challenge



9.2 Goal

Join your laptop to the robot WiFi network. Hijack the robot controller. Navigate the robot to the jury, and make it play a sound file which tells the team name.

8 Jeopardy Challenge: Minecraft

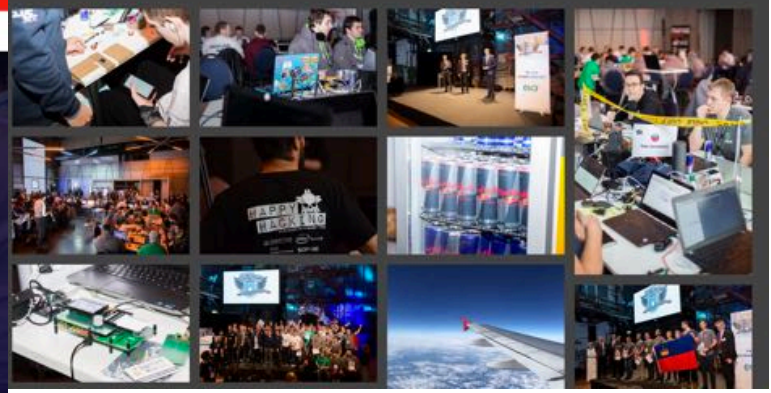
14 Achievement: CEO wants a PR platform based on

CYBER SECURITY CHALLENGE

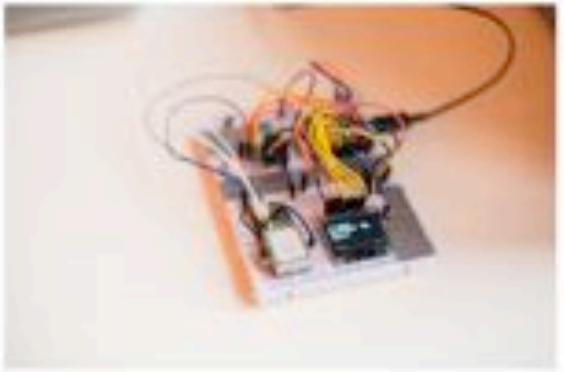
National Competitions

t nur das Hacken, sondern auch das
und der ganze Event 😬

as Team. Wenn alles gut geht dann sind
wir nächstes Jahr in Malaga – Spanien wieder dabei!



European Cyber Security Challenge 2016



Cyber Security Challenge

by NRENs, for students...

SANReN
South African National Research Network

- Information security related contest
- Capture the flag / token (jeopardy-style challenges)
- Hacking web, mobile, cryptography, IoT, reverse engineering, forensics…
- Attack & defend

Aimed at students/hobbyists → new talent

- We'd like to do this! Would you?
- Let's do it together!
- Should we join an existing contest? (e.g. European Cyber Security Challenge (ECSC))
- Hybrid model?
- What about an International / GÉANT-level final event?
- We'd love to hear from you!

TNC17

HACK POwn Attack Defend Sustain Patch Solve

"Every team had their own server with certain vulnerabilities placed by the Hacking-Lab staff. On the one hand everyone had to defend their own server and services against attacks from the opposing teams and on the other hand the teams had to patch vulnerabilities,

Interested ?

csc@sanren.ac.za

"9.2. Goal
Join your laptop to the robot WiFi network. Hijack the robot controller. Navigate the robot to the jury, and make it play a sound file which tells the team name."

Preparation

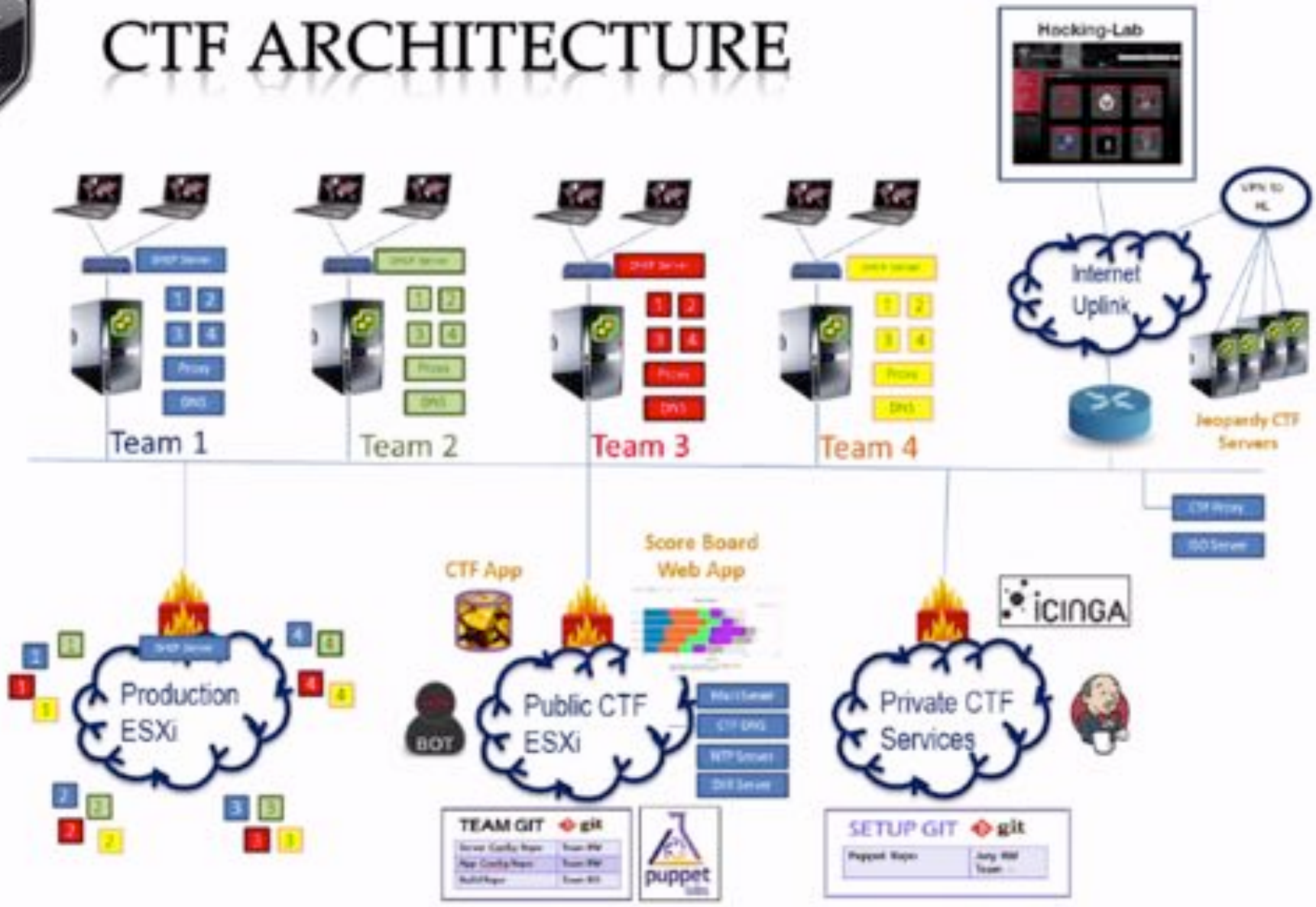
- ~~Research~~
- ~~EU Cyber Security Challenge~~
- ~~Reach out to other NRENs~~
- Hacking Lab = Partner! ☺

What is Hacking-Lab™?

Hacking-Lab is an online ethical hacking, computer network and security challenge platform, dedicated to finding and educating cyber security talents. Hacking-Lab is providing CTF and mission style challenges for international competitions like the European Cyber Security Challenge, and free OWASP TOP 10 online security labs. Hacking-Lab's goal is to raise awareness towards increased education and ethics in information security.

Hacking-Lab is popular: 40'000 users have registered, and numerous universities, organizations and companies are using it for enhancing their classes, trainings, etc.

CTF ARCHITECTURE



TYPES OF CHALLENGES

Malware Analysis

Linux Security

OSX Security

SS7 PBX

Web Hacking

Crypto Puzzles

Secure Programming

Network Security

Penetration Testing

Forensic Analysis

Database Security

Wireless Security

Reverse Engineering

Windows Security

Code Analysis

CTF TASKS


Challenges
1_Achievement
2_Attack
3_Availability
4_Code Patch
5_Defense
6_Jeopardy
7_Powned
GN
GN
JN
EN
What shall I do?
GN Gold Nugget
JN Jeopardy Nugget
EN Evidence Nugget

Are you born in **1992 or later**? Working with computers and networks is your passion and you are not (yet) a security professional? Then the European Cyber Security Challenge is for you! You have to solve security related tasks from domains such as web security, mobile security, crypto, reverse engineering, forensics and more. You have the chance to become a member of the Swiss national team competing against internatinonal teams from all over Europe! ECSC 2017 will take place in Málaga, Spain, 30 October - 3 November 2017. Meet other like-minded people. Make your passion your career.

EUROPEAN CYBER SECURITY CHALLENGE

MALAGA, SPAIN, 2017

EUROPEAN CYBER SECURITY CHALLENGE 2017

London, United Kingdom will be the host of ECSC2018!

Thank you Málaga for hosting the European Cyber Security Challenge!

ECSC2017 took place from **31st October** to **1st November 2017**.

Rank	Country
#1	Spain
#2	Romania
#3	United Kingdom
#4	Norway
#5	Estonia
	Italy
	Cyprus


Home
Score Chart
Team Switzerland
Team Austria
Team Germany
Team UK
Team Romania
Team Spain
Team Estonia
Team Greece
Team Ireland
Team Liechtenstein
8,251
10,643
12,540
14,132
7,658
8,718
6,263
4,881
0
1000
2000
3000
4000
5000
6000
7000
8000
9000
10000
11000
12000
13000
14000
15000
16000
Pwned
Achievement
Jeopardy
Code-patching
Defense
Attack
Availability

ECSC 2017

This 4th edition is performed in **Malaga**, (Spain), the days 31 of October and the 1 of November. The competition can´t be more interesting, because the Spanish team is defending their championship wined the last edition in **Düsseldorf**, Germany.

This ECSC 2017, we dispose:

- A pre-register **program of the conferences**.
- A **recruiting fair** for the young participant talents.
- The **competition** where the 15 countries participate.

Spain revalidates the title of champion of the European Cyber Security Challenge. Congratulations champions!

About ECSC 2018

The European Cyber Security Challenge is a competition where contestants are challenged to solve security related tasks from domains such as web security, mobile security, HW, RF and IoT security, crypto puzzles, reverse engineering and forensics. The points they gain depend on their ability to solve the tasks in a timely manner. Teams are also expected to do a presentation in front of the audience and the jury in the conference room. The objective of this task is to promote the idea that cybersecurity professionals should also have soft skills and the ability to communicate. In 2018, the United Kingdom will be the host of the fifth edition of ECSC. In 2018, we count on 20 European countries, each of them bring their best 10 young and promising talents in cybersecurity.

science & technology
Department:
Science and Technology
REPUBLIC OF SOUTH AFRICA

SANReN CSC 2017, TF-CSIRT Meeting
05 Feb 2018, csc@sanren.ac.za

CSIR
our future through science

So, what can you expect?

Lots of coffee, little sleep and grueling hacking challenges over a period of three days.

Challenges That You Will Face...

Start training yourself to hack, crack, root, exploit and subvert your way to the top of the CTF ladder. Challenges may include Web Hacking, Forensics, Cryptography, Binary Analsis, Password Cracking, Steganography, Reverse Engineering, Mobile Security, Not Getting Enough Sleep and Running out of Coffee. And to make matters worse, you may have to defend your own infrastructure against all the other pesky teams.

```
: void main(String[] args) {
ut.println(" In code we trust ");
```

Skills tested

- Reverse Engineering
- Web Security
- *Network Security*
- Forensics
- Crypto
- *Mobile Security*
- Penetration Testing
- Windows and Linux Support
- Password hash cracking
- ~~Secure code development~~

Challenge Setup

- Preliminary Challenges:
  - 108 preliminary candidates,
  - 29 teams
  - 12 South African Universities.
- Final round
  - 32 Final round competitors, top 8 teams from preliminary round.
  - 4 Day event, ran for 24 hours a day.
- Challenges
  - Hacking Lab Challenges
  - Password Cracking
  - Off-line Puzzle based challenges
  - Social Engineering
  - Pwn the system


Home
About
Membership
Security Events
Dashboard
Reference Projects
How it Works
Chat
Global Scoring
Mobile Services
Download
Jobs
Login / Sign up
SANReN
South African National Research Network
CHPC 2017 Candidates Competition
Challenges
How it works
My running Events
Remote
Topic
Type
Name
Level
Points
Status
Solution
Teacher
Resource
1651 Online NS Lookup Level 1
0/5
1652 Online NS Lookup Level 2
0/15
1656 DownToTheBasement
0/15
2316 Personal Password Saver
0/5
COMPASS SECURITY
My Menu
My Profile
Inbox
My Solution
Teacher

Challenges we contributed

- Hash challenge infrastructure provided by Prof. Barry Irwin. The system works by providing the tool with a seed file of potential passwords. The system generates hashes using these hashes. 11 types of hashes currently supported (bcrypt, descrypt, md5, md5_flip_sha_256, md5_salt, mysql41, nthash, pbkdf2_sha_256, sha1, sha_256, sha_256_salt). The Password hash system has its own scoring system built in. bonus points are rewarded for being the first to solve a particular hash or being the only team to solve the hash.

Hacking-Lab challenges

- The majority of the challenges we requested from them were file based or stand alone to reduce network usage, but they do offer full network range challenges, with various virtual infrastructure components.

+ To Hacking-Lab

Our additions

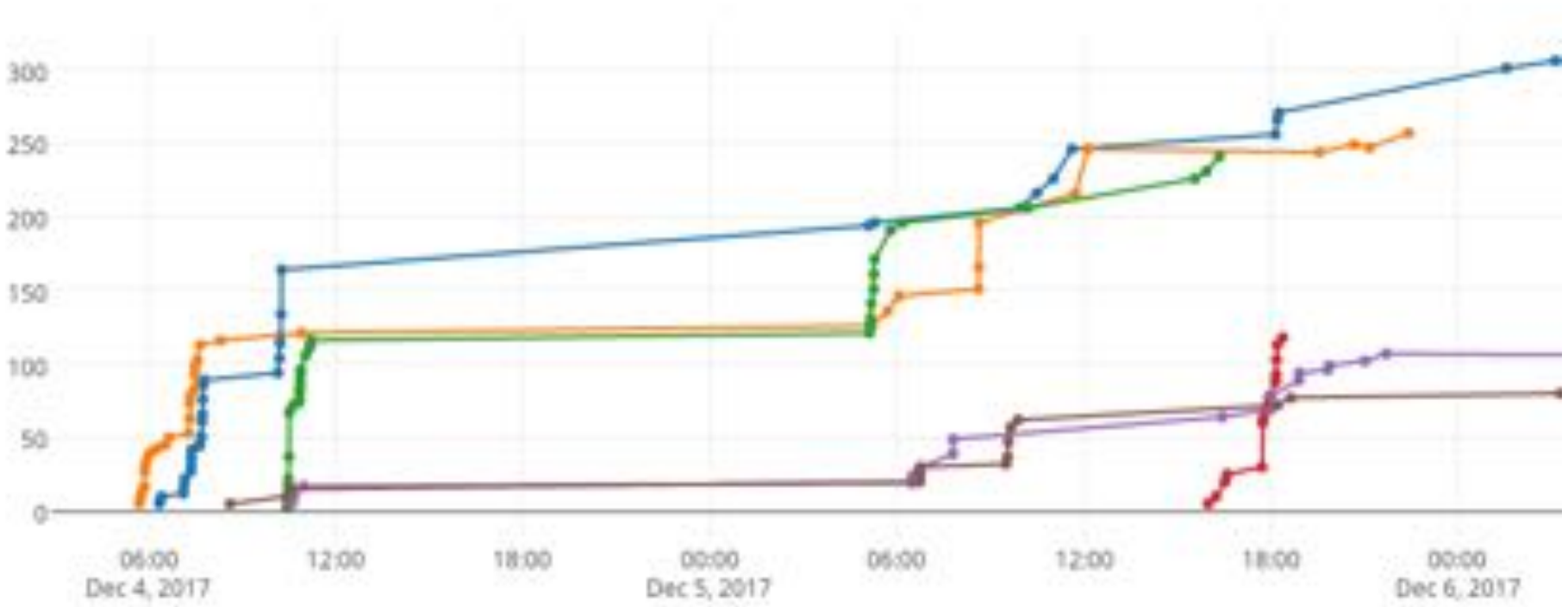
- Basic Java file reverse engineering and decompiling
- Mobile security challenges, breaking mobile device pin numbers, reversing Android APKs, Security assessment of potential malicious Android applications
- RSA Key reconstruction. Reproducing a private RSA key, when given only a partial private key (first 70 characters) and the public key.
- PDF file reconstruction to uncover hidden documents within PDF data structures.

CHPC 2017 Cyber Security Competition Ranking

User Ranking | Group Ranking | Overall Ranking

Rank	Score	Group	3038	3041	4221	4222	4223	5137	5145	5211	5213	5220	7051	7206	7366	7551	7555	7699	2715	4240	5047	5068	7207	7358	7687	7802	7354	7550	7553	7686	7705
1.	393	BitPhase																													
2.	342	Awesome Source																													
3.	326	HSN1																													
4.	180	Blitzkrieg																													
5.	173	The 4 Deons																													
6.	154	CyberPunks																													
7.	126	PUK1																													
8.	124	Insecure																													

CTFd (backup system)



HASH CHALLENGE 2017


CHPC
CENTRE FOR HIGH PERFORMANCE COMPUTING
The CHPC is the partner of choice for industry and researchers in:
Chemistry
Materials Science
Earth Sciences (Climate and Weather)
Bioinformatics
Health Sciences
Astronomy (including SKA)
Physics
Computational Mechanics/Engineering
Applied Mathematics
Computer Science
HPC Technology Evaluation
CSIR


CHPC
COMPUTING
DefinitelyNotAVirus.exe









SANReN
BlitzKrieg

SANReN
South African National
Research Network

And the winners

CSIRT
Information
Security

What's next?

- Training and bootcamps
- Sending 2018 winning team to compete in European Cyber Security Challenge (ECSC) 2019
- (sponsorships needed).

SANReN
South African National Research Network

CSIRT
Information Security

Thanks!

Join us?

csc (a) sanren.ac.za

SANReN CSC Team

cybersecuritychallenge.ac.za/

csirt.sanren.ac.za

CREDITS

- http://www.europeancybersecuritychallenge.eu/
- https://www.hacking-lab-ctf.com/
- https://www.hacking-lab.com/
- https://www.youtube.com/watch?time_continue=13&v=8M22pzybVbo
  (European Cyber Security Challenge 2016 CTF Infrastructure by Hacking Lab)
- http://www.europeancybersecuritychallenge.eu/2015/ECSC_2015_challenge_overview.pdf
- https://www.swisscyberstorm.com/challenges/
- http://www.cybersecuritychallenge.ro/
- https://cybersecurity.li/
- https://cybercamp.es/
- http://www.verbotengut.at/
- https://www.zerodays.ie/
- https://cybersecurity.li/ecsc-2016-duesseldorf/
- https://www.cscg.de/
- http://cybersecuritychallenge.org.uk/
- http://virtuaal.kehtnamtk.tk/
- http://ecsc.gr/

General CTF rules for ECSC 2016

National team is made up of up to 10 contestants, 1-2 coaches and a jury member.
Contestants should be top participants from the national challenge.
How national challenge is arranged is totally up to each nation, however, participation should be nationwide, i.e. not limited by region, belonging to specific institution etc.
There are junior and senior contestants.
Junior contestants aged 14-19, seniors 20-30 years.
There may be maximum 10 contestants in team, including maximum 5 seniors.
The contestants may not have (finished) Masters degree (or equivalent) in a Science, Technology, Engineering or Math (STEM) area.
The contestants may not have full time employment in security area.
The cutoff date for above is the beginning of national competition.
At the times other than challenge execution, the coach is responsible for well-being and behaviour of contestants and making sure that essential information reaches its recipients and is understood and acted upon.