CAPTURE THE FLAG: AN INTRODUCTION

So, You Want to CTF?

HOUSEKEEPING

PLEASE REMAIN MUTED FOR THE DURATION OF THE TRAINING SESSION.

PLEASE TYPE QUESTIONS IN THE CHAT BOX.

QUESTIONS WILL BE ADDRESSED DURING THE Q&A SESSION.

A SHORT BREAK WILL BE TAKEN AROUND THE 1-HOUR MARK.

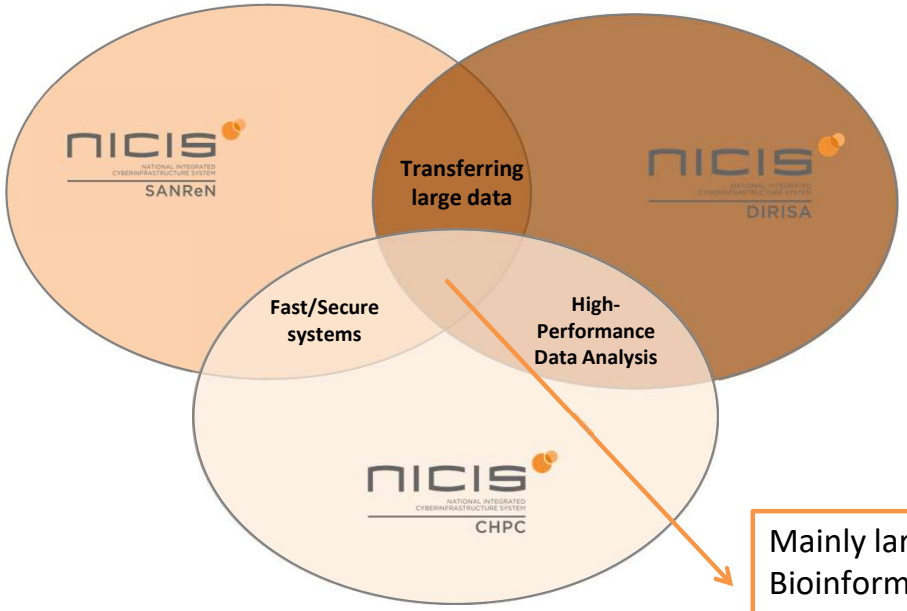
- Who (*whoami*)
- What (*What is CTFs*)
- How (*Examples*)
- Why (*Benefits*)
- Where (*Online CTFs*)
- When (*SANReN CSC*)

NICIS
NATIONAL INTEGRATED CYBERINFRASTRUCTURE SYSTEM
SANReN

YOUR HOST

- Heloise Meyer
  - PhD (ComSci)
  - Senior Network Security Specialists at SANReN, NICIS
  - Cyber Security, Mobile Security, and Digital Forensics
  - Passionate CTF Player

NATIONAL INTEGRATED CYBER INFRASTRUCTURE SYSTEM (NICIS)



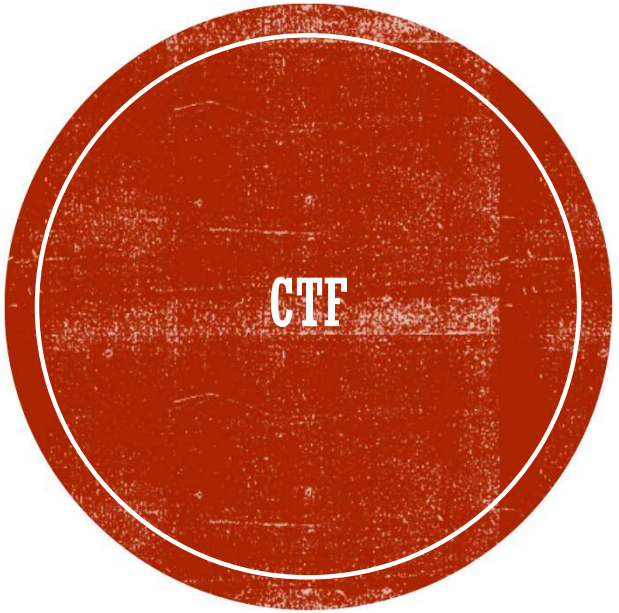
Mainly large-scale Science projects SKA, CERN, Bioinformatics, 4IR, SADC C.I. Framework, Climate Change

WHAT?

What is CTFs?

NICIS
NATIONAL INTEGRATED CYBERINFRASTRUCTURE SYSTEM
SANReN

- CTF == Capture the Flag
- InfoSec/CyberSec competition
- Wargame for “hackers” (white hats)
- Objective: *find the flag in limited time.*



FLAG

- Hidden
- Not obvious
- Difficult to access
- Case sensitive

- Format:
  - A message
  - A series of characters
  - Not always flag{…}

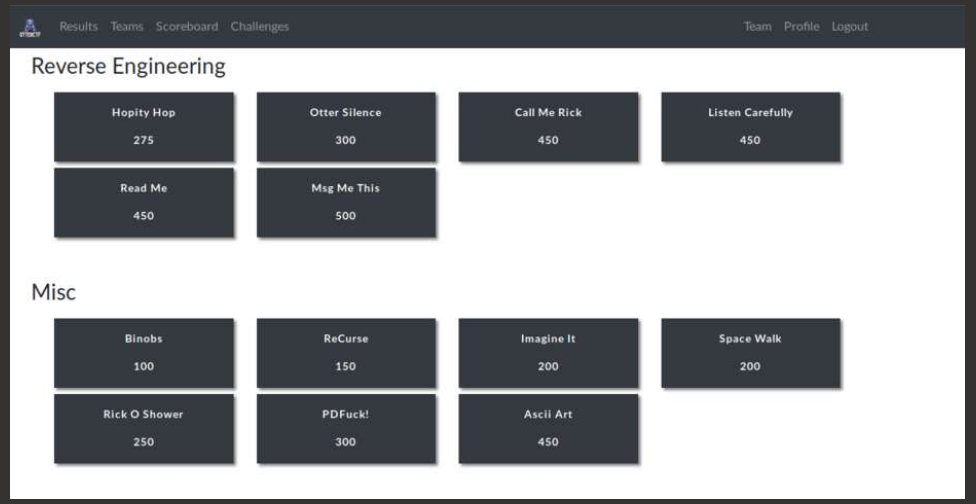
NICIS
NATIONAL INTEGRATED CYBERINFRASTRUCTURE SYSTEM
SANReN

CTF STYLES

- Jeopardy
- Attack-Defense

JEOPARDY

- Challenges are divided into categories
- Consist of different points based on difficulty
- Most CTFs are jeopardy-styled
- Team with most points win
- Hints provided for certain challenges
- Clues often in description



https://medium.com/@Blackpear1/what-is-ctf-9c05a45e5bd3

NICIS
NATIONAL INTEGRATED CYBERINFRASTRUCTURE SYSTEM
SANReN

CHALLENGES

- Crypto
  - Weaknesses in cryptography, primitives, or implementation – encodings (base64).
  - Cyberchef, dcode, cryptii, boxentriq
- Reverse Engineering
  - Exploring binary data (static or dynamic analysis) – debuggers and disassemblers.
  - Hex Editor, IDA Pro
- Web Exploitation
  - Weaknesses in web application – SQL Injection, Directory Traversal, Command Injection.
  - View Page Source Code, DevTools (F12), BurpSuite, OWASP ZAP, DirBuster
- Binary Exploitation
  - Finding a vulnerability in a program.
  - Buffer Overflow

CHALLENGES CONTI...

- Forensics
  - Searching for a needle in a haystack.
  - File signatures: Magic Numbers, binwalk
  - File system analysis: Sleuthkit's Autopsy
  - Memory analysis: Volatility
  - Steganography:
    - Art of hiding data in images or audio.
    - OpenStego, StegOnline, Steganography Online, steghide
    - Metadata: Exiftool
  - Network traffic analysis:
    - Explore captured network packets
    - Wireshark, PacketTotal

CHALLENGES CONTI...

- Mobile Security
  - Reverse engineering of mobile applications.
  - Apktool, Jadx, grep
- Password Cracking
  - Decrypt or decode a password.
  - Linux shadow file.
  - Wordlists: rockyou
  - John the Ripper, Hashcat, hydra
- Misc
  - Random puzzles requiring simply logic, knowledge, and patience to be solved.

https://defcon.org/html/links/dc-ctf.html

ATTACK-DEFENSE

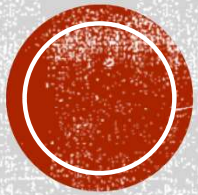
- Each team is given a machine or network.
- Round 1: Defend machine or network (identify vulnerabilities and patch).
- Round 2: Attack others machine or network.
- Points scored:
  - Attack others machine or network to place a flag.

HOW?

Get a taste of different CTF challenges

NICIS
NATIONAL INTEGRATED CYBERINFRASTRUCTURE SYSTEM
SANReN

JEOPARDY CTF EXAMPLES



A SECRET MESSAGE

- **Category**: *Crypto*
- **Level**: *Easy*

What is the Secret Message?

```
GUR PNRFNE PVCURE VF BAR BS GUR FVZCYRFG RAPELCGVBA
NYTBEVGUZF VA JUVPU RIREL YNGVA YRGGRE BS N TVIRA FGEVAT VF
FVZCYL FUVSGRQ PLPYVNPNYYL OL N PREGNVA BSSFRG. SBE
PENPXVAT GUR RAPELCGVBA, JR PBHYQ VGRENGR BIRE NYY
BCCBEGHAVGVRF NAQ NF BHE NYCUNORG HFRF WHFG 26 YNGVA
YRGGREF, JR JBHYQ BOGNVA GUR QRPELCGRQ FGEVAT VA NG ZBFG 25
GEVRF, JUVPU VF DHVGR GEVIVNY. GUR SYNT VF FRPGNYXF
```

NICIS
NATIONAL INTEGRATED CYBERINFRASTRUCTURE SYSTEM
SANReN

SO MANY LAYERS

- **Category**: *Crypto*
- **Level**: *Medium*

Find the flag in the zip file.

NICIS
NATIONAL INTEGRATED CYBERINFRASTRUCTURE SYSTEM
SANReN

CRYPTOGRAPHY CHALLENGES

- Hints
  - Explore spacing and word formation.
  - Explore variations.
  - Looking for encodings – base64.
  - XOR
  - Obligatory RSA Challenge – keep the formulas close…
- Recommended tool: CyberChef

https://tenor.com/view/winona-ryder-confused-math-formula-equation-gif-9380807

LOG IN

- **Category**: *Web*
- **Level**: *Easy*

Access the website to find the flag:
https://1-wh01.bootupctf.com/

WEB CHALLENGES

- Hints
  - View page source code (HTML, JS, CSS)
    - Check for hidden elements
  - Inspect page (F12)
    - Execute JavaScript
    - Check cookies
  - Login form → default credentials, SQL injection
  - Input form → Command injection
  - View robots.txt

- Recommended tools: BurpSuite (interception), Dirb (hidden directories)

BEAUTIFUL SUNSET

- **Category**: *Forensics*
- **Level**: *Easy*

What a beautiful sunset…

INTERESTING TRAFFIC

- **Category**: *Forensics*
- **Level**: *Medium*

View the captured network traffic. Find the flag.

NICIS
NATIONAL INTEGRATED CYBERINFRASTRUCTURE SYSTEM
SANReN

INTERESTING IMAGE

- **Category**: *Forensics*
- **Level**: *Medium*

Find the flag in the file.

NICIS
NATIONAL INTEGRATED CYBERINFRASTRUCTURE SYSTEM
SANReN

FORENSICS CHALLENGES

- Often include network capture and steganography challenges.
- Hints
  - For network captures:
    - Wireshark
      - Statistics → Conversations
      - Analyze → Follow (TCP, UDP or HTTP) Stream
      - Save As (Raw Data)
      - Start with last packets captured.
  - For images:
    - Check the file using the `file` command
    - View in Hex editor (File signature?)
    - Manipulate image (zoom in/zoom out, invert colours, etc.)
    - Embedded files? Use binwalk
    - Steganography? Use online tools to check…

NOT SO SHARP BLADE

- **Category**: *Reverse Engineering*
- **Level**: *Easy*

Use the file to find the flag.

NICIS
NATIONAL INTEGRATED CYBERINFRASTRUCTURE SYSTEM
SANReN

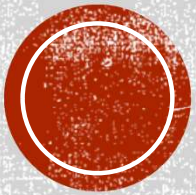
RE CHALLENGES

- Hints
  - Run/Interact with executable files (EXE or ELF).
    - Remember to assign execution rights (`chmod +x`)
  - For APK files
    - Use Apktool to decompile, dex2jar
    - Use emulator to run/explorer application
  - Use the `strings` command to search for strings in a file
  - Use a decompiler or disassembler tool
    - IDA Pro
    - Ghidra

GENERAL HINTS

- Know a scripting language (e.g., Python, PHP, Bash, Perl)
- Netcat – *TCP/IP Swiss Army Knife*
  - `nc 192.168.1.x 80`
  - `nc -lvp 4444`
  - `nc -z -v 192.168.1.x 1-999`
- Do not fear the command line/terminal
  - grep – searching for plaintext strings (`grep -iR flag /home/flag`)
  - find – search for files (`find . -name flag.txt`)
  - cat – view file contents (`cat flag.txt`)
  - nano – edit files (`nano flag.txt`)
  - file – type of file
  - strings – list of strings in file (`strings flag.txt`)
- Get familiar with Kali Linux

ATTACK-DEFENSE EXAMPLE



VULNERABLE MACHINES

- Vulnhub
  - https://www.vulnhub.com/
  - Recommended Vulnhub VMs
    - Dina
    - Toppo
    - Lampião
    - Mr Robot
    - RickdiculouslyEasy
- Damn Vulnerable Web Application (DVWA)
  - https://github.com/digininja/DVWA
- OWASP Juice Shop
  - https://owasp.org/www-project-juice-shop/
- SecGen – generate random vulnerable VMs
  - https://github.com/cliffe/SecGen

APPROACH - PENTESTING

- Reconnaissance/Enumeration
  - Discover hosts (`netdiscover -r 192.168.1.0/24`)
  - Discover open ports/services (`nmap -sV -p- 192.168.1.x`)
  - Port 80/443
    - Explore webpages (view page source)
    - View robots.txt
    - Enumerate website directories
    - Look for CMS panels (default credentials or vulnerabilities) – Drupal, Wordpress
    - Vulnerabilities – Nikto, nmap (`-sC`)
  - Port 21 (FTP)
    - anonymous login (anonymous/ anonymous)
    - File upload – reverse shell
  - Port 22 (SSH)
  - Vulnerabilities (Nessus, OpenVAS)
  - Banner grabbing
    - `nc`, `curl`, `telnet` or `nmap` (--script=banner)
      - `nc -vv 192.168.1.x 1337`

APPROACH - PENTESTING CONTI...

- Exploitation
  - Metasploit (`msfconsole`)
  - Upload a reverse shell to website (`nc -lvp 4444`)
    - Python, Perl, PHP reverse shell examples
- Privilege escalation
  - Check for credentials (MySQL database, shadow file)
    - Password cracking: Hashcat or John the Ripper
  - Local privilege escalation
    - Searchsploit
    - Exploit-db
  - Look for Privilege programs/software
    - Set Owner User IDs (SUIDs) and Set Group IDs (SGIDs) – Linux/Unix

DONOT5TOP: 1.2

- Vulnerable Virtual Machine – 7 flags to capture.
- https://www.vulnhub.com/entry/d0not5top-12,191/
- Setup
  - Download and install VirtualBox (https://www.virtualbox.org/wiki/Downloads)
    - Also install the VirtualBox Extension Pack
  - Import vulnerable VM (File → Import Appliance → Select OVA file → Accept Agreement → Import)
  - Keep default configuration
  - Start VM

WHY?

The benefits of CTFs

NICIS
NATIONAL INTEGRATED CYBERINFRASTRUCTURE SYSTEM
SANReN

- Safe environment to practice infosec (hacking) skills.
- Learn new skills or measure current skillset.
- Offensive thinker – think like a hacker.
- Improve problem solving skills.
- Help to think out of the box and intuitively.
- Job, credentials.

WHERE?

Online CTFs… Practice, practice, practice…

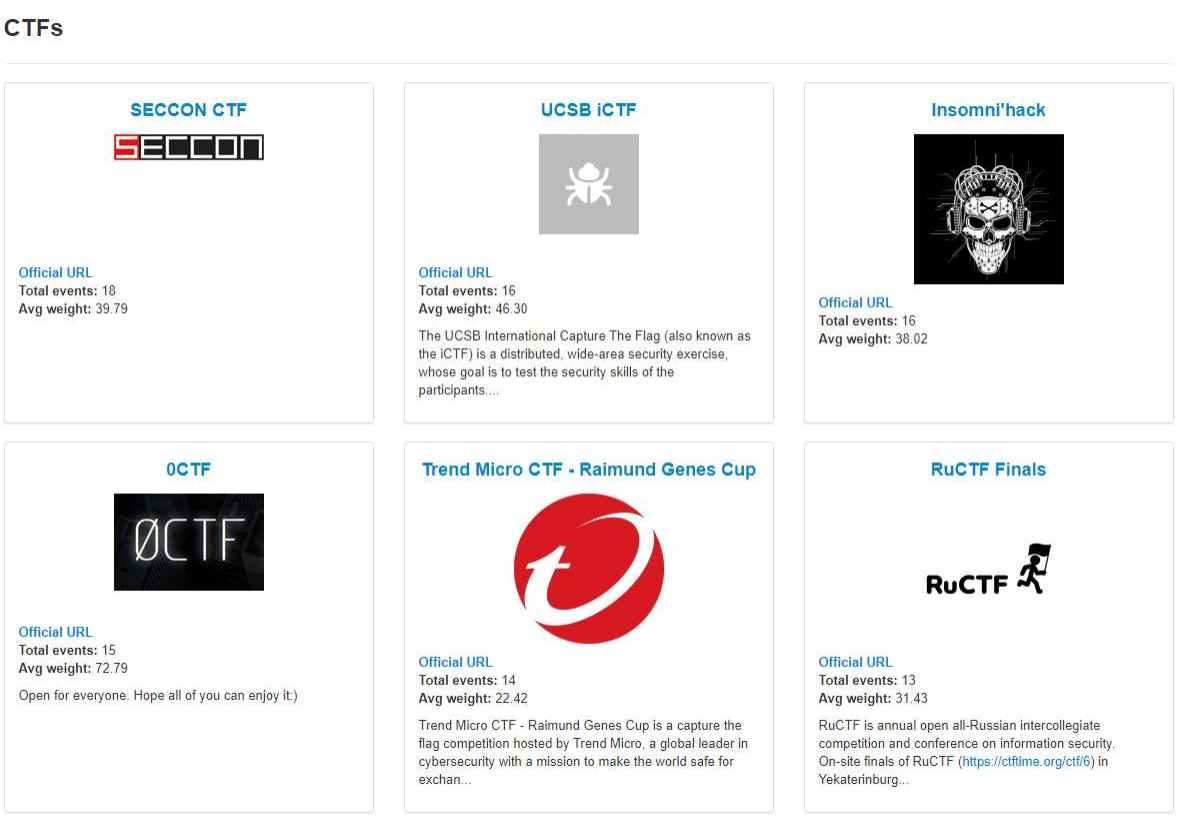
NICIS
NATIONAL INTEGRATED CYBERINFRASTRUCTURE SYSTEM
SANReN

GETTING PREPARED

- Awesome CTF – Curated list of CTF tools
- OverTheWire – learn and practice security concepts
- CTF Writeups
  - https://infosecwriteups.com/tagged/ctf
  - https://medium.com/ctf-writeups
  - https://ctftime.org/writeups
- YouTube Channels
  - NetworkChuck (https://www.youtube.com/c/NetworkChuck)
  - LifeOverflow (https://www.youtube.com/c/LiveOverflow)

CTF EVENTS

- CFTtime
  - https://ctftime.org/ctfs/
- SANS New2Cyber
- picoCTF
- Social Media (LinkedIn) Posts



https://ctftime.org/ctfs/

NICIS
NATIONAL INTEGRATED CYBERINFRASTRUCTURE SYSTEM
SANReN

WHEN?

SANReN Cyber Security Challenge (CSC) 2022

NICIS
NATIONAL INTEGRATED CYBERINFRASTRUCTURE SYSTEM
SANReN

CSC 2022

- InfoSec challenge for all Universities in SADC
- www.csc.ac.za
- 3-4 persons per team
- 2 Rounds
  - Qualification (Online for 10 days)
  - Finals (3 days, +- 1 December)
- Finals
  - Top 8 teams, max one team per University Department
  - Fully Sponsored by SANReN (Venue TBD - Mpumalanga)*
  - Jeopardy-styled CTF and Attack-Defense event.

NICIS NATIONAL INTEGRATED CYBERINFRASTRUCTURE SYSTEM SANReN

PARTICIPATION

- Open, Voluntary (SADC Region)*
- Visit: http://csc.ac.za
- View rules
- Discuss and form teams
- Register
- Teams receive notification via email once the qualification round is open.
  - Login details
- Qualification planned to be completed by end of September 2022
- Follow us on Twitter: https://twitter.com/csc_sanren

http://csc.ac.za

WRAP UP

Final thoughts

NICIS
NATIONAL INTEGRATED CYBERINFRASTRUCTURE SYSTEM
SANReN

CLOSING REMARKS

- Do not overthink the challenge.
  - Usually, challenges have a score associated with it which helps you gage how much effort should be invested in each challenge.
- Tools help but often the challenges test your understanding of the concept rather than your knowledge of a tool.
- Learn to spot various hash algorithms especially base64, these encodings are often used to hide data, display binary data or encode variables.
- Unless the challenge is specifically a password challenge, passwords used in a challenge is usually related to the subject matter or can be cracked using common password lists or by basic brute force.
  - Challenges are made to be solved in short period of time.
  - If this still does not work, you might have overlooked some other clue in the challenge.
- Golden rule of CTF
  - Practice, practice, practice…
- *"don't forget during a CTF, Google is your friend…"*


Q&A SESSION

THANK YOU

Contact details:
heloise@sanren.ac.za

NICIS
NATIONAL INTEGRATED CYBERINFRASTRUCTURE SYSTEM
SANReN