CanHack 2022
Powered by RBC

GUIDE BOOK

Ryerson University, 10 Dundas St E, Toronto, ON M5B 2G9

https://dmz.ryerson.ca/canhack/

#canhack2022

CanHack 2022

Table of Contents

1.0 Introduction

In an age of nonstop security breaches and hacks, understanding digital security matters more now than ever before. Recent high-profile attacks have highlighted how important it is for Canadian companies, not-for-profit organizations, public sector organizations and everyday citizens to strengthen their cybersecurity knowledge.

To encourage greater interest in cybersecurity literacy and computing skills among Canadian high school students, The DMZ at Ryerson University is launching CanHack, an online cybersecurity competition. This program is based on the very successful picoCTF platform developed by the Carnegie Mellon University Cylab Security and Privacy Institute. PicoCTF is an online open source computer security platform that has been used by over 50,000 students and is built to deliver an exceptional learning experience centered around a unique storyline. Led by Ryerson University's DMZ, Powered by RBC, this competition will help address the cybersecurity and privacy skills gap impacting Canadian security.

The CanHack program...

1. Establishes a basic literacy for cybersecurity and privacy at an earlier age by providing hands-on learning for students.

2. Leverages digital learning tools to develop more interest in the field of cybersecurity and computer science among students that otherwise may not have pursued a degree in computer science related fields.

3. Supplies a new technical resource for teachers to integrate coding and computational skills into lesson plans with experiential learning opportunities.

Through the competition, The DMZ & RBC will help build a more diverse, broader, and deeper workforce pipeline by leveraging its strengths in integrating diversity and inclusivity.

CanHack presents a unique opportunity to support the development of Canada's next generation of talent and to increase cybersecurity and privacy awareness among Canadian students at a critical stage in their education

1.1 Mission

CanHack's mission is to engage and educate diverse Canadian high school students in the field of cybersecurity through a fun and free web-based game competition. This guidebook addresses everything you need to know to take part in the competition.

1.2 Vision

CanHack presents a unique opportunity to support the development of Canada's next generation of talent and to increase cybersecurity and privacy awareness among Canadian students at a critical stage in their education. It is a catalyst to address the shortage of talent in the field of cybersecurity.

1.3 Goals

CanHack aims to...

- Help demonstrate cybersecurity leadership: Take initiative in combating cyber threats and protecting Canadians from potential dangers;
- Help Canadian youth prepare for the digital economy: Regardless of what career path youth choose, CanHack ensures they develop cyber security skills essential to preparing them for the future digital workforce;
- Help Canadian youth understand safe cyber and privacy practices: Improving safe online practices of Canadian consumers can defeat many online threats. CanHack supports the development of these safe online skills among young Canadians;
- Develop a pipeline of new ideas and skills: CanHack ensures the critical growth of the Canadian cybersecurity industry by increasing awareness of cyber security as a field, and;
- Build cybersecurity literacy in your organization: Use the gameplay and challenges to improve cybersecurity literacy.

1.4 CanHack 2022 Competition

The CanHack 2022 program is based on Carnegie Mellon University's popular capture-the-flag competition called PicoCTF. The game is a fun way for students to practice their skills and showcase their abilities to the tech community.

While CTF challenges are traditionally presented in a straightforward text-based manner, CanHack 2022 will leverage PicoCTF to build the experience around a unique story-driven game experience. The game is designed in collaboration with industry advisors and sponsors to appeal to students who might not otherwise be interested in participating in a computer security competition.

1.5 PicoCTF 2022

Established in 2013 by the Carnegie Mellon University Cylab Security & Privacy Institute, PicoCTF is a free online open source computer security platform for high school students centred on a unique storyline to promote cyber literacy and skills development.

PicoCTF is a capture-the-flag competition (CTF). CTFs are organized as a fun, legal way for computer security students and professionals to practice their skills and demonstrate their abilities with the technology community. In a standard-format CTF, teams race to tackle computer security challenges, searching for digital "flags" hidden in servers, embedded in encrypted text, or in binary programs. During the competition, teams earn points for submitting discovered flags. The team with the most points at the end of the competition will win. PicoCTF has been used to reach over 50,000 students and, as an open source tool, has been customized to meet local and industry needs.

Challenges are generally designed with many possible solutions and help students acquire skills in computer forensics, cryptography, reverse engineering, binary exploitation, and web security. The platform offers:

a. Open and freely available cybersecurity and privacy educational materials
b. The ability to start from basic literacy level to a professional level.
c. Differentiation in the approach to solving the challenges. Competitors may choose to work on just one component of the program such as cryptography or forensics, allowing them to play to their strengths while gathering new skills.

The game is divided into 60+ specific challenges spread across four levels, each advancing the story and increasing in difficulty.

Level 1 – Designed to challenge students' critical thinking skills
Level 2 – Designed to challenge students with introductory programming experience
Level 3 - Designed to challenge Computer Science students with a stronger background in programming
Level 4 - Contains a diverse set of problems across all categories, ranging from difficult to professional

1.6 How is picoCTF different from other CTF games?

There are several other cybersecurity competitions, including Cyberpatriot and U.S. cyber challenge. These competitions focus primarily on defensive skills and systems administration fundamentals, which are very useful and marketable skills.

PicoCTF, on the other hand, is only a two week competition that is heavily focused on exploration and improvisation, and often has elements of play. Competitions touching on

the offensive elements of computer security are essential for mounting an effective defense, as students are led to ‘know their enemy.

PicoCTF is an offensively-oriented highschool computer security competition that seeks to generate interest in cybersecurity: teaching them enough about computer security to pique their curiosity, motivating them to explore on their own, and enabling them to better defend their computers.

2.0 Learning Outcomes

As students play picoCTF, they will not only learn a great deal about cybersecurity, but will also acquire skills, habits, and knowledge tied to 21C skills, global competencies, guidance and careers, as well as the current Computer Science curriculum. There are many curricular connections which can be found in the Appendix Section of this document.

2.1 Twenty-First Century Skills and Global Competencies

The picoCTF game captures the creativity, critical thinking, and complex problem-solving skills among students. It engenders risk-taking and continuous improvement, as well as adaptability, persistence, collaboration, and digital literacy. Students need to solve challenges, based on real-world and authentic examples, by acquiring, processing, analyzing, and interpreting information. They make informed judgments, decisions, and actions to level up in the game. Through the process of playing the game, students learn how to learn, in collaborative ways by co-constructing knowledge, meaning, and context.

Students are then able to transfer their learning in different situations as they level up in the game as challenges are interdependent and interdisciplinary. Also, they do this in a safe environment where they can feel comfortable taking risks in their thinking. Games are a great means for motivation, perseverance, and resilience. Cybersecurity is a borderless problem and a global concern and through developing skills in cybersecurity we are creating responsible, global citizens to help ensure our privacy and security.

2.2 ICT Information and Communications Technology Skills

The game picoCTF provides differentiated and scaffolded learning experiences, allowing for students of different skill sets to play the game at their own level. Although no computer programming skills are required, students will gain an understanding of Python, HTML, JavaScript, Java syntax and C. Past participants of picoCTF have played with no programming experience and picked up programming knowledge along the way.

The game provides opportunities for students to develop a range of skills and knowledge, including knowledge of computer studies concepts, structures, and processes, that will allow them to participate more effectively in their communities as responsible and active citizens.

The game provides a varied approach to teaching and assessment approaches in the classroom, addressing different student needs and ensuring sound and engaging learning opportunities for every student.

By playing picoCTF, students not only gain a deeper understanding of how computers compute, but the game is a great way for computer programmers to see how various classic programming mistakes can lead to catastrophic vulnerabilities.

Specific correlations to the current Computer Studies curriculum can be found in Appendix A.

Learning outcomes specific to picoCTF can be found in Appendix B.

2.3 Guidance and Careers

Many of the skills acquired while playing the game are tied to the current Guidance and Career Education Program. The game is an excellent way to explore careers in cyber security while developing the necessary skills to work in this field.

As competitors play the game, they develop resiliency, learn to be effective members of a team, and learn to manage the resources required to complete tasks and achieve their goals.

Students develop the habits and skills they need in order to become self-directed, lifelong learners. They will pick up research skills, locate relevant information, and solve a variety of challenges. Competitors will learn to access a variety of sources, such as glossaries, videos, open-source platforms, and the Internet.

Through this experiential learning activity, students practise essential skills in cyber security, in an authentic situation, using real workplace materials, in a virtual setting. Students learn the benefits of having a broad range of skills to meet the demands of the changing global market.

2.4 Cybersecurity Skills

In the process of playing picoCTF, students will learn a variety of skills specifically tied to cybersecurity.

Data security is about protecting digital privacy by preventing unauthorized access to computers or websites. Data security is also known as information security (IS) or computer security.

Cryptography is the process of converting ordinary plain text into indiscernible text and vice-versa.

Reverse engineering is widely used by cybersecurity specialists to ensure that systems lack any major security flaws or vulnerabilities.

Binary exploitation is the process of abusing flaws in software to make an application perform functions that it wasn't designed to do.

Web security is the process of protecting and securing websites and servers, against malware.

Digital forensics is the search for and detection, recovery and preservation of evidence found on digital systems. For example, detecting how hackers broke into a confidential database, recovering deleted emails, etc.

Ethics is the moral compass that guides one's decision. There are two types of hackers. The black hat hackers use their hacking skills for nefarious reasons, while white hat hackers use their skills to break into protected systems and networks to test and assess how secure they are. The search for and detect vulnerabilities before malicious hackers do to prevent exploitation. The protagonist in the game is using hacking for the good of humanity.

Hacking - Most "hackers" are white hat hackers who work hard to identify and fix vulnerabilities in computer systems or networks. These types of hackers are in great demand in the workforce and usually command six-figure salaries.

3.0 Roles and Responsibilities

In order for the competition to run smoothly, we have laid out tasks and duties for everyone so that we are all clear on our roles and responsibilities throughout the competition.

3.1 Team Supervisor Roles and Responsibilities

Team supervisors are responsible for …

- Signing up their classes for pre-challenge workshops
- Noting all team members' usernames to track progress during the Challenge
- Protecting the competition's integrity by ensuring competitors do not receive answers to advance the game. Competitors must search for answers to the game themselves.
- Upholding the rules and principles of the game
- Acting as CanHack's main point of contact for teams as CanHack may need to contact a team about score discrepancies, registration issues, or any other competition matters
- Supervisors need to also ensure they can receive messages from the CanHack team which can be sometimes blocked by school firewalls

Please contact Naveed Tagari <naveedtagari@ryerson.ca> for further details.

3.2 Mentor Roles and Responsibilities

All supervisors and students will have access to mentors who volunteer their time to guide students throughout the game and answer any questions that may come up during the competition. Mentors are industry experts who work in the field of cybersecurity.

4.0 Support Throughout the Competition

There are a number of ways to receive support throughout the competition. There are tutorial videos, links to useful websites, and we offer workshops as well.

We will also provide virtual support to competitors through email. Competitors may request direct support from technical guides by reaching out through email dmzcanhack@ryerson.ca for any questions.

Throughout the game there will be hints provided leading students to locate the right answer.

4.1 CanHack Resource Hub

The DMZ team has created a new CanHack Resource Hub for students and teachers to utilize. This portal will include 4-8 workshop videos and other cybersecurity resources for students to learn from and reference. Students not able to attend in-person sessions at The DMZ will find all relevant content listed under the CanHack Resource Hub. The resource hub will ensure that students no matter where they are in Canada can all access and compete in CanHack 2022.

A number of resources have been curated for the competition and can be found at https://picoctf.com/resources

4.2 Teacher onboarding

All resources for teachers will be on the resource hub to provide overview information on CanHack.

5.0 Game scoring

Each challenge is assigned a point value based on its predicted difficulty. When teams solve a given challenge, the point value for that challenge is added to their score and displayed on the online scoreboard. Teams can submit unlimited educated guesses to a given challenge without penalty. In the game, each challenge is represented by gems that have 1, 2 or 3 stars indicating level of difficulty. The more challenging the problem is, the more points it is worth.

The winner of the competition will be the team with the most points (the time of the last problem solved is the tiebreaker). Teams will be encouraged to use all available resources but are forbidden to receive direct assistance from outside persons.

5.1 How winners are determined

The team that solves the most problems within the allotted time will be the winner. If more than one Team solves all of the problems, then the Team that solved the problems in the shortest amount of time will be the winner. As described in more detail below, winners (including any

tie-breakers, questions about eligibility, etc.) are determined by Carnegie Mellon Universityand Ryerson University at its sole discretion.

For teams with parents/guardians as the supervisor that are successful, the prize will be split evenly with the consent of the parents/guardians of all students involved.

5.2 Competition Prizes

Top 3 Team Prizes 1st Place — $2,000 2nd Place — $1,000 3rd Place — $750	Prizes for the Top 3 Schools/Organizations representing high school students 1st Place — $3,000 2nd Place — $2,000 3rd Place — $1,000
Top All-Female Team - $2,000	

5.3 Awards and Recognition

Winners of CanHack will be announced virtually, in April 2022.

5.4 Press and Media

Award-winning teams of the Canadian Competition may have their team names, supervisor name and Competitor's names published in one or any of the following places:

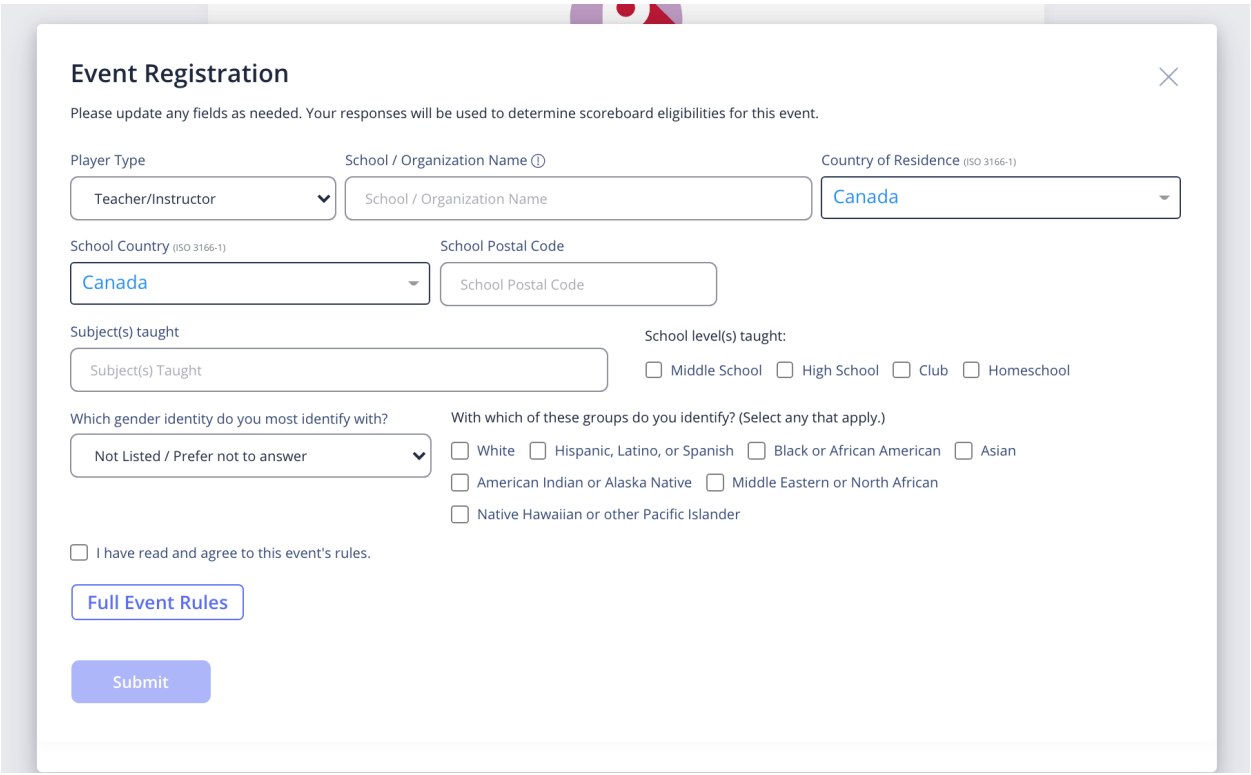
1. RBC Communications
2. DMZ Communications
3. Ryerson Communications
4. CanHack website
5. Press Releases
6. Social media
7. PicoCTF communications

6.0 How to Register - Two-Methods

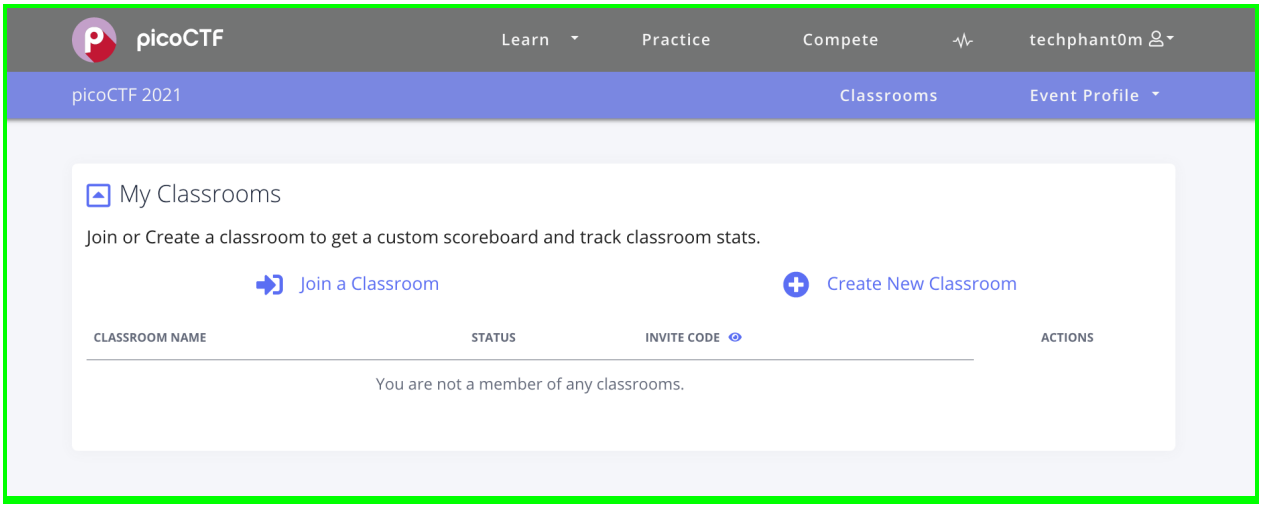
METHOD 1:

Step 1: Register first for CanHack as a Supervisor at DMZ.to/canhack if not already done so.

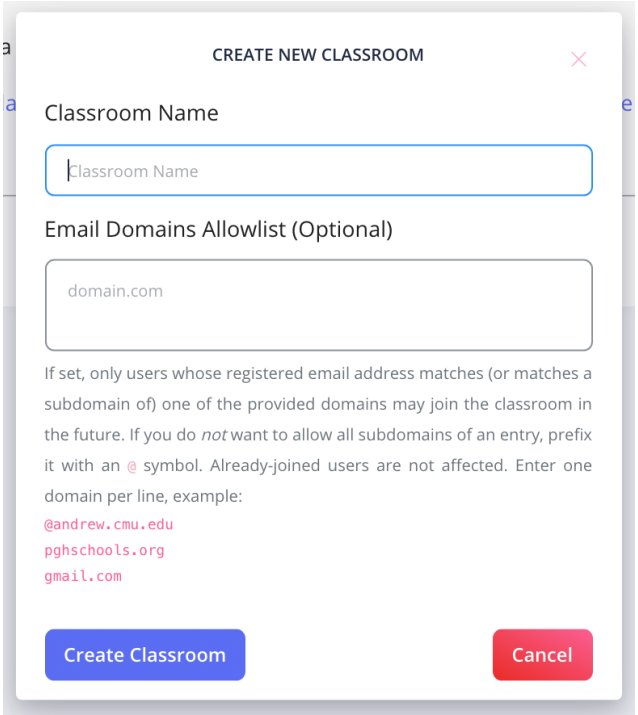
Step 2: Register as teacher on www.picoctf.com after February 1st, 2022.



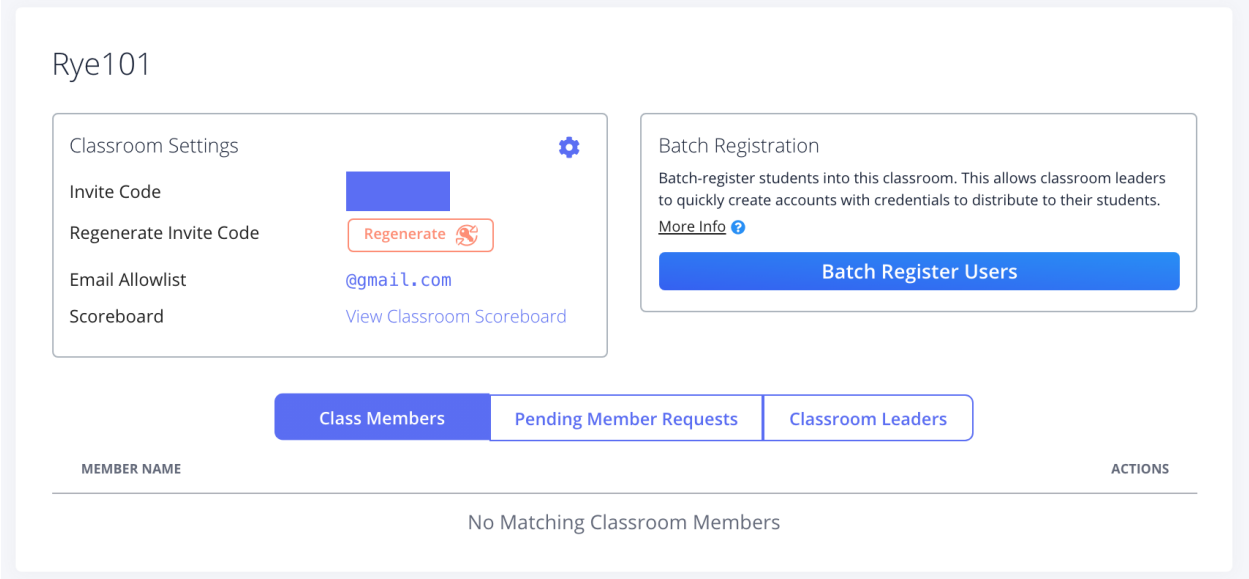
Step 3: Go to Classroom Menu, Management Tab:

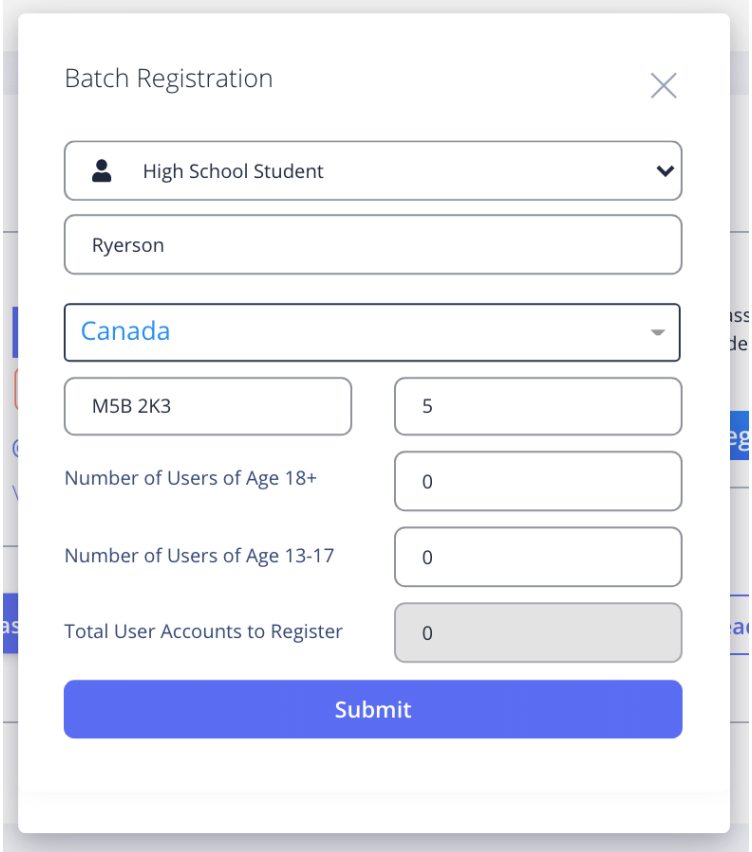


Select “Create New Classroom”, input the details:



Select “Batch Register Users”, this open will generate accounts (usernames, passwords) for the number of students you specify. The usernames can then be shared with your students and they can use this information to login.





- Accounts created through batch registration will share matching player type, country, school name, school postal code, and grade information.
- Each account will be created, already verified and assigned to your email address.
- Usernames and passwords will be created automatically to a CSV spreadsheet file to download. These username/passwords should then be distributed individually to your class members.

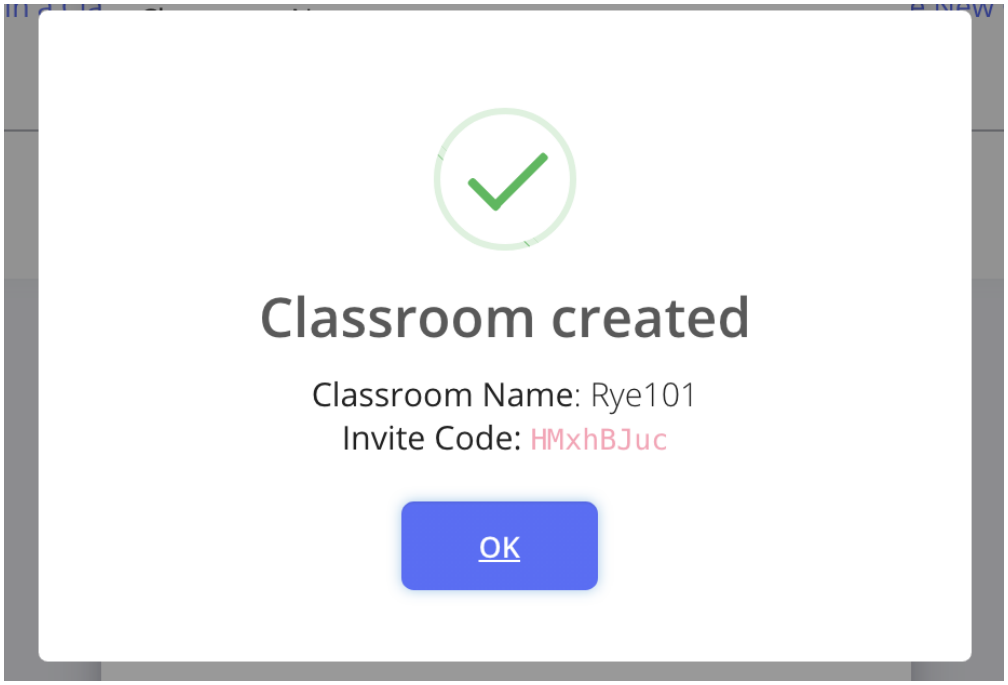
- Once a user logs into one of the generated accounts, they may then change their profile information, including username, e-mail, and password.

A download popup will come up automatically for the resulting CSV file with login username/passwords, but a **TEMPORARY LINK** is available there to "Redownload Account Credentials" also. If the teacher navigates away from the page, the credentials will be gone (which is required for security, we only have the plain-text passwords temporarily right after they are generated).

ALTERNATIVELY..

METHOD 2:

Students can create their own usernames and you can share an invite code with them to join your classroom.



Step 4. Collect all usernames and teams that your students will be using on the PicoCTF platform and fill out this excel template here: This template will have all the team names and the corresponding student's usernames.

Step 5 (MOST IMPORTANT STEP):

Head back over to dmz.to/canhack, scroll down and fill out Step 3 under the registration section by uploading the excel sheet with the team names and usernames.

The link to do this can be found here:

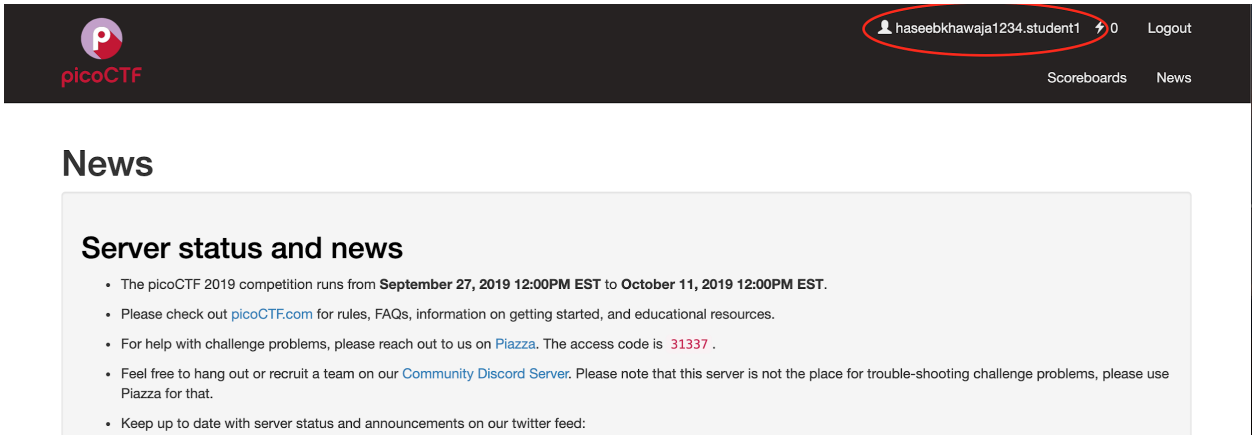
https://forms.gle/Hcet5s9jm9no5yp99

7.0 How students can join teams?

Creating a team of 5 is a great idea for students! The benefit of working together will not only push students to complete more challenges, but as each student in the team collects points by finishing the challenge, all of those points are accumulated as a whole for the team, meaning the team has a better chance at winning the prize pool!

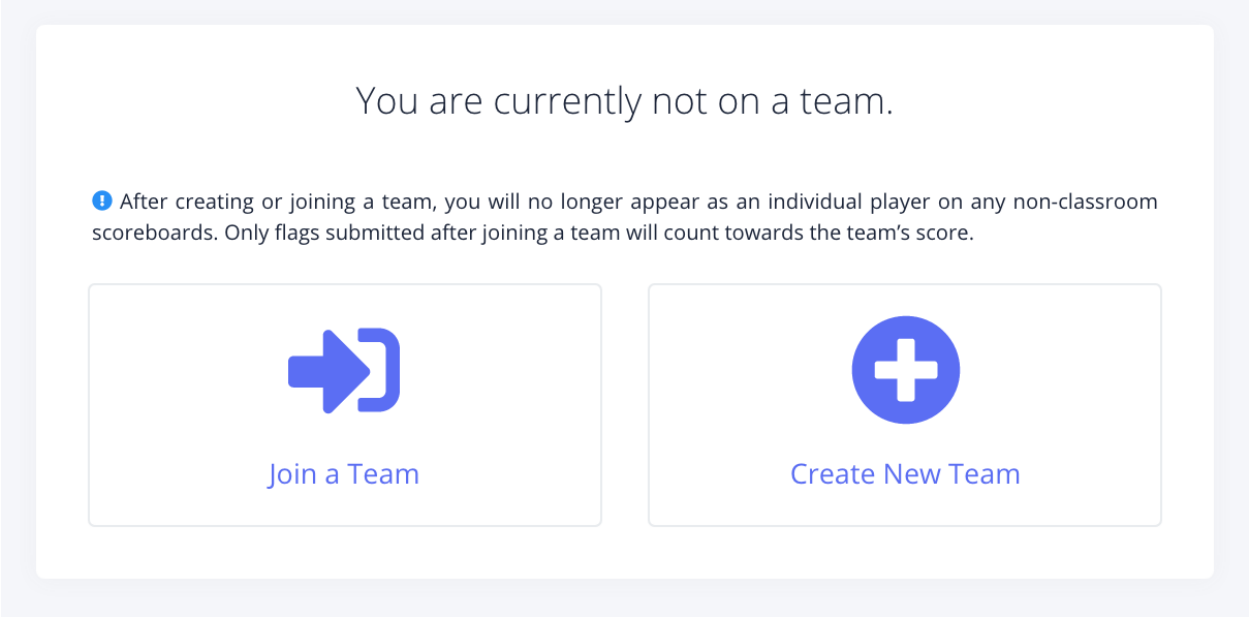
Step 1:

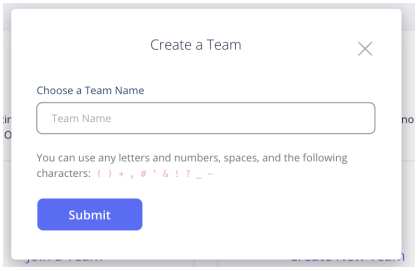
Upon creating the profiles for your students, have them log in and access their profile information by clicking on their username as shown below.

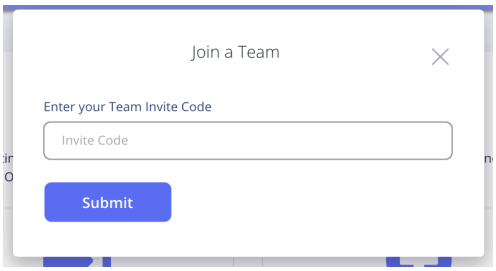


Step 2:

Under the profile section, students should see the team management section. 1 student from the team should create the desired team name and password. Once created, other students can then go on their own profiles and join that team as well as shown below:







Please note:

Once a student has joined a team, they cannot leave that team and join another one.

7.0 F.A.Q

How much time needs to be devoted to the game?

Students may spend as much or as little time playing the game as they like during the two-week competition. The game runs for over 2 weeks and the best part is, students can play this challenge on their own computers at home, at school or wherever else they like! We recommend at least 30 minutes to 1 hour of playing time per day in order to compete for the cash prizes! PicoCTF will keep running after the competition so students can continue learning after the competition is over.

What is "hacking?"

Hacking is all about curiosity, exploration, and deeply understanding how something works. Most people who identify as "hackers" are working very hard to protect people and to make technology easier and safer to use. Unfortunately, when most people hear or read about hacking in the news, the story is about people using hacking to do harm, but this couldn't be further from the truth. Career-wise, people skilled in hacking are highly sought out by companies looking to strengthen their cybersecurity. Computer security experts are in very high demand today and often are paid six-figure salaries.

What is a CTF?

CTFs (short for capture the flag) is a type of computer security competition. Contestants are presented with a set of challenges that test their creativity, technical (and googling) skills, and problem-solving ability. Challenges usually cover a number of categories, and when solved, each yields a string (called a flag) which is submitted to an online scoring service. CTFs are a great way to learn a wide array of computer security skills in a safe, legal environment, and are hosted and played by many security groups around the world for fun and practice.

What is picoCTF?

There exist several other well-established high school computer security competitions, including Cyberpatriot and US Cyber Challenge. These competitions focus primarily on systems administration fundamentals, which are very useful and marketable skills. However, we believe the proper purpose of a high school computer security competition is not only to teach valuable skills but also to get students interested in and excited about computer science. Defensive competitions are often laborious affairs and come down to running checklists and executing config scripts. Offence, on the other hand, is heavily focused on exploration and improvisation, and often has elements of play. We believe a competition touching on the offensive elements of computer security is therefore a better vehicle for 'tech evangelism' to students in North American high schools. Further, we believe that an understanding of offensive techniques is essential for mounting an effective defence, and that the tools-and-configuration focus encountered in defensive competitions does not lead students to 'know their enemy' as effectively as teaching them to actively think like an attacker.

picoCTF is an offensively-oriented highschool computer security competition that seeks to generate interest in computer science among highschoolers: teaching them enough about computer security to

pique their curiosity, motivating them to explore on their own, and enabling them to better defend their machines.

What will my students need to know?

Minimally: how to think critically. Some familiarity with programming will be helpful, but many past participants of picoCTF have played with no programming experience and learned some programming along the way. Exposure to Python, HTML, JavaScript, and C (though Java syntax is close enough for this purpose) is ideal, but in no way required.

What software do students need?

There is a web terminal available on picoCTF, but an SSH client (e.g. putty) can be helpful. Students are encouraged to use other free tools as well.

School network administrators may need to approve access or request pages/sites to whitelist for picoCTF.

What is the role of the supervisor in this competition?

But we encourage teachers to help students with Canhack 2022 in whatever way they see fit.

As a teacher, can I play too?

Absolutely! Everyone is welcome. Only students who meet the above requirementsare eligible for prizes, but we encourage teachers (and others!) to play.

How can I keep track of how my students are doing?

You can create a classroom and invite your students to join it. In your classroom dashboard, you will be able to see individual and aggregate progress stats. In addition, the scoreboard page will show a separate ranking of just your classroom members, alongside the existing public scoreboards. You may also export a complete CSV of student stats. See the Classrooms section for more information on this feature.

How much time should I allocate? Do students have to work at particular times?

We plan to have a range of challenge difficulties. Students will be able to log in at any time and spend as much or as little time as they like during the two weeks. We also expect to keep the site running after the competition so students can continue learning after the competition is over.

Do students compete individually or in teams?

Each student will register individually. Afterwards, they can compete individually or form teams of up to 5 members.

I'm still a bit confused…

No problem! Feel free to contact Naveed, Project Coordinator at naveedtagari@ryerson.ca and we would be happy to clarify anything for you.

APPENDIX

Appendix A - Computer Science Curriculum Correlations

Introduction to Computer Studies, Grade 10

A. Understanding computers

A5.1 describe different types of malware (e.g., viruses, Trojan horses, worms, spyware, adware, malevolent macros) and common signs of an intrusion, and explain how to prevent malware attacks;

A5.2 explain the importance of maintaining software updates (e.g., operating system updates, application software updates, virus definitions) to increase computer security and maintain hardware and software compatibility;

A5.3 explain the importance of preventive maintenance to manage computer performance. (e.g., defragmenting a hard drive, deleting unused software and data files);

C. Computers and Society

Social Impact:

C1.5 describe issues associated with access to online services (e.g., reliability of passwords, network security, identity theft, the permanence of information released onto the Internet);

Environmental Stewardship and Sustainability:

C2.2 identify measures that help reduce the negative effects of computers on the environment (e.g., lab regulations, school policies, corporate policies, provincial policies, paperless workplaces) and on human health (e.g., ergonomic standards).

Ethical Issues:

C3.1 describe legal and ethical issues related to the use of computers (e.g., music and video file downloading, spyware, identity theft, phishing, keystroke logging, packet sniffing, cyber bullying);

C3.2 describe safeguards (e.g., effective passwords, secure websites, firewalls, biometric data) for preventing the unethical use of computers.

Post-secondary Opportunities:

C4.3 identify groups and programs that are available to support students who are interested in pursuing non-traditional career choices in computer-related fields (e.g., mentoring programs, virtual networking/support groups,

specialized postsecondary programs, relevant trade/industry associations);

C4.4 identify the Essential Skills and work habits that are important for success in computer studies, as defined in the Ontario Skills Passport.

Introduction to Computer Science, Grade 11 University Preparation IC S3U

Topics in Computer Science:

D2. demonstrate an understanding of emerging areas of computer science research;

D2.1 demonstrate an understanding of emerging areas of research in computer science (e.g., cryptography, parallel processing, distributed computing, data mining, artificial intelligence, robotics, computer vision, image processing, human– computer interaction, security, geographic information systems [GIS]).

Postsecondary Education and Career Prospects

D3.1 research and describe career choices and trends in computer science, at the local, national, and international levels;

D3.2 identify and report on opportunities for experiential learning (e.g., co-op programs, job shadowing, career fairs) in the field of computer science;

D3.3 research and report on postsecondary educational programs leading to careers in information systems and computer science (e.g., institutions offering relevant programs, industry certifications, courses of study, entrance

requirements, length of programs, costs);

D3.4 identify groups and programs that are available to support students who are interested in pursuing non-traditional career choices related to information systems and computer science(e.g., mentoring programs, virtual networking/support groups, specialized postsecondary programs, relevant trade/industry associations);

D3.5 describe the Essential Skills and work habits that are important for success in computer studies, as identified in the Ontario Skills Passport.

Introduction to Computer Programming, Grade 11 College Preparation ICS3C

Problem-solving strategies

B1.1 use various problem-solving strategies to solve programming problems (e.g., divide and conquer, working backwards, process analysis, examples, extreme cases, tables and charts, trial and error);

Computer Environments and Systems

C2. use appropriate **file maintenance** practices to organize and safeguard data;

Safe Computing

~~D2.1 e~~explain the need for an acceptable-use policy for using computers at school and at work;

D2.3 describe procedures to safeguard data and programs from malware (e.g., viruses, spyware, adware).

Emerging Technologies

D3.1 explain how emerging technologies can affect personal rights and privacy (e.g. video surveillance, cyber bullying, identity theft);

D3.2 describe some emerging technologies and their implications for, and potential uses by various members of society;

D3.3 describe some of the solutions to complex problems affecting society that have been or are being developed through the use of advanced computer programming and emerging technologies (e.g., monitoring and regulating electrical supply and demand; using facial recognition programs

to verify the identity of persons entering a country; analyzing criminal activity by overlaying crime data on satellite imagery; analyzing large-scale meteorological data to predict catastrophic storms).

D4. postsecondary education and career prospects

D4.1 research and describe trends in careers that require computer skills, using local and national sources (e.g., local newspaper, national newspaper, career websites);

D4.2 identify opportunities for experiential learning (e.g., co-op programs, job shadowing, career fairs) related to computer science;

D4.3 research and report on postsecondary educational programs leading to careers in the field of information systems and computer science (e.g., institutions offering relevant programs, industry certifications, courses of study, entrance requirements, length of programs, costs);

D4.4 identify groups and programs that are available to support students who are interested in pursuing non-traditional career choices in computer-related fields (e.g., mentoring programs, virtual networking/support groups, specialized postsecondary programs, relevant trade/industry associations);

D4.5 describe the Essential Skills and work habits that are important for success in computer studies, as identified in the Ontario Skills Passport.

Computer Science, Grade 12 University Preparation IC S4U

Algorithm Analysis

C2.4 identify common pitfalls in recursive functions (e.g., infinite recursion, exponential growth in recursive algorithms such as Fibonacci numbers).

D. Topics in Computer Science

Ethical practices

D2.1 investigate and analyse an ethical issue related to the use of computers (e.g., sharing passwords, music and video file downloading, software piracy, keystroke logging, phishing, cyberbullying);

D2.2 describe the essential elements of a code of ethics for computer programmers (e.g., ACM [Association for Computing Machinery] and IEEE [Institute of Electrical and Electronics Engineers] standards) and explain why there is a need for such a code (e.g., plagiarism, backdoors, viruses, spyware, logic bombs);

D3. Emerging Technologies and Society

D3.1 explain the impact of a variety of emerging technologies on various members of society and on societies and cultures around the world and on the economy;

D3.2 investigate an emerging technology and produce a report using an appropriate format (e.g., technical report, website, presentation software, video).

D4. Exploring Computer Science

D4.1 report on some areas of collaborative research between computer science and other fields (e.g., bioinformatics, geology, economics, linguistics, health informatics, climatology, sociology, art), on the basis of information found in industry publications

D4.2 investigate a topic in theoretical computer science (e.g., cryptography, graph theory, logic, computability theory, attribute grammar,

automata theory, data mining, artificial intelligence, robotics, computer vision, image processing);

D4.3 research and describe careers associated with computer studies (e.g., computer scientist, software engineer, systems analyst), and the postsecondary education required to prepare for them;

D4.4 evaluate their own development of Essential Skills and work habits that are important for success in computer studies, as identified in the Ontario Skills Passport.

Computer Programming, Grade 12 College Preparation IC S4C

D2. Ethical Practices

D2.1 investigate and describe an ethical issue related to the use of computers (e.g., piracy, privacy, security, phishing, spyware, cyberbullying);

D2.2 describe the essential elements of a code of ethics for computer programmers, and explain why there is a need for such a code (e.g., plagiarism, backdoors, spyware, unethical programming practices);

D2.3 outline and apply strategies to encourage ethical computing practices at home, at school, and at work.

D3. Emerging Technologies

D3.1 describe the evolution of some emerging programming languages;

D3.2 investigate and report on innovations in information technology (e.g., webcasting, VoIP, multiplayer online gaming) and their potential impact on society and the economy;

D3.3 describe programming requirements for a variety of emerging technologies (e.g., web programming, smartphones, embedded systems).

D4. Computer-related Careers

D4.1 research and report on the range of career opportunities in software development, including duties, responsibilities, qualifications, and compensation;

D4.2 research and report on opportunities for lifelong learning in software development or a computer-related field;

D4.3 evaluate their own development of Essential Skills and work habits that are important for success in computer studies, as identified in the Ontario Skills Passport.

Appendix B - picoCTF learning outcomes

CTF categories

Dependencies / Miscellaneous

1) Linux / Command Line
    a) Students will understand the uses of the command line
    b) Students will be able to ssh to a server
    c) Students will be able utilize nc to connect to a network service
    d) Students will be able to utilize the following commands to Change/Create/Delete Files/Directories:
        i) pwd
        ii) cd
        iii) rm
        iv) cp
        v) mv
        vi) rm
        vii) mkdir
    e) Students will be able to run C executables.
    f) Students will be able to run Python...
        i) … scripts in the command line
        ii) … scripts in a file
    g) Students will be able to open and edit files utilizing the following commands:
        i) cat
        ii) more
        iii) head/tail
        iv) Shell redirection / shell piping
    h) Students will be able to utilize other commands in command line including:
        i) file
        ii) scp
        iii) whoami
    i) Students will be able make and edit files using a command line text editor (such as nano)
    j) Interfacing with the Command Line

i) Students will understand the use of:

(1) stdin / stdout / stderr

ii) Students will be able to utilize pipes.

iii) Students will be able to redirect stdin and stdout to be captured by other commands.

iv) Students will learn how to use man pages

k) Students will be able to utilize the following commands for searching and manipulating files and directories:

i) find

ii) grep

iii) strings

iv) wildcards (*)

l) Students will be able to write basic bash scripts to interact with the command line.

m) Students will be able to understand the difference between relative and absolute paths.

n) Students will be able to set environment variables.

o) Students will be able to make and view hidden files.

2) Students will understand how data is represented on a computer:

a) Different number systems (Binary, Octal, Base-64, Hexadecimal)

b) ASCII (ANSI) text

c) 2s Complement numbers

d) Little/Big Endian

3) Students will understand the difference between physical and virtual environments.

Web

1) Students will be able to view and understand the page source of a web page.

a) Students will be able to identify and understand basic javascript code.

i) Students will be able to identify static comparisons to values in a web page.

ii) Students will be introduced to javascript obfuscation techniques.

2) Students will understand the characteristics and differences between TCP and UDP.
3) Students will understand HTTP as it is used today, and the two main methods of transmitting user data:
    a) Get
    b) Post
4) Students will understand the role a proxy plays
5) Students will be able to understand the use of cookies, including:
    a) editing/modifying
    b) User agent
    c) Session Hijacking
6) Students will understand the use of:
    a) HTTPS
    b) SSL/TLS
7) Students will understand the difference between client side and server side processing.
    a) Students will be able to perform basic SQL queries.
    b) Students will be able to perform basic SQL injection attacks.
    c) Students will be able to perform blind SQL injection attacks.
9) Students will be able to execute shell injection.
    a) Students will be able to execute a PHP injection.
    b) Students will be able to execute a template injection.
10) Students will be able to execute XSS/CSRF.
11) Students will be able to modify/add HTTP headers to outgoing requests
    a) GET
    b) POST

Forensics

1) Students will be able to perform file carving.
    a) Students will understand how headers and footers in files work.
    b) Students will understand how magic numbers function.
2) Students will understand the deleting process and recover deleted files.
3) Students will be able to analyze pcaps of captured data.
4) Students will understand how data can be captured in live environments.

5) Students will be able to extract metadata from a file.
6) Students will understand the shift to mobile forensics and analyze an APK.
7) Students will understand the rationale and basic history of steganography.
    a) Students will be able to use specific programs to extract data.
    b) Students will be able to hide/extract using the least significant bit.
    c) Students will be able to hide/extract data from audio by
        i) Hiding in the shape of the noise
        ii) Using the file
8) Students will be comfortable looking through logs to find malicious activities.

Crypto

1) Students will be able to apply the following password cracking techniques:
    a) Dictionary attacks
    b) Rainbow tables
    c) Salt
    d) Hash Passing
    e) Tools
        i) Jack/John the Ripper
        ii) Hashcat
        iii) Cain and Abel
3) Students will be able to brute force a key with/without mistakes in implementation.
    a) Students will understand the role of entropy in modern cryptography.
    b) Students will be able to use frequency analysis to defeat some crypto systems.
    c) Students will understand what the birthday paradox is and how to apply it to crypto problems.
4) Students will be able to break the following historical progression of ciphers:
    a) Caesar Cipher
    b) Affine Cipher
    c) Vigenere Cipher
5) Students will understand how e-mail is signed and encrypted
6) Students will be introduced to the following crypto primitives:
    a) One-way hash function

b) Authentication
c) Symmetric Key
d) Public Key Crypto (Asymmetric Key)

9) RSA
    a) Students will be able to utilize the following basic attacks on RSA:
        i) primes too small
        ii) wrong exponent released
        iii) n product of more than 2 primes
        iv) reuse n with different exponents
        v) "create your own" plaintext by multiplication

Binaries

1) Students will be able to read C programs
2) Students will understand built-in C types (e.g. word, double-word)
3) Students will be able to understand Assembly, given the C code
4) Students will be able to write basic python programs/script
5) Students will understand what the GCC compiler does
6) Students will understand file formats for binaries (e.g. ELF, PE)
    a) PE/COFF
    b) ELF
7) Students will learn about Registers in Assembly.
8) Students will be able to understand basic Assembly operations
    a) Arithmetic Operations
    b) Control Flow Operations
    c) Logic Operations
9) Students will understand the difference between Big Endian and Little Endian
10) Students will understand the addressing in programs..
11) Students will learn about the memory/section layout of a Binary.
12) Students will learn about Memory Protections (R/RW/RWX)
13) Students will understand the layout of the stack in 32-bit programs.
14) Students will understand the x86/x86-64 calling conventions
15) Students will understand how to locate important information in a binary

a) function symbols
b) Strings

Reversing

1) Students will learn how to read and find documentation for reversing code.
2) Students will get a basic understanding of how C code is compiled to Assembly
3) Students will learn the basics of using a Disassembler
4) Students will learn the basics of using a debugger
    a) Breakpointing
    b) Reading/Writing memory
    c) Following pointers
5) Students will learn about optimizing code through dynamic programming (e.g. memoization)
6) Students will learn about emulation/virtualization
7) Students will learn about common anti-reverse engineering techniques (e.g. blocking ptrace)
8) Students will learn how to patch a binary/file.
    a) Patching bytes
    b) Hooking a function
    c) Recompiling
9) Students will learn how to read through standard decompiled code.
10) Students will gain experience working with foreign architecture assembly.
11) Students will learn how to reverse engineer C++ Code.
12) Students will learn how to use a constraint solver.

Binary Exploitation

1) Students will understand how to interact with binaries using Python programs/libraries (e.g. pwntools)
2) Students will learn how to debug a program using gdb
    a) Running
    b) Stepping
    c) Getting input from file
3) Students will learn how to exploit buffer overflow vulnerabilities
    a) Stack Buffer Overflow
    b) Heap Buffer Overflow

5) Students will learn about format string attacks and how to avoid them.
    a) Understand the risk of a user inputted format string
    b) Leak addresses with a format string
    c) Write arbitrary data to arbitrary addresses using %n
6) Students will learn about signed/unsigned overflow vulnerabilities.
7) Students will learn about techniques to squander exploitation and how to bypass them
    a) Canaries
        i) Spot where canaries are
        ii) Leak canary from stack/heap
        iii) When leaking is unlikely, bruteforce
    b) Stack randomization - ASLR
        i) Nop sled
        ii) Return to libc
        iii) Partial address overwrite
        iv) Brute-force (32-bit)
    c) NX-bit
        i) Retn-libc
        ii) ROP
        iii) Control Flow Integrity (CFI)

8) Students will understand the basics of the C memory allocator (glibc malloc)
    a) Dangling pointer/Use after free
    b) (Potentially) Faking flag bits in heap metadata
    c) Double-free
9) Students will learn how to manipulate data to leak addresses and write to memory
11) Students will gain familiarity with the C standard library
    a) Puts
    b) Printf
    c) Scanf
    d) Fgets
    e) Strncpy
    f) Strcpy

g) Snprintf

12) Students will gain experience dealing with race conditions in code.

The focus areas that CTF competitions tend to measure are vulnerability, discovery, exploit creation, toolkit creation, and operational tradecraft.

General computer security knowledge, Cryptography, Forensics, Reverse Engineering, Decryption, Social Engineering, binary exploitation, web Exploitation