

Networking & Cyber Security

Curriculum: This document can be used as a guide to prepare Canadian Cyber Defence Challenge (CCDC) participants for the competition. Most of the information will be presented to the participants in a very compressed manner. Hence, it is expected from participants to be engaged in self-study activities based on the presented information. The links below provide helpful references to support the fundamentals of cyber security.

Curriculum Outline: The curriculum is broken into four key sections:

1. Introduction to Cyber Security
2. Cyber Security Principles, Threats, and Operating Systems.
3. Networking Tools
4. Networking Tools Continued and System Hardening.

Delivery: For each chapter, it is recommended you research topics in Discover, view the Resources, collaborate in Discussion with your teammates, and engage in self-studies through Practice. We encourage you dive deeper into the topics and go beyond this guideline. It is highly recommended you use a personal computer.

The curriculum is a guide and as such can be modified accordingly to the teaching and learning styles of the instructors and the students.

If schools have any questions regarding this material, they can contact the CCDC as per contact information on the website. The CCDC is committed to ensuring that schools and students feel comfortable to engage in the event. However, master of these topics is not necessary to participate. Ultimately, the challenge event itself serves as the greatest teaching tool for all students.

Chapter 1: Introduction To Cyber Security

Chapter Summary: In this chapter, you will be introduced to the meaning of cyber security and why it is important.

Discover:

- What is Cyber Security?
- Why is cyber security important?
- What cyber security jobs/aspects interest you?
- What is the TCP/IP model and what are some examples of each layer?
- What is HTTP?
- What is a network? Define LAN and WAN
- [Youtube Video - Basic Forensic Concepts](#)

Resources:

- [PDF - Introduction to Cyber Security - Start on slide 12](#)
- [Website: Career Opportunities](#)
- [Google Doc - CCDC Workshop on March 2016](#)

Discussion Topics:

- [PDF - Cyber Ethics](#)
- [Youtube Video - Edward Snowden Interview - Do you agree with Edward Snowden?](#)
- Responsibility on actively securing personal assets such as phones and computers.
- What are the risks to online banking in a public network?
- Why should you not sniff network traffic in a public network?

Practice:

- Imagine clients of an insurance company that are unable to log onto their accounts. How should this incident be handled?

Chapter 2: Cyber Security Principles, Threats, and Linux

Chapter Summary: In this chapter, you will learn about cyber security principles, threats and the Linux operating system. Be prepared to get your hands dirty with some Linux action!

Discover:

- What is Threat Modeling?
- What is encryption and decryption?
- The history of Windows operating system (OS).
- What is Linux?
- The history of Linux OS.

Resources:

- [PDF - Principles of Cybersecurity](#)
- [Youtube Video - Confidentiality, Integrity and Availability](#)
- [Youtube Video - Vulnerabilities, Threat Vectors and Probability](#)
- [Youtube Video - Introduction to Linux and Basic Linux Commands](#)
- [PDF - Linux Cheat Sheet](#)

Discussion Topics:

- What are Cyber Threats?
 - Physical threats vs. online threats.
- What are some differences between Windows and Linux OS?

Practice:

- [Website - Installing Ubuntu inside Windows using VirtualBox](#)
- [Website - More Linux Command Knowledge](#)

Chapter 3: Networking Tools

Chapter Summary: In this chapter, you will be learning how to use Putty, Wireshark and NMap to transfer files and analyze networks.

Discover:

- What is SSH?
- What is FTP?
- What is PuTTY?
- What is WireShark?
- What is the difference between GET and POST?
- What is Nmap?
 - Why is it important to receive written authorization before scanning ports?
 - [Website - NMap Legal Issues](#)
- What is Zenmap?

Resources:

- [Website - PuTTY](#)
- [Website - Wireshark](#)
- [Website - Nmap](#)

Discussion Topics:

Practice:

- [Youtube Playlist - Wireshark Tutorial](#)
- [Youtube Playlist - Nmap Tutorial](#)

Chapter 4: Netcat and System Hardening

Chapter Summary: In this chapter, you will be learning how to use Netcat, access Firewall settings and hardening your systems.

Discover:

- What is Netcat?
- [Website: Understanding Linux Services](#)
- [25 Hardening Security Tips for Linux Servers](#)

Resources:

- [Youtube Video - Netcat - How To Communicate Between Computers](#)
- [Youtube Video - Netcat - Transfer Files](#)
- [Youtube Video - Netcat - Port Scanning](#)

Discussion Topics:

- What does system hardening mean and why is it important?

Practice:

- [PDF - Windows Microsoft Security](#)
- [Website - Windows Firewall With Advanced Security](#)
- [Harden Windows 10 - A Security Guide](#)