**Mohawk College Cyber Security Club**

**Meeting Minutes – October 8, 2020**

Num. of Attendees: 13 Start Time: 7 p.m. End Time: 8:39 p.m.

**Announcements**

* **Game Night**
  + Jordan has posted a poll regarding what games members would be interested in playing during a games night. The poll is in the general chat in the discord channel.
* **SecTor 2020 Discount**
  + October 17th – 22nd
  + Ryan was able to get a discount for club members wishing to participate in Sector 2020 - <https://sector.ca/register/>
  + $50 (down from $300)
  + Email Kevin, Ryan, or the club for more details
* **Collegiate Penetration Testing Competition**
  + November 5th – 9th 2020
  + <https://www.siberx.org/event/cptc/>
* **C3X Rescheduled**
  + <https://www.thec3x.com/>
  + Rescheduled to March 2021
  + Need a team of 10-12 people interested in competing in this blue team exercise as well as at least 2 subs

**Meeting**

* **Guest speaker Shawna Epworth**
  + Currently employed as a SOC Operations Lead at **eSentire.**
  + Security from an MDR perspective, how to succeed in the cybersecurity industry, as well as investigation overviews for Windows logs, network-based incidents, and endpoint-based incidents.
  + Resources from Shawna’s presentation are under the resources section of these minutes
  + linkedin.com/in/shawna-epworth-3a575b10a
  + [Shawna.epworth@esentire.com](mailto:Shawna.epworth@esentire.com)
* **Kevin’s Weekly Challenge Solutions**
  + Beginner password: 3ncrypt\_th1$
  + Advanced password: st@ck\_m@$t3r

**Upcoming Webinars/Events**

* **FHIR 2020 - Without Borders: Accelerating Change During a Global Pandemic**
  + October 14th – 15th - $50+ HST registration fee for students
  + <https://fhirnorth.mohawkcollege.ca/>
  + Application/Security framework for handling and securing clinical data in healthcare. Here’s a good site to learn more about the framework, particularly the Security & Privacy section: <https://www.hl7.org/fhir/>
* **Splunk Conference 2020**
  + October 20th-21st – Free!
  + <https://conf.splunk.com/>
* **Getting Started in Security with BHIS and MITRE ATT&CK w/ John Strand**
  + November 16th-18th - Pay what you want ($0-$395) codes listed on website
  + 16 Hours – 4 days of 4 hour sessions, meeting times listed on website
  + <https://register.gotowebinar.com/register/9119087065621045518?source=wwhf>

**Resources**

* **YouTube series for folks looking to get into malware analysis:**
  + <https://www.youtube.com/playlist?list=PLiFO-R_BI-kAqDPqtnOq2n70mtAZ6xg5N>
* **Malware Analysis Blogs from Active Countermeasures (ACM):**
  + <https://www.activecountermeasures.com/category/malware-of-the-day/>
* **A more complete list of status codes and their meanings:**
  + <https://msdn.microsoft.com/en-us/library/cc704588.aspx>
* **A list of Windows Event Codes, their meanings, and additional information:** 
  + <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/Default.aspx>
* **An excellent resource for packet captures and analysis information:** 
  + <https://www.malware-traffic-analysis.net/>
* **Robust decoding/encoding tool:**
  + <https://gchq.github.io/CyberChef/>