**Mohawk College Cyber Security Club**

**Meeting Minutes – October 1, 2020**

Num. of Attendees: 9 Start Time: 7 p.m. End Time: 8:30 p.m.

**Announcements**

* Near the end of each week will be a series of weekly challenges Kevin will leave the group to solve and solutions to the challenges will be taken up as a group in the next meeting! Be on the lookout on Discord for this week’s challenge! Challenges can be anything from decrypting a cipher code to analyzing a Wireshark file. Feel free to share your solutions in the ‘challenge solutions’ channel if you like!

**Meeting**

* **Over the Wire – Bandit**
  + <https://overthewire.org/wargames/bandit/>
  + Picking back up at Level 11 > 12
    - The command ‘tr’ (translate) is used to translate or delete characters, useful for simple cryptography
    - [https://www.tecmint.com/tr-command-examples-in-linux/](https://simple.wikipedia.org/wiki/Hexadecimal#:~:text=The%20hexadecimal%20numeral%20system%2C%20often,numbers%20and%20six%20extra%20symbols.)
  + Level 12 > 13
    - Hexadecimal format: <https://simple.wikipedia.org/wiki/Hexadecimal>
    - ‘file’ command is used to determine the type of a file: [https://www.geeksforgeeks.org/file-command-in-linux-with-examples](https://www.geeksforgeeks.org/file-command-in-linux-with-examples/#:~:text=file%20command%20is%20used%20to,%3Dus%2Dascii').)
    - ‘xxd’ command can be used to make a hexdump, or reverse one (use the flag ‘-r’)
    - Uncompleted
* **TryHackMe - Crash Course Pen Testing Room**
  + <https://tryhackme.com/room/ccpentesting>
  + For help downloading VPN and connection file:
    - <https://tryhackme.com/faq>
  + Nmap is a port scanning and network exploration tool
    - <https://nmap.org/book/man.html>
  + Netcat (nc) allows you to connect to ports to send and receive data, is a popular tool for reverse shells
    - <https://kapeli.com/cheat_sheets/Netcat.docset/Contents/Resources/Documents/index>
  + Finished Task 3/24

**Upcoming Webinars/Events**

* **Catch some of the Wild West Hackin’ Casts, and learn about the Fundamentals of Exploit Development**
  + October 8th
  + <https://wildwesthackinfest.com/wild-west-hackin-casts/>
* **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**

* Haven’t got your Kali VM yet? Here’s the link to the 2020.3 version for VirtualBox. Gives access to nmap and ncat tools:
  + <https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/#1572305786534-030ce714-cc3b>
* Ever want to get into Digital Forensics and Incident Response (DFIR), but can’t find a resource to hone your skills on? Take a crack at **The Stolen Szechuan Sauce**challenge!
  + <https://dfirmadness.com/the-stolen-szechuan-sauce/>
* The links below are an introduction to how ciphers work. If you like puzzles, this can be something fun for you to solve!
  + ROT13 (Rotation 13) Cipher:
    - https://en.wikipedia.org/wiki/ROT13
    - <http://practicalcryptography.com/ciphers/classical-era/rot13/>
  + Here are some other Ciphers to check out:
    - <http://practicalcryptography.com/ciphers/classical-era/>
* Some suggested organizations to follow that do awesome training webcasts on various topics in security and a recommended podcast to check out!
  + **Wild West Hackin Fest: Webcasts and Training**
  + **Black Hills Information Security**
  + **Darknet Diaries**