Mohawk College Cyber Security Club

Meeting Minutes – February 18th, 2021

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

Announcements

- Nominations for executive positions are closing on Sunday. Nominate yourself or another member here: https://forms.gle/CTmq6rg1joNy5mG46

Meeting

- **Jay Tymchuk – Guest Speaker**
  - NESA graduate
  - Twitter - @JayInfoSec, Website – securitydebriefing.com
  - APT – Advanced Persistent Threat
  - Anatomy of an attack = Delivery > Installation > Gain Authority > Laterally Move > Collect Data > Exfiltrate Data
  - An attacker's #1 goal is to achieve a domain admin
  - Everything in Windows is tied to an account, credentials are the "keys to the kingdom"
  - MITRE ATT&CK Framework
  - Different organizations provide different incident response recycle models
  - Many organizations don't have the capability to respond to advanced intrusions
  - Median dwell time is around 2 months
  - Detection (IDS/Threat Intel) also requires verification before action can be taken
  - Reactive organizations vs. Hunting organizations
  - Three main types of event logs = application, system, security
  - Hacker tool spotlight: Bloodhound
  - %COMSPEC% is the environment variable for cmd.exe
  - Adversaries may try to clear the event log to hide their tracks – watch for this
  - Event logs can not be overwritten but can be cleared – clearing is all or nothing, no individual event clearing

Resources

- List of upcoming CTFs
  - https://ctftime.org/event/list/?year=2021&online=-1&format=0&restrictions=-1&upcoming=true

- MITRE ATT&CK Framework
    - https://attack.mitre.org/
- Windows Event IDs to Know
    - https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor
- Ultimate Windows Security
    - https://www.ultimatewindowssecurity.com/
- Applied Incident Response Cheat Sheets
    - https://www.appliedincidentresponse.com/
- SANS Cheat Sheet Posters
    - https://digital-forensics.sans.org/community/posters