Assignment 1 Questions

x) Read and summarize. Some bullets is enough for a summary.

* [Hutchins et al 2011: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains](https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf). Update: Chapters Abstract, 3.2 Intrusion Kill Chain and 3.3 Courses of Action.
* [Darknet Diaries](https://darknetdiaries.com/). Pick one episode.
* [MITRE ATT&CK FAQ](https://attack.mitre.org/resources/faq/) explains the [ATT&CK Enterprise Matrix](https://attack.mitre.org/matrices/enterprise/). Explain tactic, technique and procedure in context of ATT&CK, and give an example of each. The enterprise matrix is big, you can just glimpse/browse it to see what's available instead of reading hundreds of pages.

1. How would you compare Cyber Kill Chain and ATT&CK Enterprise matrix? Who do you think could benefit from these models? (Bonus: Do you think anything is missing from either of these models?)
2. Update: Voluntary: Use either (Hutchins et al 2011) cyber kill chain or MITRE ATT&CK framework for analyzing the incident you of choosing. You can pick any incident you want, but try to pick a source that gives you enough technical and business detail to do some analysis. (If you're in a hurry, cyber kill chain is much simpler. If you're technically skillful, you might find ATT&CK interesting)

**Answers**

***Task (x)***

* **A kill chain** is a systematic process to target and engage an adversary to create desired effects
* Steps of this process as find, fix, track, target, engage, assess (F2T2EA): find adversary targets suitable for engagement; fix their location; track and observe; target with suitable weapon or asset to create desired effects; engage adversary; assess effects (U.S. Department of Defence, 2007
* The essence of an **intrusion i**s that the aggressor must develop a payload to breach a trusted boundary, establish a presence inside a trusted environment, and from that presence, take actions towards their objectives, be they
* moving laterally inside the environment or violating the confidentiality, integrity, or availability of a system in the environment.
* The intrusion kill chain is defined as reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives
* Zero-day exploit: A zero-day attack happens once that flaw, or software/hardware vulnerability, is exploited and attackers release malware before a developer has an opportunity to create a patch to fix the vulnerability



* Target was to get the company financial information days or even hours before it is released to the public via ‘newswires’ (of which there are three main ones) in order to make stock moves ahead of the announcements.
* The hacker broke into the servers through the SQL applications forms, or anywhere you have a text box, through ‘brute force’
* Took around 5 years before SEC was able to capture the adversaries through their ‘ARTEMIS’ system (from the description, I gathered it similar to ATT&CK enterprise mod of defence because it is *“like an enormous database system that holds trade records from across the sector, and it uses mathematical algorithms and advanced analytics to analyze and rank the trades depending on what the SEC is looking for”*
* Everyone got caught. Around $30Mil were made through this insider trading scheme.
* The interesting thing is similar to Max Butler (the Iceman), hackers were going after each other because they wanted a piece of the pie.

***To Question (a):***

I think quick way to describe is that ATT&CK is a body of knowledge, meta data if you will, that breaks down and learns how adversaries managed to or attempted to hack the enterprise IT network or mobile devices, while Killchain is a structured process that defines a the method or structure of the hack in order to defend the system and get ahead of the incursion before any real damage is done. (or before they get to C2). The beneficiaries of both models are any enterprise that holds data, designs, or information that can otherwise be used to harm or disable human life. Ie transportation, electricity grid, weapons, finances, ets..

For the bonus section: I can’t think of anything. I don’t know enough. I feel based on the podcasts I’ve heard so far and what I’ve read there is always a sense of reaction vs proaction. But that is impossible to guess.

***To Question (b):***

I went into this site first to get a list of hacks.

<https://www.indusface.com/blog/12-notorious-hacks-history/>

I selected the Max Ray Butler hack – a.k.a The Iceman Hacks – because I found it funny that he wanted to be the one-stop shop to the card thieves and other blackmarket.. markets.

Then I searched for any in-depth discussion or article but couldn’t find any when checking through google. I decided to use duckduckgo instead and immediately got 4 or 5 deep-dives. I decided to read and try to analyse via several sites like [this one](https://medium.com/mr-kr%C3%BCgers-world-of-crypto/how-icemans-epic-48-hour-hack-resulted-in-the-reign-of-cardersmarket-com-9f8b0eb48f7f) and [wired](https://www.wired.com/2008/12/ff-max-butler/)

I will try to use the killchain method to break down how I think he did his hack. So these are the Reconnaissance, weaponization, delivery, exploitation, installation, Command and control (C2). I have to assume his reconnaissance was simply learning or watching how the carder websites operated (I am sure he already knew but I suppose he had to “walk around” the site and code first). His method of entering was **weaponizing a password** and then **delivering that password through SQL** by *“tricking their SQL database servers into running his own commands or simply slipping in with a hacked password”* (Poulsen, 2008). The password then **exploits the system** in which he able to take all the data, content, logins, accounts info of everyone who was using the site to purchase card data and then erasing it all from their servers. Finally, he **commanded and controlled** the data and made it known to all the users where he informed them that “*Whether they liked it or not, they were now members of his own site, CardersMarket.com”* (Poulsen, 2008)

***To Question (c):***

Installing virtual machine. I used my old work laptop to do this as it is clean and nothing important is on it.. well, except my virtual riding app for cycling.

Here are the snapshots of the installation

Graphical user interface

Description automatically generated

After installing and going into the desktop for the first time

Graphical user interface, text, application, email

Description automatically generated

Snapshot of the my environment

Graphical user interface, website

Description automatically generated

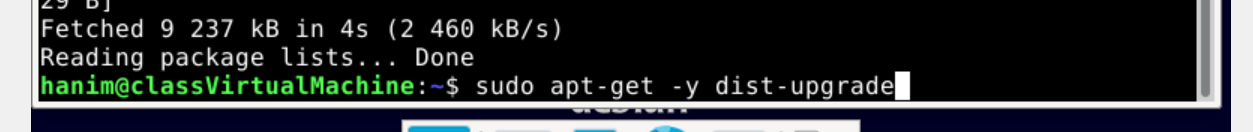
Browsing works fine (website is ultra gravel ride in Spain)

Text

Description automatically generated

Getting the updates

Graphical user interface, text

Description automatically generated

Installing the updates

Graphical user interface, text, application, email

Description automatically generated

Text

Description automatically generated

Something about auto updating the Grub

Graphical user interface

Description automatically generated

Setting up the firewall.

I didn’t feel the need to update to the guest view because I was ok with just selecting “View” in the virtual machine and upgrading the window to 150%. Maybe I will do it another time if needed.