****

**Course: CYB302**

 **Ethical Hacking
(Canadian Context)**

 **Lab 1: Hacker Mindset and Cyber Kill Chain**

 **Coordinator and Instructor:**

 **Muhamma Saleem**

**Student Name: Olushola Enoch Bayode**

**Student ID: 23077087**

**Section: 3rd Semester**

 **Activity 1:**

 **Adopting the Hacker Mindset**

**Think about the grocery store where you normally shop.**

* **What are some of the security measures used by that store to prevent the theft of cash and merchandise?**

**Answers:**

1. CCTV Cameras: the use of cctv cameras helps keep tab on all the ongoings of the store, whether it’s a big or medium size store, its not customer friendly walking around with every customer it would cost a lot but with cctv camera you can watch every customer as they shop whatever they want.
2. Security Guards: This personnel helps put some checks on the store so as not to let things get missing which could result to a great loss to the store.
3. Product Tag: This simple device helps keep the store’s product safe from being stolen.
4. Door Detection: For every product tag there needs to be an alarm fixed on the door to enable the store to know when products are being taken out of the store without being paid for either intentionally or unintentionally.
* **What ways can you think of defeating those controls?**

**Answers:**

1. Security awareness: Security awareness for both the owner, employee (cashier), guards.
2. Security Guards: Guards helps a lot by cross-checking the receipt to the goods bought to avoid theft, helps creating order and apprehend defaulters or fraudulent people who intends to impersonate.
3. CCTV cameras: There should be blind spot consideration when installing cameras (theft by the cashiers or robbers evading the store), making the cctv cabled to avoid being hacked into or additional firewall to prevent hacking into the WIFI in the case of WIFI powered cameras which helps for owners who wants to monitor from anywhere.
4. Good Doors: There should be a good door and thick glass installed so it can prevent break-ins or escapes.
5. Social Engineering: Part of the security awareness should cover how phishing links, vishing, smishing can lead to privacy disclosure or the store finance being looted.

**Activity 2: Using the Cyber Kill Chain
Choose a real-world example of a cybersecurity incident from recent news. Select an example in which there is a reasonable amount of technical detail publicly available.**

* **Describe this attack in terms of the Cyber Kill Chain:**

This is a model created by Lockheed Martin that spells out the stages of cyber attack from gathering evidence to execution of the attack.

* **How did the attacker carry out each step of the process?
Were any steps skipped?**

Each step of every process or attack consists of the following, Reconnaissance, Objectives, Weaponization, Delivery, Exploitation, ICC.

* **If there is not enough information available to definitively address an element of the Cyber Kill Chain, offer some assumptions about what may have happened.**

Taking for instance or example the attack which happened on December 2024, an attack was waged on European Space Agency’s Official Web store. The website was attacked / compromised to steal card information from customers.

**Reconnaissance**: Attackers probably made their research to identify loopholes in the European Space Agency’s Official Web store, likely focusing on unused, outdated plugins or software components, directory listing in the website.

 **Objectives**: The main objective of data theft is to harvest payment details from customers, buying products on the European Space Agency’s Official Web store.

**Weaponization**: There are different mode by which weapons to harvest the intended data but malicious code designed and spurned into the system to exploit the known vulnerability, most especially the targeted payment system.

**Delivery**: bad codes are injected into the the European Space Agency’s Official Website either through XSS scripting or using SQLi or any other codebase or database through a bad third-party plugin, subnet, link or direct exploitation of a loophole.

**Exploitation**: As soon as users access the compromised website, the evil code is executed, redirecting them to a clone payment page, fake payment page while they do password dumping so they can access your data later while still ensuring you don’t detect it was all a coy.

**Installation**: The installation phase consists of the process of embedding malicious script within the website code, ensuring it runs when users access the payment page.

**Control and Command**: The bad code mostly sent the stolen data to a server owned by the attacker, create a convert channel for data exfiltration.

**Reference**

[**https://itsecuritycanada.blogspot.com/**](https://itsecuritycanada.blogspot.com/)