Assignment 7

Name : Ishan Aakash Patel

Student ID : 146151238

Course : CYT-245

Task – 1 - Familiarize yourself with VERIS components (data collection framework, VCDB, and DBIR)

What is an Incident Pattern?

An incident pattern is a way to categorize cybersecurity incidents based on common characteristics, such as the method of attack, the target, and the outcome. This categorization helps in understanding and responding to security incidents more effectively by identifying trends and commonalities among different types of incidents. For example, incidents involving unauthorized access to systems may be grouped under a pattern like "System Intrusion." These patterns allow organizations to focus on specific types of threats and tailor their defenses accordingly.

Current Incident Patterns

The 2023 Data Breach Investigations Report (DBIR) identifies several major incident patterns that are prevalent in the cybersecurity landscape. Here are some of the key patterns:

1. **Basic Web Application Attacks**: These attacks target vulnerabilities in web applications, often to steal data or gain unauthorized access. Attackers may use techniques like SQL injection or cross-site scripting to exploit weaknesses in a web application.

2. **Denial of Service (DoS)**: This pattern involves overwhelming a system, network, or service with traffic to make it unavailable to users. DoS attacks can be carried out using botnets, where multiple systems are used to send excessive traffic to the target.

3. **Lost and Stolen Assets**: This pattern includes incidents where physical assets, such as laptops or mobile devices containing sensitive data, are lost or stolen. The loss of these assets can lead to unauthorized access to the data they contain.

4. **Miscellaneous Errors**: This pattern covers incidents caused by human error, such as misconfiguring a server or accidentally sending sensitive data to the wrong person. These errors can lead to data breaches and other security incidents.

5. **Privilege Misuse**: This pattern involves the misuse of authorized access by insiders, such as employees or contractors, to steal data or cause harm to the organization. This could involve accessing sensitive information without authorization or exceeding access permissions.

6. **Social Engineering**: This pattern includes techniques that manipulate individuals into divulging confidential information or performing actions that compromise security. Phishing, where attackers send deceptive emails to trick individuals into revealing sensitive information, is a common example.

7. **System Intrusion**: This pattern involves attackers gaining unauthorized access to systems, often through hacking or malware. System intrusions can lead to data breaches, theft of intellectual property, or ransomware attacks where data is encrypted and held for ransom.

Each of these patterns represents a different way that security can be compromised, highlighting the diverse tactics and techniques used by attackers.

Analysis of Figure 26

Figure 26 in the DBIR provides a visual representation of the prevalence of various incident patterns over time. The figure shows that "System Intrusion" has become one of the most common patterns, reflecting the increasing sophistication and targeting of cyberattacks. This pattern is particularly concerning because it often involves complex attacks, such as ransomware, that can have severe consequences for organizations. The figure also highlights that "Social Engineering" and "Privilege Misuse" are significant contributors to data breaches, emphasizing the importance of securing both technology and human elements within organizations.

Example: System Intrusion

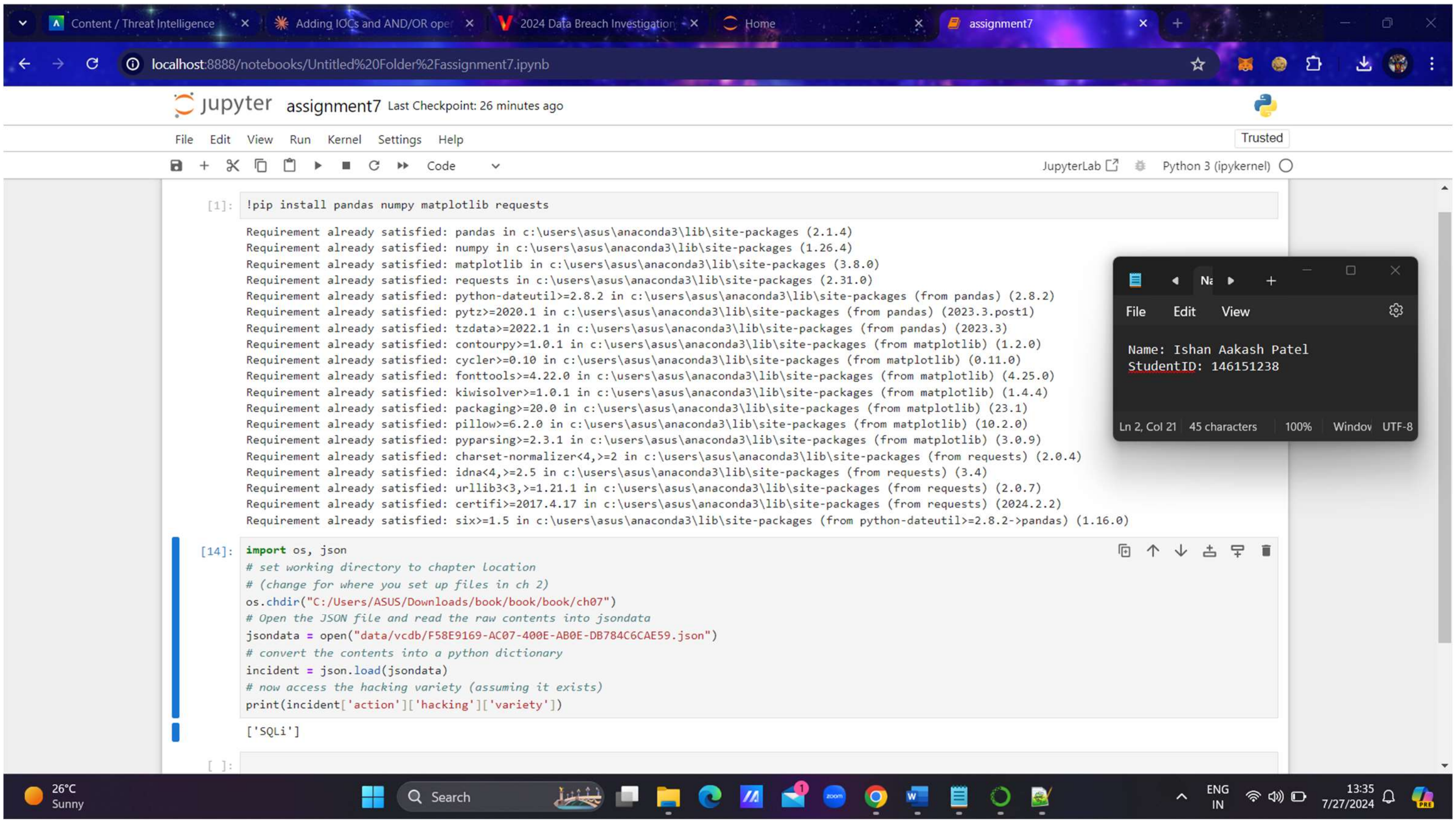
A detailed example of the "System Intrusion" pattern involves an attack where hackers gain unauthorized access to a company's network. The attack may begin with a phishing email that tricks an employee into clicking on a malicious link, leading to the installation of malware. Once inside the network, the attackers use tools to escalate privileges, allowing them to move laterally within the network and access sensitive data. The attackers may then deploy ransomware, encrypting the company's data and demanding payment for the decryption key. This type of attack can have devastating effects, including financial loss, operational disruption, and damage to the organization's reputation.

In one case, a company experienced a system intrusion after an employee clicked on a phishing link that appeared to come from a trusted source. The malware installed on the employee's computer gave the attackers access to the company's internal systems. The attackers then used this access to identify and exfiltrate sensitive data, including customer information and proprietary business data. After several days, the attackers encrypted the company's data and demanded a ransom payment in cryptocurrency to restore access. This incident highlights the importance of robust cybersecurity measures, including employee training, strong access controls, and regular security audits, to prevent and mitigate such attacks.

Conclusion

The 2023 DBIR underscores the importance of understanding incident patterns to improve cybersecurity defenses. By recognizing the common patterns of cyber incidents, organizations can better anticipate and defend against potential threats. The report's insights into patterns like "System Intrusion," "Social Engineering," and others provide a roadmap for organizations to enhance their security posture and protect sensitive information. Through a combination of technical defenses and awareness training, organizations can reduce the risk of data breaches and other security incidents, safeguarding their assets and reputation.

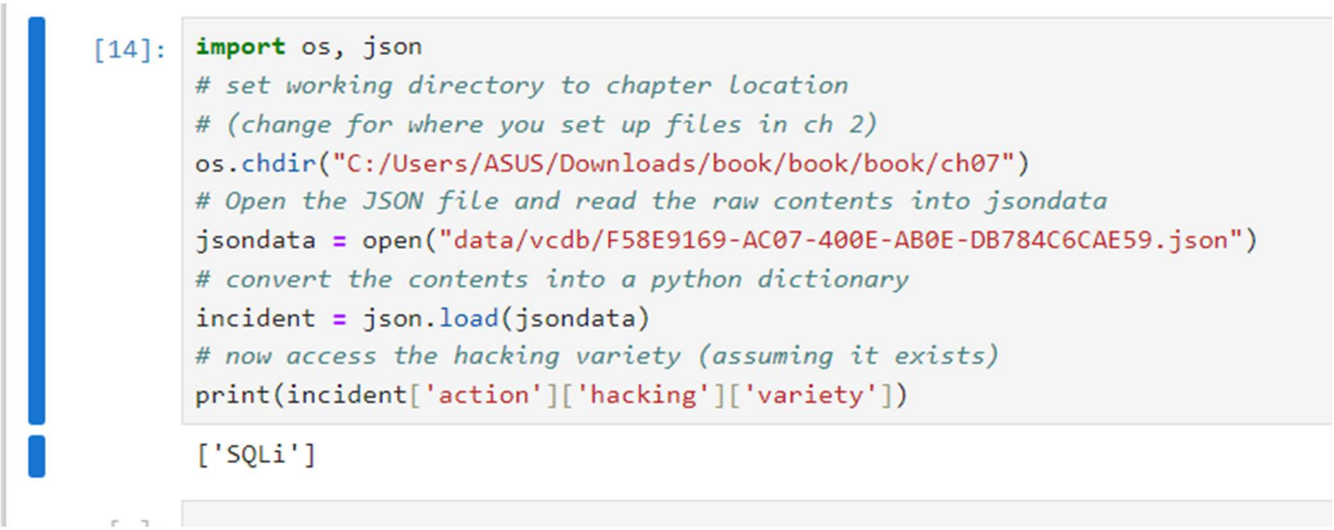
Task – 2


Content / Threat Intelligence
Adding IOCs and AND/OR oper
2024 Data Breach Investigation
Home
assignment7
localhost:8888/notebooks/Untitled%20Folder%2Fassignment7.ipynb
jupyter
assignment7 Last Checkpoint: 26 minutes ago
File Edit View Run Kernel Settings Help
Trusted
Code
JupyterLab
Python 3 (ipykernel)
26°C
Sunny
Search
ENG
IN
13:35
7/27/2024

```
[1]: !pip install pandas numpy matplotlib requests

Requirement already satisfied: pandas in c:\users\asus\anaconda3\lib\site-packages (2.1.4)
Requirement already satisfied: numpy in c:\users\asus\anaconda3\lib\site-packages (1.26.4)
Requirement already satisfied: matplotlib in c:\users\asus\anaconda3\lib\site-packages (3.8.0)
Requirement already satisfied: requests in c:\users\asus\anaconda3\lib\site-packages (2.31.0)
Requirement already satisfied: python-dateutil>=2.8.2 in c:\users\asus\anaconda3\lib\site-packages (from pandas) (2.8.2)
Requirement already satisfied: pytz>=2020.1 in c:\users\asus\anaconda3\lib\site-packages (from pandas) (2023.3.post1)
Requirement already satisfied: tzdata>=2022.1 in c:\users\asus\anaconda3\lib\site-packages (from pandas) (2023.3)
Requirement already satisfied: contourpy>=1.0.1 in c:\users\asus\anaconda3\lib\site-packages (from matplotlib) (1.2.0)
Requirement already satisfied: cycler>=0.10 in c:\users\asus\anaconda3\lib\site-packages (from matplotlib) (0.11.0)
Requirement already satisfied: fonttools>=4.22.0 in c:\users\asus\anaconda3\lib\site-packages (from matplotlib) (4.25.0)
Requirement already satisfied: kiwisolver>=1.0.1 in c:\users\asus\anaconda3\lib\site-packages (from matplotlib) (1.4.4)
Requirement already satisfied: packaging>=20.0 in c:\users\asus\anaconda3\lib\site-packages (from matplotlib) (23.1)
Requirement already satisfied: pillow>=6.2.0 in c:\users\asus\anaconda3\lib\site-packages (from matplotlib) (10.2.0)
Requirement already satisfied: pyparsing>=2.3.1 in c:\users\asus\anaconda3\lib\site-packages (from matplotlib) (3.0.9)
Requirement already satisfied: charset-normalizer<4,>=2 in c:\users\asus\anaconda3\lib\site-packages (from requests) (2.0.4)
Requirement already satisfied: idna<4,>=2.5 in c:\users\asus\anaconda3\lib\site-packages (from requests) (3.4)
Requirement already satisfied: urllib3<3,>=1.21.1 in c:\users\asus\anaconda3\lib\site-packages (from requests) (2.0.7)
Requirement already satisfied: certifi>=2017.4.17 in c:\users\asus\anaconda3\lib\site-packages (from requests) (2024.2.2)
Requirement already satisfied: six>=1.5 in c:\users\asus\anaconda3\lib\site-packages (from python-dateutil>=2.8.2->pandas) (1.16.0)
```

```
[14]: import os, json
# set working directory to chapter location
# (change for where you set up files in ch 2)
os.chdir("C:/Users/ASUS/Downloads/book/book/book/ch07")
# Open the JSON file and read the raw contents into jsondata
jsondata = open("data/vcdb/F58E9169-AC07-400E-AB0E-DB784C6CAE59.json")
# convert the contents into a python dictionary
incident = json.load(jsondata)
# now access the hacking variety (assuming it exists)
print(incident['action']['hacking']['variety'])

['SQLi']

[ ]:
```

```
Name: Ishan Aakash Patel
StudentID: 146151238
```



```
[14]: import os, json
# set working directory to chapter location
# (change for where you set up files in ch 2)
os.chdir("C:/Users/ASUS/Downloads/book/book/book/ch07")
# Open the JSON file and read the raw contents into jsondata
jsondata = open("data/vcdb/F58E9169-AC07-400E-AB0E-DB784C6CAE59.json")
# convert the contents into a python dictionary
incident = json.load(jsondata)
# now access the hacking variety (assuming it exists)
print(incident['action']['hacking']['variety'])

['SQLi']
```

The output ['SQLi'] indicates that the 'variety' of hacking in this particular incident was SQL injection.

1. ['SQLi'] is a Python list containing a single string element 'SQLi'.
2. 'SQLi' stands for SQL Injection.
3. SQL Injection is a type of cyber attack where malicious SQL statements are inserted into application queries to manipulate the database.

In the context of the VCDB (VERIS Community Database):

- This output reveals that the incident recorded in the JSON file involved a hacking attack.
- The specific 'variety' of hacking was SQL injection.
- Classifying incidents in this way helps in organizing and analyzing cybersecurity events.

SQL injection attacks can be particularly severe, as they may allow attackers to:

- Access sensitive data in the database
- Alter or delete database content
- Perform administrative operations on the database
- Execute commands on the operating system
- Potentially take control of the entire system