****

**DEPARTMENT OF**

**COMPUTER SCIENCE AND ENGENEERING**

**(CSHO331CSP)**

**ETHICAL HACKING**

**Assignment Report**

**Name: Patrick Pio**

**Register Number: 2460420**

***B. Tech – Computer Science and Engineering***

**School of Engineering and Technology,**

**CHRIST (Deemed to be University),**

**Kumbalagodu, Bengaluru-560 074**

**1. Initial Access (April 29, 2021)**

* Hackers gained entry into Colonial Pipeline's network using a **compromised password** for a **VPN (Virtual Private Network)** account.

**What went wrong:**

* The VPN account was **inactive but not disabled**.
* **Multi-Factor Authentication (MFA)** was **not enabled**.

**How it could have been prevented:**

* **Disable unused accounts** immediately.
* **Enforce MFA** on all remote access systems.

**2. Infiltration by DarkSide Ransomware Group**

* The threat actors belonged to a **cybercriminal group called DarkSide**.
* After gaining access, they **moved laterally** within the network, identifying key systems to encrypt.
* They targeted the **IT (Information Technology) systems**, not the pipeline's operational controls (OT systems).

**What went wrong:**

* Lack of **network segmentation** allowed lateral movement.
* Inadequate **monitoring** of internal activity.

**How it could have been prevented:**

* Implement **network segmentation** to limit access between systems.
* Use **Intrusion Detection/Prevention Systems (IDS/IPS)** and **log monitoring** to detect abnormal activity.

**3. Ransomware Deployment (May 7, 2021)**

* The attackers **deployed ransomware**, encrypting around **100 GB of critical business data**.
* They **exfiltrated data** beforehand to use as leverage for a **double extortion**—threatening to release stolen data if the ransom wasn’t paid.

**What went wrong:**

* Colonial had no **behavioral ransomware detection** in place.
* **No data loss prevention** measures to block exfiltration.

**How it could have been prevented:**

* Use **ransomware-specific defenses** like file behavior analytics.
* Apply **Data Loss Prevention (DLP)** tools to detect and block outbound data theft.

**4. Colonial Pipeline Shuts Down Operations**

* Out of caution and fear of the attack spreading, **Colonial voluntarily shut down the pipeline**.
* This led to a **massive fuel supply disruption** across the U.S. East Coast.

**What went wrong:**

* **No clear separation** between IT (business) and OT (operations) networks.
* No **tested incident response plan** for cyberattacks on critical infrastructure.

**How it could have been prevented:**

* **Isolate OT systems** from internet-facing IT networks.
* Develop and routinely **test an incident response plan** tailored to ransomware scenarios.

**5. Ransom Paid in Cryptocurrency**

* Colonial Pipeline paid **75 Bitcoin** (around **$4.4 million USD**) to DarkSide for a decryption tool.
* However, the tool worked **very slowly**, so Colonial mostly relied on **its own backups** to restore operations.

**What went wrong:**

* The company was **not confident in backup recovery**.
* Paying ransom **incentivized future attacks**.

**How it could have been prevented:**

* Maintain **robust, regularly tested offline backups**.
* Ensure backups are **segregated from the main network** to avoid encryption.

**6. Aftermath and FBI Response**

* On **May 12, 2021**, Colonial resumed full pipeline operations.
* The **FBI recovered part of the ransom** (~63.7 BTC) by tracking the payment and accessing a wallet.
* The U.S. government intensified efforts on **cybersecurity for critical infrastructure** following the attack.

**What went wrong:**

* Colonial lacked **real-time reporting** and **public-private threat sharing** at the time of the attack.

**How it could have been prevented:**

* Foster **real-time communication** with law enforcement and security agencies.
* Participate in **Information Sharing and Analysis Centers (ISACs)** for critical infrastructure.