## WEEK 5 ASSIGNMENT

Answer the following questions using references. Provide detailed explanations with examples.

**1. Research and identify a cybersecurity attack in the news that was the result of a malicious code attack. Describe the attack, the impact of the attack, and explain what kind of malicious code attack was used (e.g. Trojan, keystroke logger, Ransomware, etc.) Identify 2-3 steps the organization could have taken to prevent and/or mitigate the impact of the attack. Make sure to provide references and links to online articles about the attack.**

- One of the most recent notable attacks was the "Colonial Pipeline" where hackers we able to use a leaked password to infiltrate their network. The password was a key access point to the companies vpn that they used which gives access to the entire network. Since the VPN account didn't use multifactor authentication hackers were able to easily walk right into the network with said password. Then hackers simply went through the network devices and installed ransomware on them which prompted the company to pay their defined ransom of 4.4 million in crypto.

- Now obviously the largest hole in the security is that their users are not using multifactor authentication which hinders the ability for anyone to use a discovered password. Using this method limits the known possibility of password leaks and sharing among employees who are often the greatest weakness of security for a company.

Link: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

**2. An electronic mail system can be used to leak information. First explain how the leakage could occur. Then identify controls that could be applied to detect or prevent the leakage.**

- With the creation of e-mail, information leaking has become a common problem in today's world. This problem is even greater for companies who send and receive more emails than anyone, making manual monitoring impossible. Some leaks could be as simple as user error where the wrong people are sent or cc on an email. But more advanced leaks have to do with hackers monitoring the networks of the company and intercepting messages. This could be done from admin devices or accounts, or just hacking an email server that routes all the emails for the company.

- Some controls that are common among large companies are content filters that can be put in place to filter through incoming and outgoing emails. Some others are rules that only allow files to be sent to authorized accounts within the network. There are also methods of email encryption that would limit the people that could read and email despite intercepting it.

**3. Explain how information in an access log could be used to identify the true identity of an imposter who has acquired unauthorized access to a computing system. Describe several different pieces of information in the log that could be combined to identify the imposter.**

- As you have a web server you have access to the web server logs, so you could log quite a bit of information about visitors to the site, and you might be able to use that to specifically identify someone visiting the site regardless of who they log in as. If you then have access to the client systems of the potential imposter you could use the browser fingerprint to provide evidence that it was them who accessed the system. The same is true for most computer systems where detailed information is shown about who is accessing a system. Protections could be put in place for alerting IT if a new user is shown accessing a system that has defined users on it. Most servers for example log the IP address of users that are logging in. This could help to identify someone that is off your network that is gaining access to your server.

**4. a) You receive an email message that purports to come from your bank. It asks you to click a link for some reasonable sounding administrative purpose. How can you verify that the message came from your bank?**

- Some of the easiest ways is to look at the sent from email address and compare to older emails. Another method is to inspect the link and then compare that to your banks domain which then adds some confirmation on where it’s sending you. Lastly the easiest way to pin a email as a phishing or possible damaging email is does it contain urgency. The most common phishing technics that are used in this scenario promote some sort of urgency so that you want to click the link to resolve the problem.

**5. b) Now play the role of an attacker. How could you intercept the message described in part (a) and convert it to your purposes while still making both the bank and customer think the message is authentic and trustworthy?**

- Not totally clear on the scenario here but next steps as the attacker for a phishing email after someone clicks on the link is to spoof a login page of the bank. Then grab login credentials while also transferring the user to the real bank site. This allows the user to not know an attack has taken place and gets you the credentials. Then just use the credentials. There is no reason to make the bank trust you since you have the credentials? They should already trust whoever has credentials but depending on implemented security some banks have new device login features that can deter this setup. So, for arguments sake you would need to gain access of the user’s typical device first and then login and change information and settings to bypass this.