ITEC442 IOT & Cyber Security

Week 3-4

Solar Winds exploit using the Cyber Kill Chain

Questions:

- Create a table that analyses the solar winds exploit using the Cyber Kill Chain. Are there any phases that you cannot identify?
- Create a list of possible mitigations for each phase. Are there any phases you cannot mitigate?
- What tools would you utilize in each phase? Give reasons for your answer.

Answers:

Here is a table that analyzes the solar winds exploit using the Cyber Kill Chain:

Phase	Description	Possible Mitigations	Tools
Reconnaissance	The attacker gathers information about the target network, such as network architecture and system vulnerabilities.	- Implement network segmentation and access controls to limit the attacker's ability to gather information. - Regularly update software and systems to patch vulnerabilities. - Use security tools such as firewalls and intrusion detection systems to monitor network activity and alert on suspicious behavior.	- Network scanners and vulnerability assessment tools - Open source intelligence (OSINT) gathering tools
Weaponization	The attacker creates a malicious payload, such as a virus or exploit, and prepares it for delivery to the target.	- Implement strong email and web filtering to block malicious attachments and links. - Regularly update and patch software and systems to prevent exploitation of known vulnerabilities. - Use security tools such as antivirus software and endpoint protection to detect and block malicious payloads.	- Malware creation tools - Exploit development frameworks
Delivery	The attacker delivers the malicious payload to the target, typically through	- Implement strong email and web filtering to block malicious attachments and links. - Use security tools such as firewalls and intrusion prevention systems to block malicious network	- Email spamming tools - Web exploitation frameworks

	email, a website, or a network connection.	traffic. - Regularly update and patch software and systems to prevent exploitation of known vulnerabilities.	
Exploitation	The attacker uses the delivered payload to exploit a vulnerability in the target system and gain access.	- Regularly update and patch software and systems to prevent exploitation of known vulnerabilities. - Use security tools such as firewalls and intrusion prevention systems to block malicious network traffic. - Implement network segmentation and access controls to limit the attacker's ability to move laterally within the network.	-Vulnerability exploitation tools
Installation	The attacker installs a backdoor or other malicious software on the compromised system to maintain access and control.	- Regularly update and patch software and systems to prevent exploitation of known vulnerabilities. - Use security tools such as antivirus software and endpoint protection to detect and remove malicious software. - Implement network segmentation and access controls to limit the attacker's ability to move laterally within the network.	- Remote access tools
Command and Control	The attacker installs a backdoor or other malicious software on the compromised system to maintain access and control.	- Use security tools such as firewalls and intrusion prevention systems to block malicious network traffic. - Implement network segmentation and access controls to limit the attacker's ability to move laterally within the network. - Monitor network activity for unusual or suspicious communication patterns. - Use security tools such as data loss prevention (DLP) to monitor and block sensitive data exfiltration.	- Command and control infrastructure
Actions on Objectives	The attacker carries out their ultimate goals, such as stealing data or disrupting services.	- Implement network segmentation and access controls to limit the attacker's ability to move laterally within the network. - Use security tools such as data loss prevention (DLP) to monitor and block sensitive data exfiltration. - Regularly backup and secure important data to allow for recovery in the event of an attack. - Use security tools such as intrusion detection and prevention systems to monitor for and prevent malicious activity.	- Data exfiltration tools - Disruption tools

In each phase, there are a number of tools that could be utilized to mitigate the attack and protect against each stage of the Cyber Kill Chain. Some possible tools and their uses are described in the table above. It's important to note that there is.