100 Days Challenge

Day 3 Challenge 3

EXPLORE THE TERMS:

Threat, Vulnerability, Attack, Risk, exploit, asset and impact.

One of the most infamous cyber-attacks involving ransomware, the WannaCry Ransomware attack was a massive cyberattack that wreaked havoc on Windows computer systems worldwide. The attack exploited a vulnerability in Windows called Eternal Blue, which had been leaked by a hacker group a month prior. Microsoft had already released a security patch to address this vulnerability, but many users hadn't installed it. The attack infected an estimated 230,000 computers across over 150 countries. It disrupted the operations of hospitals, businesses, and government agencies worldwide. A security researcher discovered a "kill switch" that helped stop the initial spread of the worm, but victims had already paid ransoms to restore their systems before the Killswitch was found. and the total damages are estimated to reach anywhere from hundreds of millions to potentially billions of dollars. A new version of the WannaCry ransomware attack also appeared again in 2018.

Threat: The threat in this case was the WannaCry ransomware itself. Ransomware is a type of malicious software that encrypts the victim's files and demands a ransom for the decryption key.

Vulnerability: The vulnerability exploited in this attack was a security flaw in Windows known as Eternal Blue.

Attack: The attack was the WannaCry ransomware campaign. It involved deploying the ransomware across networks by exploiting the Eternal Blue vulnerability.

Risk: The risk here was the potential for widespread disruption and financial loss due to the ransomware's ability to encrypt critical files and halt operations.

Exploit: The exploit in this context was the use of EternalBlue to gain unauthorized access and execute the ransomware. EternalBlue was a tool that allowed attackers to exploit the vulnerability in Windows SMB to propagate the ransomware without needing direct user interaction.

Asset: The assets affected by the attack were the Windows computer systems and the data they contained. These assets included personal and business data, as well as the systems themselves that were critical for the operations of hospitals, businesses, and government agencies,

Impact: The impact of the WannaCry attack was extensive and severe. It caused significant operational disruption to numerous organizations, including hospitals and government agencies, which led to delays in services and operations.