Network Security - Reflections

During the case study about the Digital Enterprises, got an opportunity to research about the various tools and technologies. Came to know about the operations to improve productivity, customer experience, and business processes.

Researched and learnt about digitally modernized company uses cutting-edge technology to stay relevant and surprise customers. From customer experience to operational productivity, technology affects everything. Digital technologies help companies implement new capabilities.

Also explored challenges and concerns during COVID situation, wherein in 2020's second quarter, 16.1% of retail sales were e-commerce, up from 10.8% the year before. Businesses that already emphasized digital platforms are rushing to develop apps to capture consumer activity online.

On the above, my peer 1 response was more interesting about the platforms in response to COVID made to revisit and learn more. He highlighted that attackers have been able to make minor tweaks to exploits to circumvent security patches.

My peer 2 highlighted about the unauthorized access to financial services like credit cards or the user's personal information, such their Social Security number. And the awareness among the small and medium companies about the latest security news and how to overcome and secure their data.

Got a chance to comment on peer post on mobile security threats. Mobile security protects smartphones, tablets, and laptops using strategy, infrastructure, and software. Mobile device cybersecurity includes protecting device data, endpoints, and networking equipment. As mobile devices replace desktops, attackers will target them more.

As more people travel and work from home, mobile devices have become more common, even among corporate employees. Internet use was once limited to desktops, and only travelling employees had laptops. Mobile devices are the preferred way to browse the internet, and mobile traffic has surpassed desktops.
Mobile devices have a larger attack surface than desktops, making them a bigger security threat. Mobile devices are vulnerable to physical and virtual attacks, but desktops are immobile. Administrators must worry about physical attacks (theft and loss) and virtual threats from third-party apps and Wi-Fi hotspots (e.g., man-in-the-middle attacks). Administrators can better control network and endpoint security on stationary desktops. Users can root, add, and lose mobile devices.

Along with peers had to discuss on the recent Log4J vulnerability. We discussed about the importance of log management including how to secure. Researched how Hackers are actively scanning networks for log-related vulnerabilities such as Log4j and eight important steps to mitigate those attacks.

conducted extensive research and study on the testing of penetration for the web applications. I put in some time working on the preparation of a project plan for the website that was selected. The plan is formulated on the basis of the assumptions that were made and the security standards that were implemented. carried out research and acquired new information regarding the significance of the penetration to both the company and its customers. A penetration test, also known as a "pen test," is a test that imitates an online attack on your computer in order to locate vulnerabilities. Penetration testing is frequently used as a complementary measure to web application firewalls (WAF). Pen testing is the process of breaking into application systems like APIs or frontend/backend servers to look for vulnerabilities. One example of a vulnerability is uncleaned inputs, which could be exploited in an attack that involves code injection.

In each stage, the scope of the project was further defined. We make use of the STRIDE and DREAD methods, as well as the industry standard regulatory compliances, in order to achieve a better result. For the best possible outcome, we have considered using the appropriate tools.

In preparation for the vulnerability audit and assessment, was given the opportunity to increase my knowledge of scanning tools. Gained knowledge of the Kali Linux server and its installation. access to the appropriate tools contained within the server in order to attach the preferred website.

The penetration technique is carried out in real time, and logs are automatically gathered for subsequent examination at the same time. We put a number of commands through their paces using the tools, which allowed us to investigate the security protocols. Capable of applying the DREAD method to rank the severity of the problem and produce a recommendation tailored to the requirements of the business. Gained knowledge from the auxiliary tools, and was able to evaluate the logs to determine which produced the best results.

Being able to conceptualize the reasons why the security features are important at each stage of development and deployment is essential. was able to observe how the hackers scanned the environment as well as how the firewall was opened up.

Recommendations were provided for address the security gaps for the chosen website.

- The server needs to have latest security patches based on vendor releases
    - Best practice is to maintain N-1 version
- The application-level software needs to be patched on regular basis.
    - Best practice is to maintain N-1 version
- Only the web browsing port 80 and 443 need to opened and other to be blocked based on the traffic