DAILY ASSESSMENT FORMAT

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **18/07/2020** | **Name:** | **Nayanashree** |
| **Course:** | **Coursera** | **USN:** | **4AL16EC042** |
| **Topic:** | **Network security and database vulnerabilities** | **Semester & Section:** | **8 A** |
| **Github Repository:** | **Nayana\_online** |  |  |

|  |
| --- |
| **FORENOON SESSION DETAILS** |
|  |
| **Report**  Digital warfare and worldwide cyberattack rates are on the rise, and protection on corporate networks is even more crucial.  Databases are a key target for cybercriminals due to the often valuable nature of sensitive information locked away inside. Whether the data is financial or holds intellectual property and corporate secrets, hackers worldwide can profit from breaching a businesses' servers and plundering databases.  According to a new report issued by [Dark Reading](http://www.darkreading.com/database/util/10975/download), there are a number of key security failures that cybercriminals take advantage of. However, it is often the staff of an enterprise — database developers, administrators and the like — who create the environment necessary for attacks to gain access to data.  The researchers say that the top ten vulnerabilities often found in database-driven systems, whether during the creation phase, through the integration of applications or when updating and patching, are:  **1. Deployment Failures**  The most common cause of database vulnerabilities is a lack of due care at the moment they are deployed. Although any given database is tested for functionality and to make sure it is doing what the databases is designed to do, very few checks are made to check the database is not doing things it should not be doing.  **2. Broken databases**  The [SQL Slammer worm](https://www.zdnet.com/article/sql-slammer-worm-wreaks-havoc-on-internet/) of 2003 was able to infect more than 90 percent of vulnerable computers within 10 minutes of deployment, taking down thousands of databases in minutes. This worm took advantage of a bug that was discovered in Microsoft's SQL Server database software the previous year, but few system administrators installed a fix, leaving computers vulnerable.  By exploiting a buffer-overflow vulnerability, the worm's success demonstrates how critical installing security patches and fixes are. However, whether lacking time or resources, not enough businesses keep their systems regularly patched, leaving databases vulnerable.  **3. Data leaks**  Databases may be considered a "back end" part of the office and secure from Internet-based threats (and so data doesn't have to be encrypted), but this is not the case. Databases also contain a networking interface, and so hackers are able to capture this type of traffic to exploit it. To avoid such a pitfall, administrators should use SSL- or TLS-encrypted communication platforms.  **4. Stolen database backups**  External attackers who infiltrate systems to steal data are one threat, but what about those inside the corporation? The report suggests that insiders are also likely to steal archives — including database backups — whether for money, profit or revenge. This is a common problem for the modern enterprise, and businesses should consider encrypting archives to mitigate the insider-risk.  **5. The abuse of database features**  The research team says that over the past three years, every database exploit they've seen has been based on the misuse of a standard database feature. For example, a hacker can gain access through legitimate credentials before forcing the service to run arbitrary code. Although complex, in many cases, this access was gained through simple flaws that allow such systems to be taken advantage of or bypassed completely. Future abuse can be limited by removing unnecessary tools — not by destroying the possibility of zero-day exploits, but by at least shrinking the surface area hackers can study to launch an attack.  **6. A lack of segregation**  The separation of administrator and user powers, as well as the segregation of duties, can make it more difficult for fraud or theft undertaken by internal staff. In addition, limiting the power of user accounts may give a hacker a harder time in taking complete control of a database.  **7. Hopscotch**  Rather than taking advantage of buffer overflow and gaining complete access to a database in the first stage, cybercriminals often play a game of Hopscotch: finding a weakness within the infrastructure that can be used as leverage for more serious attacks until they reach the back-end database system. For example, a hacker may worm their way through your accounts department before hitting the credit card processing arena. Unless every department has the same standard of control, creating separate administrator accounts and segregating systems can help mitigate the risk.  **8. SQL injections**  A popular method for hackers to take, SQL injections remain a critical problem in the protection of enterprise databases. Applications are attacked by injections, and the database administrator is left to clean up the mess caused by unclean variables and malicious code which is inserted into strings, later passed to an instance of SQL server for parsing and execution. The best ways to protect against these threats are to protect web-facing databases with firewalls and to test input variables for SQL injection during development.  **9. Sub-standard key management**  Key management systems are meant to keep keys safe, but the research team often found encryption keys stored on company disk drives. Database administrators sometimes falsely believe these keys have to be left on the disk because of database failures, but this isn't true — and placing such keys in an unprotected state can leave systems vulnerable to attack.  **10. Database inconsistencies**  Finally, the researchers found that the common thread which brings all of these vulnerabilities together is a lack of consistency, which is an administrative rather than database technology problem. System administrators and database developers need to develop a consistent practice in looking after their databases, staying aware of threats and making sure that vulnerabilities are taken care of. This isn't an easy task, but documentation and automation to track and make changes can ensure that the information contained in enterprise networks is kept secure. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date:** | **18/7/2020** | **Name:** | **Nayanashree KS** | |
| **Course:** | **Salesforce** | **USN:** | **4al16ec042** | |
| **Topic:** | **Salesforce platform basics** | **Semester & Section:** | **8 A** | |
| **AFTERNOON SESSION DETAILS** | | | |
| **Report** **Understand the Impact of the Fourth Industrial Revolution on Business**Learning Objectives After completing this module, you’ll be able to:   * Explain how customer expectations are shifting in response to the Fourth Industrial Revolution. * Describe how the Fourth Industrial Revolution is transforming businesses.  Cause and Effect In [Technologies and Trends of the Fourth Industrial Revolution](https://trailhead.salesforce.com/module/technologies-and-trends-of-the-fourth-industrial-revolution), you learned about the 10 technologies behind the Fourth Industrial Revolution. If those 10 technologies are the cause, then this module explains the effect.  One of the main effects of the Fourth Industrial Revolution is increased human productivity. With technologies like AI and automation augmenting our professional lives, we’re able to make smart choices, faster than ever before.  But it’s not all rosy, and we’re not trying to sugarcoat things for you. There are some hefty moral and ethical implications for many of these innovations, and in some cases, we’re left with more questions than answers.  In this module, we talk about the impact of the Fourth Industrial Revolution, including the positive and the potentially negative. These Days, Customers Expect More Customers today expect to get an answer anytime, on any channel they choose. Whether they tweet, email, chat, or call, they want instant, personalized service.  So how did they come to expect that?  Well, the technologies around us have evolved, bringing customer expectations with them. Think about it—just 20 years ago, companies like Google, Alibaba, Facebook, Twitter, YouTube, Uber, Airbnb, Salesforce, Snapchat, Instagram, Fitbit, Spotify, and WeChat did not exist. Make no mistake about it, the services these companies provide have raised the bar for the customer experience. How can you expect a customer to wait on hold when they’re used to the speed of interaction on social media? Or when the answer to any question is one Google search away?  And let’s not forget the millennial generation. They grew up on digital technology, and they now make up more than half the workforce. As consumers, they expect businesses to anticipate their needs and provide personalized support.  Customers, whether as individuals (B2C) or businesses (B2B), are increasingly at the center of what’s known as the digital economy, which is a fancy way of saying the economy that’s built on Internet-based and digital technologies. To be successful, businesses need to shift from a transactional model, focused solely on selling products, to a relationship model, built around selling services and creating deeper connections with customers. Data Is the New Currency Every day, billions of people are sharing online. They’re posting images, videos, and tweets. They’re sending text messages. They’re liking other people’s updates.  How are they doing this sharing? They’re using connected devices. And billions of people sharing translates to billions of devices with embedded sensors, sending trillions of real-time signals to the cloud. Things like GPS coordinates, environmental data, clickstreams, and health status.  The result? Data. Lots and lots of data.  All of this data is like food for artificial intelligence. AI is driving innovation across growing numbers of products and services, and the more data you have, the better the predictions get.  Machine learning algorithms can analyze these billions of transactions and variables to make businesses smarter. They can help businesses anticipate trends in consumer demands, personalize promotions for individual customers, and optimize pricing.  Here are a few examples of machine learning innovations, organized by industry:   * **Retail**: Highlight consumer sentiments toward a brand or predict which customers are mostly likely to purchase a particular product. * **Manufacturing**: Optimize supply chain operations and predict the failure of machine parts. * **Travel**: Plan vacations with the acumen of a human assistant. * **Medicine**: Assist doctors in identifying different types of cancer cells and spotting intracranial abnormalities in real time.   Let’s dive in deeper, industry by industry, to help you understand how the new technologies of the Fourth Industrial Revolution are shaping the economy. Transportation In today’s times, do you need to own a car? Or can you simply share one?  Car-sharing services work across multiple industries—transportation, technology, insurance, finance—to provide a seamless customer experience from request to payment. In the process, they are disrupting the notion of car ownership.  What if you just need a ride? Services like Uber and Lyft have disrupted the transportation industry. With one of these services, you can use your phone to:   * Order a car to take you to a specific destination * Track the vehicle as it heads your way * Get information about the vehicle, driver, and price of the trip * Pay for the ride and optionally, add a tip and feedback for the driver   Or if you want to own a car, why not own it instead as a service, so you don’t have access to just one car, but a whole fleet based on your needs? Need a coupe for the weekend? Change your car needs in the app, and Audi swaps it out for you. Car companies are looking hard at these models now.  Advances in artificial intelligence, the Internet of things, clean energy, and other technologies can improve safety for drivers and pedestrians and potentially lead to greater use of public transportation and car-sharing services. This shift can result in reduced congestion and pollution, faster and cheaper commutes, and improved health. | | | |