**ASSESSMENT 52**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | 20-07-2020 | **Name:** | Sheela Golasangi |
| **Course:** | Coursera | **USN:** | 4AL16EC068 |
| **Topic:** | Network Security & Database Vulnerabilities | **Semester & Section:** | VIII  ‘B’ |
| **Github Repository:** | Sheela-Course |  |  |

|  |
| --- |
| **FORENOON SESSION DETAILS** |
| **REPORT**  **C:\Users\india\Pictures\Screenshots\Screenshot (1710).png**  **C:\Users\india\Pictures\Screenshots\Screenshot (1711).png**  **C:\Users\india\Pictures\Screenshots\Screenshot (1718).png**  **C:\Users\india\Pictures\Screenshots\Screenshot (1730).png**  **C:\Users\india\Pictures\Screenshots\Screenshot (1790).png**  This course gives you the background needed to understand basic network security. You will learn the about Local Area Networks, TCP/IP, the OSI Framework and routing basics. You will learn how networking affects security systems within an organization. You will learn the network components that guard an organization from cybersecurity attacks.  In addition to networking, you will learn about database vulnerabilities and the tools/knowledge needed to research database vulnerability for a variety of databases including SQL Injection, Oracle, Mongo and Couch.  You will learn about various security breach types associated with databases and organizations that define standards and provide tools for cybersecurity professionals.  This course is intended for anyone who wants to gain a basic understanding of Network Security/Database Vulnerabilities or as the fourth course in a series of courses to acquire the skills to work in the Cybersecurity field as a JrCybersecurity Analyst.  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, 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 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 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:** | 20-07-2020 | **Name:** | Sheela Golasangi |
| **Course:** | Sales force | **USN:** | 4AL16EC068 |
| **Topic:** | Trailhead Workshop Basics | **Semester & Section:** | VIII  ‘B’ |
| **Github Repository:** | Sheela-Course |  |  |
| **AFTERNOON SESSION DETAILS** | | | |
| C:\Users\User\Pictures\Screenshots\Screenshot (318).pngC:\Users\User\Pictures\Screenshots\Screenshot (319).pngLearning Objectives After completing this unit, you’ll be able to:   * Identify an organization, group, or cause you want to support with a learning event powered by Trailhead. * Discover how you can make an impact by teaching a learning event.  Introduction Everyone wants to make an impact, to give back, and make a difference. But how do you start? It can feel overwhelming, and even people with great skills and good intentions can be unsure about where to begin. Oftentimes, the first step is the hardest part.  One of the most powerful ways to help others is to teach people what you know. You don’t have to be a teacher or professional trainer to make an impact. Anyone can teach in a classroom, a conference room, a schoolroom, a Google hangout, or even your local coffee shop.  In this module, you learn how to host a learning event powered by Trailhead. You get specific techniques, best practices, and downloadable samples and guides. Learning Events with Trailhead Trailhead is the fun way to learn Salesforce. It’s gamified—you learn new skills while earning badges. Trailhead was originally designed to be a self-guided learning tool, enabling people to learn at their own pace, on their own schedule, and at any location.  But as it turns out, Trailhead also works for in-person and virtual learning events. People are coming together to learn new skills, earn badges, and connect with each other at learning events hosted by Salesforce and people in the community. Plan the Learning EventLearning Objectives After completing this unit, you’ll be able to:   * Plan the learning event you want to run. * Invite others to your learning event. * Start generating excitement on social media about your learning event. * Enact strategies for recruiting volunteers to help. * Download sample planning documents and checklists.  Start Planning Planning a learning event is a lot like planning a party. You pick a date, a location, invite people, and gather your supplies. In this unit, we take you through some best practices for planning a successful learning event. Start Your Quip Document What better way to get organized than to create a checklist in Quip? Anyone can start a [free trial of Quip](https://quip.com/), and here is a handy Quip checklist for planning your learning event.  Get the Quip checklist: [Learning Event Checklist](https://salesforce.quip.com/JL8hAgV4baZT) Download the Samples In addition to the Quip document, you get this [**downloadable pack**](https://developer.salesforce.com/files/BAM-assets.zip)with, email templates, a post-learning event survey, and more, including:   * Email templates * Post-learning event survey * Ready-made PowerPoint presentations * Signup sheet   Download the pack here: [**Trailhead Workshops Enablement Pack**](https://developer.salesforce.com/files/BAM-assets.zip) Set Your Goals, Audience, Date, and Location Start by figuring out who your event is for and what your goals are. Then decide if you are going to feature a particular public speaker at your learning event. | | | |