**DAILY ASSESSMENT FORMAT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **17/06/2020** | **Name:** | **Navya R** |
| **Course:** | **Cyber security** | **USN:** | **4AL16EC041** |
| **Topic:** | **Vulnerabilities & Password Security**  **Cryptography** | **Semester & Section:** | **8 A** |
| **Github Repository:** | **Navya-R** |  |  |

|  |
| --- |
| **FORENOON SESSION DETAILS** |
| **Image of session** |
| **Report**  Blockchain technology increasingly receives attention as a next-generation solution to a wide variety of transactional and recordkeeping problems. As often occurs with innovative technologies, many struggle with understanding its implementation details and potential risks. Organizations considering using blockchain technology and their counsel must:   Understand basic blockchain technology concepts.   Assess how its cyber risks may apply to them.   Make reasonable implementation decisions as the technology and its applications mature.  BLOCKCHAIN TECHNOLOGY DEFINED Blockchains are digital online ledgers that typically:   Are implemented in a distributed fashion.   Allow users to record transactions in a shared ledger.   Follow established policies but lack a central authority or data repository. The National Institute of Standards and Technology (NIST) emphasizes that blockchain technology:   Groups cryptographically signed transactions into blocks to form a ledger.   Makes the ledger tamper-resistant and tamper-evident by cryptographically linking each block to the previous entry after validation.   Resolves conflicts automatically using established rules.   Replicates copies of the ledger across a network of independent nodes.  Cryptocurrency is the most widely recognized application of blockchain technology. Many industries are also exploring blockchain technology based solutions to enhance efficiency, streamline business processes, and develop trust between parties with little or no knowledge of each other. For example, blockchain technology can support:   Smart contracts.   Identity management systems.   Supply chain solutions.   Public records, such as property registers.   Other applications, especially those that require sharing verified data among multiple geographically distributed parties.  BLOCKCHAIN SECURITY MEASURES Blockchain security measures vary according to each individual application but typically include:   Public-private key method encryption to manage participant access.   Transaction data integrity protection within blocks using cryptographic hashes. The technology also chronologically records data blocks by securely tying each block to the previous and later blocks. This measure: z prevents data tampering within a block because any attempt to alter the data changes the hash values, which other participants can rapidly detect; and z provides the immutability principle widely touted for blockchain recorded transactions. Specific blockchain applications may use different security measures that affect risk levels. Potential users should investigate and understand the particular measures a blockchain application uses to avoid unexpected vulnerabilities. Private blockchains require heightened scrutiny because they may not have a robust network of users, which is essential for policing attempts to mistakenly or intentionally introduce erroneous data into a blockchain.  BLOCKCHAIN NETWORK GOVERNANCE A blockchain’s integrity depends on its network governance model and the methods it uses to validate transactions. Different blockchain applications choose different mechanisms (for more details on common methods, see Blockchain Consensus Mechanisms). Some have suggested the potential for several blockchain integrity attacks, including:  Centralization of miners or the 51% attack. Any blockchain network that relies on a majority consensus to validate transactions is vulnerable if attackers compromise a sufficiently large group of its nodes. For example, bad actors may compromise a public blockchain application if they acquire or control at least 51% of its mining and consensus power. The same problem may result if multiple miners surreptitiously join forces to create a majority and manipulate the blockchain. This scenario is unlikely in a robust network with many users. Some limited blockchains, especially small private implementations, may be more vulnerable. Private blockchain applications typically vet participants and support user authentication and other controls to address this risk.   Selfish miners. Researchers have suggested a scenario where a self-interested public blockchain miner may fool others into wasting time and computing power on already validated transactions, reducing the number of miners doing real mining work and potentially making it easier to manipulate outcomes.   The eclipse attack. Blockchain technology depends on communications across a network of nodes. Disrupting node communications or disseminating or accepting false information to confirm fake transactions may compromise the network. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date:** | **17/6/2020** | **Name:** | **Navya R** | |
| **Course:** | **Java** | **USN:** | **4al16ec041** | |
| **Topic:** | **Eclipse shortcut, debugging in eclipse** | **Semester & Section:** | **8 A** | |
| **AFTERNOON SESSION DETAILS** | | | |
| **REPORT**  **Downloading and Installing Eclipse**  Before Installing Eclipse, you need to have either the Java JDK (Java development kit) or Java JRE (Java runtime engine) installed on your computer. These are available at http://java.sun.com/javase/downloads/index.jsp. Installing the JDK or JRE is reasonably simple. Detailed, step-by-step instructions, if needed, are available in the PDF Eclipse Tutorial at the https://www.arctechsoftware.com/tutorial/welcomePage.do. (Follow the link to “Beginning Eclipse”.)  For Java development, the JDK is recommended because it allows you to see documentation and source code for the standard Java classes. However, either the JDK or JRE will work for this tutorial. This tutorial is based on Eclipse 3.3, although you could use 3.2 and probably later versions as well. Here are the steps to install Eclipse 3.3 from [www.eclipse.org](http://www.eclipse.org):   Navigate to [www.eclipse.org/downloads](http://www.eclipse.org/downloads)   Select “Eclipse IDE for Java Developers”. If your platform is Linux or MacOSX, be sure to select the link to the right. Note that you can use “Eclipse IDE for Java EE Developers”, “Eclipse for RCP/Plug-in Developers”, or “Eclipse Classic” as well. All of these include the Java development portions of Eclipse used in this tutorial.  On the www.eclipse.org/downloads page, follow the link “Find out more”. Scroll your browser to display the far right-hand side of the screen to the column “Tutorials and Help”. The first tutorial is a ScreenCam tutorial that steps you through downloading and installing Eclipse on Windows. The Eclipse installation is very straightforward. There is no installation program. Instead, you just create the top-level folder and the unzip the file inside this folder. In Windows XP, for example, just copy the zip file to your root directory (e.g., “C:\”) and then unzip the downloaded zip file. This will create a folder called “C:\eclipse”. The Eclipse programs will be created in several subfolders (configuration, features, plugins, readme). The procedure for Linux is similar, except your unzip the .tar.gz file.  Program example:  class CharArrayToString  {  public static void main(String args[])  {  // Method 1: Using String object  char[] ch = {'g', 'o', 'o', 'd', ' ', 'm', 'o', 'r', 'n', 'i', 'n', 'g'};  String str = new String(ch);  System.out.println(str);    // Method 2: Using valueOf method  String str2 = String.valueOf(ch);  System.out.println(str2);  }  }  Output:  good morning  good morning | | | |