**DAILY ASSESSMENT FORMAT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **18/06/2020** | **Name:** | **Navya R** |
| **Course:** | **Cyber security** | **USN:** | **4AL16EC041** |
| **Topic:** | **Block chain and cyber security**  **Ciphers and encryption** | **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:** | **18/6/2020** | **Name:** | **Navya R** | |
| **Course:** | **Ethical hacking** | **USN:** | **4al16ec041** | |
| **Topic:** | **What is Ethical hacking?**  **Domains and process implementation under ethical hacking** | **Semester & Section:** | **8 A** | |
| **AFTERNOON SESSION DETAILS** | | | |
| **REPORT**  **Ethical Hacker** (**CEH**) is a qualification obtained by demonstrating knowledge of assessing the security of computer systems by looking for weaknesses and vulnerabilities in target systems, using the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system. This knowledge is assessed by answering multiple choice questions regarding various ethical hacking techniques and tools. The code for the C|EH exam is 312-50.  This certification has now been made a baseline with a progression to the C|EH (Practical), launched in March 2018, a test of penetration testing skills in a lab environment where the candidate must demonstrate the ability to apply techniques and use penetration testing tools to compromise various simulated systems within a virtual environment.  [Ethical hackers](https://en.wikipedia.org/wiki/Ethical_hacking) are employed by organizations to penetrate networks and computer systems with the purpose of finding and fixing security vulnerabilities. The [EC-Council](https://en.wikipedia.org/wiki/EC-Council) offers another certification, known as Certified Network Defense Architect (CNDA). This certification is designed for [United States Government](https://en.wikipedia.org/wiki/United_States_Government) agencies and is available only to members of selected agencies including some private government contractors, primarily in compliance to DOD Directive 8570.01-M.[[1]](https://en.wikipedia.org/wiki/Certified_Ethical_Hacker#cite_note-1) It is also [ANSI accredited](https://en.wikipedia.org/wiki/American_National_Standards_Institute) and is recognized as a [GCHQ](https://en.wikipedia.org/wiki/Government_Communications_Headquarters) Certified Training (GCT).  Importance of Ethical Hacking?  In the dawn of international conflicts, terrorist organizations funding cybercriminals to breach security systems, either to compromise national security features or to extort huge amounts by injecting malware and denying access. Resulting in the steady rise of cybercrime. Organizations face the challenge of updating hack-preventing tactics, installing several technologies to protect the system before falling victim to the hacker.  New worms, malware, viruses, and ransomware are multiplying every day and is creating a need for ethical hacking services to safeguard the networks of businesses, government agencies or defense.  Benefits:   1. Discovering vulnerabilities from an attacker’s POV so that weak points can be fixed. 2. Implementing a secure network that prevents security breaches. 3. Defending national security by protecting data from terrorists. 4. Gaining the trust of customers and investors by ensuring the security of their products and data. 5. Helping protect networks with real-world assessments. | | | |