**DAILY ASSESSMENT FORMAT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **18/06/2020** | **Name:** | **Varshini MN** |
| **Course:** | **Cyber security** | **USN:** | **4AL16EC089** |
| **Topic:** | **Block chain and cyber security**  **Ciphers and encryption** | **Semester & Section:** | **8th B** |
| **Github Repository:** | **varshinimn-test** |  |  |

|  |
| --- |
| **FORENOON SESSION DETAILS** |
| **Image of session** |
| **Report**  **BLOCKCHAIN TECHNOLOGY THE NEW INTERNET**  By allowing digital information to be distributed but not copied, blockchain technology created the backbone of a new type of internet.  In this guide, we are going to explain to you what the blockchain technology is, and what its properties are what make it so unique. So, we hope you enjoy this, What Is Blockchain Guide. And if you already know what blockchain is and want to become a blockchain developer please check out our in-depth blockchain tutorial and create your very first blockchain.  A blockchain is, in the simplest of terms, a time-stamped series of immutable records of data that is managed by a cluster of computers not owned by any single entity. Each of these blocks of data (i.e. block) is secured and bound to each other using cryptographic principles (i.e. chain).  The blockchain network has no central authority — it is the very definition of a democratized system. Since it is a shared and immutable ledger, the information in it is open for anyone and everyone to see. Hence, anything that is built on the blockchain is by its very nature transparent and everyone involved is accountable for their actions.  **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 technologybased 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.   **Cyber security**  Computer security, cybersecurity or information technology security is the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.  The field is becoming more important due to increased reliance on computer systems, the Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions, and the various devices that constitute the "Internet of things". Owing to its complexity, both in terms of politics and technology, cybersecurity is also one of the major challenges in the contemporary world.  Eavesdropping is the act of surreptitiously listening to a private computer "conversation", typically between hosts on a network. For instance, programs such as Carnivore and NarusInSight have been used by the FBI and NSA to eavesdrop on the systems of internet service providers. Even machines that operate as a closed system can be eavesdropped upon via monitoring the faint electromagnetic transmissions generated by the hardware; TEMPEST is a specification by the NSA referring to these attacks.  **Cryptography**  Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.  Earlier cryptography was effectively synonymous with encryption but nowadays cryptography is mainly based on mathematical theory and computer science practice  **Modern cryptography concerns with:**   * Confidentiality - Information cannot be understood by anyone * Integrity - Information cannot be altered. * Non-repudiation - Sender cannot deny his/her intentions in the transmission of the information at a later stage * Authentication - Sender and receiver can confirm each |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date:** | **18/06/2020** | **Name:** | **Varshini MN** | |
| **Course:** | **Ethical hacking** | **USN:** | **4AL16EC089** | |
| **Topic:** | **What is Ethical hacking?**  **Domains and process implementation under ethical hacking** | **Semester & Section:** | **8th B** | |
| **AFTERNOON SESSION DETAILS** | | | |
| **Report**  **Ethical Hacker**  It 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.  [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. 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.  Helping protect networks with real-world assessments. | | | |