**DAILY ASSESSMENT FORMAT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **18-06-2020** | **Name:** | **Kiran N** |
| **Course:** | **Introduction to Ethical Hacking** | **USN:** | **4al16ec031** |
| **Topic:** | **Introduction to hacking** | **Semester & Section:** | **8th and A** |
| **Github Repository:** | **Kiran-course** |  |  |

|  |
| --- |
| **FORENOON SESSION DETAILS** |
| What is Ethical Hacking?  Ethical Hacking is an authorized practice of bypassing system security to identify potential data breaches and threats in a network. The company that owns the system or network allows Cyber Security experts to perform such activities in order to test the system’s defenses. Thus, unlike malicious hacking, this process is planned, approved, and more importantly, legal.  Ethical hackers aim to investigate the system or network for weak points that malicious hackers can  exploit or destroy. They collect and analyze the information to figure out ways to strengthen the security of the system/network/applications. By doing so, they can improve the security footprint so that it can better withstand attacks or divert them.  Ethical Hackers check for key vulnerabilities include but are not limited to:  •Injection attacks  •Changes in security settings  •Exposure of sensitive data  •Breach in authentication protocols  •Components used in the system or network that may be used as access points    Types of Hackers  The practice of ethical hacking is called “White Hat”hacking, and those who perform it are called White Hat hackers. In contrast to Ethical Hacking, “Black Hat” hacking describes practices involving security violations. The Black Hat hackers use illegal techniques to compromise the system or destroy information.  Unlike White Hat hackers, “Grey Hat” hackers don’t ask for permission before getting into your system.  But Grey Hats are also different from Black Hats because they don’t perform hacking for any personal  or third-party benefit. These hackers do not have any malicious intention and hack systems for fun or  various other reasons, usually informing the owner about any threats they find. Grey Hat and Black Hat hacking are both illegal as they both constitute an unauthorized system breach, even though the  intentions of both types of hackers differ.  Roles and Responsibilities of an Ethical Hacker  Ethical Hackers must follow certain guidelines in order to perform hacking legally. A good hacker  knows his or her responsibility and adheres to all of the ethical guidelines. Here are the most important rules of Ethical Hacking:  •An ethical hacker must seek authorization from the organization that owns the system. Hackers  should obtain complete approval before performing any security assessment on the system or  network.  •Determine the scope of their assessment and make known their plan to the organization.  •Report any security breaches and vulnerabilities found in the system or network.  •Keep their discoveries confidential. As their purpose is to secure the system or network, ethical  hackers should agree to and respect their non-disclosure agreement.  •Erase all traces of the hack after checking the system for any vulnerability. It prevents malicious  hackers from entering the system through the identified loopholes.  Skills Required to Become an Ethical Hacker  An ethical hacker should have in-depth knowledge about all the systems, networks, program codes,  security measures, etc. to perform hacking efficiently. Some of these skills include:  •Knowledge of programming - It is required for security professionals working in the field of  application security and Software Development Life Cycle (SDLC).  •Scripting knowledge - This is required for professionals dealing with network-based attacks and  host-based attacks.  •Networking skills - This skill is important because threats mostly originate from networks. You  should know about all of the devices present in the network, how they are connected, and how to  identify if they are compromised.  •Understanding of databases - Attacks are mostly targeted at databases. Knowledge of database  management systems such as SQL will help you to effectively inspect operations carried out in  databases.  •Knowledge of multiple platforms like Windows, Linux, Unix, etc.  •The ability to work with different hacking tools available in the market.  •Knowledge of search engines and servers |