**DAILY ASSESSMENT FORMAT(DAY 5)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date:** | **22-June-2020** | **Name:** | **Bhuvanesh M** | |
| **Course:** | **Introduction to Ethical Hacking** | **USN:** | **4AL16EC015** | |
| **Topic:** | **Ethical hacking** | **Semester & Section:** | **8th sem & ‘A’ section** | |
| **AFTERNOON SESSION DETAILS** | | | |
| **Image of session** | | | |
| **What is Ethical Hacking?**  Ethical Hacking sometimes called as Penetration Testing is an act of intruding/penetrating into system or networks to find out threats, vulnerabilities in those systems which a malicious attacker may find and exploit causing loss of data, financial loss or other major damages.  The purpose of ethical hacking is to improve the security of the network or systems by fixing the vulnerabilities found during testing. Ethical hackers may use the same methods and tools used by the malicious hackers but with the permission of the authorized person for the purpose of improving the security and defending the systems from attacks by malicious users.  Ethical hackers are expected to report all the vulnerabilities and weakness found during the process to the management. **What do ethical hackers do?** **Scope and goal setting**  It is essential for any professional pen tester to document agreed upon scope and goals. These are the kinds of questions regarding scope you need to ask:   * What computer assets are in scope for the test? * Does it include all computers, just a certain application or service, certain OS platforms, or mobile devices and cloud services? * Does the scope include just a certain type of computer asset, such as web servers, SQL servers, all computers at a host OS level, and are network devices included? * Can the pen testing include automated vulnerability scanning? * Is [social engineering](https://www.csoonline.com/article/2124681/what-is-social-engineering.html) allowed, and if so, what methods? * What dates will pen testing be allowed on? * Are there any days or hours when penetration testing should not be tried (to avoid any unintentional outages or service interruptions)? * Should testers try their best to avoid causing service interruptions or is causing any sort of problem a real attacker can do, including service interruptions, a crucial part of the test? * Will the penetration testing be blackbox (meaning the pen tester has little to no internal details of the involved systems or applications) or whitebox (meaning they have internal knowledge of the attacked systems, possibly up and involving relevant source code)? * Will computer security defenders be told about the pen test or will part of the test be to see if the defenders notice? * Should the professional attackers (e.g., red team) try to break-in without being detected by the defenders (e.g., blue team), or should they use normal methods that real intruders might use to see if it sets off existing detection and prevention defenses? | | | |