**DAILY ASSESSMENT FORMAT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **20-June-2020** | **Name:** | **Raziya Banu** |
| **Course:** | **Introduction to Cyber Security** | **USN:** | **4AL16EC058** |
| **Topic:** | **Career and industry landscape in cyber security** | **Semester & Section:** | **8th sem & ‘B’ section** |
| **Github Repository:** |  |  |  |

|  |
| --- |
| **FORENOON SESSION DETAILS** |
| **Image of session** |
| **Report –**  In my first session today I have studied about - Career and industry landscape in cyber security  **Incident responder**  Incident responders are part of the first response security team. They are essentially cyber firefighters as they work diligently to address security threats and mitigate risks using a range of forensic tools. Responders have a focus on education and prevention involving day-to-day system monitoring and threat analysis. They also establish protocols for communication to ensure business collaboration and continuity, during and after, a breach, hack or attack.  **Computer forensics expert**  The growing mass of big data stored on devices means there is a rising demand for forensics experts. While the majority of roles in security are centred around prevention and optimisation, forensic experts investigate and analyse data following disasters and major incidents. The experienced digital team at [Fields Data Recovery](https://www.fieldsassociates.co.uk/data-recovery) take a closer look at storage devices, networks and connected devices to recover information and compile evidence for legal cases. Employed by such a company as a forensics expert, you could be working for the government, consulting and legal firms, and law enforcement agencies among others.  **Security software developer**  If you have an interest in programming and coding in addition to cybersecurity, then pursuing a career as a security software developer might be desirable. Enterprises are now building applications and software from the ground up with security in mind. If you take on this role, you will be tasked with integrating security into the design and development phases of software development. You may also have to work with clients when deploying security software.  **Security auditor**  Cybersecurity is one of the greatest challenges for modern enterprises, but SMEs and even larger corporations still struggle to implement the correct security strategies. As an auditor, you would take up a mid-level position and examine the effectiveness of an enterprise’s current IT setup and provide a report detailing any improvements and changes required. Auditors need to evaluate factors such as regulations and compliance, as well as the efficiency and effectiveness of policies.  **Security engineer**  Security engineers are arguably the most hands-on, technically focused roles available as they are not concerned with business wider strategies. Instead, engineers handle technical problems, install firewalls and antivirus software, and perform tests. You will need some knowledge of coding for this intermediate level position.  **Conclusion**  Cybersecurity is still an industry very much in its infancy, and its full career potential is yet to be realised. This is an exciting time for any student to opt for a career in the industry. It is important to remember that many of the skills you will learn will also provide you with a foundation to explore other facets of IT and tech. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **20-June-2020** | **Name:** | **Raziya Banu** |
| **Course:** | **Introduction to Ethical Hacking** | **USN:** | **4AL16EC058** |
| **Topic:** | **Career and growth ladder in ethical hacking** | **Semester & Section:** | **8th sem & ‘B’ section** |
| **AFTERNOON SESSION DETAILS** | | | |
| **Image of session** | | | |
| “To beat a hacker, you have to think like one” – Ethical Hacking Council  Hacking is the process of finding vulnerabilities in a system and using these found vulnerabilities to gain unauthorized access into the system to perform malicious activities ranging from deleting system files to stealing sensitive information. Hacking is illegal and can lead to extreme consequences if you are caught in the act. People have been sentenced to years of imprisonment because of hacking.  Nonetheless, hacking can be legal if done with permission. Computer experts are often hired by companies to hack into their system to find vulnerabilities and weak endpoints so that they can be fixed. This is done as a precautionary measure against legitimate hackers who have malicious intent. Such people, who hack into a system with permission, without any malicious intent, are known as ethical hackers and the process is known as an [ethical hacking](https://www.edureka.co/blog/what-is-ethical-hacking). ****Requirement to Become an Ethical Hacker**** How your ethical hacking career begins depends on your current field of work. If you’re not in an IT field you should definitely try shifting into one. Even though most jobs require you to have a Bachelor’s degree in computer science or cybersecurity-related field, exceptions are made for people with sound knowledge of operating systems, databases and networking! Also, it is nigh impossible to directly become an ethical hacker. Most ethical hackers begin their career as tech support engineers who climb their way up, by earning [certifications](https://www.youtube.com/watch?v=eO8l70pdVhY) like CCNA and CISSP before working towards the ultimate CEH certification. After earning your CEH certifications, is the time to market yourself as an ethical hacker! Roles & Responsibilities of an Ethical Hacker Roles and Resp - Ethical Hacking Career - Edureka  There seems to be a general misconception that a person with an ethical hacking career is only responsible for penetration testing of systems and applications. This is not true, and an ethical hacker is responsible for much more.   * Scanning open and closed ports using Reconnaissance tools like Nessus and NMAP * Engaging in social engineering methodologies * Examining patch releases by performing vigorous vulnerability analysis on them * An ethical hacker will see if he/she can evade IDS (Intrusion Detection systems), IPS (Intrusion Prevention systems), honeypots and firewalls * Ethical hackers can employ other strategies like sniffing networks, bypassing and cracking wireless encryption, and hijacking web servers and web applications   An ethical hacker strives to replicate the working of a black hat hacker by analyzing the defense protocols and social-engineering aspects of an organization. His job is to make sure the organization reacts to these situations well enough if they are already not doing so.  **Ethical Hacker Skill Set**  A person with an ethical hacking career is expected to be proficient in database handling, networking, and operating systems and also have excellent soft skills as they need to communicate problems regarding security to the rest of the organization. Other than these generalized skillsets, an ethical hacker also have a good grasp on the following skills:   * Network traffic sniffing * Orchestrate various network attacks * Exploit buffer overflow vulnerabilities * SQL injection * Password guessing and cracking * Session hijacking and spoofing * DNS spoofing | | | |