**DAILY ASSESSMENT FORMAT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **1/06/2020** | **Name:** | **Nayanashree K S** |
| **Course:** | **Cyber security** | **USN:** | **4AL16EC042** |
| **Topic:** | **Compliance**  **Governance and industry standards** | **Semester & Section:** | **8 A** |
| **Github Repository:** | **nayana\_online** |  |  |

|  |
| --- |
| **FORENOON SESSION DETAILS** |
| **Image of session** |
| **Report**  In simple terms, cyber security is the exercise of protecting computer systems from attacks. Such attacks are usually aimed at gaining unauthorized access, destroying, altering, disrupting, and gaining control of information or operations to extort money from victims. Some aspects of cyber security include network, systems, applications, information, and operational security.  For this reason, there is a need for an effective security strategy that will not only guard these systems effectively from such attacks but also detect them before they occur.  **Cyber Security Job Market Trends**   * Demand for generalist job roles relating to cybersecurity is fading off gradually and being replaced by specialized roles. Demand for artificial intelligence, IT Security forensics, and IoT security skills continue to rise as the industry takes a more pre-emptive approach. * Regulated industries like financial institutions, government operations, retail trade, energy, healthcare, are among those with higher career prospects in the cyber security field. This is due to the legal security regulations that bind their operations thanks in part to the fact that they handle massive consumer information. * Cloud security is among the IT security fields with high demand as more data and operations move to both public and private cloud platforms. Much as the security of cloud services was vested on the service providers, more industry players are joining the bandwagon to address the security matter as a whole. * While it is possible to opt into the information security without a strong educational background, the job market values education and experience. 84% of employers will set a bachelor’s degree, particularly in Information technology or computer science, and at least three years of industry experience as the minimum requirement of their job postings. * After the education qualification and work experience, 35% of employers are likely to use certifications as a criterion for acquiring the best skills. * Employers are already warming up to the idea of including security clearance in their list of requirements. [10%](https://www.burning-glass.com/blog/how-to-get-a-cybersecurity-job-in-three-charts-a-degree-a-certification-and-a-clearance/) of cybersecurity posts need a security clearance. 10% of these roles, however, take time to be filled. * With the Fortune 500 companies setting the pace, the information security employment landscape is transforming rapidly as more women take up senior positions. It was projected that by 2019, [20%](https://go.forrester.com/blogs/predictions-2019-cybersecurity/) of the CISO roles in Fortune 500 companies would be filled by women in a bid to embrace a gender-inclusive culture in the industry.   However, these 5 important factors will help shape the cyber security professional.   1. **Formal Education**   While it is not cast in stone that you have a degree to pursue a career in cybersecurity and honestly not many started at this point, employers still have some value attached to a bachelor’s degree.  With a bachelor’s degree in cybersecurity or a degree in a related field like computer science or information technology, you will have started your career on a high note and with an added advantage.   1. **Experience**   The one challenge that the cyber security field faces is a wide skills gap. This has resulted in high demand for professionals and a talent pool that does not fit the skills requirements. Skills are best acquired through learning and doing.  It is possible to gain some experience through self-learning even without a formal educational background in a related field. However, you will need deep interest, passion, and a lot of patience to achieve your goals. Secondly, you must learn the basics before getting to the practical.   1. **Certifications**   In cybersecurity, certifications matter a great deal. Certifications are skill-specific. They are one way of achieving specific goals, especially if you want to sharpen specific skills in cybersecurity or curve your career path.  Certifications like the ones listed below are good and can help you boost your skills at any point in your career.   * CISSP (Certified Information Systems Security Professional) * CISM (Certified Information Security Manager) * CEH ([Certified Ethical Hacker](https://www.simplilearn.com/cyber-security/ceh-certification)) * CCSP (Certified Cloud Security Professional) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date:** | **19/6/2020** | **Name:** | **Nayanashree K S** | |
| **Course:** | **Ethical hacking** | **USN:** | **4al16ec042** | |
| **Topic:** | **Ethical hacking on mobile platforms – Demonstration**  **Ethical hacking in network architecture - Demonstration** | **Semester & Section:** | **8 A** | |
| **AFTERNOON SESSION DETAILS** | | | |
| **REPORT** **Ethical Hacking - Process** Like all good projects, ethical hacking too has a set of distinct phases. It helps hackers to make a structured ethical hacking attack.  Different security training manuals explain the process of ethical hacking in different ways, but for me as a Certified Ethical Hacker, the entire process can be categorized into the following six phases.  Ethical Hacking Process **Ethical Hacking - Footprinting** Footprinting is a part of reconnaissance process which is used for gathering possible information about a target computer system or network. Footprinting could be both **passive** and **active**. Reviewing a company’s website is an example of passive footprinting, whereas attempting to gain access to sensitive information through social engineering is an example of active information gathering.  Footprinting is basically the first step where hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target.  During this phase, a hacker can collect the following information −   * Domain name * IP Addresses * Namespaces * Employee information * Phone numbers * E-mails * Job Information   In the following section, we will discuss how to extract the basic and easily accessible information about any computer system or network that is linked to the Internet. Domain Name Information You can use <http://www.whois.com/whois> website to get detailed information about a domain name information including its owner, its registrar, date of registration, expiry, name server, owner's contact information, etc.  Whois **Quick Fix** It's always recommended to keep your domain name profile a private one which should hide the above-mentioned information from potential hackers. Finding IP Address You can use **ping** command at your prompt. This command is available on Windows as well as on Linux OS. Following is the example to find out the IP address of tutorialspoint.com  $ping tutorialspoint.com  It will produce the following result −  PING tutorialspoint.com (66.135.33.172) 56(84) bytes of data.  64 bytes from 66.135.33.172: icmp\_seq = 1 ttl = 64 time = 0.028 ms  64 bytes from 66.135.33.172: icmp\_seq = 2 ttl = 64 time = 0.021 ms  64 bytes from 66.135.33.172: icmp\_seq = 3 ttl = 64 time = 0.021 ms  64 bytes from 66.135.33.172: icmp\_seq = 4 ttl = 64 time = 0.021 ms | | | |