**Daily Assessment Report**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **19-06-20** | **Name:** | **Anand kumar k** |
| **Course:** | **Cyber security** | **USN:** | **4AL16EC002** |
| **Topic:** |  | **Semester & Section:** | **8TH & A** |
| **Github Repository:** | **Anand-courses** |  |  |

|  |
| --- |
| **FORENOON SESSION DETAILS** |
| **Image of session** |
| Cyber security is the state or process of protecting and recovering networks, devices and programs from any type of cyberattack.  Cyberattacks are an evolving danger to organizations, employees and consumers. They may be designed to access or destroy sensitive data or extort money. They can, in effect, destroy businesses and damage your financial and personal lives — especially if you’re the victim of identity theft. Types of cyber security In order to be better protected, it’s important to know the different types of cybersecurity. These include critical infrastructure security, network security, application security, information security, cloud security, data loss prevention, and end-user education.  **Critical infrastructure security:** Consists of cyber-physical systems such as electricity grid and water purification systems.  **Network security:** Protects internal networks from intruders by securing infrastructure. Examples of network security include the implementation of two-factor authentication (2FA) and new, strong passwords.  **Application security:** Uses software and hardware to defend against external threats that may present themselves in an application’s development stage. Examples of application security include antivirus programs, firewalls and encryption.  **Information security:** Also known as InfoSec, protects both physical and digital data—essentially data in any form—from unauthorized access, use, change, disclosure, deletion, or other forms of malintent.  **Cloud security:** A software-based tool that protects and monitors your data in the cloud, to help eliminate the risks associated with on-premises attacks.  **Data loss prevention:** Consists of developing policies and processes for handling and preventing the loss of data, and developing recovery policies in the event of a cyber security breach. This includes setting network permissions and policies for data storage.  **End-user education:** Acknowledges that cyber security systems are only as strong as their potentially weakest links: the people that are using them. End-user education involves teaching users to follow best practices like not clicking on unknown links or downloading suspicious attachments in emails—which could let in malware and other forms of malicious software. Types of cyber threats There are many types of cyberthreats that can attack your devices and networks, but they generally fall into three categories. The categories are attacks on confidentiality, integrity and availability.   * **Attacks on confidentiality**. These attacks can be designed to steal your personal identifying information and your bank account or credit card information. Following these attack, your information can be sold or traded on the dark web for others to purchase and use. * **Attacks on integrity.** These attacks consist of personal or enterprise sabotage, and are often called leaks. A cybercriminal will access and release sensitive information for the purpose of exposing the data and influencing the public to lose trust in a person or an organization. * **Attacks on availability.** The aim of this type of cyberattack is to block users from accessing their own data until they pay a fee or ransom. Typically, a cybercriminal will infiltrate a network and authorized parties from accessing important data, demanding that a ransom be paid. Companies sometimes pay the ransom and fix the cyber vulnerability afterward so that they can avoid halting business activities.   Here are a few types of cyber threats that fall into the three categories listed above.  [Social engineering](https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html), a type of attack on confidentiality, is the process of psychologically manipulating people into performing actions or giving away information. Phishing attacks are the most common form of social engineering. Phishing attacks usually come in the form of a deceptive email with the goal of tricking the recipient into giving away personal information.  APTs (advanced persistent threats), a type of attack on integrity, where an unauthorized user infiltrates a network undetected and stays in the network for a long time. The intent of an APT is to steal data and not harm the network. APTs often happen in sectors with high-value information, such as national defense, manufacturing, and the finance industry.  [Malware](https://us.norton.com/internetsecurity-malware-how-can-i-tell-if-i-have-malware-and-what-can-i-do-about-it.html), or malicious software, is a type of attack on availability. It refers to software that is designed to gain access to or damage a computer without the knowledge of the owner. Malware can do everything from stealing your login information and using your computer to send spam, to crashing your computer system. Several common types of malware include spyware, keyloggers, true viruses, and worms.  Ransomware, another form of malicious software, also is a type of attack on availability. Its goal is to lock and encrypt your computer or device data—essentially holding your files hostage—and then demand a ransom to restore access. A victim typically must pay the ransom within a set amount of time or risk losing access to the information forever. Common types of ransomware include crypto malware, lockers and scareware. |
| Daily Assessment Report   |  |  |  |  | | --- | --- | --- | --- | | Date: | 19-06-20 | Name: | Anand kumar k | | Course: | Ethical hacking | USN: | 4AL16EC002 | | Topic: |  | Semester & Section: | 8TH & A | | Github Repository: | Anand-courses |  |  |  |  | | --- | | Afternoon SESSION DETAILS | | Image of session | | The word hacking is defined as an illegal use of the other’s computer system or the network resources. Hacker is the term which is formerly meant for the skillful programmer. The word hacker refers to the names of the persons who enjoys the work in learning the details of the computer systems and stretch the capabilities from the system. The system of hacking describes the fast improvement in the new programs that make the codes for the providing a better security to the system with more efficiency. The word cracker also belongs to the same field it make use of the hacking skills for the unlawful purposes like email id, intruding into other’s system. Hacking is of different types such as back door hacking, viruses and worms, Trojan horses, Denial of Services, anarchists, crackers, kiddies and ethical hacking. In the types of hacking system one of the most common hacking is **ethical hacking**. **Ethical Hacking Services** **Ethical hacking** is an emerging tools used by most of the organizations for testing network security. The security risks and vulnerabilities in a network can be recognized with the help of ethical hacking.  **Ethical hacking** is defined as the services that provides the securities for the customer’s networks, information assets and identifies the vulnerabilities to maintain the reputation of the corporate sectors before it exploit the company. This type of the hacking system provides the high securities to the customer’s methodologies and techniques to yield high qualities of infrastructures. The ethical hacking system includes some of the service like:   1. **Application Testing:**This is an uncover design or the logic flaws which result in the compromising with the unauthorized accessing of the systems, networks, applications or the information regarding the systems. This application testing is used for investigating and identifying the extent and the criticality of the problems exposure to the thick client (Java) and thin client (web browsers) applications. This application testing includes the services like client-side application testing and web application testing’s. The client-side application testing is the process of developing the software that is used for the measuring the integrated security into the client software constituents. In this system this testing application is based on the gathering of the information by observer using the reverse engineering system. 2. **War Dialing:**This is one of the services that are provided by ethical hacking. War dialing is a method of dialing a modem number to identify open modem connection that supplies access in a remote way to a network for targeting a particular system. This word is originated from the day the when the internet has come into the existence in most of the companies. This follows the method of scanning to find the strength of the network connection. The tools of War dialing work on the concept that organizations do not pay attention to dial-in ports like they do towards the firewalls. 3. **Network Testing:**The networking testing services of the ethical hacking provides the information on the exposures of the network, services, and solutions on the convergence, protocols and system devices including the virtual private network technologies. This testing process includes a number of constitutes in external and internal devices. It also analyzes the applications of the voice over Internet protocol within the environment of the organization. The main goal of the network testing application is to make obvious demonstration of the political effects on its development. By making use of this application into the organization, it provides a complete enlightenment to the work for determining the result in the organization. 4. **Wireless Security:**Wireless security services measures the security in the available architecture to provide a guidelines to ensure the system integrity and accessibility of the resources. The working of wireless security is based on the three phases. In the first phase of the operation it identifies the activeness of the wireless networks. The team of the ethical hacking demonstrates the exposure to the attackers with the space in the wireless network. In the seconds phase of this system it implements a normal users to evaluate the measures of the security that secures the infrastructures of the organization to control the accessing of the devices. During the third phase the team will try to utilize the discovered threats to gain access on other networks. This provides the security in wireless local area network, virtual private network, intrusion detection system and wireless public key infrastructure. 5. **System Hardening:**The system hardening stresses on the network vicinity. Security is the prime factor that determines the level of integrity of the information and resources used in the computing. Effective deployment of the security controls unauthorized, accidental disruption if resources in information technology. The system hardening assessment is complemented in three phases. The ethical hacking team will analyze the network to identify the loop holes in security updates and other frequent security defects. **Need for Ethical Hacking** | |