# DAILY ASSESSMENT

|  |  |  |  |
| --- | --- | --- | --- |
| Date: | 19/06/2020 | Name: | Chesmi B R |
| Course: | **Cyber security** | USN: | 4AL16EC100 |
| Topic: | **What is cyber security** | Semester & Section: | 8TH SEM & A Section |
| Github Repository: | chesmibr |  |  |

|  |
| --- |
| **FORENOON SESSION DETAILS**       Report: 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. Scale of cyber security threats While cyber-defense tactics are evolving, so are cyber security threats, with malicious software and other dangers taking new forms. And cyber security threats don’t discriminate. All individuals and organizations that use networks are potential targets. To help protect yourself, it’s important to know the three different types of cyber security threats: cybercrime, cyberattacks, and cyberterrorism.   * Cybercrime is committed by one or more individuals who target your system to cause havoc or for financial gain. * Cyberattacks are often committed for political reasons and may be designed to collect and often distribute your sensitive information. * Cyberterrorism is designed to breach electronic systems to instill panic and fear in its victims.  How to help protect against cyber security attacks  * Only use trusted sites when providing your personal information. A good rule of thumb is to check the URL. If the site includes “https://,” then it’s a secure site. If the URL includes “http://,” — note the missing “s” — avoid entering sensitive information like your credit card data or Social Security number. * Don’t open email attachments or click links in emails from unknown sources. One of the most common ways networks and users are exposed to malware and viruses is through emails disguised as being sent by someone you trust. * Always keep your devices updated. Software updates contain important patches to fix security vulnerabilities. Cyber attackers can also target outdated devices which may not be running the most current security software. * Back up your files regularly for extra protection in the event of a cyber security attacks. If you need to wipe your device clean due to a cyberattack, it will help to have your files stored in a safe, separate place.   Cyber security is constantly evolving, which can make it difficult to stay up to date. Staying informed and being cautious online are two of the best ways to help protect yourself, your networks and devices, and your business. |

**DAILY ASSESSMENT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **19/06/2020** | **Name:** | **Chesmi B R** |
| **Course:** | **Ethical Hacking** | **USN:** | **4AL16EC100** |
| **Topic:** | **Ethical hacking in network architecture- demonstration,**  **Ethical hacking in web applications-demonstration.** | **Semester & Section:** | **8TH SEM & A Section** |
| **Github Repository:** | **chesmibr** |  |  |

|  |
| --- |
| **AFTERNOON SESSION DETAILS** |
|  |

|  |
| --- |
| **Report**-  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**   The process of employing someone to hack ones company is ethical hacking. Ethical hacking is one of the tools that are used to judge the security programs of the organizations. It is also referred as penetrating testing, red teaming, intrusion testing, vulnerability and even security judgments. Each one these has different meanings in different countries. Hacking is also described as new development of the existing programs, software and code. It makes them better and more efficient. Ethical hacker can know the details of computer while hacking and become the security professional. It involves in foot-printing, scanning, tacking all the secured information. Ethical means a philosophy with morality.  Hackers hack systems to detect dangerous, unauthorized access and misuse. Threat and vulnerability are the two dangers the hacker has to face. The hacking report must be confidential as it should face the organizations security risks. If this goes wrong in any way the organization results in fatal, penalties and loss. For example: computer crime is done by misuse of their hacking skills. The need to hack is for catching the thief. Ethical hacking is the correct method to make your computers work properly. Ethical hacker needs higher level skills compared to penetration testing. Penetration testing is same as ethical hacking but the hacker uses the penetrating tools and tests the security danger. **Types of Ethical Hacking** Ethical hackers use various methods for breaking the security system in the organizations in the period of cyber attack. Various types of ethical hacks are:   1. Remote Network:  This process in especially utilized to recognize the attacks that are causing among the internet. Usually the ethical hacker always tries to identify the default and proxy information in the networks some of then are firewalls, proxy etc. 2. Remote dial up network:  Remote dial up network hack identify and try to protest from the attack that is causing among the client modern pool. For finding the open system the organizations will make use of the method called war dialing for the representative dialing. Open system is one of the examples for this type of attacks. 3. Local Network:  local network hack is the process which is used to access the illegal information by making use of someone with physical access gaining through the local network. To start on this procedure the ethical hacker should ready to access the local network directly. 4. Stolen Equipment:  By making use of the stolen equipment hack it is easy to identify the information of the thefts such as the laptops etc. the information secured by the owner of the laptop can be identified. Information like username, password and the security settings that are in the equipment are encoded by stealing the laptop. 5. Social engineering:  A [social engineering attack](https://www.mbaknol.com/business-ethics/social-engineering-attacks/) is the process which is used to check the reliability of the organization; this can be done by making use of the telecommunication or face to face communication by collecting the data which can be used in the attacks. This method is especially utilized to know the security information that is used in the organizations. 6. Physical Entry:  This Physical entry organization is used in the organizations to control the attacks that are obtained through the physical premises. By using the physical entire the ethical hacker can increase and can produce virus and other Trojans directly onto the network. 7. Application network:  the logic flaws present in the applications may result to the illegal access of the network and even in the application and the information that is provided in the applications. 8. Network testing:  In this process it mainly observes the unsafe data that is present in the internal and the external network, not only in the particular network also in the devices and including the virtual private network technologies 9. Wireless network testing:  In this process the wireless network reduces the network liability to the attacker by using the radio access to the given wireless network space. 10. Code review:  This process will observe the source code which is in the part of the verification system and will recognize the strengths and the weakness of the modules that are in the software. 11. War dialing: It simply identifies the default information that is observed in the modem which is very dangerous to the corporate organizations.  **Applications  of Ethical Hacking** Ethical hacking is nothing but the one which performs the hacks as security tests for their systems. Ethical hacking can be used in many applications in case of web applications which are often beaten down. This generally includes Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) applications are most frequently attacked because most of the firewalls and other security are things has complete access to these programs from the Internet. Malicious software includes viruses and Trojan horses which take down the system. Spam is a junk e-mail which causes violent and needless disturbance on system and storage space and carry the virus, so ethical hacking helps to reveal such attacks against in computer systems and provides the security of the system.  The main application of this is to provide the security on wireless infrastructure which is the main purpose of present business organization. Ethical hacking has become main stream in organizations which are wishing to test their intellectual and technical courage against the underworld. Ethical hacking plays important role in providing security. Resources are the computer related services that performs the tasks on behalf of user. In Ethical hacking the resources are the core services, objects code etc.  The ethical hacking has advantages of gaining access to an organizations network and information systems. This provides the security in the area of Information technology called as Infosec. This provides security to the high level attacks such as viruses and traffic trough a firewall. This has been providing the security for various applications which are even bypassing the firewalls, Intrusion-detection systems and antivirus software. This includes hacking specific applications including coverage of e-mails systems, instant messaging and [VOIP (voice over IP)](https://www.mbaknol.com/information-systems-management/voice-over-internet-protocol-voip/). The resources i.e. devices, systems, and applications that are generally used while performing the hacking process are Routers, Firewalls, Network infrastructure as a whole, wireless access points and bridges, web application and database servers, E-mail and file servers, workstations, laptops and tablet PCs, Mobile devices, client and server operating systems, client and server applications .  Ethical hacking tests both the safety and the security issues of the programs. Hence from the above context it can be stated as the ethical hacking is important in the present scenario as providing security is very important now a day. This is very important in web applications as the hacking can be easily done in this case. |