# DAILY ASSESSMENT

|  |  |  |  |
| --- | --- | --- | --- |
| Date: | 18/06/2020 | Name: | GAURAV NR |
| Course: | **Cyber security** | USN: | 4AL15EC025 |
| Topic: | **Secure system design,**   |  | | --- | | **Threats and vulnerabilities** | | Semester & Section: | 8TH SEM & A Section |
| Github Repository: | gaurav |  |  |

|  |
| --- |
| **FORENOON SESSION DETAILS**     Report:Data encryption: Threats and best practices Since it first emerged, encryption has long been held as one of the top data protection techniques available. This security approach enables the user to scramble the content of protected systems and documents and utilize a decryption key to decipher it. In this way, only authorized viewers – those with access to the key – are able to read the protected information.  Currently, encryption is leveraged in a range of different settings, including within enterprises, the armed forces, and to protect payment details on e-commerce websites. Although many are aware of the security advantages that encryption can offer, there is one main threat to its protection: the fact that some have yet to adopt it.  Lawfare contributor Paul Rosenzweig noted that for quite some time within the technology industry, it has become common knowledge that encryption, when deployed properly, can safeguard information against nearly any threat. However, many users – even those dealing with highly sensitive materials – have yet to implement it.  “Yet is has been the case for an equally long time that [very few people actually use encryption](http://www.lawfareblog.com/2014/09/the-encryption-wars-continue/) to protect their vital secrets – not journalists, not criminals, and most assuredly not the … ‘average layman user.,'” Rosenzweig wrote.  He points to a bevy of reasons as to why this is the case, especially in the current environment where threats that could be mitigated by encryption seem to run rampant. Some users may not be aware of the staunch security encryption can offer, or others may simply think they will not fall victim to an attack.“Of all of these, I tend to think complexity and laziness lead the list – that is, most encryption programs are difficult to use and need to be installed,” Rosenzwieg pointed out. “They don’t have ‘one button’ applications and they are not ‘on’ by default.”  Whatever the reason, the end result is the same: Critical information – that is no doubt an attractive target to cybercriminals – goes unprotected.  **Encryption best practices** In this spirit, it is important for all users to understand just how powerful encryption can be when it comes to guarding personal information and sensitive data belonging to a business. When applied correctly, encryption provides a near-bulletproof barrier against all unauthorized intrusion, ensuring that only those permitted to view the content are allowed to.  But what exactly is involved in “proper” encryption use? Consider the following best practices when deploying and utilizing encryption to ensure top notch security:  **Examine what needs protection** First, it is vital to understand what information needs encryption protection to decide where the technology will be deployed. In today’s threat environment, a myriad of details are considered valuable to hackers, including payment card information, names, birthdates, social security numbers and intellectual property belonging to a company. Because this data can be utilized for fraudulent purposes and is therefore fair game for cybercriminals, encryption should be put in place to prevent intrusion.  At the same time, users should consider not only what information needs protecting, but when to implement security. When data is sitting in an overarching system with its own security measures, encryption may not be necessary. On the other hand, when content is in transit, or being sent to internal or external parties, encryption is the sender’s best bet to ensure that the information is not intercepted along the way.  **Consider how encryption will interact with cloud systems** NetworkWorld contributor Linda Musthaler noted that encryption has become increasingly robust and popular due to the advent of cloud computing technology. Because the cloud vendor manages certain aspects of the system containing data, organizations [need an added protection measure](http://www.networkworld.com/article/2189817/infrastructure-management/best-practices-for-data-encryption-part-1.html) to ensure that their company information remains secure. However, when encryption is deployed within cloud-based materials like SaaS and data analytics applications, there are several important elements to consider. These include whether or not all functions of the program will remain available, if encryption will meet compliance needs and how keys will be generated.  “Cloud environments introduce all sorts of complexities to think through before selecting one or more encryption solutions,” Musthaler wrote.  While taking into account these extra precautions may seem cumbersome, including encryption in cloud security can not only offer protection for company information, but peace of mind for administrators as well.  **Get details about the encryption algorithm** Musthaler also recommends gleaning details about the algorithm being utilized from the encryption vendor. Although there are overarching requirements for primary encryption algorithms, Musthaler noted that some providers “can take liberties with how they apply the standards.” This can have an impact on the strength of the protection the encryption provides. Therefore, users should ask about the algorithm in place and how it matches up with international standards.  “[I]t’s important for you to ask your vendor questions about the specific modules they use,” Musthaler wrote. “When choosing a solution, it’s best to stick with an encryption module that adheres to industry standards.”  Brocade noted in a recent white paper that other [considerations to make with algorithms](http://www.brocade.com/downloads/documents/best_practice_guides/encryption-best-practices.pdf) include the speed of encryption, memory usage, cost, openness and range of application coverage. Factoring in these essentials will help guarantee that the proper algorithm is in place.  **Ensure proper key management** Once the technology is in place, administrators must ensure that the decryption key is properly managed. With proper control, keys can lead to serious protection issues, the white paper noted.  “After being created, keys need to be backed up and managed,” the white paper stated. “Keys can be lost, stolen or destroyed unintentionally, or they can expire after a predetermined period of time. All of these are security vulnerabilities.”  Users should select a secure location in which to keep their encryption keys, ensuring that access is limited to only those authorized. A secondary, protected site should be chosen for the backup key and these locations should be maintained for the life of the secured information and its connected key. Brocade noted that there are key management solutions as well as key vaults available that provide the proper environment to maintain keys.  When users are educated about the top-tier protection encryption can offer and deploy it with best practices in mind, they stand a much better chance of thwarting unauthorized access and keeping information secure. |

**DAILY ASSESSMENT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **18/06/2020** | **Name:** | **GAURAV NR** |
| **Course:** | **Ethical Hacking** | **USN:** | **4AL15EC025** |
| **Topic:** | **Career and growth ladder in ethical hacking**  **Domains and process implementation under ethical hacking** | **Semester & Section:** | **8TH SEM & A Section** |
| **Github Repository:** | **gaurav** |  |  |

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

|  |
| --- |
| **Report**-  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. Reconnaissance Reconnaissance is the phase where the attacker gathers information about a target using active or passive means. The tools that are widely used in this process are NMAP, Hping, Maltego, and Google Dorks. Scanning In this process, the attacker begins to actively probe a target machine or network for vulnerabilities that can be exploited. The tools used in this process are Nessus, Nexpose, and NMAP. Gaining Access In this process, the vulnerability is located and you attempt to exploit it in order to enter into the system. The primary tool that is used in this process is Metasploit. Maintaining Access It is the process where the hacker has already gained access into a system. After gaining access, the hacker installs some backdoors in order to enter into the system when he needs access in this owned system in future. Metasploit is the preferred tool in this process. Clearing Tracks This process is actually an unethical activity. It has to do with the deletion of logs of all the activities that take place during the hacking process. Reporting Reporting is the last step of finishing the ethical hacking process. Here the Ethical Hacker compiles a report with his findings and the job that was done such as the tools used, the success rate, vulnerabilities found, and the exploit processes.  Ethical hackers play an important role in industries by fixing vulnerabilities in systems and using these vulnerabilities to gain unauthorized access into to the system to perform malicious activities and deleting system files within applications.  Computers experts are hired by so many companies to hack into the systems to find week points so that they can be easily fixed. So, such people who hack into a system with the permissions without any malicious intent to improve and fix the system is Called Ethical hacker and the process which done is known as Ethical Hacking.  So many ethical hackers are using python in day to day job. Ethical Hacking, however, may be a legal variation of hacking. firms rent laptop consultants to check system security, determine vulnerabilities, and supply analysis on the way to improve the firewall. it's additionally the simplest way for presidency agencies to spot and find potential threats to national security.  Having a basic data concerning [networking](http://www.selfgrowth.com/business_networking.html) setting would be a bonus. Let’s point out the most effective programming languages it's the fundamental skills that a hacker ought to possess. Although selecting the most effective programing language is depends on the sort of attack that a hacker desires to perform. The best thanks to subsume it's to know however it works and truly works consequently thereto mind map itself. this sort of hacking we will decision as moral hacking. Mind you, it's utterly legal and presently possesses the nice scope within the city.  REASON TO FIND OUT HACKING:  Now that you just are on this page, it's quite obvious that you just either should have searched on the proper thanks to become a hacker or why you wish to find out hacking. Frankly, it's fun however solely until you follow the ethics and don’t misuse the data in the other method. Remember, if you are doing it for fun, you may be encircled with special life however with criminal intention, you may ought to pay your life in jail.   It is the hacker UN agency builds the pc system in such the simplest way that will defend the access of the hacker and would make sure that safeguard system is well used. it's the hacker UN agency makes the positive malicious attack from unknown supply gets protected. Such person is capable to use preventive measures to avoid any quite security breaches. to form positive the client or user data is well protected, the hacker comes up with a replacement answer. it's the hacker UN agency make sure that network is tested on the regular note.  Requirment FOR Ethical HACKERS:  Cyber-crimes are getting additional common and attackers additional subtle with rouge nation-states and terrorist organizations funding criminals to rear of barrel security networks either to extort hefty ransoms or compromise national security measures. Businesses are round-faced with the challenge of handling advanced security necessities that require to be updated as per dynamic hacking techniques, handling hidden vulnerabilities and evolving technologies. moral hacking companies with specially trained professionals come back to the rescue of companies whereas guaranteeing effectiveness of service and confidentiality.  **Importance Ethical Hacking Online:**  Because of Covid-19 or Lockdown which is a challenge for us to fight and defeat corona without wasting time and losing our aim. There are so many Institute who provide the candidates a specific or certified course for their better career. Online is a good way to develop your specialization in Ethical hacking. In Today’s world some people have the time in their busy day to day life and work environment to spend time training. There Are most of Institute provide online Ethical Hacking certification courses for candidates which help you to achieving their career path. Online training is good medium to learn Ethical Hacking Certification Courses.  Ethical Hacking has been a career option for so many fresher candidates and experience candidates. this can be a great career opportunity depending on your experience and skills you can earn a very good salary & profile. There are so many brand knowing industries who uses this domain they want so many candidates for the same profile with basic and advance knowledge of Ethical hacking. |