**DAILY ASSESSMENT FORMAT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **20-06-2020** | **Name:** | **Karthik J** |
| **Course:** | Cyber Security Go from Zero - Udemy | **USN:** | **4AL16EC030** |
| **Topic:** |  | **Semester & Section:** | **8TH A** |
| **GitHub Repository:** | Karthik-J |  |  |

|  |
| --- |
| **FORENOON SESSION DETAILS** |
| ***Image Section***   **History of Cyber Security** The origin of cybersecurity began with a research project. It only came into existence because of the development of viruses.  In 1969, **Leonard Kleinrock**, professor of UCLA and student, **Charley Kline**, sent the first electronic message from the UCLA SDS Sigma 7 Host computer to Bill Duvall, a programmer, at the Stanford Research Institute. This is a well-known story and a moment in the history of a digital world. The sent message from the UCLA was the word "login." The system crashed after they typed the first two letters "lo." Since then, this story has been a belief that the programmers typed the beginning message **"lo and behold."** While factually believed that **"login"** was the intended message. Those two letters of messages were changed the way we communicate with one another.  In 1970's, **Robert (Bob) Thomas** who was a researcher for BBN Technologies in Cambridge, Massachusetts created the first computer worm (virus). He realized that it was possible for a computer program to move across a network, leaving a small trail (series of signs) wherever it went. He named the program **Creeper**, and designed it to travel between Tenex terminals on the early ARPANET, printing the message "I'M THE CREEPER: CATCH ME IF YOU CAN."  An American computer programmer named **Ray Tomlinson**, the inventor of email, was also working for BBN Technologies at the time. He saw this idea and liked it. He tinkered (an act of attempting to repair something) with the program and made it self-replicating "the first computer worm." He named the program **Reaper**, the **first antivirus software** which would found copies of The Creeper and delete it. Types of Cyber Attacks Below are the different types of cyber attacks:   1. [Denial of Service Attack (DoS)](https://www.educba.com/denial-of-service-attack/) 2. Hacking 3. Malware 4. [Phishing](https://www.educba.com/what-is-phishing/) 5. Spoofing 6. [Ransomware](https://www.educba.com/what-is-ransomware/) 7. Spamming   All of the best possible technology is made easily available at our fingertips, but all using online services has some drawbacks too. We all have certainly heard about this, cyber-crime, but do we know how does it affect us and attack us? Cyber-crime is an organized computer-oriented crime that can affect people using devices on a network.  To define Cyber-crime, it is a crime committed with the help of computers and networks. It includes, hacking, phishing and spamming. These types of crimes are committed by people called Cybercriminals. These people have a set of mentality which to destroy what is good.  There can be three main motives behind cyber-crimes, viz:   1. **Monetary Benefit:** These types of criminals try to hack into the user’s personal or corporate bank details so as to gain monetary benefits out of it. These criminals can create fake ID’s and websites, or even send emails asking personal information to the users. They also may create fake accounts where the use of money is transferred. 2. **Information:** Some of the cybercriminals will try to steal some confidential information that can be sold online marketing sites, or even to some other competitor companies or use it for personal benefits. 3. **Acknowledgment**: Some of them also may not want to benefits out of it, but to showcase their name to the world of their presence.   There are a great many other services which are made available like Anti-viruses and firewalls. Yes, all of the above mentioned and cybersecurity tools make systems more secure for sure, but the human interference in the system is an important aspect too, like to pull data off one computer; one can easily access it using a pen-drive which might be affected. Types of Cyber Security All of these serious crimes are committed online and can be stopped or at the least limited to some level by using Cyber Security Tools. Some of the best Cyber Security Tools made available today are: **1.**IBMQRadarAdvisor and Watson This is by far the best security tool in use by any of the organizations. Watson, [using artificial intelligence (AI)](https://www.educba.com/what-is-artificial-intelligence/), is a self-learning and self-evolving system. What it does is, before even the threat is detected it eliminates the section. The working goes as such: IBM QRadar tracks the section. It gathers information and links online, offline and within the system with that code. It formulates a strategy to encompass it and then when an incident is raised, it kills the threat. This is one of the best online incidents – kill security tools being used. 2. Wireshark It is one of the most widely used network analyzer protocol. It assesses the vulnerable sections on the network upon which the user is working. Wireshark can gather or see the minutes of the detail and activities which are going on a network. The incoming and outgoing packets of data and the protocol which is being used in the transmission can be easily viewed. What it does is captures the live data and creates an offline analysis sheet, which helps in tracking. 3. Cryptostopper It is one of the best tools available online right now to [stop the ransomware](https://www.educba.com/ransomware-attack/) or [malware attacks](https://www.educba.com/what-is-malware/) on a system. What crypto stopper does is that it finds the bots which are encrypting the files and deletes them. It creates a pattern or a deception formula for the threat to latch it on by itself onto the formula, once it latches itself; crypto stopper detects and deletes that code. Cryptostopper makers tend to make a promise of a 9-second threat detection and elimination challenge. It isolates the workstation and the affected areas of the system so that the ransomware cannot manage to affect more and more areas. 4. N MAP It is one of the many primary and open source utilities made available for network securities. [NMAP is not only good](https://www.educba.com/what-is-nmap/) with small but large networks as well. It recognizes the hosts and the receiver on a network. Along with it, it also runs on all the distributions of operating systems. It can scan hundreds and thousands of machines on a network at a single moment. 5. Burp Suite It is another web scanning algorithm security tool, which helps to scan web-based applications. The main purpose of this tool is to check and penetrate the compromised system. It checks all the surfaces which might be affected along with the sender and destination’s requests and responses for the threat. If any threat is found, it can either be quarantined or can be eliminated. 6. OpenVAS A utility of Nessus, but very different from Nessus and Metasploit though they work the same, yet different. It is considered as one of the most stable, less loophole and use of web security tools available online at the moment.  **There are two major components of OpenVAS.**   1. **Scanner:** It scans the vulnerable sections and sends a compiled report of all of it to its manager. 2. **Manager:** It compiles all the requests which are received from the scanner and then it makes a report of all such incidences.  7. Nessus Nessus is yet another tool that checks for malicious hackers. It scans the computers on the network for unauthorized hackers who try to access the data from the internet. On average it is considered that Nessus scans for unauthorized access for 1200 times. Apart from others, it doesn’t make assumptions that certain ports are only set for web servers like Port 80 is set for Web Server only. And it is an open-source tool, which also provides a vulnerable patching assistance facility, which further helps in providing possible solutions for the affected areas. 8. Metasploit Framework Created by Rapid7 in Boston, Massachusetts. It is considered the best open-source framework which is in use for checking vulnerabilities. It has a command shell as it [runs in Unix](https://www.educba.com/what-is-unix/), so users can run their manual as well as auto commands to check and run the scripts. Metasploit Framework has some inbuilt as well as some third-party interfaces, which can be used to exploit the affected areas. 9. SolarWinds Mail Assure It is a multi-functional tool that addresses most of the email security concerns. It has data from almost 2 million domains, which comes from 85 countries. It is also offered as [Software As A Service (SAAS)](https://www.educba.com/what-is-software-as-a-service-saas/). It helps in the protection of the user’s devices from spams, viruses, phishing, and malware.  There are a lot many other online security tools available that can help in eliminating the risk along with the above-mentioned list. They are as follows:   1. Aircrack-ng 2. Touch Manager 3. MailControl  Types of Cyber Attacks A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.  We are living in a digital era. Now a day, most of the people use computer and internet. Due to the dependency on digital things, the illegal computer activity is growing and changing like any type of crime. Web-based attacks These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-  **1. Injection attacks**  It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.  **Example-** SQL Injection, code Injection, log Injection, XML Injection etc.  **2. DNS Spoofing**  DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker?s computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.  **3. Session Hijacking**  It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.  **4. Phishing**  Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.  **5. Brute force**  It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.  **6. Denial of Service**  It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-  **Volume-based attacks-** Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.  **Protocol attacks-** It consumes actual server resources, and is measured in a packet.  **Application layer attacks-** Its goal is to crash the web server and is measured in request per second.  **7. Dictionary attacks**  This type of attack stored the list of a commonly used password and validated them to get original password.  **8. URL Interpretation**  It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.  **9. File Inclusion attacks**  It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.  **10. Man in the middle attacks**  It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection. System-based attacks These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-  **1. Virus**  It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.  **2. Worm**  It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.  **3. Trojan horse**  It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.  **4. Backdoors**  It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.  **5. Bots**  A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots vulnerability assessment A vulnerability assessment process that is intended to identify threats and the risks they pose typically involves the use of automated testing tools, such as [network security scanners](https://searchsecurity.techtarget.com/definition/vulnerability-scanning), whose results are listed in a vulnerability assessment report.  Organizations of any size, or even individuals who face an increased risk of cyberattacks, can benefit from some form of vulnerability assessment, but large enterprises and other types of organizations that are subject to ongoing attacks will benefit most from vulnerability analysis.  Because security [vulnerabilities](https://whatis.techtarget.com/definition/vulnerability) can enable hackers to access IT systems and applications, it is essential for enterprises to identify and remediate weaknesses before they can be exploited. A comprehensive vulnerability assessment along with a management program can help companies improve the security of their systems. Importance of vulnerability assessments A vulnerability assessment provides an organization with information on the security weaknesses in its environment and provides direction on how to [assess the risks](https://searchcompliance.techtarget.com/definition/risk-assessment) associated with those weaknesses and evolving threats. This process offers the organization a better understanding of its assets, security flaws and overall risk, reducing the likelihood that a [cybercriminal](https://searchsecurity.techtarget.com/definition/cybercrime) will breach its systems and catch the business off guard. Types of vulnerability assessments Vulnerability assessments depend on discovering different types of system or network vulnerabilities, which means the assessment process includes using a variety of tools, scanners and methodologies to identify vulnerabilities, threats and risks.  Some of the different types of vulnerability assessment scans include the following:   * Network-based scans are used to identify possible network security attacks. This type of scan can also detect vulnerable systems on wired or wireless networks. * Host-based scans are used to locate and identify vulnerabilities in servers, workstations or other network hosts. This type of scan usually examines ports and services that may also be visible to network-based scans, but it offers greater visibility into the configuration settings and patch history of scanned systems. * Wireless network scans of an organization's Wi-Fi networks usually focus on points of attack in the wireless network infrastructure. In addition to identifying rogue [access points](https://searchmobilecomputing.techtarget.com/definition/access-point), a wireless network scan can also validate that a company's network is securely configured. * Application scans can be used to test websites in order to detect known software vulnerabilities and erroneous configurations in network or web applications. * Database scans can be used to identify the weak points in a database so as to prevent malicious attacks, such as [SQL injection attacks](https://searchsoftwarequality.techtarget.com/definition/SQL-injection).  Vulnerability assessments vs. penetration tests A vulnerability assessment often includes a penetration testing component to identify vulnerabilities in an organization's personnel, procedures or processes that might not be detectable with network or system scans. The process is sometimes referred to as vulnerability assessment/[penetration testing](https://searchsecurity.techtarget.com/definition/penetration-testing), or VAPT.  However, penetration testing is not sufficient as a complete vulnerability assessment and is, in fact, a separate process. A vulnerability assessment aims to uncover vulnerabilities in a network and recommend the appropriate mitigation or remediation to reduce or remove the risks.  A vulnerability assessment uses automated network security scanning tools. The results are listed in the vulnerability assessment report, which focuses on providing enterprises with a list of vulnerabilities that need to be fixed, without evaluating specific attack goals or scenarios.  Organizations should employ vulnerability testing on a regular basis to ensure the security of their networks, particularly when changes are made, e.g., services are added, new equipment is installed or ports are opened.  In contrast, penetration testing involves identifying vulnerabilities in a network, and it attempts to exploit them to attack the system. Although sometimes carried out in concert with vulnerability assessments, the primary aim of penetration testing is to check whether a vulnerability really exists and to prove that exploiting it can damage the application or network.  While a vulnerability assessment is usually automated to cover a wide variety of unpatched vulnerabilities, penetration testing generally combines automated and manual techniques to help testers delve further into the vulnerabilities and exploit them to gain access to the network in a controlled environment. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Date:** | | **20-06-2020** | **Name:** | **Karthik J** |  |
| **Course:** | | Introduction to Ethical Hacking- Great Learning | **USN:** | **4AL16EC030** |  |
| **Topic:** | |  | **Semester & Section:** | **8th A** |  |
|  | **AFTERNOON SESSION DETAILS** | | | | |
|  | Image of session    **Carrier Growth and Ladder in Cyber Security**  As per the 2018 HackerOne report, internet users are already facing over 166,000 registered hackers. [1] With stringent cyber laws, governments and various organizations are trying to make the internet a healthy place for its users. Now, the decision is yours, do you want to make a positive change in our world?  Ethical hackers are those professionals who choose hacking methods to serve a greater purpose in the world with a good intent to benefit others. This guide is for those:   * With basic or no knowledge of ethical hacking * With limited experience and waiting for an opportunity in ethical hacking   This guide will lead you through the beginner knowledge of ethical hacking, later acquiring expertise in the domain. One of the important requirements to become an ethical hacker would be your desire and intent to make a difference in the world.  If you want to try your hand at cybersecurity, then you must know that it is a vast industry with numerous domains such as application security, network security, and digital forensics which is sometimes further classified into other branches. So, you should be aware of your interest before you take your first step toward the industry. But if you have already made up your mind to become an ethical hacker, then stay with us. Reasons to Choose Ethical Hacking as Career Ethical hackers always have a handful of roles and responsibilities to deal with. An ethical hacker not only safeguards the data and network of an organization but is also responsible for taking preventive measures to avoid a security breach via penetration testing or any other method. It does possess a great career scope. And, the salary package is another fascinating aspect of it. However, if you are still unsure of pursuing ethical hacking as a career, then the listed reasons will serve as food for thought. 1. Scope for Career with Amazing Salary Trends The updated 2019 report by PayScale suggests the average salary of a certified ethical hacker is to be $90k. The top employers of these certified hackers include:   * Booz, Allen, and Hamilton * S. Army * S. Air Force * General Dynamics Information Technology Inc. [2]   The scope for this career route is broadening with each passing year. It has been evidently noticed that government agencies (military, law enforcement department, and national intelligence departments) and private organizations both are hiring cybersecurity experts, though IT firms are primary recruiters of ethical hackers, usually under the title of a penetration tester, security analyst, cybersecurity engineer, network security administrator, and a few others. Apart from that, service providers like airlines, hotels, and financial institutions are also hiring certified ethical hackers to protect their sensitive data. [2] 2. Growing Job Market for Certified Ethical Hackers Joblift, a UK-based job search platform, reported in 2018 that there are around 3240 job vacancies for ethical hackers. The report analyzed data for the past 24 months and declared that these job vacancies are increasing at an average of 4% per month. Another interesting calculation of the same platform mentions that 7 of every 10 job vacancies are looking for candidates with accredited credentials. [3] 3. Perfect Way to Enter Other Domains of Cybersecurity An ethical hacker possesses thorough knowledge of network security, application security, information security, and a lot more. There are organizations looking for professionals with specialized knowledge making it convenient for certified ethical hackers to take up other cybersecurity jobs, too, such as:   1. Network administrator/manager 2. Security investigator 3. Penetration tester 4. Web security administrator/manager 5. Data security analyst/specialist 6. Computer/digital forensics investigator 7. IT security administrator/consultant/manager 8. Network defense technicians   The list doesn’t end here. These are just a few of the professional profiles that an ethical hacker can easily fit into. Guide to Becoming Certified Ethical Hacker Follow the listed steps to establish yourself as a certified ethical hacker. Step 1—Understanding Ethical Hacking Ethical hacking can be defined as a simple approach of defending the system and network security of an organization by exploiting its existing vulnerabilities and weaknesses and strengthening them with appropriate countermeasures. Ethical hackers follow the same methods and techniques of a malicious hacker for finding vulnerabilities, which will later be fixed. Unlike black hat hackers, ethical hackers offer their services only when they are lawfully and legitimately employed to do so. These hired professionals report all their findings to the management board of the firm. Step 2—Skills Required to Start Your Career as an Ethical Hacker Pursuing a career in ethical hacking demands an ever-evolving attitude. You will be required to update your knowledge with the continuously changing trend. Plus, you need to have a sound technical knowledge of certain scripting or coding programming languages (such as HTML, JSP, ASP, C/C++, Java, Python, or any other strong computer language). You can consider these two points as the mandatory prerequisites for learning ethical hacking to the core.  The below-listed skills are revealed by Joblift in their survey of 2018.   * 70% job vacancies look for candidates holding accredited certifications * 25% of job vacancies are subjected to candidates with the knowledge of programming languages * 22% of job vacancies are meant for those candidates who can security check   Employers also look for soft skills, which include confidence, passion, communication skills, flexibility, and innovative nature of a candidate before hiring him/her as an ethical hacker. [3] Step 3—Ways to Acquire the Required Skills To acquire the required skills, you need to go through our three-step process to become a certified ethical hacker. Certified Network Defender An ethical hacker needs to have extensive knowledge of network security. You need to have a thorough understanding of how a network operates, various network security controls, protocols, topologies, intricate nature of network traffic, firewall configuration, vulnerability scanning of a network, and a lot more. For that deep understanding, EC-Council offers you a comprehensive skill-based program which is not only designed after intense job market research but is also recognized by the Department of Defense. This [Certified Network Defender program](https://www.eccouncil.org/programs/certified-network-defender-cnd/) will take you to a step closer to your target. Certified Ethical Hacker This is another important step in your journey. The [Certified Ethical Hacker (C|EH) program](https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/) will start by helping you learn the fundamentals of ethical hacking. Then gradually build concepts like footprinting, network scanning, system hacking, sniffing, session hijacking, web servers and web applications hacking, and many other major subject matters. This program always gets updated as per the market demand of the contemporary world. For instance, our updated C|EH program includes IoT hacking, cloud computing, vulnerability analysis, and much more. With that, to adapt professional ethical hacking skills, you will be exposed to real-time scenarios in a virtual environment. C|EH Practical [C|EH practical program](https://www.eccouncil.org/programs/certified-ethical-hacker-ceh-practical/) is designed to test your ethical hacking skills on every possible level. It is a 6-h practical exam which tests your ethical hacking techniques. This credential ensures that you have a detailed understanding of all the major aspects of ethical hacking. Other Important Tips1. Practice and Self-Learning You should understand the importance of practicing your gained technical knowledge and learning other trending ethical-hacking-related skills. The evolution of your knowledge is one of the most required steps that you need to take. You can do this by reading articles, watching videos, and interacting with experts. 2. Think Out of the Box Innovation is the key to stand out from the crowd. You need not follow the same path as other ethical hackers do. 3. Look for More Information All the information is just a click away. If you find some subject matter difficult or interesting, then try learning more about it. These days, the internet is the key to all your queries. | | | | |