**DAILY ASSESSMENT FORMAT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **18-06-2020** | **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**    **Addressing in Computer Networks**   * Network Addressing is one of the major responsibilities of the network layer. * Network addresses are always logical, i.e., software-based addresses. * A host is also known as end system that has one link to the network. The boundary between the host and link is known as an interface. Therefore, the host can have only one interface. * A router is different from the host in that it has two or more links that connect to it. When a router forwards the datagram, then it forwards the packet to one of the links. The boundary between the router and link is known as an interface, and the router can have multiple interfaces, one for each of its links. Each interface is capable of sending and receiving the IP packets, so IP requires each interface to have an address. * Each IP address is 32 bits long, and they are represented in the form of "dot-decimal notation" where each byte is written in the decimal form, and they are separated by the period. An IP address would look like 193.32.216.9 where 193 represents the decimal notation of first 8 bits of an address, 32 represents the decimal notation of second 8 bits of an address.  **Classful Addressing** An IP address is 32-bit long. An IP address is divided into sub-classes:   * Class A * Class B * Class C * Class D * Class E   **An ip address is divided into two parts:**   * **Network ID:** It represents the number of networks. * **Host ID:** It represents the number of hosts.  **IP address** An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a [computer network](https://en.wikipedia.org/wiki/Computer_network) that uses the [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) for communication. An IP address serves two main functions: host or network interface [identification](https://en.wikipedia.org/wiki/Identification_(information)) and location [addressing](https://en.wikipedia.org/wiki/Network_address).  [Internet Protocol version 4](https://en.wikipedia.org/wiki/IPv4) (IPv4) defines an IP address as a [32-bit](https://en.wikipedia.org/wiki/32-bit) number. However, because of the growth of the Internet and the [depletion of available IPv4 addresses](https://en.wikipedia.org/wiki/IPv4_address_exhaustion), a new version of IP ([IPv6](https://en.wikipedia.org/wiki/IPv6)), using 128 bits for the IP address, was standardized in 1998. [IPv6 deployment](https://en.wikipedia.org/wiki/IPv6_deployment) has been ongoing since the mid-2000s.  IP addresses are written and displayed in [human-readable](https://en.wikipedia.org/wiki/Human-readable) notations, such as 172.16.254.1 in IPv4, and 2001:db8:0:1234:0:567:8:1 in IPv6. The size of the routing prefix of the address is designated in [CIDR notation](https://en.wikipedia.org/wiki/CIDR_notation) by suffixing the address with the number of significant bits, e.g., 192.168.1.15/24, which is equivalent to the historically used subnet mask 255.255.255.0.  The IP address space is managed globally by the [Internet Assigned Numbers Authority](https://en.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority) (IANA), and by five [regional Internet registries](https://en.wikipedia.org/wiki/Regional_Internet_registry) (RIRs) responsible in their designated territories for assignment to [local Internet registries](https://en.wikipedia.org/wiki/Local_Internet_registry), such as [Internet service providers](https://en.wikipedia.org/wiki/Internet_service_providers), and other end users. IPv4 addresses were distributed by IANA to the RIRs in blocks of approximately 16.8 million addresses each, but have been exhausted at the IANA level since 2011. Only one of the RIRs still has a supply for local assignments in Africa. Some IPv4 addresses are reserved for [private networks](https://en.wikipedia.org/wiki/Private_network) and are not globally unique.  Network administrators assign an IP address to each device connected to a network. Such assignments may be on a static (fixed or permanent) or dynamic basis, depending on network practices and software features. **IP Classes** There are actually five different classes of IP networks, Class A, B, C, D and E. For the most part, Classes A - C is discussed for the purposes of designing networks. Class D is reserved for multicasting and Class E is reserved as experimental. Class D and Class E will not be covered in detail in this document. You should also note that the use of IP classes is now rarely used in practice. However, it is still important to understand this concept with respect to IP addressing and subnetting your network. With the introduction of classless inter-domain routing (CIDR), classes are no longer a critical factor in your network configuration. To determine which class an IP belongs to, you only have to look at the five high order bits. **Internet Protocol** The Internet Protocol (IP) is the principal [communications protocol](https://en.wikipedia.org/wiki/Communications_protocol) in the [Internet protocol suite](https://en.wikipedia.org/wiki/Internet_protocol_suite) for relaying [datagrams](https://en.wikipedia.org/wiki/Datagram) across network boundaries. Its [routing](https://en.wikipedia.org/wiki/Routing) function enables [internetworking](https://en.wikipedia.org/wiki/Internetworking), and essentially establishes the [Internet](https://en.wikipedia.org/wiki/Internet).  IP has the task of delivering [packets](https://en.wikipedia.org/wiki/Packet_(information_technology)) from the source [host](https://en.wikipedia.org/wiki/Host_(network)) to the destination host solely based on the [IP addresses](https://en.wikipedia.org/wiki/IP_address) in the packet [headers](https://en.wikipedia.org/wiki/Header_(computing)). For this purpose, IP defines packet structures that [encapsulate](https://en.wikipedia.org/wiki/Encapsulation_(networking)) the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information.  Historically, IP was the [connectionless](https://en.wikipedia.org/wiki/Connectionless_communication) datagram service in the original [Transmission Control Program](https://en.wikipedia.org/wiki/Transmission_Control_Program) introduced by [Vint Cerf](https://en.wikipedia.org/wiki/Vint_Cerf) and [Bob Kahn](https://en.wikipedia.org/wiki/Bob_Kahn) in 1974, which was complemented by a connection-oriented service that became the basis for the [Transmission Control Protocol](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) (TCP). The Internet protocol suite is therefore often referred to as TCP/IP.  The first major version of IP, [Internet Protocol Version 4](https://en.wikipedia.org/wiki/IPv4) (IPv4), is the dominant protocol of the Internet. Its successor is [Internet Protocol Version 6](https://en.wikipedia.org/wiki/IPv6) (IPv6), which has been in increasing [deployment](https://en.wikipedia.org/wiki/IPv6_deployment) on the public Internet since c. 2006. **Address Resolution Protocol** The Address Resolution Protocol (ARP) is a [communication protocol](https://en.wikipedia.org/wiki/Communication_protocol) used for discovering the [link layer](https://en.wikipedia.org/wiki/Link_layer) address, such as a [MAC address](https://en.wikipedia.org/wiki/MAC_address), associated with a given [internet layer](https://en.wikipedia.org/wiki/Internet_layer) address, typically an [IPv4 address](https://en.wikipedia.org/wiki/IPv4_address). This mapping is a critical function in the [Internet protocol suite](https://en.wikipedia.org/wiki/Internet_protocol_suite). ARP was defined in 1982 by [RFC](https://en.wikipedia.org/wiki/RFC_(identifier)) [826](https://tools.ietf.org/html/rfc826), which is [Internet Standard](https://en.wikipedia.org/wiki/Internet_Standard) STD 37.  ARP has been implemented with many combinations of network and data link layer technologies, such as [IPv4](https://en.wikipedia.org/wiki/IPv4), [Chaosnet](https://en.wikipedia.org/wiki/Chaosnet), [DECnet](https://en.wikipedia.org/wiki/DECnet) and Xerox [PARC Universal Packet](https://en.wikipedia.org/wiki/PARC_Universal_Packet) (PUP) using [IEEE 802](https://en.wikipedia.org/wiki/IEEE_802) standards, [FDDI](https://en.wikipedia.org/wiki/FDDI), [X.25](https://en.wikipedia.org/wiki/X.25), [Frame Relay](https://en.wikipedia.org/wiki/Frame_Relay) and [Asynchronous Transfer Mode](https://en.wikipedia.org/wiki/Asynchronous_Transfer_Mode) (ATM).  In [Internet Protocol Version 6](https://en.wikipedia.org/wiki/IPv6) (IPv6) networks, the functionality of ARP is provided by the [Neighbor Discovery Protocol](https://en.wikipedia.org/wiki/Neighbor_Discovery_Protocol) (NDP). |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Date:** | | **18-06-2020** | **Name:** | **Karthik J** |  |
| **Course:** | | Introduction to Ethical Hacking- Great Learning | **USN:** | **4AL16EC030** |  |
| **Topic:** | |  | **Semester & Section:** | **8th A** |  |
|  | **AFTERNOON SESSION DETAILS** | | | | |
|  | Image of session   **Introduction** The term ‘Hacker’ was coined in the 1960s at the Massachusetts Institute of Technology to describe experts who used their skills to re-develop mainframe systems, increasing their efficiency and allowing them to multi-task.  Nowadays, the term routinely describes skilled programmers who gain unauthorized access into computer systems by exploiting weaknesses or using bugs, motivated either by malice or mischief. For example, a hacker can create algorithms to crack passwords, penetrate networks, or even disrupt network services.  With the increased popularity of the Internet and E-Commerce, malicious hacking became the most commonly known form, an impression reinforced by its depiction in various forms of news media and entertainment. As a rule, the primary motive of malicious/unethical hacking involves stealing valuable information or financial gain.  That said, not all hacking is bad. This brings us to the second type of hacking: [Ethical hacking](https://www.simplilearn.com/cyber-security/ceh-certification). Ethical hackers are hired by organizations to look into the vulnerabilities of their systems and networks and develop solutions to prevent data breaches. Consider it a high-tech permutation of the old saying “It takes a thief to catch a thief.” **What is Ethical Hacking?** Ethical Hacking is an authorized practice of bypassing system security to identify potential data breaches and threats in a network. The company that owns the system or network allows [Cyber Security experts](https://www.simplilearn.com/cyber-security-expert-master-program-training-course) to perform such activities in order to test the system’s defenses. Thus, unlike malicious hacking, this process is planned, approved, and more importantly, legal.  [Ethical hackers](https://www.simplilearn.com/roles-of-ethical-hacker-article) aim to investigate the system or network for weak points that malicious hackers can exploit or destroy. They collect and analyze the information to figure out ways to strengthen the security of the system/network/applications. By doing so,  they can improve the security footprint so that it can better withstand attacks or divert them.  Ethical Hackers check for key vulnerabilities include but are not limited to:   * Injection attacks * Changes in security settings * Exposure of sensitive data * Breach in authentication protocols * Components used in the system or network that may be used as access points  **Importance of Ethical Hacking** [State-sponsored hacking](https://www.forbes.com/sites/zakdoffman/2019/08/10/state-sponsored-cyberattacks-challenge-the-very-concept-of-war-report/) is a way for governments to secure intelligence information about enemy states, influence politics, and more. In the era of international conflicts, the threat of cyber-terrorism, and terrorist groups funding cybercriminals, national security is continuously at risk.  Additionally, with the exponential rise of cybercrimes, agencies and businesses also need a way to counter the growing threat. Vulnerabilities in security leave the company systems susceptible to malware. Viruses, ransomware, worms, and malware are doubling in number, with the advancing technology, making ethical hacking a necessity.  Ethical hacking allows organizations to combat unauthorized access. As the hacker has no prior knowledge about the company other than what they are informed, it also provides an unbiased analysis of a company’s security architecture. Ethical hackers have to highlight loopholes in system security, test entry points, priority targets, and more. Furthermore, ethical hackers also devise strategies to safeguard sensitive information for companies, defense contractors, and government agencies.  **Ethical Hacking in Web Applications-Demonstration**  A web application is an application that is accessed by users over a network such as the Internet or an intranet. The term may also mean a computer software application that is coded in a browser-supported programming language (such as JavaScript, combined with a browser-rendered markup language like HTML) and reliant on a common web browser to render the application executable.   Web applications are popular due to the ubiquity of web browsers, and the convenience of using a web browser as a client. The ability to update and maintain web applications without distributing and installing software on potentially thousands of client computers is a key reason for their popularity, as is the inherent support for cross-platform compatibility. Common web applications include webmail, online retail sales, online auctions, wikis and many other functions.   Web hacking refers to exploitation of applications via HTTP which can be done by manipulating the application via its graphical web interface, tampering the Uniform Resource Identifier (URI) or tampering HTTP elements not contained in the URI. Methods that can be used to hack web applications are SQL Injection attacks, Cross Site Scripting (XSS), Cross Site Request Forgeries (CSRF), Insecure Communications, etc.   As an expert Ethical Hacker and Security Administrator, you need to test web applications for cross-site scripting vulnerabilities, cookie hijacking, command injection attacks, and secure web applications from such attacks. | | | | |