**DAILY ASSESSMENT FORMAT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **19-06-2020** | **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**   **Dynamic Host Configuration Protocol** The Dynamic Host Configuration Protocol (DHCP) is a [network management protocol](https://en.wikipedia.org/wiki/Network_protocol) used on [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) networks whereby a DHCP server dynamically assigns an [IP address](https://en.wikipedia.org/wiki/IP_address) and other network configuration parameters to each device on a network so they can communicate with other IP networks.[[1]](https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol#cite_note-TechTarget-1) A DHCP server enables computers to request IP addresses and networking parameters automatically from the [Internet service provider](https://en.wikipedia.org/wiki/Internet_service_provider) (ISP), reducing the need for a [network administrator](https://en.wikipedia.org/wiki/Network_administrator) or a user to manually assign IP addresses to all network devices. In the absence of a DHCP server, a computer or other device on the network needs to be manually assigned an IP address, or to assign itself an [APIPA](https://en.wikipedia.org/wiki/APIPA) address, which will not enable it to communicate outside its local subnet.  DHCP can be implemented on networks ranging in size from [home networks](https://en.wikipedia.org/wiki/Home_network) to large [campus networks](https://en.wikipedia.org/wiki/Campus_network) and regional [Internet service provider](https://en.wikipedia.org/wiki/Internet_service_provider) networks. A [router](https://en.wikipedia.org/wiki/Router_(computing)) or a [residential gateway](https://en.wikipedia.org/wiki/Residential_gateway) can be enabled to act as a DHCP server. Most residential network routers receive a globally unique IP address within the ISP network. Within a local network, a DHCP server assigns a local IP address to each device connected to the network.  [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) (IP) defines how devices communicate within and across local networks on the Internet. A DHCP server can manage IP settings for devices on its local network, e.g., by assigning IP addresses to those devices automatically and dynamically.  DHCP operates based on the [client–server model](https://en.wikipedia.org/wiki/Client%E2%80%93server_model). When a computer or other device connects to a network, the DHCP client software sends a DHCP [broadcast](https://en.wikipedia.org/wiki/Broadcasting_(computing)) query requesting the necessary information. Any DHCP server on the network may service the request. The DHCP server manages a pool of IP addresses and information about client configuration parameters such as [default gateway](https://en.wikipedia.org/wiki/Default_gateway), [domain name](https://en.wikipedia.org/wiki/Domain_name), the [name servers](https://en.wikipedia.org/wiki/Name_server), and [time servers](https://en.wikipedia.org/wiki/Time_server). On receiving a DHCP request, the DHCP server may respond with specific information for each client, as previously configured by an administrator, or with a specific address and any other information valid for the entire network and for the time period for which the allocation (lease) is valid. A DHCP client typically queries for this information immediately after [booting](https://en.wikipedia.org/wiki/Booting), and periodically thereafter before the expiration of the information. When a DHCP client refreshes an assignment, it initially requests the same parameter values, but the DHCP server may assign a new address based on the assignment policies set by administrators.  On large networks that consist of multiple links, a single DHCP server may service the entire network when aided by DHCP relay agents located on the interconnecting routers. Such agents relay messages between DHCP clients and DHCP servers located on different subnets. **ICMP (Internet Control Message Protocol)**  ICMP (Internet Control Message Protocol) is an error-reporting protocol network devices like routers use to generate error messages to the source IP address when network problems prevent delivery of IP packets. ICMP creates and sends messages to the source IP address indicating that a [gateway](https://internetofthingsagenda.techtarget.com/definition/gateway) to the Internet that a router, service or host cannot be reached for packet delivery. Any IP network device has the capability to send, receive or process ICMP messages.  ICMP is not a transport protocol that sends data between systems.  While ICMP is not used regularly in end-user applications, it is used by network administrators to troubleshoot Internet connections in diagnostic utilities including [ping](https://searchnetworking.techtarget.com/definition/ping) and [traceroute](https://whatis.techtarget.com/definition/traceroute).  One of the main protocols of the [Internet Protocol](https://searchunifiedcommunications.techtarget.com/definition/Internet-Protocol) suite, ICMP is used by routers, intermediary devices or hosts to communicate error information or updates to other routers, intermediary devices or hosts. The widely used IPv4 (Internet Protocol version 4) and the newer [IPv6](https://searchnetworking.techtarget.com/definition/IPv6-Internet-Protocol-Version-6) use similar versions of the ICMP protocol (ICMPv4 and ICMPv6, respectively).  ICMP messages are transmitted as [datagrams](https://searchnetworking.techtarget.com/definition/datagram) and consist of an IP header that encapsulates the ICMP data. ICMP packets are IP packets with ICMP in the IP data portion. ICMP messages also contain the entire IP header from the original message, so the end system knows which packet failed  The ICMP header appears after the IPv4 or IPv6 packet header and is identified as IP protocol number 1. The complex protocol contains three fields:   * The major type that identifies the ICMP message; * The minor code that contains  more information about the type field; and * The checksum that helps detect errors introduced during transmission.   Following the three fields is the ICMP data and the original IP header to identify which packets actually failed.  ICMP has been used to execute [denial-of-service](https://searchsecurity.techtarget.com/definition/denial-of-service) attacks (also called the [ping of death](https://searchsecurity.techtarget.com/definition/ping-of-death)) by sending an IP packet larger than the number of bytes allowed by the IP protocol. **What Is a Socket?** Normally, a server runs on a specific computer and has a socket that is bound to a specific port number. The server just waits, listening to the socket for a client to make a connection request.  On the client-side: The client knows the hostname of the machine on which the server is running and the port number on which the server is listening. To make a connection request, the client tries to rendezvous with the server on the server's machine and port. The client also needs to identify itself to the server so it binds to a local port number that it will use during this connection. This is usually assigned by the system.  A client's connection request  If everything goes well, the server accepts the connection. Upon acceptance, the server gets a new socket bound to the same local port and also has its remote endpoint set to the address and port of the client. It needs a new socket so that it can continue to listen to the original socket for connection requests while tending to the needs of the connected client.  The connection is made  On the client side, if the connection is accepted, a socket is successfully created and the client can use the socket to communicate with the server.  The client and server can now communicate by writing to or reading from their sockets. **File Transfer Protocol** The File Transfer Protocol (FTP) is a standard [network protocol](https://en.wikipedia.org/wiki/Network_protocol) used for the transfer of [computer files](https://en.wikipedia.org/wiki/Computer_file) between [a client and server](https://en.wikipedia.org/wiki/Client%E2%80%93server_model) on a [computer network](https://en.wikipedia.org/wiki/Computer_network).  FTP is built on a client-server model architecture using separate control and data connections between the client and the server.[[1]](https://en.wikipedia.org/wiki/File_Transfer_Protocol#cite_note-for-1) FTP users may authenticate themselves with a [clear-text](https://en.wikipedia.org/wiki/Clear_text) sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often [secured](https://en.wikipedia.org/wiki/File_Transfer_Protocol#Security) with [SSL/TLS](https://en.wikipedia.org/wiki/Transport_Layer_Security) ([FTPS](https://en.wikipedia.org/wiki/FTPS)) or replaced with [SSH File Transfer Protocol](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol) (SFTP).  The first FTP client applications were [command-line programs](https://en.wikipedia.org/wiki/Command-line_interface) developed before [operating systems](https://en.wikipedia.org/wiki/Operating_system) had [graphical user interfaces](https://en.wikipedia.org/wiki/Graphical_user_interface), and are still shipped with most [Windows](https://en.wikipedia.org/wiki/Windows), [Unix](https://en.wikipedia.org/wiki/Unix), and [Linux](https://en.wikipedia.org/wiki/Linux) operating systems.[[2]](https://en.wikipedia.org/wiki/File_Transfer_Protocol#cite_note-tcpip-2)[[3]](https://en.wikipedia.org/wiki/File_Transfer_Protocol#cite_note-net+-3) Many FTP clients and automation utilities have since been developed for [desktops](https://en.wikipedia.org/wiki/Desktop_computer), servers, mobile devices, and hardware, and FTP has been incorporated into productivity applications, such as [HTML editors](https://en.wikipedia.org/wiki/HTML_editor). **HTTPS** Hypertext Transfer Protocol Secure (HTTPS) is an extension of the [Hypertext Transfer Protocol](https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol) (HTTP). It is used for [secure communication](https://en.wikipedia.org/wiki/Secure_communications) over a [computer network](https://en.wikipedia.org/wiki/Network_operating_system), and is widely used on the Internet. In HTTPS, the [communication protocol](https://en.wikipedia.org/wiki/Communication_protocol) is encrypted using [Transport Layer Security](https://en.wikipedia.org/wiki/Transport_Layer_Security) (TLS) or, formerly, Secure Sockets Layer (SSL). The protocol is therefore also referred to as HTTP over TLS, or HTTP over SSL.  The principal motivations for HTTPS are [authentication](https://en.wikipedia.org/wiki/Authentication) of the accessed [website](https://en.wikipedia.org/wiki/Website), and protection of the [privacy](https://en.wikipedia.org/wiki/Information_privacy) and [integrity](https://en.wikipedia.org/wiki/Data_integrity) of the exchanged data while in transit. It protects against [man-in-the-middle attacks](https://en.wikipedia.org/wiki/Man-in-the-middle_attack), and the bidirectional [encryption](https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation) of communications between a client and server protects the communications against [eavesdropping](https://en.wikipedia.org/wiki/Eavesdropping) and [tampering](https://en.wikipedia.org/wiki/Tamper-evident#Tampering). In practice, this provides a reasonable assurance that one is communicating with the intended website without interference from attackers.  The authentication aspect of HTTPS requires a trusted third party to sign server-side [digital certificates](https://en.wikipedia.org/wiki/Public_key_certificate). This was historically an expensive operation, which meant fully authenticated HTTPS connections were usually found only on secured payment transaction services and other secured corporate information systems on the [World Wide Web](https://en.wikipedia.org/wiki/World_Wide_Web). In 2016, a campaign by the [Electronic Frontier Foundation](https://en.wikipedia.org/wiki/Electronic_Frontier_Foundation) with the support of web browser developers led to the protocol becoming more prevalent. HTTPS is now used more often by web users than the original non-secure HTTP, primarily to protect page authenticity on all types of websites; secure accounts; and to keep user communications, identity, and web browsing private. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Date:** | | **19-06-2020** | **Name:** | **Karthik J** |  |
| **Course:** | | Introduction to Ethical Hacking- Great Learning | **USN:** | **4AL16EC030** |  |
| **Topic:** | |  | **Semester & Section:** | **8th A** |  |
|  | **AFTERNOON SESSION DETAILS** | | | | |
|  | Image of session   **Ethical Hacking on Mobile platforms** A security professional who uses his/her hacking skills for defensive purposes is called an ethical hacker. To strengthen security, ethical hackers use their skills to find vulnerabilities, document them, and suggest ways to rectify them.  Companies that provide online services or those which are connected to the internet, must perform penetration testing by ethical hackers. Penetration testing is another name of ethical hacking. It can be performed manually or through an automation tool.  Ethical hackers work as an information security expert. They try to break the security of a computer system, network, or applications. They identify the weak points and based on that, they give advice or suggestions to strengthen the security.  Programming languages that are used for hacking include PHP, SQL, Python, Ruby, Bash, Perl, C, C++, Java, [VBScript](https://www.softwaretestinghelp.com/vbscript-tutorial-1/), Visual Basic, C Sharp, JavaScript, and HTML.  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.” **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. | | | | |