***Task 1 - Network Security***

**Introduction -**

This report will demonstrate an understanding of the fundamentals of Cloud Computing and its architectures. It will also analyse the evolution and fundamental concepts of Cloud Computing.

**Task - 1**

**Describe briefly each of the following security threats -**

**Adware**

Adware is any software application that shows commercial banners while the system is operating. Ads are distributed by pop-up windows or bars that display on the user interface of the application. Adware is usually produced for laptops, but it can also be used on mobile devices.

**Virus**

The computer infection may be a frame of pernicious code or computer program composed to alter the way a machine works and is planning to engender from one gadget to another. An infection works by including or interfacing itself to a substantial application or content that accepts macros in order to execute its code. Meanwhile , the infection has the potential to cause unintended or unfavorable results, such as hurting framework computer programs or undermining or erasing records.

**Worms**

The worm infection could be a damaging, self-replicating machine that can proliferate over the organism without human help. Worms dispense virus-like devastation, hack security computer program gaps and hypothetically take delicate data, degenerate information, and include back entryways for inaccessible get to the framework, among other issues.

**Spyware**

Spyware is malicious malware that infiltrates your machine, steals your Internet usage details, and extracts sensitive information. Spyware is known as a frame of malware — pernicious program expecting to enter or devastate your gadget, frequently without your mindfulness. Spyware captures and transmits the individual data to marketers, computer suppliers or other clients.

**Trojan**

A Trojan Horse or Trojan may be a frame of malware that's frequently utilized as true blue software. Trojans can be utilized by computer hoodlums and programmers attempting to pick up and get to buyer systems. Users are usually fooled by some form of social manipulation to load and operate Trojans on their computers. When enabled,Trojans will empower cyber hoodlums to spy on you, take touchy information, and get backdoor to get to your gadget.

**Rootkits**

Rootkit could be a noxious software that's exceptionally troublesome to identify and so exceptionally troublesome to expel. Stuxnet was one of the foremost popular and damaging rootkits in presence. This assaulted Iran's atomic locales, built by the US and Israel, and after that misplaced control of them.

**Logic bomb**

A logic bomb is a piece of code embedded into a software or software application that executes a destructive operation after a certain period of time or satisfies particular conditions.

**Botnets**

Botnets are the workhorse of the Internet. They're wired machines doing a variety of repetitive tasks to keep websites working. It is most widely used in conjunction with the Web Relay Chat. Such shapes of botnets are totally legitimate and indeed valuable for the conservation of client involvement on the Internet.

**Man-in-the-middle**

A guy-in - the-medium assault needs three groups. There's the culprit, the individual that the casualty is attempting to communicate with, and the "fellow within the middle" who's interfering with the victim's messages. Key to the circumstance is that the perpetrator isn't cognizant of the man within the center.

**DDoS**

A Disseminated Dissent of Benefit (DDoS) Attack is one of the foremost effective weapons on the Web. If you learn about an online site getting "brought down by programmers," it by and large implies that it has gotten to be a target of a DDoS attack. In brief, this infers that offenders have attempted to create a server or gadget blocked off by overpowering or collapsing websites with as well much activity.

**Spoofing**

Spoofing, as far as cybersecurity is concerned, is if someone or anything pretends to be something else in an effort to gain our confidence, gain entry to our databases, steal data, steal money, or spread ransomware. Spoofing attacks come in a variety of ways, in particular:

**Spam**

Spam is spontaneous spam email sent in bulk incidentally, frequently for commercial purposes. Much of it is sent to botnets, systems of virus-infected computers, which complicate the spammer checking operation. Agreeing to different gauges, around 80 percent of all emails within the world might be spam.

**Phishing**

Phishing is an effort of trying to deceive the receiver of a fraudulent email into opening and communicating with it. The author of the email misleads the user by having the email seem to be from a credible source, including a government agency, a retailer, or a company client.

**Spear phishing**

Spear Phishing: Like regular phishing emails, spear phishing emails involve a variety of variations. Whereas the conclusion objective is the same — to entice the beneficiary to tap on a pernicious URL or attachment— the sender customises the assault e-mail to incorporate the title, association, or portrayal of the casualty, or to incorporate the recipient's colleagues and trade associations.

**Pharming**

Pharming, the portmanteau of the terms "phishing" and "farming," is a method of cyber crime somewhat close to phishing, where information on the internet is exploited and private information is taken.

**Dumpster diving**

Dumpster Diving relates to the use of various methods to obtain information about a technology customer. In fact, dumpster diving means looking for something valuable by litter or waste. This is often achieved to discover valuable information that may help a person to gain access to a particular network.

**Tailgating**

Tailgating (often recognized as piggy backing) is among the most common security breaches currently affecting companies. Tailgating is often defined as the movement of unauthorised staff, either compelled or unintentional, behind existing customers.

**Impersonation**

Usually, an impersonation assault includes an email which seems to originate from a reliable source. Perhaps an email ambush will begin with a letter that looks like it's coming from a President, a CFO, or any other heavy-level official – such dangers are too called whale chasing e-mail assaults.

**Hoaxes**

Scams are for the most part chain letter design emails that regularly portray unordinary events, profoundly harming infections, or urban legends.

**Whaling**

A whaling assault may be a think endeavor to take touchy data from a trade, such as monetary data or individual data with respect to workers, regularly for malevolent reasons. A whaling attack is particularly focused on at best directors holding control of associations such as the Chairman, CFO, or other officials who have coordinated too touchy information.

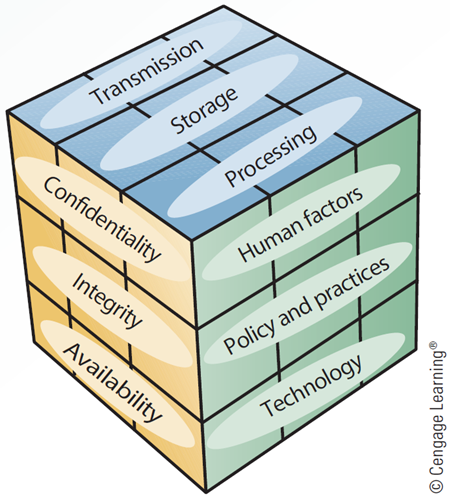
**Vishing**

Vishing. Phishing. Smishing, such words sound like a child made up and after that chosen to create the other two rhymes. However, as you likely as of now know (or will before long find), vishing, phishing, and smishing are exceptionally genuine and exceptionally genuine dangers to businesses and people alike.

**SQL injection**

SQL injection is a web security flaw that enables an intruder to interact with the requests an application creates to its database. Basically, it helps an intruder to access data that they are not usually able to retrieve. This may include data belonging to other applications or any other data that may be collected by the programme itself. In many instances, the intruder can alter or remove this data, creating permanent changes in the content or actions of the application.

**Write a report on how to minimise the impact of the above Malwares on CCL by conducting a detailed analysis of Network Security Principles using McCumber Cube - Cybersecurity Cube, involving all the technologies, devices, tools and techniques, to mitigate threats and implement a secure network.**



**John McCumber’s Framework for Evaluating Information Security for CCL**

Spoken to as a three-dimensional 3d shape Makes a difference security framework originators get it key issues to progress the viability of security measures Gives different states where points of interest may happen within the Installment, Capacity and Handling framework.

A strong security framework must give three levels of security Front-end servers: must be secured against unapproved get to Open to both inside and outside clients Back-end systems: must be kept up to preserve mystery, consistency and quality of information Corporate arrange: must be secured against obstructions, dissent of benefit assaults and unapproved access.

**Planning a Comprehensive Security System for CCL**

* **Fault-tolerant frameworks:** Guarantee accessibility within the occasion of a system disappointment by employing a combination of equipment and program.

**Methods that have been used:**

Uninterruptible power supply (UPS)

Redundant array of independent disks (RAID)

Mirror disks

**Biometric Security Measures for CCl**

* Utilize a physiological component one of a kind to an individual which cannot be stolen, misplaced, replicated, or passed on to others.

**Security Measures -**

* Facial acknowledgment, retinal filtering, and iris analysis ,fingerprints, palm prints, and hand geometry Signature analysis Vein analysis Voice recognition Vocal recognition Face acknowledgment, Eye check and iris analysing

**Nonbiometric Security Measures for CCL**

**Callback modems:**

Confirms whether a user’s get to is substantial by logging the client off and after that calling the client back at a foreordained number.

**Firewalls:**

* Combination of equipment and computer program that acts as a channel between a private arrange and outside systems.
* Network chairman characterizes rules for get to, and all other information transmissions are blocked
* Sorts: Packet-filtering firewalls, application-filtering firewalls, and intermediary servers

**Intrusion discovery systems**

Protect against outside and inside access Placed before a firewall Identify assault marks, follow designs, and produce cautions for the organize administrator Cause switches to end associations with suspicious sources Prevent DoS attacks

**Physical Security Measures for CCL**

Control get to to computers and networks Include gadgets for securing computers and peripherals from theft Cable shielding Corner bolts Electronic trackers Identification (ID) badges Proximity-release entryway openers Room shielding Steel encasements

**Access Controls for CCL**

Outlined to ensure frameworks from unauthorized get to in arrange to protect information integrity

**Types**

Terminal asset security: Eradicates the screen and signs the client off naturally after a indicated length of inactivity Passwords: Combination of numbers, characters, and images entered to permit get to to a framework

**Virtual Private Network (VPN)**

* Gives a secure section through the Web for transmitting messages and information through a private organization.
* Used so that inaccessible clients have a secure association to the organization’s arrangement. Information is scrambled some time recently it is sent with a convention such as:
* Layer Two Tunneling Protocol (L2TP)
* Internet Protocol Security (IPSec)

**Data Encryption**

* Changes information, called plaintext or cleartext, into a mixed frame called ciphertext which cannot be perused by others
* Rules for encryption: Decide how simple/complex the change handle is to be known as the encryption calculation

**Protocols which are used -**

* **Secure Sockets Layer (SSL):** Oversees transmission security on the Internet Transport Layer Security
* **Transport Layer Security (TLS):** Guarantees information security and astuteness over open networks
* **PKI (public key infrastructure)**

Enables users of a public network to securely and privately exchange data through the use of a pair of keys obtained from a trusted authority and shared through that authority

**Types of Data Encryption for CCL**

**Asymmetric**

Uses an open key known to everybody and a private or mystery key known as it were to the beneficiary known as open key encryption. Messages scrambled with an open key can be unscrambled as it were with the same calculation utilized by the open key and requires the recipient’s private key. Slow and requires a huge sum of handling power.

**Symmetric**

Same key is utilized to scramble and decode the message Known as mystery key encryption Sender and recipient must concur on the key and keep it secret Works superior with open systems, just like the Internet Sharing the key over the Web is difficult.

**Guidelines for a Comprehensive Security System for CCL**

* Organizations should understand the principles of the Sarbanes-Oxley Act of 2002
* Conduct a fundamental hazard investigation some time recently building up a security program
* Analysis makes utilize of monetary and budgeting techniques
* Information gotten makes a difference organizations weigh the taken a toll of a security system

**Summary -**

Dangers related with data advances can be minimized by introducing working framework overhauls frequently, utilizing antivirus and antispyware program, and utilizing mail security features Comprehensive security framework secures an organization’s assets, counting data, computer, and arrange equipment

**Discuss briefly a possible Network Security protocols that will enable a secure network for CCL’s London HQ, i.e. MD5, SSL, VPN, AES, SHA ½, RSA, DES, 3DES, IPSEc, DNS, HTTP, HTTPS, FTP, SMTP.**

**MD5**

MD5 (in fact called MD5 Message-Digest Calculation) could be a cryptographic hash work whose primary reason is to test that a record has not been altered. Rather than checking that two sets of information are comparative by dissecting the crude data, MD5 does this by producing a hash calculation on both sets and after that coordinating the secret word hashes to guarantee since they are the same.

**SSL**

SSL or Secure Sockets Layer is a Computer security mechanism focused on cryptography. It was first developed by Netscape in 1995 with the goal of preserving the protection, security and honesty of data in Internet communications. SSL is the precursor of today's digital TLS encryption.

**VPN**

Gives a secure entry through the Web for transmitting messages and information by means of a private arrangement. It is utilized so that inaccessible clients have a secure association to the organization’s arrangement. The information is scrambled some time recently it is sent with a convention such as:

Layer Two Tunneling Protocol (L2TP)

Internet Protocol Security (IPSec)

**AES**

The Advanced Encryption Standard (AES) is used to secure and encrypt data against unauthorized access. The encrypted process key of different lengths is used for this reason. Allocated AES-128, AES-192 or AES-256 based on the length.

**SHA ½**

SHA, or Secure Hash Calculation, may be a hashing calculation utilized in secure associations to appear the legitimacy and unwavering quality of a message to the beneficiary. The SHA calculation is the default hash calculation collection for SSL certificates.

**SHA-1 :** SHA-1 is a 160-bit fingerprint algorithm used on a file.

Until now, it was the standard for secure connexions. Nevertheless, SHA-1 was introduced in 1995, a long time ago on the Internet. Only think of the machine that you used in 1995! Since then, immense advancements in cryptographic technologies and innovations have put pressure on SHA-1 and have been shown to be unstable.

**SHA-2** : It may be a compilation of hash capacities that incorporate SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256. SHA-256 is the foremost common hash work utilized. For the most part talking, SHA-2= SHA-256. This works the same way as SHA-1, but it produces a longer unique mark when utilized on a record. Changing from SHA-1 to SHA-2 would make strides in online security and protection.

**RSA** :

RSA is a deviated plot, which guarantees that a key combination will be created (we'll see how before long), an open key and a private key will be made, and normally you'll keep your private key secure and switch around the open key.

**DES**

The Data Encryption Standard (DES) is a standard requirement for data encryption and private key cryptography (SKC) that requires only one key for encryption and decryption. Public Key Cryptography (PKC) utilises two keys, one is for encryption and another for decryption.

**3DES**

3DES is a cryptographic cypher originating from the original Data Cryptographic Standard (DES). It got to be prevalent at the conclusion of the nineties, but has since fallen out of support due to the rise of more effective calculations.

**IPSEc**

IPsec (Web security) may be an arrangement of conventions outlined to guarantee the security, privacy and verification of client communications over an IP arrangement. While the simplicity of the IPsec specifications has gained the attention of the commercial sector, due to their sophistication, this same versatility has culminated in the discovery of several protocol concerns.

**DNS**

The Domain Name System replaces the names of the domains with their corresponding IP addresses, bringing flexibility and even protection to the operation. The Domain Name Network is one of the columns of the Web, however most clients' fair exterior of the arrangement really do not know they're utilizing it each day to perform their careers, examine their emails or squander more time on their smartphones.

**HTTP**

HTTP (HyperText Transfer Protocol) is a set of rules that a website will obey when it comes to transferring data (images, pictures, audio, and other types of information) through the World Wide Web (WWW). As a user opens a tab, HTTP is already being used. It is essentially a network interface that passes through the top of the TCP / IP protocol set.

**HTTPS**

HTTPS (HyperText Transfer Protocol Secure) is a more secure variant of the standard HTTP that your average website utilises for connecting via multiple websites. When a user links to a website that uses HTTP, the client checks the IP address of the originating server that refers directly to that of the website, allowing the user to link to the IP address.

**FTP**

FTP is a Record Exchange Convention. In fairness, FTP is being utilized to exchange information to your computer. You certainly utilized FTP some time recently, indeed in the event that you didn't figure it out. In spite of the fact that you downloaded anything from the Web, counting a modern form of a program, you will have utilized FTP to do so.

**SMTP**

SMTP is a portion of the TCP / IP convention application layer. Employing a handle called "enlist and forward," SMTP exchanges the mail to and from an array. This works closely with something called the Mail Exchange Specialist (MTA) to transfer the contact to the proper gadget and email inbox. SMTP focuses out and guides how the e-mail voyages from the MTA of your machine to the MTA of another gadget, and indeed a number of computers. Utilizing the "store and forward" work depicted over, a message will travel from your gadget to its target in stages.

**Compare and contrast how transport layer protocols: DHCP and Telnet protocols can support communications across data networks in CCL.**

**Transport layer protocols: DHCP and Telnet protocols comparison**

**What is DHCP ?**

DHCP stands for energetic have arrangement convention and could be an organized convention utilized on IP systems where the DHCP framework powerfully allocates an IP address as well as other subtle elements to each have on both the arrange so that they can be associated effectively with other datasets.

In connection to the IP address, DHCP regularly gives a subnet veil, default door username, space title server (DNS) address and other related setup details. Requests for feedback (RFC) 2131 and 2132 describe DHCP as an Internet Technology Task Force (IETF)–a specification specified by the BOOTP protocol.

**Components of DHCP**

It is necessary to recognise all the components while dealing with DHCP. Here is a sample of them and what they're doing:

**DHCP server:** A networked system operating a DHCP service that contains IP addresses and related configuration details. This can be most usually a server or switch, but can be anything that serves as a have, such as an SD-WAN gadget.

**DHCP client:** endpoint which receives configuration details from a DHCP server. It may be a computer, a handheld device, an IoT endpoint, or something else that needs network connectivity. Many of them are designed to collect DHCP information by default.

**IP address pool:** the set of addresses open to DHCP users. Addresses are typically chronologically assigned from just the lowest to the largest.

**Subnet:** IP networks may be partitioned into modules identified as subnets. Subnets help create stable networks.

**Contract:** The length of the IP address information held by the DHCP application. When the lease expires, the company will extend the agreement.

**DHCP relay:** A switch or have that tunes into the client messages being transmitted on the organiser and after that passes them to an indicated hub. The server then sends the response back to the relay agent who forwards it to the device. It can be utilized to centralise DHCP servers rather than giving a space on each subnet.

**Benefits of DHCP servers**

**Correct IP setup:** The arrangement determinations of the IP address must be rectify and it is simple to form a botch whereas working with inputs such as "192.168.159.3."Typographic botches are ordinarily exceptionally troublesome to troubleshoot and the utilize of a DHCP server limits this possibility.

**Reduced IP Address Conflict:** Every connected device must have an IP address. Whereas, each address can as it were be utilized once and a rehash address can result in an issue where one or more gadgets can not be connected. This could happen when addresses are apportioned physically, especially when there are a huge number of endpoints that as it were connected routinely, such as versatile gadgets.

**Administration of IP address automation:** Without DHCP, organized chairmen would have to physically apportion and erase keys. Keep track of which framework has what address can be and work out in worthlessness, because it is nearly outlandish to get it which gadgets require to get to the organization and when they exit.

**Efficient change management:** using DHCP makes it very easy to alter urls, scopes or endpoints. For starters, a company may want to shift its IP address scheme from one set to another. The DHCP system is updated with new information and the knowledge is propagated to other endpoints.

**DHCP poses security risks in CCL**

The DHCP protocol does not require verification so that any client may access the network easily. It brings up a number of security dangers, counting unapproved servers sending terrible data to clients, unapproved clients collecting IP addresses, and IP address corruption by unapproved or malevolent clients.

Since the client has no way to approve the legitimacy of the DHCP benefit, the ruddy servers can be utilized to supply wrong arrangement data. This may trigger delusion-of-service assaults or man-in - the-medium assaults where an untrue server mediation information which can be utilized for noxious purposes.

**What is Telnet Protocol**

Telnet, created in 1969, may be a convention that provides a command line interface for inaccessible gadget or server communication, in some cases utilized for farther administration, but moreover for introductory framework setups such as arrange equipment. Telnet stands for Print Network, but can moreover be utilized as a verb;' to telnet' is to set up an association utilizing the Telnet convention.

**Security of Telnet in CCL**

Since it was set up some time recently the far reaching selection of the Net, Telnet does not utilize any shape of encryption on its possessor, rendering it excess in terms of advanced innovation. It is generally covered with the Secure Shell (SSH) standard, at slightest on the open Web, but in circumstances where Telnet is still in use, there are some ways to secure the communications.

**How does Telnet work compared to DHCP**

Since it was set up some time recently the far reaching selection of the Internet, Telnet does not utilize any frame of encryption on its claim, rendering it excess in terms of cutting edge innovation. It is generally covered with the Secure Shell (SSH) standard, at slightest on the open Web, but in circumstances where Telnet is still in use, there are some ways to secure the communications.

The buyer interfaces to the server utilizing the Telnet interface, which includes getting to the Telnet command incite utilizing the taking after sentence structure: telnet hostname interface. The shopper at that point performs commands on the computer utilizing distinctive Telnet commands on the Telnet ask. The chairman ends the Telnet arrangement through Telnet to cancel the association and sign off.

**What are the common methods of Telnet in CCL**

Telnet can be utilized to check or troubleshoot farther location or mail servers, as well as farther get to MUDs (multi-user cell recreations) and secure inside networks.

For many years, the telnet software has been the popular application to link to a remote server. Nevertheless,it sends decoded information, and SSH (Secure Shell) has nearly completely supplanted telnet as the favored strategy over interfacing to farther servers.

**USING TELNET TO TROUBLESHOOT**

To utilize telnet to troubleshoot an arrange program, you would like to know at slightest two things: the name of the remote server or the IP address. The port number for the network programme that you want to check. If you're only checking simple access to a single network programme, that's all you need to learn. However, if you want to do more in-depth tests, you will need to know the specific commands for the application you want to check (e.g. HTTP or SMTP).

**What are block and stream ciphers? What are the differences, and when would you use one vs. the other?**

**What is a Block Cipher ?**

The fundamental thought of a piece figure is to break content into generally huge pieces, ordinarily 64 or 128 bits long, and scramble each square independently. The same encryption key is utilized for each piece and is the encryption key that indicates the arrangement in which substitution, transport and other cryptographic capacities are performed on each square. Solid

calculations suggest that the turn around building of the figure, or the assurance of which capacities were executed on each push, in which arrange, is for all intents and purposes impossible.

**What is a Stream Cipher ?**

The fundamental thought of a stream figure is to isolate content into little pieces, one bit or one byte long, and scramble each square, based on a number of past squares. Stream figures utilize a partitioned encryption key— a number that must be embedded into an algorithm— for each bit or byte, so that the same bit or byte creates a modern cryptographic content each time it is scrambled. A few stream figures utilize a keystream generator that produces an arbitrary or nearly arbitrary stream of bits. The figure executes a Boolean work, known as an elite OR, between the keystream bits and the ciphertext bits.

**What is the difference between Block Cipher and stream Ciphers ?**

The most contrast between the square figure and the stream figure is that the piece figure changes plaintext to ciphertext by taking the plain content component at a time. In spite of the fact that stream figure Changes plaintext to ciphertext by taking 1 byte of plain content at a time.

|  |  |  |
| --- | --- | --- |
| **S.No** | **Block Cipher** | **Stream Cipher** |
| **1.** | Block Cipher Converts plain text to ciphertext by taking a block of plain text at a time. | Stream Cipher Changes over plain content to ciphertext by taking 1 byte of plain content at a time. |
| **2.** | Block cypher needs 64 bits or more than it. | While the stream cypher is using 8 bits. |
| **3.** | The difficulty of the block cypher is very basic. | While the flow cypher is more complex. |
| **4.** | Block cypher Uses both ambiguity and diffusion. | While the stream cypher only uses confusion. |
| **5.** | Reversing encrypted text in the block cypher is hard. | Reverse encrypted text is easy while in stream cypher. |
| **6.** | The algorithm modes used in the message cypher are: ECB (Electronic Code Book) and CBC (Cipher Message Chaining). | The algorithm modes used in stream cyphers are: CFB (Cipher Feedback) and OFB (Output Feedback). |

**Pros and Cons of both Block and Stream Ciphers**

The reality that stream figures scramble and decode information one bit at a time implies that they are especially suited to real-time equipment applications, such as sound and video applications. Stream figures are weaker and less effective than piece figures when it comes to program applications and are less regularly utilized in this field. Square figures are less demanding to actualize in applications as they scramble information in chains of length that are as of now utilized by the program. The encryption key is regularly of the same length as the square estimate.

**Conclusion -**

In conclusion, this report demonstrates an understanding of the fundamentals of Cloud Computing and its architectures. It will also analyse the evolution and fundamental concepts of Cloud Computing. It discusses the different types of Network Security devices and examines Network Security Protocols. Compare and contrast at least two major Network Security Protocols. It also discusses, using examples, the importance of Network Security.

Anon, (2020). [online] Available at: https://www.techwalla.com/articles/what-is-the-difference-between-stream-ciphers-block-ciphers [Accessed 23 Feb. 2020].

Kerravala, Z. (2020). DHCP defined and how it works. [online] Network World. Available at: https://www.networkworld.com/article/3299438/dhcp-defined-and-how-it-works.html [Accessed 23 Feb. 2020].

Anon, (2020). [online] Available at: https://swansoftwaresolutions.com/the-three-dimensions-of-the-cybersecurity-cube/ [Accessed 23 Feb. 2020].