Name:Ravindra roll.no:48 reg.no.: 11708826

EVEN ROLL NUMBER

QUESTION: 01

Worms:

A worm is a kind of standalone malware that replicate itself and doesn't need the host program to function. It can create multiple copy of itself and can do exponential damage to the systems. A worm once created will continue affecting the system and network by replicating itself.

Means of spreading:

Worms can spread and can reach the host system of computers in a number of ways. For example it can be installed by getting into the system through the email spams. This method involves human to activate the worm by clicking the spam email. This method is known as "*invocation by human intervention*". The worm can be infiltrated into our system during the boot period. It can be even send through the DMs and then once opened to be read they will be installed in our system.

Some detailed spreading ways:

Emails: emails are one of the basic ways in which the worms can be installed in our systems. Earlier the worms were embedded inside the text but soon the users started to decrypt the worms hence a new method came into practice to spread it. Nowadays the worms are embedded in form of links or any kind of attachments or images which might look benign but once they are clicked. The worms can get installed and they themselves start replying to the request emails and they even can replicate to the address books known to our email.

O.S Vulnerabilities: the O.S have some vulnerabilities in them even the Mac OS have vulnerabilities. The worms exploit these weak points to enter into the system and cause damage to the system. A worm named **Conficker** wreaked havoc to the windows users when it exploited the Server vulnerabilities and entered into the system. It affected around 15 million of the systems.

Instant Messaging: the worms can be sent to our systems using the DMs and once they enter our system and we clicked on them they start installing themselves and once installed they can replicate and can cause havoc to the system.

Phones: there are almost equal numbers of mobile users in the world as the world population. The worms attackers have sifted their focus on the mobiles phones. All mobile phones support the HTML5 in which the worms can be easily embedded and hence when opening a web address that support HTML5 we may be exploring the worms and which may get installed in our systems.

Explanation:

Every day we receive a lot of unsolicited emails. These emails because we have some sense of security from the google we never reach that part of such emails but it doesn't means we cannot reach them or we have become completely prone to them. We have a spam folder in our mails where these emails get stored. If we reach these spam emails and try to open it. There is high possibility that they may contain some worms or such malicious codes that can infect our system. These code once opened may get installed in our system by asking us visit to some websites or clicking a particular link hence. Then these such worms once entered our system may create a number of replicas and infect our entire system. They even will start sending

self-emails to the record or our contact emails we have in our emails. Hence we need to be very cautious while opening such links.

Ways of preventing our System from worms:

1. Regular software updates since the updates include security patches to prevent the system or software from various malware or the worms. The windows or the Mac OS roll out various updates to prevent the system from the malware. We need to make ourselves adopt to the latest version of the software to prevent any kind of bugs.
2. Phishing is another popular method of spread of the worms be always extra cautious while working or opening the unsolicited emails. The spam emails have become the most common feature to install various worms in our systems.
3. We should keep the best and strong internet security software while exploring the internet.
4. Always be cautious while clicking the links on social media and other related platforms.
5. Always keep a personal firewall while visiting other or unknown networks since most of the worms or such attacks are carried out when we visit the unknown networks.
6. Never provide the end users the administrator privileges because once the worms enter the administrative mode it will infect the whole system and all the related system to it too.
7. Disable the auto run in the system. While sharing network files the worms may enter our system with being embedded in the autorun.inf and may get installed when they enter into our system.
8. Deploy network access protection[NAP]

QUESTION 2:

Social engineering attacks are the attacks in which the attacker uses the human vulnerabilities instead of the system vulnerabilities to gain access and information about the user. Such attacks are being more common nowadays since the hackers are becoming more sophisticated they are creating all such emails that become very different to recognize and separate them from the solicited emails. The hackers are using human vulnerabilities like fear, anxiety and other such feelings to gain access

Ways of getting passwords of the user:

Spear phishing: in this method the attacker has pre-hand knowledge about some user example. The attacker knows the insurance the user has invested in. The bank name the user is having account. The company in which the user works.

Now suppose the attacker send a email to the user pretending to be the company email. He know the company email and has tailored it such that it seems to be coming from the company official. The attackers have become so advance that we cannot tell whether the email is from the official or some illicit hacker. Suppose they sent a email with the heading that the person need to make a urgent project and get the further info by clicking the following link. The person may click because it seem a legit email but the email address contains such small differences that it become almost impossible to detect in first go and once the person sees the email. In haste of urgency he will surely click on the link and once clicked he will be directed to website that look almost similar to the original company website. But the website is a personification of the original one. He may enter the username and password which will be stored in the hacker database.

Another way

QUID PRO QUO: the social engineering hacker may impersonate as the head of the company or any such head we may a sense of fear or respect for the person. Once the person will have taken us into the confidence that he or she is the same person he want us to think we are.

Once we are into his confidence he may ask us to log in to some website. Suppose he act as our boss and have taken us into confidence. Once our boss ask us to do any login we will very easily and if he asks to login to the particular website with our official email and we logged in. The user id and password will be received by the dubious person.

ATTACK DIFFERENCE ADMINSITRATOR'S ASSISTANT VS DATA ENTRY CLERK

To attack a administrator assistant the person need to have some access or some user level so that the hacker can dupe as the user and ask for some privilege to complete some actions and hence in turn can gain the access.

Suppose the person act as the user and ask for the administrative privilege since the hacker is acting as the user. We are supposing that the hacker has already gained access to the user level. He may then ask the administrative assistant to provide the administrative privilege to install some software into the system since the assistant now is in confidence that he is a legit user. He may try to provide the privilege and in turn may compromise his or password.

Attacking a data-entry clerk is way easier than attacking a administrative assistant. To attack the data entry he may create the website which look almost similar to the official ones and then dupe the user to login to the account acting as some superior who is asking to do the login. Or he may do the other thing around to call and pretend to be the superior and hence once taken into confidence he or she may provide all the info since he now have understood that the person asking info is the legit user.

For such things the attacker need to be smart and should have some kind of info although the info if small then also the hacker if expert can use it well to dupe the person.

In case of the administrative assistant duping the person can act as the novice and even can in-act to know nothing and hence the assistant will try to help the person to use the system by entering the guest password and once the hacker has gained access to the guest password it becomes very easy for him to gain the further access

QUESTION 3:

CIA is the acronym for the term Confidentiality, Integrity and Availability. For a network designer it is very important to follow the triad while designing the networks for data inflow and outflow. Since the data is the prime and the most important thing in the whole it world. Its safety and secure delivery is the prima. To make the delivery of the data safe and secure the CIA triad has been developed to cope with the security issues.

CONFIDENTIALITY: the data which is transferred over the networks need to be confidential and only accessible to the designated or the intended user. For this a lot of safety method and channels have been designed to deliver the data.

First of all suppose I am designing a network project of a social media account. For the social media, every user who signs up for the website need to be well authenticated to access his or her account For that nowadays in the practice of **two-factor authentication** has become norm in which the user enter the username and password. Since these two are pretty old signing in method, hackers have developed ways to crack it or if the password or the username has been compromised a extra layer of security in term of two way authentication has come in rescue. In which the user either need to enter **something he knows, something he possess or something he is**. This enhances the security since if one thing has been compromised the other thing may not.

=>For the sensitive files transfer they need to be encrypted and the decryption key or the software has to be possessed by the user so that on receiving only the data can be decrypted by the intended user. Usually the router may be compromised while in between but once the data is encrypted using some key which is known only to the user they can't be decrypted by unauthorized user.

=>If I am designing the network I need to focus on disposing the data once it is out of use or the user need to dispose the data once it is out of use. Since the data may be on longer use for the user but if it went into wrong hands then it may be used by the unintended user to gain unfair advantage.

=>The encryption key for the data transfer need to be changed on regular basis so that if the data is compromised once then also the key become useless after a certain period of time. Which would insure that if a part of data has been compromised then from henceforth the remaining data need to be safe.

=>The data once received by the user need to be backup well. The natural disaster plays a significant role in loss of data once we have backup for the data I will be safe and secure.

=> A lot of theft take place through the unsafe wifi. The wifi need to be safe and secure and encrypted since once the person logged in the wifi, it gives a huge loop to the hacker to use this to his own advantage.

=> A strong firewall need to be in place to make the network safe and secure. The firewall need to be updated on regular basis to keep it well protected. The firewall plays an important role in keeping the data safe and secure.

INTEGRITY: the data's integrity is very important. Suppose we take a simple example we send a message to our boss that some lower senior employee who is made to administer us is pestering us through unfair means. If this message get passed to the lower senior employee then what inferno fire it will unwrap.

This simple example was to state the fact that it is very important that the data we pass doesn't get hacked, robbed, or changed in between since it would mean the data has been compromised.

For the integrity of the data it need to be well encrypted before transferring the file. The encryption is a very important method to be followed while transferring sensitive data over the internet.

The file being transferred need to be enabled with version control which will signal us whether the data has been compromised in between.

It's not necessary that the integrity of the data is compromised by the hackers only there are other means too like human error, some unintended transfer errors, misconfigurations and security errors, malware, insider-threat and cyber attacks and compromised hardware.

- ⇨ The data should be traceable which means the transfer, storage and retrieval of data process should be well aware with the client whose data is being used or whose data is being stored.
- ⇨ The storage facility or the database which is being used to store the data need to reliable one. Nowadays the cloud services are the best places and they provide with the storage services. They are more safer and provide a lot of security layer for strong the data in comparison to the primary data storage devices whose database has been built a long time ago and no update to their security has been done.
- ⇨ The client data need to audited on a regular basis since the data can be compromised once stored. If the data is audited on regular basis then we can keep it safe from the unwanted attacks.
- ⇨ The access control too plays an important role in keeping the integrity of the data maintained. If the data maintains integrity then it surely will attract the new clients to our software to use it.

AVAILABILITY : The data availability is guarantee to the safe and reliable transfer or the access of the data by the authorized user only.

For maintaining the availability of the data the data transfer network need to well up to date. The network should be well assessed to prevent it from any kind of trozan or virus intentionally implanted in between to detect the data in between to use it by the hackers.

The bandwith of the data delivery should be so that the data required at the pace could be served well. The speed has become one of the factors that clients are focusing to use the networks for data delivery since time is said to be money in the corporate world.

Natural disaster plays a significant role to harm the delivery of timely data. In such tough times alternate delivery path should be prepared pre-hand to safeguard the data delivery and ensure timely delivery of the data.

In case if the data has been compromised by denial of service attacks. The security mechanism should be so prepared that the data should be made available from some other port or network and instant repair could be placed to repair the damaged network.