IS -2109

Practical 01

W.H.M.Gunathilaka
18020275

Question 1

1.

- Redirects and Pop up Ads
- Spam
- Virus
- Worms
- Spyware
- Keyloggers
- Pharming
- Adware
- Trojan
- Rogue Security Software

2.

- As the first line of defence, users should be educated to not open unknown attachments, which are a common source of viruses and spyware, and to be very cautious about clicking on any links
- Using Anti-virus/anti-spyware
- Enabling Firewall
- Spam-Download spam filtering tools and anti-virus software
- Authentications
- Use an ad blocker-Adware
- Encryption
- Create a strong password for home Internet-pharming

3.

- Using Anti-virus/anti-spyware

  Anti-virus systems should be behaviour-based and updated automatically in the background. Many anti-virus solutions also incorporate anti-spyware elements, to help cope with problems such as the theft of usernames and passwords. Suppliers include Kaspersky Lab, VIPRE Business, Norton, McAfee and Symantec. Anti-spyware suppliers include Barracuda Networks and WebRoot. Free anti-spyware solutions, such as Spybot, are also available.

- Enabling Firewall

  Enabling firewalls will make the user secure when browsing the Internet. All messages entering or leaving the network pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. This will secure the information that interchanges with outside users.

- Downloading spam filtering tools and anti-virus Software

  Spam filtering tools and anti-virus software can help to scan the emails that you received for malware. If the emails that you received contain malware, the malicious content would be

quarantined and you would be prevented from opening it. This helps to alleviate the chance of emails containing malware from infecting your computer. As such, do select spam filtering tools and anti-virus software with such features to reduce your woes of having to decipher email contents.

- Authentication

  Unauthorized accesses can be prevented through authentication. Single authentication means the use of only the password. These passwords can be easily predicted by a good hacker. And also using the same password for many applications is a highly risky activity.

  Two-factor authentication is the use of the password and something unique at the same time. This unique thing can be a one time password, PIN sent to a mobile number or swipe card. This is a good way to be secure while browsing the internet.

  Biometric authentication, also a good way of authentication, involving personal elements such as fingerprint or iris recognition, is more appropriate for high-security applications, such as financial or defence.

- Use an ad blocker-Adware

  Adware issues of web browsing can be prevented by using an add blocker.The original AdBlock for Chrome works automatically. Choose to continue seeing unobtrusive ads, whitelist favourite sites, or block all ads by default. Just click "Add to Chrome," then visit your favorite website and see the ads disappear.

- Encryption

  The easiest and most effective way of stopping sensitive and critical data being read by unauthorized personnel or outsiders is to encrypt it.

  Encryption is the process of converting the original representation of the information, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information.

  Some popular encryption softwares are Axcrypt, CryptoExpert and Veracrypt

- Create a strong password for home Internet.

  To protect against pharming, it is good to use a strong password for the home internet.Don’t use the default password written on the bottom of your router. This shows how to protect home networks against local DNS poisoning. If we have trouble remembering the password, it is good to use a passphrase instead. A passphrase is a string of nonsense words that are easy for a human to remember, but nearly impossible to brute force using a password cracking application. Unlike a conventional long and strong password, there’s no uppercase/lowercase mixing or special symbols.

Question 2

1. History is one of the features found in all web browsers, it's also called Browsing History. Addresses of recently visited websites and data associated with those websites will be recorded by History. This will help to load the website faster when we visit the website again. You can specify the number of days for which the list of history is maintained. It will also help to revisit the website in case we forgot the previously visited websites.

2. When we visit a website for the first time, browsers will take pieces of a particular web page and store them in the computer hard drive. Browser cache are known as Static assets that means parts of a website that do not change from visit to visit. The Intention behind saving these data is to help with bandwidth so when we visit the same page for next time it won't take much time because it has already been saved in the cache.

3. When we are visiting web sites web servers will send messages to our web browsers and our browser will store those messages in a small file called cookie.txt.These messages sent by web browsers are known as Cookies. Cookies only contain bits of text, this text can be userID , sessionID or any other text. If you clear your cookies, you'll be logged out of all websites and websites won't remember any settings you've changed on them. There are types of cookies: Magic Cookies and HTTP Cookies.

4. The main purpose of a cookie is to identify users and possibly prepare customized Web pages or to save site login information for you.

5. Session hijacking is an attack where a user session is taken over by an attacker. A session starts when you log into a service, for example your banking application, and ends when you log out. The attack relies on the attacker's knowledge of your session cookie, so it is also called cookie hijacking or cookie side-jacking. Although any computer session could be hijacked, session hijacking most commonly applies to browser sessions and web applications.

   Cookie theft occurs when a third party copies unencrypted session data and uses it to impersonate the real user. Cookie theft most often occurs when a user accesses trusted sites over an unprotected or public Wi-Fi network. Although the username and password for a given site will be encrypted, the session data traveling back and forth (the cookie) is not.

6.

i.

- SIDCC
- SAPISID
- SID
- APISID
- HSID
- PREF

ii. On 2022-07-26 at 12:52:23 UTC time

iii.

- HSID
- SSID
- YSC

iv. 1

v. Video View Set to Normal View Mode

Question 3

1. We must be aware of viruses. When downloading files directly from the web, we're exposing our devices to viruses. Also, it can be observed that most files that need to be downloaded are free and surely, it'll have a high cost as transforming your machine into a device full of viruses.

   Trying to download from unknown and unfamiliar websites can put your own identity and the computer's identity to stake. This could also include activities like monitoring your activities on the internet, grabbing your personal information and crashing your device on a whole. This spyware can allow predators and hackers to access any amount of details from your device and even track your activities on a real-time basis.

   Another issue is adware where unintended advertising can be attacked on a specific person. This will give way for frequent pop-up messages and ads and other predator websites and online games that aren't even part of paid ads.

2. It's an algorithm which is used to calculate a fixed size bit string value from a file. A file consists of blocks of data. The Hash converts this data into a much shorter value with fixed length and that still represents the original string.

3. How to verify on Linux

   Execute the following command

   $ md5sum

   Then you will get a random string as the output. This will have to be compared with the checksum provided on the downloads page.

   How to verify on Mac OS

   Execute the following command

   $ md5

   The output shall be

   MD5 () =

   Compare the characters with the original MD5 checksum and ensure that they match.

   How to verify on Windows

   Execute the following command

   Got the Downloads path then type, -hashfile " " MD5

   If the command is successful, then the output shall behashfile command completed successfully.

4. Following identifiers and tools will help to identify the originality of an unknown file.

1. Toolsley File Identifier Webpage

While many people might be uncomfortable about uploading their files to a website, they need not worry in this case. Do not upload the unknown files to the internet at all and the identification work is done locally on your own computer using Javascript. This means there's no issue with insecure websites, internet upload speeds, or file size limits.

2. TrID / TrIDNet

TrID is probably the most comprehensive and well known file identification utility around. It's also still in active development so missing file types can be added in the future. It is essentially split into three different parts. Firstly, you have the TrID command line tool, then there's the TrIDNet graphical user interface. Finally, you have the definitions database that holds information for over 13,000 file types.

3. ExifTool

The ExifTool program is primarily a command line tool that you can also use from the desktop. Simply extract the executable from the zip file and to identify a file, drag and drop it onto the ExifTool icon. Any extensions the file has will be ignored and its content will be scanned so it doesn't matter if the file has no extension or simply a wrong extension.

4. DROID (Digital Record Object IDentification)

DROID is an open source tool developed by the UK National Archives to batch identify different types of file formats. This makes it quite good for identifying several unknown files at once instead of one at a time. The internal database of recognized file formats is usually updated a few times a year. DROID is based on Java so is multi-platform, the Windows edition includes embedded Java in the Zip so you don't need to install it.

5. Upload Your File And Get It Identified Online

While the first option in our list is a website that actually processes the file locally on your system, there are other websites that work in a different way. You can upload a file to a website and have the website try and identify the file on a remote server. Here's a couple to try.

6. Locate Opener

Locate Opener installs itself into your right click context menu, and when you run the program executable it simply has an install/remove button for controlling the menu entry. Right click on an unrecognized or incorrectly labeled file and select LocateOpener. Depending on whether has no

extension or one it cannot identify, you will either be asked to look for the extension online at file-extension.net or to scan the file with TrID.

5.

- By the usage of Infected removable devices
- By receiving and opening spam emails on your working device
- By downloading other software that is related to the functionality of this file.
- By accessing hacked or compromised web pages to download that particular file.

References

https://aboutssl.org/most-common-browser-security-threats/
https://luminet.co.uk/top-10-common-internet-threats/
https://www.helpnetsecurity.com/2011/09/08/how-to-deal-with-internet-security-threats/
https://www.computerhope.com/jargon/h/history.htm
https://www.webdevelopersnotes.com/what-is-browser-history
https://www.bigcommerce.com/ecommerce-answers/what-browser-cache-and-why-it-important/
https://blog.hubspot.com/marketing/what-is-browser-cache-faqs
https://kb.iu.edu/d/agwm
https://www.howtogeek.com/119458/htg-explains-whats-a-browser-cookie/
https://www.kaspersky.com/resource-center/definitions/cookies
https://www.webopedia.com/DidYouKnow/Internet/all_about_cookies.asp
https://www.netsparker.com/blog/web-security/session-hijacking/
https://www.techopedia.com/definition/24633/cookie-theft
https://www.digitalocean.com/community/tutorials/how-to-verify-downloaded-files
https://www.netsparker.com/blog/web-security/session-hijacking/
https://www.techopedia.com/definition/24633/cookie-theft