It offers a high speed transmission./ වේගවත් සම්ප්‍රේශණයක් ලබාදේ.

The reason UDP is faster than TCP is because there is no form of flow control or error correction. UDPහි වේගය TCP ට වැඩි වීමට හේතු වනුයේ එහි ගැලීම් පාලනයක් හා වැරදි නිවැරදි කිරීමක් නැති නිසාය./ අවම නිසාය.

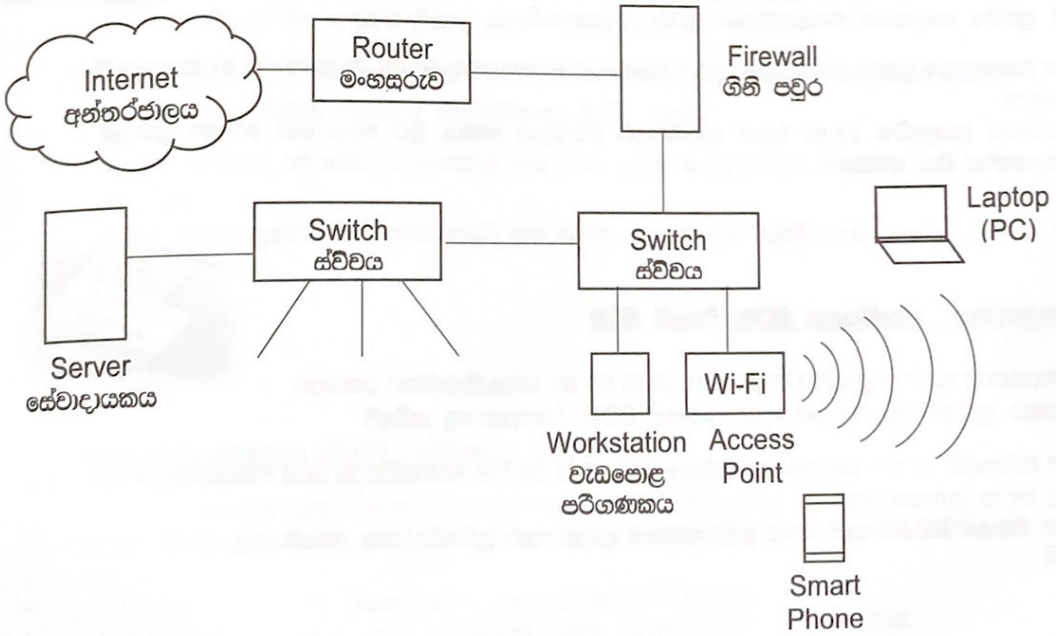
Therefor Video streaming is low quality./straming video හි ගුණාත්මක බව අඩු වන්නේ මෙම කරුණු නිසාය.

telnet

Through **Telnet**, one can access a remote computer.
දුරස්ථව ඇති පරිගණකයට ප්‍රවේශවීමට telnet භාවිත කරයි.
Telnet is an application layer protocol used on the Internet or another networks to provide a bidirectional interactive text-oriented communication facility.
වෙනත් පරිගණකයකට ප්‍රවේශ වී එයට පාඨ ආකාරයේ විධාන නිකුත් කර, එය පාලනය කිරීමට අන්තර්ජාලය හෝ වෙනත් ජාලයකට භාවිතා කරන සේවාවකි.

On the Web, HTTP and FTP protocols allow you to request specific files from remote computers, but not to actually be logged on as an user of that computer. With Telnet, you log on as a regular user with whatever privileges you may have been granted to the specific application and data computer.
http, ftp, ... මගින් වෙනත් පරිගණකයකින් ගොනුවක් ඉල්ලුම් කළද, පරිශීලකයෙකු ලෙස login නොවේ. Telnet මගින් පරිශීලකයකු ලෙස එම යන්ත්‍රයට සම්බන්ධ වී ලැබී ඇති වරප්‍රසාද අනුව වැඩසටහන් හා දත්ත මෙහෙය වනු ලබයි.

Consider the following network diagram./ පහත ජාල සටහන සලකන්න.



Physical Security of a Network – ජාලයක භෞතික ආරක්ෂාව

Physical security is the protection of personnel, hardware, programs, networks and data from physical circumstances and events.
භෞතික ආරක්ෂාව යනු පුද්ගලයන්, දෘඩාංග, ක්‍රමලේඛ ජාලා සහ දත්ත භෞතික සිදුවීම් සහ භෞතික හේතූන් තුළින් ආරක්ෂා කිරීමයි.

1. Lock up the server room - සේවාදායක පරිගණක කාමරය අගුල් දමා පැවතීම.

2. Setup Surveillance – මුරකිරීමේ ක්‍රමවේදයක් ඇති කිරීම.

3. Make sure the most vulnerable devices are kept in the standard way. - අනතුරකට භාජනය විය හැකි උපකරණ සම්මත ආකාරයට පවතිද යන්න තහවුරු කර ගැනීම.

4. Use rack mounts servers- සේවාදායක පරිගණක අඳාළ රාක්ක මත තැබීම.

5. Surge protectors, UPS, Stabilizers –

6. Follow the standard wiring for electricity power and data cabling.
දත්ත කේබල් සඳහා සහ විදුලි සැපයුම් කේබල සඳහා වයර් ඇදීමට සම්මත ක්‍රම අනුගමනය කිරීම.

Threats for computer networks –පරිගණක ජාල සඳහා තර්ජන

Spoofing attacks/ Spoofing – රැවටීම/ ප්‍රහාර

A malicious party impersonates another device or user or system on a network in order to steal data, spread malware, bypass access control ……..
ව්‍යාජ පාර්ශ්වයන් වෙනත් පුද්ගලයෙක් හෝ උපකරණයක් හෝ වැඩසටහනක් ලෙස පෙනී සිටීමන් ජාලයකට ඇතුළත්වී දත්ත සොරකම් කිරීමට malware පැතිරවීමට හෝ ප්‍රවේශ පාලනයක් මගහැරවීමට දරණ උත්සාහයකි.

The malicious party may have user name, password or another method to access the system……
පද්ධතියට ඇතුළ්වීම සඳහා ව්‍යාජ පාර්ශ්වයට පරිශීලක නාමය, මුර පදය හෝ වෙනත් ක්‍රමයක් යොදාගත්තා විය හැකිය.

Tampering – අපවේශනය කිරීම/ විකෘති කිරීම

Tampering is change the important data by an unauthorized person.
අනවසර පුද්ගලයකු වැදගත් දත්ත වෙනස් කිරීම Tampering නම්වේ.

The strength of the tampering attack depends on the knowledge and methods of the person who try to tampering.
දත්ත විකෘත කිරීමට පැමිණෙන පුද්ගලයාගේ දැනුම සහ ක්‍රමවේද මත අපවේශනය වීමේ ප්‍රමාණය රඳා පවති.

Repudiation - ප්‍රතික්ෂේප කිරීම, නොපිළි ගැනීම

The user can't prove what he has done because wrong data has entered to the log files (the repudiation of user's action)
Log files සඳහා වැරදි දත්ත ඇතුලත්ව ඇති බැවින් පරිශීලකයා කළ දේ ඔප්පු කළ නොහැකි වීම (පරිශීලකයාගේ ක්‍රියාකාරකම් ප්‍රතික්ෂේප කිරීම).

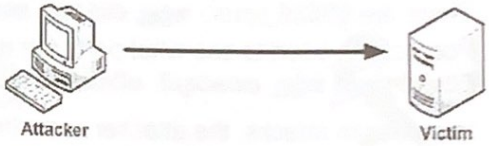
Information Disclosure (තොරතුරු අනාවරණය)

The aim of the attack is acquiring system specific information about website distribution, version numbers, location of backup files, comments on webpages, hidden files, user accounts.
මෙහිදී පද්ධතිය සම්බන්ධ විශේෂිත තොරතුරු වෙනත් පුද්ගලයකු අතට පත්වීම අදහස් කරයි.
වෙබ් අඩවිය පැතිරී ඇති අයුරු, සංස්කරණ අංක, උපස්ථ පිළිබඳ තොරතුරු, වෙබ් පිටුවල විවරණ, වෙබ් පිටුවේ සඟවා ඇති කොටස්, සැඟවුණු ගොනු, පරිශීලක ගිණුම් තොරතුරු .....

Denial of Services - සේවා සැපයීම ප්‍රතික්ෂේප කිරීම

DoS Attack

A denial of service attack is an attempt to make a machine or network resources unavailable to its intended users.
පරිගණක පද්ධතියක් මගින් හෝ ජාලයක් මගින් ලබාගන්නා සේවාවන් ලබාගත නොහැකි තත්වයකට එම පරිශීලයකයන් පත්වීම DOS Attack මගින් හඳුන්වයි.



- Large demand of services also can create this Environment.
  සේවා සඳහා පවතින ඉල්ලුම නිසාද මෙම තත්වය ඇති විය හැකිය.
- Traffic flooding attacks (Spread a huge volume of packets to the target system).
  දත්ත පැකට්ටු විශාල වශයෙන් පැතිරවීමෙන් සිදුවිය හැකිය.
- An attack may be able to prevent you from accessing email, website, online bank account....
  ඊමේල් සඳහා ප්‍රවේශ වීම, වෙබ් අඩවි සහ මාර්ග ගත බැංකු ගිණුම් සඳහා ප්‍රවේශ වීම අවහිර කිරීම.

Elevation of privileges (EoP) – (වරප්‍රසාද අභිබවා යාම)

An user try to gain beyond the authorized permission using illegal method.
නීත්‍යානුකූල නොවන ක්‍රම මඟින් තමාට ඇති වරප්‍රසාද වලට වඩා වැඩි යමක් ගැනීමට පරිශීලයකු වෑයම් කිරීම මින් අදහස් වේ.
Eg. An user with read only permission, try to change the data.
කියවීමට පමණක් අවසරය ඇති පරිශීලයකු දත්ත වෙනස් කිරීමට උත්සහ කිරීම.

Eg. A person is gaining the username and password from another person who has more privileges.
ඉහළ වරප්‍රසාද ඇති පුද්ගලයකුගේ පරිශීලක නාමය සහ මුරපදය ලබාගැනීම.

Phishing
Phishing is using fraud emails, websites, SMS and other methods attempt to gather personal and financial information.
Phishing යනු ව්‍යාජ ඊමේල්, වෙබ් අඩවි වැනි ක්‍රම භරහා පුද්ගල සහ මූල්‍ය තොරතුරු ලබා ගැනීමට උත්සහ කිරීමයි.

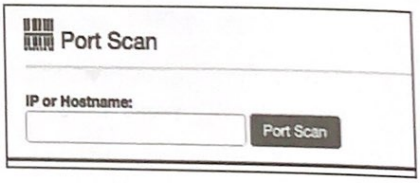
Users enter details at a fake website whose look and feel are almost identical to the legitimate one. මෙහිදි පරිශීලකයා නිතත්‍යානුකූල වෙබ් අඩවියේ ස්වරූපයට ඇති ව්‍යාජ වෙබ් අඩවියකට තම දත්ත ඇතුලත් කරයි.

Port Scan කවුළු පරීක්ෂාව
Computer applications are send & receive data packets through ports.
පරිඝණක වැඩසටහන් දත්ත පැකට්ටු යැවීම සහ ලබාගැනීම සැමවිටම කවුලු භරහා සිදුකරයි.

There are 65536 ports./ කවුලු 65536ක් ඇත.
Port scan is used to see what ports are opened.
විවෘතව ඇති කවුලු කවරේදැයි පරීක්ෂා කිරීමට Port scan භාවිත කරයි.

In port scan attacks, the attacker scan the ports to see what ports are using by the user.
ප්‍රහාරකයන්, පරිගණකයක විවෘතව ඇති කවුලු පිළිබඳ සොයා බලයි

The attacker can use this to find out what services are running.
මෙමගින් කුමන ආකාරයේ සේවාවන් ක්‍රියාත්මක වේද යන්න හඳුනාගනී.



Hacker

Hackers identify the weaknesses of a system and through weaknesses access the resources and get benefits from them.
(Steal credit card numbers, collect personal information.....)
Generally they are not damaging the system.
පද්ධතියක දුර්වල ස්ථාන හඳුනාගෙන ඔවුන්ගේ වාසිය සඳහා පද්ධතියකට අනවසරයෙන් ඇතුල්වන පද්ගලයන් (ණයපත්වල අංක ලබා ගැනීම. පුද්ගල තොරතුරු රැස් කිරීම, ----)
සාමාන්‍යයෙන් ඔවුන් පද්ධතියට හානියක් නොකරයි.

Cracker

Having gained unauthorized access, crackers destroy vital data, services ---------
Crackers are more dangerous than hackers. Security cracker is a person who trying break security of a system.
අනවසරයෙන් පද්ධතියකට ඇතුළ්වී වැදගත් දත්ත, සේවාවන් ------- විනාශ කරන පුද්ගලයා Crackers යනු hackers වඩා භයානක පුද්ගලයෙකි.
පද්ධතියක ආරක්ෂාව බිඳදමන පුද්ගලයා Security cracker නම් වේ.

Espionage – ඔත්තු බැලීම

Obtaining information without the permission of the owner.
අයිතිකරුගෙන් අවසරයක් නොමැතිව තොරතුරු ලබා ගැනීම.

Spyware, Trojan horses and cracking techniques are used for this.
Access to the commercial and finance information of an organization using illegal methods.
Spyware, Trojan horses සහ cracking techniques මෙහිදී භාවිත වේ.
ආයතනයක වාණිජ සහ මූල්‍ය තොරතුරු නීත්‍යානුකූල නොවන ක්‍රම මගින් ලබා ගැනීම.

Eaves Dropping – හොරෙන් සවන්දීම

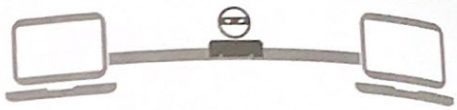
Secretly listen to others conversations./අනිත් අයගේ සංවාදවලට හොරෙන් සවන්දීම.

It is unauthorized listen to private communication such as phone calls, short messages, video conferences or fax transmission.
දුරකථන පණිවිඩ, කෙට් පණිවිඩ, විඩියෝ සම්මන්ත්‍රණ හෝ ෆැක්ස් සඳහා අනවසරයෙන් සවන්දීම.

Man in the Middle Attack (MitM) – මධ්‍ය සිට පහරදීම

It is a type of eavesdropping attack. මෙයද, යම ආකාරයක හොරෙන් සවන් දීමකි
The two original parties appear to communicate normally, the message sender does not recognize that the receiver is an unknown attacker try to access or modify the message before retransmitting to the receiver, thus the attacker controls the entire communication.
දෙපාර්ශ්වයක් දත්ත සන්නිවේදනයේ යෙදී සිටින විට, සම්ප්‍රේෂණය වන දත්ත පැකට්ටු ග්‍රහකයාට ලැබීමට පූර්ව වෙනත් පුද්ගලයකු ලබාගෙන සමස්ථ සන්නිවේදනය පාලනය කිරීම.

Data packet encryption is a good method to protect data from the man in the middle attack.
මධ්‍ය සිට දත්ත පැකට්ටු ලබාගෙන දත්ත වෙනස් කිරීම වැළැක්වීමට ගුප්තකරණය භාවිත වේ.



IP session Hijacking – IP සැසි කොල්ලකෑම

Cookies save in the user's computer to maintain some client side data. In IP session Hijacking attackers get data in cookies.
Cookies හි සේවාග්‍රහක අන්තයට සම්බන්ධ දත්ත තැන්පත්ව ඇත. IP සැසි කොල්ල කෑමෙදි පහරදෙන්නා විසින් Cookies වල ඇති වටිනා තොරතුරු ලබාගනී.

IP spoofing also belongs IP session Hijacking

Spoofing is pretending to be someone else. This a technique used to gain unauthorized access to the computer with as IP Address of a trusted host.
වෙනත් පුද්ගලයකුගේ/ සංස්කාරකයක IP ලිපිනය ලබාගෙන එය භාවිතයෙන් එම පුද්ගලයා/ සත්කාරකය ලෙස පෙනී සිටීම.

Spam

Spam is unsolicited email on the internet. Spam is flooding the internet with many copies of the same message. Most spam is commercial advertising.
The peoples' time and internet bandwidth is wasting with unwanted emails.
අන්තර්ජාලය මත අපගේ කැමැත්තකින් හෝ අවශ්‍යතාවයකින් හෝ තොරව එවනු ලබන ඊමේල් Spam ලෙස හඳුන්වයි. අන්තර්ජාලයට එකම පණිවුඩයේ පිටපත් විශාල වශයෙන් පැතිරවීමද, Spam ලෙස අන්තර්ජාලයේ විශාල දත්ත ප්‍රමාණයක් අපතේ යෑම සිදුවේ.

Adware

Adware is advertisement, but display on the screen without user permissions. Adware is an endless stream of pop-ups activities in the computer. After click on the advertisement it directs to the relevant website. Some adware for collect marketing data about user. Adware cleaners can install to remove adware.
පරිශීලකයාගේ අවසරයකින් තොරව තිරය මත ප්‍රදර්ශනය වන වෙළඳ දැන්වීම adware නමවේ. පරිගණකයේ ක්‍රියාකරන කාර්යයන් අතර අවසන් නොවන pop-ups ආකාරයට ප්‍රදර්ශනය වන වෙළඳ දැන්වීම් මාලාවක් Adware නමවේ. මෙම වෙළඳ දැන්වීම් click කළ පසු අදාළ වෙබ් අඩවියට ප්‍රවේශ වේ. සමහර Adware මගින් පරිශීලකයන් පිළිබඳ වෙළඳ දත්ත එකතු කිරීමට කටයුතු කරයි.

Malware (Malicious Code) - දෝෂ ජනක වැඩසටහන්

It is set of instructions (Program/ software) which is specifically designed to disrupt or damage a computer system.
පරිඝණකයට හානියක් කිරීමේ අරමුණින් සැලසුම් කරන ලද උපදෙස් මාලාවක් (ක්‍රමලේඛණයක්/ මෘදුකාංගයක්)

It is a common name for viruses, worms, Trojan horses, spyware … and other malicious programs.
එය viruses, worms, Trojan horses, spyware … සහ අනිකුත් ද්වේශ සහගත මෘදුකාංග සඳහා ලබාදෙන පොදු නාමයකි.

Virus (වෛරස)

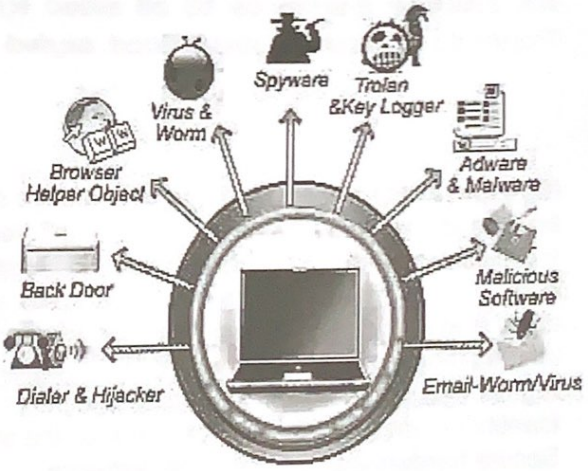
A virus is a program or piece of code that is loaded on to your computer without your knowledge and runs against your wishes.
වෛරස යනු අප නොදැනුවත්ව පරිඝණකයට ඇතුල්ව ඔබේ අපේක්ෂාවලට එරෙහිව යන වැඩසටහනක්.

Self- replicating program but need a host program to spread. Virus propagates by infecting other programs.
ස්වයංක්‍රියව පිටපත් සකස්කරගන්නා පරිඝණක වැඩසටහනකි. නමුත් පැතිරීම සඳහා වෙනත් සත්කාරක වැඩසටහනක් හා සම්බන්ධ වේ.

a virus cannot be spread without a human action.
මනිස් ක්‍රියාකාරකමකින් තොරව වෛරස පැතිරීම සිදුනොවේ.

Different types of Virus :- විවිධ වෛරස් වර්ග

- File infector viruses/ ගොනු සඳහා ආසාධනය වන වෛරස
  Infect to program files (normally infect to executable code such as .com & .exe files)
  සාමාන්‍යයෙන් .com සහ .exe වැනි වහා ක්‍රියාත්මක වියහැකි ගොනු සඳහා අසාධනය වේ.



- Boot sector viruses.
  Delete the data in the boot sector.
  "Boot Sector" හි ඇති දත්ත විනාශ කරන වෛරස.

- Macro viruses infect MS office & some other programs. මැක්‍රෝ වෛරස MS office වැනි වැඩසටහන්වලට බලපෑම් කරයි.
- Logic bomb: - trigging by an event. / යම් සිදුවීමකින් ක්‍රියාත්මක වන වෛරස
  Eg: Key stroke or connection with internet.
  විශේෂිත යතුරු කිපයක් එකවර ඇතුල්කිරීමේදී හෝ අන්තර්ජාලයට සම්බන්ධවන අවස්ථාවේ ක්‍රියාත්මකවන වෛරස.
- Time bomb:- triggered by specific time (day of the year).
  යම් නිශ්චිත වේලාවකදී ක්‍රියාත්මක වේ.

Worms

A worm is a self-replicating program that propagates form one computer to computer in a network environment no host program is required.

ස්වයං පිටපත් සාදමින් පරිඝණකයෙන් පරිඝණකයට පැතිරෙන ක්‍රමලේඛණකයකි. මේ සඳහා සත්කාරක ක්‍රමලේඛණයක් අවශ්‍ය නොවේ.

Most of time no need human intervention. බොහෝ විට මිනිස් මැදිහත් වීමක් අවශ්‍ය නොවේ.

Spyware

They can include hidden programs to spy on your activities.

ඔබේ ක්‍රියාකාරකම් රහසේ පරීක්ෂා කිරීමට සැගවී සිටින ක්‍රමලේඛණයකි.

They can even be used to steal passwords, credit card numbers.

ණයපත් අංක, මුරපද, ... වැනි දෑ සොරකම් කිරීමට මේවා යොදාගත හැකිය.

Sometimes these get installed when you download free programs from the internet.

අන්තර්ජාලයෙන් නිදහස් මෘදුකාංග සමග මෙවැනි වැඩසටහන් පැමිණිය හැකිය.

Trojan horse

A Trojan horse is a malicious code but apparently useful host program.

ප්‍රයෝජනවත් වැඩසටහනක් අකාරයට පෙන්වන ද්වේශ සහගත කේතවලින් සමන්විත වැඩසටහනකි.

When the host program is executed, Trojan does something harmfull or unwanted.

මෙම වැඩසටහන ක්‍රියාත්මක වන විට යම් හානිකර දෙයක් සිදු කරයි.

Trojans do not replicate./ට්‍රොජාන් පිටපත් සාදන්නේ නැත.

(Q) What are the security steps to protect a computer system?

Install and maintain anti-virus software – ප්‍රති වෛරස මෘදුකාංගයක් ස්ථාපනය හා නඩත්තු කිරීම.

Install firewalls and configure properly - ගිනි පවුරක් ස්ථාපනය කර අවශ්‍යතාව මත වන්‍යාසට සකස් කිරීම.

email filters – විද්‍යුත් තැපැල් පරීක්ෂා කිරීම (spam filters)

user training – පරිශීලකයන් පුහුණු කිරීම.

regular network monitoring methods, like port scanning.

Identify the methods that can be taken by the attacker. - ප්‍රහාරකරුට ගතහැකි ක්‍රම හඳුනාගැනීම.

Secure hardware and run security software

දෘඩාංගවල ආරක්ෂාව වැඩි කිරීම සහ ආරක්ෂිත මෘදුකාංග ක්‍රියාත්මක කිරීම.

Change the passwords frequently – නිරන්තරයෙන් මුරපද වෙනස් කිරීම

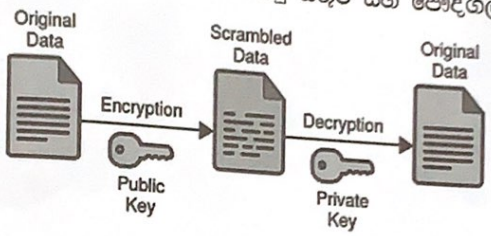
(Q) What is encryption? / ගුප්තකරණය යනු කුමක්ද?

The process of making data unreadable by other humans or computers for the purpose of preventing others from gaining access to its contents.
දත්තයක් අනිත් පුද්ගලයන් මගින් හෝ වෙනත් පරිගණක මගින් හෝ කියවිය නොහැකි තත්වයකට පත්කිරීම.

Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (ciphertext). Decryption is the process of converting ciphertext back to plaintext.

වචන වලින් සැදුණු දත්තයක් අර්ථයක් නොමැති අකුරු බවට පත්කිරීම ගුප්තකරණයයි වකේතනයෙන් නැවත වචන වලින් සැදුණු දත්ත බවට පත් කරයි.

Public key and Private key Encryption – පොදු යතුර සහ පෞද්ගලික යතුර ගුප්තකරණය



To read an encrypted file you must have the secret key/ primary Key or password that enables you to decrypt it. Illegal breaking depends on the ability of the attacker.

ගුප්තකරණය වූ ගොනුවක නැවත මුල් ලේඛනයට හැරවීමට රහස්‍ය යතුර, පුද්ගලික හෝ මුරපදයක් පැවතිය යුතුවේ. නීත්‍යානුකූල නොවන බිඳ දැමීම් ප්‍රහාර කරුගේ හැකියාව මත තීරණය වේ.

(Q) What is honey ports?

It is a computer system that is not the actual systems, it is a separate system to detect attackers.
එය පරිගණක පද්ධතියකි. සත්‍ය පරිගණක පද්ධතිය නොවේ. ප්‍රහාරකයන් හඳුනාගැනීමට නිර්මාණය කර වෙනම පවත්වාගෙන යන පරිගණක පද්ධතියකි.

Try to identify the methodologies of the attackers.
ප්‍රහාරකයන් අනුගමනය කරන ක්‍රම හඳුනාගැනීමට දරණ උත්සාහයකි.

(Q) How Does a Computer Get a Virus? පරිගණකයකට වයිරසයක් ඇතුලු වන ආකාර

- On downloading files from the Internet. / අන්තර්ජාලයෙන් ගොනු බාගත කරගැනිමේදි
- On opening an e-mail attachment and through Email.
  ඊමේල් හරහා පැමිණෙන ඇමුණුම් විවෘත කිරිමේදි
- On copying programs or files from any other infected computer.
  වයිරස ආසාධිත පරිගණකයකින් ගොනු/වැඩසටහන් පිටපත් ගැනිමේදි
- Shared infected flash drives, CD and other media.
  සැනෙලි ධාවකයන්, සංයුක්ත තැටි සහ අනෙකුත් මාධ්‍ය පොදුවේ භාවිතයේදි
- Hacking (Occasionally). / පරිගණකයට සිදුවන අනවසර ප්‍රවේශයන් මගින් (සමහරවිට)

(Q) What are the Symptoms of a computer viruses?
පරිගණකයක වයිරස ඇතිවිට දැකිය හැකි ලක්ෂණ?

- The computer runs slower than usual.
  පරිගණකය වැඩකිරිමේ වේගයට වෙනදාට වඩා අඩුවීම
- It restarts every few minutes. / නිතර restart වීම
- Applications on the computer do not work correctly.
  පරිගණක වැඩසටහන් නිසිපරිදි ක්‍රියාත්මක නොවීම
- Disks or disk drives are inaccessible. / තැටි හෝ ධාවක වලට ප්‍රවේශ වීමට නොහැකි වීම
- You see unusual error messages. / ඔබට ආසාමාන්‍ය පණිවිඩ දැකිය හැකි වීම
- An antivirus program cannot be installed on the computer, or the antivirus program will not run. / ප්‍රතිවයිරස මෘදුකාංග ස්ථාපනය කිරිමට නොහැකි වීම හෝ ක්‍රියාකාරි නොවීම.
- New icons appear on the desktop that you did not put.
  පරිගණක තිරය මත ඔබ ඇතුළත් නොකළ නව අයිකන දිස්වීම.
- File deletion & File corruption. / ගොනු මැකියාම හා හානිවීම.