Computer अनि सुरक्षाका उपायहरु : एक चर्चा

computer तथा internet को उपयोगिताको बारेमा हामी चितवनबासीले धेरै थोरै बुझिसकेका छौं । आज हामी याँहा computer तथा internet को फाईदाको बारेमा नभएर internet तथा lan मा रहेका computer को सुरक्षा प्रणालीको वारेमा चर्चा गर्नेछौं । एकातिर world trade centre ध्वस्त हुँदा पनि ८ दिन भित्र computer मा रहेको सम्पूर्ण data हरु recover गरि company जस्ताको तस्तै फेरी बजारमा आएको समाचार सुन्न पाईन्छ भने अर्को तर्फ harddisk बिग्रेर कुनै चितवनबासीको computer मा रहेको सम्पूर्ण account खत्तम भएको खवर सुन्न पाईन्छ । computer तथा internet मा हामी चितवनबासीले विगतका छोटो समयमा द्रुत गतिमा प्रगती गरिरहेका छौ यसमा कुनै शंका छैन तर data backup र security त्यस्ता विषय हुन् जसमा न त तपाई हामीले त्यती ध्यान दिएका छौ नत बिश्व भरि आफ्ना शाखाहरु भएका computer institute हरुले नै । data backup र security जस्ता बिषयलाई गम्भिरतापुर्वक आफ्नो course of study मा सामिल गर्दा यो त्यती लोभलाग्दो नदेखिनुको कारणलेपनि यसले राम्रो स्थान पाउन सकेको छैन जबकी कुनै पनि operating system को basic course पछि सबैभन्दा पहिला खड्किने बिषय हो यो data backup र security।

computer security को कुरा गर्दा सबैभन्दा अगाडी आउँछ virus। virus को कारणले यो बर्ष computer प्रयोगकर्ताहरु नराम्रोसँग प्रभावित भए भने कति त अझै पनि computer मा के problem आयो भनेर अन्यौलमै छन् । virus database मा पनि यो बर्ष अचम्म प्रकारले बृद्धि भएको देखियो । एकातिर nimda ले ठुला-ठुला organization हरुको दिमाग चाट्यो भने अर्को तर्फ klez ले normal user हरुलाई अचम्भित तुल्यायो । एकातिर redlof ले सनसनी फैलाईरहेको छ भने अर्को तर्फ opasoft नामक virus (worm) computer मा भएको कुरा धरै जसोलाई थाहै छैन । यो सब समस्याको एक मात्र सामाधान हो security तथा backup। साधारणतया security भन्नाले computer लाई सुरक्षित बनाउने भन्ने बुझिन्छ भने backup भन्नाले सम्भाब्य खतराबाट computer मा रहेको data तथा programme हरुलाई सुरक्षित राख्ने भन्ने बुझिन्छ । physical backup को बारेमा चर्चा गरिरहनु त्यति महत्वपूर्ण नदेखिएकोले याहाँ हामी security तर्फनै केन्द्रित रहनेछौं ।

चितवनको परिपेक्षमा security अन्तर्गत हामीले निम्न लिखित प्रमुख ३ कुरामा तत्काल ध्यान पुऱ्याउनु पर्ने देखिन्छ ।

१) keylogger तथा spyware
२) virus
३) attack from outside

१) **<u>keylogger तथा spyware</u>**

keylogger तथा spyware हरु त्यस्ता programme हरु हुन् जसले तपाईको computer को सम्पूर्ण activities monitoring गर्न सक्छ । यसरी यो programme ले

record गरेका कुराहरुलाई एउटा log file मा save गरेर राख्दछ र तपाई internet connected हुनु भएको मौका पारेर त्यसलाई पुर्वनियोजित e-mail address मा पठाउदछ । यसरी पठाईएको log file मा तपाईले कसैलाई लेख्नु भएको e-mail, तपाईको password, तपाईले web site मा हेर्नुभएको URL हरु साथै अरु थुप्रै महत्वपूर्ण कुराहरु हुन सक्छन् । कतिपय keylogger तथा spyware हरुलाई तपाईको anti-virus programme ले virus भनेर चिन्न सक्दैन फलस्वरुप तपाईको कृयाकलापहरु कसैले हेरीरहेको कुरा तपाईलाई थाहै हुदैन । यो programme कुनै पनि माध्यामबाट तपाईको computer सम्म पुऱ्याएर execute गरिन्छ अनि registry entry गरेर यो programme ले अर्को पल्ट देखि computer start भएदेखिनै भित्र भत्रै तपाँईको activities लाई log file मा save गरेर राख्दछ अनि तपाँई internet मा connected भएको मौका पारेर त्यो log file लाई गन्तब्यसम्म e-mail गरेर पठाउछ । यस्ता keylogger तथा spyware हरु बाट आफ्नो computer लाई सुरक्षित राख्न तपाँईलाई computer को running process को बारेमा जानकारी हुनु आवश्यक छ । Alt+Ctrl+Delete एकै चोटि press गरेर तपाँईले computer को running programme को बारेमा साधारण जानकारी पाउन सक्नुहुन्छ । यो बाहेक Ad-aware जस्ता programme ले पनि तपाईलाई यस्ता keylogger तथा spyware हरु हटाउन मद्दत गर्दछ । यो programme तपाँईले ***www.lavasoftusa.com*** बाट free मा download गर्न सक्नुहुन्छ ।

२) **<u>Virus</u>**

Virus बाट त तपाँई हामी परिचित छौं नै । सबै भन्दा बढी virus फैलने माध्याम internet हो भने virus बाट छुटकारा पाउने सबै भन्दा सशक्त, अझ भनौं एकमात्र माध्याम internet नै हो । याहाँ हामीले virus अन्तर्गत virus, trojan, worm तथा hoax सबैलाई एकै ठाँउमा समेटेका छौं । virus, trojan, worm तथा hoax हरु बनावटका हिसाबले आफैमा अलग अलग भए भनि सामाधान सबैको लगभग एउटै भएकोले सबैलाई virus अन्तर्गतनै समेटिएको हो । virus कसले बनाउछ र किन बनाउछ भन्ने प्रश्न बेला बेलामा तपाँई हाम्रो मनमा अवश्यपनि उब्जने गरेको छ । वास्तवमा virus त्यस्ता ब्यक्तिहरुको दिमागको उपज हो जसलाई आफ्नो फाईदाले भन्दा अरुको नोक्सानले सन्तुष्टि दिने गर्दछ । त्यसो भए virus बाट बच्न के गर्ने त ? प्रश्न उठ्छ । कुनै एउटा राम्रो anti-virus programme प्रयोग गर्नुहोस् । याहाँ राम्रोको अर्थ हो बढी प्रयोग हुने । जस्तैः symantec को norton वा macafee । अनि तपाईको anti-virus programme लाई नियमित रुपमा update राख्नुहोस् । e-mail मा आएका attachment हरुलाई धेरै बिचार गरेर मात्र खोल्नुहोस् । अझ attachment .exe वा .bat जस्ता executable extension मा छन् भने त खोल्दै नखोल्नुनै बुद्धिमानी हुनेछ । web surfing गर्दा पनि ActiveX र plugn-ins जस्ता software हरु download तथा install गर्दा ध्यान पुऱ्याउनुहोस् । internet security level लाई सम्भव भए high नत्र कमसे कम medium राख्नुहोस् । java based web site हरु trusted छन् भने मात्र खोल्नुहोस् । यी सब

कुरामा ध्यान पुऱ्याएर तपाईहरुले केहि हदसम्म आफ्नो computer लाई virus बाट सुरक्षित राख्न सक्नुहुन्छ । एउटा कुरा कहिल्यै नभुल्नुहोस् कि एउटा साधारण html बाट बनेको web page समेतले तपाईको computer hack गर्न सक्छ । यस बाहेक पनि अहिलेको latest anti-virus norton 2003 ले तपाईलाई untrusted web surfing मा केहि हदसम्म सुरक्षा दिन सक्छ भने यसले online scanning को सुबिधा पनि दिएको छ । online scanning को माध्यामबाट तपाईले आफ्नो computer लाई web site मा गएर online scan गर्न सक्नुहुन्छ जस्ले तपाईलाई तपाईको computer को open port अथावा security hole को बारेमा जानकारी दिन्छ । open port को बारेमा हामी attack from outside नामक आँउदो topic मा चर्चा गर्नेछौं ।

Virus को बारेमा कुरा गर्दा एउटा नाम सधै अगाडी आँउछ, त्यो हो Trojan Horse । बास्तवमा trojan horse virus नभएर एक प्रकारको security breaking programme हो जसलाई हामी virus नै भनेर चिन्दै आईरहेका छौं । धेरै पहिले देखिनै computer को दुनियामा तहल्का मच्चाउदै आईरहेका र अलग अलग नाममा हजारौको सँख्यामा रहेका यस्ता trojan हरुलाई हटाउन कुनै पनि anti-virus programme राम्रो सँग सफल भएको भेटिएको छैंन । फैलने क्षमता कम भएको र Server-Client का रुपमा काम गर्ने यस्ता torjan को मुख्य बिशेषता Remote-Administration नै हो । कुनै पनि माध्यामबाट एउटा executable file तपाईको computer मा पठाएर सो file लाई तपाईको computer मा execute गरिएपछि वा तपाई आफैले अनजानमा त्यो file लाई execute गर्नुभयो भने तपाई trojan infected हुनु भयो । तपाईलाई केहि थाहै हुदैन तर यसले काम गरिसकेको हुन्छ । यसले तपाईको computer मा कुनै निश्चित port open गर्छ अनि TCP अथवा UDP को माध्यामबाट तपाईलाई remote computer सँग connect गराउँछ । एक पटक तपाई trojan infected हुनु भएपछि अर्को तर्फबाट तपाईको computer को password हेर्ने, तपाईको महत्वपूर्ण file हरु तान्ने देखि लिएर तपाईको computer नै बन्द गर्ने जस्ता उपद्रो समेत सजिलै गर्न सकिन्छ । trojan बाट छुटकारा पाउनका निम्ति तपाईले anti-virus तथा trojan removal जस्ता programme हरु प्रयोग गर्न सक्नुहुन्छ । अर्को एउटा सटिक तर अलि मुश्किल उपाय हो netstat । command mode मा गएर (netstat -an) command प्रयोग गर्नुहोस् । यसले तपाईको computer को connection र open port को सम्पूर्ण बिवरण दिन्छ र यदि यहाँ तपाईले port 21554 open देख्नुभयो भने सावधान तपाईको computer GirlFriend नामक trojan बाट infected छ । यसरी बिभिन्न प्रकारका अलग अलग trojan ले open गर्ने अलग अलग port को list तपाईहरुले internet मा पाउन सक्नुहुन्छ । एक पटक तपाईले तपाई कुन trojan बाट infected छु भनेर पत्ता लगाउन सक्नु भयो भने त्यसैमा केन्द्रित रहेर removal download गर्न सक्नुहुन्छ अथवा धेरै जसो trojan हरु manually पनि delete भएको पाएका छौं । यी बाहेक पनि हिजो आज हामीले virus को नामले चिन्ने गरेको @m र @mm बर्गका worm हरुले पारो तताउन थालेको छ । computer को address book मा entry भएको e-mail

address मा मिल्दोजुल्दो बिषय सहित आफुलाई mail गर्न सक्ने क्षमता भएको यो worm को फैलन सक्ने क्षमता एकदमै बढी रहको पाईन्छ । राता रात पुरै बिश्वभरि फैलन सक्ने यस्ता worm हरु अन्तरर्गत something@m भन्नाले mail गर्न सक्ने क्षमता भएको भन्ने बुझिन्छ भने something@mm भन्नाले mass-mailer अर्थात एक भन्दा बढी mail गर्न सक्ने क्षमता भएको भन्ने बुझिन्छ । साधारणतया e-mail बाट फैलने यस्ता virus (worm) ले त्यत्ति धेरै हानी नगरेपनि यसको फैलने क्षमता एकदम बढी हुन्छ भने कहिले कहिँ तपाँईको e-mail address बाट तपाईको साथीलाई गाली गरेर e-mail लेखेर तपाईलाई गाली ख्वाउन पनि बेर लगाउदैन । त्यसैले सावधान तपाईको inbox मा आएको attachment साँच्चैनै तपाईकै साथीले पठाउनु भएको attachment त हो ?

३) attack from outside

साधारणतया attack from outside भन्नाले TCP वा UDP को माध्यामबाट तपाईको IP लाई लक्ष्य बनाएर गरिने attack हो । attack from outside भनेर याहाँ कुनै universal topic नभएर internet वा network बाट हुने attack लाई एउटा heading मात्र दिईको हो । यस्ता प्रकारका attack हरुलाई बुझ्न र रोक्न keylogger र virus problem लाई बुझ्न र रोक्न भन्दा अलि बढी मुश्किल छ भने यसको बारेमा जानकारी हुन अति आवश्यक पनि छ । हामीलाई यस्ता प्रकारका attack र यसबाट गर्न सकिने सुरक्षाको बारेमा राम्रोसँग थाहा नहुनुको प्रमुख कारण हो computer institute हरुले security लाई आफ्नो course मा राम्रो सँग focus नगर्नु । अझ तितो बाक्य प्रयोग गर्ने हो भने पैसा कमाउन बिहारी पाराको रङ्गीबिरङ्गी मिठाईझैं लोभलाग्दो course छान्ने धुनमा security तर्फ त वाहाँहरुले ध्याननै दिन पाउनु भएन । कुनै institute सँग छ security specilist ??

attack from outside को एउटा सबै भन्दा सामान्य किसिम हो denial of service attack अर्थात Dos Attack । यसलाई अर्को भाषामा ping flood पनि भनिन्छ । एउटा सामान्य ping command द्वारा ठुलो size को packet प्रयोग गरी target computer लाई re-boot अथावा crash गर्नुनै Dos Attack हो । यसको लागी Unix वा Linux Operating System को प्रयोग गरिन्छ किनकी Windows ले तपाईलाई ping गर्दा packet size निर्धारण गर्ने अधिकार दिदैन । तपाई internet सँग connected हुनु भएको बेलामा तपाईको computer नाटकिय रुपमा ढिलो भयो वा आपसेआप re-boot भयो भने त्यसको एउटा कारण Dos Attack पनि हुन सक्छ । यसरी Dos Attack ले तपाईको पुरै Operating System नै पनि crash गर्न सक्छ । यो त भयो computer लाई क्षती पुऱ्याउने उद्देश्यले गरिने attack। यो बाहेक पनि अर्को attack हुन्छ जुन internet connected रहेको अरुको computer मा छिर्नको लागी गरिन्छ । यसलाई हाम्रो समाजले अहिले computer crime वा hacking पनि भनेर चिन्ने गरेको छ । याहाँनेर एउटा कुरा के जानकारी दिन चहान्छु भने वास्तवमा hacking भनेको internet बाट अर्काको computer मा छिरेर अर्काको computer तहस नहस पार्नु हैन जवकी

hacker भनेको त computer को दुनियामा एउटा आदर्श नाम हो । computer को दुनियामा जती पनि नराम्रा कामहरु भए ती सब hacker हरुको थाप्लोमा राखियो र आज hacker हरु computer criminal को रुपमा चिनिन्छन् । एक पटक चितवनका जिज्ञासु युवाले computer field का एक बिशिष्ट ब्यक्तिसँग प्रश्न राखेको थियो "hacker भनेको के हो?" वाहाँले स्पष्ट जवाफ दिनु भयो "हामी यो illegal बिषयमा कुरै गर्दैनौ" जवकी वाहाँको आफ्नै institute को course मा Linux Operating System अन्तर्गत एउटा course हुन्छ "kernel hacking" । वास्तवमा hack आफुमा illegal शब्द हैन जवकी त्यसलाई हेर्ने दृष्टिकोण गलत भैदिएको छ अर्थात internet को माध्यामबाट अर्काको computer मा छिर्नु hacking हैन ।

हामीले अधिनै चर्चा गरेका थियौ open port को बारेमा । यहि open port को माध्यामबाट कोही तपाईको computer मा छिर्न सक्छ । उसले तपाईको computer को कुनै फाईल copy, paste वा delete पनि गर्न सक्छ । अझ तपाईको computer मा NetBios installed छ भने त अज झनै सजिलो हुन्छ । NetBios Windows networking मा file sharing को लागी प्रयोग हुने software हो । अखिर कसरी छिर्न सक्छ त कोही तपाईको computer मा ???

मानौं तपाई internet connected हुनुहुन्छ । कसैले तपाईको IP थाहा छ अथवा उसले ping गरेर तपाईको IP blind guess हान्छ अथवा MSN, ICQ जस्ता कुनै chat client द्वारा तपाईको IP पत्ता लगाउछ अथावा कुनै programme को माध्यामबाट तपाईको IP पत्ता लगाउछ । त्यसपछि उसले तपाईको computer को कुन port open छ भनेर scanning गर्छ । कसरी ?? जन्नु त्यती जरुरी छैन । हामी मात्र सटिक सुरक्षाको लागी process लाई बुझ्ने कोशिष गर्दै छौं । जब उसले तपाईको कुनै port open पाउछ अनि उ त्या open port को माध्याबाट तपाईको computer मा छिर्छ । यसरी एक पटक कोही तपाईको computer मा छिरेपछि यात उसले तपाईको computer को file चोर्ने अथावा तपाईको computer को महत्वपुर्ण file हरु delete गर्ने काम गर्छ वा कुनै trojan transfer गरेर तपाईको computer मा execute गरेर तपाईलाई सधैको लागी torjan infected बनाउछ । यसो गरेको खण्डमा अर्को पटक देखि उसले तपाईको computer सँग सजिलै single click को भरमा connection गर्न सक्छ । यसरी internet बाट हुने attack लाई तपाईको anti-virus software ले हेरेर बस्नु बाहेक केही गर्न सक्दैन । त्यसो भए कसरी राख्ने त यस्तो attack बाट आफ्नो computer लाई सुरक्षीत ? जवाफ हो proxy तथा firewall ।

Proxy Server

साधारण भाषामा भन्दा proxy server ले तपाईको computer को वास्तविक IP लाई लुकाएर अर्कै IP प्रयोग गरेर तपाईको computer लाई सुरक्षा प्रदान गर्छ । उदाहरणको लागी जब तपाई proxy server को माध्यामबाट कुनै remote computer सँग connect गर्नहुन्छ त्यतीखेर proxy server ले request packet header मा तपाईको वास्तविक IP नपठाएर

anonymous वा अरु computer को IP पठाउछ । भन्नुको अर्थ proxy server ले तपाईको वास्तविक identity लाई लुकाएर computer लाई सुरक्षा प्रदान गर्ने गर्छ ।

<u>Firewall</u>

कारको engine र driver को बिचमा car को engine blast भएमा driver लाई सुरक्षा दिन राखिएको भागलाई firewall भनिन्छ । वास्तवमा computer मा firewall को धेरै बिस्तृत अर्थ लाग्छ तर एउटा साधारण अवस्थामा यसलाई यसरी परिभाषित गर्न सकिन्छ । firewall भनेको तपाईलाई बाहिरी network बाट सुरक्षा दिन तपाईको computer र internet को बिचमा बस्ने device वा programme हो । firewall ले तपाईलाई internet बाट हुनसक्ने outside attack बाट सुरक्षा प्रदान गर्छ । सही प्रयोग गर्न जाने firewall धेरैनै बिश्वस्त programme साबित हुन सक्छ । यसले port scanning तथा Dos Attack जस्ता कृयाकलापहरुलाई सजिलै रोक्न सक्छ भने कुनै पनि untrusted IP लाई ban पनि गर्नसक्छ । तपाईको internet connection monitoring जस्ता थुप्रै facility हरु भएको यो programme ले तपाईको computer मा गलत नियत भएको कोही बस्यो भने चाँही केही गर्न सक्दैन । जे होस् outside attack लाई बिफल पार्नका लागी firewall बरदाननै साबित भएको छ ।

यी कुराहरुमा ध्यान पुऱ्याएर तपाईले आफ्नो computer लाई धेरै हदसम्म सुरक्षा दिन सक्नुहुन्छ । यस बाहेक पनि security सम्वन्धि हजारौ tutorial हरु तपाईहरुले internet बाट download गरेर पढ्न सक्नुहुन्छ । यस बाहेक तपाईको Windows Operating System तथा programme हरुमा पत्ता लागेको नयाँ नयाँ security hole हरु (जसको बारेमा याहाँ चर्चा गरिएको छैन) लाई update वा patch को सहायताबाट ***windowsupdate.microsoft.com*** मा गएर online नै पनि fix गर्न सक्नुहुन्छ । तपाँईहरुलाई computer मा आईपरेको कुनै पनि समस्याका लागी हामीसँग सम्पर्क राख्नुहोस् । हामी निशुल्क सल्लाह दिनका लागी सदा उपलब्ध छौ ।

"knowledge is power and with power comes a responsibility"

Santosh Joshi
Cyberhome P. Ltd.
Phone: 056-26372, 26373
"vasmasur@hotmail.com (Catch me Online)
"स्मारिका - चितवन महोत्सव २०५९" मा प्रकाशित