

कम्प्यूटर, हमारे जीवन में बहुत महत्वपूर्ण भूमिका निभाता है। वह हर प्रकार के कार्य (सरल व गोपनीय) करने में सहायता करता है। इसलिए हम अपने सिस्टम को व्यक्तिगत व सुरक्षित रखना चाहते हैं, ताकि कोई अवैध उपयोगकर्ता इसका गलत इस्तेमाल न कर सके और कोई वायरस भी सिस्टम को क्षति न पहुँचा सके।

कम्प्यूटर सिक्योरिटी को **साइबर सिक्योरिटी** या **आई टी सिक्योरिटी** के नाम से भी जाना जाता है। यह सूचना प्रौद्योगिकी की एक शाखा है जिसे खासकर कम्प्यूटरों की सुरक्षा के लिए बनाया गया है। इससे कम्प्यूटर सिस्टम तथा डेटा, जिसे ये स्टोर या एक्सेस करते हैं, की सुरक्षा होती है। सुरक्षा प्रदान करने के लिए निम्नलिखित चार तरीके इस्तेमाल किए जाते हैं।

1. सिस्टम एक्सेस कण्ट्रोल

(System Access Control)

ये एक ऐसी प्रणाली है जो किसी कम्प्यूटर में डेटा का उपयोग या उसमें कुछ परिवर्तन करने की अनुमति प्रदान करती है। आमतौर पर एक उपयोगकर्ता किसी कम्प्यूटर में लॉग इन (log-in) करता है, जिसके पश्चात् एक्सेस कण्ट्रोल तय करता है कि उस उपयोगकर्ता के लिए (उपयोगकर्ता आई डी के आधार पर) कौन-सा डेटा पहुँच में होना चाहिए और कौन-सा नहीं।

2. डेटा एक्सेस कण्ट्रोल (Data Access Control)

कौन-सा डेटा, कौन नियन्त्रित कर सकता है? इस बात की निगरानी इस कण्ट्रोल के तहत की जाती है। सिस्टम किसी भी व्यक्ति विशेष, फाइलों तथा अन्य किसी भी ऑब्जेक्ट्स की सुरक्षा के स्तरों पर आधारित होकर ही एक्सेस नियमों को बनाता है।

3. सिस्टम तथा सिक्योरिटी प्रशासन (System &

Security Administration)

इसके अन्तर्गत ऑफ लाइन प्रक्रिया का निष्पादन होता है। जिससे कोई भी सिस्टम या तो सुरक्षित बनाया जाता है या फिर उसकी सुरक्षा को तोड़ा जाता है।

4. सिस्टम डिज़ाइन (System Design)

यह कम्प्यूटर के हार्डवेयर तथा सॉफ्टवेयर की बुनियादी सुरक्षा की विशेषताओं से लाभ लेती हैं।

कम्प्यूटर सुरक्षा के घटक

(Components of Computer Security)

कम्प्यूटर सुरक्षा कई प्रकार के कोर क्षेत्रों से सम्बन्धित होती है। कम्प्यूटर सुरक्षा सिस्टम के बुनियादी घटक इस प्रकार हैं

84

(a) **गोपनीयता (Confidentiality)** किसी भी जानकारी/डेटा के अन्य अवैध व्यक्ति द्वारा एक्सेस न होने की घटना को सुनिश्चित करना, इसके अन्तर्गत आता है।

(b) **नॉन-रेपुडिएशन (Non-Repudiation)** मैसेज को भेजने वाला ऑरिजिनल व्यक्ति कहीं अपने मैसेज को स्वयं का होने से न इन्कार कर दे। इस प्रकार की सुनिश्चितता को गैर-प्रत्याख्यान (नॉन-रेपुडिएशन) कहते हैं।

(c) **प्रमाणीकरण (Authentication)** यह कम्प्यूटर सिस्टम को इस्तेमाल करने वाले व्यक्ति के वैध अथवा अवैध होने को सुनिश्चित करता है।

(d) एक्सेस कण्ट्रोल (Access Control) जिस उपयोगकर्ता को जिन संसाधनों का प्रयोग करने की अनुमति प्राप्त हो वह केवल उन्हीं संसाधनों को इस्तेमाल करे। इस बात की सुनिश्चितता को एक्सेस कण्ट्रोल कहा जाता है।

(e) उपलब्धता (Availability) सभी सिस्टमों के कार्य करने की प्रणाली का सही होना व किसी भी वैध उपयोगकर्ता को सेवाएँ देने से न मना करना। इस बात को, उपलब्धता के नाम से जाना जाता है।

(f) कूटलेखन (Cryptography) किसी सूचना को छिपाकर या गुप्त तरीके से लिखने की तकनीक को कूटलेखन कहा जाता है। इसके माध्यम से इंटरनेट पर डेटा संचरण के दौरान डेटा को सुरक्षित रखा जाता है।

कूटलेखन में सामान्यतया प्रयुक्त होने वाले तत्व निम्नलिखित हैं

(a) प्लेन टैक्स्ट (Plain Text) यह इनपुट के रूप में दिया जाने वाला ऑरिजिनल सन्देश होता है।

(b) साइफर (Cypher) यह बिट-बाई-बिट या कैरेक्टर-बाई-कैरेक्टर परिवर्तन करने की प्रक्रिया है, जिसमें सन्देश का अर्थ नहीं बदलता।

(c) साइफर टैक्स्ट (Cipher Text) यह कोडेड सन्देश या इन्क्रिप्टिड डेटा होता है जिसे उपयोगकर्ता सीधे-सीधे नहीं पढ़ सकता।

(d) इन्क्रिप्शन (Encryption) प्लेन टैक्स्ट को साइफर टैक्स्ट में परिवर्तित करने की प्रक्रिया को इन्क्रिप्शन कहते हैं। इसके तहत एक इन्क्रिप्शन एल्गोरिथ्म का प्रयोग होता है।

(e) **डिक्रिप्शन (Decryption)** यह इन्क्रिप्शन प्रक्रिया का रिवर्स होता है अर्थात् इसमें साइफर टैक्स्ट को प्लेन टैक्स्ट में परिवर्तित किया जाता है।

(f) **स्टेनोग्राफी (Stenography)** सन्देश को उसके अस्तित्व सहित छुपाने की कला को स्टेनोग्राफी कहते हैं। यह डेटा की गोपनीयता तथा एकीकरण में मदद करता है।

(g) **एकीकरण (Integrity)** यह सुनिश्चित करता है कि सूचना को किसी अवैध व्यक्ति द्वारा इस प्रकार बदला तो नहीं गया कि उसे वैध उपयोगकर्ता भी न पहचान सके। एकीकरण कम्प्यूटर सुरक्षा का एक अत्यन्त महत्वपूर्ण घटक है।

साइबर आक्रमण के स्रोत (Sources of Cyber Attacks)

कम्प्यूटर पर मुख्य रूप से सक्षम तथा भेद्य हमालावार, वायरस प्रोग्राम है। कम्प्यूटर वायरस एक छोटा सॉफ्टवेयर प्रोग्राम है, जोकि एक कम्प्यूटर से दूसरे कम्प्यूटर में फैलता है तथा कम्प्यूटर ऑपरेशनों में भी हस्तक्षेप करने की क्षमता रखता है। इस प्रकार के आक्रमण के स्रोत हैं

(a) डाउनलोडेबल प्रोग्राम्स (Down loadable Programs)

डाउनलोडेबल फाइल्स वायरस का सबसे प्रमुख तथा सम्भव स्रोत है। किसी भी प्रकार की एक्जीक्यूटेबल फाइल; जैसे-गेम्स, स्क्रीन सेवर इत्यादि इसके प्रमुख स्रोत हैं। यदि आप किसी प्रोग्राम को इंटरनेट से डाउनलोड करना चाहते हैं तो डाउनलोड करने से पहले प्रत्येक प्रोग्राम को स्कैन करना आवश्यक है।

(b) **क्रैक्ड सॉफ्टवेयर (Cracked Software)** ये सॉफ्टवेयर वायरस अटैकों के अन्य स्रोत हैं। इस प्रकार के क्रैक्ड सॉफ्टवेयर में वायरस तथा बग्स, के होने की सम्भावना अत्यधिक होती है। जिन्हें ढूँढकर सिस्टम से दूर करना बेहद कठिन है। इसलिए इंटरनेट से सूचना को किसी भी विश्वसनीय स्रोत से ही डाउनलोड करना चाहिए।

- (c) **ई-मेल अटैचमेंट्स (e-Mail Attachments)** ये अटैचमेंट्स वायरसों के मुख्य स्रोत होते हैं। इन ई-मेल अटैचमेंट्स को आसानी से हैंडल किया जा सकता है।
- (d) **इंटरनेट (Internet)** सभी कम्प्यूटर के यूजर्स, कम्प्यूटर सिस्टमों पर वायरस अटैकों से अनभिज्ञ होते हैं। इंटरनेट पर उपलब्ध क्लिक या डाउनलोड इत्यादि तत्व ही वायरसों के फैलने के लिए उत्तरदायी होते हैं।
- (e) **अज्ञात सीडी से बूटिंग करना (Booting from Unknown CD)** जब भी कम्प्यूटर कार्य नहीं कर रहा होता है उस समय कम्प्यूटर में पड़ी सी डी को निकाल लेना ही ठीक माना जाता है। यदि हम कम्प्यूटर से सी डी नहीं निकालते हैं तो यह स्वतः ही डिस्क में बूट होने लगती है, जिससे वायरस अटैक की सम्भावना बढ़ जाती है।

कम्प्यूटर सिक्योरिटी के लिए खतरा : मालवेयर

(Threats to Computer Security : Malware)

मालवेयर का अर्थ है द्वेषपूर्ण (दुष्ट) सॉफ्टवेयर (Malicious Software)। ये उस प्रकार के प्रोग्रामों का सम्मिलित रूप हैं, जिनका प्रमुख कार्य होता है कम्प्यूटर को हानि पहुँचाना; जैसे- वायरस, वामर्स, स्पाईवेयर इत्यादि। इनमें से कुछ प्रमुख तत्वों का विवरण इस प्रकार हैं

85

वायरस (Virus)

वायरस वो प्रोग्राम है जो कम्प्यूटर पर नकारात्मक प्रभाव डालते हैं। ये पीसी पर कण्ट्रोल हासिल करके उनसे असामान्य व विनाशकारी कार्यों को करवाते हैं।

वायरस स्वतः ही अपने आप को सिस्टम में कॉपी कर लेते हैं व आगे संक्रमण हेतु अन्य प्रोग्रामों के साथ स्वतः ही जुड़ जाते हैं। वायरस

कम्प्यूटर सॉफ्टवेयर के किसी भी हिस्से; जैसे- बूट ब्लॉक, ऑपरेटिंग सिस्टम, सिस्टम एरिया, फाइल्स तथा अन्य एप्लीकेशन प्रोग्राम इत्यादि को क्षति पहुँचा सकते हैं।

कुछ सामान्य वायरसों के प्रकार निम्नलिखित हैं

(i) डायरेक्ट एक्शन वायरस (**Direct Action Virus**)

यह वायरस किसी फाइल में होता है और जब उस फाइल का उपयोग किया जाता है तब यह वायरस स्वयं को क्रियान्वित कर देता है। यह वायरस केवल उन्हीं फाइलों को संक्रमित करता है, जिनके फोल्डर (autoexec.bat) फाइल पथ पर वर्णित होते हैं उदाहरण- Vienna Virus

(ii) ओवर राइट वायरस (**Over right Virus**)

यह संक्रमित फाइलों में रखे हुए डेटा व सूचना को डिलीट कर देता है।

उदाहरण Way, Trivial. 88-D इत्यादि।

(iii) बूट सेक्टर वायरस (**Boot Sector Virus**)

इसे मास्टर बूट सेक्टर वायरस या मास्टर बूट रिकॉर्ड वायरस भी कहा जाता है। यह सामान्यतः कम्प्यूटर के बूट्स-अप होने पर फैलता है, क्योंकि यह वायरस हार्ड डिस्क या फ्लॉपी डिस्क के मास्टर बूट रिकॉर्ड के बूट सेक्टर में होता है।

उदाहरण Anti exe इत्यादि।

(iv) मैक्रो वायरस (**Macro Virus**)

ये केवल उन्हीं एप्लीकेशनों तथा प्रोग्रामों को संक्रमित करता हैं,

जिनमें, .doc, .xls, .pps इत्यादि मैक्रोस होते हैं।

उदाहरण Melissa.A इत्यादि।

(v) फाइल सिस्टम वायरस (File System Virus)

यह किसी भी फाइल के डायरेक्टरी पथ को बदलकर मैमोरी प्रबन्धन में गड़बड़ कर देता है। इसे क्लस्टर वायरस या डायरेक्टरी वायरस भी कहते हैं। उदाहरण- Dir-2 Virus इत्यादि।

(vi) पॉलीमॉर्फिक वायरस (Polymorphic Virus)

यह जब भी किसी सिस्टम को संक्रमित करता है तो अपने आपको प्रत्येक बार एनकोड या एनक्रिप्ट करता है। इस प्रकार वायरस की ज्यादा-से-ज्यादा कॉपी तैयार हो जाती हैं। उदाहरण Elkern, Tuareg इत्यादि।

(vii) फैट वायरस (FAT Virus)

यह फाइलों की लोकेशन व अप्रयोगित मैमोरी स्थान के बारे में सभी प्रकार की जानकारियों को संग्रहीत करने के लिए प्रयोग होता है। उदाहरण- लिंक वायरस इत्यादि।

(viii) वेब स्क्रिप्टिंग वायरस (Web Scripting Virus)

कई वेबसाइटों में रोचक सूची को डालने के लिए कठिन कोड का इस्तेमाल होता है यह इन्हीं कोड्स को संक्रमित करता है। उदाहरण J.S. Fort night इत्यादि।

(ix) मल्टीपार्टाइट वायरस (Multipartite Virus)

यह वायरस कई तरीकों से फैलता है; जैसे- ऑपरेटिंग सिस्टम इन्स्टॉल करने पर आदि। उदाहरण flip इत्यादि।

(x) रेजिडेंट वायरस (Resident Virus)

यह अपने आप को सिस्टम की मेमोरी में स्थिर कर लेता है तथा ऑपरेटिंग सिस्टम के चलने पर सक्रिय हो जाता है। और खोले जाने वाली सभी फाइलों को प्रभावित करता है। यह रैम (RAM) में छुपा होता है। तथा द्वेषपूर्ण कोड (Malicious Code) के निष्पादन के बाद भी वही रहता है।

उदाहरण के लिए- Randex, Meve इत्यादि।

कुछ प्रमुख कम्प्यूटर वायरस निम्नलिखित हैं

वर्ष	नाम	वर्ष	नाम
1971	क्रीपर	2003	ब्लास्टर
1982	ईलके क्लोनर	2004	सैंसर
1988	द मॉरीस इंटरनेट वॉर्म	2010	स्टक्सनेट
1999	मेल्लिसा	2011	ट्रॉजन
2000	आई लव यू	2012	रूटकिट
2001	कोड रेड	2014	जैनेरिक पी यू पी
2003	एस क्यू एल स्लैमर	2014	नेट वॉर्म

2. वॉर्मस (Worms)

कम्प्यूटर वॉर्म एक अकेला ऐसा मालवेयर प्रोग्राम है, जोकि दूसरे कम्प्यूटरों में अपने आप फैलाने के लिए कॉपी करता है। वॉर्मस को ढूँढ पाना अत्यन्त कठिन है, क्योंकि ये अदृश्य फाइलों के रूप में होते हैं। ये कम्प्यूटर नेटवर्क में बैडविड्थ को नष्ट करके भी क्षति पहुँचाते हैं।

उपयोग (Unauthorized Access) की सुविधा प्रदान करता है। ये कम्प्यूटर वायरस की भाँति अपने आप को दूसरी फाइलों में सम्मिलित करने का प्रयास नहीं करते। ये सॉफ्टवेयर इंटरनेट चालित ऐप्लिकेशनों द्वारा टारगेट कम्प्यूटरों तक पहुँच सकते हैं। उदाहरण- Beast, Sub 7. Zeus, Zero Access Rootkit इत्यादि।

4. स्पाईवेयर (Spyware)

यह प्रोग्राम किसी भी कम्प्यूटर सिस्टम पर इन्स्टाल्ड होता है, जोकि सिस्टम के मालिक की सभी गतिविधियों की निगरानी तथा गलत तरीके से आगे प्रयोग होने वाली सभी जानकारी को एकत्रित करता है। इनका प्रयोग हम कानूनी या गैरकानूनी उद्देश्यों के लिए कर सकते हैं। स्पाईवेयर व्यक्तिगत सूचनाओं को दूसरे व्यक्ति के कम्प्यूटर पर इंटरनेट के माध्यम से संचरित कर सकते हैं। उदाहरण- Cool Web Search, Zango, Keyloggers, Zlob Trojan इत्यादि।

वायरस के प्रभाव (Effects of Virus)

कम्प्यूटर पर वायरस विभिन्न प्रकार के प्रभाव डाल सकते हैं। वायरसों के प्रकार पर निर्भर होते हुए, कुछ वायरसों के प्रभाव इस प्रकार हैं

1. उपयोगकर्ता के कार्य की निगरानी करना।
2. कम्प्यूटरों की दक्षता को कम करना।
3. लोकल डिस्क पर उपस्थित सभी डेटा को नष्ट करना।
4. कम्प्यूटर नेटवर्क्स व इंटरनेट कनेक्शन को प्रभावित करना।
5. मैमोरी के आकार को बढ़ाना या घटाना।
6. विभिन्न प्रकार के त्रुटि सन्देशों को डिस्प्ले करना।
7. पी सी सेटिंग्स को बदलना।
8. अनचाहे एडवरटाइजों के ऐरे को डिस्प्ले करना।
9. बूट टाइम को बढ़ाना इत्यादि।

मालवेयर दोष के लक्षण

(Symptoms of Malware Attack)


किसी भी सिस्टम के मालवेयर द्वारा प्रभावित होने को निम्न लक्षणों द्वारा समझा जा सकता है

- (i) बेमेल सन्देशों को कम्प्यूटर स्क्रीन पर डिस्प्ले करना।
- (ii) कुछ फाइलों का खो जाना।
- (iii) सिस्टम का धीमा चलना।
- (iv) पी सी का क्रैश होकर बार-बार रीस्टार्ट होना।
- (v) माउस के पाइन्टर का ग्राफिक बदलना।
- (vi) ड्राइव्स का प्रवेश योग्य न होना इत्यादि।
- (vii) एण्टीवायरस सॉफ्टवेयर का क्रियान्वयन या इन्स्टालेशन न होना।


उदाहरण- Begle, I love you, Morris, Nimda इत्यादि।

इन्हें भी जानें

3. ट्रॉजन (Trojans)

 **साइबर बुली (Cyber Bully)** यह एक व्यक्ति (बुली) होता है, जो ट्रॉजन या ट्रॉजन हॉर्स (Trojan Horse) एक प्रकार का नॉन-शेल्व किंसी व्यक्ति को ऑनलाइन विभिन्न तरीकों (जैसे- स्पैमिंग, बदनाम करना रेपलिकेटिंग मालवेयर है। जोकि किसी भी इच्छित कार्य को पूरा करते हुए या पीड़ित की नकारात्मक नकल करना) से पीड़ित करता है उसे साइबर प्रतीत होता है पर ये उपयोगकर्ता के कम्प्यूटर सिस्टम पर अनाधिकृत बुली कहते हैं।

86

 **ईगोसर्फर (Egosurfer)** वह व्यक्ति जो इंटरनेट पर किसी भी व्यक्ति विशेष के सम्बन्ध स्वयं से या किसी और से जोड़ने के लिए जानकारी एकत्रित करता है।

- ✍ **फ्लैमर (Flammer)** यह वो व्यक्ति है जो किसी फोरम या इंटरनेट मैसेज बोर्ड पर निम्न स्तरीय या बेइज्जती से भरी हुई टिप्पणी लिखता है उसे फ्लैमर कहते हैं।
- ✍ **ग्रीफर (Griefer)** ऑनलाइन गेम का एक खिलाड़ी जो दूसरे खिलाड़ियों को परेशान करता है उसे ग्रीफर कहते हैं।

कम्प्यूटर सिक्योरिटी के लिये कुछ अन्य खतरें

(Some Other Threats to Computer Security)

- (a) **स्पूफिंग (Spoofing)** अनाधिकृत (Unauthorized) डेटा को उसके अधिकृत (Authorized) उपयोगकर्ता की जानकारी के बिना एक्सेस करने की तकनीक को स्पूफिंग कहते हैं। यह नेटवर्क पर विभिन्न संसाधनों को एक्सेस करने के लिए भी इस्तेमाल होती है। आई पी स्पूफिंग (IP Spoofing) भी इसका एक प्रकार है।
- (b) **सलामी तकनीक (Salami Techniques)** इसके अन्तर्गत सिस्टम द्वारा सँभाली गई धनराशि के एक बड़े हिस्से से छोटे हिस्से को अलग किया जाता है।
- (c) **हैकिंग (Hacking)** नेटवर्क से जुड़े कम्प्यूटर में घुसपैठ करने की प्रक्रिया को हैकिंग कहते हैं। हैकिंग DOS (Denial of- Service) अटैक का परिणाम भी हो सकता है। यह कम्प्यूटर के सभी संसाधनों को वैध यूजरों द्वारा इस्तेमाल करने से दूर रखती है। इस प्रक्रिया को अन्तिम चरण तक पहुँचाने वाले व्यक्ति को **हैकर** कहते हैं।
- (d) **क्रैकिंग (Cracking)** यह कम्प्यूटर में किसी भी प्रकार के सॉफ्टवेयर या उनके घकटों को तोड़ने की प्रक्रिया है। इसमें पासवर्ड क्रैकर, ट्रोजन्स, वायरसेज, वार डायलर इत्यादि सम्मिलित हैं।
- (d) **फिशिंग (Phishing)** कम्प्यूटर की संवेदनशील जानकारियों को

धोखेबाजी से प्राप्त करने की कोशिश करना इत्यादि विशेषताओं को फिशिंग कहते हैं। इसके अन्तर्गत पासवर्ड्स, क्रेडिट कार्ड डिटेल्स इत्यादि सम्मिलित हैं। यह एक प्रकार का इंटरनेट फ्रॉड (धोखा) है, जिसमें उपयोगकर्ता को बहकाकर उसके सभी क्रेडिटिशियलों को प्राप्त कर लिया जाता है।

- (f) **स्पैम (Spam)** यह एक प्रकार से मैसेजिंग सिस्टम्स का दुरुपयोग है, जिसके अन्तर्गत अनचाहे सन्देशों को ई-मेलों के रूप में भेजा जाता है।
- (g) **एडवेयर (Adware)** यह एक ऐसा सॉफ्टवेयर पैकेज है, जोकि एडवरटाइजमेन्ट को स्वतः ही टुकड़े-टुकड़े कर स्क्रीन पर दिखाया है। इसे अधिकांशतः अनचाहें एडवरटाइजमेन्टों को दिखाने के लिए इस्तेमाल किया जाता है।
- (h) **रूटकिट्स (Rootkits)** यह एक प्रकार का मालवेयर है, जिसके द्वारा किसी कम्प्यूटर सिस्टम में एडमिनिस्ट्रेटिव स्तर की नियंत्रितता प्राप्त की जाती है व इसकी जानकारी किसी को भी नहीं होती है। रूटकिट्स को निकालना बेहद मुश्किल होता है तथा कभी-कभी पूर्णतः ऑपरेटिंग सिस्टम के पुनः इन्स्टॉलेशन की भी आवश्यकता होती है।

कम्प्यूटर सिक्योरिटी से सम्बन्धित खतरों का समाधान

(Solutions to Computer Security Threats)

कम्प्यूटर सिस्टम को अवैध-उपयोगकर्ता से बचाने के लिए अभी तक कुछ रक्षा बचाव बनाए गए हैं, जोकि इस प्रकार हैं

- (a) **एण्टीवायरस सॉफ्टवेयर (Antivirus Software)** ये उस प्रकार के सॉफ्टवेयर होते हैं, जिनका प्रयोग कम्प्यूटर को वायरस, स्पाईवेयर, वॉर्मस, ट्रोजन इत्यादि से बचाना होता है। इसमें वे प्रोग्राम भी सम्मिलित होते हैं, जिनका कार्य वायरस या अन्य मालवेयर को ढूँढकर खत्म करना होता है। Avast, Avg, Kaspersky, Symantec,

Norton, Mefee इत्यादि, लोकप्रिय एण्टीवायरस सॉफ्टवेयर हैं।

- (b) **डिजिटल सिग्नेचर (Digital Signature)** यह सिग्नेचर (हस्ताक्षर) का डिजिटल रूप है जिसे प्रेषित किए गए सन्देश को प्रमाणित करने के लिए प्रयोग किया जाता है तथा यह डाक्यूमेन्ट के ऑरिजिनल होने को भी सुनिश्चित करता है।
- (c) **फायरवॉल (Firewall)** फायरवॉल या तो सॉफ्टवेयर या फिर हार्डवेयर आधारित हो सकता है, जोकि नेटवर्क को सुरक्षित रखने में सहायताप्रद होता है। इसका प्राथमिक उद्देश्य इनकमिंग तथा आउटगोइंग नेटवर्क ट्रैफिक को, डेटा पैकेट्स विश्लेषण द्वारा नियन्त्रित करना है। फायरवॉल में प्रॉक्सी सर्वर के साथ कार्य करना या सम्मिलित होना भी उल्लेखनीय है, ताकि वह नेटवर्क की सभी जरूरतों को वर्कस्टेशन यूजर्स के लिए पूरा कर सके।
- (d) **डिजिटल सर्टिफिकेट (Digital Certificate)** डिजिटल सर्टिफिकेट सिम्योरिटी उद्देश्यों के लिए इलेक्ट्रॉनिक सन्देशों में प्रयुक्त होने वाली कॉपी है। डिजिटल सर्टिफिकेट, किसे प्रेषित किया गया था व इसे किसने प्रेषित किया था इत्यादि जानकारीयाँ इसमें सम्मिलित होती है।

कम्प्यूटर सिम्योरिटी सम्बन्धित जानकारीयाँ

(Computer Security Related Informations)

1. **प्रॉक्सी सर्वर (Proxy Server)** प्रॉक्सी सर्वर को 'प्राक्सी अथवा एप्लीकेशन-लेवल गेटवे' भी कहा जाता है। यह उपयोगकर्ता एवं सर्वर के मध्य कार्य करता है। यह नेटवर्क के सही एड्रेस को छिपाता है और नेटवर्क में आने-जाने वाले सभी सन्देशों को इंटरसेप्ट करता है।
2. **एप्लीकेशन गेटवे (Application Gateway)** यह कुछ विशिष्ट एप्लीकेशनों पर सुरक्षा कार्यविधि को लागू करता है। इन विशिष्ट

एप्लीकेशनों में फाइल ट्रांसफर प्रोटोकॉल तथा टेलनेट सेवाएँ इत्यादि सम्मिलित हैं।

87

3. **टाइम बम (Time Bomb)** यह सॉफ्टवेयर का हिस्सा है, जोकि किसी विशेष समय पर सक्रिय होता है।
4. **लॉजिक बम (Logic Bomb)** यह एक कोड होता है, जिसे कम्प्यूटर की मैमोरी में जान-बूझकर डाला जाता है। जोकि अनुकूल परिस्थितियों के मिलते ही हानिकारक रूप से सक्रिय हो जाते हैं। ये कोड अपनी नकल तैयार करने में सक्षम नहीं होते हैं।
5. **पैचस (Patches)** यह सॉफ्टवेयर का एक ऐसा भाग होता है जिसे उस सॉफ्टवेयर में सुधार करने के लिए बनाया जाता है।
6. **छद्मवेश (Masquerading)** इसमें हमलावार वैध उपयोगकर्ता होने का अभिनय करता है व अवैध रूप से विशेषाधिकार प्राप्त कर लेता है।
7. **निगरानी रखना (Eavesdropping)** इसमें हमलावर संचरित होने वाले सन्देशों के कण्टेंट की निगरानी करता है।

पासवर्ड (Password)

यह एक प्रकार का गोपनीय शब्द या कैरेक्टर्स की एक स्ट्रिंग है। जिसे उपयोगकर्ता को प्रमाणित करने के लिए प्रयोग किया जाता है, ताकि उपयोगकर्ता की पहचान या एक्सेस स्वीकृति को सत्यापित किया जा सके व संसाधनों के एक्सेस को प्राप्त किया जा सके।

पासवर्ड के सामान्यतः दो प्रकार होते हैं,

- (a) **कमजोर पासवर्ड (Weak Password)** इन्हें आसानी से याद किया जा सकता है; जैसे कि- नाम, जन्म दिवस, फोन नम्बर आदि।
- (b) **मजबूत पासवर्ड (Strong Password)** ये एल्फाबेट्स तथा संकेतों का कॉम्बिनेशन है जिसे तोड़ पाना बेहद मुश्किल है।

फाइल एक्सेस परमिशन

(File Access Permission)

अधिकांश रूप से वर्तमान फाइल सिस्टम में अनुमति को प्रदान करने के कई तरीके या अधिकार होते हैं, जिन्हें केवल कुछ खास उपयोगकर्ता और उपयोगकर्ताओं का ग्रुप ही एक्सेस कर सकता है।

ये तीन विशेष अनुमति निम्न हैं

1. **रीड परमिशन (Read Permission)** यदि आप को किसी फाइल को रीड करने की अनुमति है तो आप सिर्फ उसके कन्टेंट्स को देख सकते हैं।
2. **राइट परमिशन (Write Permission)** यह उपयोगकर्ता को फाइल के कन्टेंटों को रिमूव या उसमें बदलाव इत्यादि करने की अनुमति देता है।
3. **एक्जीक्यूट परमिशन (Execute Permission)** यह उपयोगकर्ता को फाइल को मात्र क्रियान्वित करने की अनुमति देता है।

इन्हें भी जानें

- ✂ वायरस का पूरा नाम **वाइटल इन्फॉर्मेशन रिसोर्स अण्डर सेज (Vital information resource under siege)** है।
- ✂ सबसे पहला बूट सेक्टर पीसी वायरस '**ब्रेन**' नाम का था जिसकी पहचान वर्ष 1986 में की गई।

- ✂ 'पे-लोड' एक वॉर्म के रूप में तैयार किया गया एक कोड है, जिसका डिजाइन वॉर्म से भी बड़े पैमाने पर प्रसार के उद्देश्य से किया गया।
- ✂ क्रीपर वर्ष 1971 में बी बी एन टेक्नोलॉजिस पर बॉब थॉमस द्वारा लिखित एक सेल्फ रिप्लेकिंग वायरस प्रोग्राम था।
- ✂ 'इलके क्लोनर' पहला ऐसा कम्प्यूटर प्रोग्राम था, जो 'इन दि वाइल्ड' में प्रकट करने के लिए बनाया गया था।
- ✂ गैमिया वायरस रिमूवेबल फ्लैश ड्राइव के माध्यम से प्रसारित होता है।
- ✂ भारत में सर्वप्रथम दिखाई देने वाला वाइरस 'हैप्पी बर्थडे जोशी' है।
- ✂ **ट्रांसपोर्ट लेयर सिक्योरिटी प्रोटोकॉल** (Transport layer security protocol) TLS एक क्रिप्टोग्राफिक प्रोटोकॉल है जो सुरक्षित HTTP कनेक्शन प्रदान करता है व गोपनीयता और डेटा इन्टिग्रिटी के साथ संवाद करने के लिए दोनों पार्टियों को सक्षम करता है।
- ✂ **नूब (Noob)** एक नया या अप्रशिक्षित व्यक्ति जो वेबसाइट के नियमों को नहीं जानता या उसने हाल ही में ज्वाइन किया हो, नूब कहलाता है।
- ✂ **ट्रॉल (Troll)** वह व्यक्ति जो फोरम पर या चैटिंग के दौरान किसी की कॉपी, मीमिक्री करके अथवा किसी अन्य कार्य से बदनामी करता है ट्रॉल कहलाता है।