એકમ 16

નેટવર્ક એપ્લિકેશન, વાઇરસ અને સિક્યોરિટી

(Network Application, Virus and Security)

રૂપરેખા

16.0 ઉદ્દેશો (Objective)

આ એકમના અંતે તમે –

- નેટવર્ક એપ્લિકેશન સમજી શકશો.
- કમ્પ્યૂટર સુરક્ષાના અલગ અલગ તબક્કાઓને વ્યાખ્યાયિત કરી શકશો.
- કમ્પ્યૂટરમાં થતો સુરક્ષાભંગ સમજી શકશો.
- સુરક્ષાના માપદંડો અંગે ખ્યાલ મેળવી શકશો.
- ભૌતિક અને સોફ્ટવેર સુરક્ષા સમજી શકશો.
- વાઇરસથી બચવાના ઉપાયો જાણી શકશો.

16.1 પ્રસ્તાવના (Introduction) :

આ એકમમાં નેટવર્ક એપ્લિકેશન, તેમાં આવતા વાઇરસ અને તેની સુરક્ષા માટે સિક્યોરિટી અંગે અભ્યાસ કરીશું આપણે કમ્પ્યૂટર ઉપર વધુ ભાર આપીશું. જોકે આપણે અન્ય મોટા કમ્પ્યૂટરને લાગુ પાડી શકાય તેવા માપદંડો પણ જોઈશું. આપણે કમ્પ્યૂટર સુરક્ષાના સંચાલનની ચર્ચા કરવાના છીએ. તેથી અગત્યના કેટલાક શબ્દો વ્યાખ્યાયિત કરીશું.

16.2 નેટવર્ક એપ્લિકેશન (Network Application)

નેટવર્ક એપ્લિકેશનના વિકાસના મૂળમાં એવો પ્રોગ્રામ લખવાનું છે, જે જુદી જુદી અંતિમ સિસ્ટમ પર ચાલે છે અને નેટવર્ક પર એકબીજા સાથે વાતચીત કરે છે. નેટવર્ક એપ્લિકેશનના વિકાસના મૂળમાં એવા પ્રોગ્રામ લખવાનું છે જે જુદી જુદી અંતિમ સિસ્ટમ્સ પર ચાલે છે અને નેટવર્ક પર એકબીજા સાથે વાતચીત કરે છે. તમારી નવી એપ્લિકેશન વિકસિત કરતી વખતે, તમારે સોફ્ટવેર લખવાની જરૂર છે જે બહુવિધ મશીનો પર ચાલશે, અને રાઉટર્સ અથવા ઈથરનેટ સ્વીચો જેવા નેટવર્ક કોર ડિવાઈસીસ નીચલા સ્તરો પર કાર્ય કરે છે, ખાસ કરીને નેટવર્ક સ્તર પર અથવા નીચે. અંતિમ સિસ્ટમોમાં એપ્લિકેશન સોફ્ટવેરની પુષ્ટિ કરવાથી વિશાળ એરેના ઝડપી વિકાસ અને જમાવટની સુવિધા મળી છે.

16.2.1 નેટવર્ક એપ્લિકેશનનાં ઉદાહરણો

- ઈ-મેઈલ
- વેબ
- ઈન્સ્ટન્ટ મેસેજિંગ
- દૂરસ્થ લોગિન જેમ કે ટેલનેટ અને એસએસએચ
- પી ટુ પી ફાઈલ શેરિંગ
- બે કમ્પ્યૂટર (એફટીપી) પરના બે ખાતાઓ વચ્ચે ફાઈલ સ્થાનાંતરણ
- મલ્ટિ-યુઝર નેટવર્ક નેટવર્ક
- સ્ટોર કરેલી વીડિયો ક્લિપ્સનું પ્રસારણ
- ઈન્ટરનેટ ફોન
- રીઅલ ટાઈમ વીડિયો કોન્ફરન્સિંગ

16.3 વાઈરસ (Virus)

કમ્પ્યૂટર વાઈરસ એ કમ્પ્યૂટર પ્રોગ્રામ છે જે પોતાની મેળે ક્ષતિગ્રસ્ત કમ્પ્યૂટરમાંથી કમ્પ્યૂટર માલિકની પરવાનગી વગર આપોઆપ કોપી થઈ જાય છે. વાઈરસની વ્યાખ્યા સામાન્ય છે પરંતુ તેને માલવેર (Malware) એડવેર (Adware) અને સ્પાયવેર (Spyware) પ્રોગ્રામો માટે પણ વાપરવામાં આવે છે જે ખોટું છે. આ પ્રોગ્રામોમાં ફરીથી ઉત્પન્ન કરવાની શક્તિ હોતી નથી. સાચો વાઈરસ તો એક કમ્પ્યૂટરમાંથી બીજા કમ્પ્યૂટરમાં એક્ઝ્યુટેબલ કોડ દ્વારા ફેલાય છે. જ્યારે હોસ્ટ તેને ટાર્ગેટ કમ્પ્યૂટર સુધી પહોંચાડે છે. દાખલા તરીકે, ઉપભોક્તા તેને નેટવર્ક અથવા ઈન્ટરનેટ વડે મોકલે છે અથવા રીમુવેબલ માધ્યમ દ્વારા જેમ કે ફ્લોપી ડિસ્ક, સીડી, ડીવીડી અથવા યુએસબી ડ્રાઈવ દ્વારા પહોંચાડી શકે છે. નેટવર્ક ફાઈલ સિસ્ટમમાં પડેલી ફાઈલને ક્ષતિગ્રસ્ત કરીને વાઈરસ ફેલાય છે. વાઈરસ ફેલાવવાની આદર્શ પદ્ધતિઓમાંની એક ઈ-મેઈલ્સ દ્વારા છે - ઈમેઈલમાં જોડાણ

ખોલીને, ચેપગ્રસ્ત વેબસાઈટની મુલાકાત લેવી, એક્ઝેક્યુટેબલ ફાઈલ પર ક્લિક કરવું અથવા ચેપગ્રસ્ત જાહેરાત જોવી વગેરેથી તમારી સિસ્ટમ પર વાઇરસ ફેલાય છે.

વાઇરસના પ્રકાર :

વાઇરસના મુખ્ય ત્રણ પ્રકાર પાડી શકાય.

1. બુટસેક્ટર વાઇરસ
2. મેક્રો વાઇરસ
3. ઈમેલ વાઇરસ

1. **બુટસેક્ટર વાઇરસ :** આ પ્રકારના વાઇરસ હાર્ડડિસ્ક તેમજ કમ્પ્યૂટર ચાલુ કરવા માટે વપરાતા ફ્લોપી, પેનડ્રાઈવ જેવા સેકન્ડરી સ્ટોરેજના મુખ્ય ગણાતા બુટ રેકોર્ડને નુકસાન કરે છે. આ વાઇરસ કમ્પ્યૂટર ચાલુ થતા જ એનો અમલ થઈ કમ્પ્યૂટરને ચાલુ થતું જ અટકાવી દે છે.

2. **મેક્રો વાઇરસ :** આ વાઇરસ એ મોક્રો કે સ્ક્રિપ્ટ છે તે પોતાને ટેમ્પ્લેટ કે ફાઈઅલ સાથે જોડી દે છે અને એ ફાઈલ ઓપન કરતાં જ એનો અમલ કરવાનું શરૂ કરી દે છે. દા.ત. વર્ડ ફાઈલમાં ન જોઈતા શબ્દો ઉમેરી દે છે.

3. **ઈમેલ વાઇરસ :** ઈમેલ સંદેશાની આજુબાજુ ફર્યા કરે અને એડ્રેસ બુકમાંથી સરનામા લઈ જાતે જ ઈમેલ મોકલે છે અને એકમાંથી બીજા કમ્પ્યૂટરમાં પોતાનો ફેલાવો કરે છે.

16.3.1 વાઇરસનો ઈતિહાસ :

બી.બી.એન. ટેક્નોલોજીસના એન્જિનિયર રોબર્ટ થોમસને વર્ષ 1971માં પ્રથમ કમ્પ્યૂટર વાઇરસનો આવિષ્કાર કર્યો હતો. પ્રથમ વાઇરસને **"ક્રીપર"** વાઇરસ નામ આપવામાં આવ્યું હતું, અને આરપાનેટના મેઈનેમ કમ્પ્યૂટર પર થોમસ દ્વારા હાથ ધરવામાં આવેલા પ્રાયોગિક પ્રોગ્રામમાં કમ્પ્યૂટર સ્ક્રીનો પર સંદેશ પ્રદર્શિત કરાયેલ : "હું ક્રિપર છું; જો તમે મને પકડી શકો તો પકડો."

કમ્પ્યૂટર વાઇરસના ઇતિહાસમાં સંભવિત સૌ પ્રથમ મોટો વાઇરસ **"એલ્ક ક્લોનર"** હતો. એલ્ક ક્લોનર ફ્લોપી ડિસ્ક દ્વારા એપલ ઓપરેટિંગ સિસ્ટમોને ચેપ લગાવે છે. ચેપગ્રસ્ત એપલ કમ્પ્યુટર્સ પર પ્રદ એક રમૂજી સંદેશ હતો. રિચાર્ડ સ્કેન્ટાએ 1982માં કિશોર વયે આ વાઇરસ વિકસિત કર્યો હતો. કમ્પ્યૂટર વાઇરસને એક મજાક તરીકે ડિઝાઈન કરવામાં આવ્યા હોવા છતાં, તે પણ સમજાયું કે કેવી રીતે દૂષિત પ્રોગ્રામ કમ્પ્યૂટરની મેમરીમાં ઈન્સ્ટોલ કરી શકાય છે અને વપરાશકર્તાઓને તે ચેપી પ્રોગ્રામને દૂર કરતા અટકાવી શકે છે.

1983માં ફ્રેડ કોહેન એ **"કમ્પ્યૂટર વાઇરસ - થિયરી અને પ્રયોગો"** નામના એક શૈક્ષણિક પેપર લખવાનો પ્રયાસ કર્યો, જેમાં દૂષિત કાર્યક્રમો વિશે વિગતો આપી. ત્યારબાદ "કમ્પ્યૂટર વાઇરસ" શબ્દ અમલમાં આવ્યો.

16.3.2 વાઇરસ ચેપના ચિન્હો :

કોઈપણ કમ્પ્યૂટર વપરાશકર્તા માટે આ ચેતવણી ચિહ્નોથી વાકેફ હોવું ખૂબ જ મહત્વપૂર્ણ છે.

- સિસ્ટમની ધીમી કામગીરી.
- કમ્પ્યૂટર સ્ક્રીન પર બિનજરૂરી માહિતી વારંવાર પ્રદર્શિત કરે છે.
- અમુક કાર્યક્રમો તેમની પોતાની રીતે કામ કરવા લાગે છે.
- ફાઈલ તેમના પોતાના જેવી નવી ફાઈલો અથવા પ્રોગ્રામ્સ કમ્પ્યૂટરમાં બનાવી દે છે.
- ફાઈલો, ફોલ્ડરો અથવા પ્રોગ્રામ્સ ડીલીટ અથવા દૂષિત થઈ ગયા હોય છે.
- હાર્ડ ડ્રાઈવનો અવાજ કરવો.

જો તમે ઉપરોક્ત કોઈ પણ ચિહ્નો પર આવે છે, તો પછી તમારા કમ્પ્યૂટરને વાઇરસ અથવા માલવેરથી ચેપ લાગવાની સંભાવના છે.

16.3.3 નુકસાનકારક સોફ્ટવેર :

કેટલાક પ્રોગ્રામ એવા હોય છે જે કમ્પ્યૂટર માટે નુકસાનકારક હોય છે, જે ખરેખર વાઇરસ ગણાતા નથી પરંતુ આવા વાઇરસ સોફ્ટવેરમાં છુપાયેલા હોય છે જે ઈન્ટરનેટ પરથી ડાઉનલોડિંગ વખતે પ્રસરે છે.

માલવેર : આ એક પ્રોગ્રામ, ફાઈલ કે સૂચનાઓનો સમૂહ છે, જે ઉપયોગકર્તાની પરવાનગી વગર કમ્પ્યૂટરને નુકસાન પહોંચાડે છે.

સ્પાયવેર : આ એક એવો પ્રોગ્રામ છે જે આપણા કમ્પ્યૂટરની માહિતી ભેગી કરી અન્ય જાહેરાત કરતી કંપની અને રસ ધરાવતા વ્યક્તિઓને પહોંચાડવા માટે આપણા કમ્પ્યૂટરમાં ડાઉનલોડિંગ વખતે પોપ-અપ વિન્ડોમાં કોઈ વિકલ્પ ક્લિક કરવાથી આવી જાય છે.

વોર્મ : આ એક એવો પ્રોગ્રામ છે જે સુધારા વધારાની જગ્યાએ વારંવાર પોતાની વધુ નકલો બનાવતો જાય છે, અને કમ્પ્યૂટર ધીમું પડી બંધ થઈ જાય છે.

ટ્રોજન હોર્સ : આનો મુખ્ય ઉદ્દેશ હુમલાખોરોને ગુપ્ત માહિતી પહોચાડવાનો છે. જે કમ્પ્યૂટર લોગીન કરી યુઝરનેમ પાસવર્ડ વગેરે ચોરી કરી અન્ય વ્યક્તિને પહોંચાડી દે છે.

બ્રાઉઝર હાઈજેકર : આ એક એવો પ્રયોગ છે, જે બ્રાઉઝરની ગોઠવણી બદલી અન્ય વેબસાઈટ ચાલુ કરી દે છે તેમજ ડિફોલ્ટ હોમ પેજ, સર્ચ પેજ વગેરે બદલી નાખે છે.

16.3.4. વાઈરસ ચેપથી બચવાના ઉપાયો :

- વિલંબ કર્યા વગર તરત જ તમામ આદેશો બંધ કરો અને એન્ટીવાઈરસ સોફ્ટવેર ડાઉનલોડ કરો.
- જો તમને ખાતરી ન હોય કે શું કરવું, તો કોઈ અધિકૃત કમ્પ્યૂટર કર્મચારીઓની સહાય મેળવો.
- સલામત મોડ (સેફ મોડ)નો ઉપયોગ કરી કમ્પ્યૂટરને રીબુટ કરો. સલામત મોડ પર કામ કરવાથી નકારાત્મક ફાઈલોને દૂર કરવામાં મદદ મળે છે, કારણ કે તે ખરેખર ચલાવવામાં આવતી નથી અથવા આ મોડમાં સક્રિય થતી નથી.
- અસ્થાયી ફાઈલોને ડિલીટ કરવી. આ અભિગમ વાઈરસ સ્કેનિંગ પ્રક્રિયાને ઝડપી બનાવવામાં મદદ કરે છે.
- ડિસ્ક ક્લીનઅપ ટૂલ કમ્પ્યૂટર પર તમારી હંગામી ફાઈલોને દૂર કરવામાં મદદ કરે છે.
- એન્ટીવાઈરસ પોગ્રામ કમ્પ્યૂટરમાં દાખલ કરો. તેની સાથે માલવેર સ્કેનર પણ ઈન્સ્ટોલ કરવું.
- સ્કેનડિસ્ટ યુટિલિટીનો ઉપયોગ કરો, જેથી ખરાબ સેક્ટર તથા ફાઈલ, ફોલ્ડર વગેરેની માહિતી જાણી શકાય.
- કમ્પ્યૂટરમાં હાર્ડવેર અને નેટવર્ક માટે ફાયરવોલ ચાલુ રાખવી.
- એન્ટીવાઈરસ તથા એન્ટી માલવેર સોફ્ટવેરનો ઉપયોગ કરવો.
- ઈન્ટરનેટમાં http ને બદલે https પ્રોટોકોલનો ઉપયોગ કરવો.
- ક્લાઉડ એન્ટીવાઈરસનો ઉપયોગ કરવો. દા.ત. પાંડા ક્લાઉડ એન્ટીવાઈરસ, ક્રાઉડ સ્ટ્રાઈક, સીબી ડિફેન્સ, ઈમ્યુનેટ કોમોડો ગ્રૂપ.
- ઓનલાઈન સ્કેનિંગ કરી પ્રોગ્રામ ડાઉનલોડ કરવા.

સોફ્ટવેર સુરક્ષા :

ચાલક પદ્ધતિ, અનુવાદ કે અન્ય સોફ્ટવેર કાર્યક્રમો માટે હંમેશાં મૂળ સોફ્ટવેર જ વાપરો. આવાં સોફ્ટવેર માટે વધુ પૈસા ચૂકવવા પડશે, પરંતુ તેઓ વિશ્વસનીય હશે અને કંઈક તકલીફ થાય તો બદલી શકાય તેવાં હશે. કમ્પ્યૂટરને બંધ કરવા માટે જરૂરી પગલાં લીધા પછી જ કમ્પ્યૂટરને બંધ કરો, જેથી ફાઇલો વગેરે ખરાબ ન થઈ જાય. જો તમે તમારો પોતાનો વિનિયોગ બનાવ્યો હોય તો તેના અમલ માટે ગુપ્ત સંકેતની જોગવાઈ રાખો. ગુપ્ત સંકેત (Password) ટાઇપ કરતી વખતે સ્ક્રીન પર દેખાય નહીં તેની કાળજી રાખવી.

નેટવર્ક સુરક્ષા :

નેટવર્ક તંત્ર માટે વધારે સારી સુરક્ષાની જરૂર પડે છે. કારણ કે આવી પરિસ્થિતિમાં ભૌતિક સુરક્ષાના માપદંડો પણ નકામા બની જાય છે. (તમારા મશીનના રૂમને તાળું મારીને બંધ રાખવો તેમ છતાં નેટવર્ક દ્વારા બીજા કોઈ કમ્પ્યૂટર વડે અન્ય વ્યક્તિ માહિતી મેળવી શકતી હોય તો ગમે તેટલી ભૌતિક સુરક્ષા વ્યર્થ છે.) વળી ક્યારે, કોણ તમારી માહિતી ક્યાંથી મેળવી રહ્યું છે, તે જાણવું ઘણું અઘરું છે. લેનમાં મોટે ભાગે એક સર્વર (Server) હોય છે, જે નેટવર્કમાંની સર્વભાગ્ય માહિતી પોતાની પાસે રાખે છે અને અન્ય કાર્યમથકોની વિનંતીઓને માન આપી તે પૂરી પાડે છે. મોટે ભાગે લેનમાં ગુપ્ત સંકેતની સુવિધા આપવામાં આવે છે. તદુપરાંત નીચે મુજબ અન્ય પગલાં લઈ શકાય.

- સર્વરને દૂર રાખો અને તે મર્યાદિત વ્યક્તિઓથી જ તેનો ઉપયોગ થઈ શકે તેવી ગોઠવણ કરો.
- અમુક પ્રકારના નેટવર્કમાં કમ્પ્યૂટર દ્વારા જે કાર્ય પાર પાડવામાં આવે તેની નોંધ રાખવાની વ્યવસ્થા હોય છે, તેનો ઉપયોગ થઈ શકે છે.
- નેટવર્કના વાયરોમાં અનધિકૃત જોડાણ ન કરી શકાય તે માટે તેમને બને તો એવી રીતે ગોઠવો કે કે જોડાણ અશક્ય બને. શક્ય હોય તો પ્રકાશીય તાર (Optical Fibre)નો પ્રયોગ કરો.
- માહિતી સંચારમાં સંકેતલિપિના પ્રયોગ કરો. જોકે તેનાથી નેટવર્કનો કાર્યભાર વધી જશે.
- ખૂબ સંવેદનશીલ નેટવર્ક માટે પ્રકાશીય તારનો પ્રયોગ કરવો હિતાવહ છે. જોકે તારમાં કઈ રીતે પ્રકાશ ચાલુ બંધ થાય છે તે જો જાણી શકાય તો તેમાંથી પણ માહિતી 'સાંભળી'ને 'ચોરી' શકાય છે.
- પ્રત્યાયનમાં ગુપ્તસંકેત પસાર નહીં થાય તેની કાળજી રાખો. જો તેમ ન કરી શકાય તો ગુપ્તસંકેતોને સાંકેતિક સ્વરૂપ

16.4 સારાંશ (Summary)

આજના આધુનિક યુગમાં કમ્પ્યૂટર એપ્લિકેશનો દ્વારા ઈન્ટરનેટની મદદથી માહિતીનો વિસ્ફોટ થયો છે, તેમાં પણ માહિતી સુરક્ષાની ખાતરી એ દરેક સંસ્થા માટે વધુ ને વધુ અગત્યની બાબત બનતી જાય છે. કમ્પ્યૂટર અને નેટવર્ક પર માહિતી ખોવાય નહીં, બગડી ન જાય, તેનો અનધિકૃત વ્યક્તિ દ્વારા દુરુપયોગ ન થાય કે વચ્ચેથી તેને સાંભળી કે ચોરી ન શકાય તે માટેનાં ઘણાં ટાંચા સાધનો અને રીતો ઉપલબ્ધ છે. જો કાર્યકર્તા કર્મચારીઓમાં સુરક્ષાની ભાવનાનો વિકાસ કરવામાં ન આવે તો સુરક્ષા માટેનાં કોઈ પણ પગલાં સફળ બની શકે નહીં. માહિતી વિજ્ઞાન અને સુરક્ષાની નીતિ ઉપલા સ્તરે વ્યાખ્યાયિત થાય અને તેનું સખતાઈથી પાલન થાય તે તેની સફળતા માટે ખૂબ જરૂરી છે. ખાસ કરીને મોટા તંત્રો માટે ઘણા બધા સુરક્ષા માપદંડો અસ્તિત્વ ધરાવે છે. કમ્પ્યૂટરના વધતા જતા ઉપયોગને ધ્યાનમાં રાખીએ તો કમ્પ્યૂટરની સુરક્ષા તરફ પણ ધ્યાન આપવાની ઝાઝી જરૂર છે. આવા વાઇરસથી બચવા માટે સોફ્ટવેર સુરક્ષા, નેટવર્ક સુરક્ષા, ઈન્ટરનેટ સુરક્ષા, ક્લાઉટ કમ્પ્યૂટિંગ વગેરે પર ધ્યાન આપવાની જરૂર છે.

તમારી પ્રગતિ ચકાસો

નોંધ : (1) નીચે આપેલી જગ્યામાં તમારા ઉત્તર લખો.

(2) એકમનાં અંતે આપેલા ઉત્તરો સાથે તમારા ઉત્તરને સમજાવો.

1. નેટવર્ક એપ્લિકેશન એટલે શું ? તેની ઉદાહરણ આપી ચર્ચા કરો.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

2. કમ્પ્યૂટર વાઇરસ એટલે શું ? તેનાં પ્રકારો સમજાવો.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

3. કમ્પ્યૂટર વાઇરસનો ઇતિહાસ જણાવી તેનાં ચેપ લાગવાનાં લક્ષણોની ચર્ચા કરો.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

4. કમ્પ્યૂટર વાઇરસના ચેપથી બચવાના ઉપાયો જણાવો.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

5. સોફ્ટવેર સુરક્ષા પર ટૂંકનોંધ લખો.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

6. નેટવર્ક સુરક્ષા પર ટૂંકનોંધ લખો.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

7. ક્લાઉડ એન્ટીવાઇરસ સોફ્ટવેરના નામ જણાવો.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

8. ..... એક પ્રોગ્રામ, ફાઇલ કે સૂચનાઓના સમૂહ છે, જે ઉપયોગકર્તાની પરવાનગી વગર કમ્પ્યૂટરને નુકસાન પહોંચાડે છે.

9. ..... મુખ્ય ઉદ્દેશ હુમલાખોરોને ગુપ્ત માહિતી પહોંચાડવાનો છે, જે કમ્પ્યૂટર લોગીન કરી યુઝરનેમ, પાસવર્ડ વગેરે ચોરી કરી અન્ય વ્યક્તિને પહોંચાડી દે છે.

10. ..... એક એવો પ્રોગ્રામ છે, જે સુધારા-વધારાની જગ્યાએ વારંવાર પોતાની વધુ નકલો બનાવતો જાય છે અને કમ્પ્યૂટર ધીમું પડી બંધ થઈ જાય છે.

11. ..... એક એવો પ્રોગ્રામ છે, જે બ્રાઉઝરની ગોઠવણી બદલી અન્ય વેબસાઇટ ચાલુ કરી દે છે તેમજ ડિફોલ્ટ હોમ પેજ, સર્ચ પેજ વગેરે બદલી નાખે છે.

12. .....નો ઉપયોગ કરતી ખરાબ સેક્ટર તથા ફાઇલ ફોલ્ડર વગેરેની માહિતી જાણી શકાય.

13. ..... એ "કમ્પ્યૂટર વાઇરસ - થિયરી અને પ્રયોગો" નામનો એક શૈક્ષણિક પેપર લખવાનો પ્રયાસ કર્યો, જેમાં દૂષિત કાર્યક્રમો વિશે વિગતો આપી.

14. પ્રથમ વાઇરસને ..... નામ આપવામાં આવ્યું હતું

16.5 તમારી પ્રગતિ ચકાસો (ઉત્તર સહિત) (Answer the Self Check Exercise)

1. નેટવર્ક એપ્લિકેશનના વિકાસના મૂળમાં એવો પ્રોગ્રામ લખવાનું છે, જે જુદી જુદી અંતિમ સિસ્ટમ પર ચાલે છે અને નેટવર્ક પર એકબીજા સાથે વાતચીત કરે છે. નેટવર્ક એપ્લિકેશનના વિકાસના મૂળમાં એવા પ્રોગ્રામ લખવાનું છે જે જુદી જુદી અંતિમ સિસ્ટમ્સ પર ચાલે છે અને નેટવર્ક પર એકબીજા સાથે વાતચીત કરે છે. તમારી નવી એપ્લિકેશન વિકસિત કરતી વખતે, તમારે સોફ્ટવેર લખવાની જરૂર છે જે બહુવિધ મશીનો પર ચાલશે, અને રાઉટર્સ અથવા ઈથરનેટ સ્વીચો જેવા નેટવર્ક કોર ડિવાઈસીસ નીચલા સ્તરો પર કાર્ય કરે છે, ખાસ કરીને નેટવર્ક સ્તર પર અથવા નીચે. અંતિમ સિસ્ટમોમાં એપ્લિકેશન સોફ્ટવેરની પુષ્ટિ કરવાથી વિશાળ એરેના ઝડપી વિકાસ અને જમાવટની સુવિધા મળી છે.

   નેટવર્ક એપ્લિકેશનનાં ઉદાહરણો

   - ઈ-મેઈલ
   - વેબ
   - ઈન્સ્ટન્ટ મેસેજિંગ
   - દૂરસ્થ લોગિન જેમ કે ટેલનેટ અને એસએસએચ
   - પી ટુ પી ફાઈલ શેરિંગ
   - બે કમ્પ્યૂટર (એફટીપી) પરના બે ખાતાઓ વચ્ચે ફાઈલ સ્થાનાંતરણ
   - મલ્ટિ-યુઝર નેટવર્ક નેટવર્ક
   - સ્ટોર કરેલી વીડિયો ક્લિપ્સનું પ્રસારણ
   - ઈન્ટરનેટ ફોન
   - રીઅલ ટાઈમ વીડિયો કોન્ફરન્સિંગ

2. કમ્પ્યૂટર વાઇરસ એ કમ્પ્યૂટર પ્રોગ્રામ છે જે પોતાની મેળે ક્ષતિગ્રસ્ત કમ્પ્યૂટરમાંથી કમ્પ્યૂટર માલિકની પરવાનગી વગર આપોઆપ કોપી થઈ જાય છે. વાઇરસની વ્યાખ્યા સામાન્ય છે પરંતુ તેને માલવેર (Malware) એડવેર (Adware) અને સ્પાયવેર (Spyware) પ્રોગ્રામો માટે પણ વાપરવામાં આવે છે જે ખોટું છે. આ

પ્રોગ્રામોમાં ફરીથી ઉત્પન્ન કરવાની શક્તિ હોતી નથી. સાચો વાઈરસ તો એક કમ્પ્યૂટરમાંથી બીજા કમ્પ્યૂટરમાં એક્ઝ્યુટેબલ કોડ દ્વારા ફેલાય છે. જ્યારે હોસ્ટ તેને ટાર્ગેટ કમ્પ્યૂટર સુધી પહોંચાડે છે. દાખલા તરીકે, ઉપભોક્તા તેને નેટવર્ક અથવા ઈન્ટરનેટ વડે મોકલે છે અથવા રીમુવેબલ માધ્યમ દ્વારા જેમ કે ફ્લોપી ડિસ્ક, સીડી, ડીવીડી અથવા યુએસબી ડ્રાઈવ દ્વારા પહોંચાડી શકે છે. નેટવર્ક ફાઈલ સિસ્ટમમાં પડેલી ફાઈલને ક્ષતિગ્રસ્ત કરીને વાઈરસ ફેલાય છે. વાઈરસ ફેલાવવાની આદર્શ પદ્ધતિઓમાંની એક ઈ-મેઈલ્સ દ્વારા છે - ઈમેઈલમાં જોડાણ ખોલીને, ચેપગ્રસ્ત વેબસાઈટની મુલાકાત લેવી, એક્ઝેક્યુટેબલ ફાઈલ પર ક્લિક કરવું અથવા ચેપગ્રસ્ત જાહેરાત જોવી વગેરેથી તમારી સિસ્ટમ પર વાઈરસ ફેલાય છે.

વાઈરસના મુખ્ય ત્રણ પ્રકાર પાડી શકાય.

1. બુટસેક્ટર વાઈરસ
2. મેક્રો વાઈરસ
3. ઈમેલ વાઈરસ

3. બી.બી.એન. ટેક્નોલોજીસના એન્જિનિયર રોબર્ટ થોમસને વર્ષ 1971માં પ્રથમ કમ્પ્યૂટર વાઈરસનો આવિષ્કાર કર્યો હતો. પ્રથમ વાઈરસને **"ક્રીપર"** વાઈરસ નામ આપવામાં આવ્યું હતું, અને આરપાનેટના મેઈનેમ કમ્પ્યૂટર પર થોમસ દ્વારા હાથ ધરવામાં આવેલા પ્રાયોગિક પ્રોગ્રામમાં કમ્પ્યૂટર સ્ક્રીનો પર સંદેશ પ્રદર્શિત કરાયેલ : "હું ક્રિપર છું; જો તમે મને પકડી શકો તો પકડો."

કમ્પ્યૂટર વાઈરસના ઈતિહાસમાં સંભવિત સૌ પ્રથમ મોટો વાઈરસ **"એલ્ક ક્લોનર"** હતો. એલ્ક ક્લોનર ફ્લોપી ડિસ્ક દ્વારા એપલ ઓપરેટિંગ સિસ્ટમોને ચેપ લગાવે છે. ચેપગ્રસ્ત એપલ કમ્પ્યુટર્સ પર પ્રદ એક રમૂજી સંદેશ હતો. રિચાર્ડ સ્ક્રેન્ટાએ 1982માં કિશોર વયે આ વાઈરસ વિકસિત કર્યો હતો. કમ્પ્યૂટર વાઈરસને એક મજાક તરીકે ડિઝાઈન કરવામાં આવ્યા હોવા છતાં, તે પણ સમજાયું કે કેવી રીતે દૂષિત પ્રોગ્રામ કમ્પ્યૂટરની મેમરીમાં ઈન્સ્ટોલ કરી શકાય છે અને વપરાશકર્તાઓને તે ચેપી પ્રોગ્રામને દૂર કરતા અટકાવી શકે છે.

1983માં ફ્રેડ કોહેન એ **"કમ્પ્યૂટર વાઈરસ - થિયરી અને પ્રયોગો"** નામના એક શૈક્ષણિક પેપર લખવાનો પ્રયાસ કર્યો, જેમાં દૂષિત કાર્યક્રમો વિશે વિગતો આપી. ત્યારબાદ "કમ્પ્યૂટર વાઈરસ" શબ્દ અમલમાં આવ્યો.

વાઈરસ ચેપના ચિન્હો :

કોઈપણ કમ્પ્યૂટર વપરાશકર્તા માટે આ ચેતવણી ચિહ્નોથી વાકેફ હોવું ખૂબ જ મહત્વપૂર્ણ છે.

- સિસ્ટમની ધીમી કામગીરી.

- કમ્પ્યૂટર સ્ક્રીન પર બિનજરૂરી માહિતી વારંવાર પ્રદર્શિત કરે છે.
- અમુક કાર્યક્રમો તેમની પોતાની રીતે કામ કરવા લાગે છે.
- ફાઈલ તેમના પોતાના જેવી નવી ફાઈલો અથવા પ્રોગ્રામ્સ કમ્પ્યૂટરમાં બનાવી દે છે.
- ફાઈલો, ફોલ્ડરો અથવા પ્રોગ્રામ્સ ડીલીટ અથવા દૂષિત થઈ ગયા હોય છે.
- હાર્ડ ડ્રાઈવનો અવાજ કરવો.

જો તમે ઉપરોક્ત કોઈ પણ ચિહ્નો પર આવે છે, તો પછી તમારા કમ્પ્યૂટરને વાઇરસ અથવા માલવેરથી ચેપ લાગવાની સંભાવના છે.

4. **વાઇરસ ચેપથી બચવાના ઉપાયો :**

- વિલંબ કર્યા વગર તરત જ તમામ આદેશો બંધ કરો અને એન્ટીવાઇરસ સોફ્ટવેર ડાઉનલોડ કરો.
- જો તમને ખાતરી ન હોય કે શું કરવું, તો કોઈ અધિકૃત કમ્પ્યૂટર કર્મચારીઓની સહાય મેળવો.
- સલામત મોડ (સેફ મોડ)નો ઉપયોગ કરી કમ્પ્યૂટરને રીબુટ કરો. સલામત મોડ પર કામ કરવાથી નકારાત્મક ફાઇલોને દૂર કરવામાં મદદ મળે છે, કારણ કે તે ખરેખર ચલાવવામાં આવતી નથી અથવા આ મોડમાં સક્રિય થતી નથી.
- અસ્થાયી ફાઇલોને ડિલીટ કરવી. આ અભિગમ વાઇરસ સ્કેનિંગ પ્રક્રિયાને ઝડપી બનાવવામાં મદદ કરે છે.
- ડિસ્ક ક્લીનઅપ ટૂલ કમ્પ્યૂટર પર તમારી હંગામી ફાઇલોને દૂર કરવામાં મદદ કરે છે.
- એન્ટીવાઇરસ પોગ્રામ કમ્પ્યૂટરમાં દાખલ કરો. તેની સાથે માલવેર સ્કેનર પણ ઈન્સ્ટોલ કરવું.
- સ્કેનડિસ્ટ યુટિલિટીનો ઉપયોગ કરો, જેથી ખરાબ સેક્ટર તથા ફાઇલ, ફોલ્ડર વગેરેની માહિતી જાણી શકાય.
- કમ્પ્યૂટરમાં હાર્ડવેર અને નેટવર્ક માટે ફાયરવોલ ચાલુ રાખવી.
- એન્ટીવાઇરસ તથા એન્ટી માલવેર સોફ્ટવેરનો ઉપયોગ કરવો.
- ઈન્ટરનેટમાં http**s**ને બદલે **https** પ્રોટોકોલનો ઉપયોગ કરવો.
- ક્લાઉડ એન્ટીવાઇરસનો ઉપયોગ કરવો.
- ઓનલાઇન સ્કેનિંગ કરી પ્રોગ્રામ ડાઉનલોડ કરવા.

5. **સોફ્ટવેર સુરક્ષા :**

ચાલક પદ્ધતિ, અનુવાદ કે અન્ય સોફ્ટવેર કાર્યક્રમો માટે હંમેશાં મૂળ સોફ્ટવેર જ વાપરો. આવાં સોફ્ટવેર માટે વધુ પૈસા ચૂકવવા પડશે, પરંતુ તેઓ વિશ્વસનીય હશે અને કંઈક તકલીફ થાય તો બદલી શકાય તેવાં હશે. કમ્પ્યૂટરને બંધ કરવા માટે જરૂરી પગલાં લીધા પછી જ કમ્પ્યૂટરને બંધ કરો, જેથી ફાઇલો વગેરે ખરાબ ન થઈ જાય. જો તમે તમારો પોતાનો વિનિયોગ બનાવ્યો હોય તો તેના અમલ માટે ગુપ્ત સંકેતની જોગવાઈ રાખો. ગુપ્ત સંકેત (Password) ટાઇપ કરતી વખતે સ્ક્રીન પર દેખાય નહીં તેની કાળજી રાખવી.

6. **નેટવર્ક સુરક્ષા :**

નેટવર્ક તંત્ર માટે વધારે સારી સુરક્ષાની જરૂર પડે છે. કારણ કે આવી પરિસ્થિતિમાં ભૌતિક સુરક્ષાના માપદંડો પણ નકામા બની જાય છે. (તમારા મશીનના રૂમને તાળું મારીને બંધ રાખવો તેમ છતાં નેટવર્ક દ્વારા બીજા કોઈ કમ્પ્યૂટર વડે અન્ય વ્યક્તિ માહિતી મેળવી શકતી હોય તો ગમે તેટલી ભૌતિક સુરક્ષા વ્યર્થ છે.) વળી ક્યારે, કોણ તમારી માહિતી ક્યાંથી મેળવી રહ્યું છે, તે જાણવું ઘણું અઘરું છે. લેનમાં મોટે ભાગે એક સર્વર (Server) હોય છે, જે નેટવર્કમાંની સર્વભાગ્ય માહિતી પોતાની પાસે રાખે છે અને અન્ય કાર્યમથકોની વિનંતીઓને માન આપી તે પૂરી પાડે છે. મોટે ભાગે લેનમાં ગુપ્ત સંકેતની સુવિધા આપવામાં આવે છે. તદુપરાંત નીચે મુજબ અન્ય પગલાં લઈ શકાય.

- સર્વરને દૂર રાખો અને તે મર્યાદિત વ્યક્તિઓથી જ તેનો ઉપયોગ થઈ શકે તેવી ગોઠવણ કરો.
- અમુક પ્રકારના નેટવર્કમાં કમ્પ્યૂટર દ્વારા જે કાર્ય પાર પાડવામાં આવે તેની નોંધ રાખવાની વ્યવસ્થા હોય છે, તેનો ઉપયોગ થઈ શકે છે.
- નેટવર્કના વાયરોમાં અનધિકૃત જોડાણ ન કરી શકાય તે માટે તેમને બને તો એવી રીતે ગોઠવો કે કે જોડાણ અશક્ય બને. શક્ય હોય તો પ્રકાશીય તાર (Optical Fibre)નો પ્રયોગ કરો.
- માહિતી સંચારમાં સંકેતલિપિના પ્રયોગ કરો. જોકે તેનાથી નેટવર્કનો કાર્યભાર વધી જશે.
- ખૂબ સંવેદનશીલ નેટવર્ક માટે પ્રકાશીય તારનો પ્રયોગ કરવો હિતાવહ છે. જોકે તારમાં કઈ રીતે પ્રકાશ ચાલુ બંધ થાય છે તે જો જાણી શકાય તો તેમાંથી પણ માહિતી 'સાંભળી'ને 'ચોરી' શકાય છે.
- પ્રત્યાયનમાં ગુપ્તસંકેત પસાર નહીં થાય તેની કાળજી રાખો. જો તેમ ન કરી શકાય તો ગુપ્તસંકેતોને સાંકેતિક સ્વરૂપ.

7. પાંડા ક્લાઉડ એન્ટીવાઇરસ, ક્રાઉડ સ્ટ્રાઇક, સીબી ડિફેન્સ, ઇમ્યુનેટ કોમોડો ગ્રૂપ. ગ્રૂપ એ ક્લાઉડ એન્ટીવાઇરસના નામ છે.
8. માલવેર.
9. ટ્રોજન હોર્સ

10. વર્મ
11. બ્રાઈઝર હાઈઝેકર
12. સ્કેનટીસ્ટ યુટીલીટી
13. 1983માં ફ્રેડ કોહેન
14. ક્રિપર

16.6 ચાવીરૂપ શબ્દો (Key Words)

ઈમેલ (E-mail) : ઈમેલનું નામ ઈલેક્ટ્રોનિક ઈમેલ છે, જે ઈન્ટરનેટ પર પત્ર મોકલવા માટે ઉપયોગી છે.

નેટવર્ક (Network) : નેટવર્ક એ એક પ્રકારનું બે સંસાધનનું જોડાણ છે, જે પોતાની માહિતી વહેંચવા માટે તેનો ઉપયોગ કરે છે.

ફાઈલ શેરીંગ (File Sharing) : નેટવર્કમાં ફાઈલની અદલા-બદલી કે વહેંચણીને ફાઈલ શેરિંગ તરીકે ઓળખવામાં આવે છે.

ફ્લોપી (Floppy) : પાતળા પ્લાસ્ટિકની બનેલી ચુંબકીય તકતી, જેના ઉપર કમ્પ્યૂટર દ્વારા માહિતી લખી શકાય કે વાંચી શકાય.

મલ્ટીયુઝર (Multi User) : કમ્પ્યૂટરમાં એક જ માહિતી કે પ્રોગ્રામનો એક કરતાં વધુ ઉપભોક્તા તેનો ઉપયોગ કરે તેને મલ્ટીયુઝર કહેવામાં આવે છે.

લોગીન (Login) : નેટવર્કિંગ વ્યવસ્થામાં કમ્પ્યૂટરમાંની સવલતોનો ઉપયોગ કરવા માટે દરેક ઉપયોગકર્તાને આપવામાં આવતો અધિકાર.

સર્વર (Server) : કમ્પ્યૂટરોની આંતરિક (નેટવર્કિંગ) વ્યવસ્થાનું એક એવું કમ્પ્યૂટર, જે તેની સાથે જોડેલાં તમામ પટમથકોને માહિતી ફાઈલ કે પ્રોગ્રામ ફાઈલોને લખવા/વાંચવાની સવલત આપે છે.

16.7 સંદર્ભ અને વિશેષ વાંચન (References and Further Reading)

* Forouzan, B.A. (2000). TCP/IP Protocol Suite. 1st ed. New Delhi, India : Tata McGraw-Hill Publishing Company Limited.

https://en.wikipedia.org./wiki/virus

• • •