हेल्लो दोस्त,

मेरा नाम युगल जोशी है सबसे पहले तो आपका इस बुक को खरीदने के लिए धन्यवाद .

यह ebook मैंने hindi भाषी छात्रों के लिए बनाई है. इस बुक में आपको महत्वपूर्ण सवालों के जवाब मिलेंगे जो अक्सर exam में पूछे जाते है. आशा करता हूँ कि यह बुक आपके लिए लाभकारी होगी. तथा यह बुक आसान भाषा में है. अगर आपको लगता है कि इस बुक (cryptography & network security) में कही पर कोई सवाल या टॉपिक नहीं है तो मुझे contact जरुर करें. मैं आपको वह टॉपिक send करूँगा.

अगर आपको इस बुक के लिए कोई सुझाव है तो हमें बताएं.
मेरा फ़ोन no. 9761480219 है आप मुझे whatsapp या call कर सकते है. या आप ehindistudy.com में comment करके भी बता सकते है. धन्यवाद.

लेखक :- युगल

MD5 क्या है?

MD5 :-

MD5 का पूरा नाम message digest 5 है। इसका 1991 में Ronald rivest ने अविष्कार किया था।

MD5 एक cryptographic hash एल्गोरिथ्म है जो कि हेक्साडेसीमल फॉर्मेट में hash वैल्यू को produce करता है। MD5 एल्गोरिथ्म 128-बिट hash वैल्यू को produce करता है।

MD2 और MD4 भी message digest एल्गोरिथ्म है लेकिन ये पुरानी एल्गोरिथ्म है जबकि MD5 तीसरा एल्गोरिथ्म है ये नया एल्गोरिथ्म है।

MD2 तथा MD4 का स्ट्रक्चर MD5 की तरह समान होता है परन्तु MD2 एल्गोरिथ्म का प्रयोग 8-बिट मशीन में किया जाता है और MD-4 का प्रयोग 32-बिट मशीन में किया जाता है।

MD-5, MD4 की तरह fast नही है परन्तु यह MD4 से ज्यादा secure है।

What is Digital signature डिजिटल सिग्नेचर क्या है?

Digital signature :-

डिजिटल हस्ताक्षर(signature) को हम निम्न बिंदुओं के आधार पर आसानी से समझ सकते है:-

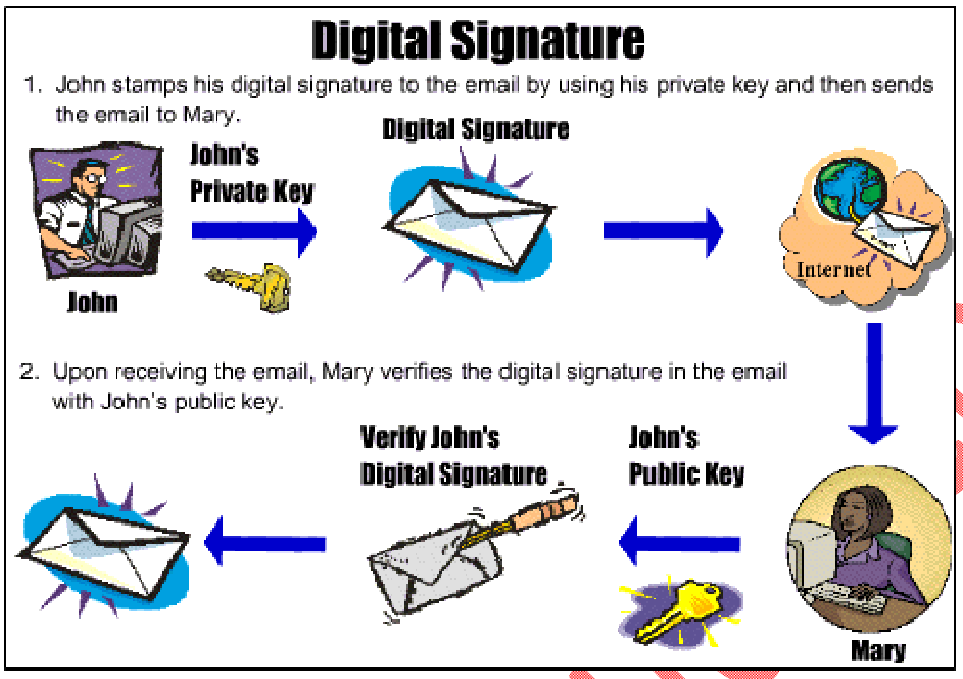
1:-डिजिटल हस्ताक्षर एक गणितीय तकनीक है जिसका प्रयोग किसी message, या इलेक्ट्रॉनिक डॉक्यूमेंट की authenticity तथा integrity को सुनश्चित करने के लिए किया जाता है।

2:-डिजिटल हस्ताक्षर(signature) हाथ के द्वारा किये गए हस्ताक्षर की तरह ही समान है परन्तु हाथ के द्वारा किये गए हस्ताक्षर में उतनी विश्वसनीयता तथा security नही होती जबकि डिजिटल हस्ताक्षर में security होती है।

3:-digital signature यह सुनश्चित करता है कि message या कोई अन्य इलेक्ट्रॉनिक डॉक्यूमेंट original है और यह message किस व्यक्ति ने भेजा है तथा यह message बदला हुआ(altered) नही है।

4:-डिजिटल हस्ताक्षर public key cryptography की विधि पर आधारित है। इसमें दो keys का प्रयोग किया जाता है। message को encrypt करने वाली key को public के लिए रखा जाता है और message को decrypt करने वाली key को secret रखा जाता है।

5:-डिजिटल हस्ताक्षर का प्रयोग ज्यादातर e-commerce वेबसाइट जैसे:- OLX, shopclues तथा ऑनलाइन बैंकिंग के लिए किया जाता है जिससे कि हमारा transaction सुरक्षित हो सकें।



What is HTTPS ?

HTTPS :-

HTTPS को निम्नलिखित बिंदुओं के आधार पर आसानी से समझ सकते है:-

1:-HTTPS का पूरा नाम Hyper Text Transfer Protocol Secure है।

2:-HTTPS एक ऐसा प्रोटोकॉल है जिसके द्वारा इंटरनेट में ब्राउज़र से किसी भी वेबसाइट पर सुरक्षित कम्युनिकेशन किया जा सकता है।

3:-HTTPS, HTTP का एक encrypted version है। इस का मतलब यह है कि ब्राउज़र तथा वेबसाइट के मध्य जितना भी कम्युनिकेशन होता है उसको encrypt किया जाता है।

4:-Https का ज्यादातर प्रयोग ऑनलाइन shopping तथा banking को सुरक्षित करने के लिए करते है।

5:-Https दो प्रोटोकॉल से मिलकर बना होता है :-
*HTTP
*SSL(Secure Socket Layer)/TLS(Transport Layer Security)

6:-Https को netscape ने विकसित किया था।

WHAT IS SSH?

SSH in hindi:-

SSH का पूरा नाम secure shell है, इसे कभी-कभी secure socket shell भी कहते है। remote logins के लिए SSH एक सुरक्षित प्रोटोकॉल है।

SSH, दूसरे कंप्यूटर के साथ सुरक्षित कम्यूनिकेट करने की विधि है। SSH एक नेटवर्क प्रोटोकॉल है जिससे कि डेटा या सूचना को सुरक्षित channels के माध्यम से दो devices के मध्य transmit किया जाता है।
SSH एक नेटवर्क को attacks से सुरक्षा करता है।

SSH अन्य रिमोट shells जैसे:-rlogin, rsh, rcp, और rdist का replacement है। SSH अन्य remote shells की तरह समान होता है परन्तु SSH डेटा को encrypt करता है जिससे की डेटा secure हो जाता है।

SSH द्वारा डेटा को encrypt करने के लिए public key cryptography का प्रयोग किया जाता है जिसमें दो अलग-अलग keys का प्रयोग किया जाता है डेटा को encrypt करने वाली key को public के लिए रखा जाता है और डेटा को decrypt करने वाली key को secret रखा जाता है।

SSH को SSH Communications Security Ltd. ने विकसित किया था।

What is SSL in hindi

SSL किसे कहते है?:-

SSL का पूरा नाम secure socket layer है। यह एक ऐसी टेक्नोलॉजी है जिससे हम server(वेबसाइट) तथा client(ब्राउज़र) के मध्य एक encrypted link को established करते है जिससे हमें website तथा browser के मध्य सुरक्षित connection उपलब्ध होता है।

दूसरे शब्दों में कहें तो इंटरनेट में डेटा को ऑनलाइन ट्रान्सफर करने के लिए यह एक security प्रोटोकॉल है। इस encryption तकनीक का निर्माण नेटस्केप ने 1990 में किया था।

SSL में दो keys का प्रयोग किया जाता है। एक public key होती है जो sender तथा receiver दोनों को पता होती है तथा एक private key होती है जो सिर्फ receiver को पता होती है।

SSL का प्रयोग ज्यादातर क्रेडिट कार्ड नंबर, डेबिट कार्ड नंबर, ऑनलाइन transaction व अन्य महत्पूर्ण documents को सुरक्षित transmit करने के लिए किया जाता है।

बहुत सारी वेबसाइट SSL प्रोटोकॉल का प्रयोग करती है जिसके कारण वेबसाइट हमेशा http:// से शुरू ना होकर https:// से शुरू होती है।

SSL कैसे काम करता है?

निम्नलिखित steps से हम समझ सकते है कि SSL काम कैसे करता है:-

1:-प्रथम step में, एक ब्राउज़र SSL द्वारा सुरक्षित वेबसाइट से connect करने की कोशिश करता है।

2:-इसके बाद, ब्राउज़र वेबसाइट से खुद को identify करने के की request करता है।

3:-इसके बाद, वेबसाइट ब्राउज़र को SSL certificate की copy भेजता है।

4:-इसके बाद, ब्राउज़र यह check करता है कि SSL certificate सही है या नही। अगर यह सही है तो ब्राउज़र वेबसाइट को एक message भेजता है।

5:-अंत में, वेबसाइट ब्राउज़र को एक acknowledgement भेजता है और इस प्रकार वेबसाइट तथा ब्राउज़र के मध्य SSL encrypted session शुरू हो जाता है।

What is hashing?

Hashing in hindi:-

characters के समूह में से fixed length value या key को generate करने की प्रक्रिया hashing कहलाती है। hashing की इस प्रक्रिया में value या key को generate करने के लिए गणितिय फंक्शन का प्रयोग किया जाता है।

या दूसरे शब्दों में कहें तो “मैसेज या डेटा में hashing algorithm को apply करके hash वैल्यू को create किया जाता है।”

hashing algorithm को hash function भी कहा जाता है।

उदाहरण के द्वारा हम हैशिंग को आसानी से समझ सकते है:-

माना पंकज एक मैसेज कमल को भेजता है तो इस मैसेज के लिए hash वैल्यू को generate तथा encrypt किया जाता है तथा इस hash वैल्यू को मैसेज के साथ भेज दिया जाता है। जब कमल इस मैसेज को receive करता है तो वह इस मैसेज के साथ-साथ hash को भी decrypt करता है। इसके बाद, कमल मैसेज से एक और hash को create करता है, यदि यह दोनो hash समान होंगे तभी सुरक्षित ट्रांसमिशन सम्भव हो पायेगा।

PGP क्या है?

PGP in hindi:-

PGP का पूरा नाम pretty good privacy है। PGP एक encryption तथा decryption कंप्यूटर प्रोग्राम है जो कि इंटरनेट में ईमेल messages को encrypt तथा decrypt करने के लिए प्रयोग में लाया जाता है।

PGP, public key cryptography की विधि पर आधारित है। इसमें दो keys का प्रयोग किया जाता है। message को encrypt करने वाली key को public के लिए रखा जाता है और message को decrypt करने वाली key को secret रखा जाता है।

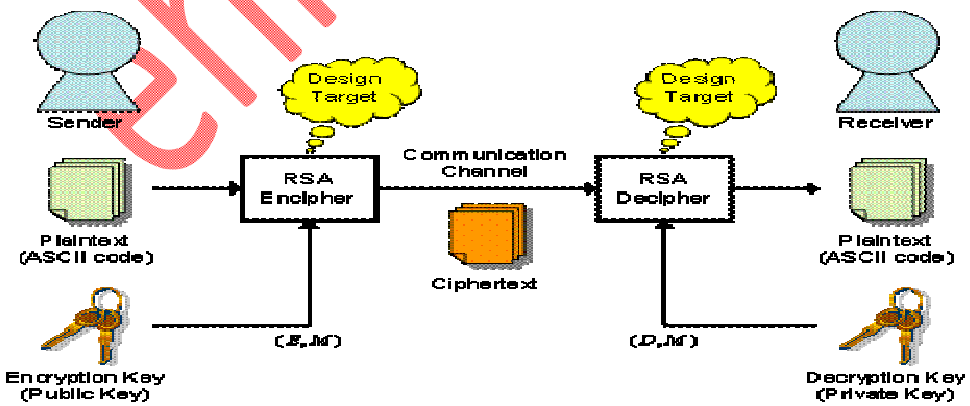
PGP का सबसे बड़ा फायदा यह है कि हम PGP का प्रयोग आसानी से कर सकते है तथा यह एकदम मुफ़्त है। PGP का अविष्कार Philip Zimmerman ने किया था।

RSA क्या है?

RSA एक public key cryptography है और इसका प्रयोग ज्यादातर sensitive डेटा को असुरक्षित नेटवर्क (जैसे:-internet) में सुरक्षित transmission करने के लिए किया जाता है।

RSA को इसका नाम इसके वैज्ञानिक Ron Rivest, Adi Shamir और Leonard Adleman के कारण पड़ा। इसको इन्होंने सन् 1977 में develop किया था।

RSA में दो अलग-अलग keys का प्रयोग किया जाता है डेटा को encrypt करने वाली key को public के लिए रखा जाता है और डेटा को decrypt करने वाली key को secret रखा जाता है।

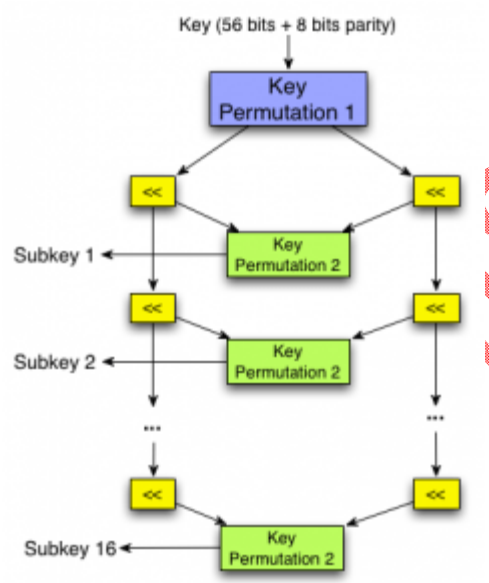


DES क्या है?-

DES का पूरा नाम data encryption standard है। DES एक symmetric-key encryption विधि है जिसमें message को encrypt तथा decrypt करने के लिए एक ही key का प्रयोग किया जाता है अर्थात Sender तथा receiver दोनों के पास समान private key होती है।

यह 56-bit key का प्रयोग करके 64-bit data को encrypt करता है।

DES को 1976 में IBM ने develop किया था। DES का प्रयोग अब नही किया जाता है क्योंकि अब यह विधि पुरानी हो गयी है अब इसका स्थान AES(Advanced Encryption Standard ने ले लिया है।



L2TP क्या है?

L2TP का पूरा नाम layer 2 tunneling protocol है। L2TP एक VPNs protocol है जो कि खुद encryption उपलब्ध नही कराता बल्कि यह encryption protocol पर निर्भर रहता है जो कि

privacy को उपलब्ध कराने के लिए tunnels से होकर गुजरता है। L2TP को Virtual Dialup Protocol भी कहते है क्योंकि यह PPTP का extension(विस्तार) है।

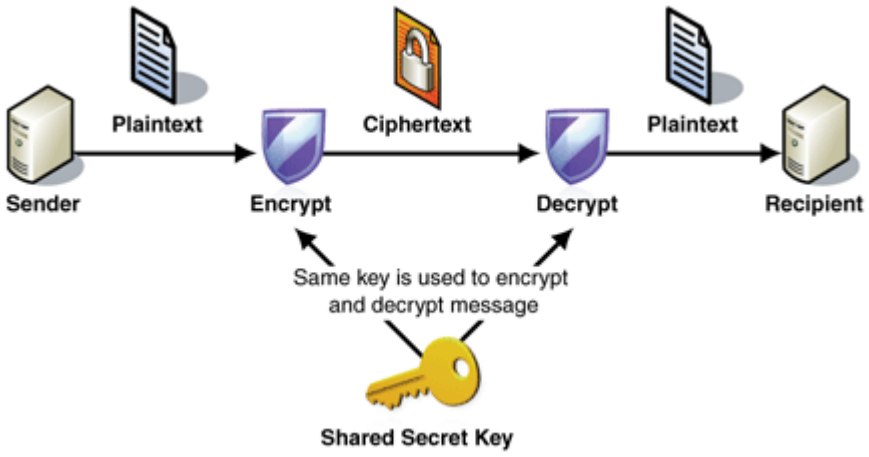
L2TP एक OSI model का session layer protocol है। L2TP दो प्रोटोकॉल से मिलकर बना होता है एक PPTP तथा दूसरा L2F(layer 2 forwarding).

L2TP tunnel के LAC (L2TP Access Concentrator) और LNS (L2TP Network Server) दो endpoint होते है। LAC, टनल के initiator(चालक) की तरह कार्य करता है जबकि LNS, सर्वर की तरह कार्य करता है।

L2TP की गति PPTP से कम है लेकिन यह PPTP से ज्यादा सुरक्षित है।

Symmetric and asymmetric key cryptography क्या है?

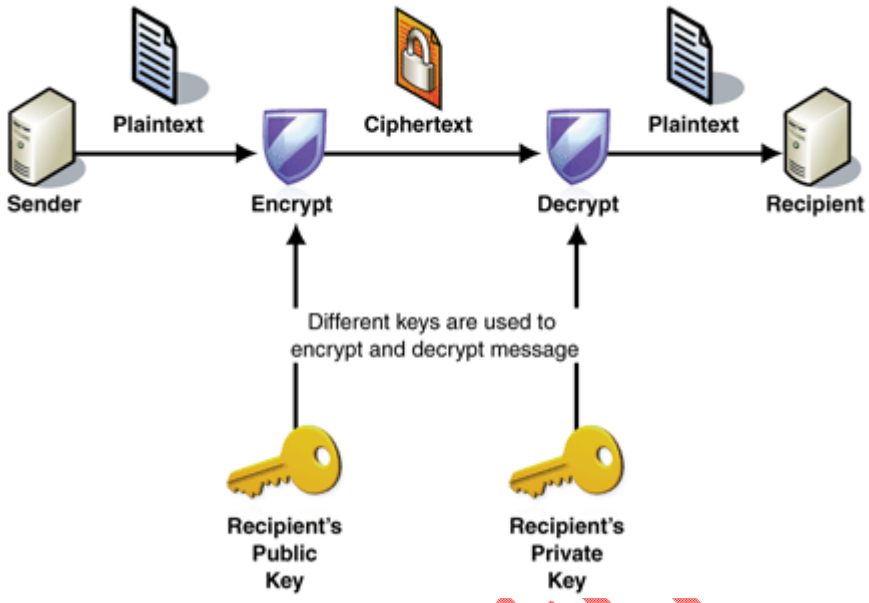
symmetric key cryptography in hindi:-



symmetric key cryptography वह cryptography है जिसमें एक ही key का प्रयोग plain text के encryption तथा cipher text के decryption के लिए किया जाता है।

इस प्रकार की cryptography में sender तथा receiver के पास एक ही समान key होती है। Symmetric key cryptography को private key cryptography भी कहते है।

Asymmetric key cryptography in hindi:-



Asymmetric key cryptography में दो अलग-अलग keys का प्रयोग data को encrypt तथा decrypt करने के लिए किया जाता है। इसमें एक public key होती है जो सबको पता होती है और दूसरी secret key होती है जो सिर्फ रिसीवर(receiver) को पता होती है।

इसे public key cryptography भी कहा जाता है।

उदहारण के लिए यदि युगल एक message कमल को send करता है तो वह कमल की public key का प्रयोग message को encrypt करने के लिए करेगा तथा उसके बाद कमल उस message को अपनी private या secret key के द्वारा उसे decrypt करेगा।

Asymmetric key cryptography में देखने वाली बात यह है कि सिर्फ public key का प्रयोग message को encrypt करने के लिए किया जाता है तथा केवल secret key का प्रयोग message को decrypt करने के लिए किया जाता है।

Encryption and Decryption in hindi

Encryption in hindi:-

Cryptography में, encryption एक ऐसी प्रक्रिया है जिसमें data या information को secret codes में convert कर दिया जाता है जिसे cipher text कहते है। Cipher text को आसानी से समझा नही जा सकता है इसे सिर्फ expert ही समझ सकते है।

जो original data या information होती है उसे हम plain text कहते है और उसे cipher text में encrypt कर दिया जाता है।

Encryption का मुख्य उद्देश्य डिजिटल डेटा या इनफार्मेशन(जो internet के माध्यम से transmit होता है) को सुरक्षित करना है।

encrypted data को पढ़ने के लिए आपके पास एक key होनी चाहिए जिससे कि आप उसे decrypt कर सके।

Encryption के प्रकार:-Encryption दो प्रकार का होता है:-
1:-Asymmetric encryption(Public-key cryptography)
2:-symmetric encryption(Private-key cryptography)

Decryption:-

Decryption एक ऐसी प्रक्रिया जिसमें encrypted data को वापस original data में convert किया जाता है।

जो encrypted डेटा होता है उसे cipher text कहा जाता है और जो original डेटा होता है उसे plain text कहा जाता है तथा Cipher text को plain text में बदलना Decryption कहलाता है। इसके लिए भी एक key की आवशयक्ता होती है जिससे कि डेटा decrypt हो सके।

Cryptography क्या है?

Cryptography in hindi:-

Cryptography का अर्थ है "the art of protecting data". अर्थात अपने data या information को सुरक्षित रखना।

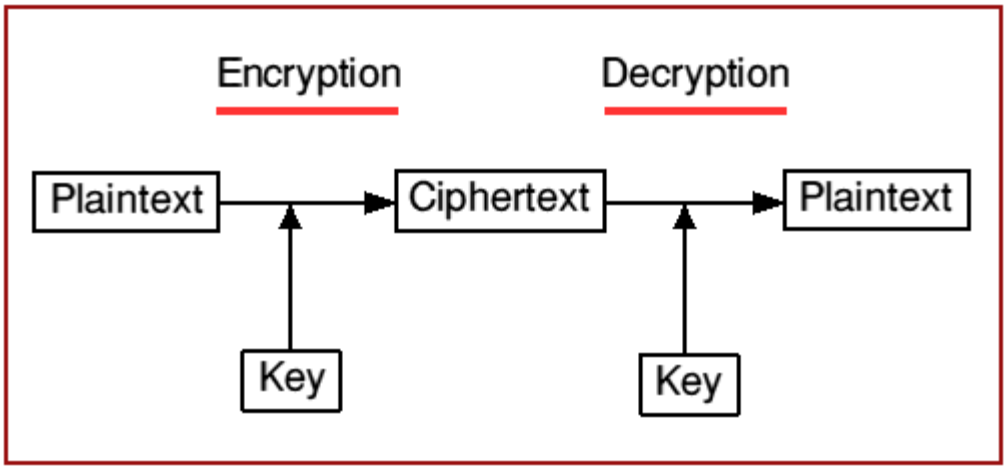
लेकिन सबसे पहले मन में सवाल उठता है कि कैसे?

हम अपने data या information को unreadable secrets codes में बदल दिए जाते है जिन्हें हम cipher text कहते है और वो ही लोग इसे decrypt करके read कर सकते है जिनके पास इसकी secret key होगी। Decrypt हुए data को हम plain text कहते है।

Cryptography का प्रयोग E-mail मैसेज, credit card तथा अन्य महत्वपूर्ण information को protect करने के लिए किया जाता है। यह data की security तथा integrity बनाये रखती है।

आज के युग में Cryptography द्वारा बहुत ही जटिल गणितीय समीकरण का प्रयोग data को decrypt तथा encrypt करने में किया जाता है।

Cryptography में encryption और decryption दो process होती है।
encryption में plain text को cipher text में convert किया जाता है। Decryption में cipher text को plain text में convert किया जाता है।



Encryption:- Cryptography में, encryption एक ऐसी प्रक्रिया है जिसमें data या information को secret codes में convert कर दिया जाता है जिसे cipher text कहते है। Cipher text को आसानी से समझा नही जा सकता है इसे सिर्फ expert ही समझ सकते है।

जो original data या information होती है उसे हम plain text कहते है और उसे cipher text में encrypt कर दिया जाता है।

Encryption का मुख्य उद्देश्य डिजिटल डेटा या इनफार्मेशन(जो internet के माध्यम से transmit होता है) को सुरक्षित करना है।

encrypted data को पढ़ने के लिए आपके पास एक key होनी चाहिए जिससे कि आप उसे decrypt कर सके।

Encryption के प्रकार:-Encryption दो प्रकार का होता है:-
1:-Asymmetric encryption (Public-key cryptography)
2:-symmetric encryption(Private-key cryptography)

Decryption:- Decryption एक ऐसी प्रक्रिया जिसमें encrypted data को वापस original data में convert किया जाता है।

जो encrypted डेटा होता है उसे cipher text कहा जाता है और जो original डेटा होता है उसे plain text कहा जाता है तथा Cipher text को plain text में बदलना Decryption कहलाता है। इसके लिए भी एक key की आवश्यक्ता होती है जिससे कि डेटा decrypt हो सके।

PPTP क्या है समझाइये?

PPTP in hindi

PPTP का पूरा नाम point-to-point tunneling protocol है।

PPTP एक ऐसी तकनीक है जिसके द्वारा virtual private network(VPNs) का निर्माण किया जाता है जिससे कि messages या data को एक node से दूसरे node सुरक्षित तरीके से भेजा जा सके।

PPTP के द्वारा हम अपने data या messages को सुरक्षित तरीके से tunnels में से होकर गुजारते है जिससे कि उसे कोई भी नही देख पाता है।

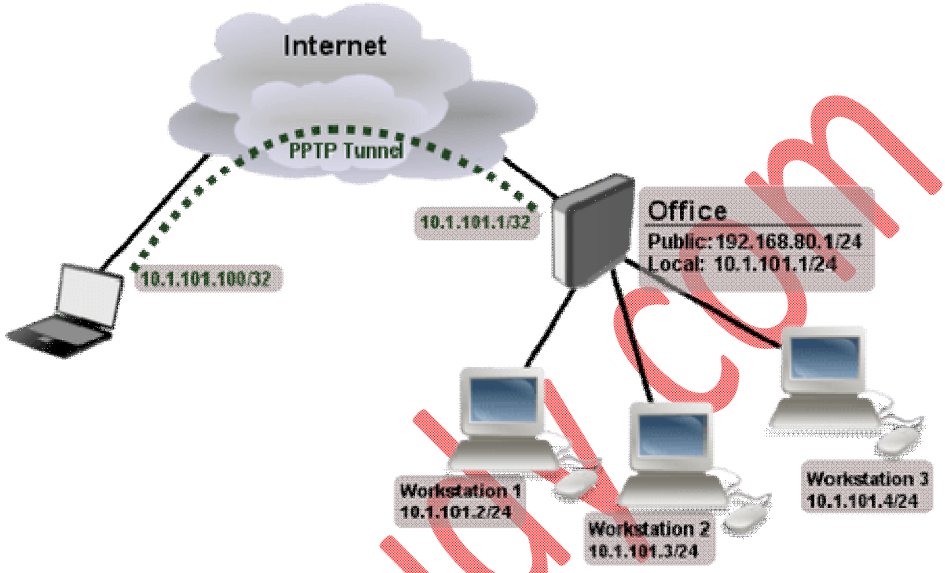


image source

उदहारण के लिए:- जब एक user किसी नेटवर्क(जैसे- wi-fi) का प्रयोग करता है तो वह PPTP VPN का भी प्रयोग करता है जिससे कि उसकी सारी online activity encrypt हो जाती है। अगर कोई उस user के connection को तोड़कर उसके data या information को चुराना चाहे तो वह ऐसा नही कर पाता है क्योंकि जो भी data या information होती है वह tunnels के अंदर होती है.

Ethical Hacking क्या है?

Ethical Hacking in Hindi:-

Ethical hacking को white hat hacking भी कहा जाता है। Ethical hacking में अन्य hacking की तरह ही कंप्यूटर सिस्टम को hack किया जाता है परन्तु इसका मकसद कंप्यूटर सिस्टम में

vulnerabilities तथा अन्य threats को खोजना होता है। इन vulnerabilities तथा threats को खोजने के बाद उन्हें fix किया जाता है। जिससे कोई अन्य hacker इसका फायदा ना उठा सकें।

जबकि इसके विपरीत जो non-ethical hacker होते है वे इन vulnerabilities तथा threats का प्रयोग अपने फायदे के लिए करते है। Non-ethical hacker को हम black hat hacker भी कहते है।

Ethical hacker के पास programming की अच्छी knowledge होती है। जैसे:-C,C++,JAVA etc.

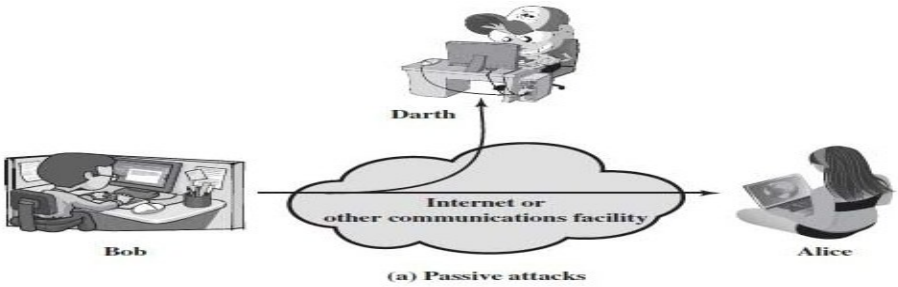
Ethical hacker का मुख्य उद्देश्य कंप्यूटर सिस्टम में vulnerabilities तथा threats को खोजकर उन्हें fix करना है। जिससे कि कंप्यूटर सिस्टम और भी secure(सुरक्षित) हो सकें।

Active attack और passive attack क्या है?

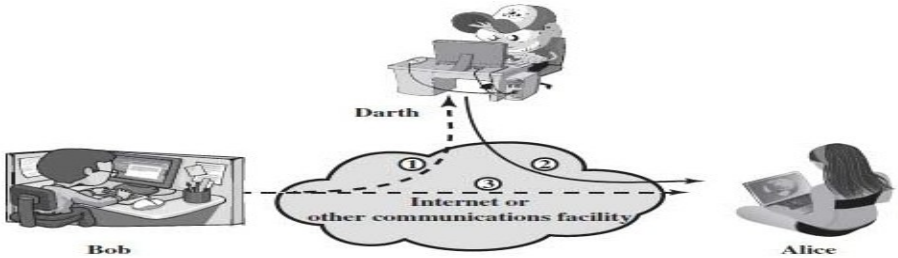
types of security attacks in hindi:-

attacks मुख्यतय दो प्रकार के होते है जो निम्न है:-
1:-Passive attack
2:-Active attack

1:-Passive attack:- Passive attack वह attack होता है जिसमें एक attacker अनधिकृत(unauthorized) तरीके से दो systems को मॉनिटर करता है, और जो messages या information दोनों systems के मध्य transmit हुए है उनको सिर्फ monitor करता है परन्तु messages को modify नही करता है। passive attack का मुख्य उद्देश्य संवेदनशील information तथा password को चुराना होता है।



(a) Passive attacks



(b) Active attacks

2:-Active attack:- Active attack वह attack होता है जिसमें attacker दो systems मध्य messages को transmit करता है तथा उन messages को modify करता है। उन modified messages को व्यक्ति को भेज दिए जाते है। उस व्यक्ति को पता भी नही चलता है कि ये messages कोई attacker भेज रहा है तथा ये modified है।

Attacker को समझाइये?

Attacker:-

attacker वह व्यक्ति होता है जो जानबूझकर और पूरे intentions के साथ हमारे कंप्यूटर सिस्टम को attack करता है और वह महत्वपूर्ण तथा संवेदनशील data या information को destroy, alter तथा steal कर लेता है तथा उसका गलत प्रयोग करता है।

Attacker को black hat hacker भी कहा जाता है क्योंकि इनका मकसद ज्यादा से ज्यादा हानि पहुँचाने का होता है। Attacker हमारे कंप्यूटर में malicious viruses, worms, तथा software

को डाल देते है जिससे हमारा कंप्यूटर viruses और worms की चपेट में आकर damage हो जाता है।

कुछ को छोड़कर ज्यादातर attacker के पास programming knowledge नही होती है। ये websites से tools तथा software डाउनलोड करके attacks करते है। ये अपने फायदे के लिए सारें security laws तथा policies को तोड़ते है।

Hacking क्या है?

HACKING:-

Hacking एक ऐसी प्रक्रिया है जिसमें आपके नेटवर्क में घुसकर आपके system से आपकी सारी मूल्यवान information को चुरा लिया जाता है तथा सिस्टम में viruses छोड़कर सारी information को मिटा दिया जाता है और इस सूचना का गलत इस्तेमाल किया जाता है। वह व्यक्ति जो hacking की प्रक्रिया को अंजाम देता है hacker कहलाता है। Hacker एक well skilled programmer होता है जिसे programming की अच्छी खासी knowledge होती है।

दूसरे शब्दों में कहे तो," Hacker वह व्यक्ति होता है जो कंप्यूटर सिस्टम में unauthorized access पाने के लिए कोड्स और पासवर्ड को तोड़ता है।"

Hacker निम्नलिखित कारणों से hacking को अंजाम देते है।
1:-Money के लिए।
2:-Fun(मजे) के लिए।
3:-सूचनाओं को चुराने के लिए।
4:-Revenge(बदला) लेने के लिए।
5:-spam भेजने के लिए।
6:-Malicious फाइल्स के execution के लिए।
7:-communication को insecure करने के लिए।

8:-आपके सिस्टम का प्रयोग करने के लिए।
9:-किसी वास्तविक target पर attack करने के लिए।
10:-चुनौतियों के लिए।

IPv4 & IPv6 क्या है?:-

IPv4 in hindi:-

IPv4 का पूरा नाम internet protocol version 4 है, यह इन्टरनेट प्रोटोकॉल का चौथा version है. यह एक कनेक्शन विहीन protocol है जिसका प्रयोग packet switched layer नेटवर्क्स(जैसे:-ethernet) में किया जाता है.

इसका प्रयोग नेटवर्क में डेटा पैकेट्स को को होस्ट डिवाइस से डेस्टिनेशन डिवाइस तक डिलीवर करने में किया जाता है.

IPv4 को आजकल भी बहुत से devices में प्रयोग किया जाता है. परन्तु आजकल के devices IPv4 तथा IPv6 दोनों को सपोर्ट करते है.

IPv6 in hindi:-

IPv6 का पूरा नाम internet protocol version 6 है. यह IPv4 का latest version है तथा इसमें बेहतर तथा एडवांस्ड features है.

IPv4 तथा IPv6 में मुख्य अंतर:-

दोनों ip versions में मुख्य अंतर निम्नलिखित है:-

IPv6

1:-इसमें 128 बिट्स लम्बाई का एड्रेस होता है.

2:-IPv6 एड्रेस एक बाइनरी संख्या होती है जिसे हेक्साडेसीमल में प्रदर्शित किया जाता है.

3:-इसमें fragmentation केवल sender के द्वारा की जाती है

4:-यह मोबाइल नेटवर्क के लिए ज्यादा अनुकूल है.

5:-इसमें header field की संख्या 8 है.

6:-इसकी शुरुआत 1999 में हुई थी.

IPv4

1:-इसमें 32 बिट्स लम्बाई का एड्रेस होता है.

2:- IPv4 एड्रेस भी बाइनरी संख्या होती है जिसे डेसीमल में प्रदर्शित किया जाता है.

3:-इसमें fragmentation sender तथा forwarding routers दोनों के द्वारा की जाती है.

4:-यह मोबाइल नेटवर्क के लिए थोडा कम अनुकूल है.

5:-इसमें header field की संख्या 12 है

6:-इसकी शुरुआत 1981 में हुई थी.

हमें IPv4 तथा IPv6 को समझने के लिए पहले IP address को समझना पड़ेगा.

what is OSI model ?

OSI MODEL in hindi:-

OSI मॉडल का पूरा नाम Open Systems Interconnection है इसे ISO(International Organization
for Standardization) ने 1978 में विकसित किया था और इस मॉडल में 7 layers होती है।

OSI मॉडल किसी नेटवर्क में दो यूज़र्स के मध्य कम्युनिकेशन के लिए एक reference मॉडल है। इस मॉडल की प्रत्येक लेयर दूसरे लेयर पर निर्भर नही रहती है लेकिन एक लेयर से दूसरे लेयर में डेटा का ट्रांसिमिशन होता है।

OSI मॉडल यह describe करता है कि किसी नेटवर्क में डेटा या सूचना कैसे send तथा receive होती है। OSI मॉडल के सभी layers का अपना अलग अलग काम होता है जिससे कि डेटा एक सिस्टम से दूसरे सिस्टम तक आसानी से पहुँच सके। OSI मॉडल यह भी describe करता है कि नेटवर्क हार्डवेयर तथा सॉफ्टवेयर एक दूसरे के साथ लेयर के रूप में कैसे कार्य करते है।

7 layers of OSI MODEL IN HINDI:-

OSI मॉडल में निम्नलिखित 7 layers होती हैं आइये इन्हें विस्तार से जानते है:-

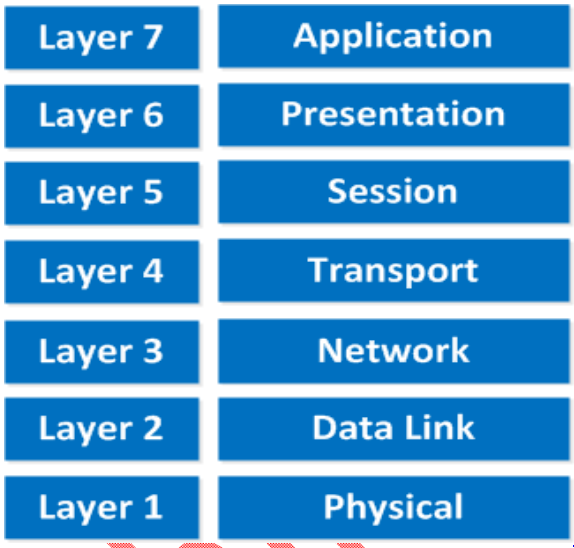


image source

1:-PHYSICAL LAYER(फिजिकल लेयर):- OSI मॉडल में physical लेयर सबसे निम्नतम लेयर है। यह लेयर फिजिकल तथा इलेक्ट्रिकल कनेक्शन के लिए जिम्मेदार रहता है जैसे:- वोल्टेज, डेटा रेट्स आदि।

इस लेयर में डिजिटल सिग्नल, इलेक्ट्रिकल सिग्नल में बदल जाता है।

इस लेयर में नेटवर्क की topology अर्थात layout of network(नेटवर्क का आकार) का कार्य भी इसी लेयर में होता है।

फिजिकल लेयर यह भी describe करता है कि कम्युनिकेशन wireless होगा या wired होगा।

इस लेयर को बिट यूनिट भी कहा जाता है।

2:-Data link layer(डेटा लिंक लेयर):- OSI मॉडल में डेटा लिंक लेयर नीचे से दूसरे नंबर की लेयर है। इस लेयर की दो sub-layers होती है:-
**MAC*(मीडिया एक्सेस कण्ट्रोल), तथा
**LLC*(लॉजिक लिंक कण्ट्रोल)

इस लेयर में नेटवर्क लेयर द्वारा भेजे गए डेटा के पैकेटों को decode तथा encode किया जाता है तथा यह लेयर यह भी ensure करता है कि डेटा के ये पैकेट्स त्रुटि रहित हो।

इस लेयर को फ्रेम यूनिट भी कहा जाता है।

3:-Network layer(नेटवर्क लेयर):- नेटवर्क लेयर OSI मॉडल का तीसरा लेयर है इस लेयर में switching तथा routing तकनीक का प्रयोग किया जाता है। इसका कार्य लॉजिकल एड्रेस अर्थात I.P. address भी उपलब्ध कराना है।

नेटवर्क लेयर में जो डेटा होता है वह पैकेट(डेटा के समूह) के रूप में होता है और इन पैकेटों को source से destination तक पहुँचाने का काम नेटवर्क लेयर का होता है।

इस लेयर को पैकेट यूनिट भी कहा जाता है।

4:-Transport layer(ट्रांसपोर्ट लेयर):-ट्रांसपोर्ट लेयर OSI मॉडल की चौथी लेयर है। इस लेयर का प्रयोग डेटा को नेटवर्क के मध्य में से सही तरीके से ट्रान्सफर किया जाता है। इस लेयर का कार्य दो कंप्यूटरों के मध्य कम्युनिकेशन को उपलब्ध कराना भी है।

इसे सेगमेंट यूनिट भी कहा जाता है।

5:-Session layer(सेशन लेयर):- सेशन लेयर OSI मॉडल की पांचवी लेयर है जो कि बहुत सारें कंप्यूटरों के मध्य कनेक्शन को नियंत्रित करती है।

सेशन लेयर दो डिवाइसों के मध्य कम्युनिकेशन के लिए सेशन उपलब्ध कराता है अर्थात जब भी कोई यूजर कोई भी वेबसाइट खोलता है तो यूजर के कंप्यूटर सिस्टम तथा वेबसाइट के सर्वर के मध्य तक सेशन का निर्माण होता है।

आसान शब्दों में कहें तो सेशन लेयर का मुख्य कार्य यह देखना है कि किस प्रकार कनेक्शन को establish, maintain तथा terminate किया जाता है।

6:-Presentation layer(प्रेजेंटेशन लेयर):- presentation लेयर OSI मॉडल का छटवां लेयर है। इस लेयर का प्रयोग डेटा का encryption तथा decryption के लिए किया जाता है। इसे डेटा compression के लिए भी प्रयोग में लाया जाता है। यह लेयर ऑपरेटिंग सिस्टम से सम्बंधित है।

7:-Application layer(एप्लीकेशन लेयर):- एप्लीकेशन लेयर OSI मॉडल का सातवाँ(सबसे उच्चतम) लेयर है। एप्लीकेशन लेयर का मुख्य कार्य हमारी वास्तविक एप्लीकेशन तथा अन्य लयरों के मध्य interface कराना है।

एप्लीकेशन लेयर end user के सबसे नजदीक होती है। इस लेयर के अंतर्गत HTTP, FTP, SMTP तथा NFS आदि प्रोटोकॉल आते है।

यह लेयर यह नियंत्रित करती है कि कोई भी एप्लीकेशन किस प्रकार नेटवर्क से access करती है।

एक non-technical बात

OSI मॉडल में 7 layers होती है उनको याद करना थोडा मुश्किल होता है इसलिए नीचे आपको एक आसान तरीका दिया गया है जिससे कि आप इसे आसानी से याद कर सकें:-
P-Pyare(प्यारे)
D-Dost(दोस्त)
N-Naveen(नवीन)
T-tumhari(तुम्हारी)
S-Shaadi(शादी)
P-Pe(पे)
A-Aaunga(आऊंगा).

EDI kya hai? & EDI working (कार्यविधि)

EDI in hindi:-

EDI का पूरा नाम इलेक्ट्रॉनिक डेटा इंटरचेंज(electronic data interchange) है। यह एक ऐसा कम्युनिकेशन सिस्टम है जिसमें कि एक कंप्यूटर से दूसरे कंप्यूटर में डेटा को इलेक्ट्रॉनिक रूप में एक कंप्यूटर से दूसरे कंप्यूटर में ट्रांसफर करते है।

क्योंकि डेटा को ट्रान्सफर करने में paperwork नही करना पड़ता है इसलिए इसमें किसी मनुष्य के हस्तक्षेप की आवश्यकता नही पड़ती है।

आजकल EDI का प्रयोग सबसे ज्यादा B2B e-commerce में किया जाता है। EDI के द्वारा बहुत ही अधिक डेटा का ट्रान्सफर किया जाता है जिसके कारण इसमें डेटा को bidirectional फॉर्मेट में व्यवस्थित किया जाता है।

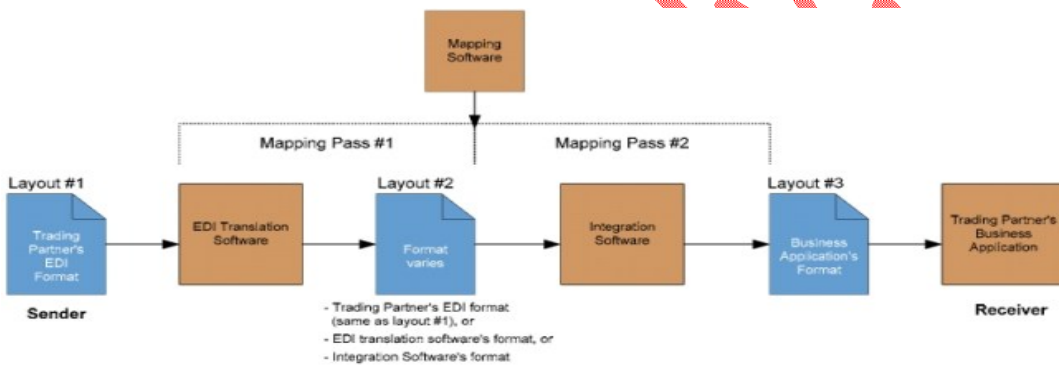


Fig:-कार्यप्रणाली

advantage of EDI in hindi:-

1:-इसमें डाक्यूमेंट्स को ट्रान्सफर करने में समय बहुत ही कम लगता है क्योंकि डेटा इलेक्ट्रॉनिक रूप में ट्रान्सफर होता है।

2:-क्योंकि data entry कंप्यूटर में होती है इसलिए इसमें गलतियों की गुंजाइश बहुत ही कम होती है।

3:-इसमें डेटा को आसानी से exchange कर सकते है अर्थात् इसमें technical complexity कम हो जाती है।

4:-इसमें डेटा का ट्रान्सफर इसके लाभ निम्नलिखित है:-

कम कीमत(cost) में हो जाता है।

5:-इसमें paperwork नही करना पड़ता है।

6:-इसमें डेटा का आदान-प्रदान बेहतर होता है तथा accuracy अधिक होती है।

EDI working in hindi(इसकी कार्यप्रणाली):-

इसकी कार्यप्रणाली में निम्नलिखित स्टेप्स होते है:-

1:–सबसे पहले जिन डॉक्यूमेंट या डेटा को ट्रांसफर करना होता है उसको हम तैयार करते है अर्थात डेटा को इकट्ठा तथा सुव्यवस्थित किया जाता है।

2:-फिर इन डाक्यूमेंट्स को ट्रांसलेटर सॉफ्टवेयर के द्वारा EDI फॉर्मेट में translate किया जाता है।

3:-जब हम डाक्यूमेंट्स को EDI फॉर्मेट में ट्रांसलेट कर लेते है तो डाक्यूमेंट्स exchange होने के लिए तैयार हो जाते है। तब हम अपने business सहयोगी से connect करते है और डाक्यूमेंट्स को exchange करते है। डाक्यूमेंट्स का ट्रांसफर HTTP, HTTPS तथा FTP प्रोटोकॉल्स कम्युनिकेशन विधियों के द्वारा किया जाता है।

4:-यह डाक्यूमेंट्स recipient मेलबॉक्स में तब रहता है जब तक कि वह मेलबॉक्स से डाक्यूमेंट्स को देख तथा प्रोसेस नही कर लेता है।

Domain name system(DNS) क्या है?

DOMAIN NAME SYSTEM(DNS)

DNS एक ऐसी इंटरनेट सेवा है जो कि Domain names को IP एड्रेस में बदल देता है।

Domain Name System(DNS) सेवा का प्रयोग इसलिए किया जाता है क्योंकि मनुष्य Domain name (जैसे-ehindistudy.com) को आसानी से याद कर सकता है जबकि जो इंटरनेट होता है वह IP एड्रेस पर आधारित होता है।

DNS सर्वर के द्वारा हम अपनी इच्छानुसार ब्राउज़र में किसी भी वेबसाइट के नाम को टाइप करके उस वेबसाइट से connect कर सकते है जबकि हमें IP address (जैसे:-120.23.149.59) टाइप करने की जरुरत नही पड़ती है।

अगर कोई एक DNS सर्वर domain name को translate नही कर पाता तो यह दूसरे DNS सर्वर से domain name को translate करने के लिए कहता है और यह प्रक्रिया तब तक चलती रहती है जब तक कि domain name को translate नही किया जाता।

DNS को 1983 में Paul Mockapetris और Jon Postel ने प्रस्तावित किया था।

DNS को अच्छी तरह से समझने के लिए हमें domain name तथा IP ADDRESS को भी समझना पड़ेगा।

Physical address & Logical address क्या है?

physical address in hindi:-

Physical address को MAC एड्रेस भी कहते है। यह एड्रेस यूनिक होता है क्योंकि इसे change नही किया जा सकता है।

फिजिकल एड्रेस main मैमोरी में स्टोर होता है, यह एक 48 बिट एड्रेस है जो कि NIC कार्ड में उपस्थित होता है।

इस एड्रेस का प्रयोग डेटा लिंक लेयर में किया जाता है। यह एड्रेस नेटवर्क में कंप्यूटर को identify करने का कार्य करता है।

उदाहरण के लिए MAC एड्रेस:- 05-0h-77-7i-88-9a एक हेक्साडेसीमल वैल्यू होती है।

Logical address:-

इस एड्रेस को virtual एड्रेस भी कहते है तथा यह एड्रेस virtual मैमोरी में स्टोर रहता है।

यह एड्रेस CPU द्वारा generate होता है। यह हर सिस्टम के लिए अलग-अलग होता है तथा इसे change किया जा सकता है।

इस एड्रेस का प्रयोग नेटवर्क लेयर में किया जाता है।

लॉजिकल एड्रेस एक I.P. एड्रेस होता है तथा यह एक 32-बिट एड्रेस होता है।
उदाहरण के लिए IP एड्रेस:-190.10.134.76

TCP/IP MODEL को समझाइये?

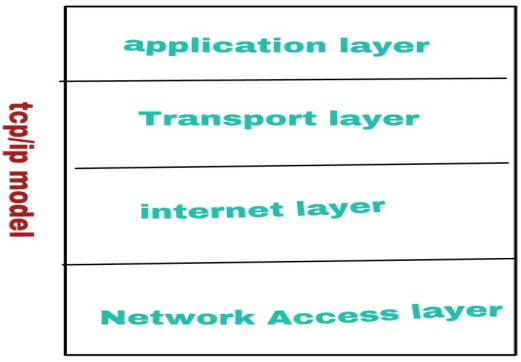
TCP/IP model in hindi:-

TCP/IP का पूरा नाम Transmission control protocol(TCP) तथा internet protocol(IP) है।

TCP/IP वर्ल्ड वाइड वेब का एक प्रोटोकॉल है जिसे हम इंटरनेट कहते है।

TCP/IP मॉडल end-to-end कम्युनिकेशन उपलब्ध कराता है।

TCP/IP को 1970 तथा 1980 के दशक के मध्य U.S. department of defense(D.O.D.) ने विकसित किया था।



TCP/IP मॉडल में 4 लेयर होती है जो निम्न है:-
1:-Host-to-network(network access) layer
2:-Internet layer
3:-Transport layer
4:-Application layer

1:-Network Access layer:-यह लेयर TCP/IP मॉडल की सबसे निम्नतम लेयर है। नेटवर्क एक्सेस लेयर यह describe करती है कि किस प्रकार डेटा नेटवर्क में sent होता है।

2:-Internet layer:-यह लेयर ट्रांसपोर्ट लेयर तथा एप्लीकेशन लेयर के मध्य स्थित होती है। यह लेयर नेटवर्क में connectionless कम्युनिकेशन उपलब्ध कराती है।

इसमें डेटा को IP datagrams के रूप में पैकेज किया जाता है यह datagram source तथा destination IP एड्रेस को contain किये रहते है जिससे कि डेटा को आसानी से sent तथा receive किया जा सकें।

3:-Transport layer:-यह लेयर डेटा के ट्रांसमिशन के लिए जिम्मेदार होती है यह लेयर एप्लीकेशन लेयर तथा इंटरनेट लेयर के मध्य स्थित होती है। इस लेयर में दो मुख्य प्रोटोकॉल कार्य करते है:-
1:-Transmission control protocol(TCP)
2:-User datagram Protocol(UDP)

4:-Application layer:-यह लेयर TCP/IP मॉडल की सबसे उच्चतम लेयर है। यह लेयर ऍप्लिकेशन्स को नेटवर्क सर्विस उपलब्ध करने से सम्बंधित होती है। यह लेयर यूजर को कम्युनिकेशन उपलब्ध कराती है; जैसे:-वेब ब्राउज़र, ई-मेल, तथा अन्य ऍप्लिकेशन्स के द्वारा।

application लेयर ट्रांसपोर्ट लेयर को डेटा भेजती है तथा उससे डेटा receive करती है।

2 tier & 3 tier architecture को समझाइये?

हम निम्न तरीके से यह समझ सकते है:-

2 tier architecture :-

2 tier architecture जो होता है वह client-server architecture पर आधारित होता है। इसमें क्लाइंट तथा सर्वर के मध्य direct कम्युनिकेशन होता है तथा क्लाइंट तथा सर्वर के मध्य कोई तीसरा मध्यवर्ती नही होता है।

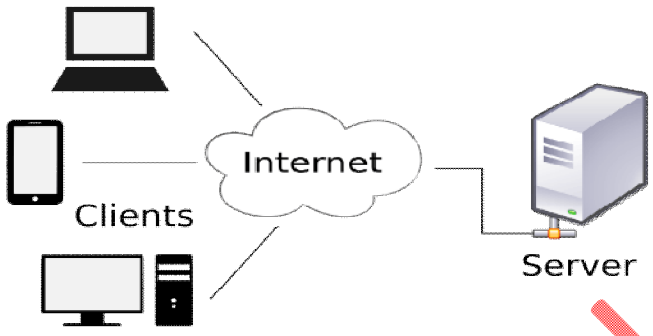


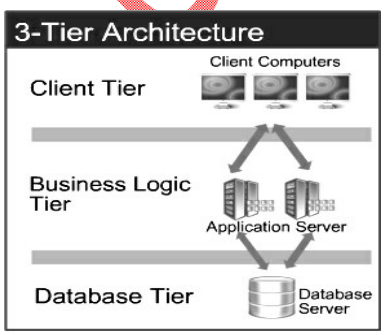
Fig:-2-tier architecture

जैसा की चित्र में दिखाया गया है, 2 tier architecture में दो tier होती है:-
1:-data tier
2:-client tier.

इस architecture में क्लाइंट, सर्वर को कोई task परफॉर्म करने के लिए request करता है तथा सर्वर उस task को पूरा करके क्लाइंट की request को पूरा करता है।

3 tier architecture in hindi:-

जिस तरह 2-tier architecture क्लाइंट सर्वर आर्किटेक्चर होता है उसी तरह 3 tier architecture जो होता है वो client, server तथा database architecture होता है।



जैसा कि चित्र में दिखाया गया है 3 tier architecture में 3 tier होते है:-
1:-Client tier
2:-Businesses logic tier
3:-database tier

इस architecture में क्लाइंट, सर्वर को request भेजता है और सर्वर इस request को डेटाबेस को भेज देता है। फिर डेटाबेस request को पूरा करके सर्वर को भेजता है तथा सर्वर इसको क्लाइंट को वापस भेज देता है।

Virus dropper क्या है?

virus dropper:-

वायरस ड्रॉपर एक प्रकार का malware होता है जो कि वायरस को सिस्टम में drop(install) करने के लिए बनाया गया होता है। वायरस ड्रॉपर हमारे सिस्टम की hard disk तथा अन्य मेमोरी एरिया में वायरस को install कर देते है।

ड्रॉपर जो है वह वायरस नही होता है क्योंकि यह स्वयं वायरस की तरह खुद की copy को create नही कर सकता है।

वायरस ड्रॉपर को detect कर पाना बहुत मुश्किल होता है क्योंकि ये खुद infected नही होता है बल्कि ये वायरस को carry करता है। तथा वायरस ड्रॉपर एक नए प्रकार का वायरस है जिसके कारण इसे antivirus सॉफ्टवेयर भी डिटेक्ट नही कर पाते है।

ड्रॉपर के अंदर वायरस का code को इस प्रकार स्थापित होता है कि जिसके कारण virus scanners भी इसे डिटेक्ट नही कर पाते है तथा वायरस ड्रॉपर कंप्यूटर सिस्टम को infected कर देते है।

What is Social engineering?

Social engineering in hindi:-

Social engineering एक कला है जिसमें लोगों को बहुत ही चालाकी से manipulate(छल) करके उनसे निजी जानकारी प्राप्त कर ली जाती है।

social engineering का प्रयोग हैकर करते है। वे लोगों को इस प्रकार जाल में फांस लेते है जिससे लोग उन पर विश्वास कर लेते है और फिर trick में फंसाकर सारी महत्वपूर्ण सूचना जैसे:- पासवर्ड, बैंक की जानकारी तथा अन्य महत्वपूर्ण information को आपसे प्राप्त कर लेते है।

सोशल इंजीनियरिंग में 4 steps होते है:-

1:-सबसे पहले हैकर आपके बारें में सूचना को एकत्रित करते है।
2:-फिर आपको विश्वास में लेकर आपके साथ relationship को बेहतर करते है।
3:-फिर जब आपके relation हैकर से सही हो जाते है तो वह इसका फायदा उठाते है।
4:-और अंत में अपने गलत motive को अंजाम देते है।

उदाहरण के लिए:- आपके दोस्त का फेसबुक अकाउंट हैक हो जाता है, और उस अकाउंट से आपको मैसेज आता है। क्योंकि मेसेज दोस्त के अकाउंट से आया है आप उस पर विश्वास कर लेते है। उस मेसेज में एक लिंक होता है जिसे आप click करते है और इस प्रकार आप malware से infected

हो जाते है। जिससे साइबर अपराधी आपके सिस्टम में control कर लेते है तथा आपकी sensitive information को चुरा लेते है।

What is phishing?

Phishing attack:-

जिस प्रकार मछली (fish) को पकड़ने जाल फेंका जाता है उसी प्रकार लोगों के क्रेडिट कार्ड, बैंक की जानकारी, पासवर्ड तथा अन्य संवेदनशील जानकरी को चुराने के लिए साइबर अपराधी लोगों के e-mail, फेसबुक, तथा अन्य कम्युनिकेशन साधनों में एक link भेजते है।

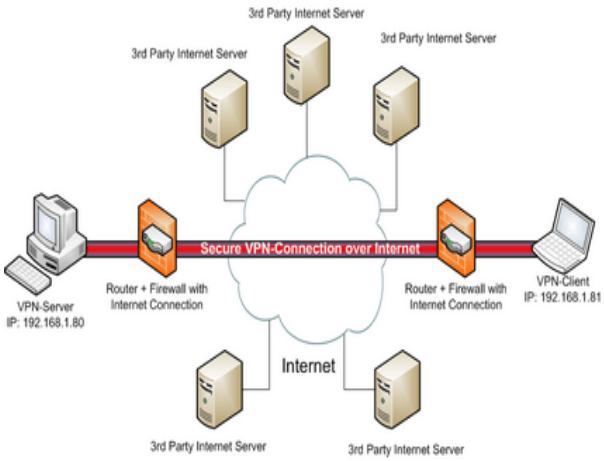
यह link हमें एक बहुत बड़ी व अच्छी कंपनी (जैसे-फेसबुक, paypal) से आया हुआ प्रतीत होता है।

वे हमें इस लिंक में click करने के लिये कहते है ये लिंक वह हजारों लोगों को भेजते है कुछ लोग इस trick में फंस जाते है।

आसान शब्दों में कहें तो phishing का प्रयोग लोगों को मुर्ख बनाने के लिए किया जाता है।

उदहारण के लिए:- एक व्यक्ति को फेसबुक में एक message आता है, उसमें paypal account का fake लिंक होता है। उसमें लिखा होता है इस लिंक पर click करके अपनी personal सूचना को update करें, नही तो आपका paypal account को permanently block कर दिया जायेगा।

VPN क्या है?



source:-VPN diagram in hindi

VPN को हम निम्न बिंदुओं के आधार पर आसानी से समझ सकते है:-

1:-VPN का पूरा नाम virtual private network (वर्चुअल प्राइवेट नेटवर्क) है।

2:-VPN ऐसी तकनीक है जो असुरक्षित पब्लिक नेटवर्क (जैसे:-इंटरनेट) के ऊपर एक सुरक्षित नेटवर्क बनाता है।

3:-VPN का प्रयोग बहुत सारें विभागों में महत्वपुर्ण व संवेदशील सूचना तथा डेटा को protect करने के लिए किया जाता है।

4:-VPN एक encrypted कनेक्शन का निर्माण करता है जिससे कोई भी डेटा इससे होकर गुजरता है वह encrypt हो जाता है जिससे उसे कोई भी हानि नही पहुँचा सकता।

5:-अगर आप VPN नेटवर्क का इस्तेमाल लैपटॉप में करते है तो आप कही से भी अपनी कंपनी का काम कर सकते है।

6:-VPN के द्वारा आप blocked websites को भी access कर सकते है ।

7:-अगर आप अपना ip address बदलना चाहते है तो VPN आपको ये facility उपलब्ध कराता है।

What is intrusion detection system (IDS)?

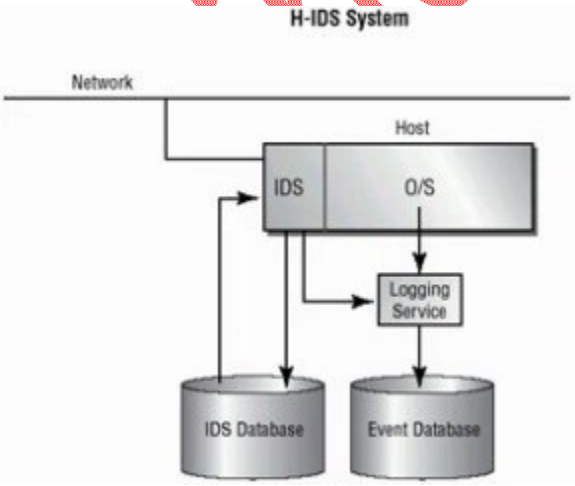
IDS in hindi:-

IDS का पूरा नाम intrusion detection system है। IDS एक प्रकार का security सॉफ्टवेयर है जिसका प्रयोग सिस्टम तथा नेटवर्क को unwanted तथा unauthorized access से सुरक्षित करने के लिए किया जाता है। यह हैकर, attacker तथा अन्य खतरनाक attacks से सिस्टम को बचाता है।

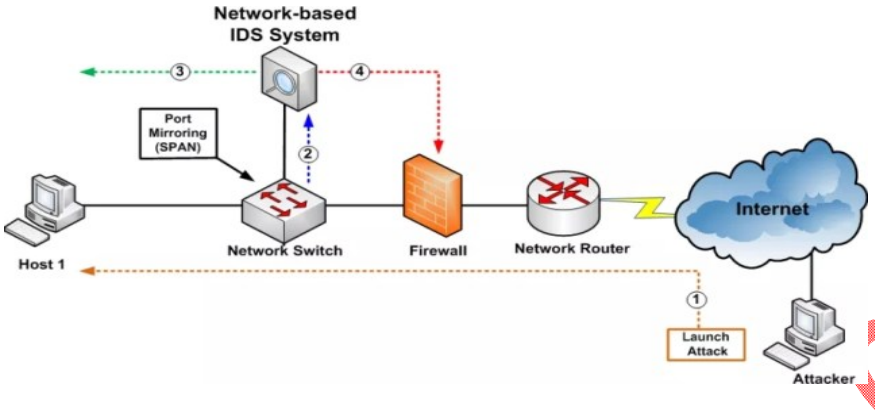
जैसा कि इसका नाम है यह नेटवर्क तथा सिस्टम में intrusions को detect करने के लिए प्रयोग किया जाता है और जैसे ही कोई intrusions मिलता है तो यह alert कर देता है।

IDS का प्रयोग विभिन्न तरीके से malicious traffic को डिटेक्ट करने के लिए किया जाता है। IDS के दो प्रकार निम्न है:-
1:-Host based IDS
2:-Network based IDS.

1:-Host based IDS(HIDS):- HIDS होस्ट(host) में इनस्टॉल रहता है और यह केवल उस traffic को देखता है जो उस होस्ट में उत्पन्न होता है या उस होस्ट से होकर गुजरता है। अगर कोई malicious activity दिखाई देती है तो यह केवल इसी होस्ट में detect करता है।



2:-Network based IDS(NIDS):- NIDS उन सभी hosts को देखता है जो नेटवर्क में उपस्थित होते है तथा इनमें होने वाले सभी malicious traffic को डिटेक्ट करता है। NIDS सम्पूर्ण नेटवर्क को monitor करता है।



What is Botnet?

Botnet:-

Botnet को jombie army भी कहा जाता है। Botnet प्राइवेट कंप्यूटरों का एक नेटवर्क होता है जो कि zombie से संक्रमित हुए रहते है(जिसका पता इन कंप्यूटरों के मालिकों को भी नही होता है) तथा इन कंप्यूटरों के समूह का प्रयोग अन्य कंप्यूटरों को संक्रमित करने के लिए किया जाता है।

अन्य कंप्यूटरों को संक्रमित करने के लिए ये virus, malware तथा अन्य खतरनाक तत्वों को भेजते है।

Botnet में प्रत्येक कंप्यूटरों को 'bot' कहा जाता है। Botnet का अर्थ है:- Bot का अर्थ है रोबोट तथा net का अर्थ है नेटवर्क।

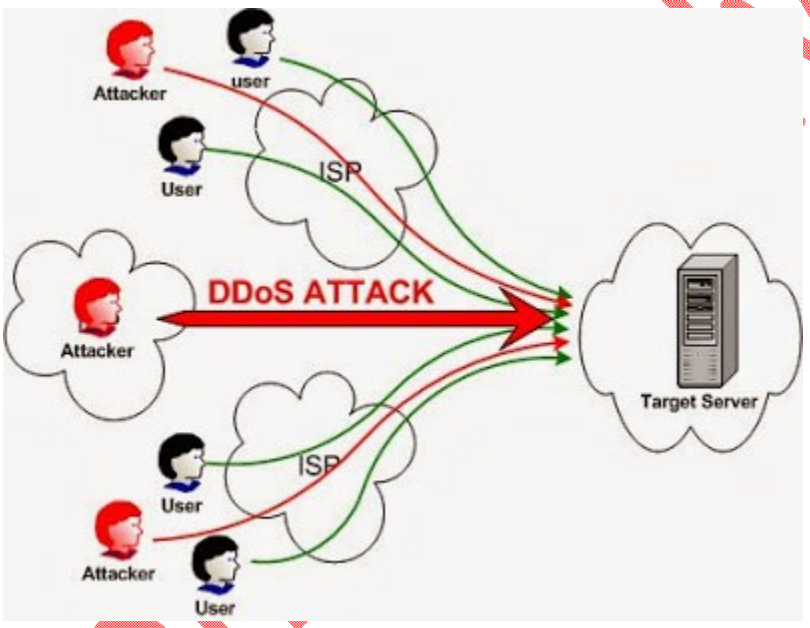
What is DoS attack?

Denial Of Service attack:-

DoS अटैक को Denial of service अटैक कहते है इस अटैक का प्रयोग हैकर किसी नेटवर्क या मशीन को उस पर access करने वाले यूज़र्स के लिए unavailable कर देते है। इस अटैक का मुख्य उद्देश्य यूज़र्स को किसी सर्विस जैसे-इंटरनेट पर access करने से रोकना है।

इस अटैक का हैकर बहुत बड़े हथियार की तरह प्रयोग करते है और उन सभी services को यूज़र्स के लिए unavailable कर दिया जाता है जो कि इंटरनेट से जुडी हुई होती है। DoS अटैक में नेटवर्क या मशीन को ओवरलोड कर दिया जाता है जिस कारण लोग उस पर access नही कर पाते है।

DoS अटैक में नेटवर्क या मशीन को unavailable करने के लिए सिर्फ एक कंप्यूटर और एक इंटरनेट कनेक्शन की आवश्यकता होती है।



DDoS अटैक DoS का ही विस्तृत रूप है, DDoS का पूरा नाम distributed denial of service अटैक है परन्तु इस अटैक में नेटवर्क या मशीन को unavailable करने के लिए एक से ज्यादा कंप्यूटर और एक से ज्यादा इंटरनेट कनेक्शन की आवश्यकता होती है।

what is checksum?

Checksum verification:-

“checksum का प्रयोग दो समूहों के डेटा की तुलना करने के लिये किया जाता है और यह सुनश्चित किया जाता है कि दोनों समूहों का डेटा समान है और उसमें कोई त्रुटि नही है।”

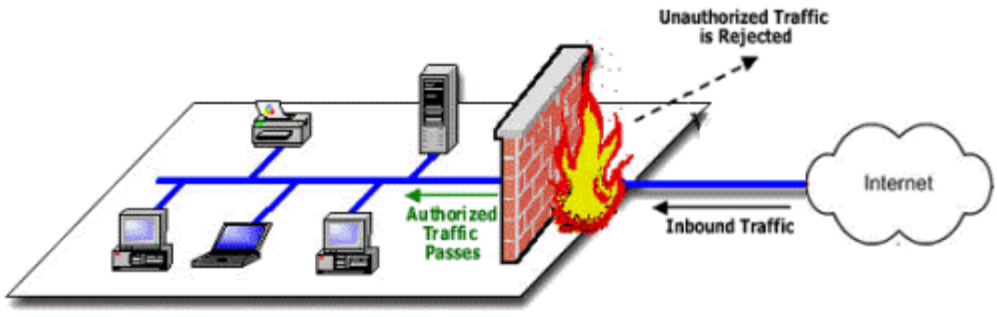
इस विधि में sender डेटा की checksum वैल्यू को generate करता है तथा डेटा को receiver को send कर देता है। इसके बाद receiver उस डेटा की इसी तरह calculation करता है और checksum वैल्यू को generate करता है। यदि दोनों वैल्यू match करती है तो ये समझा जाता है कि डेटा का transmission सही तरीके से हुआ है उसमें कोई त्रुटि नही है।

checksum डेटा में त्रुटियों को detect करने की विधि है। checksum को हम hash sum भी कहते है।

checksum का प्रयोग डेटा(जो कि एक स्टोरेज एरिया से दूसरे में transmit हुई है) की integrity को सुनश्चित करने के लिए किया जाता है।

What is firewall in hindi and types of firewall

firewall:-



फ़ायरवॉल को निम्न बिंदुओं के आधार पर आसानी से समझ जा सकता है:-

1:-फ़ायरवॉल एक नेटवर्क को सुरक्षित करने वाला डिवाइस या सिस्टम होता है जो कि unauthorized यूज़र्स तथा खतरनाक तत्वों को नेटवर्क में access करने से बचाता है।

2:-फ़ायरवॉल हार्डवेयर तथा सॉफ्टवेयर दोनों प्रकार का होता है।

3:-फ़ायरवॉल हमारे नेटवर्क के लिए फ़िल्टर की तरह कार्य करता है जो harmful information को रोक देता है।

4:-फ़ायरवॉल को किसी private नेटवर्क तथा इंटरनेट के मध्य स्थापित किया जाता है और जितना भी इन दोनों के मध्य डेटा का कम्युनिकेशन होता है वह फ़ायरवॉल से होकर गुजरता है। यह एक दीवार की तरह कार्य करता है जो कि आग रूपी unsafe or harmful डेटा से नेटवर्क को protect करता है।

5:-फ़ायरवॉल उसी ट्रैफिक को अपने से गुजरने देता है जो उसकी policy के अनुसार सही हो।

6:-फ़ायरवॉल किसी भी प्रकार के attack के लिए एक barrier की तरह कार्य करता है। जिससे hacker नेटवर्क को हैक नही कर पाते है और जिससे हमारी सारी महत्वपूर्ण सूचना चोरी हो जाने से बच जाती है।

7-वह प्रत्येक व्यक्ति जो अपने सिस्टम से इंटरनेट में access करता है उसको अवश्य ही फ़ायरवॉल को स्थापित करना चाहिए।

types of firewall in hindi:-

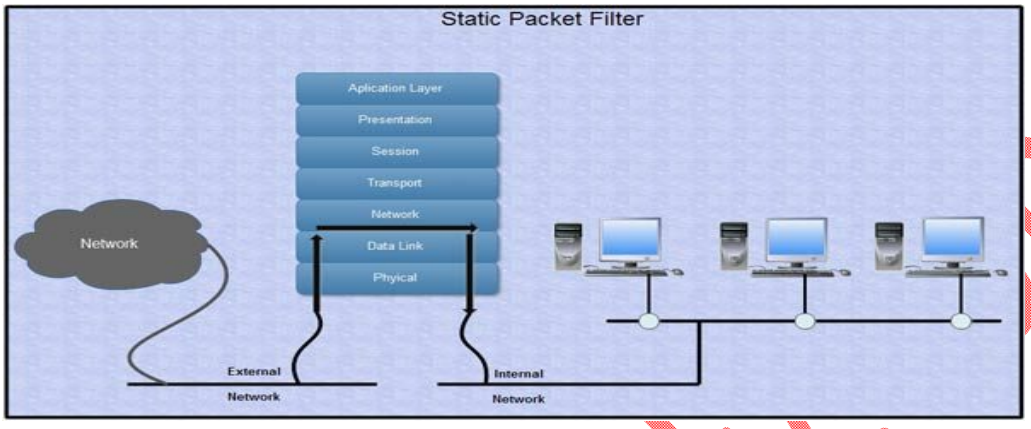
फ़ायरवॉल निम्नलिखित प्रकार के होते है:-

1:-packet filter firewall:-यह फ़ायरवॉल OSI मॉडल के नेटवर्क लेयर में कार्य करता है। यह फ़ायरवॉल अंदर जाने वाले तथा बाहर आने वाले पैकेटों को analyze करता है तथा यह केवल उन्हीं पैकेटों को अपने से गुजरने देता है जो फ़ायरवॉल policy के अनुसार सही हों।

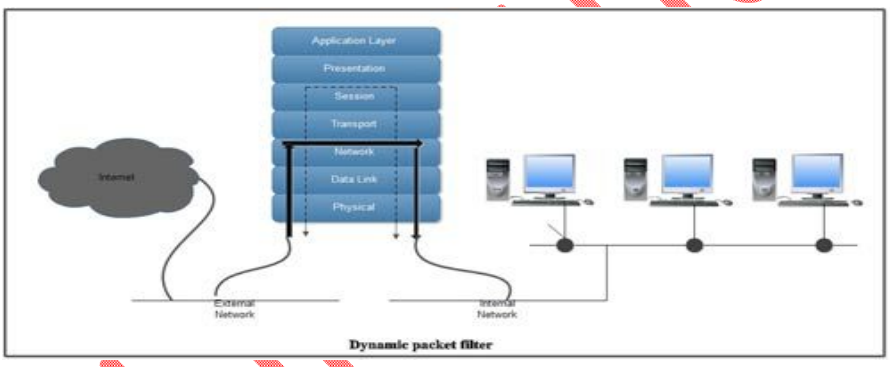
प्रत्येक पैकेट की यह फ़ायरवॉल जाँच करता है तब निर्णय लेता है कि यह पैकेट आगे देना चाहिए या नही। यह local नेटवर्क को घुसपैठ से बचता है।

Packet filter firewall दो प्रकार के होते है जो निम्न है:-

(a):-stateless packet filter:- इस फ़ायरवॉल में पैकेट्स के बारें में जानकारी नही होती है। इस प्रकार के फ़ायरवॉल को static फ़ायरवॉल कहते है। ये फ़ायरवॉल इतने प्रभावी नही होते है।

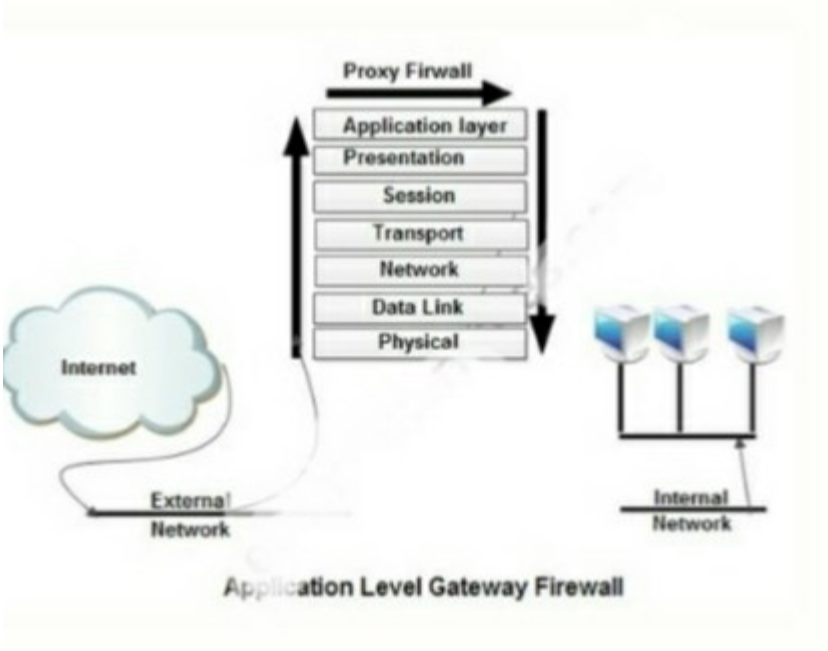


(b):-stateful packet filter:-यह फ़ायरवॉल पैकेट्स के बारें में जानकारी उपलब्ध कराता है। इसे dynamic फ़ायरवॉल भी कहते है। ये फ़ायरवॉल अधिक सुरक्षा provide कराते है।



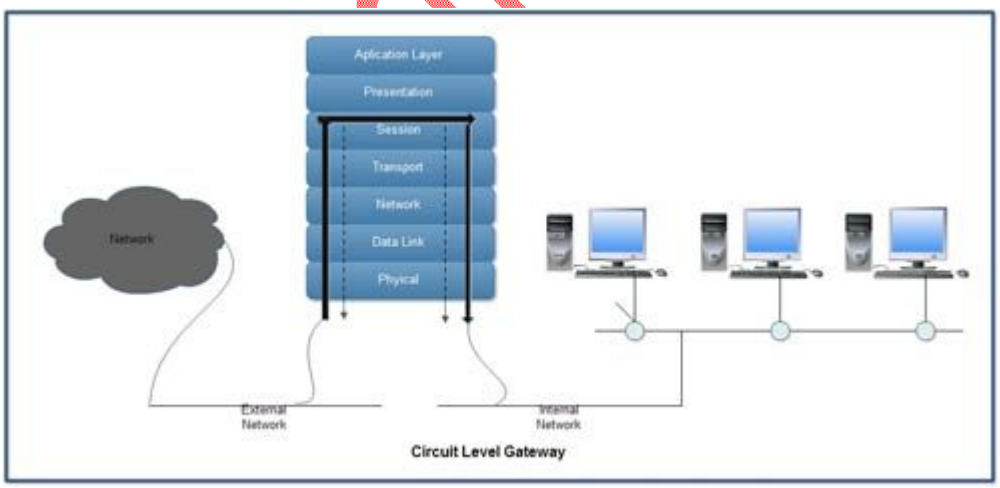
(2):-Application level gateway firewall:-इसे application proxy भी कहते है। यह फ़ायरवॉल एप्लीकेशन की सूचना के आधार पर पैकेट को अपने से गुजरने देता है या पैकेट को रोक देता है। एप्लीकेशन की सूचना पैकेट में उपलब्ध रहती है।

यह फ़ायरवॉल एक प्रकार का proxy server है जो कि applications को proxy उपलब्ध करता है।



(3):-Circuit-level gateway firewall:-यह फ़ायरवॉल OSI मॉडल के session layer में कार्य करता है। यह फ़ायरवॉल TCP(transmission control protocol) या UDP(user datagram protocol) की security को उपलब्ध कराता है।

यह फ़ायरवॉल TCP या UDP में प्रत्येक पैकेट को analyze करता है तथा फ़ायरवॉल policy के अनुसार यह पकेटों पर action लेता है।



What is Trojan horses?

Trojan horse:-

Trojan horse एक हानिकारक कंप्यूटर प्रोग्राम होता है जो कि हमारे सिस्टम में नियंत्रण कर लेता है और malicious action को अंजाम देता है। Trojan, वायरस की तरह अपनी copy तो create नही कर सकते परन्तु ये वायरस को सिस्टम में install कर सकते है।

Trojan horse को trojan भी कहते है, trojan को लोग धोके से डाउनलोड कर लेते है यह सोच कर की यह फ़ाइल सही है परन्तु ऐसा नही होता बल्कि यह लोगो को फ़साने के लिए trick होती है।
उदाहरण के लिए:- एक दोस्त की फेसबुक id हैक हो जाती है और उसकी id से एक मैसेज आता है कि इस गेम को डाउनलोड करो यह बहुत बढ़िया गेम है, परन्तु वह गेम ना होकर एक trojan होता है।

एक Trojan क्या कर सकता है?:-

1:- एक Trojan, सिस्टम की फाइलों तथा डेटा को डिलीट कर सकता है।
2:-महत्पूर्ण information तथा पासवर्ड को चुरा सकता है।
3:-सिस्टम को lock कर सकता है।
4:-malware को डाउनलोड करके install कर सकता है।
5:-सिस्टम को दोबारा शुरू कर सकता है।
6:-CD को infect कर सकता है।
7:-सिस्टम की स्क्रीन में मैसेज को show कर सकता है।
8:-प्रोग्राम को बन्द कर सकता है।

What is Worms?

Computer Worms:-

worm एक कंप्यूटर प्रोग्राम या वायरस होता है जो अपनी खुद की copy बना लेता है और दूसरे कंप्यूटर में spread हो जाता है।

worm भी virus की तरह ही समान होते है लेकिन worm स्वतन्त्र होते है इन्हें दूसरे कंप्यूटर में spread होने के लिए किसी person की आवश्यकता नही होती है बल्कि ये स्वयं ही दूसरे कंप्यूटर में फ़ैल जाता है। worms नेटवर्क का प्रयोग करके अपनी copy को दूसरे कंप्यूटरों में भेजता है।

worm नेटवर्क में e-mail, web page, तथा chat message के द्वारा आसानी से दूसरे कंप्यूटरों में फ़ैल जाते है।

Worm कंप्यूटर की बहुत ही crucial फाइलों को delete कर सकता है। Worm कंप्यूटर को धीमा कर देता है जिससे कंप्यूटर के प्रोग्राम काम करना बन्द कर देते है।

types of computer worms in hindi:-

कंप्यूटर worms निम्नलिखित प्रकार के होते है:-
1:-E-mail worm:- ये worm infect हुए ई-मेल message के कारण फैलते है।

2:- Internet Worms:- ये worm इंटरनेट में ऐसे कंप्यूटर को ढूंढते है जिनको infect किया जा सकता है। अगर ऐसे सिस्टम मिलते है तो यह उनको infect कर देता है।

3:- File sharing worm:- ये worm कंप्यूटर में ऐसे नाम से फोल्डर बनाकर save हो जाते है जिससे हमें शक भी नही होता है कि worm इस folder में स्टोर हो सकता है।

4:-IRC worm:- इस प्रकार के worm अन्य सिस्टम में message के द्वारा infected link भेज देते है। जिससे दूसरे सिस्टम में भी यह worm चले जाता है।

Types of virus?

Types of computer virus in hindi:-

कंप्यूटर में बहुत प्रकार के वायरस होते है कुछ निम्न है:-

1:-Boot virus:- बूट वायरस सिस्टम की फ्लॉपी तथा हार्ड डिस्क को infect करता है। इस प्रकार के वायरस से बचने के लिए हमें यह देखना चाहिए कि फ्लॉपी डिस्क अच्छी तरह से write(लिखी) हो तथा हमें unknown फ्लॉपी डिस्क को डिस्क ड्राइव में रखकर सिस्टम को start नही करना चाहिए। इस प्रकार के वायरस को Master Boot Sector Virus भी कहते है।

2:-Macro virus:- मैक्रो वायरस मैक्रो प्रोग्रामिंग लैंग्वेज का प्रयोग करके बनाये जाते है। ये वायरस फाइल्स को infected करते है।

3:-e-mail virus:- e- mail वायरस एक नया वायरस है। यह message के आस पास घूमता रहता है और यह बहुत सारें e-mail address को अपने आप send हो जाता है।

4:-Memory resident virus:-ये वायरस RAM में स्टोर रहते है। और RAM मेमोरी को infected करते है जिससे सिस्टम खुलते ही बन्द हो जाता है।

5:-file virus:- फ़ाइल वायरस .exe files,.zip files तथा .bin files के साथ जुड़े रहते है। ये वायरस execute होने वाली फाइल्स को infect कर देता है।

5:-network virus:- ये वायरस लोकल एरिया नेटवर्क में spread हो जाता है और नेटवर्क को slow कर देता है। यह इंटरनेट के माध्यम से भी फ़ैल जाता है।

6:- Polymorphic Virus:-यह वायरस बहुत ही complicated वायरस है जो कि कंप्यूटर के functions को effect करता है। इस प्रकार के वायरस को detect कर पाना बहूत मुश्किल होता है क्योंकि ये वायरस हर बार अपने आप को खुद ही encrypt कर लेता है जिससे इसका signature बदल जाता है।

What is virus?

VIRUS in hindi:-

virus को हम निम्न बिंदुओं के आधार पर आसानी से समझ सकते है:-

1:-virus एक छोटा प्रोग्राम होता है जो कि हमारे सिस्टम में किसी बड़े प्रोग्राम को संक्रमित(infected) कर देता है जिससे कि सिस्टम ठीक ढंग से कार्य नही कर पाता या ख़राब हो जाता है।

2:-वायरस अपने खुद की copy बना लेता है तथा दूसरे computers में किसी माध्यम(जैसे:- pendrive, CD आदि) से चले जाता है और उसे भी infected कर देता है। इस प्रकार एक वायरस बहुत सारें कंप्यूटरों को infected कर देता है।

3:-वायरस का मुख्य उद्देश्य डेटा तथा महत्वपूर्ण जानकारी को infected करके नष्ट तथा चुराना होता है।

4:-जितने भी वायरस होते है वो man-made होते है मतलब वायरस इंसान के द्वारा ही बनाये जाते है ये खुद नही उत्पन्न होते है।

5:-सबसे पहले वायरस का नाम Elk Cloner था जिसको 1982 में Rich Skrenta ने लिखा था।

6:-वायरस को e-mail के जरिये बहुत जल्दी तथा आसानी से भेजा जा सकता है।

7:-वायरस से बचने के लिए antivirus सॉफ्टवेयर का प्रयोग किया जाता है।

वायरस क्या कर सकता है?:-

1:-files को destroy कर सकता है।
2:-सिस्टम को slow कर सकता है।
3:-अपने आप सिस्टम में message को show कर सकता है।
4:-सिस्टम में अपना पूरा नियंत्रण कर सकता है।

IT act 2000 क्या है?

information technology act 2000 को ITA 2000 भी कहते है. यह भारतीय संसद का एक एक्ट है इसे 17 अक्टूबर 2009 को एक घोषणा द्वारा इसे संशोधित किया गया.

यह एक्ट साइबर क्राइम, ई कॉमर्स से सम्बन्धित क़ानून है.

हम सभी इन्टरनेट में बहुत सारी activities करते है जैसे:- ब्राउज़िंग, selling, surfing आदि. तो इन सभी को सुरक्षित करने के लिए एक act बनाया गया जिसे हम IT act 2000 कहते है. इस act के तहत आपको इनफार्मेशन टेक्नोलॉजी का इस्तेमाल करने के प्रावधान क्या है, नियम क्या है बताये गये हैं.

आजकल हमारे सभी काम electronically होता है पहले हम verbal कम्युनिकेशन करते थे. परन्तु हम आजकल e communication (जैसे- फेसबुक, whatsapp, ट्विटर आदि) करते है, पहले सामान दुकान में जाकर खरीदते थे परन्तु आज e commerce वेबसाइट (जैसे:- amazon, snapdeal) से खरीद लेते है. और हमारी governance भी e governance हो गयी है.

लेकिन इसका नेगेटिव पार्ट यह है कि जो अपराधी है वह इसमें अपराध करते है तो उनके लिए एक law बनाया गया है जिसे हम IT act 2000 कहते है तथा इसमें बहुत से प्रावधान है.

IT act में 13 भाग तथा 90 अनुभाग है. तथा यह इंडियन पैनल कोड, 1860, इंडियन एविडेंस एक्ट, 1872, बैंकर्स बुक एविडेंस एक्ट, 1891, रिज़र्व बैंक ऑफ़ इंडिया एक्ट, 1934 आदि पर आधारित है.

cyber crime क्या है?

साइबर क्राइम:- क्राइम वह काम है जो क़ानून के विरुद्ध तथा मानवता के विरुद्ध किये जाते है. और वह क्राइम जो इन्टरनेट, साइबर तथा नेटवर्क पर किये जाते है, वह सारें के सारें साइबर क्राइम कहलाते है.

दुसरे शब्दों में कहें तो यह एक illegal activity है जिसे कंप्यूटर या इन्टरनेट के द्वारा किया जाता है.

types of cyber crime:- साइबर के बहुत प्रकार के हो सकते है यहाँ कुछ निम्न है:-

1:- हैकिंग
2:- denial of service attack
3:- computer fogery
4:- phishing
5:- spoofing
6:- threatning
7:- online gambling
8:- pornography
9:- piracy

किताब खरदने के लए धयवाद तथा आपके लए एक सुवधा:- अगर आपको लगता है क इसम कोई टॉपक या notes नहं है तो आप मुझे बता सकते है. म आपको वह टॉपक send कंगा. आप मुझे whatsapp तथा call कर सकते है. मेरा मोबाइल नंबर 9761480219 है. वेबसाइट:- www.ehindistudy.com