Are you safe? the threat of hackers, pc hijacing, worms, and web security

ABSTRACT

Web security is one of the complicated stuff and basically these subject is only handle by good trainers and well experience persons now a days as people are widely using WIRED networks so, first we need to understand the basic concepts of security in this network world. Web security is branch of computerscienceespecially related to the internet. Itsmain objectives is to establish the rules and measurements to be taken against the attacks caused over internet. Network is defined as a set of interlinking lines resembling a net and the computer network is a system of interconnected computers. Internet was created to share information and in last few decades, the internet has been affected by many of the security attacks. some of these threats which are caused in the internet are spoofing man in the middle attack, denial of service , hijacking , worms, hackers, password sniffing etc……

Introduction:

Internet provides many benefits at the same time it also creates very tremendous security problems. According to study

Which is conducted by United States of America Online and the national internet security, almost eighty %of the computers in the US are affected by spyware and almost twenty % of the machines have viruses.

The internet represents an incorrect channel for information which has to be exchanged were leading to high risk of fraud. so , to protect the transfer of data we use different kinds of methods. and the strategies and methodologies of web security often differs some, how from other web

technologies because of it’s elusive objectives network security is generally considered as security protector of an organisation by keeping out rid of intruders. data is to be protected in the organisation from the hackers who are trying to capture the messages .

Network security:

Network security is generally considered as giving protection for the organization by keeping far from the hackers. Information security mainly focuses on protecting the data resource from malware attacks or simple mistakes which are done by people in organisation with help of DLP techniques.

Information security:

Information security means protecting information from the unauthorised users, the two terms information security and computer security and information assurance which are often used differently. These all fields which are interrelated and share some commongoalsof protectingconfidentiality, integrity and availability.

Governments, corporations, military, hospitals, financial institutions, and some private businesses. Huge amount of confidential information about all their specific employees, products, customers and research. All these information will be collected with processed and store computers and also can be transmittedacross all other network . protecting confidential information is very important in business requirement and in all cases an ethical and legal requirement should be done.

Three core principles of information security:

Confidentiality

Integrity

Availability

Confidentiality:

in this confidential information can only accessed or copied by users who are right to authorised so confidentiality is maintained. When there is only correct need to use. When the external user tries to access the information who are not actually authorised to use the information then confidentiallyfailureoccurs

Integrity:

This helps to protect the un-authorised modification or any information destruction from external. Means data cannot be change without proper authorisation.

Availability:

In this the information which is present in computer systems and that information is protected by security controls whenever information is needed.

ex:

Denial of service attack

Security vulnerabilities:

The internet explorer has thrall down to one and many security vulnerabilities and some of these vulnerabilities like spyware, computer viruses and adware are made possible by exploitable errors and bugs in the architecture of internet explorer. The errors may be as Spyware which is installed in computers in which important information will be copied without our knowledge and this kind of malware is very hard to detect. Adware as well is one of malwares which is in the form ofadvertisementon computer when you are

downloading anything on the system . lastly Computer virus is one of the viruses which are created by computer itself.

Software security is most important for consumers, vendorsbecause attackers that create attacks even may cause fairly large sequential effects and when all these attacks has been discovered then required software is sold for the consumers depending on the vulnerabilities.

Some of the vulnerabilities are:

Web servers

Exposures

Workstation Service

Windows authentication

Windows RAS

MSQL

Instant Messaging

File Sharing Applications

Mail Client

Instant Messaging

Protection against these vulnerabilities:

Apply latest service packs and require security updates and http services also for the operating system and any other applications are loaded to that same host. And for the high level security we consider the automatic update features so that they are up to date.

1) It’s better to install the host based antivirus and also intrusion detection software in the system. so that the updates are done for log files frequently.

2) It’s better to disable all unused script interpreters like for ex: perl, perlscript, vb script, jscript and javascript and php.

3) If it’s possible enable logging option and check the logs frequently . so, that we can summarise the updates events which are occurred in the system.

4) Use the sys log so that system can store an operating system and http logs safely to another system.

5) Remove all the system tools which are often used by attackers for ex: tftp (. exe), ftp. exe, cmd. exe , bash, net. exe and remote. exe and telnet (. exe).

6) Limit all the applications which are running on host-http and also its which are the services supporting it.

7) Use unique passwords and naming conventions on all public facing system rather than on internal system. Because when ever any information leaked from the public system shouldn’t make any attacks in the internal systems.

IPSec:

Internet protocol security is acommunicationprotocol which is based on IP and internet protocol. Security appends

security of communication to IP . both TCP/IP and UDP/IP acquire the security from it.

IPSec also provides integrity ensurance , encryption , Authentication of each data stream. Internet protocol security is a protocol which suite in protecting the internet protocol communications by authenticating, encrypting the each of data stream.

IPSec is internet protocol security in which windows XP 2000 , 2003 machines had built this mechanism . IPSec is like a protocol were it is designed for protecting all individual TCP/IP packets which are travelling in our network by using public encryption key.

IPSec is used to protect the servers and workstations by using mechanism called as firewalls. Were firewall is like a software which is design to permit

or reject the network transactions by creating some rules and it is used to protect the network by allowing correct information to pass from it. So, many computers are included by software firewall to protect unauthorised threats from outside.

We can block the specific users with the help of IPSec:

It is easy by creating simple policy which will tell a computer to block all the specific IP traffic which are created by them. Internet traffic uses HTTP, HTTPS, which uses tcp ports like 80 and 443 as their destination ports respectively. so, by blocking these specific traffics you will be able to manage stopping the specific require computer from browsing internet. You can also block specific user when the person is surfing or browsing the internet.

IPSec policy must be created for blocking all the internet traffics in computer. Which will block all HTTP traffic. For this we can change this policies specifically for any computer by influncing the computer IPSec policy and we can also configure the group policy object on the specific site and as a domain or as a organisation unit.

For example:

Finding the correct balancing between taste of user and function is very difficult . let us consider one of the site www. LLOYDS. com, this is online banking system site which is used by all users but, specific people can only login account which has account in this in this bank. The new users can access total information about the bank. So, the admin can manage all users information that when the visitor is login and if any transactions are made by

him and this information is kept confidential for the bank safety. Here admin can track the user information regarding his visiting the pages.

Web traffic is defined as the amount of data sent and received by users to specific web site. Internet traffic is defined as flow of data in this we can able to know no of persons visited and number of pages used

by persons. These site checks the incoming and outgoing traffics so that no of pages which are popular and able to know these pages are viewed by the people in particular country.

Web traffic measuring:

Web traffic is measured to check the popularity of internet sites and single pages within sites.

Web traffic is also measured by packet sniffing.

Types:

No of visitors

Pages viewed by each user

Duration of visit

Duration of pages

Domain class

Important requested pages

Requested entry and exit pages

Busy times

And Top paths

The fundamental truth of success of web product development is made by keeping user in mind. Direct correlation exists between the techniques which are used for customers experience who are using the online services. Now a days both personal and professional activities are done online and most of the organisations uses multiple sites . so, online success depends on website and its applications.

Measurements of user experience:

There are different kinds for user experience they are classified in 3 types depending on the customer and his satisfaction.

First stage: General Knowledge

In this type it provides basic idea of the site or its performance

Second stage: understanding behaviour of user

In this understanding what the user is doing and were problem exists.

Third stage: influencing the users

This is last stage were websites and applications are forced to all users to influence Success to create positive experience.

COOKIES:

Cookie is also known as web cookie and browser cookie and HTTP cookie, it is like piece of text which is stored on user computer by their net browser . cookies are created by Netscape to give memory for servers and browsers.

server will not remember about the web pages which sent to browser for this problem cookies were introduced . these cookies are very easy to maintain.

Cookies working:

Name-value

Expire date

Domain

And path

Name and value:

Every cookie has name and value which contains the actual information. these two pairs are used for our benefit as easy for searching by name and what value is assigned for it.

Expire date:

Every cookie has expiry time after that cookies are smashed so, we have to specify expiry time for cookies or else when ever browser closes it will smash.

Domain:

Each cookie has domain and path were domain specifies the browser to which a particular cookie should sent. Path has to set a specific directory where the cookies are active.

Conclusion:

As lots of information available at web services i. e. World Wide Web and these are successful in providing services to all the user with the help of web security that provides all the benefits of using a safe web access and continuous data transmission between both the end devices. Machine surviving has been changed because of increase of internet population It figures out, all the relevant information regarding the user at client side and traces out web sites accessed during the web session.

References:

http:///www. semissourain. com

http:///www. econ. berkeley. edu. com

http:///en. wikipedia. org

http:///www. tu-dresden. de

http:///en. wikipedia. org//websecurity

http:///www. sans-ssi. org

http:///www. freewebs. com

http:///www. myfastpc. com

http:///www. foruxfund. ees. net. nz

http:///en. wikipedia. org//ipsec