ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Problems Occurs In Web and Its Solutions

Prasanna Venkatesh K*, Nithyalakshmi S
Sri Krishna College Of Engineering And Technology, Coimbatore,India

Abstracts

Web security is related to internet and to secure the data transformation through network. It is developed to overcome the problems occurred by the hackers. The private data are destroyed by the unauthorized hackers through virus. Here the paper discusses about the occurrence of problems and solutions.

Keywords: Web, internet.

Introduction

Web security is computer security which related to the internet and also called as network security. Its objective is to establish rules and measures to use against attacks over the internet. The internet represents an insecure channel for exchanging information leading to a high risk of fraud such as phishing.

There are some methods of attacking like masquerading, message tampering, exploiting etc. The security can be done by several ways including frequent change of password and user id. Security encompasses equipment deployment, authenticating users, guarding data, tracking user activity. There are several types of securities namely network layer security, security token, electronic mail security.

There are many security risk will occur while using the internet. Risk is a measure of the cost of vulnerability, which takes into account the probability of a successful attack.

Problems

There are several problems occurs while using internet. Some of the issues are:

Denial of Service
Denial of Service attacks are increases, such as SYN Flood, Ping of Death and LAND Attack, its not only to theft information, but to disable a device so users no longer have access to network resources.

Using Trojan Horses or other malicious attachments, hackers plant tools on hundreds and sometimes thousands of computers to be used in future attacks.

To protect your own LAN from attacks, you need to prevent your LAN computers from being compromised and used in attacks on others.

Authorization
Hackers break the network can view, alter, or destroy private files. Hackers has control others computer and access their confidential data.

Hackers may use a variety of readily available tools to break into the network.

Virus
Viruses are destructive programs that attach themselves to E-mail, applications and files. Once on your LAN computers, viruses can damage data or cause computer crashes. Users can quickly damage entire networks by unknowingly downloading and launching dangerous computer viruses.

Viruses can also be used as delivery mechanisms for hacking tools, putting the security of the organization in doubt, even if a firewall is installed.

Capturing Data
Hackers using programs called packet sniffers can capture your data as it passes from your network over the internet and convert it into a readable format.
The source and destination users of this information never even know that their confidential information has been tapped.

Error Handling
Error handling is dealing with exceptions. Exceptions such as user data validation messages, missing pages should be handled by the code so that a custom page is displayed that does not provide any system information to the user.

It is the process of responding to the occurrence, during computation. It is provided by specialized programming language constructs.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Hardware exceptions mechanisms are processed by CPU.

Phishing
It is the process of acquiring information such as username, passwords and credit card details by masquerading. Phishing is typically carried out by email spoofing it directs user to enter details in fake website. The risk grows even larger in social media such as Facebook, Twitter. Hackers use these websites to attack persons using it in workplace, home or in public.

Validation of Data
All data used in website must be validated for type, length and syntax. All data written as output needs to be safe to view in a browser, email client.

The most secure way to do this is to terminate on suspicious input and also whitelist strategy is used.

Secure output handling is primarily associated with preventing cross-site scripting vulnerabilities.

Malicious File Execution
Malicious file execution vulnerabilities are found in many applications. Uploaded files may also contain a malicious payload so should not be stored in web accessible locations.

It allows attackers to perform Remote root kit installation, Root kit execution, Hostile data being uploaded to session files, log data.

Protection

The problems are reduced by some protection. Some are:

Packet Filter Firewall
It is one of the basic firewalls. First step in protecting internal users from external network threats is to implement this type of security. The routers used in packet filter are difficult to configure. It allows only those packets to pass which are allowed as per the firewall policy.

Typically implemented on DSL or Ethernet routers, packet filter firewalls are vulnerable to a number of hacker attacks, not to mention difficult to set up and maintain.

Proxy Servers
It acts as an intermediary for requests from clients seeking resource from other servers. Proxy servers are used for Monitoring and filtering, Logging, Content-control software, Bypassing filters and censorship.Proxy servers can be difficult to set up and maintain for non-technical users.

Stateful Packet Inspection
Stateful packet inspection is a sophisticated firewall technology found in large enterprise firewalls. It's based on advance packet-handling technology that is transparent to users on the LAN, requires no client configuration, and secures the widest array of IP protocols.

It is also well suited to protect networks against the growing threat of Denial of Service attacks.

Virus Protection
Computer viruses and other malicious programs, which attach themselves to applications and files in memory or on disks, are a leading security threat to internet-connected networks.

Users with infected machines may not discover viruses immediately, they can quickly and unwittingly spread damaging viruses throughout a network.

Text Screening
It stops internet pages from loading when the filter words on a predefined list are encountered in either the URL or body of a page. Text screening is most effective when used in conjunction with other filtering measures and must be used with caution.

URL Blocking
Blocks content via content filter lists provided by a trusted third-party content filtering organization that continuously searches the internet looking for offensive sites. It can be done by using some code in windows explorer.

Gateway Security
A gateway security product allows to centralize the management of LANsecurity at one point of interface instead of on each client computer on network.

Security at the gateway means security is positioned at the internet entry point to the network. It will monitor all the inbound and the outbound traffic.

It provides high performance, Real-Time Protection, Reliability etc.

Up-to Date Protection
The security products that can easily adapt to the changing threats by providing the ability to update the

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

software that provides protection against the latest hacker attacks. Software updates over the life of the product should be factored into the total cost of the solution. The updates should be easy to perform, if not automatic, so that the security product can keep pace with the latest threats.

Conclusion

Buying a Swiss Army knife won't make you a locksmith or buying a whip won't make you a lion tamer, the purpose of this paper is to raise awareness about the infringements and thereby to create robustness. Therefore, it is convenient to think of the better infrastructure with various layers like way we would protect against rust by applying a variety of paints,chemicals and anti-oxidants in layers, a systems administrator puts in place several specialized security solutions each addressing specific problem areas.

References

1. John M.D. Hunter, 2001, "An information security handbook"
2. Bishop, Venkatramanayya "Introduction to computer security" Pearson Education Publication.
3. Troy McMillan, "Computer Network Security"
4. Lee Barken, "Wireless Hacking".
5. J.E Ettinger, "Information Security".
6. Shari Lawrence Pfleeger, Charles P. Pfleeger, "Security in Computing".
7. Josef Pieprzyk, Thomas Hariono, Jennifer Seberry, "Fundamentals of Computer Security"