WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Computer Network Security

Assistant prof. Ms. Kalpna N. Rode, Ms. Anuja Ravindra Patil, Ms. Shweta Vidyasagar Tare, Ms. Saniya Sharad Kandane

Electronics & Telecommunications Engineering Department
Sharad Institute Of Technology College Of Engineering, Yadrav, Ichalkarnji, India

ABSTRACT :

The security of computer networks plays a strategic role in modern computer systems. Security became a big concern with the looks of the net and understanding the history of security allows a far better understanding of emergence of security technology. The protection threats increasing day by day and making high speed wired/wireless network and internet services .In this paper we try to test most different varieties of security mechanism that will be applied in step with the necessity and architecture of network. Network security is becoming increasingly important to private computer users, businesses, and therefore the military. Security became a significant concern with the appearance of the web, and understanding the history of security allows a much better understanding of the emergence of security technology. Many security threats can occur thanks to the structure of the web. If the internet's architecture is modified, it can reduce the amount of possible attacks which will be sent across the network. Knowing the attack methods enables us to reply with adequate security. Many businesses use firewalls and encryption mechanisms to guard themselves from the web. To remain connected to the net, businesses create an "intranet."

Introduction :-

Network security is that the process of taking preventative measures to shield the underlying networking infrastructure from unauthorized access , misuse, malfunction, modification, destruction or improper disclosure. Because of internet and new networking technology , the planet is becoming more inter-connected . The foremost basic example of network security is password protection where user of network oneself chooses. Every company or organization that handles great amount of information features a degree of solution against many cyber threats. The internet is classed as an information network. Because this data network is created of computer-based routers, special programs, like "Trojan horses," planted within the routers, can obtain information. Because the synchronous network, which is formed from switches, doesn't buffer data, it's not prone to attackers. That's why data networks, like the web, and other networks that connect with the web, place a premium on security.

Security Attacks :-

Passive attacks :-

The first type of attack is passive attack. A passive attack, can monitor, observe, or build use of systems data obviously functions. However, it doesn't how any impact on system resources and also the data can stay unchanged. The victim is difficult to note passive attacks as this kind of attack is conducted on the QT. Passive attack aims to achieve data or scare opens ports and vulnerabilities of the network. In passive attacks, the attacker observes the messages, then copy and save them and may use it for malicious purposes. The attacker doesn't try and change the knowledge or content he/she gathered. Although passive attacks don't harm the system, they will be a danger for the confidentiality of the message.

Active attacks :-

An active attack would be a network exploit during which the attackers will modify or alter the content or an effect the system resource. It'll cause damage to the victims. The attackers can perform passive attacks to collect info before they start playacting vigorous attack. The attackers try to disrupt and compelled the lock of the system. The victims can get informed concerning the active attack. This type of attack can threaten their integrity and accessibility. An energetic attack is tougher to perform compared to a passive attack.

Active attack is a type of cyber attack in which a hacker attempts to change or transform the content of messages or information.

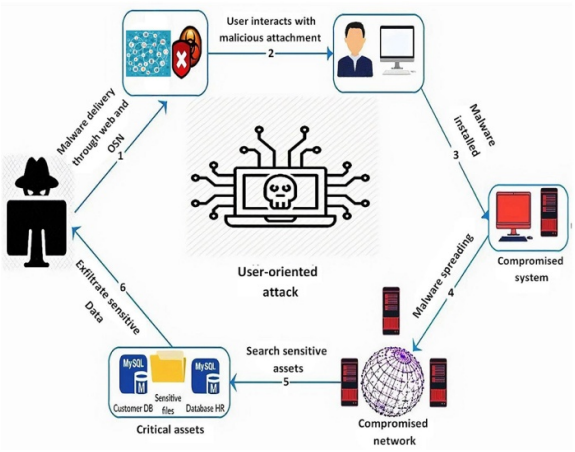
While active attacks are easily detectable and most victims are informed that their network has been compromised, it is exceedingly difficult to prevent them.

You can prevent attacks by having powerful firewalls and intrusion prevention systems (IPS) in place, but you also need to make sure you have a strategy to detect such attacks and recover from active attacks.

Active attacks can prove to be extremely costly; not only can an attacker disrupt your network's processing, they can also jeopardize your sensitive information. If your computer or network's security is vulnerable in the slightest, you can become an easy target for active attacks

Spyware attack:-

A serious computer security threat, spyware is any program that monitors your online activities or installs programs without your consent for profit or to capture personal information. And this capture information is maliciously used because the legitimate user for that individual quite work. Spyware may be a variety of malicious software that's installed on your computer or mobile device without your consent. It can gain access to your sensitive personal information then relay it to other parties, some malicious. Although the term "spyware" may sound like something right out of a detective movie, this sneaky software is anything but entertaining. Spyware is really one in every of the foremost common threats on the net today. It can easily infiltrate your device and, thanks to its covert nature, it are often hard to detect. To this end, consider this your ultimate guide to simply what's spyware, what does spyware do, and the way to get rid of spyware, do you have to become a victim.



Phishing Attack:-

In phishing attack the hacker creates a fake science system that appears exactly reasonably a popular site rather like the SBI bank or PayPal. The phishing a component of the attack is that the hacker than sends an e-mail message trying to trick the user into clicking a link that finishes up within the fake site. When the user attempts to travel surfing with their account information, the hacker records the username and password so tries that information on the 000 site. Phishing is additionally a variety of social engineering attack often accustomed steal user data, including login credentials and master card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which could end within the installation of malware, the freezing of the system as a component of a ransomware attack or the revealing of sensitive information

5) **Hijack Attack :-** In a hijack attack, a hacker takes over a session between you and another individual and disconnects the opposite individual from the communication. You continue to believe that you just are reprimand the first party and should send private information to the hacker by accidently. An attack during which the attacker is in a position to insert himself or herself between a claimant and a verifier following a successful authentication exchange between the latter two parties. The attacker is ready to pose as a subscriber to the verifier or the other way around to regulate session data exchange. Sessions between the claimant and also the RP are often similarly compromised.

6) **Password Attack :-** An attacker tries to crack the passwords stored in a very network account database or a password-protected file. There are three major kinds of password attacks: a dictionary attack, a brute-force attack, and a hybrid attack. A dictionary attack uses a glossary file, which could be a list of potential passwords [9]. A brute-force attack is when the attacker tries every possible combination of characters. A password attack refers to any of the assorted methods want to maliciously authenticate into password-protected accounts. These attacks are typically facilitated through the utilization of software that expedites cracking or guessing passwords. The foremost common attack methods include brute forcing, dictionary attacks, password spraying, and credential stuffing.

Types of network security protection

1) **Firewall :-** Firewalls place a barrier between your trusted internal network and untrusted outside networks, like the Internet. A set of defined rules are employed to block or allow traffic. A firewall can be software, hardware, or both. The free firewall efficiently manages traffic on your PC, monitors in/out connections, and sources all connections when you are online.

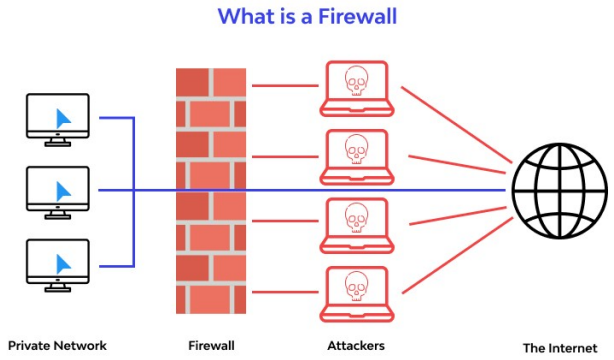
A firewall is network security system that manages and regulates the network traffic based on some protocols. A firewall establishes a barrier between a trusted internal network and the internet.

Firewalls exist both as software that run on a hardware and as hardware appliances. Firewalls that are hardware-based also provide other functions like acting as a DHCP server for that network.

Most personal computer use software-based to secure data from threats from the internet. Many router that pass data between networks contain firewall components and conversely, many firewalls can perform basic routing functions.

Firewalls are commonly used in private networks or intranets to pervert unauthorized access from the internet. Every message entering or leaving the intranet goes through the firewall to be examined for security measures.

An ideal firewall configuration consist of both hardware and software based device. A firewall also help in providing remote access to a private network through secure authentication certificates and logins.

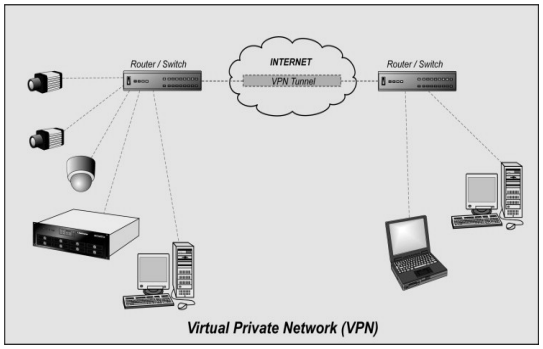


2) **Application security**

It is essential to possess application security since no app is formed perfectly. Any application can comprise vulnerabilities or holes that attackers use to enter your network. Application security thus encompasses the software, hardware and processes you choose on for closing those holes. Application security is that the discipline of processes, tools and practices on the point of protect applications from threats throughout the entire application lifecycle. Cyber criminals are organized, specialized, and motivated to go looking out and exploit vulnerabilities in enterprise applications to steal data, belongings, and sensitive information.

3) Virtual private network.

VPN is another kind of network security capable of encrypting the connection from an end point to a network, mainly over the online. A far off VPN access typically uses IP set for secure Sockets layer to authenticate the communication between web and device. A virtual private network (VPN) allows your company to securely extend its private intranet over the prevailing framework of a public network, just like the net. With VPN, your company can control network traffic while providing important security measures like authentication and data privacy.



4) Anti-Malware Software and Scanners :- Viruses, worms and Trojan horses are all samples of malicious software, or Malware for brief. Special so called anti-Malware tools are wont to detect them and cure an infected system. Malware, short for malicious software, is software used or created by hackers to disrupt machine operation, gather sensitive information, or gain access to non-public computer systems. While it's often software, it can even appear within the kind of scripts or code. 'Malware' could be a general term want to sit down with a spread of kinds of hostile, intrusive, or annoying

software

5) Email Security:-

Email gateways are the amount one threat vector for a security breach. Attackers use personal information and social engineering tactics to form sophisticated phishing campaigns to deceive recipients and send them to sites serving up malware. An email security application blocks incoming attacks and controls outbound messages to prevent the loss of sensitive data. Email security is also a term for describing different procedures and techniques for safeguarding email accounts, content, and communication against unauthorized access, loss or compromise. Email is usually accustomed spread malware, spam and phishing attacks. Attackers use deceptive messages to entice recipients to dispense with sensitive information, open attachments or click on hyperlinks that install malware on the victim's device. Email is additionally a typical entry point for attackers looking to attain a foothold in an enterprise network and procure valuable company data. Email encryption involves encrypting, or disguising, the content of email messages to protect potentially sensitive information from being read by anyone aside from intended recipients. Email encryption often includes authentication.

Conclusion :-

Network security is an essential area that is gaining traction as the internet grows in size. To evaluate the necessary changes in security technology, the security threats and internet protocol were analyzed. The majority of security technology is software-based, but several common hardware devices are included. The current state of network security is unimpressive. With the importance of the network security area, it was believed that new approaches to security, both hardware and software, would be actively investigated. It was surprising to realize that the majority of the progress was taking place in the same technologies that are already in use. In the near future, the combination of IPv6 and security measures such as firewalls, intrusion detection, and authentication procedures will be successful in protecting intellectual property. To deal with future dangers, the network security area may need to evolve more quickly.

References:

1. Kartalopoulos, S. V., "Differentiating Data Security and Network ssSecurity,"Communications,2008.ICC'08.IEEEInternatio nalConferenceon,pp.1469-1473,19-23May2008
2. Network Security Types of attacks [Online] available: http://computernetworkingnotes.com/network-security-access-listsstandards-and-extended/types-of-attack.html.
3. Network Security [Online] available: http://en.wikipedia.org/wiki/Network_security.
4. ―Network Security: History, Importance, and Future‖, University of Florida Department of Electrical and Computer Engineering, Bhavya Daya
5. Dr. G. Padmavathi, Mrs. D. Shanmugapriya, ―A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks‖, (IJCSIS) International Journal of Computer Science and Information Security,Vol. 4, No. 1 & 2,2009.
6. Network Security Types of attacks [Online] available: http://computernetworkingnotes.com/network-security-access-listsstandards-and-extended/types-of-attack.html.
7. Securing the Intelligent Network [Online] available: http://www.trendmicro.co.in/cloud-content/us/pdfs/securityintelligence/white-papers/wp_idc_network-overwatch-layer_threat-mngmt.pdf
8. Network Security Types of attacks [Online] available: http://computernetworkingnotes.com/network-security-access-listsstandards-and-extended/types-of-attack.html