IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Network security includes all kind of security OS antivirus IDS and others

Abinash Kumar Singh

Abstract

Network security has become a lot necessary to private laptop users, organizations, and also the military. Computer network security plays a key role in modern computer systems. A number of software tools have been developed to ensure high levels of protection from malicious attacks. Computer technology is improving rapidly, and network technology, as well as web technology, is progressing at a rapid rate along with this. An appropriate pattern matching intrusion detection system for network security has been proposed in this paper due to its capability to detect and prevent attacks from malicious network users. A recent research topic has been the potential of intrusion detection systems to detect and prevent attacks from malicious network users. This paper rapidly presents the possibility of Computer security. Antivirus solutions are presently a typical part of the computer framework. The paper in this manner hopes to raise measurements of comprehension about the security of the security items. The different security tools that are accessible are Firewall, Intrusion Detection System, and Honeypot. Each tool has its own components, benefits, and hindrances. The analysis of this paper will disclose to you that how an enemy of infection perceives the infections and sanitize the records. The rule manner of thinking of this paper is to tell how it works and secure your system unmistakable sorts of malware, contaminations, and worms.

Keywords: **Security, Network Security, Viruses, Threats, IDs, Firewall**

Introduction

Network and laptop security area unit essential to the monetary health of each organization. Over the past few years, Internet-enabled business, or e-business, has drastically improved potency and revenue growth. E-business applications like e-commerce, supply-chain management, and remote access permit corporations to contour processes, lower operative prices, and increase client satisfaction. Such applications need mission-critical networks that accommodate voice, video, and knowledge traffic, and therefore these networks should be ascendable to support increasing numbers of users and the want for larger capability and performance. However, as networks change additional and additional applications and area unit obtainable to additional and additional users, they become ever additional susceptible to a wider vary of security threats. To combat those threats and make sure that e-business transactions don't seem to be compromised, security technology should play a serious role in today's networks. With the process of time, Computer innovation has been

extraordinarily created and the present system correspondence framework has spread to each edge of the world, including political, monetary, military and all strolls of public activity. It assumes a critical job. Regardless, other than fun and solace, PC moreover passes on to us a lot of safety chances on account of its straightforwardness and Network. Customers are right now taking a gander at incalculable risks. Is PC coordinating safe Criminal cases are a large part of the time visitors of private and worldwide consideration. Reports on orderly security weaknesses are rarely remarkable. Shows the expound on security weaknesses of information system by the U.S. security affiliation CERT/CC [1]. Framework Security on the Internet and on Local Area Networks is currently at the bleeding edge of PC network-related issues. Without acceptable affirmation or framework security, various individuals, associations, and governments are at risk for losing that benefit. Framework security is the cycle by which mechanized information assets are guaranteed, the targets of safety are to get grouping, care for uprightness, and assurance availability. Taking into account this, it is fundamental that all frameworks be protected from risks and weaknesses all together for a business to achieve its fullest potential [2]. Usually, these risks are persevering because of weaknesses, which can rise out of mis-masterminded gear or programming, helpless framework plan, inborn advancement deficiencies, or end-customer indiscretion. An interconnected PC or contraptions that share the product and equipment resources for numerous customers. All of these networks are being given a unique convey suggested as Internet Protocol (IP)Address which is numerically portrayed and Structured as A: B: C: D where A, B, C, D are described in the reach from 0-255. A, B, C addresses the organization address and D describes the area of the PC or the device on the customer end. Frameworks are available at any place in your life. While the sharing of resources and information in an interconnected correspondence arrangement is fundamental, power gets to constraints. As a result, structures can be weak against maltreatment by various customers through access encroachment attempts. In mid-eighties, the rule fundamental pressure for PC customers was that antivirus or malignant code were happening into their systems. Along these lines, we expected to take basic steps towards this. In this way, there are on a very basic level.

Two fundamental alternatives exist:

1. Your system in a very protecting bubble that means isolate's structure; become independent from the net or another transmission media neither utilize CD-ROMs nor another removable circle. on these lines, by doing this we have got a perfect knowledge preparing machine however there's no knowledge to live. just in case there's no info that may enter in your structure thus you would possibly have an associate degree optimum system there aren't any contaminations.

2. Install antivirus programming so there's harmony within the client's mind that no infection can enter their framework. The essential concern is that however, the program makes an attempt to stay from diseases getting into your laptop. Antivirus programming laptop programs square measure a lot of tasks that square measure accustomed analyze your info and afterward if capture any spoiled record, it cleans it. There square measure varied ways in which to contend with separate or channel any info dependent upon wherever it begins from. For e.g., it works contrastingly whereas genuinely taking a glance at the CD-ROMs and whereas separating the messages and seeing over the LANs. Norms for all antiviruses square measure one thing similar anyway there's refined differentiation [27].

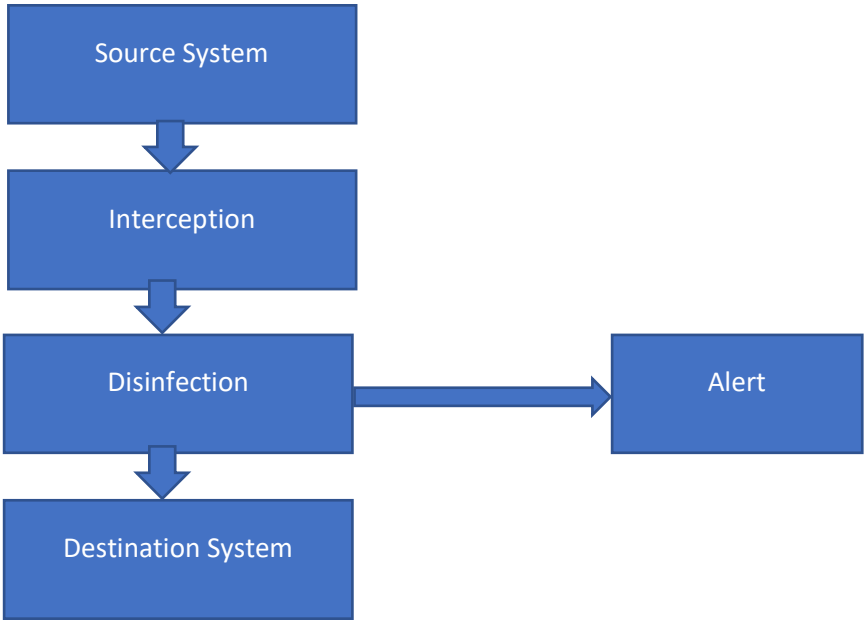


Fig1. There are subtle differences between antiviruses.

The information starts from the supply structure and may reach the target system. supply system may well be in any capability sort of a floppy circle, hard plate, etc. and objective structure may well be a tough plate of a computer or any ISP (Internet Service Provider) that stores the messages sends them once a shopper needed. the knowledge interpretation system shifts looking on exceptional elements or notwithstanding whether or not it's accomplished in operating structure. This elucidation system is express for each OS or relying upon the section during which the antivirus program is actual. For e.g., in windows eight a virtual driver is employed that screens the activity of circles. Consequently, each time the knowledge is gotten to through floppy circle or arduous plate then the antivirus program can catch the examine and build a decision to the plate and a brief time later examine the knowledge with the target that anybody will examine it safely. All of those exercises worked through the half in windows XP/2000. All antivirus programmings have a selected understanding framework [26]. it is not created for the OS however moreover numerous applications too. a little of the time clarification frameworks is not obtainable by the antivirus program or by any application. Thusly, it uses numerous resources. Resources that subtly take data and pass it to the antivirus and then it's at the knowledge and sanitizes the record. For the purpose once {the data the knowledge the data} has been checked mistreatment any procedure then 2 assignments area unit performed: the best information is shipped off the interpretation stage with the target that it will continue towards the target structure.

Prepared message is shipped to the UI. UI will vary for e.g., in antivirus for workstations, the message is displayed on the screen expressly and antivirus for staff, the alert message may well be shipped off the letter drop. It does not play out any extraordinary event. it's Associate in Nursing unusually direct and helpful security confederate that provides pattern-setting advancement. notwithstanding after you copy some of the bytes in your structure then antivirus ought to check for seventy,000 infections while not meddlesome with the traditional development of the computer, and also the client cannot comprehend these activities. It provides uncommon state security.

Community safety refers to the numerous countermeasures installed area to defend the network and information saved on or passing through it. network protection works to keep the community safe from cyberattacks, hacking tries, and worker negligence. There are 3 components of community safety: hardware, software, and cloud offerings. The networks security policy should stipulate that every computer system in the community is stored up to date and, ideally, are all blanketed by way of the equal anti-virus package—if only to preserve upkeep and replace charges to a minimum. it is also important to update the software itself on an everyday basis. Virus authors regularly make getting past the anti-virus packages their first precedence.

- hardware appliances are servers or devices that perform sure protection capabilities inside the networking environment. hardware can be installed out of the direction of community visitors, or "out-of-line," but it's greater typically hooked up inside the direction of traffic, or "in-line."
- community security software, which incorporates antivirus programs, may be installed on gadgets and nodes throughout the network to offer brought detection and risk remediation.
- Cloud offerings seek advice from offloading the infrastructure to a cloud issuer. The set-up is usually much like how network visitors pass-thru in-line hardware home equipment, but incoming community visitors are redirected to the cloud provider instead.

There are different types of security

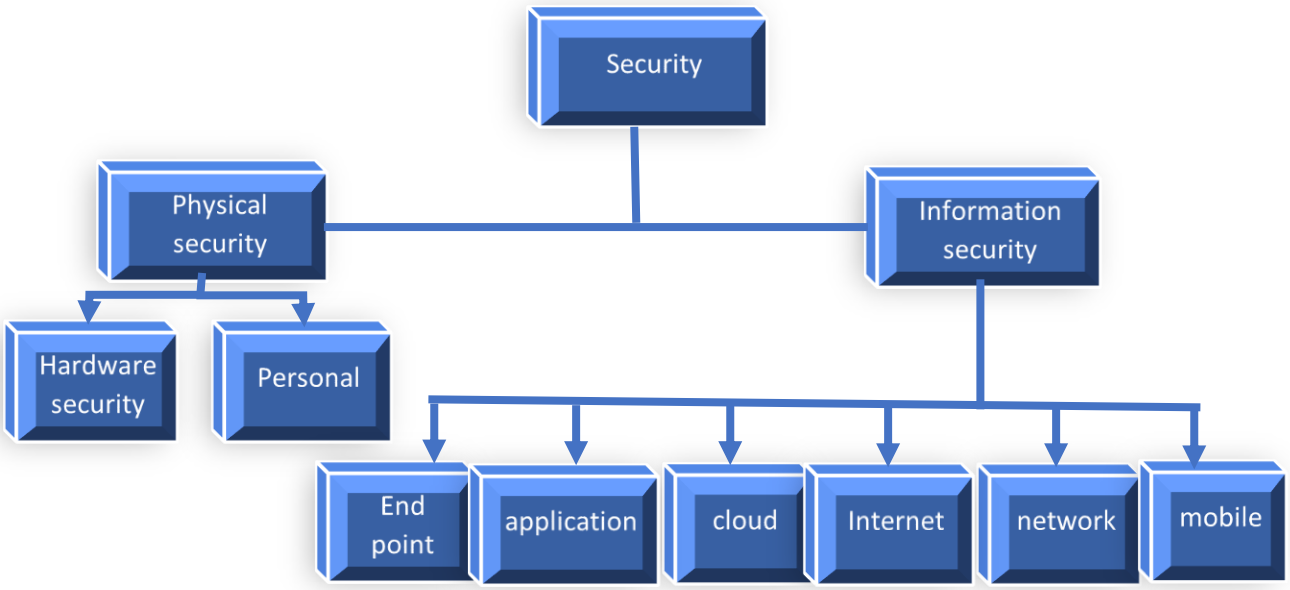


Fig2: Types of security

Physical security:

Physical security involves the protection of data, equipment, human resources, software, and frameworks from physical tasks that can hurt an organization. This includes psychological abuse, fire, calamity, theft, etc.

Information security:

Information security minimizes the risks to information to achieve protection, integrity, and availability. It integrates Application Security, Cloud Security, End Point Security, Internet Security, Mobile Security, and Network Security.

Application security: Each device and software product in your networking environment opens up the possibility of hackers breaking in. It is crucial to keep all programs up-to-date and patched to guard against cyberattacks exploiting security vulnerabilities to gain access to sensitive data. Application security is the combination of hardware, software, and best practices that you use to identify security issues and close security gaps[29].

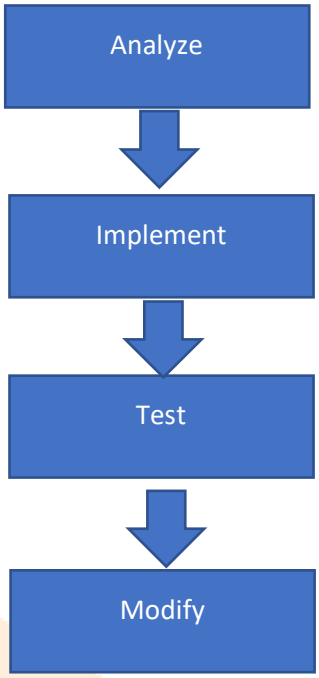
Mobile device security. The overwhelming majority of folks have mobile devices that carry some variety of personal or sensitive knowledge we might wish to keep protected. this is often an incontrovertible fact that hackers' area unit conscious of and might simply cash in on. Implementing mobile device security measures will limit device access to a network, which could be a necessary step to making sure network traffic stays personal and doesn't get out through vulnerable mobile connections.

NETWORK SECURITY:

System security implies the insurance of system and data together with instrumentation and programming advances from the risks. Most essential risks consolidate worms, spyware, Trojan horses, contaminations, party time attack, Denial of Service attack, data catch, and discount extortion. Framework Security goes when numerous layers of Security. Dares to shield Network from attacks:

Analysis: The definite wants of the organization and therefore the dangers that might infer on it are gathered and are being bust right down to decide this framework.

1. **Implementation:** The point-by-point necessities of the framework and therefore the perils that might suggest on it are assembled to boot are being pinched right down to opt for this system.
2. **Testing:** specifically, once the safety structure is complete it's wont to perform tests on numerous types of perils victimization associate vast no of trials to ensure that almost all of the options are operating exactly and are totally obtaining the framework against any risks.
3. **Modify**: within the wake of Testing is contend out the outcomes can uncover the inadequacies of your framework and wherever it all right is also modified to expand the productivity of the safety framework.



Techniques for Network Security:

Network Scanning: These are speedy and may gainfully examine the hosts, dependent upon the number of hosts offered within the framework. they are very automatic and are offered with numerous software gadgets that expect the experience to unravel the results. In like manner, these frameworks don't seem to be too excessive.

Vulnerability scanning: this type of framework is employed to understand the famous weaknesses as an example of the surface helplessness and will offer counsel on riddance those discovered weaknesses. Similarly, these are everything except onerous to run and open at unbelievable prices.

Penetration Testing: Entrance Testing affirms the weaknesses that are past the surface defect level what is a lot of, are on and on mishandled to increment a lot of noticeable adequacies, wherever the weaknesses don't seem to be theoretical. it's an uncommonly long interaction since all of the hosts open on intensive or medium assessed frameworks are tried severally. this might be unsafe whenever overseen by new analyzers.

Password Cracking: This framework is employed to quickly notice the mysterious expression of the client or the framework, and may clearly exhibit the character of the mysterious expression to be broken. Regardless, some affiliations do not reinforce this sort of technique because of likewise, have restricted the center person's objections to swearing off hacking.

Log Reviews: this sort of system goes most likely because the wellspring of {information} which supplies the howling information subject to these records, that makes the task redundant to truly summary and automatic instruments do not prove faultlessly for these in light-weight of the actual fact that they'll channel the crucial information.

Currently offered network security solutions

The number of individuals interfacing with the web is growing apace. The comfort and therefore the organization the online offers are considerably necessary nonetheless the risks enclosed and malicious interferences are what are more extending bit by bit. Abuse of laptop frameworks is obtaining dynamically typical. it's fully elementary for business affiliation too as people to safeguard their information from veritable perils that may conceive to take their data. There are numerous security game plans open on the lookout. a number of them take once Firewall, Intrusion Detection System (IDS), Honeypot that are explained beneath.

A. Firewall

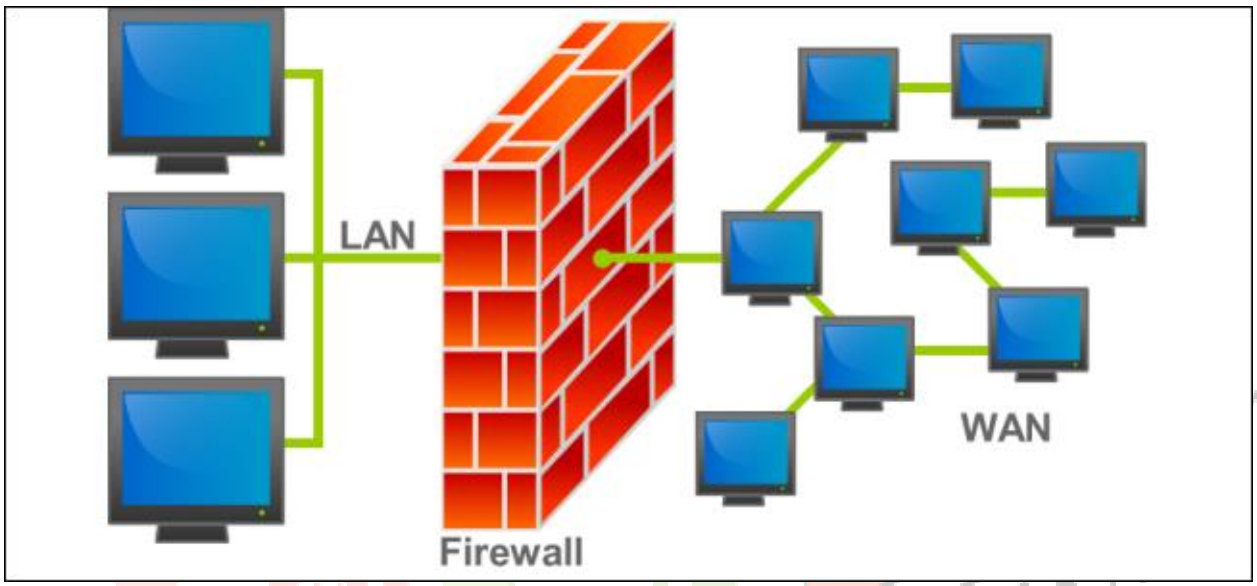


Fig4: Firewall, www.erpublications.com [10]

A firewall could be a mixture of hardware and programming that isolates an association's internal framework from totally different frameworks, empowering a few packs to pass and obstructing others. Its skills to avoid unapproved or unlawful conferences enraptured toward the devices within the framework regions it guarantees. Firewalls are organized to ensure against unauthenticated smart logins from the remainder of the planet. The firewall is thought about as a couple of sections: one that exists to face traffic, and therefore the alternative that exists to permit traffic. Generally, amounts of firewalls are passed on within the most ideal spots of the supervised framework for pleasing, composed, and begin to complete framework security confirmation. Executives that organize with the firewalls have ought to be cautious whereas setting the firewall rules [4].

Types of Firewalls

• Packet-Filtering Router

A packet-Filtering that applies tons of rules to every drawing nearer and dynamic informatics cluster and a moment later advance or discards the bundle. The switch is meant to channel bundles heading in 2 ways in which. Separating rules rely on the information contained in a corporation bundle, which contains the supply informatics address, objective informatics address, source, and objective vehicle level location, informatics convention field, and interface The parcel channel is habitually started as an outline of rules dependent upon matches to fields within the informatics or TCP header. just in case there's a match to 1 of the basics, that customary is invoked to decide on if to advance or discard the pack. just in case there's no match to any norm, a default move is created. The default action will either be to discard or advance the cluster.

• Application-level gateways

An application-level portal goes regarding as a transfer of use level traffic. it's otherwise referred to as negotiator server. The client contacts the access employing a TCP/IP application, as an example, Telnet or FTP, and therefore the section moves toward the client for the name of the distant host to be gotten to. At the purpose, once the consumer reacts and provides a considerable consumer ID and confirmation information, the door contacts the appliance on the remote host and transfers TCP parts containing the appliance data between the 2 endpoints. On the off probability that the door doesn't execute the negotiator code for an exact application, the administration isn't upheld and cannot be sent over the firewall. Application-level gateways can overall be safer than package channels. it's something however tough to log and review all approaching traffic at the appliance level. the basic hindrance of this sort of access is that the further handling overhead on every association.

• Circuit level gateways

The Circuit level passage is AN freelance framework or it o.k. could also be a selected capability performed by AN application-level door for specific applications. A circuit-level door doesn't permit a conclusion-to-end TCP association, the access sets up 2 TCP associations. One affiliation is about up among itself and a TCP client on an interior host and one in every of itself and a TCP client on an external host. At the purpose, once the 2 affiliations are developed, the access systematically moves TCP segments from one relationship with the opposite while not investigation the substance. the safety work includes working out that associations are going to be permissible [5].

Advantages of Firewalls: Following are the advantages of Firewalls:

I. Firewalls will keep the traffic that is non-authentic.

ii. Firewalls will channel those shows and organizations that may be simply abused.

iii. A firewall helps to urge the interior framework by activity names or within structures from the external hosts.

Firewalls have the following disadvantages:

I. Firewalls use a bunch of rules that are literally supposed to isolate legitimate traffic from non-certifiable traffic.

ii. The firewall cannot react to a framework attack nor will begin effective counter-measures.

iii. Most firewalls do not analyze the substance of the information distributes makeup framework traffic.

iv. Firewalls cannot keep assaults originating from the computer networks.

v. Filtering principles of the firewall cannot keep attacks ranging from the appliance layer [16].

iv. Firewalls will decide broadened work of system traffic on one framework.

B. Intrusion Detection System (IDS)

Interruption Detection System (IDS) causes information frameworks to manage assaults. this can be practiced by gathering information from AN assortment of frameworks and system sources. the information gathered is poor down for conceivable security problems. An intrusion detection system (IDS) could be a device or software system application that monitors a network for malicious activity or policy violations. Any malicious activity or violation is usually reported or collected centrally employing security info and an event management system. Some IDS are capable of responding to detected intrusion upon discovery. These are classified as intrusion bar systems (IPS). An IDS accumulates and breaks down information from totally different zones within a computer or a system to acknowledge conceivable security breaks. The interferences may fuse attacks each from outside the affiliation and likewise within the affiliation. [16].

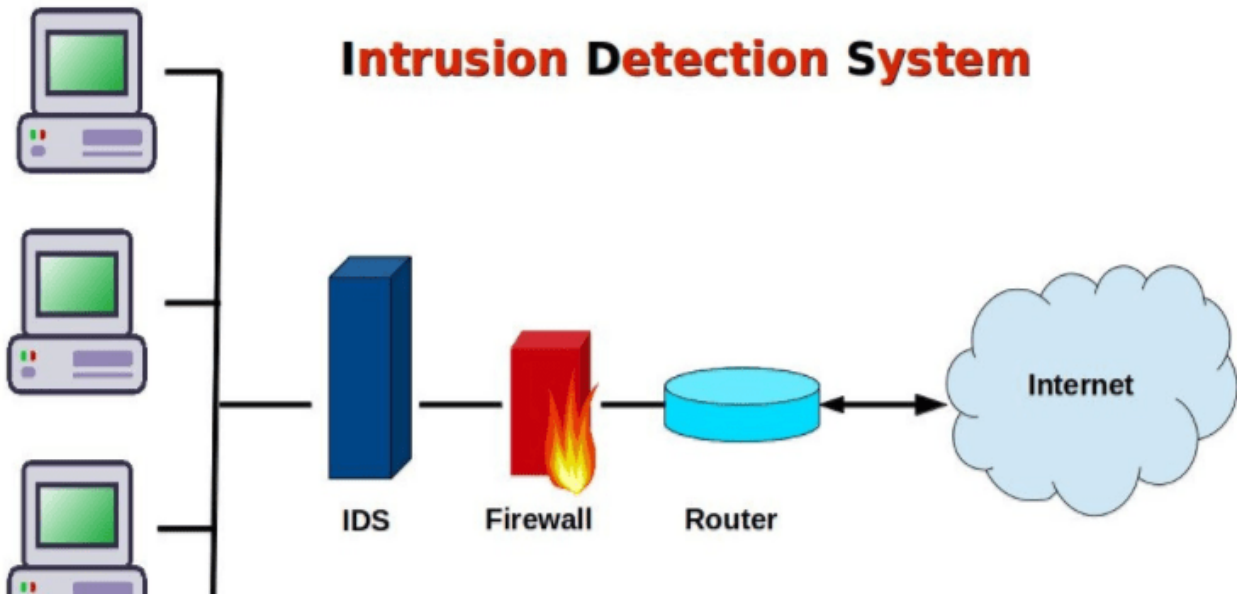


Fig5: Intrusion detection System www.erpublications.com **[26]**

Advantage of IDS:

I) IDS square measure less exacting to send because it does not influence existing frameworks or foundation.

ii) Network-based IDS sensors will determine varied assaults by checking the parcel headers for any vindictive assault like TCP SYN assault, divided parcel assault, then forth.

iii) IDS screens traffic on a continual. during this manner, organize based mostly IDS will acknowledge pernicious actions as they happen.

iv) IDS device sent external the firewall will understand malevolent attacks on resources behind the firewall [17].

Disservices of IDS:

I) IDS is not Associate in Nursing choice in distinction to solid shopper ID and confirmation instrument.

ii) IDS is not a solution for all security issues.

iii) Human mediation is needed to look at the assault once it's known and elaborate.

iv) False up-sides happen once IDS mistakenly understands the quality activity as being vindictive.

v) False negatives happen once IDS fails to understand the damaging activity [17].

Honeypot

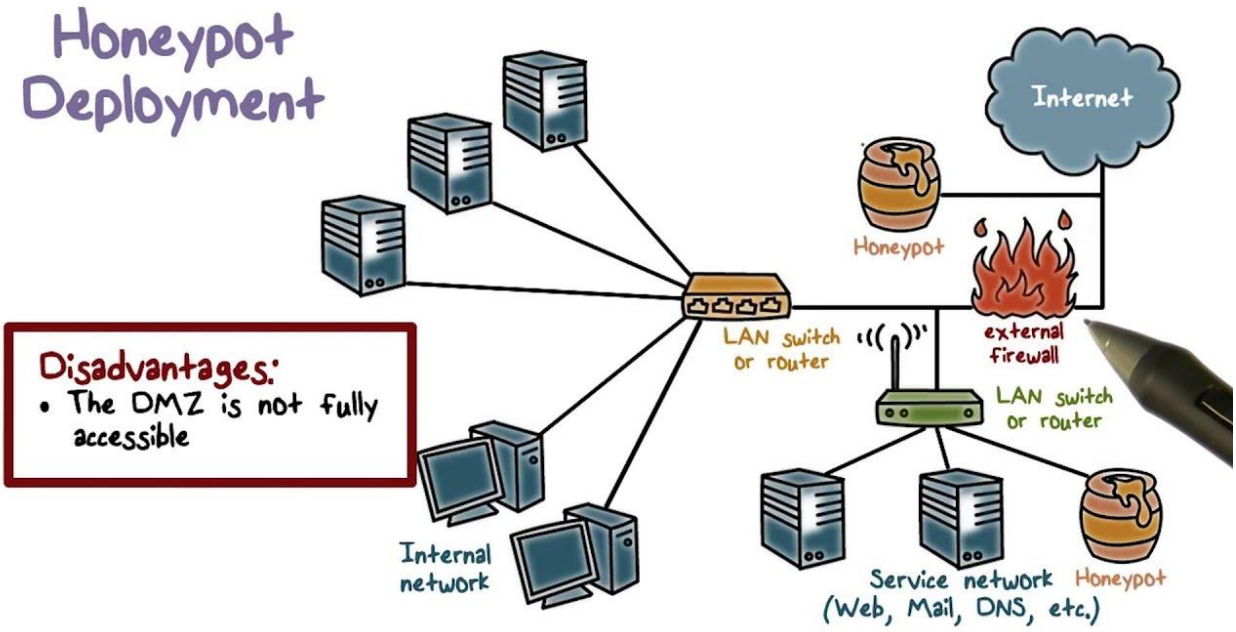


Fig 6: Diagram of a production honeypot deployed in a DMZ to detect attacks [27]

A honeypot could be a catch set to understand, prevent from, or somehow or another equilibrium tries at unapproved usage of knowledge structures. By and huge it contains a computer, info, or a system website that has all the earmarks of being a chunk of a system, nevertheless is de facto disconnected what is a lot of, noticed, and that looks to

contain info or a resource of essential value to aggressors. A honeypot works by casual attackers into a basic cognitive process that it's a veritable system. The attackers attack the system while not understanding that they're being watched. At the purpose, once associate aggressor endeavors to trade off a honeypot, its assault connected knowledge, as an example, the information science address of the aggressor, are going to be gathered. This movement done by the aggressor provides vital knowledge and examination on assaulting procedures, enabling framework executives to follow back to the wellspring of assault whenever needed [10]. By and huge honeypots is divided into 2 categories.

Production Honeypots: Creation honeypots square measure want to facilitate a relationship in guaranteeing its inward IT institution. These safe the connection by policing its IT condition to understand attacks. These honeypots square measure valuable in obtaining programmers with criminal aims. The execution and game arrange of those honeypots square measure moderately less requesting than analysis honeypots in light-weight of the very fact that these have less clarification and needless limit. on these lines, they equally provide less verification regarding programmer's attack models and aims. analysis Honeypots: analysis honeypots square measure remarkable. they're supposed to collect but abundant knowledge as may well be expected regarding the programmers and their exercises. Their elementary mission is to research the peril's affiliations may defy, for example, World Health Organization the aggressor's square measure, the means they're shaped, what quite instruments they use to attack varied systems, and wherever they obtained those contraptions. whereas generation honeypots fit the police, investigate honeypots go regarding set about approach act move as their insight partner and their central goal is to collect knowledge about the aggressor. the data gathered by analysis honeypots can facilitate the connection with amelioratory fathom the developers attack models, manners of thinking, and the way they work [19].

Advantages of Honeypot:

1. **Small Data Sets:** Honeypots presumably gather info once someone or one thing is connecting with them. Associations that may which can that will log an outsized variety of alarms multi-day with standard advancements will simply log 100 cautions with honeypots. This makes the data honeypots gather a great deal higher esteem, less stern to supervise, and a lot of simples to interrupt down.

2. **Reduced False Positives:** one of the most effective difficulties with most location advancements is that the age of false positives or false cautions. It's just liked the tale of the „boy World Health Organization cried wolf". the larger the chance that a security innovation creates a false positive the lot of unsure the innovation is going to be sent. Honeypots considerably reduce false positives. Any action with honeypots is by definition unapproved, creating it to a good degree productive at recognizing assaults.

3. **Catching False Negatives:** Another take a look at customary advances is neglecting to tell apart obscure assaults. this can be a basic distinction among honeypots and standard computer security innovations that rely upon legendary marks or upon factual identification. Mark-based mostly security developments by definition suggest that "someone can get harmed" before the new attack is found associated an imprint is scattered. Verifiable revelation in like manner suffers from probabilistic dissatisfactions – there's some non-zero chance that another quiet attack can go unseen.

Honeypots after all will while not an awfully exceptional stretch understands and catch new attacks against them. Any activity with the king protea is associated with inconsistency, creating new or disguised attacks with success arise.

4. **Encryption:** It does not create a distinction if associate assault or pernicious action is disorganized, the king protea can catch the movement. As an associate's ever-increasing variety of associations receive encoding within their surroundings, (for example, SSH, IPsec, and SSL) this turns into a motivating issue. king proteas will do that in light-weight of the very fact that the encoded tests associated assaults get together with the Honeypot as a finish purpose, wherever the action is decoded by the king protea.

5. **IPV6:** Honeypots add any IP condition, paying very little mind to the information science convention, together with IPv6. information sciencev6 is that the new IP commonplace that varied associations, as an example, the Department of Defense, and various nations, as an example, Japan, square measure effectively embrace. varied gift advances, for example, firewalls or IDS sensors, cannot manage IPv6.

6. **Highly Flexible:** Honeypots square measure unbelievably convertible, with the power to be utilized in a grouping of conditions, everything from a Social Security variety embedded into associate info base, to a complete arrangement of PCs planned to be broken into.

7. **Minimal Resources**: Honeypots need negligible assets, even on the largest of systems. a simple, maturing Pentium computer will screen really an enormous variety of information science addresses [21].

Disadvantages of Honeypots:

Aside from each one of the favorable circumstances, honeypots to boot have some weaknesses. Burdens of honeypots square measure recorded underneath:

1. **Risk:** Honeypots square measure a security quality the difficulty manufacturers to go with, there's a hazard that associate aggressor might utilize a king protea to assault or mischief different non-honeypot frameworks. This hazard shifts with the kind of king protea used. for example, basic king protea, as an example, the detector has virtually no hazard. Honeynets, the associate with progressively impressive arrangements, have a lot of hazards [22]. The hazard levels square measure variable for varied kinds of king protea organizations. the everyday guideline is that a lot of confused the trickery, a lot of noteworthy the hazard. Honeypots that square measure high-collaboration, as an example, the information I Honeynets square measure inalienably increasingly dangerous on the grounds that there's a true computer enclosed.
2. **Limited Field of View:** Honeypots simply observe or catch what cooperates with them. they're not associated with a distant gizmo that catches action to every single different framework. Rather, they presumably have esteem once squarely communicated with. From multiple points of reading, honeypots fit a magnifying instrument. [25] they need an affected field of reading, but a field of reading that provides them unbelievable detail of information.
3. **Discovery and Fingerprinting:** Despite the very fact that the danger of revelation of a king protea is small for content kiddies and worms, there's reliably an effort that fashionable black hats would have the capability to seek out the king protea [23].

Conclusion

Considering everything, a serious framework security organ is basic for guaranteeing systems. If you have extraordinary framework security, your association or affiliation is guaranteed against obstruction, delegates stay beneficial. System security causes you to meet necessary administrative consistency. Guaranteeing your client's data infers no cases emanating from cases about data. Several approaches can help ensure the safety and protection of your community. Avoid security vulnerabilities by performing the following steps. It is necessary to have an updated antivirus program. Make sure no network user is granted unnecessary or excessive access. Keeping the running gadget up to date is very important. The distinctive sorts of firewall, interruption identification framework, and hostile to infection scanner, where they are sent and their capacities and individual conduct were examined, alongside a few instances of interference and attack to which they are used to get against. In this paper, we examined how antivirus programming functions. This kind of profound statistics can help us with deciding on the best antivirus for your framework so that you can give good protection on your pc.

References

[1] Translated by Cheng Peiqing, et al. *Computer network security. Publishing House of Electronics Industry*, **1994**.9
[2] Li Wenlong. Face to face with a hacker. *internet world*.**1999**(2):2~8

[3] International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 6, Issue. 5, May 2017, pg.235 – 237

[4] Network Security Threats and Protection Models kamit5@iitk.ac.in, mahotsan@iitk.ac.in Department of Computer Science and Engineering Indian Institute of Technology Kanpur Technical Report – CSE-101507

[5] Rebecca Bace and Peter Mell. Intrusion detection systems. NIST Special Publication on Intrusion Detection System.

[6] J Balthrop, F Esponda, S Forrest, and M Glickman. Coverage and generalization in an artificial immune system. Proceedings of GECCO, pages 3–10, 2002.

[7] Internet Security Threats Will Affect U.S. Consumer' Holiday Shopping Online http://www.bsacybersafety.com/news/2005-Holiday-Online-Shopping.cfm

[8] Executable compression https://en.wikipedia.org/wiki/Executable_compression.

[9] Attacking antivirus, Feng Xue, Technical lead, Nevis Labs, Nevis Network, Inc.

[10] **Firewall Diagram from Wikimedia Commons**, **Chris Dag on Flickr**, CHRIS HOFFMAN What Does a Firewall Actually Do?

[11]. K. Scarfone and P. Mell," Guide to Intrusion Detection and Prevention Systems (IDPS)," Gaithersburg, MD, Rep. *NIST Special Publication 800-94, Feb. 2007.*

[12]. D. Rozenblum, "Understanding Intrusion Detection System," www.sans.org/reading_room/whitepapers/detection/understanding-intrusiondetection-systems_337, October 31, 2003.

[13]. S. Nassar, A.E. Sayed, N. Aiad, "Improve the Network Performance By using Parallel Firewalls," in Proc. of 6th International Conference on Networked Computing, May 2010, pp. 1-5.

[14]. S. Ioannidis et al., "Implementing a Distributed Firewall," in Proceedings of the ACM Computer and Communication Security (CCS), pp. 190-199, 2000.

[15]. W. Stallings, Cryptography and Network Security Principles and Practices. 4th ed., Prentice Hall, 2005.

[16]. X. Jhang, C. Li, W. Zheng, "Intrusion Prevention System Design." in Proc. of 4th International Conference on Computer and Information Technology, pp. 386-390, Sept. 2004.

[17]. A. Samrah, "Intrusion Detection Systems; Definition, Need and Challenges," http://www.sans.org/reading_room/whitepapers/detection/intrusion-detectionsystems-definition-challenges_343, October 31, 2003.

[18]. Harek Haugerud, "Intrusion detection and firewall security," Available: http://www.iu.hio.no/teaching/materials/MS004A/html/pictures/ids.png.

[19]. Levin, J. and Labella, R., "The Use of Honeynets to Detect Exploited Systems across Large Enterprise Networks", IEEE Proceedings, pp.92-99, 18 June 2003.

[20]. "Honeypot Security", http://www.infosec.gov.hk/english/technical/files/honeypots.pdf.

[21]. Ryan Talabs," Honeypots 101: What's in it for me?" http://www.philippinehoneynet.org/, Fetched 21/06/2011.

[22]. Tang, X. "The Generation of Attack Signatures Based on Virtual Honeypots", International Conference on Parallel and Distributed Computing, Applications and Technologies, 2010, pp.435-439.

[23]. "Snort", http://www.snort.org/assets/166/snort_manual.pdf.

[24]. John E. Canavan," Fundamentals of Network Security", http://www.artechhouse.com.

[25]. Provo's, N., "A Virtual Honeypot Framework", SSYM"04 Proceedings of the 13th conference on USENIX Security Symposium, *Volume 13, 2004*.

[26] intrusion detection system http://www.cyberinject.com/what-type-of-ids-intrusion-detection-system-should-you-use/.

[27] Honeypot Deployment, https://www.youtube.com/watch?v=FBnTeryebzc

[28] International Journal of Advanced Research in Computer Science and Software Engineering, Volume *3, Issue 4, April 2013, ISSN: 2277 128X*.

[29] "Network Security: An Approach Towards Secure Computing", Rahul Pareek, Volume *2, No. 7, July 2011, ISSN: 2229-37IX*