Computer Security

Your Name (First M. Last)

School or Institution Name (University at Place or Town, State)

 **Computer Security**

**Introduction**

 An intrusion detection system (IDS) is a method and system which critically monitors a computer system for activities that are indicative of actual or attempted access by unauthorized computers or persons. The system operates by detecting the unauthorized access attempting to enter into the network systems after the comparison of the user profile to user behavior that detects events to notify control function regarding the unauthorized entry into the operational mechanism. In the contemporary age, the threat of intrusion in the critical and complex operations of businesses has accelerated. The strategic security dimensions of the intrusion detection systems have undergone drastic changes in recent years to confront the grave challenges faced by the businesses. Before the potential advent of intrusion detection, firewalls assumed the responsibility of catering the cyber threats and risks faced by organizations. However, the threats as cross-site scripting (XXS) and SQL injections used to penetrate the firewall and further gave birth to the emergence of intrusion detection. Large and small businesses can harness the productive aspects of IDS by placing it strategically as the network detection to utilize the hardware sensors at strategic points of the network of an organization. Primarily, it has the potential to detect plausible attempts or changes to rewrite the system files or critical activities produced within the organization. The essential technique used by them is signature based or anomaly to determine the threats. Irrefutably, the intrusion detection system has brought a paradigm shift in the operational management of the businesses and has equipped them with significant force to confront them.

**Discussion**

 Nowadays, a wide range of organizations has advanced to utilize the next generation firewalls since their features have significantly grown. However, several cons also exist as the utilization of threat intelligence and security from different vendors. Since the landscape of threat keeps changing persistently, it is a challenging task to rely on the next generation firewalls. It is critical to highlight that the intrusion prevention systems are also prone to identifying false alarms besides recognizing the malicious activity. Hence, the configuration of IDS systems ought to determine the difference between the normal traffic in comparison to the malicious activity to execute the safe traffic on the network of the organization(“Intrusion detection systems – SecTools Top Network Security Tools,” n.d.).

 There exist several types of IDS that are operated via distinguished techniques and policies. Some of the essential aspects pertinent to the deployment of IDS are listed as follows:

* The IDS is placed a strategic point to assess the outbound and inbound traffic from and to all the devices of the network.
* The host intrusion detection systems (HIDS) operate on all devices or computers with direct access to both the enterprise internal network and the internet. HIDS works efficiently in comparison to NIDS in a manner that it can detect the malicious traffic which NIDS has failed to identify.
* One of the essential techniques is the utilization of signature-based intrusion detection system. It supervises all the packets traversing the networks and further compares them with a database of attributes or signature of the malicious threats similar to antivirus software.
* The anomaly-based intrusions detection supervises the network traffic and compares it with an established baseline with the primary aim to determine the appropriate settings. The protocols, ports, bandwidths and other devices are the elements which must be considered. The administrators of the network are potentially alerted by the anomaly based intrusion about a critical malicious activity.

Moreover, these detection systems were classified into the categories of passive and active. A passive IDS detects the malicious activity and generates log entries or alerts but refrains from taking potential actions. On the other hand, active IDS known as the intrusion prevention and detection system generates log entries but can also be configured to take potential actions. Blocking access to the restricted resources or blocking the IP are the essential objectives that can be pursued while configuring the active IDS. Snort, an open source, is one of the most common IDS which is freely available to be used for detecting emerging perils. Most of the Linux and Unix systems can serve as the potential platform to compile it and is also available for windows. The IDS is capable of offering a wide range of services to monitor the traffic to identify the instance where an intrusion or a breach has been made by unauthorized sources. The implementation phase comprises a network security appliance, software running on customized hardware or a cloud-based system to secure systems and data in cloud deployment(“What it is Network intrusion detection system?,” 2012).

Furthermore, there exist widespread benefits of IDS. The fundamental capability it harnesses is strengthening the competence of an organization to determine the security incidents. Nowadays, several organizations have advanced to manifest the benefits of IDS listed as the assistance in analyzing the quantity and type of threats and further using the essential information to transform variations in the security systems or introduce efficient controls (Pharate, Bhat, & Mhetre, 2015). Organizations can also detect complexities or bugs within the network device configuration. All of these metrics can be further integrated to assess future threats. One of the most profound benefits of IDS is the privilege offered to the businesses to accomplish regulatory compliance in true letter and spirits. The regulatory compliance of a business is the adherence to regulations, laws, specifications and guidelines pertinent to various strategic business purposes. If a business violates the provisions of the regulatory compliance, federal fines and legal punishment is imposed. After implementing the IDS, businesses can meet the security regulations by underpinning thorough visibility across the networks. The IDS logs playa an instrumental role. Businesses, these days, can employ them as an essential part of the documentation to demonstrate they are adhering to the compliance requirements.

Besides, the IDS maximizes the security network and response of an organization. Since sensors can locate the network devices and hosts, the data in the network packets can be inspected and the operating system of the services can also be examined. The alternative to this process is the application of manual configuration. IDS proves to be productive to a significant extent in comparison to the manual censuses of the connected networks. In addition, the reliance on the technological framework has become imperative for businesses to expand and experience sustainable growth. With the surge of e-commerce businesses, high profile applications and online banking, it is evident that the organizations seek the finest protection to shield themselves against the unauthorized entities. However, the peril of network intrusion transcends the significantly publicized instances as reflected by the website defacement. It will be, irrefutably, a misnomer to infer that the adversity of intrusion is pertinent to the internet platforms and businesses only. In essence, the risk of network intrusion looms over each organization which possesses a critical network exposed to the outsiders.

The primary manifestation underpinning the need and growth of each business is widespread and string network of connectivity. Even the businesses devoid of the potential presence of the internet in their ventures are also prone to intrusions and hacker attacks. None of the leading businesses in the modern era are immune to the peril of a breach or unauthorized access. Several businesses operating network nurture the competence to permit the outside contractors and members of the organization to remotely connect to the systems. However, it renders the system susceptible to a breach or intrusion of a third party. All these adversities are confronted by the installation of a strong firewall in the network operations and accessibility of the organization. However, it lacks the potential to shield the crucial framework of a business. Data communications, external connectivity, voice-over IP and internet access are the prominent aspects prone to intrusion or damage (“How Your Small Business Benefits from Network Security,” 2017). IDS serves the purpose to confront all the adversities related to the security of an organization by identifying the breach and unwanted activity in an appropriate time.

Likewise, the comprehension of the various dimensions of the IDS is imperative for the businesses to strengthen the security paradigms and ensure profound and sustainable protection for the future. Signature-based is the crux of most of the IDS. It is similar to the functioning of a virus scanner by exploring a signature or known identity for every event of an intrusion. The hackers can employ a wide range of techniques to deceive the signature-based method. Thus, it is paramount to ensure the regular updates of the signature. The signature-based IDS primarily manifests the execution in the form of a database of preserved signatures. Unicode offers a uniform representation of every character in each language by offering a unique identifier or a specific code point for every character. Since signature-based IDS is prone to overlook the characters represented in Unicode format, it becomes suitable for the intruder to submit the URL constituting an exploit which allows other programs to be executed on the host system. Therefore, it is imperious for businesses to discover other IDS than the signature based.

Businesses aspiring to implement a profound and competent solution ought to consider the anomaly-based IDS. It is a complex structure that captures the headers of the packets headed toward the network. Consequently, the legal and known traffic is filtered, comprising the web traffic to web servers of businesses, mail traffic to mail servers, outgoing traffic from organizations’ employees and DNS traffic from the DNS server (Javaid, Niyaz, Sun, & Alam, 2015). These security metrics yield potential advantage to a business in comparison to the utilization of a signature-based IDS. For instance, it is adept at determining unusual or new traffic by determining the probes and sweeps toward the network hardware. Businesses can, thus, avail themselves of the early signs of intrusion as scans and probes are the predecessors of each attack. Telnet, for example, deployed on a network router to meet the maintenances is not updated timely. Anomaly-based IDS becomes the ultimate platform for identifying various threats from web and port anomalies to miscalculated attacks because of the deliberate mistakes in URL. A critical appraisal of the security trends in the contemporary framework of businesses reveals that even complex and leading organizations lack the experience to analyze signature and anomaly-based intrusion detection networks.

 The growth and strength of each business lie at the very heart of identifying the lacunas in the network operations and removing them by strengthening the security metrics comprehensively. The consumption of resources because of the advent of huge or unwanted traffic is a major concern for businesses. The assistance offered by the IDS to the relevant controls is essential to combat these security risks. The IDS shields other security metrics and shares their workload to regulate the flow of traffic. Intrusion protection system IPS is similar to the IDS to determine and block the attacks. IPS technologies can be employed in several forms where the dedicated software and hardware are prominently used. However, the cost factors associated with this kind of IPS may consume exorbitant price. It profoundly reciprocates by preventing the attacks from affecting business and further establishing a controlled baseline for operational activities of a business.

**Conclusion**

In the contemporary age, the personal information of an individual is prone to be stolen or authorized. The large scale businesses face detrimental consequences because of the breach of the security network. The fundamental technique pursued by businesses is the identification of unauthorized access. The primary objective of organizations is to safeguard their assets that are crucial for the protection of the tangible assets of a company. The IDS emerges as the ultimate option to place a consolidated system of identification of threats. The Intrusion detection system has assumed a critical role in the paradigm of the growth and sustainability of businesses. It is fundamentally deployed to monitor the network traffic and taking plausible actions to alert in case of a breach. Technology has advanced to shape and define implications for several businesses. The intruders have also cultivated these trends to adopt innovative security threats to launch elaborate attacks. Therefore, the need of the hour is to implement a strategic IDS on complex and critical networks. As deliberated above, it not only monitors the firewall, files and routers but also underpins a pattern of malicious activities to assist the business to organize and implement controls profoundly. Moreover, it enables businesses to meet the needs necessary for compliance. The bottom line is that the current state of technological advancement has made it the key for businesses to shield themselves of potential intruders by implementing IDS.

References

How Your Small Business Benefits from Network Security. (2017, November 24). Retrieved April 5, 2019, from Business.org website: https://www.business.org/it/cyber-security/how-your-small-business-benefits-from-network-security/

Intrusion detection systems – SecTools Top Network Security Tools. (n.d.). Retrieved April 5, 2019, from https://sectools.org/tag/ids/

Javaid, A. Y., Niyaz, Q., Sun, W., & Alam, M. (2015). A Deep Learning Approach for Network Intrusion Detection System. *BICT*. https://doi.org/10.4108/eai.3-12-2015.2262516

Pharate, A., Bhat, H., & Mhetre, N. A. (2015). *LOCATION 2 . 1 Host Based Network Intrusion Detection :*

What it is Network intrusion detection system? (2012, February 27). Retrieved April 5, 2019, from COMBOFIX website: https://combofix.org/what-it-is-network-intrusion-detection-system.php