Networking Assignment

**Name**

**Institutional Affiliation**

Networking Assignment

**Suitable Detection System that can Operate on Gateway**

An intrusion detection system (IDS) comprises of a software application or device that is bestowed in monitoring a network, servers, or systems for malicious operations. In a network environment that is made up of client-server architecture, application of network intrusion and detection system (NIDS) is inevitable. Ideally, NIDS that depend on signatures must update the signature database regularly. The most suitable intrusion detection system that can reside on gateway is Gateway Intrusion Detection system, which is designed to prevent malicious traffic and generating alerts on suspicious traffic (Malav et al., 2016). With an ideal gateway, it becomes possible for it to stop all known exploits. In the client server architecture, gateway IDS prevents suspect packets and preventing successful intrusions. Based on the basic theory of operations of gateway IDS over client and server architecture, it makes forward/ drop decisions where packets pass over the network.

**Transport Layer Security (TLS)**

TLS is a broadly adopted security protocol that has been developed to facilitate data privacy as well as communication over the network/ internet. TLS can be authenticated using public key infrastructure between web applications (clients) and servers. In the encryption of web traffic, both TLS and HTTP are the protocols that offer encryption and authentication in reassuring people that they are connecting to the websites that they intend. In the client server architecture, mutual authentication is implemented suing Public Key Infrastructure, where each security exit obtains some random data through authentication and by checking digital signature through public key. Some openssl commands in creation of the all the necessary certificates as shown below.

1. *openssl version -a for checking the version of SSL*
2. *openssl genrsa -out yourdomain.key 2048 for generating the key using RSA algorithms.*
3. *openssl rsa -text -in yourdomain.key -noout for decoding the private as weoo as viewing contents*
4. *openssl req -new -key yourdomain.key -out yourdomain.csr*

*for creating a CSR file through your newly generated private key*.

**Explain How PKI Mechanism can be Extended to Provide PKI Authentication**

Notably, PKI tends to link public keys with some entities that offer unique identities, which are referred to as subscribers. Such linkage is made easier through the process of registration and certificate issue by authorized organizations known as Certificate Authority (CA). In ensuring that PKI offers authentication, the process of registration requires requests to be made to the organization such as Registration Authority (RA). Additionally, in extending PKI to offer authentication, the idea is having one or more trusted parties digitally sign documents certifying that a specific cryptographic key belongs to a particular user or device (Zhao et al., 2007). Extending PKI authentication to the client browser may take a different route, which requires installation of Digital Authentication Client Plugin and installing it as an extension to the browser. Upon installation, the final step is to enroll for a certificate and then reboot the system, which is accompanied by enrollment email. With PKI authentication, it is considered to be more resilient to brute force attacks does not necessary require end users to remember anything meaning that the security of PKI is stronger as compared to other security mechanisms such as use of traditional passwords. With extension of PKI authentication to the client browser, it adds security that is being offered via the installation of SSL. This makes it possible to offer a higher level of security that cannot be compromised by the hackers. However, PKI authentication on the client browser is not normally used on the internet since browsers normally do not allow submission of arbitrary requests. In this case, all the communication through HTTP requests maybe blocked making website appear untrusted.

**Inspection of TLS Encrypted Traffic by IDS**

Indeed, it is required for the intrusion detection system designed to be able to inspect the TLS inspected traffic through daisy chain of devices to decrypt and re-encrypt the traffic encrypted with the TLS. Additionally, with the IDS, the whole process helps the organizations to monitor for the potential threats such as malware based on the incoming encrypted traffic. The whole concept of inspecting of the TLS encrypted traffic allow organizations to monitor the outbound encrypted traffic for data exfiltration as well as active command and control communications with the malicious servers (Borkar, 2019). With the server and gateway managed by the organization, TLS inspection would be done by the IDS residing on the server side. This would require configuration of policy-based rules that an idea does, which can respond in real time to stop any immediate threats. IDS would also play a critical role on TLS encrypted traffic to ensure decryption and re-encryption is done by preventing any malicious operations from penetrating to the server and organization systems. Additionally, with the construction of secure gateway as a remote access solution on the server network configuration, this will be important as it will escalate the security within the organization computer and information systems

References

Borkar, P. (2019). IPS Security: How Active Security Saves Time and Stops Attacks in their Tracks. *Accessed on*, *13*, 2019.

Malav, S., Avinash, M. S., Satish, N. S., & Sandeep, S. C. (2016). Network security using IDS, IPS & honeypot. *International Journal of Recent Research in Mathematics computer Science and Information Technology*, *2*(2), 27-30.

Zhao, S., Aggarwal, A., & Kent, R. D. (2007, July). PKI-based authentication mechanisms in grid systems. In *2007 International Conference on Networking, Architecture, and Storage (NAS 2007)* (pp. 83-90). IEEE.