**Assessment 1d- Bi-weekly Report (week 7-8)**

Network Address translation (NAT) is a process where a network device is assigned a public IP address to a group of devices in the internal network. The primary purpose of using NAT is to make public Ip addresses reusable, as a result, limiting the number of public IP addresses be used by the company. However, besides making IP reusable for firms it also adds a layer of security, by hiding devices such as computers, servers, information systems to the outside world.

However, when an internal host needs to communicate with the outside world, it will be assigned a public IP address by converting the private IP address to public, and hence, this translation is done by NAT itself. However, ALG (Application Layer Gateway) is a security component that enhances the NAT security employed in a computer network. The additional security provided by ALG is that it allows customized NAT traversal filters to be integrated into the gateway to support port and address translation. Moreover, ALG allows TCP/UDP ports to communicate with ports used by server applications but, a firewall might allow only a limited number of ports. Also, ALG will work as a medium between application server and the internet, providing security with means to application protocols.

By not implementing ALG, these ports would get blocked and the network administrator would need to manually open a large number of ports in the firewall, as a result, this would lead ports susceptible to attacks. Furthermore, the ALG is similar to a proxy server that resides between the client and the server. The ALG intercepts the message without the application being configured and the client being aware of whereas, in a proxy the client is aware about it and connects to it.

However, even after deploying an Application Layer gateway, gaps would still exists in the organizations security posture due to the following

* In the Application Layer Gateway the entire packet is scanned based on the rules defined that will enable it to filter out. However, the only function it will be able to do is block packets that defy rules but not scan the contents of the packet, as a result, won’t be able to detect attacking signatures
* The application layer gateway works at only the Application Layer of the OSI model, scanning each packet and checking if the type of data is correct for the specific application to communicate. This hinders its capability to be aware of other layers of the OSI layer, hence, lacks the feature of deep packet inspection and not providing the level of security
* The use of WPA3 itself has some serious flaws, allowing an intruder to establish a twin copy of the Wi-Fi network. This makes it susceptible to attacks and information can be extracted and, hence security infrastructure weakened due to WPA3s backward capability.

Solution

* Use web application firewalls that offer more protection by deep scanning contents of packets and see if there are contents that match the attacking vectors
* Implement a stateful inspection firewall also known as a deep packet inspection uses all the layers within the OSI layer included in the packets, including the examination of the data itself.
* Implement end-point security allowing endpoint security software to secure devices in an enterprise network. application controls prevents users from creating unauthorized applications that would create flaws in networks

# References

* www.sciencedirect.com. (n.d.). *Application Layer Gateway - an overview | ScienceDirect Topics*. [online] Available at: https://www.sciencedirect.com/topics/computer-science/application-layer-gateway.
* ‌Forcepoint. (2018). *What is Endpoint Security?* [online] Available at: https://www.forcepoint.com/cyber-edu/endpoint-security.