University of Essex Online

Launching into Cyber Security January 2021

Collaborative Learning Discussion 2

Summary Post

The last two weeks' discussion was interested in learning several kinds of software and hardware security issues. It was very knowledgeful for the network's firewall security levels and more critical knowledge about other software security like the Data Loss Prevention, Secure DNS, and MFA.

Next-Generation Firewall can help to protect our network from external threats, identify attacks, malware and other capabilities by checking each packets going through it using deep content inspection.

(Luvaha, 2021) agreed with the use of Intrusion detection systems (IDS) and how using deferent types of the IDS system like HIDS, NIDS, or PIDS can add more protection and monitoring to any infrastructure that uses it. When the Wireless IDS can screen and investigate the wireless traffics to detect any data breach.

The point raised by Anum about the NAT technology and the weaknesses by using it slightly correct, NAT uses a high amount of processor and memory utilisation when several numbers of NATs implement in a small firewall model. Usually, it is recommended to use a medium or large firewall model when high numbers of NATs and policies need to be implanted, but that will cost the extra business money.

Anum mentions that the IT professional guys should be highly skilled and familiar with IDS support and implementation to avoid any abnormal issues. (Rashid, 2021).

Back to Jan's post, IDS and IPS are an advanced form of packet inspection if they get deployed professionally and strip out any TLS encryption of the traffic to let the IDS and IPS scan it probably. The point of Zero-days is entirely correct, and the support security team should keep all the IDS or IPS databases up-to-date to avoid any malware attacks and keep the network protected and secured. (Kufner, 2021)

Furthermore, Samiya mentioned that any organisation should use the hardware and software firewall as two security levels when the hardware firewall can filter the packets, which refers to the dependency on the control of the source and destination IP addresses. The proxy or the software firewall acts like a dual-home host connected to two different networks or external networks. (Nova, 2021).

(Kan, 2021) raised a perfect point about the Out-of-band management and how border network devices should be protected from outside access, as that will avoid any external threats or Denial of Service attacks.

A practical, managed firewall will significantly reduce risk to the business. Without a firewall, the business could easily succumb to a cyber-attack, causing the loss of all critical data. This would not only disrupt business processes; it would also reduce productivity and likely damage the reputation and brand. (Netstar, 2021)

References:

- Luvaha, D. (2021) Collaborative Learning Discussion 2, Initial Post by Ahmad Alkam, 06 March 2021. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=245271
- Rashid, A. (2021) Collaborative Learning Discussion 2, Initial Post by Ahmad Alkam, 09 March 2021. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=245271
- Kufner, J. (2021) Collaborative Learning Discussion 2, Initial Post by Ahmad Alkam, 06 March 2021. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=245271
- Nova, S. (2021) Collaborative Learning Discussion 2, Initial Post by Ahmad Alkam, 06 March 2021. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=245271
- Khan, U. (2021) Collaborative Learning Discussion 2, Initial Post by Ahmad Alkam, 13 March 2021. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=245271
- Netstar (2021) Why do I need a firewall?. Available from: https://www.netstar.co.uk/why-do-i-need-a-firewall-business/ [Accessed 20 Mach 2021].