Resumen

Hoy en día, todo el mundo ha oído hablar de la ciberseguridad como una medida contra los ataques informáticos; todo el mundo lo sufre diariamente; y todo el mundo lo puede evitar de alguna manera. Para las pequeñas redes, como una casa o un local, las medidas de seguridad que interfieren son sencillas, como por ejemplo las ACLs (access lists), la autenticación o las contraseñas; en las grandes redes, como una empresa, las medidas que interfieren aumentan y algunos ejemplos son el firewall, el IDS (sistema de detección de intrusos, NIDS por red y HIDS por sistema), las VLANS (redes de área local virtuales), etc. En particular, en el presente trabajo se mostrará un método (muy útil y poco común) fundamentado en el port mirroring o también llamado la duplicación de puertos. Habrá un puerto del conmutador que pertenecerá a una VLAN donde capturará todo el tráfico que se lo enviará a otro puerto dentro de la misma VLAN donde estará un IDS que comprobará que todo el tráfico que circula por ese puerto es correcto y que no se detectan intrusiones o ataques informáticos de ningún tipo como por ejemplo el malware para el robo de datos, Man-in-the-Middle, o denegación de servicios (DoS, DDoS) que son los mas típicos. En conclusión, este método conduce a una infraestructura de red más segura y más controlada para el entorno de la empresa ya que puede producir resultados altamente detallados para registro y análisis del monitoreo donde puede incluso bloquear los signos de intrusión y sobrecarga maliciosa de la red.

Palabras clave: port mirror, IDS, monitoreo, ataques informáticos, tráfico de red, paquetes capturados.

Abstract

Nowadays, everyone has heard of cyber security as a measure against cyber attacks; everyone suffers from it on a daily basis; and everyone can prevent it in some way. For small networks, such as a house or premises, the interfering security measures are simple, such as ACLs (access lists), authentication or passwords; for big networks, such as an enterprise, the interfering measures increase and some examples are firewall, IDS (intrusion detection system, NIDS per network and HIDS per system), VLANS (virtual local area networks), etc. In particular, this paper will show a (very useful and uncommon) method based on port mirroring. There will be a port of the switch that will belong to a VLAN where it will capture all the traffic that will be sent to another port within the same VLAN where there will be an IDS that will check that all the traffic flowing through that port is correct and that no intrusions or computer attacks of any kind are detected, such as malware for data theft, Man-in-the-Middle, or denial of services (DoS, DDoS), which are the most typical ones. In conclusion, this method leads to a more secure and more controlled network infrastructure for the enterprise environment as it can produce highly detailed results for logging and monitoring analysis where it can even block signs of intrusion and malicious network overload.

Keywords: port mirror, IDS, monitoring, computer attacks, network traffic, captured packets.