Investigación de Herramientas de Pentesting en Sistemas SCADA.

Eduardo Vásquez P.; Helder Castrillón C.

Herramienta	**Referencia**	**Título**
Shodan, Nessus	[1]	Identifying SCADA Vulnerabilities Using Passive and Active Vulnerability Assessment Techniques
Nmap, ZMap, Nessus, Passive Vulnerability Scanner, Shodan, Tshark, Ettercap, Phyton UDP_DoS.py	[2]	Vulnerability Analysis of Network Scanning on SCADA Systems
Kali Linux, Wireshark	[3]	Network Security Analysis SCADA System Automation on Industrial Process
Smod pentesting tool	[4]	Analysis of SCADA Security using Penetration Testing: A case study on Modbus TCP Protocol

Referencias.

[1] S. Samtani, S. Yu, H. Zhu, M. Patton, and H. Chen, “Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques,” *IEEE Int. Conf. Intell. Secur. Informatics Cybersecurity Big Data, ISI 2016*, pp. 25–30, 2016, doi: 10.1109/ISI.2016.7745438.

[2] K. Coffey, R. Smith, L. Maglaras, and H. Janicke, “Vulnerability Analysis of Network Scanning on SCADA Systems,” *Secur. Commun. Networks*, vol. 2018, 2018, doi: 10.1155/2018/3794603.

[3] H. Hilal and A. Nangim, “Network security analysis SCADA system automation on industrial process,” *2017 Int. Conf. Broadband Commun. Wirel. Sensors Powering, BCWSP 2017*, vol. 2018-Janua, pp. 1–6, 2018, doi: 10.1109/BCWSP.2017.8272569.

[4] J. Luswata, P. Zavarsky, B. Swar, and D. Zvabva, “Analysis of SCADA Security Using Penetration Testing: A Case Study on Modbus TCP Protocol,” *29th Bienn. Symp. Commun. BSC 2018*, no. Bsc, pp. 1–5, 2018, doi: 10.1109/BSC.2018.8494686.