World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:18, No:12, 2024

On the Resilience of Operational Technology Devices in Penetration Tests

Authors : Marko Schuba, Florian Kessels, Niklas Reitz

Abstract : Operational technology (OT) controls physical processes in critical infrastructures and economically important industries. With the convergence of OT with classical information technology (IT), rising cybercrime worldwide and the increasingly difficult geopolitical situation, the risks of OT infrastructures being attacked are growing. Classical penetration testing, in which testers take on the role of an attacker, has so far found little acceptance in the OT sector - the risk that a penetration test could do more harm than good seems too great. This paper examines the resilience of various OT systems using typical penetration test tools. It is shown that such a test certainly involves risks, but is also feasible in OT if a cautious approach is taken. Therefore, OT penetration testing should be considered as a tool to improve the cyber security of critical infrastructures.

Keywords : penetration testing, OT, ICS, OT security
Conference Title : ICCSCIT 2024 : International Conference on Computer Science, Cybersecurity and Information Technology
Conference Location : New York, United States
Conference Dates : December 09-10, 2024