ISSN 2473-4901
v7 n5600

Teaching Case

Rubber Duckies in the Wild:
Proof of concept lab for USB pen testing tool

Anthony Serapiglia
Saint Vincent College, Latrobe, PA, 15650
Anthony.Serapiglia@stvincent.edu

Abstract

Ethical Hacking has matured into a widely accepted and necessary part of the cybersecurity world. Actively probing and testing the defenses of a network or business system is essential to maintaining CIA benchmarks of Confidentiality, Integrity, and Availability. Penetration testing has evolved into a special subset of the industry. Companies and organizations of all sizes and across a range of industries rely on Pen testers to proactively identify weakness in cyber-defenses before a real attack effects real damage. One of the primary objectives of penetration testers is the creation of a remotes access shell into a system. A common method of achieving this is through the use of "rubber ducky" USB devices that when inserted into computing services activate an active session from inside a network to allow remote access to the pen tester. This teaching case provides background and instructions on incorporating a proof-of-concept rubber ducky build into an undergraduate cybersecurity course.

Keywords: Penetration Testing, Ethical Hacking, Cybersecurity, Rubber Ducky, White Hat Hacking

An updated version of this manuscript may be found at https://cppj.info