Research Abstract: Holistic Penetration Testing and its Potency

Brad Regeski

In linear terms, A penetration tester discovers B exploit in the designated area of the system and gains access to C product, A + B = C.

But in the hyper-connected world we know today, the exponential occurrences of exploits and vulnerabilities rises across many different systems, programs and applications. The company-defined scope of a normal penetration test limits the potential ability and potency of any penetration test, but this remains the popular approach in the industry today, as dynamic companies very often develop new products/applications which require vulnerability assessments before being deployed. Limiting the test to just the new product, and failing to calculate for the entirety of the broad scope of the system, allows for malicious attackers to bypass these “product-defined areas” and find exploits on the other side of the system that allow them access into the new, desired product.

In new holistic terms, A penetration tester finds Z exploit on the other side of the system which magnifies to comprise the entire “alphabet” of the system and then gain access to the desired C product, A(Z)=A…Z=C.

In the proposed paper, an analyzation of the experimental holistic penetration testing will occur, regarding its benefits, potential damages, and a comparison to the regular pre-defined pen test. Said comparison will be calculated by real-world examples of potential threats, the potential approach by both, and their own calculations of the popular OWASP Risk Rating Methodology [1], an equation used to determine potential risk and cost to business entities.

Keywords: Cyber-Security, Technology, Security, Computer-Science, Hacking, Penetration Testing, Computer Ethics

[1]-https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology