Penetration testing - A systematic review of the literature

Appendix A - The complete list of reviewed articles

Fredrik Heiding, Robert Lagerström

1 Conclusion

Penetration testing is a fast growing field within cyber security. The study has performed an in depth analysis of articles within penetration testing and ethical hacking in order to analyze the domain. The articles were divided in four different clusters: *C1: New penetration testing tools, C2: New penetration testing methods, C3: Penetration testing something* and *C4: Informative research about penetration testing.* A majority of the highly cited articles comes from conference papers which may be a deviation from other academic fields, and conference papers also had the most articles in sheer numbers (from the analyzed papers). Penetration testing a single device or otherwise exploiting a vulnerability can be sufficient material for an academic publication, but it depends on surrounding contexts such as where the article is sent for publication and how the study was conducted, it also appears to be beneficial if the paper uses the penetration testing result to analyze a larger area or an underlying problem. The articles were generally published more frequently in later years and most of the findings seem to indicate that penetration testing will grows in the future, both as an academic field and as a commercial practice.