Penetration testing - A systematic review of the literature

Appendix A - The complete list of reviewed articles

Fredrik Heiding, Robert Lagerström

References

[1] Akond Rahman and Laurie Williams. A bird's eye view of knowledge needs related to penetration testing. In *Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security*, pages 1–2, 2019.

[2] Seungsoo Lee, Jinwoo Kim, Seungwon Woo, Changhoon Yoon, Sandra Scott-Hayward, Vinod Yegneswaran, Phillip Porras, and Seungwon Shin. A comprehensive security assessment framework for software-defined networks. *Computers & Security*, 91:101720, 2020.

[3] Segundo Moisés T Toapanta, Marjorie Isanoa Sinche, and Luis Enrique Mafla Gallegos. A cyber environment approach to mitigate vulnerabilities and threats in an electoral process in ecuador. In *Proceedings of the 2019 2nd International Conference on Education Technology Management*, pages 97–104, 2019.

[4] Valentina Casola, Alessandra De Benedictis, Massimiliano Rak, and Umberto Villano. A methodology for automated penetration testing of cloud applications. *International Journal of Grid and Utility Computing*, 11(2):267–277, 2020.

[5] Thuy D Nguyen, Steve C Austin, and Cynthia E Irvine. A strategy for security testing industrial firewalls. In *Proceedings of the Fifth Annual Industrial Control System Security (ICSS) Workshop*, pages 38–47, 2019.

[6] Keyur Patel. A survey on vulnerability assessment & penetration testing for secure communication. In *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, pages 320–325. IEEE, 2019.

[7] Alberto Giaretta, Michele De Donno, and Nicola Dragoni. Adding salt to pepper: A structured security assessment over a humanoid robot. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pages 1–8, 2018.

[8] Saraswati Maddala and Sonali Patil. Agentless automation model for post exploitation penetration testing. In *International Conference on Intelligent Computing, Information and Control Systems*, pages 529–539. Springer, 2019.

[9] Joshua Eckroth, Kim Chen, Heyley Gatewood, and Brandon Belna. Alpaca: Building dynamic cyber ranges with procedurally-generated vulnerability lattices. In *Proceedings of the 2019 ACM Southeast Conference*, pages 78–85, 2019.

[10] Yugansh Khera, Deepansh Kumar, Nidhi Garg, et al. Analysis and impact of vulnerability assessment and penetration testing. In *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, pages 525–530. IEEE, 2019.

[11] Ajay M Patel and Hiral R Patel. Analytical study of penetration testing for wireless infrastructure security. In *2019 International Conference on Wireless Communications Signal*

Processing and Networking (WiSPNET), pages 131–134. IEEE, 2019.

[12] Stefan Marksteiner and Zhendong Ma. Approaching the automation of cyber security testing of connected vehicles. In *Proceedings of the Third Central European Cybersecurity Conference*, pages 1–3, 2019.

[13] Fabrizio Baiardi. Avoiding the weaknesses of a penetration test. *Computer Fraud & Security*, 2019(4):11–15, 2019.

[14] Nuthan Munaiah, Akond Rahman, Justin Pelletier, Laurie Williams, and Andrew Meneely. Characterizing attacker behavior in a cybersecurity penetration testing competition. In *2019 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)*, pages 1–6. IEEE, 2019.

[15] Y Mirsky, T Mahler, I Shelef, and Y Elovici. Ct-gan: malicious tampering of 3d medical imagery using deep learning. 2019, 2019.

[16] Ryan Brunner, Sang Keun Oh, Jesse Ramirez, Paul Houck, Nathaniel Stickney, and Raymond Blaine. Design for an educational cyber range. HotSoS '19, New York, NY, USA, 2019. Association for Computing Machinery.

[17] R. H. Abdul Raman. Enhanced automated-scripting method for improved management of sql injection penetration tests on a large scale. In *2019 IEEE 9th Symposium on Computer Applications Industrial Electronics (ISCAIE)*, pages 259–266, 2019.

[18] Aaron Yi Ding, Gianluca Limon De Jesus, and Marijn Janssen. Ethical hacking for boosting iot vulnerability management: A first look into bug bounty programs and responsible disclosure. ICTRS '19, New York, NY, USA, 2019. Association for Computing Machinery.

[19] M. Azaharimohdyusof and A. Samadshibghatullah. Experimental assessment of freeware penetration testing tools against network environment. *International Journal of Advanced Science and Technology*, 28(1):339–350, 2019. cited By 0.

[20] Prashast Srivastava, Hui Peng, Jiahao Li, Hamed Okhravi, Howard Shrobe, and Mathias Payer. Firmfuzz: automated iot firmware introspection and analysis. In *Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things*, pages 15–21, 2019.

[21] Ahmad Salah Al-Ahmad and Hasan Kahtan. Fuzz test case generation for penetration testing in mobile cloud computing applications. In *International Conference on Intelligent Computing & Optimization*, pages 267–276. Springer, 2018.

[22] Da-Yu Kao, Yun-Ya Chen, and Fuching Tsai. Hacking tool identification in penetration testing. In *2020 22nd International Conference on Advanced Communication Technology (ICACT)*, pages 256–261. IEEE, 2020.

[23] Yu Ye, Jun Guo, Xunjian Xu, Qinpu Li, Hong Liu, and Yuelun Di. High-risk problem of penetration testing of power grid rainstorm disaster artificial intelligence prediction system and its countermeasures. In *2019 IEEE 3rd Conference on Energy Internet and Energy System Integration (EI2)*, pages 2675–2680. IEEE, 2019.

[24] Defiana Arnaldy and Audhika Rahmat Perdana. Implementation and analysis of penetration techniques using the man-in-the-middle attack. In *2019 2nd International Conference of Computer and Informatics Engineering (IC2IE)*, pages 188–192. IEEE, 2019.

[25] Jasmin A Caliwag, Roxanne A Pagaduan, Reynaldo E Castillo, and Walter Van J Ramos. Integrating the escaping technique in preventing cross site scripting in an online inventory system. In *Proceedings of the 2019 2nd International Conference on Information Science and Systems*, pages 110–114, 2019.

[26] Rajiv Kumar and Katlego Tlhagadikgora. Internal network penetration testing using

free/open source tools: Network and system administration approach. In *International Conference on Advanced Informatics for Computing Research*, pages 257–269. Springer, 2018.

[27] G. Yadav, A. Allakany, V. Kumar, K. Paul, and K. Okamura. Penetration testing framework for iot. In *Proceedings - 2019 8th International Congress on Advanced Applied Informatics, IIAI-AAI 2019*, pages 477–482, 2019.

[28] Dimitri Michel Stallenberg and Annibale Panichella. Jcomix: a search-based tool to detect xml injection vulnerabilities in web applications. In *Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, pages 1090–1094, 2019.

[29] Anis Kothia, Bobby Swar, and Fehmi Jaafar. Knowledge extraction and integration for information gathering in penetration testing. In *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pages 330–335. IEEE, 2019.

[30] Philipp Zech, Michael Felderer, and Ruth Breu. Knowledge-based security testing of web applications by logic programming. *International Journal on Software Tools for Technology Transfer*, 21(2):221–246, 2019.

[31] Md Moniruzzaman, Farida Chowdhury, and Md Sadek Ferdous. Measuring vulnerabilities of bangladeshi websites. In *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, pages 1–7. IEEE, 2019.

[32] Suneel Randhawa, Benjamin Turnbull, Joseph Yuen, and Jonathan Dean. Mission-centric automated cyber red teaming. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pages 1–11, 2018.

[33] Nikolaos Koutroumpouchos, Georgios Lavdanis, Eleni Veroni, Christoforos Ntantogian, and Christos Xenakis. Objectmap: detecting insecure object deserialization. In *Proceedings of the 23rd Pan-Hellenic Conference on Informatics*, pages 67–72, 2019.

[34] Marwa Elsayed and Mohammad Zulkernine. Offering security diagnosis as a service for cloud saas applications. *Journal of information security and applications*, 44:32–48, 2019.

[35] Koichi Funaya, Samir Bajaj, Kumar Sharad, and Alok Srivastava. Optimizing the sequence of vulnerability scanning injections. In *2018 IEEE Conference on Dependable and Secure Computing (DSC)*, pages 1–2. IEEE, 2018.

[36] Mujahid Shah, Sheeraz Ahmed, Khalid Saeed, Muhammad Junaid, Hamayun Khan, et al. Penetration testing active reconnaissance phase–optimized port scanning with nmap tool. In *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, pages 1–6. IEEE, 2019.

[37] Ge Chu and Alexei Lisitsa. Penetration testing for internet of things and its automation. In *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pages 1479–1484. IEEE, 2018.

[38] Geeta Yadav, Kolin Paul, Alaa Allakany, and Koji Okamura. Iot-pen: A penetration testing framework for iot. In *2020 International Conference on Information Networking (ICOIN)*, pages 196–201. IEEE, 2020.

[39] Tomas Zitta, Marek Neruda, Lukas Vojtech, Martina Matejkova, Matej Jehlicka, Lukas Hach, and Jan Moravec. Penetration testing of intrusion detection and prevention system in low-performance embedded iot device. In *2018 18th International Conference on Mechatronics-Mechatronika (ME)*, pages 1–5. IEEE, 2018.

[40] Dain Overstreet, Hayden Wimmer, and Rami J Haddad. Penetration testing of the amazon echo digital voice assistant using a denial-of-service attack. In *2019 SoutheastCon*, pages 1–6.

IEEE, 2019.

[41] John Mikulskis, Johannes K Becker, Stefan Gvozdenovic, and David Starobinski. Poster: Snout-an extensible iot pen-testing tool. 2019.

[42] Reynaldo E Castillo, Jasmin A Caliwag, Roxanne A Pagaduan, and Aira Camille Nagua. Prevention of sql injection attacks to login page of a website application using prepared statement technique. In *Proceedings of the 2019 2nd International Conference on Information Science and Systems*, pages 171–175, 2019.

[43] Muhammad Imran, Muhammad Faisal, and Noman Islam. Problems and vulnerabilities of ethical hacking in pakistan. In *2019 Second International Conference on Latest trends in Electrical Engineering and Computing Technologies (INTELLECT)*, pages 1–6. IEEE, 2019.

[44] Ralph Ankele, Stefan Marksteiner, Kai Nahrgang, and Heribert Vallant. Requirements and recommendations for iot/iiot models to automate security assurance through threat modelling, security analysis and penetration testing. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*, pages 1–8, 2019.

[45] Haitao Sun, Chengjie Jin, Xiaohan Helu, Hui Lu, Man Zhang, and Zhihong Tian. Research on android infiltration technology based on the silent installation of an accessibility service. *International Journal of Distributed Sensor Networks*, 16(2):1550147720903628, 2020.

[46] Guanyu Su, Fang Wang, and Qi Li. Research on sql injection vulnerability attack model. In *2018 5th IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS)*, pages 217–221. IEEE, 2018.

[47] Sundar Krishnan and Mingkui Wei. Scada testbed for vulnerability assessments, penetration testing and incident forensics. In *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, pages 1–6. IEEE, 2019.

[48] Ankur Chattopadhyay, Kevin Grondahl, Jason Ruckel, and Thomas Everson. Secure coding and ethical hacking workshops with nao for engaging k-12 female students in cs. In *2019 Research on Equity and Sustained Participation in Engineering, Computing, and Technology (RESPECT)*, pages 1–2. IEEE, 2019.

[49] Yashu Liu, Zhihai Wang, and Shu Tian. Security against network attacks on web application system. In *China Cyber Security Annual Conference*, pages 145–152. Springer, Singapore, 2018.

[50] Tao Tao, Yuan Chen, Bijing Liu, Xueqi Jin, Mingyuan Yan, and Shouling Ji. Security analysis of bioinformatics web application. In *International Conference on Security with Intelligent Computing and Big-data Services*, pages 383–397. Springer, 2018.

[51] Shai Cohen, Tomer Gluck, Yuval Elovici, and Asaf Shabtai. Security analysis of radar systems. In *Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy*, pages 3–14, 2019.

[52] Renato Rojas, Ana Muedas, and David Mauricio. Security maturity model of web applications for cyber attacks. In *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, pages 130–137, 2019.

[53] Christof Ebert. Security requirements engineering: From tara to pentest. In *2019 IEEE 27th International Requirements Engineering Conference (RE)*, pages 500–501. IEEE, 2019.

[54] Vaclav Oujezsky, David Chapcak, Tomas Horvath, and Petr Munster. Security testing of active optical network devices. In *2019 42nd International Conference on Telecommunications and Signal Processing (TSP)*, pages 9–13. IEEE, 2019.

[55] Arjun Shakdhe, Suyash Agrawal, and Baijian Yang. Security vulnerabilities in consumer iot applications. In *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecu-*

rity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), pages 1–6. IEEE, 2019.

[56] Ahmad Salah Al-Ahmad, Hasan Kahtan, Fadhl Hujainah, and Hamid A Jalab. Systematic literature review on penetration testing for mobile cloud computing applications. *IEEE Access*, 7:173524–173540, 2019.

[57] Arianit Maraj, Ermir Rogova, and Genc Jakupi. Testing of network security systems through dos, sql injection, reverse tcp and social engineering attacks. *International Journal of Grid and Utility Computing*, 11(1):115–133, 2020.

[58] Georg Thomas, Oliver Burmeister, Gregory Low, et al. The importance of ethical conduct by penetration testers in the age of breach disclosure laws. *Australasian Journal of Information Systems*, 23, 2019.

[59] Marcus Botacin, Anatoli Kalysch, and André Grégio. The internet banking [in] security spiral: Past, present, and future of online banking protection mechanisms based on a brazilian case study. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*, pages 1–10, 2019.

[60] Pengfei Shi, Futong Qin, Ruosi Cheng, and Kunsong Zhu. The penetration testing framework for large-scale network based on network fingerprint. In *2019 International Conference on Communications, Information System and Computer Engineering (CISCE)*, pages 378–381. IEEE, 2019.

[61] Patrick Speicher, Marcel Steinmetz, Jörg Hoffmann, Michael Backes, and Robert Künnemann. Towards automated network mitigation analysis. In *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, pages 1971–1978, 2019.

[62] Pierre Jourdan and Eliana Stavrou. Towards designing advanced password cracking toolkits: Optimizing the password cracking process. In *Adjunct Publication of the 27th Conference on User Modeling, Adaptation and Personalization*, pages 203–208, 2019.

[63] Mariano Ceccato, Paolo Tonella, Cataldo Basile, Paolo Falcarin, Marco Torchiano, Bart Coppens, and Bjorn De Sutter. Understanding the behaviour of hackers while performing attack tasks in a professional setting and in a public challenge. *Empirical Software Engineering*, 24(1):240–286, 2019.

[64] Rahul Emani, Edward J Glantz, Christopher Gamrat, and Michael K Hills. Using the raspberry pi in it education. In *Proceedings of the 20th Annual SIG Conference on Information Technology Education*, pages 153–153, 2019.

[65] Andy Kenner, Stephan Dassow, Christian Lausberger, Jacob Krüger, and Thomas Leich. Using variability modeling to support security evaluations: virtualizing the right attack scenarios. In *Proceedings of the 14th International Working Conference on Variability Modelling of Software-Intensive Systems*, pages 1–9, 2020.

[66] Joseph M Hatfield. Virtuous human hacking: The ethics of social engineering in penetration-testing. *computers & security*, 83:354–366, 2019.

[67] Arvind Goutam and Vijay Tiwari. Vulnerability assessment and penetration testing to enhance the security of web application. In *2019 4th International Conference on Information Systems and Computer Networks (ISCON)*, pages 601–605. IEEE, 2019.

[68] K Nagendran, A Adithyan, R Chethana, P Camillus, and KB Bala Sri Varshini. Web application penetration testing. *Int. J. Innov. Technol. Explor. Eng*, 8(10):1029–1035, 2019.

[69] Andrea Valenza. Web security training [at] unige: an experience. In *Proceedings of the Conference Companion of the 3rd International Conference on Art, Science, and Engineering of Programming*, pages 1–6, 2019.

[70] Dean Richard McKinnel, Tooska Dargahi, Ali Dehghantanha, and Kim-Kwang Raymond Choo. A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability assessment. *Computers & Electrical Engineering*, 75:175–188, 2019.

[71] Shih-jen Chen, Chung-huang Yang, and Shao-wei Lan. A distributed network security assessment tool with vulnerability scan and penetration test. 2007.

[72] Gu Hsin Lai. A light-weight penetration test tool for ipv6 threats. In *2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pages 49–52. IEEE, 2014.

[73] Charles P Pfleeger, Shari Lawrence Pfleeger, and Mary Frances Theofanos. A methodology for penetration testing. *Computers & Security*, 8(7):613–620, 1989.

[74] Pulei Xiong and Liam Peyton. A model-driven penetration test framework for web applications. In *2010 Eighth International Conference on Privacy, Security and Trust*, pages 173–180. IEEE, 2010.

[75] Takanobu Watanabe, Zixue Cheng, Mizuo Kansen, and Masayuki Hisada. A new security testing method for detecting flash vulnerabilities by generating test patterns. In *2010 13th International Conference on Network-Based Information Systems*, pages 469–474. IEEE, 2010.

[76] Jianbin Hu and Cong Tang. A novel framework to carry out cloud penetration test. *International Journal of Computer Network and Information Security*, 3(3):1, 2011.

[77] Mahin Mirjalili, Alireza Nowroozi, and Mitra Alidoosti. A survey on web penetration test. *Advances in Computer Science: an International Journal*, 3(6):107–121, 2014.

[78] Matt Bishop. About penetration testing. *IEEE Security & Privacy*, 5(6):84–87, 2007.

[79] Anestis Bechtsoudis and Nicolas Sklavos. Aiming at higher network security through extensive penetration tests. *IEEE latin america transactions*, 10(3):1752–1756, 2012.

[80] Lei Liu, Jing Xu, Hongji Yang, Chenkai Guo, Jiehui Kang, Sihan Xu, Biao Zhang, and Guannan Si. An effective penetration test approach based on feature matrix for exposing sql injection vulnerability. In *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, volume 1, pages 123–132. IEEE, 2016.

[81] Aileen G Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu, and Monique Jones. An overview of penetration testing. *International Journal of Network Security & Its Applications*, 3(6):19, 2011.

[82] Wei Tian, Ju-Feng Yang, Jing Xu, and Guan-Nan Si. Attack model based penetration test for sql injection vulnerability. In *2012 IEEE 36th Annual Computer Software and Applications Conference Workshops*, pages 589–594. IEEE, 2012.

[83] Jerry Hart. Criminal infiltration of financial institutions: a penetration test case study. *Journal of Money Laundering Control*, 2010.

[84] Hilary Berger and Andrew Jones. Cyber security & ethical hacking for smes. In *Proceedings of the The 11th International Knowledge Management in Organizations Conference on The changing face of Knowledge Management Impacting Society*, pages 1–6, 2016.

[85] Prashant S Shinde and Shrikant B Ardhapurkar. Cyber security analysis using vulnerability assessment and penetration testing. In *2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)*, pages 1–5. IEEE, 2016.

[86] Deris Stiawan, Mohd Yazid Idris, Abdul Hanan Abdullah, Fahad Aljaber, and Rahmat Budiarto. Cyber-attack penetration test and vulnerability analysis. *International Journal of Online and Biomedical Engineering (iJOE)*, 13(01):125–132, 2017.

[87] Andrey Petukhov and Dmitry Kozlov. Detecting security vulnerabilities in web applications using dynamic analysis with penetration testing. *Computing Systems Lab, Department of*

Computer Science, Moscow State University, pages 1–120, 2008.

[88] Ecir Uğur Küçüksille, Mehmet Ali Yalçınkaya, and Samet Ganal. Developing a penetration test methodology in ensuring router security and testing it in a virtual laboratory. In *Proceedings of the 8th International Conference on Security of Information and Networks*, pages 189–195, 2015.

[89] Rahmat Budiarto, Sureswaran Ramadass, Azman Samsudin, and Salah Noor. Development of penetration testing model for increasing network security. In *Proceedings. 2004 International Conference on Information and Communication Technologies: From Theory to Applications, 2004.*, pages 563–564. IEEE, 2004.

[90] Filip Holik, Josef Horalek, Ondrej Marik, Sona Neradova, and Stanislav Zitta. Effective penetration testing with metasploit framework and methodologies. In *2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI)*, pages 237–242. IEEE, 2014.

[91] Charles C. Palmer. Ethical hacking. *IBM Systems Journal*, 40(3):769–780, 2001.

[92] Ajinkya A Farsole, Amruta G Kashikar, and Apurva Zunzunwala. Ethical hacking. *International Journal of Computer Applications*, 1(10):14–20, 2010.

[93] Neeraj Kumar Rathore. Ethical hacking & security against cyber crime. *Journal on Information Technology (JIT)*, 5(1):7–11, 2016.

[94] Syed A Saleem. Ethical hacking as a risk management technique. In *Proceedings of the 3rd annual conference on Information security curriculum development*, pages 201–203, 2006.

[95] Zouheir Trabelsi and Margaret McCoey. Ethical hacking in information security curricula. *International Journal of Information and Communication Technology Education (IJICTE)*, 12(1):1–10, 2016.

[96] Gurpreet K Juneja. Ethical hacking: A technique to enhance information security. *International Journal of Innovative Research in Science, Engineering and Technology*, 2(12):7575–7580, 2013.

[97] Bryan Smith, William Yurcik, and David Doss. Ethical hacking: the security justification redux. In *IEEE 2002 International Symposium on Technology and Society (ISTAS'02). Social Implications of Information and Communication Technology. Proceedings (Cat. No. 02CH37293)*, pages 374–379. IEEE, 2002.

[98] Lei Liu, Jing Xu, Chenkai Guo, Jiehui Kang, Sihan Xu, and Biao Zhang. Exposing sql injection vulnerability through penetration test based on finite state machine. In *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, pages 1171–1175. IEEE, 2016.

[99] Aury M Curbelo and Alfredo Cruz. Faculty attitudes toward teaching ethical hacking to computer and information systems undergraduates students. In *Proceedings of the Eleventh LACCEI Latin American and Caribbean Conference for Engineering and Technology*, 2013.

[100] Sankalp Singh, James Lyons, and David M Nicol. Fast model-based penetration testing. In *Proceedings of the 2004 Winter Simulation Conference, 2004.*, volume 1. IEEE, 2004.

[101] Kevin P Haubris and Joshua J Pauli. Improving the efficiency and effectiveness of penetration test automation. In *2013 10th International Conference on Information Technology: New Generations*, pages 387–391. IEEE, 2013.

[102] DANISH Jamil and Muhammad Numan Ali Khan. Is ethical hacking ethical. *International journal of Engineering Science and Technology*, 3(5):3758–3763, 2011.

[103] Pulei Xiong, Bernard Stepien, and Liam Peyton. Model-based penetration test framework for web applications using ttcn-3. In *International Conference on E-Technologies*, pages 141–154.

Springer, 2009.

[104] Rainer Böhme and Márk Félegyházi. Optimal information security investment with penetration testing. In *International Conference on Decision and Game Theory for Security*, pages 21–37. Springer, 2010.

[105] Christian Mainka, Vladislav Mladenov, Juraj Somorovsky, and Jörg Schwenk. Penetration test tool for xml-based web services. In *ESSoS Doctoral Symposium 2013*, page 31, 2013.

[106] Christian Mainka, Juraj Somorovsky, and Jörg Schwenk. Penetration testing tool for web services security. In *2012 IEEE Eighth World Congress on Services*, pages 163–170. IEEE, 2012.

[107] Daniel Geer and John Harthorne. Penetration testing: A duet. In *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, pages 185–195. IEEE, 2002.

[108] Nitin A Naik, Gajanan D Kurundkar, Santosh D Khamitkar, and Namdeo V Kalyankar. Penetration testing: A roadmap to network security. *arXiv preprint arXiv:0912.3970*, 2009.

[109] Rina Elizabeth López de Jiménez. Pentesting on web applications using ethical-hacking. In *2016 IEEE 36th Central American and Panama Convention (CONCAPAN XXXVI)*, pages 1–6. IEEE, 2016.

[110] Wang Jiajia. Research of penetration test based on mobile internet. In *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, pages 2542–2545. IEEE, 2016.

[111] Radoslav Bozhinovski, Vesna Dimitrova, Boro Jakimovski, and Sashko Ristov. Security penetration test on fcse's it services. 2013.

[112] Brad Arkin, Scott Stender, and Gary McGraw. Software penetration testing. *IEEE Security & Privacy*, 3(1):84–87, 2005.

[113] Zouheir Trabelsi and Walid Ibrahim. Teaching ethical hacking in information security curriculum: A case study. In *2013 IEEE Global Engineering Education Conference (EDUCON)*, pages 130–137. IEEE, 2013.

[114] John Yeo. Using penetration testing to enhance your company's security. *Computer Fraud & Security*, 2013(4):17–20, 2013.

[115] GA Adegbite, OJ Emuoyibofarhe, FA Ajala, and JA Awokola. A cybersecurity approach for evaluating mobile agents. *Journal of Applied Security Research*, 12(2):253–259, 2017.

[116] Hira Asghar, Zahid Anwar, and Khalid Latif. A deliberately insecure rdf-based semantic web application framework for teaching sparql/sparul injection attacks and defense mechanisms. *computers & security*, 58:63–82, 2016.

[117] Mohammad Shakibazad. A framework to create a virtual cyber battlefield for cyber maneuvers and impact assessment. *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, 43(3):615–625, 2019.

[118] Harshit Gujral, Sangeeta Mittal, and Abhinav Sharma. A novel data mining approach for analysis and pattern recognition of active fingerprinting components. *Wireless Personal Communications*, 105(3):1039–1068, 2019.

[119] Chad Calvert, Taghi M Khoshgoftaar, Maryam M Najafabadi, and Clifford Kemp. A procedure for collecting and labeling man-in-the-middle attack traffic. *International Journal of Reliability, Quality and Safety Engineering*, 24(01):1750002, 2017.

[120] Miao Liu and Bin Wang. A web second-order vulnerabilities detection method. *IEEE Access*, 6:70983–70988, 2018.

[121] Wang Lina, Li Huai, and Zhao Lei. Ajax web automatic testing model based on simulation of users. *Journal of Huazhong University of Science and Technology (Natural Science Edition)*,

(3):1, 2016.

[122] Joseph V DeMarco. An approach to minimizing legal and reputational risk in red team hacking exercises. *Computer Law & Security Review*, 34(4):908–911, 2018.

[123] Yusep Rosmansyah, Mora Ritonga, and Ariq Hardi. An attack-defense tree on e-exam system. *International Journal of Emerging Technologies in Learning (iJET)*, 14(23):251–260, 2019.

[124] Zang Yichao, Zhou Tianyang, Ge Xiaoyue, and Wang Qingxian. An improved attack path discovery algorithm through compact graph planning. *IEEE Access*, 7:59346–59356, 2019.

[125] A Venkata Lakshmi. Analysis and protection of networks from crossfire attacks.

[126] R. Vignesh and K. Rohini. Analysis to determine the scope and challenging responsibilities of ethical hacking employed in cyber security. *International Journal of Engineering and Technology(UAE)*, 7(3.27 Special Issue 27):196–199, 2018. cited By 1.

[127] Fernando Román Muñoz, Esteban Alejandro Armas Vega, and Luis Javier García Villalba. Analyzing the traffic of penetration testing tools with an ids. *The Journal of Supercomputing*, 74(12):6454–6469, 2018.

[128] Shefali Sachdeva, Romuald Jolivot, and Worawat Choensawat. Android malware classification based on mobile security framework. *IAENG International Journal of Computer Science*, 45(4):514–522, 2018.

[129] Boris Svilicic, Junzo Kamahara, Jasmin Celic, and Johan Bolmsten. Assessing ship cyber risks: a framework and case study of ecdis security. *WMU Journal of Maritime Affairs*, 18(3):509–520, 2019.

[130] Martin Vondrek, Jan Pluskal, and O Ryavy. Automated man-in-the-middle attack against wi-fi networks. *The Journal of Digital Forensics, Security and Law: JDFSL*, 13(1):59–80, 2018.

[131] MALIK Qasaimeh, A Shamlawi, and TARIQ Khairallah. Black box evaluation of web application scanners: standards mapping approach. *Journal of Theoretical and Applied Information Technology*, 96(14):4584–4596, 2018.

[132] Young B Choi and Kenneth P LaCroix. Building a penetration testing device for black box using modified linux for under 50 usd. *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS*, 8(1):15–18, 2017.

[133] Madeline Cheah, Siraj A Shaikh, Jeremy Bryans, and Paul Wooderson. Building an automotive security assurance case using systematic security evaluations. *Computers & Security*, 77:360–379, 2018.

[134] Kai Simon, Cornelius Moucha, and Jörg Keller. Contactless vulnerability analysis using google and shodan. *J. UCS*, 23(4):404–430, 2017.

[135] Dan WANG, Mingchang GU, and Wenbing ZHAO. Cross-site script vulnerability penetration testing technology [j]. *Journal of Harbin Engineering University*, 38(11):1769–1774, 2017.

[136] Ben Rafferty. Dangerous skills gap leaves organisations vulnerable. *Network Security*, 2016(8):11–13, 2016.

[137] Nuno Antunes and Marco Vieira. Designing vulnerability testing tools for web services: approach, components, and tools. *International Journal of Information Security*, 16(4):435–457, 2017.

[138] Aidan F Browne, Stacey Watson, and Wesley B Williams. Development of an architecture for a cyber-physical emulation test range for network security testing. *IEEE Access*, 6:73273–73279, 2018.

[139] Wiman Kang, Gyoocheol Lee, Sangphil Kim, and Jong-Bae Kim. Diagnostic model of vulnerability based on penetration testing. *International Information Institute (Tokyo). Information*,

19(6B):2257, 2016.

[140] Izzat Alsmadi and Emad Abu-Shanab. E-government website security concerns and citizens' adoption. *Electronic Government, an International Journal*, 12(3):243–255, 2016.

[141] Alex Zhu and Wei Qi Yan. Exploring defense of sql injection attack in penetration testing. *International Journal of Digital Crime and Forensics (IJDCF)*, 9(4):62–71, 2017.

[142] Steve Mansfield-Devine. Friendly fire: how penetration testing can reduce your risk. *Network Security*, 2018(6):16–19, 2018.

[143] Marcel Steinmetz, Jörg Hoffmann, and Olivier Buffet. Goal probability analysis in probabilistic planning: Exploring and enhancing the state of the art. *Journal of Artificial Intelligence Research*, 57:229–271, 2016.

[144] Kevin Kusnardi and Dennis Gunawan. Guillou-quisquater protocol for user authentication based on zero knowledge proof. *Telkomnika*, 17(2), 2019.

[145] Steve Mansfield-Devine. Hiring ethical hackers: the search for the right kinds of skills. *Computer Fraud & Security*, 2017(2):15–20, 2017.

[146] Sameer Dixit. Holding the fort: a business case for testing security. *Network Security*, 2016(6):16–18, 2016.

[147] Dorottya Papp, Kristóf Tamás, and Levente Buttyán. Iot hacking–a primer. *Infocommunications Journal*, 11(2):2–13, 2019.

[148] J Smile Manuel, V Anatha Narayanan, and M Sethumadhavan. Lopt: Lora penetration testing tool. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 8.

[149] Michele Peroli, Federico De Meo, Luca Viganò, and Davide Guardini. Mobster: A model-based security testing framework for web applications. *Software Testing, Verification and Reliability*, 28(8):e1685, 2018.

[150] D. Bhatt. Modern day penetration testing distribution open source platform-kali linux-study paper. *International Journal of Scientific and Technology Research*, 7:233–237, 04 2018.

[151] Mihai Carabas, Costin Carabas, Laura Gheorghe, Razvan Deaconescu, and Nicolae Tapus. Monitoring and auditing mobile operating systems. *International Journal of Space-Based and Situated Computing*, 6(1):54–63, 2016.

[152] Tian-yang Zhou, Yi-chao Zang, Jun-hu Zhu, and Qing-xian Wang. Nig-ap: a new method for automated penetration testing. *Frontiers of Information Technology & Electronic Engineering*, 20(9):1277–1288, 2019.

[153] Daniel Dalalana Bertoglio and Avelino Francisco Zorzo. Overview and open issues on penetration test. *Journal of the Brazilian Computer Society*, 23(1):2, 2017.

[154] Irfan Ahmed and Vassil Roussev. Peer instruction teaching methodology for cybersecurity education. *IEEE Security & Privacy*, 16(4):88–91, 2018.

[155] Y Zh Aitkhozhayeva, AA Ziro, Zh A Zhaibergenova, and AG Baltabay. Penetration testing. *BULLETIN OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN*, (6):39–44, 2018.

[156] Deris Stiawan, Yazid Idris, Hanan Abdullah, Maha Alqurashi, and Rahmat Budiarto. Penetration testing and mitigation of vulnerabilities windows server. 18:501–513, 01 2016.

[157] Chung-Kuan Chen, Zhi-Kai Zhang, Shan-Hsin Lee, and Shiuhpyng Shieh. Penetration testing in the iot age. *Computer*, 51(4):82–85, 2018.

[158] Teddy Surya Gunawan, Muhammad Kasim Lim, Mira Kartiwi, Noreha Abdul Malik, and Nanang Ismail. Penetration testing using kali linux: Sql injection, xss, wordpres, and wpa2 attacks. *Indonesian Journal of Electrical Engineering and Computer Science*, 12(2):729–737,

2018.

[159] V. Sahiti, P. Tilakchand, B. Kowshik, P. Avinash, and S.L. Kavya. Penetration testing using wireshark and defensive mechanisms against mitm. *International Journal of Recent Technology and Engineering*, 7(6):880–885, 2019. cited By 0.

[160] CV Arjun. Penetration testing: Vulnerability analysis in a virtual environment. *Journal of Engineering and Applied Sciences*, 12(Specialissue9):8723–8729, 2017.

[161] Nick Thompson. Putting security at the heart of app development. *Network Security*, 2017(11):7–8, 2017.

[162] Jacqueline M Archibald and Karen Renaud. Refining the pointer "human firewall" pentesting framework. *Information & Computer Security*, 2019.

[163] Mohamed C Ghanem and Thomas M Chen. Reinforcement learning for efficient network penetration testing. *Information*, 11(1):6, 2020.

[164] Md Maruf Hassan, Touhid Bhuyian, M Khaled Sohel, Md Hasan Sharif, and Saikat Biswas. Saisan: an automated local file inclusion vulnerability detection model. *International Journal of Engineering & Technology*, 7(2-3):4, 2018.

[165] P.V. Raju, K.V.S.N. Rama Rao, and G.S. Prasad. Securing android applications from known vulnerabilities through penetration testing. *International Journal of Engineering and Advanced Technology*, 8(4):1936–1939, 2019. cited By 0.

[166] Hafsa Ashraf, Mamdouh Alenezi, Muhammad Nadeem, and Yasir Javid. Security assessment framework for educational erp systems. *International Journal of Electrical and Computer Engineering (IJECE)*, 9(6):5570–5585, 2019.

[167] Kanya Varathan. Security support for iot device using pentration testing tools. *Journal of Advanced Research in Dynamical and Control Systems*, 11:2321–2326, 04 2019.

[168] Massimo Ficco, Michał Choraś, and Rafał Kozik. Simulation platform for cyber-security and vulnerability analysis of critical infrastructures. *Journal of computational science*, 22:179–186, 2017.

[169] Stephan Kleber, Lisa Maile, and Frank Kargl. Survey of protocol reverse engineering algorithms: Decomposition of tools for static traffic analysis. *IEEE Communications Surveys & Tutorials*, 21(1):526–561, 2018.

[170] Joshua Eckroth. Teaching cybersecurity and python programming in a 5-day summer camp. *Journal of Computing Sciences in Colleges*, 33(6):29–39, 2018.

[171] Irfan A Siddavatam, Sachin Parekh, Tanay Shah, and Faruk Kazi. Testing and validation of modbus/tcp protocol for secure scada communication in cps using formal methods. *Scalable Computing: Practice and Experience*, 18(4):313–330, 2017.

[172] Steve Mansfield-Devine. The best form of defence–the benefits of red teaming. *Computer Fraud & Security*, 2018(10):8–12, 2018.

[173] William Knowles, Alistair Baron, and Tim McGarr. The simulated security assessment ecosystem: Does penetration testing need standardisation? *Computers & Security*, 62:296–316, 2016.

[174] Ihab Darwish, Obinna Igbe, and Tarek Saadawi. Vulnerability assessment and experimentation of smart grid dnp3. *Journal of Cyber Security and Mobility*, 5(1):23–54, 2016.

[175] Gitanjali S. and Sasikala D. Vulnerability assessment of web applications using penetration testing. *International Journal of Recent Technology and Engineering (IJRTE)*, 2019.

[176] Mohd Zamri Murah and Abdullah Ahmed Ali. Web assessment of libyan government e-government services. *assessment*, 9(12), 2018.

[177] Angelo Ciampa, Corrado Aaron Visaggio, and Massimiliano Di Penta. A heuristic-based

approach for detecting sql-injection vulnerabilities in web applications. In *Proceedings of the 2010 ICSE Workshop on Software Engineering for Secure Systems*, pages 43–49, 2010.

[178] Paul Ammann, Joseph Pamula, Ronald Ritchey, and Julie Street. A host-based approach to network attack chaining analysis. In *21st Annual Computer Security Applications Conference (ACSAC'05)*, pages 10–pp. IEEE, 2005.

[179] Dejan Baca, Martin Boldt, Bengt Carlsson, and Andreas Jacobsson. A novel security-enhanced agile software development process applied in an industrial setting. In *2015 10th International Conference on Availability, Reliability and Security*, pages 11–19. IEEE, 2015.

[180] B Hebbard, P Grosso, T Baldridge, C Chan, D Fishman, P Goshgarian, T Hilton, J Hoshen, K Hoult, G Huntley, et al. A penetration analysis of the michigan terminal system. *ACM SIGOPS Operating Systems Review*, 14(1):7–20, 1980.

[181] Carlos Sarraute, Gerardo Richarte, and Jorge Lucángeli Obes. An algorithm to find optimal attack paths in nondeterministic scenarios. In *Proceedings of the 4th ACM workshop on Security and artificial intelligence*, pages 71–80, 2011.

[182] Dianxiang Xu, Weifeng Xu, Michael Kent, Lijo Thomas, and Linzhang Wang. An automated test generation technique for software quality assurance. *IEEE Transactions on Reliability*, 64(1):247–268, 2014.

[183] Johannes Obermaier and Martin Hutle. Analyzing the security and privacy of cloud-based video surveillance systems. In *Proceedings of the 2nd ACM international workshop on IoT privacy, trust, and security*, pages 22–28, 2016.

[184] Herbert H Thompson. Application penetration testing. *IEEE Security & Privacy*, 3(1):66–69, 2005.

[185] Nuno Antunes and Marco Vieira. Assessing and comparing vulnerability detection tools for web services: Benchmarking approach and examples. *IEEE Transactions on Services Computing*, 8(2):269–283, 2014.

[186] Humberto Abdelnur, R State, Isabelle Chrisment, and C Popi. Assessing the security of voip services. In *2007 10th IFIP/IEEE International Symposium on Integrated Network Management*, pages 373–382. IEEE, 2007.

[187] James P McDermott. Attack net penetration testing. In *Proceedings of the 2000 workshop on New security paradigms*, pages 15–21, 2001.

[188] Scott Wolchok, Eric Wustrow, Dawn Isabel, and J Alex Halderman. Attacking the washington, dc internet voting system. In *International Conference on Financial Cryptography and Data Security*, pages 114–128. Springer, 2012.

[189] Serge Gorbunov and Arnold Rosenbloom. Autofuzz: Automated network protocol fuzzing framework. *IJCSNS*, 10(8):239, 2010.

[190] Nuno Antunes and Marco Vieira. Benchmarking vulnerability detection tools for web services. In *2010 IEEE International Conference on Web Services*, pages 203–210. IEEE, 2010.

[191] Mary Micco and Hart Rossman. Building a cyberwar lab: lessons learned: teaching cybersecurity principles to undergraduates. In *Proceedings of the 33rd SIGCSE technical symposium on Computer science education*, pages 23–27, 2002.

[192] Ben Smith, Andrew Austin, Matt Brown, Jason T King, Jerrod Lankford, Andrew Meneely, and Laurie Williams. Challenges for protecting the privacy of health information: required certification can leave common vulnerabilities undetected. In *Proceedings of the second annual workshop on Security and privacy in medical and home-care systems*, pages 1–12, 2010.

[193] Victor Chang, Yen-Hung Kuo, and Muthu Ramachandran. Cloud computing adoption framework: A security framework for business clouds. *Future Generation Computer Systems*, 57:24–

41, 2016.

[194] Nuno Antunes and Marco Vieira. Comparing the effectiveness of penetration testing and static code analysis on the detection of sql injection vulnerabilities in web services. In *2009 15th IEEE Pacific Rim International Symposium on Dependable Computing*, pages 301–306. IEEE, 2009.

[195] Prabhakaran Kasinathan, Gianfranco Costamagna, Hussein Khaleel, Claudio Pastrone, and Maurizio A Spirito. An ids framework for internet of things empowered by 6lowpan. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 1337–1340, 2013.

[196] Prabhakaran Kasinathan, Claudio Pastrone, Maurizio A Spirito, and Mark Vinkovits. Denial-of-service detection in 6lowpan based internet of things. In *2013 IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob)*, pages 600–607. IEEE, 2013.

[197] David Byers and Nahid Shahmehri. Design of a process for software security. In *The Second International Conference on Availability, Reliability and Security (ARES'07)*, pages 301–309. IEEE, 2007.

[198] Hossein Siadati, Bahador Saket, and Nasir Memon. Detecting malicious logins in enterprise networks using visualization. In *2016 IEEE Symposium on Visualization for Cyber Security (VizSec)*, pages 1–8. IEEE, 2016.

[199] Marcel Böhme, Van-Thuan Pham, Manh-Dung Nguyen, and Abhik Roychoudhury. Directed greybox fuzzing. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 2329–2344, 2017.

[200] Weidong Cui, Jayanthkumar Kannan, and Helen J Wang. Discoverer: Automatic protocol reverse engineering from network traces. In *USENIX Security Symposium*, pages 1–14, 2007.

[201] Stephen McLaughlin, Dmitry Podkuiko, and Patrick McDaniel. Energy theft in the advanced metering infrastructure. In *International Workshop on Critical Information Infrastructures Security*, pages 176–187. Springer, 2009.

[202] Nuno Antunes and Marco Vieira. Enhancing penetration testing with attack signatures and interface monitoring for the detection of injection vulnerabilities in web services. In *2011 IEEE International Conference on Services Computing*, pages 104–111. IEEE, 2011.

[203] Aleksandar Milenkoski, Marco Vieira, Samuel Kounev, Alberto Avritzer, and Bryan D Payne. Evaluating computer intrusion detection systems: A survey of common practices. *ACM Computing Surveys (CSUR)*, 48(1):1–41, 2015.

[204] Diana Senn, David Basin, and Germano Caronni. Firewall conformance testing. In *IFIP International Conference on Testing of Communicating Systems*, pages 226–241. Springer, 2005.

[205] William GJ Halfond, Shauvik Roy Choudhary, and Alessandro Orso. Improving penetration testing through static and dynamic analysis. *Software Testing, Verification and Reliability*, 21(3):195–214, 2011.

[206] Farid Daryabar, Ali Dehghantanha, and Nur Izura Udzir. Investigation of bypassing malware defences and malware detections. In *2011 7th International Conference on Information Assurance and Security (IAS)*, pages 173–178. IEEE, 2011.

[207] Martin Mink and Felix C Freiling. Is attack better than defense? teaching information security the right way. In *Proceedings of the 3rd annual conference on Information security curriculum development*, pages 44–48, 2006.

[208] Martin R Albrecht and Kenneth G Paterson. Lucky microseconds: A timing attack on

amazon's s2n implementation of tls. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 622–643. Springer, 2016.

[209] Ole Martin Dahl and Stephen D Wolthusen. Modeling and execution of complex attack scenarios using interval timed colored petri nets. In *Fourth IEEE International Workshop on Information Assurance (IWIA'06)*, pages 12–pp. IEEE, 2006.

[210] Stephen McLaughlin, Dmitry Podkuiko, Sergei Miadzvezhanka, Adam Delozier, and Patrick McDaniel. Multi-vendor penetration testing in the advanced metering infrastructure. In *Proceedings of the 26th Annual Computer Security Applications Conference*, pages 107–116, 2010.

[211] Juraj Somorovsky, Andreas Mayer, Jörg Schwenk, Marco Kampmann, and Meiko Jensen. On breaking {SAML}: Be whoever you want to be. In *Presented as part of the 21st {USENIX} Security Symposium ({USENIX} Security 12)*, pages 397–412, 2012.

[212] Bernhard Garn, Ioannis Kapsalis, Dimitris E Simos, and Severin Winkler. On the applicability of combinatorial testing to web application security testing: a case study. In *Proceedings of the 2014 Workshop on Joining AcadeMiA and Industry Contributions to Test Automation and Model-Based Testing*, pages 16–21, 2014.

[213] Andrew Austin and Laurie Williams. One technique is not enough: A comparison of vulnerability discovery techniques. In *2011 International Symposium on Empirical Software Engineering and Measurement*, pages 97–106. IEEE, 2011.

[214] Yufei Gu, Yangchun Fu, Aravind Prakash, Zhiqiang Lin, and Heng Yin. Os-sommelier: Memory-only operating system fingerprinting in the cloud. In *Proceedings of the Third ACM Symposium on Cloud Computing*, pages 1–13, 2012.

[215] William GJ Halfond, Shauvik Roy Choudhary, and Alessandro Orso. Penetration testing with improved input vector identification. In *2009 International Conference on Software Testing Verification and Validation*, pages 346–355. IEEE, 2009.

[216] Matthew Denis, Carlos Zena, and Thaier Hayajneh. Penetration testing: Concepts, attack methods, and defense strategies. In *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, pages 1–6. IEEE, 2016.

[217] William GJ Halfond, Saswat Anand, and Alessandro Orso. Precise interface identification to improve testing and analysis of web applications. In *Proceedings of the eighteenth international symposium on Software testing and analysis*, pages 285–296, 2009.

[218] Josip Bozic and Franz Wotawa. Purity: a planning-based security testing tool. In *2015 IEEE International Conference on Software Quality, Reliability and Security-Companion*, pages 46–55. IEEE, 2015.

[219] Michael Hooper, Yifan Tian, Runxuan Zhou, Bin Cao, Adrian P Lauf, Lanier Watkins, William H Robinson, and Wlajimir Alexis. Securing commercial wifi-based uavs from common security attacks. In *MILCOM 2016-2016 IEEE Military Communications Conference*, pages 1213–1218. IEEE, 2016.

[220] Junia Valente and Alvaro A Cardenas. Security & privacy in smart toys. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, pages 19–24, 2017.

[221] Marcelo Invert Palma Salas and Eliane Martins. Security testing methodology for vulnerabilities detection of xss in web services and ws-security. *Electronic Notes in Theoretical Computer Science*, 302:133–154, 2014.

[222] Michael Felderer, Matthias Büchler, Martin Johns, Achim D Brucker, Ruth Breu, and Alexander Pretschner. Security testing: A survey. In *Advances in Computers*, volume 101, pages 1–51. Elsevier, 2016.

[223] Ebenezer A Oladimeji, Sam Supakkul, and Lawrence Chung. Security threat modeling and analysis: A goal-oriented approach. In *Proc. of the 10th IASTED International Conference on Software Engineering and Applications (SEA 2006)*, pages 13–15. Citeseer, 2006.

[224] Matthias Büchler, Johan Oudinet, and Alexander Pretschner. Semi-automatic security testing of web applications from a secure model. In *2012 IEEE Sixth International Conference on Software Security and Reliability*, pages 253–262. IEEE, 2012.

[225] Shivam Bhasin, Jean-Luc Danger, Sylvain Guilley, and Zakaria Najm. Side-channel leakage and trace compression using normalized inter-class variance. In *Proceedings of the Third Workshop on Hardware and Architectural Support for Security and Privacy*, pages 1–9, 2014.

[226] Mariano Ceccato, Cu D Nguyen, Dennis Appelt, and Lionel C Briand. Sofia: An automated security oracle for black-box testing of sql-injection vulnerabilities. In *2016 31st IEEE/ACM International Conference on Automated Software Engineering (ASE)*, pages 167–177. IEEE, 2016.

[227] Bingchang Liu, Liang Shi, Zhuhua Cai, and Min Li. Software vulnerability discovery techniques: A survey. In *2012 fourth international conference on multimedia information networking and security*, pages 152–156. IEEE, 2012.

[228] Vincent Urias, Brian Van Leeuwen, and Bryan Richardson. Supervisory command and data acquisition (scada) system cyber security analysis using a live, virtual, and constructive (lvc) testbed. In *MILCOM 2012-2012 IEEE Military Communications Conference*, pages 1–8. IEEE, 2012.

[229] Juraj Somorovsky. Systematic fuzzing and testing of tls libraries. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1492–1504, 2016.

[230] Shanai Ardi, David Byers, and Nahid Shahmehri. Towards a structured unified process for software security. In *Proceedings of the 2006 international workshop on Software engineering for secure systems*, pages 3–10, 2006.

[231] Victor Chang and Muthu Ramachandran. Towards achieving data security with the cloud computing adoption framework. *IEEE Transactions on services computing*, 9(1):138–151, 2015.

[232] Vidar Kongsli. Towards agile security in web applications. In *Companion to the 21st ACM SIGPLAN symposium on Object-oriented programming systems, languages, and applications*, pages 805–808, 2006.

[233] Andrew Austin, Ben Smith, and Laurie Williams. Towards improved security criteria for certification of electronic health record systems. In *Proceedings of the 2010 ICSE Workshop on Software Engineering in Health Care*, pages 68–73, 2010.

[234] Trajce Dimkov, André Van Cleeff, Wolter Pieters, and Pieter Hartel. Two methodologies for physical penetration testing using social engineering. In *Proceedings of the 26th annual computer security applications conference*, pages 399–408, 2010.

[235] Junia Valente and Alvaro A Cardenas. Understanding security threats in consumer drones through the lens of the discovery quadcopter family. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, pages 31–36, 2017.

[236] Zouheir Trabelsi and Latifa Alketbi. Using network packet generators and snort rules for teaching denial of service attacks. In *Proceedings of the 18th ACM conference on Innovation and technology in computer science education*, pages 285–290, 2013.

[237] Hsiu-Chuan Huang, Zhi-Kai Zhang, Hao-Wen Cheng, and Shiuhpyng Winston Shieh. Web application security: Threats, countermeasures, and pitfalls. *Computer*, 50(6):81–85, 2017.