# REFERENCES

Aguirre-Anaya, E., Gallegos-Garcia, G., Luna, N. S., and Vargas, L. A. V., "A new procedure to detect low interaction honeypots," *International Journal of Electrical and Computer Engineering*, volume 4(6) p. 848, 2014.

Arkin, O., "ICMP usage in scanning," *Black Hat Briefings*, 2000.

Bana, S. and Kaur, D. D., "Fingerprint recognition using image segmentation," *International Journal of Advanced Engineering Sciences and Technologies*, volume 5(0) p. 1, 2011.

Bao, J., Ji, C.-p., and Gao, M., "Research on network security of defense based on Honeypot," in "Computer Application and System Modeling (ICCASM), 2010 International Conference on," volume 10, pp. V10–299, IEEE, 2010.

Barnes, J. and Crowley, P., "k-p0f: a high-throughput kernel passive os fingerprinter," in "Architectures for Networking and Communications Systems (ANCS), 2013 ACM/IEEE Symposium on," pp. 113–114, IEEE, 2013.

Bennett, M. and Waltz, E., *Counterdeception principles and applications for national security*, Artech House Norwood, MA, 2007.

Bodmer, S., Kilger, M., Carpenter, G., and Jones, J., *Reverse Deception: Organized Cyber Threat Counter-Exploitation*, McGraw Hill Professional, 2012.

Catakoglu, O., Balduzzi, M., and Balzarotti, D., "Automatic Extraction of Indicators of Compromise for Web Applications," in "Proceedings of the 25th International Conference on World Wide Web," pp. 333–343, International World Wide Web Conferences Steering Committee, 2016.

Chang, J.-S., Jeon, Y.-H., Sim, S., and Kang, A. N., "Information Security Modeling for the Operation of a Novel Highly Trusted Network in a Virtualization Environment," *International Journal of Distributed Sensor Networks*, volume 2015, 2015.

Chen, Y.-C., Liao, Y., Baldi, M., Lee, S.-J., and Qiu, L., "OS Fingerprinting and Tethering Detection in Mobile Networks," in "Proceedings of the 2014 Conference on Internet Measurement Conference," pp. 173–180, ACM, 2014.

Chowdhury, N. and Boutaba, R., "Network virtualization: state of the art and research challenges," *Communications Magazine, IEEE*, volume 47(7) pp. 20–26, 2009.

Doubleday, H., Maglaras, L., and Janicke, H., "SSH Honeypot: Building, Deploying and Analysis," , 2016.

Fossi, M., Egan, G., Haley, K., Johnson, E., Mack, T., Adams, T., Blackbird, J., Low, M. K., Mazurek, D., McKinney, D. et al., "Symantec internet security threat report trends for 2010," *Volume*, volume 16 p. 20, 2011.

Ghosh, A. K., "E-Commerce security: No Silver Bullet," in "Database Security XII," pp. 3–16, Springer, 1999.

Gorzelak, K., Grudziecki, T., Jacewicz, P., Jaroszewski, P., Juszczyk, Ł., and Kijewski, P., "Proactive Detection of Security Incidents II - Honeypots," Technical report, Tech. Rep., ENISA, 2012.

Heckman, K. E., Stech, F. J., Schmoker, B., Tsow, A. W., and Thomas, R. K., *Cyber Denial, Deception and Counter Deception*, Springer, 2015.

Holz, T. and Raynal, F., "Detecting honeypots and other suspicious environments," in "Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC," pp. 29–36, IEEE, 2005.

Innes, S. and Valli, C., "Honeypots: How do you know when you are inside one?" in "Australian Digital Forensics Conference," p. 28, 2006.

Kao, C.-N., Chang, Y.-C., Huang, N.-F., Salim, S., Liao, I.-J., Liu, R.-T., Hung, H.-W. et al., "A predictive zero-day network defense using long-term port-scan recording," in "Communications and Network Security (CNS), 2015 IEEE Conference on," pp. 695–696, IEEE, 2015.

Kohno, T., Broido, A., and Claffy, K. C., "Remote physical device fingerprinting," *Dependable and Secure Computing, IEEE Transactions on*, volume 2(2) pp. 93–108, 2005.

Kothari, C. R., *Research methodology: Methods and techniques*, New Age International, 2004.

Kott, A., Wang, C., and Erbacher, R. F., *Cyber Defense and Situational Awareness*, Springer, 2014.

Krawetz, N., "Anti-honeypot technology," *Security & Privacy, IEEE*, volume 2(1) pp. 76–79, 2004.

Lee, D., Rowe, J., Ko, C., and Levitt, K., "Detecting and defending against Web-server fingerprinting," in "Computer Security Applications Conference, 2002. Proceedings. 18th Annual," pp. 321–330, IEEE, 2002.

Mijumbi, R., Serrat, J., Gorricho, J.-L., Bouten, N., De Turck, F., and Boutaba, R., "Network function virtualization: State-of-the-art and research challenges," , 2015.

Mukkamala, S., Yendrapalli, K., Basnet, R., Shankarapani, M., and Sung, A., "Detection of virtual environments and low interaction honeypots," in "Information Assurance and Security Workshop, 2007. IAW'07. IEEE SMC," pp. 92–98, IEEE, 2007.

Nemade, S., Darekar, M. M. A., and Bachhav, M. J., "Honeypot security system: An efficient approach of securing E-Banking network," *International Research Journal of Multidisciplinary Studies*, volume 1(5), 2015.

Oosterhof, M., "Kippo Github pull," , 2015, URL `https://github.com/desaster/kippo/pull/148/commits/19241a374dec3e8d198e7d679ed4e5c6cefe1e2c`.

Panchenko, A., Niessen, L., Zinnen, A., and Engel, T., "Website fingerprinting in onion routing based anonymization networks," in "Proceedings of the 10th annual ACM workshop on Privacy in the electronic society," pp. 103–114, ACM, 2011.

Piller, K. and Wolfgarten, S., "Honeypot forensics," *Ernst&Young Risk Advisory Services ppt. Retrieved on November*, volume 16 p. 2005, 2004.

Rowe, N. C., "Deception in Defense of Computer Systems from Cyber Attack," *Cyber Warfare and Cyber Terrorism*, pp. 97–104, 2008.

Rowe, N. C., Duong, B. T., and Custy, E. J., "Fake honeypots: a defensive tactic for cyberspace," in "Information Assurance Workshop, 2006 IEEE," pp. 223–230, IEEE, 2006.

Schmerl, B., Gennari, J., Sadeghi, A., Bagheri, H., Malek, S., Cámara, J., and Garlan, D., "Architecture Modeling and Analysis of Security in Android Systems," , 2016.

Shamsi, Z., Nandwani, A., Leonard, D., and Loguinov, D., "Hershel: single-packet OS fingerprinting," in "ACM SIGMETRICS Performance Evaluation Review," volume 42, pp. 195–206, ACM, 2014.

Shostack, A., *Threat modeling: Designing for security*, John Wiley & Sons, 2014.

Sochor, T. and Zuzcak, M., "Attractiveness Study of Honeypots and Honeynets in Internet Threat Detection," in "Computer Networks," pp. 69–81, Springer, 2015.

Sokol, P., Kleinova, L., and Husak, M., "Study of attack using honeypots and honeynets lessons learned from time-oriented visualization," in "EUROCON 2015-International Conference on Computer as a Tool (EUROCON), IEEE," pp. 1–6, IEEE, 2015.

Spitzner, L., *Honeypots: tracking hackers*, volume 1, Addison-Wesley Reading, 2003.

Stech, F. J. and Elsässer, C., "Midway revisited: detecting deception by analysis of competing hypothesis," Technical report, DTIC Document, 2004.

Thompson, D. R., Di, J., and Daugherty, M. K., "Teaching RFID information systems security," *Education, IEEE Transactions on*, volume 57(1) pp. 42–47, 2014.

Tzu, S., *The art of war*, Shambhala Publications, 2011.

Zadeh, H., Mansoori, M., and Welch, I., "Evaluation of fingerprinting techniques and a windows-based dynamic honeypot," in "Proceedings of the Eleventh Australasian Information Security Conference-Volume 138," pp. 59–66, Australian Computer Society, Inc., 2013.

Zakaria, W. Z. A., Kiah, M. L. M., Siew, H., Pooi, A., Bashir, U., Abbas, M., Awang, M. N. H., Ali, J. M., Zainal, R., and Ali, N. M. M., "A review of dynamic and intelligent honeypots," *ScienceAsia*, volume 39(2) pp. 1–5, 2013.

Zheng, X., Jiang, J., Liang, J., Duan, H., Chen, S., Wan, T., and Weaver, N., "Cookies lack integrity: real-world implications," in "24th USENIX Security Symposium (USENIX Security 15)," pp. 707–721, 2015.