

DAFTAR PUSTAKA

- [1] I. Lunden, "Gartner: Device Shipments Break 2.4B Units In 2014, Tablets To Overtake PC Sales In 2015," 2014. [Online]. Available: <http://techcrunch.com/2014/07/06/gartner-device-shipments-break-2-4b-units-in-2014-tablets-to-overtake-pc-sales-in-2015/>.
- [2] G. R. and A. T. (GREAT), "Kaspersky Security Bulletin 2014," p. 94551, 2014.
- [3] C. C. Ho and C.-Y. Ting, "A conceptual framework for smart mobile honeypots," 2012.
- [4] E. Al Awadhi, K. Salah, and T. Martin, "Assessing the security of the cloud environment," *2013 7th IEEE GCC Conf. Exhib.*, pp. 251–256, 2013.
- [5] J. Ma, K. Chai, Y. Xiao, T. Lan, and W. Huang, "High-interaction honeypot system for SQL injection analysis," *Proc. - 2011 Int. Conf. Inf. Technol. Comput. Eng. Manag. Sci. ICM 2011*, vol. 3, pp. 274–277, 2011.
- [6] L. Li, H. Sun, and Z. Zhang, "The research and design of honeypot system applied in the LAN security," *ICSESS 2011 - Proc. 2011 IEEE 2nd Int. Conf. Softw. Eng. Serv. Sci.*, pp. 360–363, 2011.
- [7] E. Uzun, "An Automated Bot Detection System through Honeypots for Large-Scale," pp. 255–270, 2014.
- [8] Z. Zhan, M. Xu, and S. Xu, "Characterizing Honeypot-Captured Cyber Attacks: Statistical Framework and Case Study," vol. 8, no. 11, pp. 1775–1789, 2013.
- [9] R. Koch, M. Golling, and G. Dreo, "Attracting sophisticated attacks to secure systems: A new honeypot architecture," *2013 IEEE Conf. Commun. Netw. Secur. CNS 2013*, pp. 409–410, 2013.
- [10] E. Alata, V. Nicomette, M. Kaâniche, M. Dacier, and M. Herrb, "Lessons learned from the deployment of a high-interaction honeypot," *Proc. - Sixth Eur. Dependable Comput. Conf. EDCC 2006*, vol. 22, pp. 39–44, 2006.
- [11] R. Zhang, W. Yao, and Z. Jia, "Research on cooperative anti-worm system model based on distributed honeypots," *Int. Conf. Internet Technol. Appl. ITAP 2010 - Proc.*, no. 97025001200701, 2010.
- [12] M. Freeman and A. Woodward, "SmartPot - Creating a 1 st Generation Smartphone Honeypot," *Aust. Digit. FORENSICS Conf.*, pp. 24–31, 2007.
- [13] E. Vasilomanolakis, S. Karuppayah, M. Fischer, M. Mühlhäuser, M. Plasoianu, L. Pandikow, and W. Pfeiffer, "This Network is Infected: HosTaGe - a Low-interaction Honeypot for Mobile Devices," in *Proceedings of the Third ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*, 2013, pp. 43–48.
- [14] E. Vasilomanolakis, S. Karuppayah, M. Mühlhäuser, and M. Fischer, "HosTaGe : a Mobile Honeypot for Collaborative Defense," pp. 1–4, 2014.
- [15] B. Krishnamurthy, "Mohonk: mobile honeypots to trace unwanted traffic early," *Proc. ACM SIGCOMM Work. Netw. Troubl. Res. theory Oper. Pract. meet malfunctioning Real.*, pp. 277–282, 2004.
- [16] C. Mulliner, S. Liebergeld, and M. Lange, "Poster : HoneyDroid - Creating a Smartphone Honeypot," *IEEE Symp. Secur. Priv.*, 2011.

- [17] M. Wählisch, S. Trapp, C. Keil, J. Schönfelder, T. C. Schmidt, and J. Schiller, "First insights from a mobile honeypot," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 42, p. 305, 2012.
- [18] M. Wählisch, A. Vorbach, C. Keil, J. Schönfelder, T. C. Schmidt, and J. H. Schiller, "Design, implementation, and operation of a mobile honeypot," *CoRR*, 2013.
- [19] S. Liebergeld, M. Lange, and C. Mulliner, "Nomadic HoneyPots : A Novel Concept for Smartphone HoneyPots," *Work. Mob. Secur. Technol. (MoST'13), conjunction with 34th IEEE Symp. Secur. Privacy.*, 2013.
- [20] E. Gelenbe, G. Gorbil, D. Tzovaras, S. Liebergeld, D. Garcia, M. Baltatu, and G. Lyberopoulos, "Security for smart mobile networks: The NEMESYS approach," *2013 IEEE Glob. High Tech Congr. Electron. GHTCE 2013*, pp. 63–69, 2013.
- [21] P. Niels, "Developments of the Honeyd Virtual HoneyPot." [Online]. Available: <http://www.honeyd.org/background.php>.
- [22] S. O. Hunter, E. Stalmans, B. Irwin, and J. Richter, "Remote fingerprinting and multisensor data fusion," *2012 Inf. Secur. South Africa - Proc. ISSA 2012 Conf.*, pp. 1–8, 2012.
- [23] D. Hoffstadt, N. Wolff, S. Monhof, and E. Rathgeb, "Improved detection and correlation of multi-stage VoIP attack patterns by using a Dynamic HoneyNet System," *IEEE Int. Conf. Commun.*, pp. 1968–1973, 2013.
- [24] I. Gashi, B. Sobesto, S. Mason, V. Stankovic, and M. Cukier, "A study of the relationship between antivirus regressions and label changes," *2013 IEEE 24th Int. Symp. Softw. Reliab. Eng. ISSRE 2013*, pp. 441–450, 2013.
- [25] K. G. A. and E. P. M. Polychronakis. N., "Comprehensive Shellcode Detection Using Runtime Heuristics," in *26th Annual Computer Security Applications Conference*, 2010, pp. 287–297.
- [26] S. C. Sawyer and B. Williams, *Using Information Technology, Intro*, 4th ed. McGraw-Hill Higher Education, 2000.
- [27] S'to, *Wireless Kungfu : Networking & Hacking*. Jasakom, 2007.
- [28] J. M. Sinambela, "Keamanan Wireless LAN (Wifi)," no. April, 2007.
- [29] O. H. Alliance, "Android Overview." [Online]. Available: http://www.openhandsetalliance.com/android_overview.html. [Accessed: 01-Jun-2015].
- [30] O. H. Alliance, "Industry Leaders Announce Open Platform for Mobile Devices." [Online]. Available: http://www.openhandsetalliance.com/press_110507.html. [Accessed: 01-Jun-2015].
- [31] Z. Islam, "Google Play Matches Apple's iOS With 700,000 Apps." [Online]. Available: <http://www.tomsguide.com/us/Google-Play-Android-Apple-iOS,news-16235.html>. [Accessed: 01-Jun-2015].
- [32] J. Rosenberg, "Google Play hits 25 billion downloads." [Online]. Available: <http://officialandroid.blogspot.ca/2012/09/google-play-hits-25-billion-downloads.html>. [Accessed: 01-Jun-2015].

- [33] “Developer Economics 2013 Q3.” [Online]. Available: <https://www.developereconomics.com/reports/developer-economics-2013-q3/>. [Accessed: 01-Jun-2015].
- [34] S. Lance, “The Value of HoneyPots, Part One: Definitions and Values of HoneyPots,” 2010. [Online]. Available: <http://www.symantec.com/connect/articles/value-honeypots-part-one-definitions-and-values-honeypots>.
- [35] K. Zuhdi, “KEJAHATAN MENGGUNAKAN INTERNET DI INDONESIA,” 2011. [Online]. Available: <http://blog.ub.ac.id/kurniawanzuhdi/2011/12/05/kejahatan-menggunakan-internet-di-indonesia/>. [Accessed: 10-Feb-2015].
- [36] W. Aprilia, “Modus Kejahatan Dalam Teknologi Informasi,” 2011. [Online]. Available: <http://apriawakhyuni.blogspot.com/2011/03/modus-modus-kejahatan-dalam-teknologi.html>.
- [37] “Backtrack-linux.org.”
- [38] “Backtrack 5 ARM mirror location.” [Online]. Available: <http://www.filewatcher.com/m/BT5-GNOME-ARM.7z.1142317778-0.html>.
- [39] “Debian ‘squeeze’ Release Information,” 2013. [Online]. Available: <https://www.debian.org/releases/squeeze/>. [Accessed: 11-May-2015].
- [40] “Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290).” [Online]. Available: <https://technet.microsoft.com/en-us/library/security/ms10-061.aspx>. [Accessed: 11-May-2015].