Progettazione e sviluppo di un sistema multi-livello di rilevamento delle intrusioni

Tesi di Laurea Magistrale in Ingegneria Informatica

D. Thevanantham

Relatore: Prof. Giuseppe Lo Re

Correlatore: Prof. Alessandra De Paola

Progettazione e sviluppo di un sistema multi-livello di rilevamento delle intrusioni

Tesi di Laurea di
Diluxon Thevanantham

Relatore:
Prof. Giuseppe Lo Re

Correlatore:
Prof.ssa Alessandra De Paola

Sommario

Nel presente elaborato viene presentato il lavoro di tesi svolto, intitolato "Progettazione e sviluppo di un sistema multi-livello di rilevamento delle intrusioni". L'obiettivo generale di questa tesi è quello di progettare e sviluppare un nuovo sistema per affrontare il problema del rilevamento delle intrusioni. Il rilevamento delle intrusioni è una tecnica usata per rilevare le attività malevole nel traffico internet con lo scopo di proteggere una rete informatica. Oggi, il rilevamento delle intrusioni è considerata un'attività di fondamentale importanza, dato il valore che hanno assunto le informazioni che transitano sulla rete internet.

In questa tesi è proposto un sistema a multi-livello che sfrutta le tecniche di apprendimento automatico per rilevare il traffico dei dati malevoli. Il sistema prevede anche un metodo di aggiornamento dei dati per tenere il sistema sempre aggiornato. All'interno dell'elaborato sono descritte e discusse dettagliatamente tutte le fasi di ricerca e sperimentazione che hanno portato a scegliere i componenti che compongono il sistema proposto, inoltre viene descritta la procedura usata per scegliere le caratteristiche più rappresentative del dataset utilizzato. Infine sono riportate le conclusioni e le proposte per uno sviluppo futuro per migliorare le prestazioni del sistema presentato.

Indice

1 Introduzione

La sicurezza informatica ricopre un ruolo cruciale nella realtà d'oggi. Tant'è vero che il dipartimento della difesa degli Stati Uniti ha definito la scienza della sicurezza, *Cyber Science*, come priorità alta per i suoi investimenti nel settore della scienza e tecnologia [2]. Con il termine "Sicurezza Informatica" si intende l'insieme delle tecnologie e processi progettati per proteggere i dati da attacchi informatici di vario tipo. Proteggere è inteso come la capacità di garantire l'integrità, la riservatezza e la disponibilità delle informazioni. Si sente sempre più spesso parlare di *cybercrime* e attacchi hacker [3] [4] [5]. Con l'aumentare delle informazioni, che transitano via internet, sono aumentate anche le intrusioni informatiche, una tipologia di crimine informatico, che hanno come obiettivo proprio queste informazioni. Infatti, secondo il Rapporto *Clusit* 2021 [1], nel 2020 gli attacchi informatici sono cresciuti del 12% a livello globale e se paragonati al 2017 la crescita è stata del 66%. Sono tante le violazioni, imputabili a criminali malintenzionati, che hanno colpito i servizi medici, i rivenditori ed gli enti pubblici. Tuttavia, tutte le aziende che operano in rete potrebbero essere vittime di violazioni dei dati o spionaggio aziendale.

1.1 Come proteggere i dati?

L'efficacia dei nuovi metodi degli attacchi e la complessità, sempre crescente, dei sistemi informatici da proteggere hanno reso meno efficaci le contromisure di sicurezza informatica utilizzate fino qualche tempo fa. Principalmente le misure adottate consistevano in firewall e apparecchiature che bloccavano i tentativi di accesso da esterno e applicazioni software come antivirus, installate sui singoli host. Questi strumenti sono ancora oggi necessari, ma non sono sufficienti per garantire una maggiore sicurezza informatica.

Uno strumento divenuto essenziale per la sicurezza informatica sono i sistemi di rilevazione delle intrusioni, in inglese *intrusion detection system* (IDS). Gli IDS sono usati per rilevare gli attacchi ai sistemi informatici, quindi il loro compito non è

bloccare o filtrare i vari attacchi, ma servono solo a rilevarli. Una rilevazione veloce può aiutare le aziende a evitare danni maggiori, reagendo in tempo ai vari attacchi.
Gli IDS sono spesso raggruppate in due categorie: sistemi basati sulle firme (*misuse*) e sistemi basati sulle anomalie (*anomaly*). I sistemi di rilevazione *misuse* sono sistemi che si basano sulla firma degli attacchi noti. In pratica, le attività di rete che hanno una firma o un comportamento noto come caratteristico di un attacco vengono considerate come tali e quelle attività che non corrispondono ai comportamenti o alle firme noti come attacchi vengono considerate come benigne. I sistemi di questa categoria spesso sono molto efficaci, ma non sono in grado di rilevare nuovi attacchi detti attacchi *zero day*. Il motivo, come si può intuire, è la mancanza delle firme note per quegli attacchi.
I sistemi basati sulla rilevazione delle anomalie utilizzano metodi statistici o apprendimento automatico per distinguere i comportamenti anomali e da quelli normali. Questi tipi di sistemi sono in grado di rilevare anche gli attacchi *zero day*. Però, spesso il tasso di allarme di falsi positivi è alto, in quanto anche i comportamenti normali, non osservati prima, vengono classificati come comportamenti anomali.

In questo lavoro di tesi, viene proposto un sistema di rilevazione delle intrusioni a multi-livelli che sfrutta le tecniche di apprendimento automatico. Il sistema usa sia l'apprendimento supervisionato che quello non supervisionato, in strati diversi, con lo scopo di distinguere, prima, gli attacchi dai comportamenti benigni e poi classificare l'eventuale attacco, individuando la famiglia di attacco di appartenenza. Così da permette agli amministratori di rete di adottare delle contromisure adatte alla tipologia di attacco in corso. Il sistema prevede anche un meccanismo di aggiornamento dell'insieme di dati inizialmente utilizzati per l'apprendimento.

L'elaborato è organizzato in sei capitoli:

- **Stato dell'arte**: in questo capitolo viene fatta una panoramica delle tecniche di apprendimento automatico impiegate nel contesto di rilevamento delle intrusioni.
- **Sistema di rilevamento delle intrusioni proposto**: in questo capitolo viene presentato il sistema proposto nel dettaglio.

- **Apprendimento automatico**: in questo capitolo si introduce il concetto di apprendimento automatico e successivamente vengono descritti gli algoritmi di apprendimento automatico usati in questo lavoro di tesi.
- **Preparazione dei dati**: in questo capitolo vengono descritti il dataset e gli strumenti usati. Successivamente si descriverà il tipico flusso di operazioni impiegate per preparare il dataset alle successive analisi e le tecniche adottate in questo progetto di tesi.
- **Risultati sperimentali**: in questo capitolo sono presentati e discussi i risultati sperimentali ottenuti: prima i risultati di selezione delle migliori caratteristiche e dell'algoritmo di classificazione, successivamente i risultati dell'analisi di clustering.
- **Conclusione**: in questo capitolo sono discussi i principali risultati raggiunti dall'analisi e dagli esperimenti fatti, e sono discussi dei possibili sviluppi futuri del sistema proposto.

Bibliografia

[1] https://clusit.it/rapporto-clusit/

[2] Z.J. Lemnios, “Testimony before the United States house of representatives committee on armed services, Subcommittee on Emerging Threats and Capabilities”, 2011.

[3] https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T

[4] https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack

[5] https://www.cybersecitalia.it/attacco-hacker-a-luxottica-e-ospedali-le-vulnerabilita-erano-note-da-tempo/8614/

[6] Gilbert R. Hendry, Shanchieh J. Yang, "Intrusion signature creation via clustering anomalies", Proc. SPIE 6973, Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2008, 69730C (17 March 2008); doi: 10.1117/12.775886; https://doi.org/10.1117/12.775886

[7] A. AlEroud and G. Karabatis, "A Contextual Anomaly Detection Approach to Discover Zero-Day Attacks," 2012 International Conference on Cyber Security, 2012, pp. 40-45.

[8] https://hdbscan.readthedocs.io/en/latest/how_hdbscan_works.html

[9] L. Breiman, J. Friedman, R. Olshen, and C. Stone, “Classification and Regression Trees”, Wadsworth, Belmont, CA, 1984.

[10] Quinlan J.R., “C4. 5: Programs for Machine Learning.” Elsevier, 58-60, 2014.

[11] Quinlan J.R., “Induction of decision trees.”, Mach Learn 1, 81–106, 1986.

[12] L.Breiman, “Random Forests -- Random Features”, Technical Report 567, September 1999.

[13] H. Zhang “The Optimality of Naive Bayes”, Proc. FLAIRS, 2004.

[14] Haneen Arafat Abu Alfeilat, Ahmad B.A. Hassanat, Omar Lasassmeh, Ahmad S. Tarawneh, Mahmoud Bashir Alhasanat, Hamzeh S. Eyal Salman, and V.B. Surya Prasath, “Big Data” 221-248, 2019.

[15] R. Sheikhpour, M. A. Sarram, S. Gharaghani, and M. A. Z. Chahooki, ‘‘A survey on semi-supervised feature selection methods,’’ Pattern Recognit., vol. 64, pp. 141–158, Apr. 2017.

[16] R. Panigrahi and S. Borah, ‘‘A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems,’’ Int. J. Eng. Technol., vol. 7,no. 24, pp. 479–482, 2018.

[17] Jupyter https://jupyter.org/

[18] Numpy https://numpy.org/

[19] Pandas https://pandas.pydata.org/

[20] Scikit Learn https://scikit-learn.org/

[21] Matplotlib https://matplotlib.org/

[22] R. Sheikhpour, M. A. Sarram, S. Gharaghani, and M. A. Z. Chahooki, ‘‘A survey on semi-supervised feature selection methods,’’ Pattern Recognit., vol. 64, pp. 141–158, Apr. 2017.

[23] Bhatia, N., & Vandana, “Survey of Nearest Neighbor Techniques”, International Journal of Computer Science and Information Security, 302–305, 2010.

[24] https://en.wikipedia.org/wiki/Curse_of_dimensionality

[25] Charu C. Aggarwal, “Data Mining”, Springer, 2015.

[26] Kurniabudi et al.: CICIDS-2017 Dataset Feature Analysis With Information Gain for Anomaly Detection.

[27] T. A. Alhaj, M. M. Siraj, A. Zainal, H. T. Elshoush, and F. Elhaj, “Feature selection using information gain for improved structural-based alert correlation” PLoS ONE, vol. 11, no. 11, 2016, Art. no. E0166017.

[28] Y. Sugianela and T. Ahmad, "Pearson Correlation Attribute Evaluation-based Feature Selection for Intrusion Detection System" 2020 International Conference on Smart Technology and Applications (ICoSTA), 2020, pp. 1-5.

[29] Q. R. S. Fitni and K. Ramli, "Implementation of Ensemble Learning and Feature Selection for Performance Improvements in Anomaly-Based Intrusion Detection Systems," 2020 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT), 2020, pp. 118-124.

[30] CICFlowmeter-V4.0 (CICFlowMeter,2021),(Habibi Lashkari et al., 2021).

[31] V. Vijayakumar and V. Neelanarayanan, "Intrusion detection model using chi square feature selection and modifed Naïve Bayes classifer," in Smart Innovation, Systems and Technologies, vol. 49. Cham, Switzerland: Springer, 2016, p. 15.

[32] Sharafaldin, I., Lashkari, A. and Ghorbani, A.Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization.

[33] The hdbscan Clustering Library https://hdbscan.readthedocs.io/en/latest/index.html

[34] L. McInnes, J. Healy, S. Astels, hdbscan: Hierarchical density based clustering In: Journal of Open Source Software, The Open Journal, volume 2, number 11. 2017.

[35] McInnes L, Healy J. Accelerated Hierarchical Density Based Clustering In: 2017 IEEE International Conference on Data Mining Workshops (ICDMW), IEEE, pp 33-42. 2017.

[36] https://hdbscan.readthedocs.io/en/latest/parameter_selection.html

[37] Campello, Ricardo JGB, Davoud Moulavi, and Jörg Sander. “Density-based clustering based on hierarchical density estimates.” Pacific-Asia conference on knowledge discovery and data mining. Springer, Berlin, Heidelberg, 2013.

[38] https://cdn-images-1.medium.com/max/2560/1*L-hr07E_ygPJEqDXgaoGQA.png

[39] Martin Ester, Hans-Peter Kriegel, Jiirg Sander and Xiaowei Xu “A Density-Based Algorithm for Discovering Clusters in Large Spatial Databases with Noise”. KDD-96 Proceedings, 2016.

[40] Gower, J. C., and G. J. S. Ross. “Minimum Spanning Trees and Single Linkage Cluster Analysis.” Journal of the Royal Statistical Society. Series C (Applied Statistics), vol. 18, no. 1, [Wiley, Royal Statistical Society], 1969, pp. 54–64.

[41] Justin Eldridge, Mikhail Belkin and Yusu Wang. “Beyond Hartigan Consistency:Merge Distortion Metric for Hierarchical Clustering.” stat. ML, 2015

[42] R. C. Prim, "Shortest connection networks and some generalizations," in The Bell System Technical Journal, vol. 36, no. 6, pp. 1389-1401, Nov. 1957.

[43] C. Kruegel and T. Toth, “Using decision trees to improve signaturebased intrusion detection,” in Proc. 6th Int. Workshop Recent Adv. Intrusion Detect., West Lafayette, IN, USA, 2003, pp. 173–191.

[44] Snort 2.0. Sourcefire [Online]. Available: http://www.sourcefire.com/ technology/whitepapers.htm, accessed on Jun. 2014.

[45] R. Lippmann, J. Haines, D. Fried, J. Korba, and K. Das, “The 1999 DARPA offline intrusion detection evaluation,” Comput. Netw., vol. 34, pp. 579–595, 2000.

[46] L. Bilge, E. Kirda, C. Kruegel, and M. Balduzzi, “EXPOSURE: Finding malicious domains using passive DNS analysis,” presented at the 18th Annu. Netw. Distrib. Syst. Secur. Conf., 2011.

[47] P. A. Vikhar, "Evolutionary algorithms: A critical review and its future prospects," 2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC), 2016.

[48] W. Li, “Using genetic algorithms for network intrusion detection,” in Proc. U.S. Dept. Energy Cyber Secur. Group 2004 Train. Conf., 2004, pp. 1–8.

[49] https://datatracker.ietf.org/doc/html/rfc791

[50] J. Hansen, P. Lowry, D. Meservy, and D. McDonald, “Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection,” Decis. Support Syst., vol. 43, no. 4, pp. 1362–1374, Aug. 2007.

[51] D. E. Goldberg and J. H. Holland, “Genetic algorithms and machine learning,” Mach. Learn., vol. 3, no. 2, pp. 95–99, 1988.

[52] R. Agrawal, T. Imielinski, and A. Swami, “Mining association rules between sets of items in large databases,” in Proc. Int. Conf. Manage. Data Assoc. Comput. Mach. (ACM), 1993, pp. 207–216.

[53] L. A. Zadeh, "Fuzzy sets," Information and Control, vol. 8, no. 3, pp. 338-353, 1965.

[54] A. Tajbakhsh, M. Rahmati, and A. Mirzaei, “Intrusion detection using fuzzy association rules,” Appl. Soft Comput., vol. 9, pp. 462–469, 2009.
[55] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, “A detailed analysis of the KDD Cup 1999 data set,” in Proc. 2nd IEEE Symp. Comput. Intell. Secur. Defense Appl., 2009, pp. 1–6.
[56] Q. -V. Dang, "Studying the Fuzzy clustering algorithm for intrusion detection on the attacks to the Domain Name System," 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), 2021, pp. 271-274.
[57] M. MontazeriShatoori, L. Davidson, G. Kaur and A. H. Lashkari, "Detection of doh tunnels using time-series classification of encrypted traffic", DASC/PiCom/CBDCom/CyberSciTech, pp. 63-70, 2020.
[58] L. Breiman, “Random forests,” Mach. Learn., vol. 45, no. 1, pp. 5–32, 2001.
[59] R. Polikar, “Ensemble based systems in decision making,” IEEE Circuits Syst. Mag., vol. 6, no. 3, pp. 21–45, Third Quart. 2006.
[60] J. Zhang, M. Zulkernine, and A. Haque, “Random-forests-based network intrusion detection systems,” IEEE Trans. Syst. Man Cybern. C: Appl. Rev., vol. 38, no. 5, pp. 649–659, Sep. 2008.
[61] L. Bilge, D. Balzarotti, W. Robertson, E. Kirda, and C. Kruegel, “Disclosure: Detecting botnet command and control servers through large-scale netflow analysis,” in Proc. 28th Annu. Comput. Secur. Appl. Conf. (ACSAC’12), Orlando, FL, USA, Dec. 3–7, 2012, pp. 129–138.
[62] M. Panda and M. R. Patra, “Network intrusion detection using Naive Bayes,” Int. J. Comput. Sci. Netw. Secur., vol. 7, no. 12, pp. 258–263, 2007.
[63] N. B. Amor, S. Benferhat, and Z. Elouedi, “Naïve Bayes vs. decision trees in intrusion detection systems,” in Proc ACM Symp. Appl. Comput., 2004, pp. 420–424.
[64] K. Mehrotra, C. Mohan, S. Ranka, “Elements of Artificial Neural Networks”, The MIT Press,Cambridge, 2000.
[65] G. Scott. “Knowledge-based artificial neural networks for process modeling and control”, TheUniversity of Wisconsin, Madison, 1993.
[66] J. Cannady, “Artificial neural networks for misuse detection,” in Proc. 1998 Nat. Inf. Syst. Secur. Conf., Arlington, VA, USA, 1998, pp. 443–456.
[67] R. P. Lippmann and R. K. Cunningham, “Improving intrusion detection performance using keyword selection and neural networks,” Comput. Netw., vol. 34, pp. 597–603, 2000.
[68] Agate V., De Paola A., Ferraro P., Lo Re G., Morana M., SecureBallot: A secure open source e-Voting system, (2021) Journal of Network and Computer Applications, 191, art. no. 103165, DOI: 10.1016/j.jnca.2021.103165
[69] Agate V., De Paola A., Lo Re G., Morana M.A Simulation Software for the Evaluation of Vulnerabilities in Reputation Management Systems (2021) ACM

Transactions on Computer Systems, 37 (1-4), art. no. 3458510 DOI: 10.1145/3458510

[70] Concone F., Lo Re G., Morana M., SMCP: a Secure Mobile Crowdsensing Protocol for fog-based applications, (2020) Human-centric Computing and Information Sciences, 10 (1), art. no. 28, DOI: 10.1186/s13673-020-00232-y

[71] Bordonaro A., De Paola A., Lo Re G., Morana M., Smart Auctions for Autonomic Ambient Intelligence Systems, (2020) Proceedings - 2020 IEEE International Conference on Smart Computing, SMARTCOMP 2020, art. no. 9239687, pp. 180 – 187, DOI: 10.1109/SMARTCOMP50058.2020.00043

[72] Agate V., De Paola A., Lo Re G., Morana M. DRESS: A distributed RMS evaluation simulation software, (2020) International Journal of Intelligent Information Technologies, 16 (3), DOI: 10.4018/IJIIT.2020070101

[73] Agate V., Curaba M., Ferraro P., Lo Re G., Morana M., Secure e-voting in smart communities, (2020) CEUR Workshop Proceedings, 2597, pp. 1 – 11

[74] Agate V., De Paola A., Lo Re G., Morana M. A Platform for the Evaluation of Distributed Reputation Algorithms, (2019) Proceedings of the 2018 IEEE/ACM 22nd International Symposium on Distributed Simulation and Real Time Applications, DS-RT 2018, art. no. 8601020, pp. 182 – 189, DOI: 10.1109/DISTRA.2018.8601020

[75] De Paola A., Gaglio S., Lo Re G., Morana M. A hybrid system for malware detection on big data, (2018) INFOCOM 2018 - IEEE Conference on Computer Communications Workshops, pp. 45 – 50, DOI: 10.1109/INFCOMW.2018.8406963

[76] De Paola A., Favaloro S., Gaglio S., Lo Re G., Morana M., Malware detection through low-level features and stacked denoising autoencoders, (2018) CEUR Workshop Proceedings, 2058

[77] Concone F., De Paola A., Lo Re G., Morana M., Twitter analysis for real-Time malware discovery, (2017) 2017 AEIT International Annual Conference: Infrastructures for Energy and ICT: Opportunities for Fostering Innovation, AEIT 2017, 2017-January, pp. 1 – 6, DOI: 10.23919/AEIT.2017.8240551

[78] Agate V., De Paola A., Lo Re G., Morana M., Vulnerability evaluation of distributed reputation management systems, (2017) ValueTools 2016 - 10th EAI International Conference on Performance Evaluation Methodologies and Tools, pp. 235 – 242, DOI: 10.4108/eai.25-10-2016.2266868

[79] Agate V., De Paola A., Gaglio S., Lo Re G., Morana M., A framework for parallel assessment of reputation management systems, (2016) ACM International Conference Proceeding Series, 1164, pp. 121 – 128, DOI: 10.1145/2983468.2983474

[80] Agate V., de Paola A., Lo Re G., Morana M., A simulation framework for evaluating distributed reputation management systems, (2016) Advances in Intelligent Systems and Computing, 474, pp. 247 – 254, DOI: 10.1007/978-3-319-40162-1_27