ANALISIS PERBANDINGAN PERFORMA *INTRUSION DETECTION SYSTEM* (IDS) DALAM MENDETEKSI SERANGAN *PORT SCANNING* DAN *DISTRIBUTED DENIAL OF SERVICE* (DDOS)

SKRIPSI

Diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar
Sarjana Teknik Sistem Telekomunikasi

Oleh
Farhan Maulana
NIM 1908952

PROGRAM STUDI SISTEM TELEKOMUNIKASI
KAMPUS UPI DI PURWAKARTA
UNIVERSITAS PENDIDIKAN INDONESIA
2024

LEMBAR HAK CIPTA

ANALISIS PERBANDINGAN PERFORMA *INTRUSION DETECTION SYSTEM* (IDS) DALAM MENDETEKSI SERANGAN *PORT SCANNING* DAN *DISTRIBUTED DENIAL OF SERVICE* (DDOS)

Oleh

Farhan Maulana

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Teknik pada Program Studi Sistem Telekomunikasi

Universitas Pendidikan Indonesia

Januari 2024

LEMBAR PENGESAHAN

SKRIPSI

FARHAN MAULANA

1908952

ANALISIS PERBANDINGAN PERFORMA *INTRUSION DETECTION SYSTEM* (IDS) DALAM MENDETEKSI SERANGAN *PORT SCANNING* DAN *DISTRIBUTED DENIAL OF SERVICE* (DDOS)

Disetujui dan Disahkan Oleh Pembimbing.

Pembimbing 1

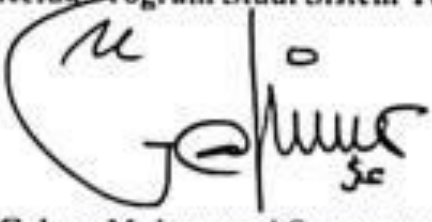
Galura Muhammad Suranegara, S.Pd., M.T.
NIP. 920190219920111101

Pembimbing 2

Ahmad Fauzi, S.Si., M.T.
NIP.920171219820915101

Mengetahui,

Ketua Program Studi Sistem Telekomunikasi



Galura Muhammad Suranegara, S.Pd., M.T.
NIP. 920190219920111101

PERNYATAAN ANTI PLAGIARISME

Dengan ini saya menyatakan bahwa skripsi saya dengan judul "Analisis Perbandingan Performa *Intrusion Detection System* (IDS) Dalam Mendeteksi Serangan *Port Scanning* dan *Distributed Denial of Service* (DDoS)" ini beserta seluruh isinya adalah benar – benar karya saya sendiri.

Saya tidak melakukan penjiplakan atau pengutipan dengan cara – cara yang tidak sesuai dengan etika keilmuan yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung risiko atau sanksi yang diberikan apabila di kemudian hari ditemukan adanya pelanggaran etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya saya ini.

Purwakarta, Januari 2024

Farhan Maulana

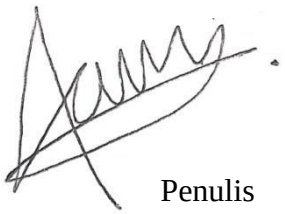
NIM. 1908952

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan kehadirat Allah SWT atas segala nikmat dan izin-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisis Perbandingan Performa *Intrusion Detection System* (IDS) Dalam Mendeteksi Serangan *Port Scanning* dan *Distributed Denial of Service* (DDoS)". Shalawat serta salam semoga selalu tercurah limpahkan kepada junjungan kita Nabi Muhammad SAW, juga kepada keluarganya, sahabatnya dan kepada umat-Nya yang senantiasa mengikuti dan melaksanakan ajarannya hingga akhir zaman. *Aamiin ya Rabbal'alamin.*

Semoga karya tulis ini dapat memberikan manfaat dalam pengembangannya. *Aamiin ya Rabbal'alamin.* Segala kebenaran hanya milik Allah SWT, dan seluruh kekurangan hanya milik saya semata.

Purwakarta, Januari 2024



Penulis

UCAPAN TERIMA KASIH

Allhamdullilahirabibil Alaamiin, puji serta syukur penulis curah limpahkan kepada kehadirat Allah SWT, yang telah memberikan penulis rahmat, taufik, dan hidayah-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisis Perbandingan Performa *Intrusion Detection System* (IDS) Dalam Mendeteksi Serangan *Port Scanning* dan *Distributed Denial of Service* (DDoS)", yang merupakan sebagian syarat untuk menyelesaikan Program Sarjana Teknik Program Studi Sistem Telekomunikasi Universitas Pendidikan Indonesia.

Penulis menyadari bahwa tersusunnya skripsi ini tidak terlepas dari izin dan ridho Allah SWT, serta bantuan, dukungan, bimbingan dan nasehat dari berbagai pihak selama penyusunan skripsi ini. Pada kesempatan ini, penulis mengucapkan terima kasih kepada:

1. Allah SWT dengan segala rahmat serta karunia-Nya, yang selalu memberikan kesehatan, kemudahan, dan kelancaran kepada penulis dalam menyelesaikan skripsi ini.
2. *Umi* penulis, Erni Susilowati, S.Pd. yang selalu memberikan cinta, kasih sayang, materi dan doa. Tanpa-nya penulis tidak mungkin bisa berada diposisi ini, hingga penulis mampu menyelesaikan program sarjana ini dari awal hingga akhir.
3. *Abi* penulis, Sugeng Priyatno yang selalu memberikan cinta, kasih sayang, motivasi dan doa. Tanpa-nya penulis tidak mungkin bisa berada diposisi ini, hingga penulis mampu menyelesaikan program sarjana ini dengan baik.
4. Adik penulis, Salma Khairunnisa, yang selalu memberikan motivasi, kasih sayang, dan doa, hingga penulis mampu menyelesaikan program sarjana ini dengan baik.
5. Prof. Yayan Nurbayan, M.Ag. selaku Direktur Universitas Pendidikan Indonesia Kampus Purwakarta.
6. Prof. Turmudi, M.Ed., M.Sc., Ph.D. selaku Direktur Universitas Pendidikan Indonesia Kampus Purwakarta periode 2015-2023.
7. Dr. Idat Muqodas, S.Pd., M.Pd., Kons. selaku Wakil Direktur Bidang Akademik dan Kemahasiswaan Universitas Pendidikan Indonesia Kampus Purwakarta.

8. Dr. Suci Utami Putri, M.Pd. selaku Wakil Direktur Bidang Sumber Daya, Keuangan dan Umum Universitas Pendidikan Indonesia Kampus Purwakarta
9. Bapak Galura Muhammad Suranegara, S.Pd., M.T. selaku Ketua Program Studi Sistem Telekomunikasi Universitas Pendidikan Indonesia Kampus Purwakarta. Serta selaku Dosen Pembimbing I yang selalu memberikan ilmu, waktu, arahan, motivasi dan pengalaman kepada penulis dengan penuh kesabaran hingga penulis dapat menyelesaikan skripsi ini dengan baik.
10. Bapak Ahmad Fauzi, S.Si., M.T. selaku Ketua Program Studi Sistem Telekomunikasi Universitas Pendidikan Indonesia Kampus Purwakarta periode 2019 - 2023. Serta selaku Dosen Pembimbing II yang selalu memberikan ilmu, waktu, arahan, motivasi dan pengalaman kepada penulis dengan penuh kesabaran hingga penulis dapat menyelesaikan skripsi ini dengan baik.
11. Bapak Syifaul Fuada, S.Pd., M.T. selaku Dosen Wali Akademik penulis, yang selalu memberikan bimbingan semasa penulis melaksanakan perkuliahan.
12. Seluruh dosen dan tenaga pendidik Program Studi Sistem Telekomunikasi UPI Kampus Purwakarta yang tidak dapat disebutkan satu-persatu, yang telah memberikan ilmu, pengalaman, serta motivasi selama penulis berkuliah.
13. Aldewo Dillon, Adisty Nurrahmah Laili, Banda Subagja, Ega Restu Gumelar, Fauziyah Rhaudhatul Jannah, Herdi Rizky Pratama, Karina Oktafianti, Muhamad Baha'udin, Muhammad Fathan Mubina, Mohammad Luthfan Faohan, Raihan Fakhri Rabbani, Riyadh Ahmad Faridz, yang senantiasa membersamai penulis ketika berjuang bersama-sama dalam menyusun skripsi.
14. Teman-teman Sistem Telekomunikasi Angkatan 2019 yang telah membersamai dan memberikan penulis pengalaman yang berharga dalam menjalankan masa-masa perkuliahan dan hidup di perantauan.
15. Teman-teman Himpunan Mahasiswa Sistem Telekomunikasi yang telah membersamai, memberikan pengalaman, dan pembelajaran yang berharga kepada penulis yang luar biasa.
16. Rekan-rekan Badan Eksekutif Mahasiswa UPI Purwakarta yang telah memberikan pembelajaran dan pengalaman yang berharga selama penulis menjalankan tanggung jawabnya.

17. Teman-teman Departemen Pengembangan Sumber Daya Organisasi BEM UPI Purwakarta Kabinet Kolaborasi Aspiratif yang senantiasa membersamai, berjuang, dan memberikan pengalaman berharga kepada penulis selama menjalankan tanggung jawabnya.
18. Semua pihak yang tidak dapat disebutkan satu-persatu, yang telah membantu penulis baik langsung atau tidak langsung dalam melakukan proses selama perkuliahan dan mengerjakan skripsi ini.

ABSTRAK

ANALISIS PERBANDINGAN PERFORMA *INTRUSION DETECTION SYSTEM* (IDS) DALAM MENDETEKSI SERANGAN *PORT SCANNING* DAN *DISTRIBUTED DENIAL OF SERVICE* (DDOS)

Seiring berkembangnya teknologi dan semakin beragamnya peningkatan jumlah penyusupan ke jaringan, hampir setiap organisasi termasuk lembaga pemerintah dan perusahaan dipaksa untuk menerapkan *Intrusion Detection System* (IDS). Saat ini IDS menjadi salah satu alternatif untuk memantau lalu lintas jaringan dari intrusi. Penelitian ini membandingkan performa NIDS *Snort, Suricata,* dan *Zeek* terbaru dalam mendeteksi serangan *Port Scanning* (PS) dan *Distributed Denial of Service* (DDoS). Penelitian ini dilakukan dengan menggunakan lingkungan virtual dengan meninjau performa *confusion matrix*, kecepatan deteksi serangan, CPU *usage, memory usage,* dan *network usage*. Hasil pada penelitian ini menunjukan keberagaman disetiap parameter yang digunakan, setiap NIDS yang digunakan memiliki karakteristik dan keunggulannya masing-masing. Pada penelitian ini *Suricata* unggul dalam mendeteksi intrusi dengan tingkat TPR pada *case* PS 96,98% dan pada *case* DDoS 98,08%, kemudian dalam kecepatan deteksi, *Zeek* lebih unggul dengan kecepatan rata-rata pada *case* PS 105,21 DR/m dan pada *case* DDoS 491,96 DR/m, dan pada *resource usage Snort* unggul dibandingkan *Suricata* dan *Zeek*. Tinjauan kinerja yang komprehensif seperti ini belum pernah dipertimbangkan dalam penelitian sebelumnya. Analisis menyeluruh ini diharapkan dapat memberikan manfaat besar bagi para praktisi dan peneliti dalam pemilihan NIDS yang optimal dan sesuai kebutuhan mereka.

Kata Kunci: NIDS, *Snort, Suricata, Zeek, Cybersecurity*.

ABSTRACT

COMPARATIVE ANALYSIS OF INTRUSION DETECTION SYSTEM (IDS) PERFORMANCE IN DETECTING PORT SCANNING AND DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS

As technology develops and the number of intrusions into the network increases, almost every organization including government agencies and companies are forced to implement an Intrusion Detection System (IDS). Currently, IDS is one of the alternatives to monitor network traffic that occurs, as well as maintain network security to avoid unwanted and destructive attacks. This research compares the performance of the latest Snort, Suricata, and Zeek NIDS in detecting Port Scanning (PS) and Distributed Denial of Service (DDoS) attacks. This research was conducted using a virtual environment by reviewing confusion matrix performance, attack detection speed, CPU usage, memory usage, and network usage. The results in this study show diversity in each parameter used, each NIDS used has its own characteristics and advantages. In this study Suricata excels in detecting intrusions with a TPR rate in the PS case of 96.98% and in the DDoS case of 98.08%, then in detection speed Zeek is superior with an average speed in the PS case of 105.21 DR/m and in the DDoS case of 491.96 DR/m, and in resource usage Snort is superior to Suricata and Zeek. Such a comprehensive performance review has never been considered in previous research. This comprehensive analysis is expected to be of great benefit to practitioners and researchers in the selection of an optimal NIDS that suits their needs.

***Keywords*:** *NIDS, Snort, Suricata, Zeek Cybersecurity.*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR ISTILAH

CPU (*Central Processing Unit*)

Otak komputer yang bertanggung jawab untuk mengeksekusi instruksi program, serta mengelola alur interaksi dengan perangkat keras lainnya.

DoS (*Denial of Service*)

Serangan yang dilakukan dengan cara membanjiri sumber daya atau layanan komputer.

DDoS (*Distributed Denial of Service)*

Serangan dengan jaringan yang terdistribusi yang dilakukan dengan cara membanjiri sumber daya atau layanan komputer.

DR (*Detection Rate)*

Ukuran suatu sistem dapat mengenali dan melaporkan keberadaan ancaman keamanan yang mencoba merusak atau mengakses system.

FNR (*False Negative Rate)*

mengukur sejauh mana sistem gagal mengidentifikasi *instance* positif.

FPR (*False Positive Rate)*

mengukur sejauh mana sistem memberikan alarm palsu dengan mengidentifikasi *instance* negatif sebagai positif.

FTP (*File Transfer Protocol)*

Protokol untuk mentransfer *file* antara perangkat dalam jaringan.

HIDS (*Host-Based Intrusion Detection System)*

Sistem deteksi intrusi yang berfokus pada melindungi satu host atau sistem komputer secara individu.

HTTP (*Hypertext Transfer Protocol)*

Protokol komunikasi untuk mentransfer data di browser.

IDS (*Intrusion Detection System)*

Sistem yang mendeteksi aktivitas mencurigakan atau ancaman keamanan di jaringan atau sistem komputer.

IDPS (*Intrusion Detection Prevention System)*

Sistem keamanan yang melibatkan kemampuan deteksi intrusi dan pencegahan intrusi dalam satu platform.

IP (*Internet Protocol)*

Protokol komunikasi yang digunakan untuk mengidentifikasi dan lokalisasi perangkat di jaringan komputer.

KB (*Kilobyte*)

Satuan pengukuran kecepatan transfer data atau bandwidth dalam komputer dan jaringan

NIDS (*Network-Based Intrusion Detection System)*

Sistem deteksi intrusi yang berfokus pada pemantauan lalu lintas jaringan.

PS (*Port Scanning*)

Usaha untuk menemukan port-port yang terbuka pada suatu sistem atau jaringan.

QoS (*Quality of Service)*

Kebijakan untuk meningkatkan kualitas pengalaman pengguna dalam jaringan.

RAM (*Random Access Memory)*

Memori semu pada komputer yang menyimpan data sementara yang dapat diakses dengan cepat oleh prosesor.

SAR (*System Activity Report*)

Alat yang digunakan pada penelitian ini untuk menganalisa parameter *resource usage.*

Snort

Sistem deteksi intrusi yang digunakan pada penelitian ini untuk mendeteksi dan menganalisis aktivitas jaringan yang mencurigakan.

Suricata

Sistem deteksi intrusi yang digunakan pada penelitian ini untuk mendeteksi dan menganalisis aktivitas jaringan yang mencurigakan.

TCP (*Transmission Control Protocol*)

Protokol komunikasi dalam model OSI yang menyediakan koneksi yang handal dan terurut antara dua perangkat dalam jaringan.

TNR (*True Negative Rate)*

mengukur sejauh mana sistem dapat mengidentifikasi dengan benar *instance* negatif.

TPR (*True Positive Rate)*

Ukuran sejauh mana sistem dapat mengidentifikasi dengan benar *instance* positif.

Zeek

Sistem deteksi intrusi yang digunakan pada penelitian ini untuk mendeteksi dan menganalisis aktivitas jaringan yang mencurigakan.

DAFTAR PUSTAKA

Akhriana, A., & Irmayana, A. (2020). Web App Pendeteksi Jenis Serangan Jaringan Komputer Dengan Memanfaatkan Snort Dan Log Honeypot. *CCIT Journal*, *12*(1), 85–96. https://doi.org/10.33050/ccit.v12i1.604

Anonim. (2023a). *An Open Source Network Security Monitoring Tool*. [Online]. Diakses dari. https://suricata.io/

Anonim. (2023b). *Suricata is Far more than an IDS/IPS*. [Online]. Diakses dari. https://zeek.org/about/

Anonim. (2023c). *What is Snort?* [Online]. Diakses dari. https://www.snort.org/

Bada, G. K., Nabare, W. K., & Quansah, D. K. K. (2020). Comparative Analysis of the Performance of Network Intrusion Detection Systems: Snort, Suricata and Bro Intrusion Detection Systems in Perspective. *International Journal of Computer Applications*, *176*(40), 39–44. https://doi.org/10.5120/ijca2020920513

Bhosale, D. A., & Mane, V. M. (2015). Comparative Study and Analysis of Network Intrusion Detection Tools. *International Conference on Applied and Theoretical Computing and Communication Technology, iCATccT 2015*, 312–315. https://doi.org/10.1109/ICATCCT.2015.7456901

Boukebous, A. A. E., Fettache, M. I., Bendiab, G., & Shiaeles, S. (2023). A Comparative Analysis of Snort 3 and Suricata. *2023 IEEE IAS Global Conference on Emerging Technologies, GlobConET 2023*. https://doi.org/10.1109/GlobConET56651.2023.10150141

Bouteraa, I., Derdour, M., & Ahmim, A. (2020). Intrusion detection using classification techniques: A comparative study. *International Journal of Data Mining, Modelling and Management*, *12*(1), 65–86. https://doi.org/10.1504/IJDMMM.2020.105596

Bouziani, O., Benaboud, H., Chamkar, A. S., & Lazaar, S. (2019). A Comparative Study of Open Source IDSs According to Their Ability to Detect Attacks. *ACM International Conference Proceeding Series*, 27–29. https://doi.org/10.1145/3320326.3320383

Chovanec, M., Hasin, M., Havrilla, M., & Chovancová, E. (2023). Detection of

HTTP DDoS Attacks Using NFStream and TensorFlow. *Applied Sciences (Switzerland)*, *13*(11). https://doi.org/10.3390/app13116671

Dwi Bayu Rendro, Ngatono, W. N. A. (2020). Analisis Monitoring Sistem Jaringan Komputer Menggunakan Software Nmap. *PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer*, *7*(2), 108–115. https://doi.org/10.30656/prosisko.v7i2.2522

Gupta, A., & Sharma, L. Sen. (2020). Performance Evaluation of Snort and Suricata Intrusion Detection Systems on Ubuntu Server. *Lecture Notes in Electrical Engineering*, *597*, 811–821. https://doi.org/10.1007/978-3-030-29407-6_58

Hajj, S., El Sibai, R., Bou Abdo, J., Demerjian, J., Makhoul, A., & Guyeux, C. (2021). Anomaly-based Intrusion Detection Systems: The Requirements, Methods, Measurements, and Datasets. *Transactions on Emerging Telecommunications Technologies*, *32*(4), 1–36. https://doi.org/10.1002/ett.4240

Hoover, C., & Thompson, D. R. (2022). *Comparative Study of Snort 3 and Suricata Intrusion Detection Systems*. https://scholarworks.uark.edu/csceuht/105

Hu, Q., Yu, S. Y., & Asghar, M. R. (2020). Analysing Performance Issues of Open-source Intrusion Detection Systems in High-speed Networks. *Journal of Information Security and Applications*, *51*, 102426. https://doi.org/10.1016/j.jisa.2019.102426

Isa, F. M., Saad, S., Firdaus, A., & Fadzil, A. (2019). Comprehensive Performance Assessment on Open Source Intrusion Detection System. In *Proceedings of the Third International Conference on Computing, Mathematics and Statistics (iCMS2017)*. Springer Singapore. https://doi.org/10.1007/978-981-13-7279-7

Kumar, S., Gupta, S., & Arora, S. (2021). Research Trends in Network-Based Intrusion Detection Systems: A Review. *IEEE Access*, *9*, 157761–157779. https://doi.org/10.1109/ACCESS.2021.3129775

Lukman, & Suci, M. (2020). Analisis Perbandingan Kinerja Snort dan Suricata Sebagai Intrusion Detection System dalam Mendeteksi Serangan Syn Flood pada Web Server Apache. *Respati*, *15*(2), 6. https://doi.org/10.35842/jtir.v15i2.343

Mishra, B., & Smirnova, I. (2021). Optimal Configuration of Intrusion Detection

Systems. *Information Technology and Management*, *22*(4), 231–244. https://doi.org/10.1007/s10799-020-00319-z

Mispriatin, M., Ginting, J. G. A., & Arifwidodo, B. (2022). Analisis Kinerja Honeypot Dionaea Dan Cowrie Dalam Mendeteksi Serangan. *Prosiding Seminar Nasional Teknoka*, *6*(2502), 170–178. https://doi.org/10.22236/teknoka.v6i1.448

Nisa, M. U., & Kifayat, K. (2020). Detection of Slow Port Scanning Attacks. *1st Annual International Conference on Cyber Warfare and Security, ICCWS 2020 - Proceedings*. https://doi.org/10.1109/ICCWS48432.2020.9292389

Obaid, H. S., & Abeed, E. H. (2020). DoS and DDoS Attacks at OSI Layers. *International Journal of Multidisciplinary Research and Publications Hadeel S. Obaid and Esamaddin H*, *2*(8), 1–9.

Ozkan-Okay, M., Samet, R., Aslan, O., & Gupta, D. (2021). A Comprehensive Systematic Literature Review on Intrusion Detection Systems. *IEEE Access*, *9*, 157727–157760. https://doi.org/10.1109/ACCESS.2021.3129336

Paramita, R. W. D. (2021). *Metode Penelitian Kuantitatif*. WIDYA GAMA PRESS.

Prabowo, W. A., Fauziah, K., Nahrowi, A. S., Faiz, M. N., & Muhammad, A. W. (2023). *Strengthening Network Security : Evaluation of Intrusion Detection and Prevention Systems Tools in Networking Systems*. *14*(9), 1–10.

Ralianto, A. D., & Cahyono, S. (2021). Perbandingan Nilai Akurasi Snort dan Suricata dalam Mendeteksi Intrusi Lalu Lintas di Jaringan. *Info Kripto*, *15*(2), 69–75. https://doi.org/10.56706/ik.v15i2.10

Saranya, T., Sridevi, S., Deisy, C., Chung, T. D., & Khan, M. K. A. A. (2020). Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review. *Procedia Computer Science*, *171*(2019), 1251–1260. https://doi.org/10.1016/j.procs.2020.04.133

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, *2018-Janua*(Cic), 108–116. https://doi.org/10.5220/0006639801080116

Waleed, A., Jamali, A. F., & Masood, A. (2022). Which open-source IDS ? Snort ,

Suricata or Zeek. *Computer Networks*, *213*(June), 109116. https://doi.org/10.1016/j.comnet.2022.109116

Wang, Z., Liu, Y., He, D., & Chan, S. (2021). Intrusion Detection Methods Based on Integrated Deep Learning Model. *Computers and Security*, *103*. https://doi.org/10.1016/j.cose.2021.102177

Zhou, D., Yan, Z., Fu, Y., & Yao, Z. (2018). A Survey on Network Data Collection. *Journal of Network and Computer Applications*, *116*(May), 9–23. https://doi.org/10.1016/j.jnca.2018.05.004