PENGUJIAN KERENTANAN APACHE LOG4J PADA CVE-2021-44228 TERHADAP ANCAMAN REMOTE ACCESS TROJAN DENGAN METODE PENETRATION TESTING EXECUTION STANDARD

SKRIPSI

MUHAMMAD NUR IRSYAD **1807422020**

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
2023

PENGUJIAN KERENTANAN APACHE LOG4J PADA CVE-2021-44228 TERHADAP ANCAMAN REMOTE ACCESS TROJAN DENGAN METODE PENETRATION TESTING EXECUTION STANDARD

SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan

untuk Memperoleh Diploma Empat Politeknik

MUHAMMAD NUR IRSYAD

1807422020

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
2023

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama	: Muhammad Nur Irsyad
NIM	: 1807422020
Jurusan	: TIK – Teknik Informatika dan Komputer
Program Studi	: TMJ – Teknik Multimedia dan Jaringan
Judul Skripsi	: Pengujian Kerentanan Apache Log4j pada CVE-2021-44228 terhadap Ancaman Remote Access Trojan dengan Metode Penetration Testing Execution Standard

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 07 Februari 2023
Yang membuat pernyataan,

Muhammad Nur Irsyad
NIM. 1807422020

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

Nama	: Muhammad Nur Irsyad
NIM	: 1807422020
Jurusan	: TIK – Teknik Informatika dan Komputer
Program Studi	: TMJ – Teknik Multimedia dan Jaringan
Judul Skripsi	: Pengujian Kerentanan Apache Log4j pada CVE-2021-44228 terhadap Ancaman Remote Access Trojan dengan Metode Penetration Testing Execution Standard

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Kamis tanggal 26 bulan Januari tahun 2023 dan dinyatakan **LULUS**.

Disahkan oleh:

Pembimbing I	: Ariawan Andi Suhandana, S.Kom., M.T.I.	(.....)
Penguji I	: Dr. Prihatin Oktivasari, S.Si., M.Si.	(.....)
Penguji II	: Ayu Rosyida Zain, S.ST., M.T.	(.....)
Penguji III	: Fachroni Arbi Murad, S.Kom., M.Kom.	(.....)

Mengetahui:

Jurusan Teknik Informatika dan Komputer
Ketua,

Dr. Anita Hidayati, S.Kom., M.Kom.
NIP. 197908032003122003

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya lah, penulis dapat menempuh masa perkuliahan hingga akhir dan menyusun laporan skripsi ini sampai selesai. Penulis juga menyadari bahwa masa tersebut dapat dilewati dengan maksimal karena bantuan moral dan bimbingan yang kuat dari berbagai pihak yang terlibat. Oleh karena itu, penulis akan mencoba menggunakan kesempatan ini untuk mengucapkan terima kasih kepada pihak-pihak sebagai berikut:

1. Ibu Anita Hidayati, S.Kom., M.Kom., selaku ketua jurusan, dan Bapak Mauldy Laya, S.Kom., M.Kom. selaku mantan ketua jurusan, Teknik Informatika dan Komputer di Politeknik Negeri Jakarta
2. Bapak Defiana Arnaldy, S.Tp., M.Si., selaku ketua program studi dalam Teknik Multimedia dan Jaringan di Politeknik Negeri jakarta
3. Bapak Ariawan Andi Suhandana, S.Kom., M.T.I, selaku dosen pembimbing yang telah menyediakan waktunya untuk membantu penulis dalam segala aspek penyusunan laporan skripsi ini
4. Rekan kolega kelas 1NAP1 serta seluruh tugas pengajar dan staff dari CCIT-FTUI dan Politeknik Negeri Jakarta
5. Orang tua dan keluarga, selaku pihak internal yang memberi dukungan penulis untuk terus berusaha dan berdoa dalam setiap kegiatan

Akhir kata, semoga laporan ini memiliki ilmu yang bermanfaat bagi para pembaca, serta penulis berharap Tuhan Yang Maha Esa dapat terus membalas segala kebaikan dan memberikan kesehatan yang baik untuk semua pihak.

Penulis,

Muhammad Nur Irsyad
NIM. 1807422020

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, Saya yang bertanda tangan di bawah ini:

Nama	: Muhammad Nur Irsyad
NIM	: 1807422020
Jurusan	: TIK – Teknik Informatika dan Komputer
Program Studi	: TMJ – Teknik Multimedia dan Jaringan

Demi mengembangkan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul:

Pengujian Kerentanan Apache Log4j pada CVE-2021-44228 terhadap Ancaman RemoteAccess Trojan dengan Metode Penetration Testing Execution Standard

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini, Politeknik Negeri Jakarta berhak menyimpan, mengalihmediakan / memformatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis / pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyatan ini saya buat dengan sebenarnya.

Depok, 07 Februari 2023
Yang membuat pernyataan,

Muhammad Nur Irsyad
NIM. 1807422020

Pengujian Kerentanan Apache Log4j pada CVE-2021-44228 terhadap Ancaman RemoteAccess Trojan dengan Metode Penetration Testing Execution Standard

ABSTRAK

Salah satu ancaman siber berskala global pada akhir 2021 disebabkan oleh kerentanan Apache Log4j dengan referensi CVE-2021-44228, yang membuat penyerang dapat membentuk remote access ke dalam sistem target dengan memanfaatkan lemahnya netralisasi dari ekspresi input pengguna. Dikarenakan tingginya kefektifan eksploitasi, penelitian diupayakan untuk dapat mengembangkan kerentanan yang dikemas sebagai Remote Access Trojan (RAT); menjadikannya media eksploitasi yang independen dan terbahrukan tanpa terpengaruhi oleh patch yang tersedia. Proses penelitian dimulai dengan membangun dan merancang seluruh instrumen penelitian yang akan diujikan dalam metode Penetration Testing Execution Standard. Metode tersebut meliputi pemodelan vektor serangan menggunakan attack tree, hingga melakukan eksploitasi. Vektor serangan yang digunakan yaitu Hands-on-Keyboard pada aplikasi pengguna, serta BadUSB sebagai distribusi payload RAT-nya. Setelah menyelesaikan tujuan akhir eksploitasi, yaitu mendapatkan rekamanan aktivitas pengguna, pengujian dieskalasi untuk membangun backdoor dengan payload RAT yang disisipkan pada berkas di dalam sistemnya. Mitigasi yang digunakan juga mengadaptasi rekomendasi vendor, seperti penghapusan fungsi JNDI lookup dan pengamanan koneksi inbound. Hasil analisis akhir pengujian berupa data dari sumber daya sistem yang direkam dalam tiga fase, yaitu pra-eksploitasi, pasca-eksploitasi dan pasca-mitigasi. Data tersebut menunjukkan bahwa adanya pemakaian sumber daya yang relatif lebih rendah dengan menggunakan vektor BadUSB daripada Hands-on-Keyboard, dengan kapabilitas dan fleksibilitas serangan yang sama memumpuni.

Kata Kunci: Apache Log4j, CVE-2021-44228, Remote Access Trojan, Penetration Testing Execution Standard, White-box Testing.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam dunia siber, potensi ancaman serangan dapat muncul dikarenakan terdapatnya celah kerentanan dalam suatu sistem maupun aplikasi. Hal ini membuat target dapat dieksploitasi penyerang melalui berbagai vektor serangan yang sesuai dengan dilandasi berbagai macam latar belakang (Calín et al., 2020). Salah satu dampak ancaman siber, yaitu kebocoran data internal, dapat disebabkan dikarenakan adanya kerentanan sistem yang membuat suatu *malware* tertanam di dalam sistem target. Dampak dari eksploitasi tersebut salah satunya dapat memberikan penyerang suatu kapabilitas untuk mengontrol sistem target secara jarak jauh, tanpa dibutuhkannya supervisi pengguna sistem secara langsung (Yin & Khine, 2019).

Salah satu kasus ancaman siber yang muncul pada akhir November 2021 dengan penyebab yang serupa disebabkan oleh kerentanan Log4Shell, yaitu istilah untuk kerentanan *library* Apache Log4j terhadap eksploitasi *remote shell*. Hal ini lalu dikonfirmasi oleh perusahaan Oracle pada 10 Desember 2021, yang menyatakan bahwa kerentanan dengan referensi CVE-2021-44228 tersebut disebabkan melalui penyalahgunaan ekspresi khusus dalam fitur *logging*-nya. Mekanisme eksploitasi tersebut diawali dengan sistem target mengunduh dan menjalankan berkas *malware* dalam bahasa pemrograman Java, untuk kemudian membangun koneksi jarak jauh secara penuh, baik itu berpola *reverse shell* maupun *bind shell*, tanpa ada autentikasi di antaranya (Apache, 2021; CVE, 2021; Khan & Neha, 2016; Oracle, 2021).

Tingkat ancaman juga terefleksikan dengan didapatkannya *Common Vulnerability Scoring System* (CVSS) dalam nilai tertinggi dari seluruh kerentanan Apache Log4j yang pernah dipublikasikan, yaitu bernilai 10.0 dengan status kritis (Apache, 2021). Kerentanan juga mengancam salah satu perusahaan global, yaitu Cisco, dengan 60 lebih produk yang rentan dikarenakan integrasinya dengan *library* tersebut, baik pada *platform* layanan *cloud* maupun aplikasinya (Cisco, 2021). Kedua pernyataan tersebut secara tidak langsung menggambarkan tingginya efisiensi serangan dan luasnya implementasi kerentanan untuk dijadikan area eksplotasi. Walaupun sudah

ada mitigasi valid melalui *patch* yang dikeluarkan vendor, kerentanan tersebut pada dasarnya tetap dapat dimanfaatkan untuk penyerangan melalui pendekatan yang berbeda. Maka dari itu, penelitian ini ditunjukkan untuk adanya pengembangan terhadap pembentukan vektor serangannya. Dengan begitu, tidak hanya *library* Apache Log4j dapat dieksploitasi seperti pada umumnya, namun kerentanannya juga berpotensi untuk berperan sebagai media dari penyerangan itu sendiri.

Berdasarkan uraian di atas, penelitian ini ditunjukkan untuk diadakannya pengujian kerentanan pada *library* Apache Log4j yang didasarkan dari referensi CVE-2021-44228 dalam upaya pengembangan model eksploitasinya. Pengembangan tersebut dilakukan dengan kerentanan yang dikemas dalam ancaman *Remote Access Trojan* (RAT) melalui vektor serangan BadUSB. Seluruh rangkaian eksploitasi nantinya didasarkan pada metode *Penetration Testing Execution Standard* (PTES) sebagai panduan pengujian dan analisisnya. Analisis akhir penelitian berupa perbandingan dampak dari pemakaian sumber daya sistem target dalam dua penggunaan *library* Apache Log4j yang berbeda, yaitu kerentanan sebagai target eksploitasi penyerang, dan kerentanan sebagai vektor untuk penyerang melakukan eksploitasinya.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang dipaparkan di atas, maka rumusan masalah dalam penelitian dapat dijabarkan sebagai berikut:

1. Bagaimana tahap rancang bangun instrumen pengujian dan integrasinya dengan *library* Apache Log4j yang sesuai pada referensi CVE-2021-44228?
2. Bagaimana pendekatan pengujian serta mitigasi pada kerentanan Apache Log4j terkait ancaman RAT, yang didasarkan dalam metode PTES?
3. Bagaiamana analisis kondisi sumber daya sistem target terhadap seluruh fase pengujian yang dilakukan dalam dua vektor serangan yang berbeda?

1.3 Batasan Masalah

Adanya pembatasan suatu masalah digunakan untuk menghindari pelebaran pokok masalah dari lingkup yang seharusnya. Dengan begitu, perumusan batasan masalah dapat membuat penelitian menjadi lebih terarah untuk mencapai tujuannya. Beberapa batasan masalah dalam penelitian ini dijabarkan sebagai berikut yang telah disesuaikan dengan setiap rumusan masalahnya:

1. Batasan dalam perancangan instrumen pengujian
   a) Komponen esensial yang berperan pada proses pengujian adalah mesin *Laptop* yang berbasiskan OS Linux pada distro Linux Mint, terdapatnya program Java, serta tersedianya minimal satu slot USB *type*-A
   b) *Framework* Java yang digunakan untuk membangun aplikasi pengguna dan penyerang adalah Maven, dengan *library* Apache Log4j pada versi 2.14.1 dan Java 8 pada versi 1.8.0_351 build 10. Berdasarkan poin a, seluruh *payload*, program, serta seluruh perintah pada skrip pendukung akan disesuaikan hanya pada lingkungan Linux
2. Batasan dalam implementasi pengujian dan mitigasinya
   a) Pengujian dilakukan dalam lingkup *white-box testing* yang berbasiskan metode PTES. Dua vektor serangan yang digunakan yaitu *Hands-on-Keyboard*, untuk menyerang aplikasi target, dan BadUSB, untuk menyerang sistem target. Hal yang membedakan di antara keduanya yaitu bentuk pemanfaatan dan implementasi dari *library* Apache Log4j pada perspektif penyerang serta target pengujian
   b) Bentuk mitigasi dibedakan pada lingkup aplikasi target dan sistem target, yang mana mencangkup analisis kode statis, seperti pengaturan konfigurasi dari dependensi Apache Log4j dan netralisasi input ekspresi pada aplikasi, serta pengamanan utilitas *firewall* sistem dan restriksi akses pada layanan `cron`
   c) Proses pengujian dilakukan dalam 2 tahap, yaitu pra dan pasca mitigasi, sehingga tergambarnya pencapaian yang dapat dianalisa terhadap besar dampak sumber daya pada sistem target dari pengujian melalui kedua vektor serangan tersebut
3. Batasan dalam mengukur kondisi sumber daya sistem pada mesin target
   a) Pemantauan sumber daya dilakukan pada 3 tahap periode. yaitu saat sistem dalam kondisi normal, serta pasca-eksploitasi dan pasca-mitigasi
   b) Kategori parameter sumber daya sistem yang diukur yaitu utilitas CPU, okupasi memori, utilitas jaringan, serta performa *disk*, yang direkam untuk setiap skenario atau fase pengujian terhadap vektor serangannya

1.4 Tujuan dan Manfaat

Berdasarkan rumusan masalah yang telah dipaparkan, adapun tujuan serta manfaat yang ingin dicapai dalam pembentukan penelitian ini. Tujuan penelitian dijabarkan sebagai berikut:

1. Memberikan bentuk kontribusi terhadap pengembangan *Proof-of-Concept* (PoC) pada kerentanan *library* Apache Log4j pada CVE-2021-44228, terkhusus dalam pengembangannya terhadap ancaman RAT melalui vektor serangan BadUSB. Dengan begitu, maka terdapatnya pembaharuan dalam arah dari penggunaan kerentanan tersebut untuk tidak hanya menjadi objek eksploitasi yang dapat diserang melalui vektor *Hands-on-Keyboard*
2. Menganalisis signifikansi perubahan dari kondisi sumber daya sistem target terhadap eksploitasi dan mitigasi yang diberikan, beserta perbandingannya dari dua vektor serangan yang diujikan

Berdasarkan tujuan penelitian yang hendak dicapai, diharapkan pula adanya manfaat dari penelitian ini baik secara teoretis dan praktis, yaitu sebagai berikut:

1. Bagi masyarakat, penelitian ini diharapkan dapat memberikan wawasan terkait pentingnya kerentanan terhadap teknologi yang digunakan pada aplikasi sehari-hari oleh pengguna, dan besarnya dampak potensi kerusakan dari ancaman serangannya
2. Bagi praktisi keamanan, penelitian ini diharapkan dapat memberikan adanya sumbangan pemikiran pada analisis keamanan dalam dunia siber, serta sebagai dasar tambahan dalam mengkaji lebih lanjut pengembangan kerentanan Apache Log4j pada referensi CVE-2021-44228
3. Bagi penulis, penelitian ini digunakan sebagai bentuk implementasi dari pengembangan ilmu yang dipelajari selama masa kuliah di Politeknik Negeri Jakarta, serta diharapkan dapat memberikan kontribusi referensi kepustakaan terkait keamanan siber pada lingkungan kampus

1.5 Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini mendeskripsikan latar belakang serta urgensi masalah, perumusan masalah, batasan penelitian, tujuan & manfaat penelitian, serta struktur penelitian

BAB II TINJAUAN PUSTAKA

Bab ini membahas landasan teori yang digunakan dalam pembahasan penelitian dari sumber yang kredibel. Adapun penjabaran terkait penelitian sejenis sebagai penunjang dari penelitian sebelumnya dalam waktu 10 tahun terakhir

BAB III METODE PENELITIAN

Bab ini memaparkan atribut inti dari penelitian, seperti metode yang digunakan dalam melakukan penelitian, tahapan dalam mendapatkan hasil pengujian dan analisisnya, serta penjelasan singkat terhadap objek yang diteliti dalam penelitian

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjabarkan mengenai bagaimana tahapan dalam merancang, membangun, instrumen pengujian, melakukan pengujian pada program dan kerentanan sistem, serta mengevaluasi dan menganalisis hasil pengujiannya

BAB V PENUTUP

Bab penutup menjelaskan mengenai pembuktian terhadap rumusan masalah yang ingin dicapai dalam penelitian dan garis besar dari hasil analisis yang dapat diambil. Adapun saran pribadi yang diberikan terkait dengan hasil pengujian yang sifatnya konstruktif untuk topik penelitian dapat dikembangkan lebih lanjut

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan proses pengujian serta hasil analisis yang didapatkan dalam pembahasan sebelumnya, berikut merupakan bentuk kesimpulan yang disesuaikan dengan rumusan masalah terhadap laporan penelitian ini:

1. Perancangan serta pembangunan instrumen pengujian dimulai dengan mendefinisikan topologi jaringan, mendesain skema penyimpanan *payload*, serta menggambarkan alur kerja komponen aplikasi dan layanannya. Terkait dengan integrasinya pada *library* Apache Log4j, terdapat dua spesifik instrumen yang berperan penting dalam jalannya tahap eksploitasi, yaitu aplikasi *desktop* GUI sebagai target pengujian pada sisi pengguna, serta aplikasi layanan HTTP Java sebagai bagian dari vektor serangan BadUSB pada sisi penyerang. Untuk dapat menyesuaikan dengan konteks kerentanan dalam referensi CVE-2021-44228, kedua instrumen utama tersebut menggunakan *library* Apache Log4j pada versi 2.14.1 sebagai tahap integrasinya
2. Rangkaian pengujian melalui metode PTES meliputi pemindaian dan analisis kerentanan serta pemodelan vektor serangan dalam diagram *attack tree*. Adanya pendekatan dalam lingkup *white-box testing* memberikan penguji kapabilitas untuk mengakses informasi secara penuh dalam merumuskan kegiatan tersebut. Selain pengujian dalam aplikasi target, adapun implementasi dari ancaman RAT berupa layanan *payload* yang didistribusikan melalui perangkat BadUSB untuk berjalan di belakang latar sistem target. Tolak ukur keberhasilan dari eksploitasi ditandai dengan didapatkannya aset berupa tangkapan aktivitas pengguna, yang mencangkup pengambilan gambar layar laptop dan kamera, serta perekaman audio mikropon. Eskalasi pada tahap tersebut berupa penstabilan *remote access* yang telah didapatkan melalui implementasi *backdoor* pada RAT yang tersisip pada berkas gambar milik pengguna. Berdasarkan kedua vektor serangan yang ditunjukkan, yaitu HoK dan BadUSB, pendekatan mitigasi yang diambil yaitu dengan mereferensikan cangkupan area dari serangan

tersebut, yang meliputi perubahan konten konfigurasi dan dependensi, penggunaan netralisasi input pengguna, serta pengamanan utilitas *firewall* dan layanan `cron`

3. Terkait proses pengujiannya, adapun tahap pengambilan data terhadap sumber daya sistem yang meliputi fase pra-eksploit, pasca-eksploit dan pasca-mitigasi. Informasi yang telah dikumpulkan kemudian dikatagorikan menjadi beberapa parameter pengukuran, utilitas CPU, okupasi memori, utilitas jaringan, serta performa *disk*. Hasil data dari pengujian tersebut menunjukkan bahwa terdapatnya penggunaan sumber daya sistem yang relatif lebih rendah dengan penggunaan vektor BadUSB dibandingkan HoK, yang mana tetap dapat meraih tujuan pengujian yang sama dalam pemanfaatan *library* Apache Log4j yang berbeda. Selain itu, hasil terhadap keefektifan dari seluruh prioritas mitigasi yang diaplikasikan telah direfleksikan dengan nilai dari parameter pada fase ketiga yang kiranya relatif mendekati stabil dalam mencegah kedua vektor serangan tersebut

5.2 Saran

Pada penelitian ini, disimpulkan bahwwa kerentanan *library* Apache Log4j dalam referensi CVE-2021-44228 tidak hanya dapat dieksploitasi dari sisi pengguna, namun memiliki potensi untuk menjadi vektor serangan yang tersendiri pada sisi penyerang. Dengan adanya integrasi layanan yang sifatnya modular, ancaman yang dikemas dalam serangan RAT tersebut dapat dikembangkan untuk meraih aset target yang lebih besar dalam utilitas yang lebih kuat, seperti pemanfaatan *rootkit* untuk menyembunyikan proses *payload* yang berjalan di belakang latar. Adapun harapan agar penelitian ini bisa menjadi pijakan referensi untuk pengembangan lebih lanjut, baik dalam sisi analisis motde pengujiannya ataupun analisis teradap perbandingan hasil dari setiap fase pengujian yang dilakukan.

DAFTAR PUSTAKA

Apache. (2021). *Apache Log4j Security Vulnerabilities, Apache Software Foundation*. https://logging.apache.org/log4j/2.x/security.html

Apache. (2022a). *Apache Log4j 2 v. 2.17.2 User's Guide, Apache Software Foundation*. https://logging.apache.org/log4j/2.x/log4j-users-guide.pdf'

Apache. (2022b). *Changes - Release History, Apache Software Foundation*.

Bojović, P. D., Bašičević, I., Pilipović, M., Bojović, Ž., & Bojović, M. (2019). *The rising threat of hardware attacks: A keyboard attack case study*. *November*, 1–7. https://www.researchgate.net/publication/331312670

Calín, M., Anchez, S. ´, Carrillo De Gea, J. M., Jos´, J., Luis, J., Fern´fernández-Alemán, F., Alemán, A., Jes´, J., Garcerán, J., Garcerán, G., & Toval, A. (2020). *Software Vulnerabilities Overview: A Descriptive Study, Tsinghua Science and Technology*. https://doi.org/10.26599/TST.2019.9010003

CEH. (2013). *Trojans and Backdoors - Module 06, EC-Council*. http://security watch.pcmag.com

Cisco. (2021). *Vulnerabilities in Apache Log4j Library Affecting Cisco Products: December 2021*. https://tools.cisco.com/security/center/content/CiscoSecurity Advisory/cisco-sa-apache-log4j-qRuKNEbd

CVE. (2021). *CVE-2021-44228, CVE Mitre Org.* https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228

CWE. (2022, October 13). *CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection'), CWE Mitre Org.* https://cwe.mitre.org/data/definitions/917.html

Dalalana, D. B., & Zorzo, A. F. (2017). Overview and Open Issues on Penetration Test. *Journal of the Brazilian Computer Society*, *23*(1). https://doi.org/10.1186/s13173-017-0051-1

FIRST. (2019). *Common Vulnerability Scoring System version 3.1 Specification Document Revision 1*. 1–24. https://www.first.org/cvss/

Hama Saeed, M. A. (2020). Malware in Computer Systems: Problems and Solutions. *IJID (International Journal on Informatics for Development)*, *9*(1), 1. https://doi.org/10.14421/ijid.2020.09101

Helmke, M., Hudson, A., & Hudson, P. (2019). *Ubuntu Unleashed: 2019 Edition, Pearson Education, Inc.*

HHS. (2022). *Log4j Vulnerabilities and the Health Sector, HHS Cybersecurity Program*.

Hiesgen, R., Nawrocki, M., Schmidt, T. C., & Wählisch, M. (2022). *The Race to the Vulnerable: Measuring the Log4j Shell Incident*. http://arxiv.org/abs/2205.02544

Ingoldsby, T. R. (2021). *Attack Tree-based Threat Risk Analysis, Amenaza Technologies Limited*. www.amenaza.com

Ismail, N. M. (2020). *Rancang Bangun Aplikasi Gamifikasi Untuk Hafalan Al-Quran Menggunakan Audio Fingerprint Berbasis Android*.

Khadadiya, N. (2021, December 27). *Log4Shell Simplified - All you need to know about Log4j CVE-2021-44228, InfoSec Write-ups*. https://infosecwriteups.com/log4shell-simplified-all-you-need-to-know-about-cve-2021-44228-3c70d59c307a

Khan, A., & Neha, R. P. (2016). Analysis of Penetration Testing and Vulnerability in Computer Networks. *GRD Journals-Global Research and Development Journal for Engineering* |, *1*(6). www.eeye.com

LiveAction. (2022). *Hands On Keyboard Attack: Why Detection Just Became Critical*. https://www.liveaction.com/resources/blog/hands-on-keyboard-attack-why-detection-just-became-critical/#:~:text=A hands-on keyboard attack, other end of this technique.

Madhavi, D. (2016). A White Box Testing Technique in Software Testing: Basis Path Testing. *Journal for Research*, *2*(4), 12–17. www.journalforresearch.org

Maji, S., Jain, H., Pandey, V., & Siddiqui, A. (2022). *White Hat Security-An Overview of Penetration Testing Tools*. https://ssrn.com/abstract=4159095

Maraj, A., Rogova, E., & Jakupi, G. (2020). Testing of Network Security Systems through DoS, SQL Injection, Reverse TCP and Social Engineering Attacks. In *Int. J. Grid and Utility Computing* (Vol. 11, Issue 1). https://doi.org/10.1504/IJGUC.2020.103976

Nanny, Prayudi, Y., & Riadi, I. (2019). Peningkatan Keamanan Data Terhadap Serangan Remote Access Trojan (RAT) pada Cybercriminal Menggunakan Metode Dynamic Static. *Jurnal Instek*, *4*(2), 161–170.

Ningsih, S. W. (2021). Analisis Pengujian Kerentanan Situs Pemerintahan XYZ dengan PTES. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *8*(3), 1543–1556. https://doi.org/10.35957/jatisi.v8i3.1224

OMG. (2011a). *Activity Diagrams*. https://www.uml-diagrams.org/activity-diagrams.html

OMG. (2011b). *UML Class and Object Diagrams Overview*. https://www.uml-diagrams.org/class-diagrams-overview.html

Oracle. (2010a). *Controlling Access to the crontab Command, Oracle Corporation*. https://docs.oracle.com/cd/E19253-01/817-0403/sysrescron-23/index.html

Oracle. (2010b). *inetOrgPerson Object Class, Oracle Corporation*. https://docs.oracle.com/cd/E19225-01/820-6551/bzbpb/index.html

Oracle. (2021). *Oracle Security Alert Advisory - CVE-2021-44228, Oracle Corporation*. https://www.oracle.com/security-alerts/alert-cve-2021-44228.html

PTES. (2021). *The Penetration Testing Execution Standard Documentation - Release 1.1, The PTES Team*. https://pentest-standard.readthedocs.io/en/latest/tree.html

Rajasinghe, R. (2022). *Remote Code Execution Security Flaw in Apache Log4j2*. *May*. https://doi.org/10.13140/RG.2.2.14272.20486

Roy, U. K. (2015). *Advanced Java programming, Oxford University Press*. https://india.oup.com/product/advanced-java-programming-9780199455508

Saroeval, M., & Bhadola, S. (2022). *Network Utility Tools Best Practices*. *9*(6), 96–103.

Shevchenko, N., Chick, T. A., O'riordan, P., Scanlon, T. P., & Woody, C. (2018). *Threat Modeling: A Summary Of Available Methods, Carneige Mellon University: Software Engineering*.

Sukic, C., & Saracevic, M. (2012). UML and JAVA as effective tools for implementing algorithms in computer graphics. *Tem Journal*, *1*(2), 111.

Yin, K. S., & Khine, M. A. (2019). Optimal Remote Access Trojans Detection Based on Network Behavior. *International Journal of Electrical and*

Computer Engineering, *9*(3), 2177–2184. https://doi.org/10.11591/ijece.v9i3.pp2177-2184

ZyTrax. (2022). *LDAP for Rocket Scientists, ZyTrax Inc.* https://www.zytrax.com/books/ldap/

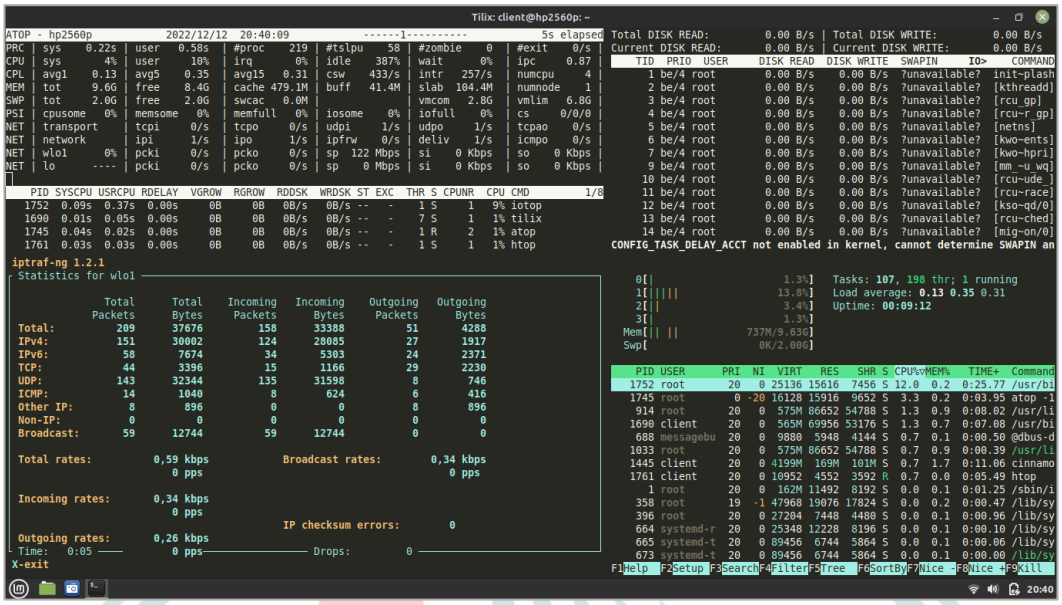
LAMPIRAN

L1 – Daftar riwayat hidup

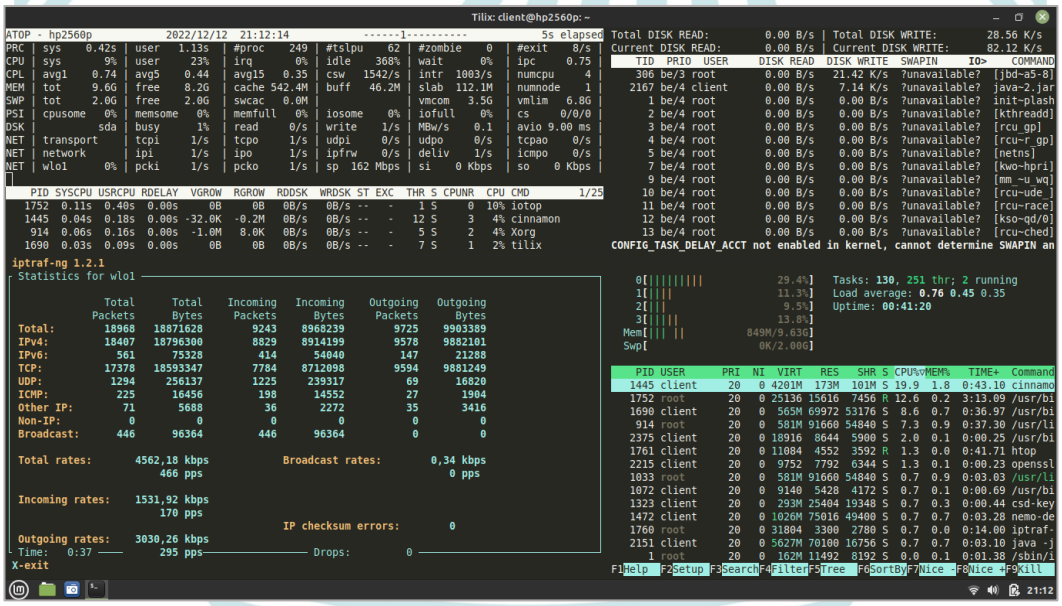
Muhammad Nur Irsyad

Menempuh pendidikan dasar di SDI An-Nizomiyah hingga tahun 2011 dan di SD YPVDP Bontang tahun 2012, pendidikan menengah di SMP YPVDP Bontang tahun 2015 dan di SMAI Al-Azhar 2 Pejaten hingga tahun 2018. Saat ini, penulis menempuh pendidikan kerja sama di CCIT-FTUI dan Politeknik Negeri Jakarta pada program D4, dalam jurusan Teknik Informatika dan Komputer,

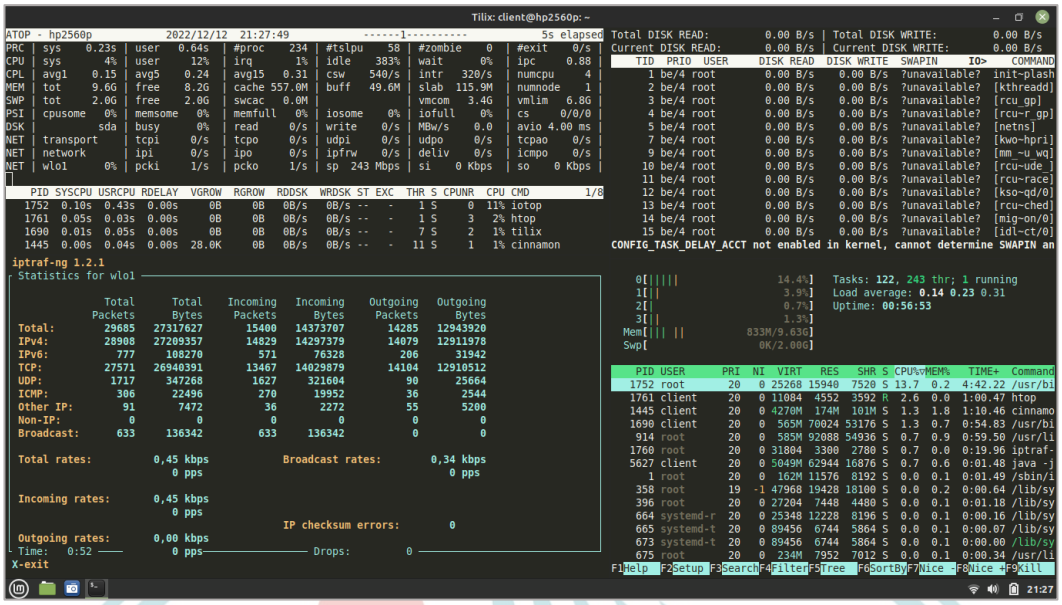
L2 – Sumber daya sistem target (pra-eksplotasi) pada vektor serangan BadUSB



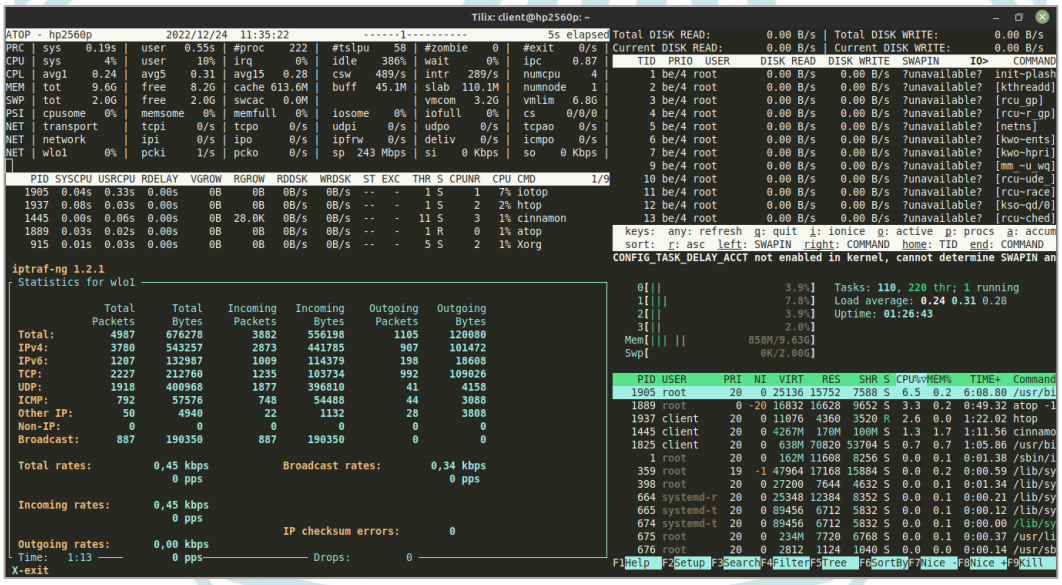
L3 – Sumber daya sistem target (pasca-eksplotasi) pada vektor serangan BadUSB



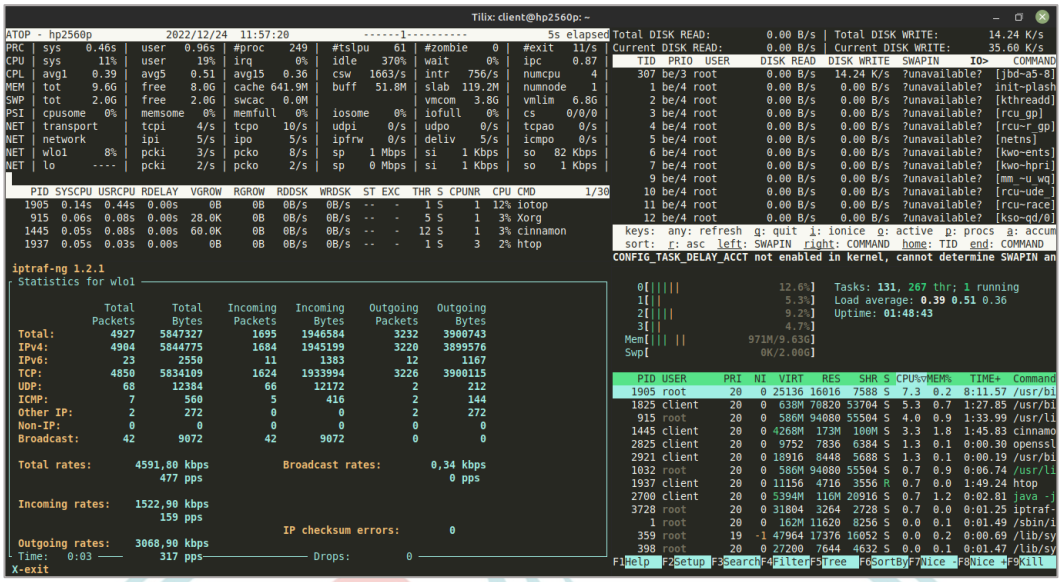
L4 – Sumber daya sistem target (pasca-mitigasi) pada vektor serangan BadUSB



L5 – Sumber daya sistem target (pra-eksplotasi) pada vektor serangan HoK



L6 – Sumber daya sistem target (pasca-eksplotasi) pada vektor serangan HoK



L7 – Sumber daya sistem target (pasca-mitigasi) pada vektor serangan HoK