

**ANALISIS 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**

**2022**



**ANALISIS 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 Gelar Sarjana Terapan Politeknik**

**MUHAMMAD NUR IRSYAD**

**1807422020**

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN**

**JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER**

**POLITEKNIK NEGERI JAKARTA**

**2022**

1. SURAT PERNYATAAN BEBAS PLAGIARISME
2. Saya yang bertanda tangan di bawah ini:
3. Nama : Muhammad Nur Irsyad
4. NIM : 1807422020
5. Jurusan : TIK - Teknik Informatika dan Komputer
6. Program Studi : TMJ - Teknik Multimedia dan Jaringan
7. Judul Skripsi : Analisis Kerentanan Apache Log4j pada CVE-
8. 2021-44228 terhadap Ancaman Remote Access Trojan dengan Metode Penetration Testing
9. Execution Standard
10. Menyatakan dengan sebenarnya bahwa skripsiini 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.
11. Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung cirri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatantersebut.
12. Depok, \_\_ \_\_\_\_ 2022
13. Yang membuat pernyataan,
14. Muhammad Nur Irsyad
15. NIM. 1807422020
16. lembar pengesahan
17. Skripsi diajukan oleh:
18. Nama : Muhammad Nur Irsyad
19. NIM : 1807422020
20. Program Studi : TMJ - Teknik Multimedia dan Jaringan
21. Judul Skripsi : Analisis Kerentanan Apache Log4j pada CVE-
22. 2021-44228 terhadap Ancaman Remote Access Trojan dengan Metode Penetration Testing
23. Execution Standard
24. Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari \_\_, tanggal \_\_, bulam \_\_\_\_, tahun \_\_, dan dinyatakan **LULUS**.
25. Disahkan oleh:
26. Pembimbing I : Ariawan Andi Suhandana, S.Kom., M.T.I. ( . . . . . . . . . . )
27. Penguji I : Defiana Arnaldy, S.Tp., M.Si. ( . . . . . . . . . . )
28. Penguji II : Fachroni Arbi Murad, S.Kom., M.Kom. ( . . . . . . . . . . )
29. Penguji III : Asep Kurniawan, S.Pd., M.Kom. ( . . . . . . . . . . )
30. Mengetahui:
31. Jurusan Teknik Informatika dan Komputer
32. Ketua
33. Mauldy Laya , S.Kom., M.Kom.

NIP. 197802112009121003

1. KATA PENGANTAR
2. Aaa
3. Depok, \_\_ \_\_\_\_ 2022
4. Muhammad Nur Irsyad
5. SURAT PERNYATAAN PERSETUJUAN PUBLIKASI
6. SKRIPSI UNTUK KEPENTINGAN AKADEMIS
7. Sebagai sivitas akademik Politeknik Negeri Jakarta, Saya yang bertanda tangan di bawah ini:
8. Nama : Muhammad Nur Irsyad
9. NIM : 1807422020
10. Jurusan : TIK - Teknik Informatika dan Komputer
11. Program Studi : TMJ - Teknik Multimedia dan Jaringan
12. Demi mengembangkan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul:
13. Analisis Kerentanan Apache Log4j pada CVE-2021-44228 terhadap Ancaman Remote Access Trojan dengan Metode Penetration Testing Execution Standard
14. Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalihmediakan / formatkan, 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.
15. Depok, \_\_ \_\_\_\_ 2022
16. Yang membuat pernyataan,
17. Muhammad Nur Irsyad
18. NIM. 1807422020
19. ABSTRAK
20. Aaa
21. **Kata kunci**: aaa
22. DAFTAR ISI

[SURAT PERNYATAAN BEBAS PLAGIARISME 3](#__RefHeading___Toc367_39133471121)

[lembar pengesahan 4](#__RefHeading___Toc367_391334711211)

[KATA PENGANTAR 5](#__RefHeading___Toc367_39133471122)

[SKRIPSI UNTUK KEPENTINGAN AKADEMIS 6](#__RefHeading___Toc13633_770190716)

[ABSTRAK 7](#__RefHeading___Toc367_39133471123)

[DAFTAR ISI 8](#__RefHeading___Toc367_3913347112)

[DAFTAR gambar 9](#__RefHeading___Toc367_39133471124)

[DAFTAR TABEL 10](#__RefHeading___Toc367_391334711241)

[pendahuluan 11](#__RefHeading___Toc369_3913347112)

[1.1 Latar Belakang 11](#__RefHeading___Toc371_3913347112)

[1.2 Rumusan Masalah 14](#__RefHeading___Toc371_39133471121)

[1.3 Batasan Masalah 14](#__RefHeading___Toc371_391334711216)

[1.4 Tujuan dan Manfaat 15](#__RefHeading___Toc371_3913347112163)

[1.5 Sistematika Penulisan 16](#__RefHeading___Toc371_39133471121631)

[1.1.1 Setelah Pendahuluan 18](#__RefHeading___Toc373_3913347112)

[1.1.1.1 Apelagi Si 18](#__RefHeading___Toc375_3913347112)

[DAFTAR pustaka 19](#__RefHeading___Toc367_3913347112411)

1. DAFTAR gambar
2. DAFTAR TABEL

BAB 1

1. pendahuluan
2. 1.1 Latar Belakang

Selama dua dekade lebih, kehadiran internet menjadi salah satu faktor penting dalam terintegrasinya komunikasi secara global. Setiap tindakan bisnis, ekonomi, dan sosial dari berbagai macam lapisan masyarakat mayoritas sudah dilakukan dalam lingkup siber ini. Dengan adanya faktor akses internet yang mudah didapatkan, banyaknya aktor siber yang semakin mudah terhubung antara satu sama lain, seperti organisasi pemerintahan, masyarakat, dan aktivis siber. Tidak hanya itu, hadirnya konsep anonimitas juga berpeluang untuk mengundanng penjahat siber di dalamnya. Dengan demikian, maka hadirlah juga tantangan di dalamnya yang dikenal sebagai ancaman siber (Li and Liu, 2021)⁠(Li and Liu, 2021). Potensi serangan dan ancaman siber ini muncul dikarenakan adanya celah kerentanan terhadap sistem maupun infrastruktur, baik itu dikarenakan oleh kesalahan manusia maupun program dalam logika bisnisnya. Hal tersebut yang kemudian membolehkan sistem untuk diserang melalui berbagai macam perantara yang sesuai dengan bentuk celahnya. Masalah kerentanan ini yang lalu dieksploitasi oleh penyerang dengan landasan untuk manfaat pribadi dan berbagai macam faktor lainnya (Calín *et al.*, 2020)⁠(Calín *et al.*, 2020).

Pada penerapannya, kerentanan-kerentanan yang telah terekspos tersebut akan diklasifikasi dan dievaluasi oleh para praktisi keamanan sistem. Kegiatan ini dilakukan dalam rangka proses identifikasi kerentanan secara resmi untuk nantinya direkam kedalam National Vulnerability Database (NVD) menggunakan referensi Common Vulnerability Exposure (CVE). Untuk memberikan gambaran mengenai besar pengaruh kerentanan terhadap suatu sistem, CVE memanfaatkan suatu standar yaitu Common Vulnerability Scoring System (CVSS). CVSS umum digunakan dalam mengukur dan menganalisa potensi tingkat kerusakan serta dampak dari kerentanan dan ancaman terhadap aset-aset yang dilindungi (Dobrovoljc, Trček and Likar, 2017; Ruohonen, 2019).

Dalam keamanan siber, bentuk aset yang perlu diamankan dapat berupa komputer atau perangkat keras, informasi internal, jaringan, hingga perangkat lunak dari penyalahgunaan otorisasi dari proses bisnis yang seharusnya. Dikarenakan ancaman siber menjadi salah satu isu penting yang selalu berkembang pada skala global, maka hal ini mendorong pula untuk berkembangnya pertahanan pada suatu aset serta kebijakan bisnis perusahaan, terutama dalam mencegah kebocoran data internal (Alghamdi, Cordeiro and Barbosa, 2021). Salah satu penyebab terjadinya kebocoran data adalah adanya kerentanan sistem terhadap serangan malware yang sudah tertanam ke dalam sistem korban, baik dengan mendownload file malware ataupun menerima phising email. Hal ini yang kemudian membuat penyerang dapat mengontrol sistem korban secara jarak jauh untuk mengambil aset dan informasi digital secara transparan terhadap supervisi sistem korban (Yin and Khine, 2019).

Salah satu kasus ancaman siber yang muncul pada akhir November 2021 dengan penyebab yang serupa adalah ancaman Log4Shell, yaitu istilah untuk kerentanan terhadap produk Apache Log4j terhadap serangan remote shell. Hal ini dikonfirmasi oleh Oracle dalam publikasinya pada 10 Desember 2021, yang menjelaskan bahwa kerentanan dengan referensi CVE-2021-44228 tersebut menyebabkan penyerang untuk dapat mengontrol sistem korban melalui penyalahgunaan dalam fitur *logging*. Langkah awal iniyang kemudian digunakan untuk mengunduh dan menjalankan *payload malware* yang dirancang dalam bahasa pemrogramanJava. Adanya eksekusi a*rbitrary code* tersebut yang nantinya akan membangun koneksi remote, baik secara *reverse shell* maupun *bind shell*; secara penuh mengontrol sistem korban tanpa ada autentikasi diantaranya (Khan and Neha, 2016; Apache, 2021; CVE, 2021; Oracle, 2021). Berdasarkan dampaknya. kerentanan tersebut memberikan resiko yang tinggi terhadap perusahaan secara global, seperti Adobe Creative Cloud, Cisco, IBM, hingga Amazon Web Service (AWS). Hal ini.dikarenakan teknologi *open*-*source* tersebut digunakan dalam berbagai *platform*, seperti cloud service, web service dan software development, sehingga ada potensi besar pada pengembangan kerentanan tersebut untuk memaksimalkan serangannya (Nath, 2022).

Selain itu, kerentanan CVE-2021-44228 juga merupakan satu-satunya kerentanan Log4j yang memiliki nilai CVSS tertinggi, yaitu 10.0 dengan status severity critical. Hal yang membuatnya berbeda dari kerentanan Log4j lainnya adalah kerentanan tersebut menjadikannya sebagai pelopor untuk 3 kerentanan Log4j yang baru, yang mana hasil pengembangannya hanya berdurasi kurang dari tiga minggu (26/11/2021 – 11/12/2021). Hal ini berbeda dengan 2 kasus kerentanan sebelum adanya Log4Shell ini, yang mana memiliki periode interval hingga 4 tahun lebih (29/01/2017 – 26/11/2021). Maka dari itu, pengembangan kerentanan pada CVE-2021-44228 tergolong cepat dikarenakan fleksibilitas dan media serangannyayang luas (Apache, 2021).

Dalam rangka mendalami kerentanan tersebut, peneliti berupaya untuk menganalisa ancaman Apache Log4j pada referensi CVE-2021-44228 terhadap pengembangan eksploitasinya. Hal ini dilakukan dengan adanya pengujian pada post exploitation menggunakan ancaman *remote access trojan* dalam bentuk *persistence backdoor.* Keseluruhan tahapan pengujian akanberbasiskan pada model *Penetration* *Testing Execution Standard* (PTES) untuk mendapatkan hasil yang akurat pada suatu lingkup panduan pengujian (Dalalana and Zorzo, 2017). Implementasi pengujian dilakukan dalam serangan *remote code execution* (RCE) dengan memanfaatkan URL *entry manipulation* secara *hands*-*on*-*keyboard* yang didasari pada miskonfigurasi aplikasi serta lemahnya validasi request input pengguna (Biswas *et al.*, 2018). Pengujian kemudian dikembangkan dengan menyisipkan *backdoor* kedalam sistem target untuk dapat mempertahankan akses yang sudah didapatkan. Adapun mitigasi yang diadaptasikan merujuk kepada pendekatan *static* analysis untuk mendeteksi source code dan algoritma program yang menjadi sumber celah kerentanan*,* serta pemanfaatan *system utility* layaknya program dan port monitoring tools*,* dalam meminimalisir ancaman tersebut. Hal tersebut kemudian akan dijadikan sebagai tolak ukur untuk dianalisis mengenai seberapa luas dan besarnya tingkat keberhasilan mitigasi tersebut(CEH, 2013; Muñoz and Mirosh, 2016; Kaushik *et al.*, 2021).

1. 1.2 Rumusan Masalah
2. Berdasarkan latar belakang masalah yang telah dipaparkan di atas, maka rumusan masalah dalam penelitian dapat dijabarkan sebagai berikut:
3. Bagaimana perancangan infrastruktur instrumen dengan integrasi Log4j dalam lingkup white box testing?
4. Bagaimana pendekatan mitigasi terhadap tingkat keberhasilan pengujian ancaman *remote access trojan* pada kerentanan Log4j?
5. 1.3 Batasan Masalah
6. Adanya pembatasan suatu masalah digunakan untuk menghindari potensi pelebaran pokok masalah dari lingkup yang seharusnya, sehingga dapat membuat penelitian lebih terarah untuk tercapainya tujuan dari penelitian ini. Beberapa batasan masalah dalam penelitian ini kemudian dijabarkan sebagai berikut:
7. Batasan dalam perancangan infrastruktur instrumen
   1. Demonstrasi dilakukan dalam lingkup virtual dengan rancangan arsitektur client-server secara lokal (ldap-*server*, GUI *desktop* ldap-*client, attacker machine*) pada platform Linux
   2. Pengujian kerentanan dilakukan dengan pendekatan white box testing, dan hanya ditujukan untuk *library* Log4j dalam versi 2.0-*beta*9 hingga 2.14.1 (Java 8) yang sesuai dengan referensi CVE-2021-44228, sehingga tidak mencangkup *security patch* terakhir, yaitu versi 2.17.1 per tanggal 28/12/2021
8. Batasan dalam implementasi mitigasi dan pengujiannya
   1. Bentuk mitigasi mencangkupi pendekatan *static analysis* serta pemanfaatan *system utility*, tidak mencangkup bentuk pengaplikasian *system update* ataupun *security patch*
   2. Proses pengujian dilakukan dalam 2 tahap, yaitu pra dan pasca adanya mitigasi, sehingga tergambarnya pencapaian yang dapat dianalisa besar tingkat keberhasilannya
9. 1.4 Tujuan dan Manfaat
10. Berdasarkan rumusan masalah dalam sub-bab sebelumnya, maka adapun tujuan serta manfaat yang ingin dicapaikan dalam pembentukan penelitian ini. Tujuan penelitian dijabarkan sebagai berikut:
11. Membangun instrumen penelitian, yang mencangkup keseluruhan infrastruktur baik untuk sisi penyerang dan sisi korban
12. Mampu melakukan keseluruhan proses pengujian dalam white box testing yang spesifik terhadap kerentanan pada versi Log4j pada batasan masalah, sehingga lingkup objek penelitian tidak melebar dari yang ditunjukkan
13. Mampu mengimplementasikan pendekatan mitigasi yang sesuai dengan teknologi dan platform infrastruktur yang diujikan
14. Menyajikan data hasil pengujian yang dapat dianalisis terkait dengan tingkat keberhasilan mitigasi dan dampak pengembangan ancamannya

Berdasarkan tujuan penelitian yang hendak dicapai, diharapkan pula penelitian ini mempunyai manfaat dalam sisi pendidikan, teknologi, serta keamanan dalam general, baik secara langsung maupun tidak langsung. Adapun manfaat penelitian yang dijabarkan sebagai berikut:

1. Manfaat teoretis
   1. Memberikan sumbangan pemikiran pada analisis keamanan siber, baik dari sisi pendekatan serangan serta mitigasinya terhadap kerentanan Log4j dan ancaman pengembangan *remote access trojan*
   2. Sebagai pijakan referensi untuk penelitian sejenis terkait pada kerentanan Log4j kedepannya, serta sebagai kajian lebih lanjut dalam analisis ancaman *remote access trojan* terhadap teknologi Log4j dan tingkat keefektifan terhadap mitigasinya
2. Manfaat praktis
3. Bagi pembaca

Penelitian ini dapat dijadikan sebagai salah satu penggambaran terhadap besarnya dampak kerusakan terhadap kerentanan Log4j yang diharapkan dapat memberikan kewaspadaan pada pemakaian aplikasi yang kiranya memiliki kerentanan serupa

1. Bagi pengembang aplikasi

Penelitian ini dapat membantu memaparkan seberapa jauh eksploitasi kerentanan Log4j dan seberapa efektif pendekatan mitigasinya yang sifatnya temporer dan lebih preventif tersebut

Bagi perusahaan

1. Penelitian ini dapat dijadikan sebagai contoh kasus penjabaran dari dampak kerentanan Log4j terhadap sisi pengguna produk perusahaan yang rentan, sehingga diharapkan bisa memberikan suatu pertimbangan dan kesadaran mengenai pentingnya keamanan dalam sisi infrastruktur
2. 1.5 Sistematika Penulisan
3. Sistematika penulisan berikut dibentuk untuk mempermudah dalam penyusunan proposal penelitian ini dengan penulisan yang baik. Sistematika penulisan yang digunakan dijabarkan sebagai berikut:
4. **BAB 1 PENDAHULUAN**
5. Bab pendahuluan mendeskripsikan mengenai latar belakang serta bagaimana urgensi masalah, perumusan masalah, menentukan batasan-batasan masalah, mendefinisikan tujuan dan manfaat penelitian, serta sistematika struktur penulisan dalam merancang laporan penelitian ini
6. **BAB II TINJAUAN PUSTAKA**
7. Bab tinjauan pustaka berisikan seluruh teori-teori landasan yang digunakan dalam inti pembahasan pada rancangan penelitian dari berbagai sumber yang kredibel. Adapun penjabaran terkait penelitian sejenis yang digunakan sebagai penunjang dan pengembangan dari penelitian yang sebelumnya dalam kurun waktu 10 tahun terakhir
8. **BAB III PERENCANAAN DAN REALISASI**
9. Bab perencanaan dan realisasi menjelaskan tahapan-tahapan yang dilakukan dalam membangun instrumen penelitian dan bagaimana proses pengujian kerentanan dapat berlangsung terhadap objek penelitian menggunakan metodologi ataupun framework yang sudah ditentukan
10. **BAB IV PEMBAHASAN**
11. Bab pembahasan memaparkan bagaimana data yang didapatkan dari hasil pengujian untuk dianalisa menggunakan pendekatan statistika. Metrik penilaian bersifat kualitatif dalam bentuk katagorikal, yaitu dalam bentuk pencapaian ataupun milestone terhadap setiap parameter-parameter dalam pengujian
12. **BAB V PENUTUP**
13. Bab penutup menjelaskan mengenai pembuktian terhadap tujuan yang ingin dicapai dalam penelitian dan bagaimana hasil penelitiannya. Adapun saran yang diberikan terkait dengan hasil pengujian yang sifatnya konstruktif
14. 1.1.1 Setelah Pendahuluan
15. "Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum."
16. 1.1.1.1 Apelagi Si
17. "Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum."
18. "Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum."
19. adwd
20. DAFTAR pustaka
22. Calín, M. *et al.* (2020) *Software Vulnerabilities Overview: A Descriptive Study, Tsinghua Science and Technology*. doi:10.26599/TST.2019.9010003.
23. Li, Y. and Liu, Q. (2021) ‘A Comprehensive Review Study of Cyber-attacks and Cyber Security; Emerging Trends and Recent Developments’, *Energy Reports*, 7, pp. 8176–8186. doi:10.1016/j.egyr.2021.08.126.