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 Diploma Empat Politeknik

MUHAMMAD NUR IRSYAD

1807422020

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
2022

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	: Analisis Kerentanan Apache Log4j Pada CVE-2021-44228 terhadap Ancaman Remote Access Trojan Dengan Metode Penetration Testing Execution Standard

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.

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.

Depok, __ ____ 2022
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	: Analisis 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 __, tanggal __, bulam ____, tahun __, dan dinyatakan **LULUS**.

Disahkan oleh:

Pembimbing I	: Ariawan Andi Suhandana, S.Kom., M.T.I.	(. . . . .)
Penguji I	: Defiana Arnaldy, S.Tp., M.Si.	(. . . . .)
Penguji II	: Fachroni Arbi Murad, S.Kom., M.Kom.	(. . . . .)
Penguji III	: Asep Kurniawan, S.Pd., M.Kom.	(. . . . .)

Mengetahui:

Jurusan Teknik Informatika dan Komputer
Ketua

Mauldy Laya , S.Kom., M.Kom.
NIP. 197802112009121003

KATA PENGANTAR

AA

Depok, __ ____ 2022

Muhammad Nur Irsyad

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:

Analisis Kerentanan Log4Shell pada CVE-2021-44228 terhadap Ancaman Remote Access 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 / 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.

Depok, __ ____ 2022
Yang membuat pernyataan,

Muhammad Nur Irsyad
NIM. 1807422020

ABSTRAK

AA

Kata Kunci: aaa

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam dunia siber, potensi ancaman dapat muncul dikarenakan terdapatnya celah kerentanan pada suatu sistem maupun infrastruktur. Hal tersebut membuat sistem dapat diserang melalui berbagai 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). Salah satu dampak ancaman siber, kebocoran data internal, disebabkan karena kerentanan sistem mnembuat malware boleh tertanam di dalam sistem korban. Hal ini membuat penyerang dapat mengontrol sistem korban secara jarak jauh untuk mengambil aset serta informasi digital secara transparan terhadap supervisi pertahanan sistem korban (Yin and Khine, 2019).

Salah satu kasus ancaman siber yang muncul pada akhir November 2021 dengan penyebab yang serupa adalah kerentanan Log4Shell, yaitu istilah pada kerentanan library Apache Log4j terhadap serangan remote shell. Hal ini juga dikonfirmasi oleh Oracle pada 10 Desember 2021, yang menjelaskan bahwa kerentanan dengan referensi CVE-2021-44228 tersebut menyebabkan penyerang dapat mengontrol sistem korban melalui penyalahgunaan user input dalam fitur logging nya. Langkah awal ini digunakan untuk mengunduh dan menjalankan arbitary code dalam program Java. Adanya eksekusi payload tersebut nantinya dapat membangun koneksi remote secara penuh, baik dengan reverse shell maupun bind shell, tanpa ada autentikasi diantaranya (Khan and Neha, 2016; Apache, 2021; CVE, 2021; Oracle, 2021). Salah satu perusahaan global yang menggunakan library Apache Log4j, Cisco, memiliki lebih dari 60 produk serta fitur yang terpengaruh terhadap kerentanan tersebut. Hal ini didukung karena library Apache Log4j memiliki fleksibilitas dalam implementasinya di berbagai macam platform, seperti cloud service dan software development (Cisco, 2021).

Ancaman global tersebut terefleksikan pada status referensi CVE-2021-44228 yang merupakan satu-satunya kerentanan Apache Log4j dengan nilai Common Vulnerability Scoring System (CVSS) tertinggi, yaitu 10.0. Hal yang juga membuatnya berbeda dari kerentanan Apache Log4j lainnya adalah kerentanan tersebut menjadi pelopor untuk 3 kerentanan Apache Log4j yang baru dalam waktu kurang dari tiga minggu (26/11/2021 – 11/12/2021) (Apache, 2021). Walaupun kerentanan CVE-2021-44228 sudah diperbaiki pada versi Apache Log4j selanjutnya, efesiensi dan efektivitas eksploitasi kerentanan ini tetap dapat dimanfaatkan dari sisi penyerang sebagai media serangan yang kuat dan stabil.

Adapun berdasarkan uraian diatas, penelitian ini ditunjukkan untuk menganalisa ancaman kerentanan Apache Log4j pada referensi CVE-2021-44228 terhadap pengembangan eksploitasinya dengan pendekatan whitebox testing. Pengembangan dilakukan pada pengujian post exploitation menggunakan ancaman Remote Access Trojan secara persistence. Keseluruhan tahapan pengujian berbasiskan pada model Penetration Testing Execution Standard (PTES) sebagai lingkup panduan pengujian dan analisisnya (Dalalana and Zorzo, 2017). Tahap eksploitasi pengujian didasarkan pada serangan Remote Code Execution (RCE) dengan memanfaatkan JNDI Inection. Dua bentuk vektor serangan yang akan digunakan adalah Hands-on-Keyboard dan BadUSB, yang mana keduanya memanfaatkan miskonfigurasi aplikasi atau sistem, serta lemahnya validasi request input pengguna (Biswas *et al.*, 2018). Pengujian kemudian dikembangkan dengan menyisipkan backdoor ke dalam sistem target untuk mempertahankan stabilitas akses, yang mana memanfaatkan kerentanan Apache Log4j sebagai komponen utamanya. Mitigasi yang diadaptasikan merujuk kepada pendekatan static analysis serta pemanfaatan program pemantuan dan konfigurasi internal sistem. Analisis keseluruhan pengujian dilakukan pada hasil eksploitasi dari pasca mitigasi, yang nantinya digunakan sebagai tolak ukur untuk mengetahui seberapa luas dan besarnya tingkat keberhasilan mitigasi terhadap ancaman tersebut (CEH, 2013; Muñoz and Mirosh, 2016; Kaushik *et al.*, 2021).

1.2 Rumusan Masalah

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

1. Bagaimana tahap rancang bangun instrumen pengujian dan integrasinya dengan Apache Log4j yang sesuai dengan referensi CVE-2021-44228?
2. Bagaimana analisa pengujian serta mitigasinya pada kerentanan Apache Log4j terkait ancaman Remote Access Trojan dalam lingkup white box testing dengan berbasiskan metode PTES?
3. Bagaiamana dampak kondisi sumber daya sistem pada pengujian terhadap ancaman Remote Access Trojan?

1.3 Batasan Masalah

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:

1. Batasan dalam perancangan instrumen pengujian
   a) Instrumen dirancang pada model arsitektur client-server secara lokal dengan memanfaatkan virtualisasi Docker container
   b) Framework Java yang digunakan untuk membangun aplikasi utama pengguna dan penyerang adalah Maven, dengan *library* Apache Log4j pada versi 2.14.1 dalam versi Java 8 yaitu 1.8.0_181 dan 1.8.0_321
   c) Mesin komputer yang dipakai berbasiskan platform Linux, sehingga seluruh payload, program, serta skrip akan disesuaikan ke arah tersebut
2. Batasan dalam implementasi pengujian dan mitigasinya
   a) Pengujian dilakukan dengan berbasiskan metode PTES dalam lingkup white box testing. Vektor serangan yang digunakan berlandaskan pada kerentanan Log4Shell, yaitu serangan Hands-on-Keyboard dan BadUSB. Hal yang membedakan diantaranya adalah pemanfaatan kerentanan tersebut dari perspektif penyerang serta target

b) Bentuk mitigasi mencangkup pendekatan deteksi ancaman, dengan implementasi *static analysis,* pemanfaatan program pemantauan serta konfigurasi internal sistem, serta analisis terhadap implementasi pembaharuan versi Apache Log4j pada 2.15.0, 2.16.0, dan 2.17.0
c) Proses pengujian dilakukan dalam 2 tahap, yaitu pra dan pasca adanya mitigasi, sehingga tergambarnya pencapaian yang dapat dianalisa besar tingkat keberhasilannya

3. Batasan dalam mengukur kondisi sumber daya sistem pada mesin target
   a) Pemantauan sumber daya dilakukan pada 3 tahap pengujian. yaitu saat sistem dalam kondisi normal, pre mitigasi, dan pasca mitigasi
   b) Parameter sumber daya yang diukur adalah CPU Utilization, CPU Time Consumption, Memory Occupation, Network Utilization, Disk Read & Write, dan User's Activity

1.4 Tujuan dan Manfaat

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

1. Memberikan adanya suatu kontribusi pengembangan Proof-of-Concept (PoC) terhadap ancaman Apache Log4j pada CVE-2021-44228, terkhusus dalam pengembangan Remote Access Trojan
2. Menganalisis tingkat keberhasilan dari pengujian terhadap mitigasinya pada penggunaan attack vector Hands-on-Keyboard dan Bad USB dengan metode PTES secara dalam lingkup white box testing

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 oleh pengguna, dan bagaimana dampak potensi dari ancaman serangannya
2. Bagi praktisi keamanan, penelitian ini diharapkan dapat memberikan sumbangan pemikiran pada analisis keamanan dalam dunia siber, serta sebagai

dasar tambahan dalam mengkaji lebih lanjut terhadap kerentanan Apache Log4j pada referensi CVE-2021-44228 dan selanjutnya

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 keamanan siber pada lingkungan kampus hingga global

1.5 Sistematika Penulisan

BAB I PENDAHULUAN

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

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 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 analisanya, serta penjelasan singkat terhadap objek yang diteliti dalam laporan ini

BAB IV HASIL DAN PEMBAHASAN

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

BAB V PENUTUP

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

BAB II
TINJAUAN PUSTAKA

2.1 Remote Access Trojan

Trojan dalam lingkup siber dapat diartikan sebagai medium untuk bagaimana serangan malware dikemas sedemikian rupa agar serangan tetap bersifat false negative terhadap sistem keamanan. Payload trojan dapat dikirim menggunakan berbagai macam pendekatan, seperti phishing, adware, ataupun dengan social engineering. Berdasarkan cara serangnya, tipe Remote Access Trojan (RAT) dispesifikasikan untuk mengontrol sistem korban sepenuhnya secara jarak jauh, atau remote, yang memanfaatkan koneksi berarsitektur client-server di antaranya. Pendekatan ini dimanfaatkan oleh penyerang untuk dapat mengontrol aset serta resource korban untuk dikelola sepenuhnya secara kontinuitas (CEH, 2013; Hama Saeed, 2020). Dalam membangun remote access, keberhasilan serta stabilitas koneksi bergantung kepada topologi infrastruktur jaringannya, terutama terhadap peranan firewall (Maraj, Rogova and Jakupi, 2020). Secara umum, terdapat 2 bentuk payload yang dapat digunakan untuk melakukan remote access, yaitu secara reverse dan bind, yang mana keduanya ditunjukkan untuk mengontrol sistem korban melalui akses shell yang didapatkannya.

2.1.1 Reverse & Bind Shell TCP

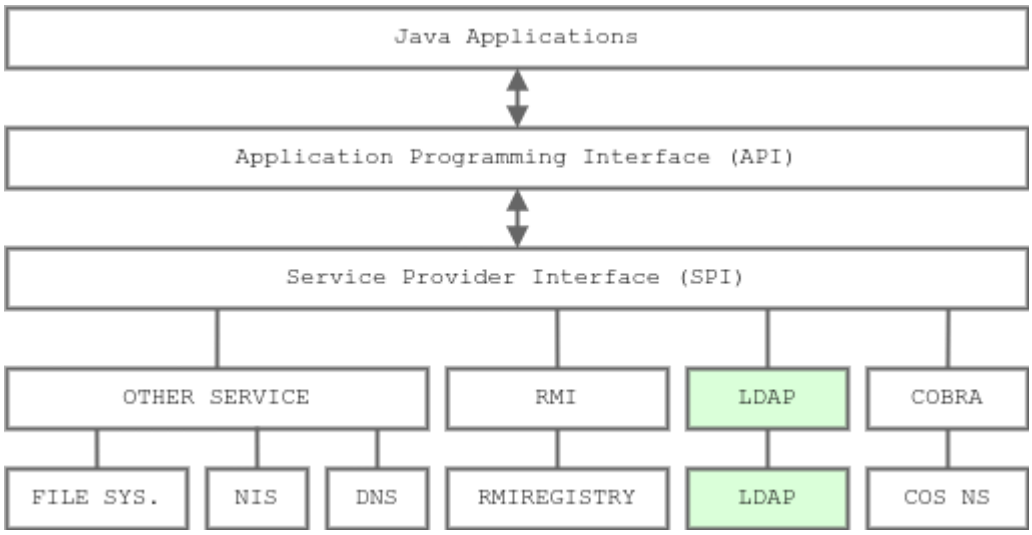
Bind shell bekerja dengan membuka layanan koneksi TCP di mesin korban pada port tertentu, yang juga disebut sebagai listener. Koneksi tersebut kemudian disambungkan oleh mesin penyerang untuk mendapatkan shell korban melalui remote access nya. Dikarenakan listener dilakukan dari mesin korban, hal ini harus disesuaikan dengan inbound rules yang mungkin terdapat dalam firewall, baik berupa eksternal maupun firewall sistem, sehingga koneksi listener dapat berfungsi sebagaimana harusnya (Saroeval and Bhadola, 2022).

Berbeda dengan payload bind shell, reverse shell bekerja dengan membuat listener dari mesin penyerang, lalu membutuhkan sistem korban untuk menyambungkan koneksi tersebut. Pendekatan ini akan merendahkan potensi isu terkait peranan firewall. Hal ini

disebabkan karena koneksi yang keluar dari mesin korban, atau outbound connection, memiliki kontrol yang lebih longgar daripada inbound connection pada firewall, sehingga sistem akan menanggap komunikasi tersebut sebagai koneksi yang valid dari sistem korban (Maraj, Rogova and Jakupi, 2020).

2.2 Apache Log4j

Apache Log4j merupakan framework Java yang umum digunakan untuk mengaudit berbagai macam pesan error hinnga info debug, baik pada perangkat lunak, jaringan, hingga layanan cloud computing (Rajasinghe, 2022). Dalam melakukan fungsinya, Apache Log4j juga dapat terintegrasi dengan berbagai macam layanan naming and directory untuk mencari dan mengambil objek data di dalamnya. Hal ini dilakukan melalui penggunaan Java Naming and Directory Interface (JNDI). Pencarian objek dalam suatu layanan, atau fungsi lookup, dapat JNDI lakukan baik dalam lingkup remote ataupun lokal (Apache, 2022).



Gambar 2.1 Arsitektur JNDI

Sumber: Roy, 2015

Pada gambar 2.1 di atas merupakan arsitektur dari penggunaan JNDI dalam suatu aplikasi Java. JNDI terdiri dari dua komponen utama, yaitu JNDI Application Programming Interface (API), serta JNDI service Provider Interface (SPI). JNDI SPI merupakan suatu mekanisme agar konektivitas layanan naming and directory dapat

tersedia pada aplikasi secara dinamis. Konektivitas tersebut yang kemudian digunakan oleh Apache Log4j untuk mengakses informasi serta objek di dalam layanan tersebut menggunakan modul dari JNDI API. Sala satu layanannya yaitu Lightweight Directory Access Protocol (LDAP) (Roy, 2015).

2.2.1 Lightweight Directory Access Protocol

LDAP merupakan salah satu layanan dengan arsitektur client-server yang berbasiskan struktur direktori dalam melakukan penyimpanan informasi. Bentuk konfigurasinya menggunakan format file tersendiri, yaitu LDAP Data Interchange Format (LDIF), yang berisikan skema suatu direktori informasi. Penggunaan beberapa skema LDIF secara terpisah dapat membantu dalam mendesain dan mempopulasi data agar lebih tergorganisir (Helmke, Hudson and Hudson, 2019).

Dalam penyimpanan datanya, LDAP menggunakan suatu object yang berisikan koleksi atribut dalam mendefinisikan suatu entri pada skema, yang disebut sebagai object class. Object class pun dapat dilakukan pewarisan atau inheritence, baik bersifat abstrak ataupun struktural, sehingga penggunaan child objcet class dapat mereferensikan atribut parent object class nya (Oracle, 2010). Berikut pada tabel 2.1 merupakan contoh pewarsian pada atribut dalam object class inetOrgperson:

Tabel 2.1 Atribut pewarisan object class inetOrgPerson

No.	Atribut	Deskripsi	Object Class Pewaris
1	uid	ID unik pengguna	top (user)
2	description	informasi entri	person
3	inetUserStatus	status keaktifan akun	inetUser
4	ou	nama unit organisasi	organizationalPerson
5	mail	Alamat email pengguna	-

Sumber: Oracle, 2010