



**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 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, \_\_ \_\_ 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 \_\_, bulan \_\_\_\_,  
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 pernyataan ini saya buat dengan sebenarnya.

Depok, \_\_ \_\_ 2022  
Yang membuat pernyataan,

Muhammad Nur Irsyad  
NIM. 1807422020

## **ABSTRAK**

AA

**Kata Kunci:** aaa

## DAFTAR ISI

<b>HALAMAN JUDUL .....</b>	<b>Error! Bookmark not defined.</b>
<b>SURAT PERNYATAAN BEBAS PLAGIARISME.....</b>	<b>iii</b>
<b>LEMBAR PENGESAHAN .....</b>	<b>iv</b>
<b>KATA PENGANTAR.....</b>	<b>v</b>
<b>SKRIPSI UNTUK KEPENTINGAN AKADEMIS.....</b>	<b>vi</b>
<b>ABSTRAK .....</b>	<b>vii</b>
<b>DAFTAR ISI .....</b>	<b>viii</b>
<b>DAFTAR GAMBAR.....</b>	<b>x</b>
<b>DAFTAR TABEL .....</b>	<b>xi</b>
<b>BAB I PENDAHULUAN.....</b>	<b>1</b>
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah .....	3
1.4 Tujuan dan Manfaat .....	4
1.5 Sistematika Penulisan .....	5
<b>BAB II TINJAUAN PUSTAKA.....</b>	<b>6</b>
2.1 Remote Access Trojan.....	6
2.1.1 Reverse & Bind Shell TCP .....	6
2.2 Apache Log4j.....	7
2.2.1 Lightweight Directory Access Protocol .....	8
2.2.2 Kerentanan CVE-2021-44228 .....	8
2.3 White-Box Testing .....	9
2.4 Penetration Testing Execution Standard .....	9
2.4.1 Common Vulnerability Scoring System .....	10
2.4.2 Attack Tree.....	12
2.4.3 Hands-on-Keyboards.....	13
2.4.4 BadUSB .....	13
2.5 Unified Modelling Language.....	14
2.6 Penelitian Sejenis .....	16
<b>BAB III METODE PENELITIAN .....</b>	<b>18</b>
3.1 Rancangan Penelitian.....	18



3.2	Tahapan Penelitian .....	18
3.3	Objek Penelitian.....	19
<b>BAB IV HASIL DAN PEMBAHASAN.....</b>		<b>20</b>
4.1	Perancangan Sistem .....	20
4.1.1	Desain Topologi Jaringan.....	20
4.1.2	Desain Skema LDAP .....	22
4.2	Implementasi Sistem .....	22
4.2.1	Implementasi Sistem Pengguna .....	22
4.2.2	Implementasi Sistem Penyerang .....	22
4.2.2.1	Instalasi dan Konfigurasi Layanan OpenLDAP .....	22
4.2.2.2	Instalasi dan Konfigurasi Layanan Apache HTTP Server .....	22
4.2.2.3	Pengembangan Aplikasi Layanan HTTP Go .....	22
4.2.2.4	Pengembangan Aplikasi Layanan HTTP Java .....	23
4.2.2.5	Pengembangan Payload Java .....	23
4.2.2.5	Pengembangan BadUSB.....	23
4.3	Pengujian Kerentanan Aplikasi pada Sistem Target .....	23
4.3.1	Pre-Engagement.....	23
4.3.2	Intelligence Gathering.....	23
4.3.3	Threat Modelling .....	23
4.3.4	Vulnerability Analysis.....	23
4.3.5	Exploitation.....	24
4.3.6	Post-Exploitation.....	24
4.3.7	Reporting.....	24
4.4	Hasil Pengujian Kerentanan.....	24
<b>BAB V PENUTUP .....</b>		<b>25</b>
5.1	Kesimpulan .....	25
5.2	Saran .....	25
<b>DAFTAR PUSTAKA.....</b>		<b>26</b>

## **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 aplikasi. Hal tersebut membuat sistem dapat diserang melalui berbagai perantara yang sesuai dengan bentuk celahnya untuk lalu dieksploitasi oleh penyerang dengan berbagai macam landasan motivasi (Calín et al., 2020). Salah satu dampak ancaman siber, yaitu kebocoran data internal, disebabkan oleh kerentanan sistem yang membuat suatu *malware* dapat tertanam di dalam sistem korban. Eksploitasi tersebut salah satunya dapat membuat penyerang untuk mengontrol dan mengambil aset digital di dalam sistem korban secara jarak jauh tanpa supervisi terhadap pertahanan sistem korban (Yin & 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 *input* pengguna dalam fitur *logging*-nya. Eksploitasi tersebut diawali dengan sistem pengguna yang mengunduh dan menjalankan *malware* dalam bahasa pemrograman Java. Adanya eksekusi *malware* tersebut dapat membangun koneksi jarak jauh secara penuh, baik itu berpola *reverse shell* maupun *bind shell*, tanpa ada autentikasi diantaranya (Apache, 2021; CVE, 2021; Khan & Neha, 2016; Oracle, 2021). Salah satu perusahaan global yang menggunakan *library* Apache Log4j, yaitu Cisco, memiliki lebih dari 60 produk serta fitur yang terpengaruh terhadap kerentanan tersebut. Hal tersebut didukung karena *library* Apache Log4j memiliki fleksibilitas dalam bentuk implementasinya di berbagai macam platform, seperti pada layanan *cloud* 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 membuat Log4Shell berbeda dari kerentanan Apache Log4j lainnya adalah kerentanan tersebut menjadi pelopor untuk tiga kerentanan baru dalam kurang dari tiga minggu (26/11/2021 – 11/12/2021) (Apache, 2021). Walaupun kerentanan CVE-2021-44228 sudah diperbaiki pada versi selanjutnya, efesiensi dan efektivitas eksploitasi kerentanan tetap dapat dimanfaatkan dari sisi penyerang sebagai media eksploitasi independen yang kuat dan stabil.

**Berdasarkan** uraian diatas, penelitian ini ditunjukkan untuk menganalisa ancaman kerentanan Apache Log4j pada referensi CVE-2021-44228 terhadap pengembangan eksploitasinya dengan pendekatan *white-box testing*. Pengembangan dilakukan dengan memanfaatkan kerentanan u/ntuk menjadi serangan *Remote Access Trojan* (RAT) secara independen dan persisten. Keseluruhan tahapan pengujian nantinya akan berbasiskan pada model *Penetration Testing Execution Standard* (PTES) sebagai **panduan dalam pengujian dan analisisnya** (Dalalana & Zorzo, 2017). **Tahap** eksploitasi pengujian didasarkan pada serangan *Remote Code Execution* (RCE) dengan memanfaatkan *JNDI Injection*. Dua bentuk vektor serangan yang digunakan adalah *Hands-on-Keyboard*, atau *direct access*, serta *BadUSB*, atau *removeable media*, yang keduanya memanfaatkan kelemahan konfigurasi dan validasi pada aplikasi atau sistem (Biswas et al., 2018). **Serangan pasca eksploitasi** dilakukan dengan menyisipkan program *backdoor*, yang dirancang dengan kerentanan *library* Apache Log4j, ke dalam sistem target untuk mempertahankan stabilitas akses yang didapat. Mitigasi yang diadaptasikan merujuk pada pendekatan analisis statis, seperti pemanfaatan konfigurasi aplikasi serta penggunaan program pemindaian proses dalam sistem. **Keseluruhan** analisis pengujian dilakukan dengan mengukur bagaimana dampak kondisi sumber daya sistem target terhadap pengujian dalam tiga tahapan periode, yaitu saat pra eksploitasi, pasca eksploitasi, serta pasca mitigasi (CEH, 2013; Kaushik et al., 2021; Muñoz & Mirosh, 2016).

## 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 dengan referensi CVE-2021-44228?
2. Bagaimana analisis pengujian serta mitigasi pada kerentanan Apache Log4j terkait ancaman RAT, dalam lingkup *white-box testing* berbasiskan metode PTES?
3. Bagaimana dampak kondisi sumber daya sistem target pada seluruh tahap pengujian terhadap ancaman RAT?

## 1.3 Batasan Masalah

Adanya pembatasan suatu masalah digunakan untuk menghindari pelebaran pokok masalah dari lingkup yang seharusnya. Dengan begitu, batasan masalah dapat membuat penelitian lebih terarah untuk tercapainya tujuan dari penelitian ini. Beberapa batasan masalah dalam penelitian ini 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 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 yaitu *Hands-on-Keyboard* dan *BadUSB*. Hal yang membedakan diantara kedua vektor serangan adalah pemanfaatan dan implementasi dari kerentanan tersebut dalam perspektif penyerang serta target

- b) Bentuk mitigasi mencakup pendekatan deteksi ancaman dengan implementasi analisis statis, pemanfaatan program pemantauan serta konfigurasi internal sistem, dan analisis terhadap pembaharuan *library* Apache Log4j pada versi 2.15.0, 2.16.0, dan 2.17.0
  - c) Proses pengujian dilakukan dalam 2 tahap, yaitu pra dan pasca adanya mitigasi, sehingga tergambarinya pencapaian yang dapat dianalisa besar tingkat dampak sumber daya pada sistem target
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, pasca eksploitasi, dan pasca mitigasi
  - b) Parameter sumber daya yang diukur antara lain *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 dicapai dalam pembentukan penelitian ini. Tujuan penelitian dijabarkan sebagai berikut:

1. Memberikan adanya suatu kontribusi dalam pengembangan *Proof-of-Concept* (PoC) terhadap kerentanan Apache Log4j pada CVE-2021-44228, terkhusus dalam pengembangan ancaman RAT
2. Menganalisis implementasi pengujian serta mitigasinya pada penggunaan vektor serangan *Hands-on-Keyboards* dan *BadUSB* dengan metode PTES 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 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 terhadap kerentanan Apache Log4j pada referensi CVE-2021-44228 dan referensi kedepannya

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 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 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 laporan ini

### **BAB IV HASIL DAN PEMBAHASAN**

Bab ini menjabarkan mengenai 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 analisis penelitiannya. Adapun saran pribadi yang diberikan terkait dengan hasil pengujian yang sifatnya konstruktif untuk dapat dikembangkan lebih lanjut



## BAB II

### TINJAUAN PUSTAKA

#### 2.1 Remote Access Trojan

*Trojan* dalam lingkup keamanan siber dapat diartikan sebagai medium untuk serangan *malware* dapat dikemas sedemikian rupa, agar serangan bersifat *false negative* terhadap suatu sistem keamanan. Suatu *payload*, dalam konteks ini adalah *trojan*, dapat dikirim menggunakan berbagai macam pendekatan, seperti melalui *phishing* dan *social engineering*. Berdasarkan bentuk serangannya, jenis *Remote Access Trojan* (RAT) dispesifikasikan untuk mengontrol sistem korban sepenuhnya secara jarak jauh dengan memanfaatkan koneksi berarsitektur client-server. Pendekatan ini dimanfaatkan oleh penyerang untuk mengontrol aset dari sistem korban sepenuhnya secara kontinuitas (CEH, 2013; Hama Saeed, 2020). Dalam membangun koneksi *remote access*, keberhasilan serta stabilitasnya bergantung kepada topologi infrastruktur jaringan, terutama terhadap peranan *firewall* (Maraj et al., 2020). Secara umum, terdapat dua bentuk *payload trojan* yang dapat digunakan untuk melakukan *remote access*, yaitu dengan koneksi *reverse* dan *bind*, yang mana keduanya ditunjukkan untuk mengontrol sistem korban melalui akses *shell* yang didapatkannya.

##### 2.1.1 Reverse & Bind Shell TCP

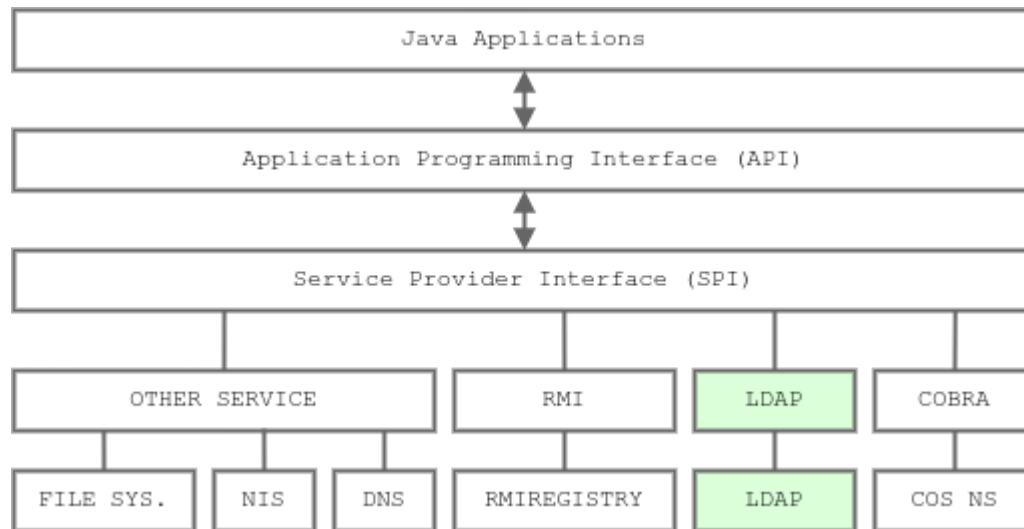
*Bind shell* bekerja dengan membuka layanan koneksi *Transmission Control Protocol* (TCP) di mesin korban pada nomor *port* tertentu, yang juga disebut sebagai *listener*. Koneksi tersebut kemudian disambungkan oleh mesin penyerang untuk mendapatkan *shell* korban melalui koneksi *remote access* nya. Dikarenakan *listener* dilakukan dari mesin korban, hal ini harus disesuaikan dengan *inbound rules* yang terdapat dalam *firewall*, baik itu berbasiskan di dalam jaringan atau mesin, sehingga koneksi *listener* dapat berfungsi sebagaimana harusnya (Saroeval & 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 tersebut merendahkan potensi isu terkait peranan *firewall*. Hal ini

disebabkan karena koneksi yang keluar dari mesin korban, atau *outbound connection*, memiliki kontrol yang umumnya lebih longgar daripada *inbound connection* pada firewall. Dengan begitu, sistem akan menanggapi komunikasi tersebut sebagai koneksi yang valid dan normal untuk sistem korban (Maraj et al., 2020).

## 2.2 Apache Log4j

Apache Log4j merupakan suatu *library* Java yang menyediakan fitur *logging* untuk dapat diimplementasikan dalam berbagai macam *platform*, yang pada umumnya adalah layanan *cloud* (HHS, 2022). Dalam melakukan fungsinya, *library* Apache Log4j dapat terintegrasi dengan berbagai macam layanan, seperti layanan *Naming and Directory*, untuk mencari dan mengambil objek data di dalamnya ke dalam berkas *logging*. Hal ini dapat dilakukan melalui penggunaan *Java Naming and Directory Interface* (JNDI). Pencarian objek dalam suatu layanan menggunakan fungsi *lookup* dapat JNDI lakukan, baik dalam lingkup layanan lokal maupun berbeda jaringan (Apache, 2022).



Gambar 2.1 Arsitektur JNDI

Sumber: Roy, 2015

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 dapat tersedia pada aplikasi secara dinamis.

**Konektivitas** tersebut yang kemudian digunakan oleh *library* Apache Log4j untuk mengakses informasi serta objek di dalam layanan tersebut menggunakan modul JNDI API. **Salah** satu layanan *Naming and Directory* yang dapat terintegrasi secara bawaan adalah Lightweight Directory Access Protocol (LDAP) (Roy, 2015).

### 2.2.1 Lightweight Directory Access Protocol

**LDAP** merupakan layanan *client-server* yang berbasiskan struktur direktori dalam melakukan penyimpanan informasi atau objek di dalamnya. **Bentuk** konfigurasi LDAP berisikan skema suatu direktori informasi dengan menggunakan format file tersendiri, yaitu LDAP *Data Interchange Format* (LDIF). **Penggunaan** beberapa skema LDIF secara terpisah dapat membantu dalam mendesain dan mempopulasi data dalam skala besar agar keseluruhan skema lebih terorganisir (Helmke et al., 2019).

**Dalam** penyimpanan datanya, LDAP menggunakan suatu entitas yang berisikan atribut dalam mendefinisikan suatu entri pada skema, yang disebut sebagai *object class*. Suatu *Object class* dapat mereferensikan struktur *object class* di atasnya, baik itu bersifat abstrak ataupun struktural. **Dengan** begitu, setiap *objcet class* dapat juga menggunakan atribut dari *object class* pewarisnya (Oracle, 2010). **Berikut** pada tabel 2.1 merupakan contoh pewarsian dalam object class *inetOrgperson* dari *top*:

**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

### 2.2.2 Kerentanan CVE-2021-44228

**Pada** Desember 2021, Apache Software Foundation resmi mempublikasikan bahwa *library* Apache Log4j dari versi 2.0-beta9 hingga 2.14.1 rentan terhadap serangan *Remote Code Execution* (RCE). **Publikasi** ini disertakan dengan saran mitigasi yang

ditawarkan hingga pada perilisan ke versi 2.17.0. **Kerentanan ini** dikategorikan sebagai *zero-day vulnerability* karena eksploitasinya yang ditemukan oleh publik sebelum adanya *patch* atau publikasi resmi dari vendor.

**Secara** garis besar, eksploitasi dilakukan dengan menginjeksi pesan dalam format khusus yang didukung oleh *library* secara bawaan, yaitu *Message Lookup Substitution*. **Pesan** tersebut kemudian diinterpretasi dan dieksekusi saat penulisan entri *logging* melalui format tersebut. **Adapun** pemanfaatan layanan seperti LDAP dan HTTP yang dirancang khusus oleh penyerang karena mampu untuk menyimpan referensi *payload*. **Payload** yang dirancang berupa berkas *class* Java untuk dipanggil oleh fungsi *lookup* JNDI (Hiesgen et al., 2022; Rajasinghe, 2022). **Berikut** contoh format pesan yang dapat digunakan beserta penggunaannya dengan JNDI dan layanan LDAP untuk eksploitasi:

```
${jndi:ldap://domain.com/cn=payload,dc=domain,dc=com }
```

### 2.3 White-Box Testing

*White-box testing* merupakan salah satu bentuk pengujian dengan pelaku memiliki seluruh informasi, akses kontrol, ataupun kendali terhadap pengembangan lingkungan pengujian. **Pengujian** secara *white-box*, atau *full-knowledge*, umum digunakan dalam tiga tujuan utama, yaitu kebutuhan introspeksi, stabilitas, serta ketelitian terhadap objek pengujian. **Dalam lingkup** pengujian kerentanan, pendekatan ini diharapkan dapat mengetahui serta mendeteksi potensi adanya kerusakan, hingga diluar lingkup yang seharusnya, terhadap keamanan suatu sistem (Madhavi, 2016; Midian, 2002).

### 2.4 Penetration Testing Execution Standard

**PTES** merupakan salah satu *framework* pengujian yang tersedia untuk menjalankan evaluasi keamanan dengan berstandar bisnis dan industri secara komprehensif. **Salah** satu keunggulan PTES yaitu tersedianya panduan perencanaan yang konkrit dalam mendefinisikan bagaimana keseluruhan tahapan dapat dijalankan dengan baik dan benar (Dalalana & Zorzo, 2017). **Secara** garis besarnya, **PTES** terdiri dari 7 tahapan utama yang mencakup seluruh kebutuhan dan analisis dasar dalam menjalankan pengujian keamanan, yaitu sebagai berikut:

1. *Pre-Engagement*: mendefinisikan lingkup instrumen pengujian, yang juga mencakup waktu estimasi pengerjaan, objek yang diteliti, bentuk surat izin dari pihak ketiga, serta tujuan utama dari dilakukannya pengujian
2. *Intelligence Gathering*: mengumpulkan kelengkapan informasi yang berkaitan dengan karakteristik objek pengujian, baik dilakukan secara aktif maupun pasif
3. *Threat Modelling*: menggambarkan bagaimana ancaman dapat dilakukan serta melakukan pemetaan terhadap aset primer dan sekunder yang dapat ditargetkan. Hal ini memudahkan penguji dan pembaca untuk memahami kerentanan apa yang ditemukan dan yang akan dieksploitasi dari objek pengujian
4. *Vulnerability Analysis*: menganalisis cakupan kerentanan dari pemodelan sebelumnya, sehingga dapat mendefinisikan vektor serangan yang efektif serta lingkungan pengujiannya untuk tahap eksploitasi
5. *Exploitation*: melakukan eksploitasi berdasarkan skema dan tujuan yang sudah dirancang sebelumnya, karena keakuratan informasi yang sudah didapatkan akan mempengaruhi keberhasilan tahap eksploitasi secara keseluruhan
6. *Post-Exploitation*: mengembangkan hasil eksploitasi menjadi serangan yang lebih konsisten dan stabil untuk tujuan kontinuitas, sehingga menunjukkan seberapa jauh kerentanan dapat dieksploitasi
7. *Reporting*: mendokumentasikan seluruh tahapan dan hasil kegiatan secara struktural dan informatif. Tahapan ini juga mencakup kesimpulan dan saran serta bagaimana pendekatan mitigasinya (Ningsih, 2021; PTES, 2021)

#### 2.4.1 Common Vulnerability Scoring System

**CVSS** merupakan salah satu *framework* untuk menentukan karakteristik dan tingkatan kerentanan pada suatu teknologi. **Penilaian** CVSS terbagi menjadi 3 grup utama, yaitu *Base*, *Temporal*, dan *Environmental*. **Dalam** implementasinya, penggunaan seluruh metrik grup dapat menspesifikasikan tingkat kerentanan yang lebih sesuai dan akurat dengan penyesuaian lingkungan skenario pengujiannya. (PTES, 2021). **Pada** tabel 2.2 berikut merupakan parameter dari metrik grup *Base* dalam CVSS versi 3.1, tabel 2.3 untuk metrik grup *Temporal*, serta 2.4 untuk metrik grup *Environmental*:

**Tabel 2.2** Keterangan metrik grup Base pada CVSS versi 3.1

Parameter	Deskripsi	Metrik	
<i>Attack Vector</i>	konteks mengenai area jangkauan eksploitasi yang dapat dilakukan	<i>Network</i>	N
		<i>Adjacent</i>	A
		<i>Local</i>	L
		<i>Physical</i>	P
<i>Attack Complexity</i>	tingkat kondisi yang harus dipenuhi agar eksploitasi dapat dilakukan	<i>Low</i>	L
		<i>High</i>	H
<i>Privilege Required</i>	ketergantungan terhadap tingkatan hak tertentu untuk menjalankan eksploitasi	<i>None</i>	N
		<i>Low</i>	L
		<i>High</i>	H
<i>User Interaction</i>	kondisi eksploitasi yang membutuhkan interaksi langsung pengguna	<i>None</i>	N
		<i>Required</i>	R
<i>Scope</i>	adanya dampak eksploitasi di luar cangkupan utama area kerentanan	<i>Changed</i>	U
		<i>Unchanged</i>	C
<i>Confidentiality</i>	besarnya akses terhadap aset sistem yang dapat dikelola dari hasil eksploitasi	<i>High</i>	H
		<i>Low</i>	L
		<i>None</i>	N
<i>Integrity</i>	tingkat kerusakan integritas pada aset sistem dari hasil eksploitasi	<i>High</i>	H
		<i>Low</i>	L
		<i>None</i>	N
<i>Availability</i>	besarnya sumber daya sistem serta layanan yang terganggu dari hasil eksploitasi	<i>High</i>	H
		<i>Low</i>	L
		<i>None</i>	N

Sumber: FIRST, 2019

**Tabel 2.3** Keterangan metrik grup Temporal pada CVSS versi 3.1

Parameter	Deskripsi	Metrik	
<i>Exploit Code Maturity</i>	tingkat status ketersediaan, keberagaman teknik, serta keaktifan eksploitasi dalam sisi industri dan global	<i>Not Defined</i>	X
		<i>High</i>	H
		<i>Functional</i>	F
		<i>PoC</i>	P
		<i>Unproven</i>	U
<i>Remediation Level</i>	tingkat remediasi yang tersedia untuk publik, baik itu dari vendor resmi ataupun masih belum ditemukan	<i>Not Defined</i>	X
		<i>Unavailable</i>	U
		<i>Workaround</i>	W
		<i>Temp. Fix</i>	W

		<i>Official Fix</i>	O
<i>Report Confidence</i>	tingkat validasi laporan ataupun isu eksploitasi terhadap kerentanan, seperti publikasi resmi dan penelitian	<i>Not Defined</i>	X
		<i>Confirmed</i>	C
		<i>Unknown</i>	U
		<i>Reasonable</i>	R

Sumber: FIRST, 2019

**Tabel 2.4** Keterangan metrik grup Environmental pada CVSS versi 3.1

Parameter	Deskripsi	Metrik	
<i>Security Requirement</i>	pengaruh kerentanan terhadap prinsip dasar keamanan aset dan layanan sistem dalam model CIA Triad	<i>Not Defined</i>	X
		<i>High</i>	H
		<i>Low</i>	L
		<i>Medium</i>	M
<i>Modified Base</i>	adaptasi penilaian pada metrik grup Base yang disesuaikan kembali dengan lingkungan pengujian		

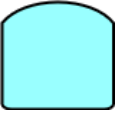



Sumber: FIRST, 2019

Dalam mengimplementasikan perumusan keseluruhan nilainya, FIRST menyediakan kalkulator CVSS versi 3.1 yang dapat diakses secara daring pada halaman web-nya. Nilai akhir setiap metrik grup dikemas dalam skala numerik, mulai dari tidak berbahaya sama sekali hingga pada status kritis (FIRST, 2019).

#### 2.4.2 Attack Tree

*Attack tree* merupakan *framework* untuk menggambarkan rangkaian vektor serangan dengan tujuan utamanya digambarkan pada puncak diagram. *Attack tree* didasarkan pada perspektif penyerang dalam melakukan eksploitasi. Untuk mencapai tujuan utama (*root node*) dari suatu *attack tree*, penyerang terlebih dahulu menjabarkan berbagai langkah-langkah (*leaf node*) serta sub tujuan (*intermediate node*) yang dapat diraih untuk mencapai puncak tersebut. Setiap *intermediate node* dapat bersifat *AND* atau *OR*, yang digunakan untuk mendeskripsikan syarat suksesi terhadap langkah-langkah serta sub tujuan yang berada dibawahnya (Ingoldsby, 2021; Shevchenko et al., 2018). Pada tabel 2.5 berikut merupakan simbol serta deskripsi dari komponen utama dalam diagram *attack tree*:

Tabel 2.5 Deskripsi simbol attack tree

Simbol	Nama	Deskripsi
	<i>OR Node</i>	dibutuhkan dua atau lebih <i>node</i> yang sukses untuk dapat mencapai atau melanjutkan <i>node</i> yang ada di atasnya
	<i>AND Node</i>	hanya membutuhkan salah satu <i>node</i> yang sukses untuk mencapai atau melanjutkan <i>node</i> yang ada di atasnya
	<i>Leaf Node</i>	menggambarkan vektor serangan yang bersifat independen dan tidak dapat memiliki <i>node</i> dibawahnya lagi
	<i>Line</i>	menggambarkan relasi setiap komponen yang tersambung diantaranya

Sumber: Ingoldsby, 2021

### 2.4.3 Hands-on-Keyboard

*Hands-on-Keyboard* merupakan salah satu vektor serangan berjenis *direct access* yang mana penyerang menggunakan perangkat *keyboard* target untuk melakukan eksploitasi secara langsung. **Dikarenakan** sudah mendapatkan akses awal di dalam sistem, hal ini mempermudah penyerang untuk menjalankan serangan, terkhusus yang bertipe lokal. **Pengontrolan** serta filterisasi *keystroke* pada tingkatan sistem dan aplikasi merupakan salah satu langkah dalam menghadapi ancaman siber ini sebagai pencegahan lapisan keamanan yang terdepan (LiveAction, 2022).

### 2.4.4 BadUSB

*BadUSB* merupakan salah satu vektor serangan berjenis *removable media* berupa perangkat keras *microcontroller*. **Perangkat** tersebut ditunjukkan untuk mengemulasi perangkat *Human Interface Device* (HID) dalam sistem target, dengan mengambil karakteristik *keyboard*, *mouse*, hingga pemindai sidik jari. **Tidak** seperti perangkat penyimpanan eksternal, penggunaan perangkat HID tidak dilakukan pemindaian oleh



sistem, sehingga *BadUSB* dapat langsung menginjeksi *payload* ke dalam mesin target. Dalam halnya mengemulasi *keyboard*, keseluruhan rangkaian injeksi *keystroke* akan tertampil di layar target karena serangan bersifat di depan layar, atau *foreground*. Kelemahan ini diminimalisir dengan kecepatan *keystroke* per huruf hingga milidetik untuk menyelesaikan seluruh injeksinya, sehingga durasi serangan dapat berkurang secara signifikan daripada dilakukan secara manual (Bojović et al., 2019).

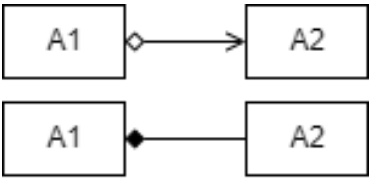
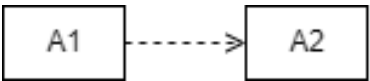
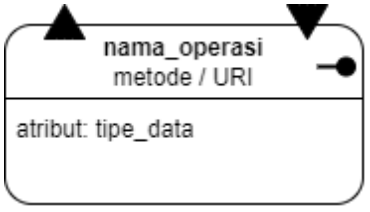
## 2.5 Unified Modelling Language

*Unified Modeling Language* (UML) merupakan bentuk standarisasi visual dari skema pada suatu sistem untuk menjabarkan seluruh komponen secara dinamis. UML juga dapat digunakan untuk menganalisa berbagai macam tingkatan dalam sistem aplikasi, seperti struktur ataupun aktivitas penggunaan aplikasi. Contoh dua bentuk penggunaan UML yang mereferensikan kegiatan tersebut adalah *class diagram* dan *activity diagram* (Sukic & Saracevic, 2012).

*Class diagram* merupakan bagian dari diagram struktur UML yang menggambarkan tingkatan *class* dan *interface* pada suatu aplikasi atau sistem. Pendekatan ini umum digunakan pada perancangan aplikasi dalam bahasa pemrograman berprinsip *object-oriented*, seperti Java. Adanya perancangan tersebut dapat menunjukkan relasi dalam komponen *class* seperti variabel, fungsi, dependensi terhadap suatu *interface*, serta bentuk konektivitas terhadap integrasinya pada suatu layanan. (OMG, 2011b; Sukic & Saracevic, 2012). Berikut pada tabel 2.4 merupakan simbol dan keterangan yang digunakan pada *class diagram*:

Tabel 2.6 Deskripsi simbol class diagram


Simbol	Nama	Deskripsi
<div>nama_class</div>	Class	pengklasifikasian suatu objek
<div>- atribut: tipe_data</div>	Atribut	properti variabel dalam <i>class</i>
<div>+ operasi(tipe_data): tipe_data</div>	Operasi	fungsi atau metode dalam <i>class</i>

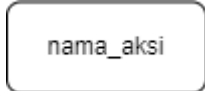

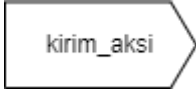
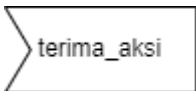
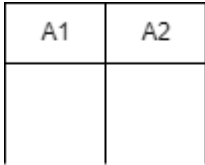
	Asosiasi & Kardinal	relasi statis terhadap besarnya implementasi objek atau atribut dalam <i>class</i> lain; dinotasikan dengan kardinalitas
<p>0..0 // 0..1 // 1..1 // 0..* // m..n</p>		ukuran berapa elemen dalam <i>class</i> lain yang terasosiasi
	Dependensi	relasi abstrak terhadap referensi suatu elemen dalam <i>class</i> lain pada lingkup fungsi
	REST	proses pemanggilan fungsi dari layanan <i>Representational State Transfer</i> (REST) terhadap logika aplikasi

Sumber: Ismail, 2020; OMG, 2011

Berbeda dengan class diagram, activity diagram merupakan bagian dari diagram kegiatan UML yang menunjukkan alur kontrol suatu objek pada rangkaian kondisi dari suatu aktivitas. Salah satu tujuan utama penggunaan activity diagram yaitu dapat menggambarkan bagaimana aktivitas sistem dapat dijalankan menggunakan berbagai macam sudut pandang komponen di dalamnya (Ismail, 2020; OMG, 2011a). Aktivitas dalam sistem pun dapat dijabarkan menjadi beberapa diagram berdasarkan suatu fungsi atau modul untuk memberikan kejelasan yang lebih terperinci. Berikut pada tabel 2.5 merupakan simbol dan keterangan yang digunakan pada activity diagram:

Tabel 2.7 Deskripsi simbol activity diagram

Simbol	Nama	Deskripsi
	Inisiasi	<i>node</i> untuk memulai alur aktivitas
	Final	node untuk menyelesaikan alur aktivitas

	Aksi	aksi kegiatan dengan kata kerja, yang juga digunakan untuk memanggil suatu operasi
	Keputusan	<i>node</i> untuk mengontrol keputusan alur aktivitas dengan memberikan keluaran benar dan salah
	Sinyal Kirim	<i>node</i> untuk memberikan input agar diproses pada aksi atau <i>node</i> selanjutnya
	Sinyal Terima	<i>node</i> untuk menerima input yang datang agar dilanjutkan ke aksi atau <i>node</i> selanjutnya
	Partisi	pemberian notasi terhadap alur kegiatan dalam karakteristik yang sama, baik secara vertikal ataupun horizontal

**Sumber:** Ismail, 2020; OMG, 2011a

## 2.6 Penelitian Sejenis

**Penyusunan** laporan ini menggunakan referensi dari penelitian sebelumnya yang sejenis dan relevan dengan topik. **Adapun** pembahasan penelitian terhadap studi kasus yang digunakan untuk mengembangkan aspek analisis penelitian ini.

**Penelitian** Rajasinghe Ravindu (2022) yang berjudul ‘*Remote Code Execution Security Flaw in Apache Log4j2*’, berisikan analisis eksploitasi kerentanan CVE-2021-44228 terhadap serangan RCE pada *white-box testing*. Serangan yang peneliti gunakan berupa *JNDI Injection* melalui HTTP header X-API-Version. **Bentuk** akhir eksploitasi adalah didapatkannya *reverse shell* TCP sitem korban menggunakan program *netcat*. **Adapun** bentuk deteksi dan mitigasi yang diimplementasikan yaitu berupa analisis statis,

dengan pemeriksaan berkas *log* dan mematikan opsi *lookup* dari modul JNDI dalam konfigurasi Log4j (Rajasinghe, 2022).

**Penelitian** Shita Widya Ningsih (2021) dengan judul ‘Analisis Pengujian Kerentanan Situs Pemerintahan XYZ dengan PTES’, berisikan analisis pengujian kerentanan dalam lingkup *black-box testing*. Dengan adanya penggunaan PTES, langkah serta informasi setiap tahapan dapat dipaparkan secara terstruktur. Dari berbagai temuan yang didapatkan, peneliti melakukan eksploitasi kerentanan dengan prioritas tertinggi, yaitu pada *Reflected Cross Site Scripting* (XSS) dan *Clickjacking*. Walaupun peneliti menggunakan keseluruhan tahap dari PTES, tahap eksploitasi tidak ditunjukkan untuk mendapatkan akses *remote shell* dari sistem target, sehingga serangan tidak dapat dikembangkan ke dalam tahap pasca eksploitasi. Bentuk remediasi yang disarankan adalah penggunaan *Web Application Firewall* (WAF) serta adanya pendekatan analisis statis dengan mengamankan konfigurasi opsi *header* aplikasi serta filterisasi masukan pengguna (Ningsih, 2021).

**Penelitian** yang dilakukan Nanny, Prayudi serta Riadi (2019) dengan judul ‘Peningkatan Keamanan Data Terhadap Serangan *Remote Access Trojan* (RAT) pada *Cybercriminal* Menggunakan Metode *Dynamic Static*’, ditunjukkan untuk dapat mensimulasikan cara kerja serangan RAT beserta mitigasinya dalam lingkup *white-box testing*. Infrastruktur jaringan lokal dibangun menggunakan dua buah *laptop* untuk mesin pengujian serta dua buah *router* Mikrotik. Vektor serangan yang digunakan untuk mendistribusikan *payload* RAT-nya adalah dengan memanfaatkan fitur *file sharing* dalam sistem target. Selain untuk deteksi ancaman, *router* Mikrotik juga digunakan untuk mengontrol koneksi jaringan dengan memasang fungsi *firewall* untuk memblokir koneksi *reverse shell* TCP pada nomor *port* yang ditemukan. Penelitian ini juga diunggulkan dengan adanya analisis forensik pada berkas serta koneksi *trojan* tersebut. Analisis akhir dilakukan dengan adanya komparasi sumber daya dalam sistem korban pada sebelum diserang, saat diserang, serta saat penyerangan pasca mitigasi (Nanny et al., 2019).

## **BAB III**

### **METODE PENELITIAN**

#### **3.1 Rancangan Penelitian**

**Landasan** yang digunakan dalam pembuatan penelitian ini adalah metode kuantitatif eksperimental. **Dalam** penelitian ini, peneliti menentukan dua bentuk variabel yang digunakan pada analisis akhir dari pengujian dalam lingkup PTES, yaitu variabel kontrol yang berupa ukuran sumber daya sistem target yang tidak dieksploitasi, serta variabel terikat yang berupa perubahan kondisi sumber daya sistem pasca eksploitasi dan pasca mitigasi. **Adapun** penggunaan batasan masalah untuk menyesuaikan bentuk pengujian dan perancangan instrumennya, agar hasil penelitian tidak terpengaruh dari faktor di luar aspek pengujian yang seharusnya. Terkait **teknik** pengumpulan data, penelitian ini difokuskan pada tipe sekunder, yang mencakup referensi penelitian kepustakaan terdahulu serta studi dokumentasi dari sumber primer dan sekunder, seperti dari situs resmi vendor serta contoh PoC dari sumber terbuka. **Dengan adanya** data tersebut, peneliti dapat menguji serta menganalisis pengembangan permasalahan pada studi kasus ataupun penelitian terdahulu.

#### **3.2 Tahapan Penelitian**

**Terdapat** tahapan-tahapan yang sifatnya prosedural dalam melakukan penelitian ini, yang dapat dijabarkan ke dalam beberapa poin utama sebagai berikut:

1. Perumusan Masalah

**Peneliti** mengumpulkan bahan literatur terkait untuk mengidentifikasi masalah yang akan diangkat atau dikembangkan pada objek penelitian. **Tahap** ini juga digunakan untuk mendapatkan gambaran bentuk pengujian serta analisisnya

2. Pengumpulan Data & Teori

**Peneliti** mengumpulkan informasi terkait terhadap objek penelitian dari sumber yang kredibel, seperti bagaimana perancangan dan implementasi lingkungan pengujiannya. Seluruh **informasi** yang didapatkan tersebut dirumuskan menjadi suatu batasan masalah dan landaan dalam memberikan paparan kajian teori

### 3. Perancangan dan Pembangunan Instrumen Pengujian

**Pada** tahap ini, peneliti merancang dan membangun instrumen pengujian yang didasarkan pada rumusan batasan masalah. **Instrumen** penelitian mencakup lingkungan pengujian, sistem serta layanan yang akan digunakan, suatu target aplikasi, serta program pendukung pengujian lainnya, seperti skrip *payload*

### 4. Pengujian

**Peneliti** melakukan pengujian kerentanan dari objek penelitian yang didasarkan pada metode PTES, dengan menggunakan instrumen pengujian yang telah dibangun pada tahap sebelumnya

### 5. Analisis Hasil Pengujian

**Selain** menganalisis pengujian dari tahap sebelumnya, adapun dokumentasi data dari hasil pengujian untuk mengukur besar dampak pengujian terhadap sistem target melalui beberapa periode pengukuran sumber daya yang berbeda

## 3.3 Objek Penelitian

**Objek** yang diteliti dalam penelitian ini adalah kerentanan dari *library* Apache Log4j terhadap ancaman serangannya dalam referensi CVE-2021-44228. **Dengan** adanya objek penelitian, seluruh instrumen pengujian beserta tahapan pengujiannya dilakukan atas landasan tersebut. **Pada** implementasinya, selain mengandalkan sistem target untuk memiliki kerentanan tersebut, objek penelitian kemudian dikembangkan untuk menjadi satu vektor serangan yang independen untuk mencapai tujuan yang sama, yaitu meraih tahap eksploitasi akhir melalui ancaman RAT.

## BAB IV

### HASIL DAN PEMBAHASAN

#### 4.1 Perancangan Sistem

**Tahap** perancangan sistem dilakukan untuk mendapatkan gambaran implementasi serta integrasinya antar suatu komponen dalam pengujian dengan yang lain. **Keseluruhan** sistem terbagi menjadi dua komponen utama, yaitu pada sisi penyerang serta sisi target pengguna. **Pada** sisi target pengguna, perancangan ditunjukkan untuk mengembangkan aplikasi *desktop* yang dijadikan sebagai target kerentanan. **Dalam** kasus ini, target aplikasi berupa program autentikasi lokal sederhana dengan adanya integrasi dari *library* Apache Log4j untuk fitur riwayat autentikasi. **Pada** sisi penyerang, perancangan mencakup pengembangan *payload* RAT, perangkat *BadUSB*, serta beberapa layanan di dalamnya yang digunakan untuk mendukung penyerangan secara utuh.

**Perancangan** sistem berikut meliputi bentuk desain topologi jaringan yang akan digunakan serta struktur skema penyimpanan LDAP untuk sisi penyerang. **Adapun** seluruh layanan yang dibutuhkan terancang pada suatu *docker container*, sedangkan perancangan aplikasi dan program akan dimasukkan ke dalam bab dari implementasi sistem. **Berikut pada** tabel 4.1 merupakan spesifikasi perangkat keras, virtual dan lunak dalam merancang dan mengimplementasikan sistem:

**Tabel 4.1** Spesifikasi perangkat

No.	Perangkat Keras	Spesifikasi	
1	ASUS VivoBook 14 X407UAR ( laptop A )	Processor	Intel i3-7020U
		OS	Linux Mint 20.3
		CPU	2.30 GHz
		RAM	12144240 kB
2	HP EliteBook 2560P ( laptop B )	Processor	Intel i5-2520M
		OS	Linux Mint 20.3
		CPU	2.50 GHz
		RAM	10107488 kB
3	DigiSpark Attiny 85 Mini USB	Flash Memory	6 kB + 2kB bootloader
		LED	Power + Status (pin0)

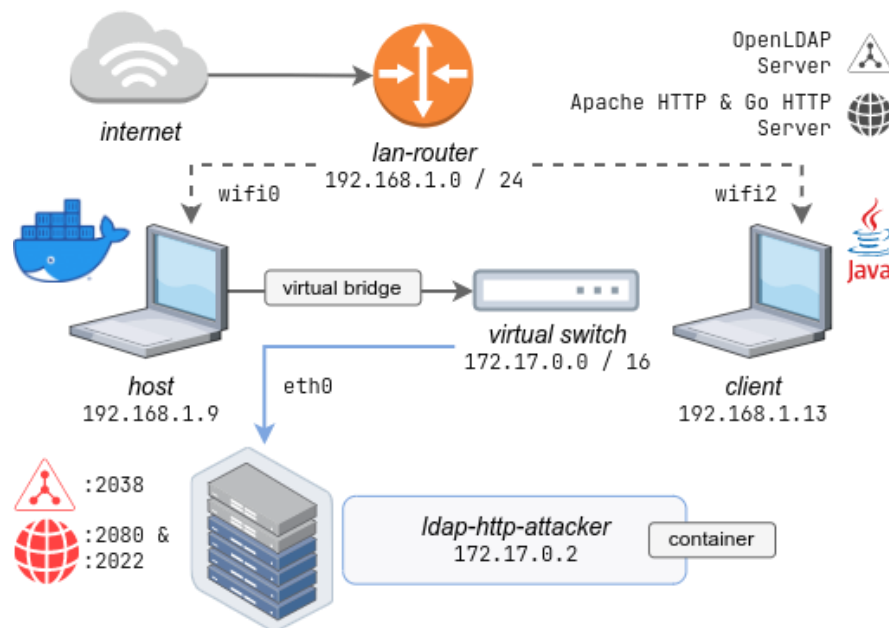
No.	Perangkat Virtual	Spesifikasi	
1	ldap-http-attacker ( container A )	OS	Ubuntu Server 20.04
		Shell	/bin/bash
		Port Bindings	2000 – 2100 / TCP
No.	Perangkat Lunak	Spesifikasi	
1	Apache HTTP Server ( 2.4.41 )		
2	OpenLDAP Server ( 2.4.49 )		
3	Oracle Java SDK ( 1.8.0_181 ) & ( 1.8.0_333 )		
4	Apache Maven ( 3.6.3 )		
5	Apache Log4j ( 2.14.1 ) , ( 2.15.0 ) , ( 2.16.0 ) & ( 2.17.0 )		
6	Go ( 1.18.3 )		
7	Arduino IDE ( 1.8.19 )		

#### 4.1.1 Desain Topologi Jaringan

**Dalam** membangun keseluruhan sistem, adapun topologi jaringan yang dirancang untuk menggambarkan keseluruhan arsitektur jaringan terhadap setiap komponen di dalamnya. **Berikut** merupakan keterangan terhadap komponen dalam topologi jaringan pada gambar 4.1 yang direferensikan dari tabel 4.1 diatas:

1. **Skema** pengujian secara utuh akan dilakukan dalam dua buah laptop. **Laptop A** digunakan untuk menjalankan berbagai layanan yang dibutuhkan selama proses pengujian, sedangkan laptop B digunakan sebagai objek pengujian pada sisi target pengguna. **Selain itu**, laptop A juga dimanfaatkan sebagai sisi penyerang untuk menjalankan mayoritas dari seluruh tahap penyerangan
2. **Dalam** laptop A, seluruh layanan yang dibutuhkan oleh pengujian dijalankan menggunakan virtualisasi *docker* pada *container A*. **Adapun** layanan yang dibangun yaitu LDAP menggunakan OpenLDAP pada nomor port :2038, serta *Hypertext Transfer Protocol* (HTTP) menggunakan Apache HTTP Server dan Go HTTP pada nomor port :2022 dan :2080. **Selain** dalam container A, layanan HTTP juga dibangun menggunakan Java sebagai bentuk serangan di dalam sistem target pengguna untuk memperluas area kerentanan
3. **Lingkup** topologi berupa *Local Area Network* (LAN), dengan konektivitas seluruh komponen berlandaskan satu jaringan yang sama





Gambar 4.1 Topologi jaringan

#### 4.1.2 Desain Skema LDAP

Hands-on-Keyboard

### 4.2 Implementasi Sistem

Objek yang diteliti

#### 4.2.1 Implementasi Sistem Pengguna

[ Pengembangan Aplikasi Desktop GUI ]

#### 4.2.2 Implementasi Sistem Penyerang

[ Pengembangan Aplikasi Desktop GUI ]

##### 4.2.2.1 Instalasi dan Konfigurasi Layanan OpenLDAP

[ Pengembangan Aplikasi Desktop GUI ]

##### 4.2.2.2 Instalasi dan Konfigurasi Layanan Apache HTTP Server

[ Pengembangan Aplikasi Desktop GUI ]

##### 4.2.2.3 Pengembangan Aplikasi Layanan HTTP Go

[ Pengembangan Aplikasi Desktop GUI ]

#### **4.2.2.4 Pengembangan Aplikasi Layanan HTTP Java**

[ Pengembangan Aplikasi Desktop GUI ]

#### **4.2.2.5 Pengembangan Payload Java**

[ snippet properties, nama Object, reverseshell ]

[ minimum viable product ]

#### **4.2.2.5 Pengembangan Perangkat BadUSB**

[ instalasi + setup full ]

[ pembuatan base64 script ]

### **4.3 Pengujian Kerentanan Aplikasi pada Sistem Target**

[ PTES ]

#### **4.3.1 Pre-Engagement**

[ dokumentasi ]

#### **4.3.2 Intelligence Gathering**

[ dalemin info info aplikasi gui + sistem client ]

[ OWASP dependency check ]

[ OSSIndex Maven ]

#### **4.3.3 Threat Modelling**

[ attended : act. diag client (user // gui) & attacker (ldap // http // system) ]

[ unattended : act. diag client (system) & attacker (java // ldap // http // system) ]

[ aset primer ]

[ aset sekunder ]

#### **4.3.4 Vulnerability Analysis**

[ dalemin cve-2021-44228 ]

[ bikin cvss internal, base score ambil dari official, kita yg environ]

[ attack trees ]

[ deskripsi lab testing ]

[ hardware spec + container + bad usb ]

[ software spec + tools ]

#### **4.3.5 Exploitation**

[ berdasarkan attack tree : 2 attack vector ]

[ BadUSB Malware + Hands-on-Keyboard ]

#### **4.3.6 Post-Exploitation**

[ cronjob – daemon persistence ]

[ libprocesshider.c – hide process ]

#### **4.3.7 Reporting**

[ mitigasi untuk exploit, ulang tahapan & post-exploitation ]

[ notepad >> static analysis >> config >> firewall >> dll ]

### **4.4 Hasil Pengujian Kerentanan**

[ hasil pengujian whitebox kerentanan sistem ]

[ tingkat keberhasilan mitigasi terhadap ancaman RAT ]

[ pengaruh performa sistem terhadap ancaman RAT ]

## **BAB V**

### **PENUTUP**

#### **5.1 Kesimpulan**

[ abc ]

#### **5.2 Saran**

[ abc ]

## DAFTAR PUSTAKA

- Apache. (2021). *Apache Log4j Security Vulnerabilities*, Apache Software Foundation. <https://logging.apache.org/log4j/2.x/security.html>
- Apache. (2022). *Apache Log4j 2 v. 2.17.2 User's Guide*, Apache Software Foundation. <https://logging.apache.org/log4j/2.x/log4j-users-guide.pdf>
- Biswas, S., Sohel, M. K., Hasan Khan Sajal, M. M., & Afrin, T. (2018). *A Study on Remote Code Execution Vulnerability in Web Applications*, *International Conference on Cyber Security and Computer Science*. <https://www.researchgate.net/publication/328956499>
- 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://securitvwatch.pcmag.com>
- Cisco. (2021). *Vulnerabilities in Apache Log4j Library Affecting Cisco Products: December 2021*. <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/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>
- 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., & Wählich, 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](http://www.amenaza.com)
- Ismail, N. M. (2020). *Rancang Bangun Aplikasi Gamifikasi Untuk Hafalan Al-Quran Menggunakan Audio Fingerprint Berbasis Android*.

- Kaushik, K., Aggarwal, S., Mudgal, S., Saravgi, S., & Mathur, V. (2021). A Novel Approach to Generate a Reverse Shell: Exploitation and Prevention. *International Journal of Intelligent Communication, Computing, and Networks*, 2(2). <https://doi.org/10.51735/ijiccn/001/33>
- 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](http://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](http://www.journalforresearch.org)
- 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>
- Midian, P. (2002). Perspectives on penetration testing - Black box vs. white box. *Network Security*, 2002(11), 10–12. [https://doi.org/10.1016/S1353-4858\(02\)11009-9](https://doi.org/10.1016/S1353-4858(02)11009-9)
- Muñoz, A., & Mirosh, O. (2016). *A Journey from JNDI/LDAP Manipulation to Remote Code Execution Dream Land, BlackHat USA*. <https://www.blackhat.com/>
- 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. (2010). *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>
- Sarooval, 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>