



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

SKRIPSI

MUHAMMAD NUR IRSYAD

1807422020

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



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

SKRIPSI

**Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan
untuk Memperoleh Diploma Empat Politeknik**

MUHAMMAD NUR IRSYAD

1807422020

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

2023



Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

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

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

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

Depok, 07 Februari 2023
Yang membuat pernyataan,

POLITEKNIK
NEGERI
JAKARTA



Muhammad Nur Irsyad
NIM. 1807422020



Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

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

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

Disahkan oleh:

Pembimbing I : Ariawan Andi Suhandana, S.Kom., M.T.I.

Penguji I : Dr. Prihatin Oktivasari, S.Si., M.Si.

Penguji II : Ayu Rosyida Zain, S.ST., M.T.

Penguji III : Fachroni Arbi Murad, S.Kom., M.Kom.

Mengetahui:

Jurusan Teknik Informatika dan Komputer
Ketua,

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



Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

KATA PENGANTAR

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

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

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

Penulis,

Muhammad Nur Irsyad
NIM. 1807422020



Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

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

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

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

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

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

Demikian pernyataan ini saya buat dengan sebenarnya.

Depok, 07 Februari 2023
Yang membuat pernyataan,



Muhammad Nur Irsyad
NIM. 1807422020



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

ABSTRAK

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

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

Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



DAFTAR ISI

HALAMAN JUDUL	ii
SURAT PERNYATAAN BEBAS PLAGIARISME	iii
LEMBAR PENGESAHAN	iv
KATA PENGANTAR	v
SURAT PERNYATAAN PERSETUJUAN PUBLIKASI	vi
ABSTRAK	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	x
DAFTAR TABEL	xi
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan dan Manfaat	4
1.5 Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA	6
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	9
2.3 White-Box Testing	10
2.4 Penetration Testing Execution Standard	10
2.4.1 Common Vulnerability Scoring System	11
2.4.2 Attack Tree.....	13
2.4.3 Hands-on-Keyboard.....	14
2.4.4 BadUSB	14
2.5 Unified Modelling Language.....	14
2.6 Penelitian Sejenis	16
BAB III METODE PENELITIAN	18
3.1 Rancangan Penelitian.....	18
3.2 Tahapan Penelitian	18
3.3 Objek Penelitian.....	20
BAB IV HASIL DAN PEMBAHASAN	21
4.1 Perancangan Sistem	21
4.1.1 Desain Topologi Jaringan.....	22
4.1.2 Desain Skema LDAP	23
4.2 Implementasi Sistem.....	24
4.2.1 Implementasi Sistem Pengguna	25

Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

4.2.2	Implementasi Sistem Penyerang	28
4.2.2.1	Instalasi dan Konfigurasi Layanan OpenLDAP	28
4.2.2.2	Instalasi dan Konfigurasi Layanan Apache HTTP Server	31
4.2.2.3	Pengembangan Aplikasi Layanan HTTP Go	32
4.2.2.4	Pengembangan Aplikasi Layanan HTTP Java	35
4.2.2.5	Pengembangan Payload Java	38
4.2.2.5	Pengembangan Perangkat BadUSB	39
4.3	Pengujian Kerentanan Aplikasi dan Sistem Target	41
4.3.1	Pre-Engagement	41
4.3.2	Intelligence Gathering	42
4.3.3	Threat Modelling	44
4.3.4	Vulnerability Analysis	45
4.3.5	Exploitation	47
4.3.6	Post-Exploitation	52
4.3.7	Implementasi Mitigasi	54
4.4	Analisis Hasil Pengujian Kerentanan	60
BAB V PENUTUP		63
5.1	Kesimpulan	63
5.2	Saran	64
DAFTAR PUSTAKA		65
LAMPIRAN		68





DAFTAR GAMBAR

Gambar 2.1 Struktur dependensi library apache log4j.....	7
Gambar 2.2 Arsitektur JNDI	8
Gambar 3.1 Diagram tahapan penelitian.....	19
Gambar 4.1 Topologi jaringan	23
Gambar 4.2 Skema DIT layanan LDAP	23
Gambar 4.3 Activity diagram pada fitur login	25
Gambar 4.4 Class diagram aplikasi desktop GUI	26
Gambar 4.5 Tampilan antarmuka aplikasi desktop GUI.....	28
Gambar 4.6 Verifikasi entri payload dalam layanan LDAP.....	31
Gambar 4.7 Activity diagram pada endpoint properties	33
Gambar 4.8 Activity diagram pada endpoint captures	34
Gambar 4.9 Activity diagram aplikasi layanan HTTP java	36
Gambar 4.10 Class diagram aplikasi layanan HTTP java.....	36
Gambar 4.11 Tampilan logging aplikasi layanan HTTP java	38
Gambar 4.12 Hasil pemetaan attack tree.....	44
Gambar 4.13 Pembuatan koneksi listener dalam sistem penyerang	48
Gambar 4.14 Injeksi alamat payload dalam aplikasi target	48
Gambar 4.15 Remote access melalui vektor serangan HoK.....	49
Gambar 4.16 Proses penulisan skrip BadUSB dalam console.....	49
Gambar 4.17 Remote access melalui vektor serangan BadUSB.....	50
Gambar 4.18 Data aset tangkapan dalam endpoint capture	51
Gambar 4.19 Pengunduhan berkas aset tangkapan.....	52
Gambar 4.20 Kolase aset tangkapan dari sistem target.....	52
Gambar 4.21 Proses penyisipan arsip payload ke dalam berkas gambar.....	53
Gambar 4.22 Netralisasi pesan dengan percent encoding.....	58
Gambar 4.23 Restriksi hak akses pengguna terhadap layanan cron	60

Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

DAFTAR TABEL

Tabel 2.1 Atribut pewarisan object class inetOrgPerson.....	9
Tabel 2.2 Keterangan metrik grup base pada CVSS versi 3.1	11
Tabel 2.3 Keterangan metrik grup temporal pada CVSS versi 3.1	12
Tabel 2.4 Keterangan metrik grup environmental pada CVSS versi 3.1	12
Tabel 2.5 Deskripsi simbol attack tree	13
Tabel 2.6 Deskripsi simbol class diagram.....	15
Tabel 2.7 Deskripsi simbol activity diagram.....	16
Tabel 4.1 Spesifikasi perangkat.....	21
Tabel 4.2 Keterangan atribut skema LDAP penyerang.....	24
Tabel 4.3 Hasil tahap pre-engagement	41
Tabel 4.4 Hasil tahap intelligence gathering pada aplikasi target.....	42
Tabel 4.5 Hasil tahap intelligence gathering pada sistem target	44
Tabel 4.6 Asesi nilai CVSS v3.1 terhadap pengujian.....	47
Tabel 4.7 Informasi konfigurasi layanan dalam container A	47
Tabel 4.8 Rekomendasi pembaharuan versi library apache log4j.....	56
Tabel 4.9 Hasil data sumber daya sistem target pada vektor HoK.....	61
Tabel 4.10 Hasil data sumber daya sistem target pada vektor BadUSB	61



Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

BAB I PENDAHULUAN

1.1 Latar Belakang

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

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

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

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

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

1.2 Rumusan Masalah

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

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

1.3 Batasan Masalah

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

Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

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

1.4 Tujuan dan Manfaat

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

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

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

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

1.5 Sistematika Penulisan

BAB I PENDAHULUAN

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

Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

BAB II TINJAUAN PUSTAKA

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

BAB III METODE PENELITIAN

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

BAB IV HASIL DAN PEMBAHASAN

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

BAB V PENUTUP

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

Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

POLITEKNIK
NEGERI
JAKARTA



Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

BAB V PENUTUP

5.1 Kesimpulan

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

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

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

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

5.2 Saran

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

Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta





DAFTAR PUSTAKA

- Apache. (2021). *Apache Log4j Security Vulnerabilities*, Apache Software Foundation. <https://logging.apache.org/log4j/2.x/security.html>
- Apache. (2022a). *Apache Log4j 2 v. 2.17.2 User's Guide*, Apache Software Foundation. <https://logging.apache.org/log4j/2.x/log4j-users-guide.pdf>
- Apache. (2022b). *Changes - Release History*, Apache Software Foundation.
- Bojović, P. D., Bašičević, I., Pilipović, M., Bojović, Ž., & Bojović, M. (2019). *The rising threat of hardware attacks: A keyboard attack case study*. November, 1–7. <https://www.researchgate.net/publication/331312670>
- Calín, M., Anchez, S. ', Carrillo De Gea, J. M., Jos', J., Luis, J., Fern'fernández-Alemán, F., Alemán, A., Jes', J., Garcerán, J., Garcerán, G., & Toval, A. (2020). *Software Vulnerabilities Overview: A Descriptive Study*, Tsinghua Science and Technology. <https://doi.org/10.26599/TST.2019.9010003>
- CEH. (2013). *Trojans and Backdoors - Module 06*, EC-Council. <http://securitywatch.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>
- CWE. (2022, October 13). *CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')*, CWE Mitre Org. <https://cwe.mitre.org/data/definitions/917.html>
- Dalalana, D. B., & Zorzo, A. F. (2017). Overview and Open Issues on Penetration Test. *Journal of the Brazilian Computer Society*, 23(1). <https://doi.org/10.1186/s13173-017-0051-1>
- FIRST. (2019). *Common Vulnerability Scoring System version 3.1 Specification Document Revision 1*. 1–24. <https://www.first.org/cvss/>
- Hama Saeed, M. A. (2020). Malware in Computer Systems: Problems and Solutions. *IJID (International Journal on Informatics for Development)*, 9(1), 1. <https://doi.org/10.14421/ijid.2020.09101>
- Helmke, M., Hudson, A., & Hudson, P. (2019). *Ubuntu Unleashed: 2019 Edition*, Pearson Education, Inc.
- HHS. (2022). *Log4j Vulnerabilities and the Health Sector*, HHS Cybersecurity Program.
- Hiesgen, R., Nawrocki, M., Schmidt, T. C., & 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
- Ismail, N. M. (2020). *Rancang Bangun Aplikasi Gamifikasi Untuk Hafalan Al-Quran Menggunakan Audio Fingerprint Berbasis Android*.
- Khadadiya, N. (2021, December 27). *Log4Shell Simplified - All you need to know about Log4j CVE-2021-44228*, InfoSec Write-ups. <https://infosecwriteups.com/log4shell-simplified-all-you-need-to-know-about-cve-2021-44228-3c70d59c307a>

Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

- Khan, A., & Neha, R. P. (2016). Analysis of Penetration Testing and Vulnerability in Computer Networks. *GRD Journals-Global Research and Development Journal for Engineering* |, 1(6). www.eeye.com
- LiveAction. (2022). *Hands On Keyboard Attack: Why Detection Just Became Critical*. <https://www.liveaction.com/resources/blog/hands-on-keyboard-attack-why-detection-just-became-critical/#:~:text=A hands-on keyboard attack, other end of this technique.>
- Madhavi, D. (2016). A White Box Testing Technique in Software Testing: Basis Path Testing. *Journal for Research*, 2(4), 12–17. www.journalforresearch.org
- Maji, S., Jain, H., Pandey, V., & Siddiqui, A. (2022). *White Hat Security-An Overview of Penetration Testing Tools*. <https://ssrn.com/abstract=4159095>
- Maraj, A., Rogova, E., & Jakupi, G. (2020). Testing of Network Security Systems through DoS, SQL Injection, Reverse TCP and Social Engineering Attacks. In *Int. J. Grid and Utility Computing* (Vol. 11, Issue 1). <https://doi.org/10.1504/IJGUC.2020.103976>
- Nanny, Prayudi, Y., & Riadi, I. (2019). Peningkatan Keamanan Data Terhadap Serangan Remote Access Trojan (RAT) pada Cybercriminal Menggunakan Metode Dynamic Static. *Jurnal Instek*, 4(2), 161–170.
- Ningsih, S. W. (2021). Analisis Pengujian Kerentanan Situs Pemerintahan XYZ dengan PTES. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, 8(3), 1543–1556. <https://doi.org/10.35957/jatisi.v8i3.1224>
- OMG. (2011a). *Activity Diagrams*. <https://www.uml-diagrams.org/activity-diagrams.html>
- OMG. (2011b). *UML Class and Object Diagrams Overview*. <https://www.uml-diagrams.org/class-diagrams-overview.html>
- Oracle. (2010a). *Controlling Access to the crontab Command*, Oracle Corporation. <https://docs.oracle.com/cd/E19253-01/817-0403/sysrescron-23/index.html>
- Oracle. (2010b). *inetOrgPerson Object Class*, Oracle Corporation. <https://docs.oracle.com/cd/E19225-01/820-6551/bzbp/index.html>
- Oracle. (2021). *Oracle Security Alert Advisory - CVE-2021-44228*, Oracle Corporation. <https://www.oracle.com/security-alerts/alert-cve-2021-44228.html>
- PTES. (2021). *The Penetration Testing Execution Standard Documentation - Release 1.1*, The PTES Team. <https://pentest-standard.readthedocs.io/en/latest/tree.html>
- Rajasinghe, R. (2022). *Remote Code Execution Security Flaw in Apache Log4j2*. May. <https://doi.org/10.13140/RG.2.2.14272.20486>
- Roy, U. K. (2015). *Advanced Java programming*, Oxford University Press. <https://india.oup.com/product/advanced-java-programming-9780199455508>
- Saroeval, M., & Bhadola, S. (2022). *Network Utility Tools Best Practices*. 9(6), 96–103.
- Shevchenko, N., Chick, T. A., O’riordan, P., Scanlon, T. P., & Woody, C. (2018). *Threat Modeling: A Summary Of Available Methods*, Carneige Mellon University: *Software Engineering*.
- Sukic, C., & Saracevic, M. (2012). UML and JAVA as effective tools for implementing algorithms in computer graphics. *Tem Journal*, 1(2), 111.
- Yin, K. S., & Khine, M. A. (2019). Optimal Remote Access Trojans Detection Based on Network Behavior. *International Journal of Electrical and*

Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

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

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



© Hak Cipta milik Jurusan TIK Politeknik Negeri Jakarta

Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta





Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

LAMPIRAN

L1 – Daftar riwayat hidup



Muhammad Nur Irsyad

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



POLITEKNIK
NEGERI
JAKARTA



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

Terminal output for L2 showing system resources and network statistics. The top section displays system status (PRC, CPU, MEM, SWP, PSI, NET) and disk I/O. The middle section shows network statistics for wlo1, including total packets, incoming/outgoing rates, and IP checksum errors. The bottom section shows a list of processes with columns for PID, USER, PRI, NI, VIRT, RES, SHR, S, CPU%, MEM%, TIME+, and Command.

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

Terminal output for L3 showing system resources and network statistics. The top section displays system status (PRC, CPU, MEM, SWP, PSI, NET) and disk I/O. The middle section shows network statistics for wlo1, including total packets, incoming/outgoing rates, and IP checksum errors. The bottom section shows a list of processes with columns for PID, USER, PRI, NI, VIRT, RES, SHR, S, CPU%, MEM%, TIME+, and Command.

Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
2. Dilarang mengutip hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
3. Dilarang mengutip dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta



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

```

TiliX client@hp2560p: ~
ATOP - hp2560p 2022/12/12 21:27:49 ----- 5s elapsed
PRC sys 0.23s user 0.64s #proc 234 #tslpu 58 #zombie 0 #exit 0/s
CPU sys 4% user 12% irq 1% idle 38% wait 0% ipc 0.87
CPL avg1 0.15 avg5 0.24 avg15 0.31 csw 540/s intr 320/s numcpu 4
MEM tot 9.6G free 8.2G cache 557.0M buff 49.6M slab 115.9M numnode 1
SWP tot 2.0G free 2.0G swcac 0.0M vmcon 3.4G vmlin 6.8G
PSI cpusome 0% memsome 0% memfull 0% iosome 0% iofull 0% cs 0/0/0
OSK sda busy 0% read 0/s write 0/s MBw/s 0.0 avio 4.00 ms
NET transport tcp1 0/s tcpo 0/s udp1 0/s udpo 0/s tcpsa 0/s
NET network ip1 0/s ipo 0/s iprw 0/s deliv 0/s icmpo 0/s
NET wlo1 0% pck1 1/s pcko 1/s sp 243 Mbps si 0 Kbps so 0 Kbps

Total DISK READ: 0.00 B/s Total DISK WRITE: 0.00 B/s
Current DISK READ: 0.00 B/s Current DISK WRITE: 0.00 B/s

TID PRIO USER DISK READ DISK WRITE SWAPIN ID COMMAND
1 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [init+ssh]
2 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [kthreadd]
3 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [rcu_gp]
4 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [rcu-r_gp]
5 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [netns]
7 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [kwo-hpri]
9 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [mm-u_wq]
10 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [rcu-ude_]
11 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [rcu-race]
12 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [kso-qd/0]
13 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [rcu-ched]
14 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [mig-on/0]
15 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [tid-ct/0]

CONFIG_TASK_DELAY_ACCT not enabled in kernel, cannot determine SWAPIN an

PID SYSCPU USRCPU RDELAY VGRROW RGRROW RDDSK WRDASK ST EXC THR S CPUNR CPU CMD 1/8
1752 0.10s 0.43s 0.00s 0B 0B 0B/s 0B/s -- 1 5 0 1% iotop
1761 0.05s 0.03s 0.00s 0B 0B 0B/s -- 1 5 3 2% htop
1698 0.01s 0.05s 0.00s 0B 0B 0B/s -- 7 5 2 1% tilix
1445 0.00s 0.04s 0.00s 28.0K 0B 0B/s -- 11 5 1 1% cinnamon

iptraf-ng 1.2.1
Statistics for wlo1

Total Packets Total Incoming Incoming Outgoing Outgoing
Packets Bytes Packets Bytes Packets Bytes
Total: 29685 27317627 15400 14373707 14285 12943920
IPv4: 28908 27209357 14829 14297379 14079 12911978
IPv6: 777 108270 571 76328 206 31942
TCP: 27571 26940391 13467 14029879 14104 12910512
UDP: 1717 347268 1827 321694 90 25664
ICMP: 306 22496 270 19952 36 2544
Other IP: 91 7472 36 2272 55 5200
Non-IP: 0 0 0 0 0 0
Broadcast: 633 136342 633 136342 0 0

Total rates: 0.45 kbps Broadcast rates: 0.34 kbps
pps pps

Incoming rates: 0.45 kbps IP checksum errors: 0
pps pps

Outgoing rates: 0.00 kbps
pps pps

Time: 0:52 Drops: 0
X-exit
  
```

- Hak Cipta:**
- Dilangut mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 - Dilarang mengutip dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

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

```

TiliX client@hp2560p: ~
ATOP - hp2560p 2022/12/24 11:35:22 ----- 5s elapsed
PRC sys 0.19s user 0.55s #proc 222 #tslpu 58 #zombie 0 #exit 0/s
CPU sys 4% user 18% irq 0% idle 38% wait 0% ipc 0.87
CPL avg1 0.24 avg5 0.21 avg15 0.28 csw 489/s intr 289/s numcpu 4
MEM tot 9.6G free 8.2G cache 613.6M buff 45.1M slab 110.1M numnode 1
SWP tot 2.0G free 2.0G swcac 0.0M vmcon 3.2G vmlin 6.8G
PSI cpusome 0% memsome 0% memfull 0% iosome 0% iofull 0% cs 0/0/0
OSK sda busy 0% read 0/s tcpo 0/s udpi 0/s udpo 0/s tcpsa 0/s
NET transport ip1 0/s ipo 0/s iprw 0/s deliv 0/s icmpo 0/s
NET network ip1 0/s ipo 0/s iprw 0/s deliv 0/s icmpo 0/s
NET wlo1 0% pck1 1/s pcko 0/s sp 243 Mbps si 0 Kbps so 0 Kbps

Total DISK READ: 0.00 B/s Total DISK WRITE: 0.00 B/s
Current DISK READ: 0.00 B/s Current DISK WRITE: 0.00 B/s

TID PRIO USER DISK READ DISK WRITE SWAPIN ID COMMAND
1 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [init+ssh]
2 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [kthreadd]
3 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [rcu_gp]
4 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [rcu-r_gp]
5 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [netns]
6 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [kwo-hpri]
7 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [kwo-hpri]
9 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [mm-u_wq]
10 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [rcu-ude_]
11 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [rcu-race]
12 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [kso-qd/0]
14 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [rcu-ched]

keys: any: refresh q: quit i: ionice q: active p: proc a: accum
sort: r: asc left: SWAPIN right: COMMAND home: TID end: COMMAND
CONFIG_TASK_DELAY_ACCT not enabled in kernel, cannot determine SWAPIN an

PID USER PRI NI VIRT RES SHR S CPU%MEM% TIME+ Command
1905 root 20 0 25136 15752 7588 S 6.5 0.2 6:08.80 /usr/br
1889 root 0 -20 10832 16628 9552 S 3.3 0.2 0:49.32 atop -1
1937 client 20 0 11076 4360 3520 R 2.6 0.0 1:22.02 htop
1445 client 20 0 4267M 170M 100M S 1.3 1.7 1:11.56 cinnamon
1825 client 20 0 638M 70820 53704 S 0.7 0.7 1:05.80 /usr/br
1 root 20 0 638M 70820 53704 S 0.0 0.1 0:01.38 /sbin/i
359 root 19 -1 47968 17168 15884 S 0.0 0.2 0:00.59 /lib/sy
398 root 20 0 27200 7644 4632 S 0.0 0.1 0:01.34 /lib/sy
664 systemd-r 20 0 25348 12384 8352 S 0.0 0.1 0:00.21 /lib/sy
665 systemd-t 20 0 89456 6712 5832 S 0.0 0.1 0:00.12 /lib/sy
674 systemd-t 20 0 89456 6712 5832 S 0.0 0.1 0:00.00 /lib/sy
675 root 20 0 234M 7720 6768 S 0.0 0.1 0:00.37 /usr/li
676 root 20 0 2812 1124 1640 S 0.0 0.0 0:00.14 /usr/sb

0||| 3.9% Tasks: 110, 220 thr: 1 running
1||| 7.8% Load average: 0.24 0.31 0.28
2||| 3.9% Uptime: 01:26:43
3||| 2.0%
Mem||| 858M/9.63G
Swp| 0K/2.00G
  
```




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

```
Tilix client@hp2560p:~$ top
ATOP - hp2560p 2022/12/24 11:57:20 -----1----- 5s elapsed
PRC sys 0.46s user 0.96s #proc 249 #tslpu 61 #zombie 0 #exit 11/s Total DISK READ: 0.00 B/s Total DISK WRITE: 14.24 K/s
CPU sys 11% user 19% irq 0% idle 37% wait 0% ipc 0.87 Current DISK READ: 0.00 B/s Current DISK WRITE: 35.60 K/s
CPL avgl 0.30 avg5 0.31 avg15 0.36 csw 1603/s intr 756/s numcpu 4 TID PRIO USER DISK READ DISK WRITE SWAPIN IO-> COMMAND
MEM tot 9.6G free 2.0G cache 641.9M buff 51.0M slab 119.2M vmnode 1 1 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [init-plash]
SWP tot 2.0G free 2.0G swcac 0.0M vmcom 3.8G vmlim 0.8G 3 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [kthreadd]
PSI cpusome 0% memsome 0% memfull 0% losome 0% iofull 0% cs 0/0/0 4 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [rcu_gp]
NET transport tcp1 4/s tcpo 10/s udp1 0/s udpo 0/s tcpsa 0/s 5 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [netns]
NET network ip1 5/s ipo 5/s iptrw 0/s deliv 5/s icmpo 0/s 6 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [kwo-wants]
NET wlo1 8% pck1 3/s pcko 8/s sp 1 Mbps si 1 kbps so 82 kbps 7 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [kwo-hpri]
NET lo ---- pck1 2/s pcko 2/s sp 0 Mbps si 1 kbps so 1 kbps 9 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [mm-u_wq]
PID SYSPCPU USRCPU RDELAY VGRROW RGRROW RDDSK WRDCK ST EXC THR S CPUNR CPU CMD 1/30
1905 0.14s 0.44s 0.00s 0B 0B 0B/s 0B/s -- - 1 S 1 12% itop 10 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [rcu-race]
915 0.06s 0.08s 0.00s 28.0K 0B 0B/s 0B/s -- - 5 S 1 3% Xorg 12 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [kso-gd/0]
1445 0.05s 0.08s 0.00s 60.0K 0B 0B/s 0B/s -- - 12 S 1 3% cinnamon keys: any: refresh q: quit i: ionice g: active p: proc a: accum
1937 0.05s 0.03s 0.00s 0B 0B 0B/s 0B/s -- - 1 S 3 2% htop sort: r: asc left: SWAPIN right: COMMAND home: TID end: COMMAND
CONFIG_TASK_DELAY_ACCT not enabled in kernel, cannot determine SWAPIN an

iptraf-ng 1.2.1
Statistics for wlo1
Total Packets Total Bytes Incoming Packets Incoming Bytes Outgoing Packets Outgoing Bytes
Total: 4927 5847327 1695 1946584 3232 3900743
IPV4: 4904 5844775 1684 1945189 3220 3895976
IPV6: 23 2550 11 1383 12 1167
TCP: 4850 5834109 1624 1933994 3226 3900115
UDP: 68 12384 66 12172 2 212
ICMP: 7 560 5 416 2 144
Other IP: 2 272 0 0 2 272
Non-IP: 0 0 0 0 0 0
Broadcast: 42 9072 42 9072 0 0
Total rates: 4591,80 kbps Broadcast rates: 0,34 kbps
477 pps 0 pps
Incoming rates: 1522,90 kbps IP checksum errors: 0
159 pps
Outgoing rates: 3068,90 kbps
317 pps
Time: 0:03 Drops: 0
X-exit
```

Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin dari Jurusan TIK Politeknik Negeri Jakarta

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

```
Tilix client@hp2560p:~$ top
ATOP - hp2560p 2022/12/24 13:52:40 -----1----- 5s elapsed
PRC sys 0.27s user 0.62s #proc 234 #tslpu 56 #zombie 0 #exit 0/s Total DISK READ: 0.00 B/s Total DISK WRITE: 0.00 B/s
CPU sys 5% user 12% irq 0% idle 38% wait 0% ipc 0.89 Current DISK READ: 0.00 B/s Current DISK WRITE: 0.00 B/s
CPL avgl 0.06 avg5 0.15 avg15 0.17 csw 476/s intr 300/s numcpu 4 TID PRIO USER DISK READ DISK WRITE SWAPIN IO-> COMMAND
MEM tot 9.6G free 8.0G cache 676.2M buff 60.3M slab 128.0M vmnode 1 1 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [init-plash]
SWP tot 2.0G free 2.0G swcac 0.0M vmcom 3.5G vmlim 0.8G 2 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [kthreadd]
PSI cpusome 0% memsome 0% memfull 0% losome 0% iofull 0% cs 0/0/0 3 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [rcu_gp]
NET transport tcp1 0/s tcpo 0/s udp1 0/s udpo 0/s tcpsa 0/s 4 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [rcu-r_gp]
NET network ip1 0/s ipo 0/s iptrw 0/s deliv 0/s icmpo 0/s 5 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [netns]
NET wlo1 0% pck1 0/s pcko 0/s sp 1 Mbps si 0 kbps so 0 kbps 7 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [kwo-hpri]
NET lo ---- pck1 0/s pcko 0/s sp 0 kbps si 0 kbps so 0 kbps 9 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [mm-u_wq]
PID SYSPCPU USRCPU RDELAY VGRROW RGRROW RDDSK WRDCK ST EXC THR S CPUNR CPU CMD 1/6
1905 0.12s 0.41s 0.00s 0B 0B 0B/s 0B/s -- - 1 S 1 1% itop 10 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [rcu-race]
1937 0.07s 0.03s 0.00s 0B 0B 0B/s 0B/s -- - 1 S 2 2% htop 11 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [rcu-race]
1445 0.01s 0.04s 0.00s -0.2M 0B 0B/s 0B/s -- - 11 S 0 1% cinnamon 12 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [kso-gd/0]
1825 0.00s 0.05s 0.00s 0B 0B 0B/s 0B/s -- - 7 S 3 1% tilix 13 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [rcu-ched]
3724 0.03s 0.02s 0.00s 0B 0B 0B/s 0B/s -- - 1 R 3 1% atop 14 be/4 root 0.00 B/s 0.00 B/s ?unavailable? [mig-on/0]
915 0.01s 0.03s 0.00s -64.0K 0B 0B/s 0B/s -- - 5 S 1 1% Xorg keys: any: refresh q: quit i: ionice g: active p: proc a: accum
sort: r: asc left: SWAPIN right: COMMAND home: TID end: COMMAND
CONFIG_TASK_DELAY_ACCT not enabled in kernel, cannot determine SWAPIN an

iptraf-ng 1.2.1
Statistics for wlo1
Total Packets Total Bytes Incoming Packets Incoming Bytes Outgoing Packets Outgoing Bytes
Total: 18397 7945746 11152 2957021 7245 4986725
IPV4: 15881 7722166 8946 2762741 6935 4959425
IPV6: 2516 223514 2206 194214 310 29300
TCP: 13785 7268772 6621 2298563 7884 4972289
UDP: 2582 322460 2521 515016 61 6644
ICMP: 1987 143960 1930 139936 57 4024
Other IP: 123 10488 80 4640 43 5848
Non-IP: 0 0 0 0 0 0
Broadcast: 1414 305798 1414 305798 0 0
Total rates: 0,34 kbps Broadcast rates: 0,34 kbps
0 pps 0 pps
Incoming rates: 0,34 kbps IP checksum errors: 0
0 pps
Outgoing rates: 0,80 kbps
0 pps
Time: 1:58 Drops: 0
X-exit
```