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

SKRIPSI

MUHAMMAD NUR IRSYAD **1807422020**

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

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

SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk Memperoleh Gelar Sarjana Terapan Politeknik

MUHAMMAD NUR IRSYAD
1807422020

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

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

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

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

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

Depok, __ ____ 2022

Yang membuat pernyataan,

Muhammad Nur Irsyad

NIM. 1807422020

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

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

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari __, tanggal __, bulam ____, tahun __, dan dinyatakan **LULUS**.

Disahkan oleh:

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

Mengetahui:

Jurusan Teknik Informatika dan Komputer

Ketua

Mauldy Laya , S.Kom., M.Kom.

NIP. 197802112009121003

KATA PENGANTAR

Aaa

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 Apache Log4j pada CVE-2021-44228 terhadap Ancaman Remote Access Trojan dengan Metode Penetration Testing Execution Standard

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

Depok, __ ____ 2022

Yang membuat pernyataan,

Muhammad Nur Irsyad

NIM. 1807422020

ABSTRAK

Aaa

Kata kunci: aaa

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam dunia siber, potensi ancaman dalam lingkup ini dapat muncul dikarenakan adanya celah kerentanan terhadap suatu sistem maupun infrastruktur, baik itu dikarenakan oleh kesalahan manusia maupun program dalam logika bisnisnya. Hal tersebut membuat sistem untuk dapat diserang melalui berbagai macam perantara yang sesuai dengan bentuk celahnya. Masalah kerentanan ini yang lalu dieksploitasi oleh penyerang dengan landasan untuk manfaat pribadi dan berbagai macam faktor lainnya (Calín *et al.*, 2020). Salah satu dampak ancaman siber, yaitu kebocoran data internal, dapat disebabkan karena adanya kerentanan sistem terhadap serangan malware yang tertanam ke dalam sistem korban. Hal ini membuat penyerang dapat mengontrol sistem korban secara jarak jauh untuk mengambil aset dan informasi digital secara transparan terhadap supervisi pertahanan sistem korban (Yin and Khine, 2019).

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

tersebut. Hal ini didukung karena library Apache Log4j memiliki fleksibilitas dalam implementasinya di berbagai macam platform, seperti cloud service dan software development (Cisco, 2021).

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

Adapun berdasarkan uraian diatas, penelitian ini ditunjukkan untuk menganalisa ancaman kerentanan Apache Log4j pada referensi CVE-2021-44228 terhadap pengembangan eksploitasinya dengan pendekatan whitebox testing. Pengembangan dilakukan pada pengujian post exploitation menggunakan ancaman Remote Access Trojan secara persistence. Keseluruhan tahapan pengujian berbasiskan pada model Penetration Testing Execution Standard (PTES) sebagai lingkup panduan pengujian dan analisisnya (Dalalana and Zorzo, 2017). Tahap eksploitasi pengujian didasarkan pada serangan Remote Code Execution (RCE) dengan memanfaatkan URL Entry Manipulation. Dua bentuk attack vector yang akan digunakan adalah Hands-on-Keyboard dan BadUSB, yang mana keduanya memanfaatkan miskonfigurasi aplikasi atau sistem, serta lemahnya validasi request input pengguna (Biswas *et al.*, 2018). Pengujian kemudian dikembangkan dengan menyisipkan backdoor ke dalam sistem target untuk mempertahankan stabilitas akses, yang mana memanfaatkan kerentanan Apache Log4j sebagai komponen utamanya. Mitigasi yang diadaptasikan merujuk kepada pendekatan static analysis serta pemanfaatan program monitoring dan

konfigurasi internal sistem. Analisis keseluruhan pengujian dilakukan pada hasil eksploitasi dari pasca mitigasi, yang nantinya digunakan sebagai tolak ukur untuk mengetahui seberapa luas dan besarnya tingkat keberhasilan mitigasi terhadap ancaman tersebut (CEH, 2013; Muñoz and Mirosh, 2016; Kaushik *et al.*, 2021).

1.2 Rumusan Masalah

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

1. Bagaimana merancang instrumen penelitian dan integrasinya dengan Apache Log4j dalam lingkup white box testing?
2. Bagaimana pengaruh pengujian serta mitigasi terhadap tingkat keberhasilannya pada kerentanan Apache Log4j dalam referensi CVE-2021-44228

1.3 Batasan Masalah

Adanya pembatasan suatu masalah digunakan untuk menghindari potensi pelebaran pokok masalah dari lingkup yang seharusnya, sehingga dapat membuat penelitian lebih terarah untuk tercapainya tujuan dari penelitian ini. Beberapa batasan masalah dalam penelitian ini kemudian dijabarkan sebagai berikut:

1. Batasan dalam perancangan infrastruktur instrumen
   a) Instrumen dirancang pada model arsitektur client-server secara lokal dengan memanfaatkan virtualisasi Docker container
   b) Framework Java yang digunakan untuk membangun aplikasi utama pengguna dan penyerang adalah Maven, dengan *library* Apache Log4j pada versi 2.14.1, yang sesuai dengan referensi CVE-2021-44228
   c) Mesin komputer menggunakan platform Linux dengan GNOME 3 sebagai dasar Desktop Environment nya, sehingga seluruh payload, program, serta skrip akan disesuaikan ke arah tersebut
2. Batasan dalam implementasi mitigasi dan pengujiannya
   a) Pengujian kerentanan dilakukan dengan pendekatan white box testing, dan hanya ditujukan untuk *library* Log4j dalam versi 2.0-*beta*9 hingga

2.14.1 (Java 8) yang sesuai dengan referensi CVE-2021-44228, sehingga tidak mencangkup *security patch* terakhir, yaitu versi 2.17.1 per tanggal 28/12/2021

b) Bentuk mitigasi mencangkupi pendekatan *static analysis* serta pemanfaatan *system utility*, tidak mencangkup bentuk pengaplikasian *system update* ataupun *security patch*

c) Proses pengujian dilakukan dalam 2 tahap, yaitu pra dan pasca adanya mitigasi, sehingga tergambarnya pencapaian yang dapat dianalisa besar tingkat keberhasilannya

1.4 Tujuan dan Manfaat

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

1. Membangun instrumen penelitian, yang mencangkup keseluruhan infrastruktur baik untuk sisi penyerang dan sisi korban
2. Mampu melakukan keseluruhan proses pengujian dalam white box testing yang spesifik terhadap kerentanan pada versi Log4j pada batasan masalah, sehingga lingkup objek penelitian tidak melebar dari yang ditunjukkan
3. Mampu mengimplementasikan pendekatan mitigasi yang sesuai dengan teknologi dan platform infrastruktur yang diujikan
4. Menyajikan data hasil pengujian yang dapat dianalisis terkait dengan tingkat keberhasilan mitigasi dan dampak pengembangan ancamannya

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

1. Manfaat teoretis

a) Memberikan sumbangan pemikiran pada analisis keamanan siber, baik dari sisi pendekatan serangan serta mitigasinya terhadap kerentanan Log4j dan ancaman pengembangan *remote access trojan*
b) Sebagai pijakan referensi untuk penelitian sejenis terkait pada kerentanan Log4j kedepannya, serta sebagai kajian lebih lanjut dalam analisis ancaman *remote access trojan* terhadap teknologi Log4j dan tingkat keefektifan terhadap mitigasinya

2. Manfaat praktis
   a) Bagi pembaca

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

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

      Bagi perusahaan
   c) Penelitian ini dapat dijadikan sebagai contoh kasus penjabaran dari dampak kerentanan Log4j terhadap sisi pengguna produk perusahaan yang rentan, sehingga diharapkan bisa memberikan suatu pertimbangan dan kesadaran mengenai pentingnya keamanan dalam sisi infrastruktur

1.5 Sistematika Penulisan

Sistematika penulisan berikut dibentuk untuk mempermudah dalam penyusunan proposal penelitian ini dengan penulisan yang baik. Sistematika penulisan yang digunakan dijabarkan sebagai berikut:

BAB 1 PENDAHULUAN

Bab pendahuluan mendeskripsikan mengenai latar belakang serta bagaimana urgensi masalah, perumusan masalah, menentukan batasan-batasan masalah, mendefinisikan tujuan dan manfaat penelitian, serta sistematika struktur penulisan dalam merancang laporan penelitian ini

BAB II TINJAUAN PUSTAKA

Bab tinjauan pustaka berisikan seluruh teori-teori landasan yang digunakan dalam inti pembahasan pada rancangan penelitian dari berbagai sumber yang kredibel. Adapun penjabaran terkait penelitian sejenis yang digunakan sebagai penunjang dan pengembangan dari penelitian yang sebelumnya dalam kurun waktu 10 tahun terakhir

BAB III PERENCANAAN DAN REALISASI

Bab perencanaan dan realisasi menjelaskan tahapan-tahapan yang dilakukan dalam membangun instrumen penelitian dan bagaimana proses pengujian kerentanan dapat berlangsung terhadap objek penelitian menggunakan metodologi ataupun framework yang sudah ditentukan

BAB IV PEMBAHASAN

Bab pembahasan memaparkan bagaimana data yang didapatkan dari hasil pengujian untuk dianalisa menggunakan pendekatan statistika. Metrik penilaian bersifat kualitatif dalam bentuk katagorikal, yaitu dalam bentuk pencapaian ataupun milestone terhadap setiap parameter-parameter dalam pengujian

BAB V PENUTUP

Bab penutup menjelaskan mengenai pembuktian terhadap tujuan yang ingin dicapai dalam penelitian dan bagaimana hasil penelitiannya. Adapun saran yang diberikan terkait dengan hasil pengujian yang sifatnya konstruktif

BAB II
TINJAUAN PUSTAKA

2.1 Remote Access Trojan

ABC

2.1.1 Reverse & Bind Shell TCP

ABC

2.2 Apache Log4j

ABC

2.2.1 Lightweight Directory Access Protocol

ABC

2.2.2 Java

ABC

2.2.3 Maven

ABC

2.3 Penetration Testing Execution Standard

ABC

2.3.1 White Box Testing

ABC

2.3.2 Common Vulnerability Scoring System

ABC

2.3.3 Attack Trees

ABC

2.3.4 Hands-on-Keyboard Attack

ABC

2.3.5 BadUSB Malware

ABC

2.4 Unified Modelling Language

ABC

2.4.1 Class Diagram

ABC

2.4.2 Activity Diagram

ABC

2.5 Software Testing

ABC

2.5.1 Integration Testing

ABC

2.5.2 Alpha Testing

ABC

2.6 Docker Container

ABC

2.7 Penelitian Sejenis

ABC

BAB III
METODE PENELITIAN

3.1 Rancangan Penelitian

[kuantitatif + eksperimental]

[analisis data berdasarkan hasil dari pengujian apliksi serta sistem]

[penelitian menitik beratkan pada analisa pengujian sistem berdasarkan hasil pre dan post mitigasi, fokus pada tingkat keberhasilan mitigasi terhadap ancaman RAT]

3.2 Tahapan Penelitian

[berdasarkan metode PTES secara whitebox]

3.3 Objek Penelitian

[kerentanan apache log4j - cve-2021-44228]

BAB IV
HASIL DAN PEMBAHASAN

4.1 Perancangan Sistem

[rangkum deskripsi – singgung topologi, skema ldap, dan class diagram C vs A]

4.1.1 Desain Topologi Jaringan

[desain topologi]

4.1.2 Desain Skema LDAP

[desain skema ldap C vs A]

4.1.3 Desain Class Diagram Aplikasi

[desain class diagram aplikasi C vs A]

4.2 Implementasi Sistem

[instalasi konfigurasi, serta pembangunan aplikasi dan tools, sisi C vs A]

4.2.1 Implementasi Sistem Pengguna

[server ldap serta aplikasi ldap client berbentuk gui]

4.2.1.1 Instalasi dan Konfigurasi OpenLDAP Server

[docker puull + docker exec]

[install open ldap]

[ldif dari skema ldap bab 3]

[test ldapsearch client]

4.2.1.2 Pengembangan Aplikasi GUI Desktop LDAP Client

[structure tree]

[activity diagram]

[pom,xml]

[snippet properties, Log4j, LDAP Operation, LogPanel]

[minimum viable product]

4.2.2 Implementasi Sistem Penyerang

[server ldap serta java http + payload]

4.2.2.1 Instalasi dan Konfigurasi OpenLDAP Server

[docker puull + docker exec]

[install open ldap]

[ldif dari skema ldap bab 3]

[test ldapsearch attacker]

4.2.2.2 Instalasi dan Konfigurasi Apache HTTP Server

[pakai container yg sudah ada]

[install apache2]

[proses buat virtual host + touch file payload]

[test curl + lynx]

4.2.2.3 Pengembangan Aplikasi Java HTTP Server

[structure tree]

[activity diagram]

[pom,xml]

[snippet properties, socketa ddr, Log4j, header payload]

[minimum viable product]

4.2.2.4 Pengembangan Payload Java

[snippet properties, nama Object, reverseshell]

[minimum viable product]

4.2.2.5 Pengembangan BadUSB

[instalasi + setup full]

[pembuatan base64 script]

4.3 Pengujian Aplikasi dan Sistem

[pengujian whitebox, baik untuk aplikasi dan kerentanan sistem]

4.3.1 Prosedur Pengujian Aplikasi

[uji 1 : integration testing + alpha testing]

4.3.1.1 integration Testing

[client]

- LDAP Context
- Log4j Rolling Files
- Config Properties

[attacker java http]

- Remote Config Properties
- Log4j Rolling Files

[attacker java payload]

- Remote Config Properties

[bad USB]

- Open Gnome Program (Calculator)

4.3.1.2 Alpha Testing

[client]

- LDAP Authentication Entries
- Log4j Message Lookup Subtitution
- Remote JNDI Lookup Context

[attacker java http]

- Custom HTTP Header Request
- Log4j Message Lookup Subitition

[attacker java payload]

- Local Encrypted Reverse Shell

[bad USB]

- Local Payload Injection
- Curl Java HTTP Service

4.3.2 Prosedur Pengujian Kerentanan Sistem

[uji 2 : PTES]

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

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

4.3.2.1 Pre-Engagement

[hardware spec + container + bad usb]

[software spec + tools]

4.3.2.2 Intelligence Gathering

[dalemin info info aplikasi gui + sistem client]

[OWASP dependency check]

[OSSIndex Maven]

4.3.2.3 Threat Modelling

[attack trees]

4.3.2.4 Vulnerability Analysis

[dalemin cve-2021-44228 + cvss]

4.3.2.5 Exploitation

[berdasarkan attack tree : 2 attack vector]

[BadUSB M alware + Hands-on-Keyboard]

4.3.2.6 Post-Exploitation

[cronjopb – hidden daemon persistence]

4.3.2.7 Reporting

[mitigasi untuk exploit & post-exploitation]

4.3.2.8 Post-Mitigation Exploitation

[ulang tahapan exploit & post-exploitation]

4.4 Hasil Pengujian Aplikasi dan Sistem

[hasil pengujian whitebox, baik untuk aplikasi dan kerentanan sistem]

4.4.1 Evaluasi Hasil Pengujian Aplikasi

[test case sedian pake evaluation matrix, passed atau nda]

4.4.2 Evaluasi Hasil Pengujian Kerentanan Sistem

[evaluation matrix pre dan post mitigasi, tingkat keberhasilan]

BAB V
PENUTUP

5.1 Kesimpulan

ABC

5.2 Saran

ABC

DAFTAR PUSTAKA

Apache (2021) *Apache Log4j Security Vulnerabilities, Apache Software Foundation*. Available at: https://logging.apache.org/log4j/2.x/security.html (Accessed: 17 March 2022).

Biswas, S. *et al.* (2018) *A Study on Remote Code Execution Vulnerability in Web Applications, International Conference on Cyber Security and Computer Science*. Available at: https://www.researchgate.net/publication/328956499.

Calín, M. *et al.* (2020) *Software Vulnerabilities Overview: A Descriptive Study, Tsinghua Science and Technology*. doi:10.26599/TST.2019.9010003.

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

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

CVE (2021) *CVE-2021-44228, CVE Mitre Org.* Available at: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228 (Accessed: 4 May 2022).

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

Kaushik, K. *et al.* (2021) 'A Novel Approach to Generate a Reverse Shell: Exploitation and Prevention', *International Journal of Intelligent Communication, Computing, and Networks*, 2(2). doi:10.51735/ijiccn/001/33.

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

Muñoz, A. and Mirosh, O. (2016) *A Journey from JNDI/LDAP Manipulation to Remote Code Execution Dream Land, BlackHat USA*. Available at: https://www.blackhat.com/ (Accessed: 14 March 2022).

Oracle (2021) *Oracle Security Alert Advisory - CVE-2021-44228, Oracle Corporation*. Available at: https://www.oracle.com/security-alerts/alert-cve-2021-44228.html (Accessed: 17 March 2022).

Yin, K.S. and Khine, M.A. (2019) 'Optimal Remote Access Trojans Detection Based on Network Behavior', *International Journal of Electrical and Computer Engineering*, 9(3), pp. 2177–2184. doi:10.11591/ijece.v9i3.pp2177-2184.