DETEKSI *EXPLOIT REVERSE* HTTPS DENGAN METODE *DECISION TREE*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer (S1)

OLEH:

AZZAN DAFFA AL KAUTSAR

09011382025110

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

LEMBAR PENGESAHAN

DETEKSI EXPLOIT REVERSE HTTPS DENGAN METODE DECISION TREE

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer (S1)

Oleh:
AZZAN DAFFA AL KAUTSAR
09011382025110

Palembang, 16 Januari 2025
Mengetahui,

Pembimbing Tugas Akhir I	Pembimbing Tugas Akhir II
Prof. Ir. Deris Stiawan, M.T., Ph.D	**Nurul Afifah, M.Kom**
NIP. 197806172006041002	**NIP. 199211102023212049**

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.
NIP.196612032006041001

ii

AUTHENTICATION PAGE

DETECTION OF REVERSE HTTPS EXPLOIT USING THE DECISION TREE METHOD

SKRIPSI

Submitted To Complete One Of The Requirements For Obtaining A Bachelor's Degree in Computer Science

By:

AZZAN DAFFA AL KAUTSAR

09011382025110

Palembang, 16 January 2025

Acknowledge,

Final Project Advisor I	Final Project Advisor II
Prof. Ir. Deris Stiawan, M.T., Ph.D	**Nurul Afifah, M.Kom**
NIP. 197806172006041002	**NIP. 199211102023212049**

Head Of The Computer System Department

Dr. Ir. Sukemi, M.T.

NIP.196612032006041001

iii

LEMBAR PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Senin

Tanggal : 30 Desember 2024

Tim Penguji :

1. **Ketua : Huda Ubaya, S.T., M.T.**
2. **Penguji : Dr. Ir. Ahmad Heryanto, S.Kom., M.T.**
3. **Pembimbing I : Prof. Ir. Deris Stiawan, M.T., Ph.D.**
4. **Pembimbing II : Nurul Afifah, M.Kom.**

Mengetahui.

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP.196612032006041001

iv

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Azzan Daffa Al Kautsar

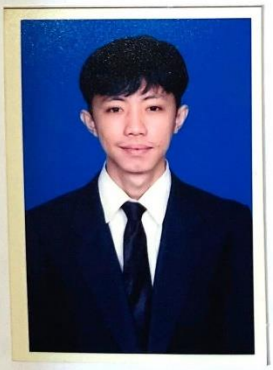
NIM : 09011382025110

Judul : Deteksi *Exploit Reverse* HTTPS Dengan Metode *Decision Tree*

Hasil Pengecekan Software *iThenticate/Turnitin* : 6%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil pengjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan tugas akhir ini, maka saya menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.



Palembang, Januari 2025

Yang menyatakan

Azzan Daffa Al Kautsar

NIM. 09011382025110

v

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh,

Puji dan syukur penulis ucapkan atas kehadirat Allah SWT. Yang telah melimpahkan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan penyusunan tugas akhir dengan judul **"Deteksi *Exploit Reverse HTTPS* dengan Metode *Decision Tree*"**.

Pada penyusunan tugas akhir ini tidak terlepas dari peran berbagai pihak yang telah memberikan dukungan doa, semangat, motivasi dan bimbingan pada penulis. Oleh karena itu, pada kesempatan ini penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Allah SWT. yang telah memberikan nikmat Kesehatan dan Kesempatan kepada penulis dalam penyusunan tugas akhir ini.
2. Kedua orang tua tercinta yang selalu memberikan dukungan moral maupun finansial, serta do'a yang tiada hentinya.
3. Bapak Dr. Erwin, M.Si selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
5. Bapak Prof. Ir. Deris Stiawan, M.T., Ph.D., IPU., ASEAN Eng., CPENT. selaku Dosen Pembimbing Akademik dan Pembimbing I Tugas Akhir Penulis yang telah meluangkan waktu untuk membimbing dan memberikan motivasi selama pengerjaan Tugas Akhir.
6. Mbak Nurul Afifah, M.Kom. selaku Pembimbing II Tugas Akhir yang telah meluangkan waktu untuk membimbing penulis dalam pengerjaan Tugas Akhir dari awal penulisan laporan Tugas Akhir.
7. Mbak Sari Anhar selaku admin yang telah membantu dalam proses administrasi Tugas Akhir Penulis.
8. Teman-teman satu kelompok riset yang selalu memberikan semangat dan solusi kepada penulis.
9. Teman-teman seperjuangan Jurusan Sistem Komputer Unggulan 2020.

10. Seluruh pihak yang tidak dapat penulis sebutkan satu per satu, yang telah memberikan semangat serta doa.
11. Almamater

Penulis menyadari bahwa laporan ini masih jauh dari kesempurnaan, oleh karena itu penulis dengan senang hati menerima kritik dan saran serta masukkan dari pembaca yang bersifat membangun agar lebih baik lagi dikemudian hari. Penulis berharap semoga laporan ini dapat bermanfaat bagi kita semua khususnya bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya. Demikian yang dapat penulis sampaikan.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Palembang, Januari 2025
Penulis,

Azzan Daffa Al Kautsar
NIM. 09011382025110

DETEKSI EXPLOIT REVERSE HTTPS DENGAN METODE DECISION TREE

Azzan Daffa Al Kautsar (09011382025110)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email: azzndfa31@gmail.com

ABSTRAK

Exploit Reverse HTTPS merupakan sebuah konsep teknik serangan malware yang dilakukan oleh penyerang untuk mengekspos kelemahan dalam lapisan HTTPS pada sistem atau aplikasi untuk mencuri atau mengambil informasi penting dari target. Penelitian ini menggunakan dataset dari COMNETS *Research Lab* Universitas Sriwijaya yang berupa data mentah dalam bentuk .pcap yang dihasilkan dari skenario eksperimen realistis untuk mendeteksi kelemahan pada lapisan HTTPS secara *Dynamic Analysis* dan metode *Decision Tree.* Hasil dari penelitian ini membuktikan bahwa metode *Decision Tree* mampu mendeteksi serangan *Reverse* HTTPS dengan mencapai performa terbaik dengan tingkat *accuracy* sebesar 97,36%.

Kata Kunci : *Android, Malware, Reverse HTTPS, Dynamic Analysis, Decision Tree.*

DETECTION OF REVERSE HTTPS EXPLOIT USING THE DECISION TREE METHOD

Azzan Daffa Al Kautsar (09011382025110)

Department Of Computer Systems, Faculty of Computer Science

Sriwijaya University

Email : azzndfa31@gmail.com

ABSTRACT

Reverse HTTPS Exploit is a malware attack technique used by attackers to exploit vulnerabilities in the HTTPS layer of systems or applications to steal or extract critical information from a target. This study utilizes a dataset from the COMNETS Research Lab at Universitas Sriwijaya, consisting of raw data in .pcap format generated from realistic experimental scenarios to identify weaknesses in the HTTPS layer through Dynamic Analysis and the Decision Tree method. The findings of this research demonstrate that the Decision Tree method is capable of detecting Reverse HTTPS attacks, achieving optimal performance with an accuracy rate of 97.36%.

Keywords : *Android, Malware, Reverse HTTPS, Dynamic Analysis, Decision Tree*

DAFTAR ISI

LEMBAR PENGESAHAN ..... Error! Bookmark not defined.

AUTHENTICATION PAGE ..... Error! Bookmark not defined.

LEMBAR PERSETUJUAN ..... Error! Bookmark not defined.

HALAMAN PERNYATAAN ..... Error! Bookmark not defined.

KATA PENGANTAR ..... **vi**

ABSTRAK ..... **viii**

ABSTRACT ..... **ix**

DAFTAR ISI ..... **x**

DAFTAR GAMBAR ..... **xiv**

DAFTAR TABEL ..... **xvii**

BAB I **1**

PENDAHULUAN **1**

1.1 Latar Belakang 1

1.2 Rumusan Masalah 2

1.3 Batasan Masalah 3

1.4 Tujuan Penelitian 3

1.5 Manfaat Penelitian 3

1.6 Metodologi Penelitian 4

1.6.1 Studi Pustaka (Literature) 4

1.6.2 Pengumpulan Data 4

1.6.3 Pemeriksaan 4

1.6.4 Analisis 5

1.6.5 Kesimpulan dan Saran 5

1.7 Sistematika Penulisan 5

BAB II ..... Error! Bookmark not defined.

TINJAUAN PUSTAKA ..... Error! Bookmark not defined.

2.1 Pendahuluan ..... **Error! Bookmark not defined.**

2.2 Penelitian Terkait ..... **Error! Bookmark not defined.**

2.3 Landasan Teori ..... **Error! Bookmark not defined.**

2.3.1 Android ..... **Error! Bookmark not defined.**

2.3.2 Andoid Package ..... **Error! Bookmark not defined.**

2.3.3 Malware ..... **Error! Bookmark not defined.**

2.3.4 Mobile Trojan Metasploit ..... **Error! Bookmark not defined.**

2.3.5 Deteksi Malware ..... **Error! Bookmark not defined.**

2.3.6 Visualisasi Malware ..... **Error! Bookmark not defined.**

2.3.7 Reverse HTTPS ..... **Error! Bookmark not defined.**

2.3.8 Wireshark ..... **Error! Bookmark not defined.**

2.3.9 CICFlowmeter ..... **Error! Bookmark not defined.**

2.3.10 Machine Learning ..... **Error! Bookmark not defined.**

2.3.11 Decision Tree ..... **Error! Bookmark not defined.**

2.3.12 Confusion Matrix ..... **Error! Bookmark not defined.**

BAB III ..... Error! Bookmark not defined.

METODOLOGI PENELITIAN ..... Error! Bookmark not defined.

3.1 Pendahuluan ..... **Error! Bookmark not defined.**

3.2 Spesifikasi Software dan Hardware ..... **Error! Bookmark not defined.**

3.2.1 Perangkat Lunak (Software) ..... **Error! Bookmark not defined.**

3.2.2 Perangkat Keras (Hardware) ..... **Error! Bookmark not defined.**

3.3 Kerangka Kerja Penelitian ..... **Error! Bookmark not defined.**

3.4 Perancangan Sistem ..... **Error! Bookmark not defined.**

3.5 Dataset ..... **Error! Bookmark not defined.**

3.6 Dynamic Analysis ..... **Error! Bookmark not defined.**

3.7 Identifikasi Sumber Data ..... **Error! Bookmark not defined.**

3.8 Proses Pembuatan Fitur (Label) ..... **Error! Bookmark not defined.**
3.9 Data Understanding ..... **Error! Bookmark not defined.**
3.10 Exploratory Data Analysis ..... **Error! Bookmark not defined.**
3.11 Preprocessing ..... **Error! Bookmark not defined.**
3.11.1 Feature Selection ..... **Error! Bookmark not defined.**
3.11.2 Label Encoder ..... **Error! Bookmark not defined.**
3.12 Random Oversampling ..... **Error! Bookmark not defined.**
3.13 Splitting Data ..... **Error! Bookmark not defined.**
3.14 Decision Tree ..... **Error! Bookmark not defined.**
3.14.1 Kriteria Model ..... **Error! Bookmark not defined.**
3.14.2 Import Library ..... **Error! Bookmark not defined.**
3.14.3 Train Test Split ..... **Error! Bookmark not defined.**
3.14.4 Model Fit ..... **Error! Bookmark not defined.**
3.14.5 Model Predict ..... **Error! Bookmark not defined.**
3.14.6 Hasil Prediksi ..... **Error! Bookmark not defined.**
3.15 Visualisasi Decision Tree ..... **Error! Bookmark not defined.**
3.16 Evaluasi Model ..... **Error! Bookmark not defined.**
BAB IV ..... Error! Bookmark not defined.
HASIL DAN ANALISIS ..... Error! Bookmark not defined.
4.1 Pendahuluan ..... **Error! Bookmark not defined.**
4.2 Identifikasi Sumber dan Ekstraksi Data ..... **Error! Bookmark not defined.**
4.3 Analisa Data ..... **Error! Bookmark not defined.**
4.3.1 Persiapan Lingkungan Terkendali ..... **Error! Bookmark not defined.**
4.3.2 Behavioral Dynamic Analysis ..... **Error! Bookmark not defined.**
4.4 Pembuatan Label di Dataset ..... **Error! Bookmark not defined.**
4.5 Data Understanding ..... **Error! Bookmark not defined.**
4.6 Exploratory Data Analysis ..... **Error! Bookmark not defined.**
4.7 Preprocessing ..... **Error! Bookmark not defined.**

4.7.1 Feature Selection ..... **Error! Bookmark not defined.**

4.7.2 Label Encoder ..... **Error! Bookmark not defined.**

4.8 Random Oversampling ..... **Error! Bookmark not defined.**

4.9 Splitting Data ..... **Error! Bookmark not defined.**

4.10 Model Decision Tree ..... **Error! Bookmark not defined.**

4.11 Validasi Hasil ..... **Error! Bookmark not defined.**

4.11.1 Gini Index ..... **Error! Bookmark not defined.**

4.11.2 Entropy ..... **Error! Bookmark not defined.**

4.11.3 Evaluasi Nilai Validasi Data Training dan Data Testing .**Error! Bookmark not defined.**

4.12 Visualisasi Decision Tree ..... **Error! Bookmark not defined.**

BAB V ..... Error! Bookmark not defined.

KESIMPULAN DAN SARAN ..... Error! Bookmark not defined.

5.1 Kesimpulan ..... **Error! Bookmark not defined.**

5.1 Saran ..... **Error! Bookmark not defined.**

DAFTAR PUSTAKA **7**

DAFTAR GAMBAR

Gambar 2.1 Ilustrasi Struktur Decision Tree.....**Error! Bookmark not defined.**
Gambar 2.2 Contoh Confusion Matrix.....**Error! Bookmark not defined.**
Gambar 3.1 Kerangka Kerja Penelitian .....**Error! Bookmark not defined.**
Gambar 3.2 Perancangan Sistem.....**Error! Bookmark not defined.**
Gambar 3.3 Skenario Topologi .....**Error! Bookmark not defined.**
Gambar 3.4 Upaya TA mengirim Trojan ke 2 calon korban **Error! Bookmark not defined.**
Gambar 3.5 Sesi Reverse HTTPS yang didapatkan TA 2 dari korban..... **Error! Bookmark not defined.**
Gambar 3.6 Feature Selection.....**Error! Bookmark not defined.**
Gambar 3.7 Label Encoder .....**Error! Bookmark not defined.**
Gambar 3.8 Flowchart Random Oversampling .....**Error! Bookmark not defined.**
Gambar 3.9 Random Oversampling.....**Error! Bookmark not defined.**
Gambar 3.10 Splitting Data.....**Error! Bookmark not defined.**
Gambar 3.11 Import Library .....**Error! Bookmark not defined.**
Gambar 3.12 Train Test Split .....**Error! Bookmark not defined.**
Gambar 3.13 Pembuatan Model Decision Tree .....**Error! Bookmark not defined.**
Gambar 3.14 Model Predict .....**Error! Bookmark not defined.**
Gambar 3.15 Hasil Prediksi .....**Error! Bookmark not defined.**
Gambar 4.1 Tampilan Dataset *Victim Reverse* HTTPS.pcap **Error! Bookmark not defined.**
Gambar 4.2 Proses Ekstraksi Data menggunakan CICFLowMeter..... **Error! Bookmark not defined.**
Gambar 4.3 Hasil Ekstraksi Dataset Victim Reverse HTTPS.....**Error! Bookmark not defined.**
Gambar 4.4 Tampilan Oracle VM VirtualBox .....**Error! Bookmark not defined.**
Gambar 4.5 Tampilan Suricata.....**Error! Bookmark not defined.**
Gambar 4.6 Membuka Rules pada Suricata.....**Error! Bookmark not defined.**
Gambar 4.7 Membuat Rules pada Suricata.....**Error! Bookmark not defined.**
Gambar 4.8 Membuka File Konfigurasi Suricata ..**Error! Bookmark not defined.**

Gambar 4.9 Menambahkan local.rules ke bagian rule-files. **Error! Bookmark not defined.**
Gambar 4.10 Menjalankan Suricata..... **Error! Bookmark not defined.**
Gambar 4.11 Hasil Alerts Suricata..... **Error! Bookmark not defined.**
Gambar 4.12 Mengkategorikan Malware ..... **Error! Bookmark not defined.**
Gambar 4.13 Sebelum Pembuatan Label ..... **Error! Bookmark not defined.**
Gambar 4.14 Setelah Pembuatan Label ..... **Error! Bookmark not defined.**
Gambar 4.15 Diagram Lingkaran Exploratory Data Analysis .... **Error! Bookmark not defined.**
Gambar 4.16 Grafik Histogram Exploratory Data Analysis **Error! Bookmark not defined.**
Gambar 4.17 Mengecek DataFrame dan Baris Duplikat ..... **Error! Bookmark not defined.**
Gambar 4.18 Menghapus Baris Duplikat..... **Error! Bookmark not defined.**
Gambar 4.19 Feature Selection pada Data..... **Error! Bookmark not defined.**
Gambar 4.20 Data setelah Label Encoder..... **Error! Bookmark not defined.**
Gambar 4.21 Tipe Data setelah Label Encoder..... **Error! Bookmark not defined.**
Gambar 4.22 Hasil Random Oversampling ..... **Error! Bookmark not defined.**
Gambar 4.23 Split Data..... **Error! Bookmark not defined.**
Gambar 4.24 Model Decision Tree ..... **Error! Bookmark not defined.**
Gambar 4.25 Pembagian Data Training dan Data Testing 50:50 **Error! Bookmark not defined.**
Gambar 4.26 Confusion Matrix pada Data 50:50 .. **Error! Bookmark not defined.**
Gambar 4.27 Grafik Precision Recall pada Data 50:50 ..... **Error! Bookmark not defined.**
Gambar 4.28 Grafik ROC pada Data 50:50 ..... **Error! Bookmark not defined.**
Gambar 4. 29 Grafik Information Gain pada Data 50:50 .... **Error! Bookmark not defined.**
Gambar 4.30 Pembagian Data Training dan Data Testing 60:40 **Error! Bookmark not defined.**
Gambar 4.31 Confusion Matrix pada Data 60:40 .. **Error! Bookmark not defined.**

Gambar 4.32 Grafik Precision Recall pada Data 60:40 ..... **Error! Bookmark not defined.**
Gambar 4.33 Grafik ROC pada Data 60:40 .....**Error! Bookmark not defined.**
Gambar 4.34 Grafik Information Gain pada Data 60:40 ..... **Error! Bookmark not defined.**
Gambar 4.35 Pembagian Data Training dan Data Testing 70:30 **Error! Bookmark not defined.**
Gambar 4.36 Confusion Matrix pada Data 70:30 .**Error! Bookmark not defined.**
Gambar 4.37 Grafik Precision-Recall pada Data 70:30..... **Error! Bookmark not defined.**
Gambar 4.38 Grafik ROC pada Data 70:30 .....**Error! Bookmark not defined.**
Gambar 4.39 Grafik Information Gain pada Data 70:30 ..... **Error! Bookmark not defined.**
Gambar 4.40 Pembagian Data Training dan Data Testing 80:20 **Error! Bookmark not defined.**
Gambar 4.41 Confusion Matrix pada Data 80:20 ..**Error! Bookmark not defined.**
Gambar 4.42 Grafik Precision-Recall pada Data 80:20..... **Error! Bookmark not defined.**
Gambar 4.43 Grafik ROC pada Data 80:20 .....**Error! Bookmark not defined.**
Gambar 4.44 Grafik Information Gain pada Data 80:20 ..... **Error! Bookmark not defined.**
Gambar 4.45 Pembagian Data Training dan Data Testing 90:10 **Error! Bookmark not defined.**
Gambar 4.46 Confusion Matrix pada Data 90:10 ..**Error! Bookmark not defined.**
Gambar 4.47 Grafik Precision-Recall pada Data 90:10..... **Error! Bookmark not defined.**
Gambar 4.48 Grafik ROC pada Data 90:10 .....**Error! Bookmark not defined.**
Gambar 4.49 Grafik Information Gain pada Data 90:10 ..... **Error! Bookmark not defined.**
Gambar 4.50 Pembagian Data Training dan Data Testing 50:50 **Error! Bookmark not defined.**
Gambar 4.51 Confusion Matrix pada Data 50:50 ..**Error! Bookmark not defined.**

Gambar 4.52 Grafik Precision-Recall (Entropy) pada Data 50:50 ..... **Error! Bookmark not defined.**
Gambar 4.53 Grafik ROC (Entropy) pada Data 50:50 ..... **Error! Bookmark not defined.**
Gambar 4.54 Grafik Information Gain (Entropy) pada Data 50:50..... **Error! Bookmark not defined.**
Gambar 4.55 Pembagian Data Training dan Data Testing 60:40 **Error! Bookmark not defined.**
Gambar 4.56 Confusion Matrix pada Data 60:40 ..**Error! Bookmark not defined.**
Gambar 4.57 Grafik Precision-Recall pada Data 60:40..... **Error! Bookmark not defined.**
Gambar 4.58 Grafik ROC pada Data 60:40 .....**Error! Bookmark not defined.**
Gambar 4.59 Grafik Information Gain pada Data 60:40 ..... **Error! Bookmark not defined.**
Gambar 4.60 Pembagian Data Training dan Data Testing 70:30 **Error! Bookmark not defined.**
Gambar 4.61 Confusion Matrix pada Data 70:30 ..**Error! Bookmark not defined.**
Gambar 4.62 Grafik Precision-Recall pada Data 70:30..... **Error! Bookmark not defined.**
Gambar 4.63 Grafik ROC pada Data 70:30 .....**Error! Bookmark not defined.**
Gambar 4.64 Grafik Information Gain pada Data 70:30 ..... **Error! Bookmark not defined.**
Gambar 4.65 Pembagian Data Training dan Data Testing 80:20 **Error! Bookmark not defined.**
Gambar 4.66 Confusion Matrix pada Data 80:20 ..**Error! Bookmark not defined.**
Gambar 4.67 Grafik Precision-Recall pada Data 80:20..... **Error! Bookmark not defined.**
Gambar 4.68 Grafik ROC pada Data 80:20 .....**Error! Bookmark not defined.**
Gambar 4.69 Grafik Indormation Gain pada Data 80:20..... **Error! Bookmark not defined.**
Gambar 4.70 Pembagian Data Training dan Data Testing 90:10 **Error! Bookmark not defined.**

Gambar 4.71 Confusion Matrix pada Data 90:10 ..**Error! Bookmark not defined.**
Gambar 4.72 Grafik Precision-Recall pada Data 90:10..... **Error! Bookmark not defined.**
Gambar 4.73 Grafik ROC pada Data 90:10 .....**Error! Bookmark not defined.**
Gambar 4.74 Grafik Information Gain pada Data 90:10 ..... **Error! Bookmark not defined.**
Gambar 4.75 Visualisasi Decision Tree .....**Error! Bookmark not defined.**

DAFTAR TABEL

Tabel 2.1 Studi Pustaka ..... **Error! Bookmark not defined.**
Tabel 2.2 Perbandingan Algoritma DT yang Umum digunakan. **Error! Bookmark not defined.**
Tabel 3.1 Spesifikasi Software ..... **Error! Bookmark not defined.**
Tabel 3.2 Spesifikasi Hardware ..... **Error! Bookmark not defined.**
Tabel 3.3 Perangkat pada pembuatan skenario ..... **Error! Bookmark not defined.**
Tabel 3.4 Spesifikasi VPS ..... **Error! Bookmark not defined.**
Tabel 3.5 Dataset Normal Traffic ..... **Error! Bookmark not defined.**
Tabel 3.6 Dataset Victim Reverse HTTPS ..... **Error! Bookmark not defined.**
Tabel 3.7 Dataset *Attack* & Normal TA Network... **Error! Bookmark not defined.**
Tabel 3.8 Penjelasan Fitur pada Dataset ..... **Error! Bookmark not defined.**
Tabel 3.9 Evaluasi Model ..... **Error! Bookmark not defined.**
Tabel 4.1 Nilai Validasi Data Training dan Data Testing 50:50 .. **Error! Bookmark not defined.**
Tabel 4.2 Nilai Validasi Data Training dan Data Testing 60:40 .. **Error! Bookmark not defined.**
Tabel 4.3 Nilai Validasi Data Training dan Data Testing 70:30 .. **Error! Bookmark not defined.**
Tabel 4.4 Nilai Validasi Data Training dan Data Testing 80:20 .. **Error! Bookmark not defined.**
Tabel 4.5 Nilai Validasi Data Training dan Data Testing 90:10 .. **Error! Bookmark not defined.**
Tabel 4.6 Nilai Validasi Data Training dan Data Testing 50:50 .. **Error! Bookmark not defined.**
Tabel 4.7 Nilai Validasi Data Training dan Data Testing 60:40 .. **Error! Bookmark not defined.**
Tabel 4.8 Nilai Validasi Data Training dan Data Testing 70:30 .. **Error! Bookmark not defined.**
Tabel 4.9 Nilai Validasi Data Training dan Data Testing 80:20 .. **Error! Bookmark not defined.**

Tabel 4.10 Nilai Validasi Data Training dan Data Testing 90:10 **Error! Bookmark not defined.**
Tabel 4.11 Perbandingan Validasi Hasil Gini.....**Error! Bookmark not defined.**
Tabel 4.12 Perbandingan Validasi Hasil Entropy...**Error! Bookmark not defined.**
Tabel 4.13 Perbandingan Hasil Gini dan Entropy..**Error! Bookmark not defined.**

BAB I
PENDAHULUAN

1.1 Latar Belakang

Era di mana aplikasi mobile semakin menguasai pengalaman digital, keamanan aplikasi Android menjadi fokus utama. Android, sebagai sistem operasi seluler yang dominan, menghadapi tantangan keamanan yang signifikan karena tingginya tingkat adopsi dan keterbukaan platform. Malware Android menimbulkan ancaman serius yang dapat menyebabkan kerugian finansial, pencurian data, dan gangguan pada perangkat pengguna.

Eksploit Reverse HTTPS adalah sebuah konsep teknik serangan yang dapat dimanfaatkan oleh pihak yang tidak berwenang untuk mengekspos kelemahan dalam lapisan keamanan HTTPS pada sistem atau aplikasi Android[1]. Latar belakang ini bertujuan untuk menyelidiki dan memahami tantangan keamanan yang muncul akibat potensi eksploitasi reverse HTTPS dalam konteks aplikasi Android.

Machine learning telah menjadi bagian integral dari perkembangan teknologi, memberikan kemampuan sistem untuk belajar dari data dan meningkatkan kinerja tanpa perlu pemrograman yang eksplisit. Decision Tree adalah salah satu teknik machine learning yang digunakan untuk pengambilan keputusan dan klasifikasi data[2]. Secara visual, Decision Tree dapat diibaratkan sebagai pohon keputusan, di mana setiap cabang mewakili keputusan atau pengujian terhadap suatu fitur, dan setiap daun mewakili hasil akhir atau klasifikasi. Algoritma ini bekerja dengan membagi data menjadi subset berdasarkan fitur-fitur yang paling informatif, membentuk struktur pohon keputusan yang dapat dengan cepat dan efektif mengklasifikasikan data baru[3].

Penelitian menggunakan Mobile-TrojanMetasploit Traffic Dataset sebagai basis data, yang dihasilkan dari skenario eksperimen yang mendekati kejadian nyata. Dataset ini mencakup informasi terkait aplikasi yang mencoba melakukan eksploitasi reverse HTTPS, memberikan dasar yang kuat untuk

pengujian dan pengembangan metode deteksi. Penggunaan Mobile-TrojanMetasploit Traffic Dataset dari skenario eksperimen yang mendekati kejadian nyata memberikan nilai tambah signifikan pada penelitian ini. Dataset ini menciptakan lingkungan uji yang realistis, memungkinkan penelitian untuk lebih efektif memodelkan ancaman siber yang sebenarnya[4].

Menurut penelitian "Automatic detection of cyberbullying using multi-feature based artificial intelligence with deep decision tree classification"[5] memiliki performa akurasi 93%. Penelitian ini bertujuan untuk mengembangkan model klasifikasi otomatis baru yang mengidentifikasi teks-teks cyberbullying tanpa memasangkannya ke dalam ruang berdimensi besar.

Menurut penelitian "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade"[6] memiliki performa dengan akurasi 88%. Penelitian ini bertujuan untuk mengetahui efektifitas Machine Learning tiap tahun.

Menurut penelitian "Early Detection of the Advanced Persistent Threat Attack Using Performance Analysis of Deep Learning"[7]. Penelitian ini memiliki performa dengan akurasi 95%. Penelitian ini bertujuan untuk mendeteksi Advanced Persistent Threat (APT).

Menurut penelitian "TROJAN TRAFFIC DETECTION BASED ON MACHINE LEARNING"[8] memiliki performa dengan akurasi 96%. Penelitian ini bertjuan untuk menganalisis fitur perilaku jaringan dan lalu lintas jaringan dari beberapa Trojan khas seperti Zeus dan Weasel, dan mengusulkan algoritma deteksi lalu lintas Trojan berdasarkan Machine Learning.

Menurut penelitian "Malware Detection: A Framework for Reverse Engineered Android Applications Through Machine Learning Algorithms"[9] memiliki performa akurasi 96 %. Penelitian ini bertujuan mendeteksi malware pada aplikasi Android.

1.2 Rumusan Masalah

Berikut ini rumusan masalah penelitian Tugas Akhir yang akan dilakukan:

1. Bagaimana cara melakukan ekstraksi fitur pada dataset *Victim Reverse* HTTPS?
2. Bagaimana cara mendeteksi *Behavior Exploit Reverse* HTTPS pada dataset *Victim Reverse* HTTPS secara *Dynamic Analysis*?
3. Bagaimana hasil validasi dari deteksi menggunakan metode *Decision Tree* pada dataset dan sejauh mana model dapat mendeteksi secara akurat?

1.3 Batasan Masalah

Berikut ini rumusan masalah penelitian Tugas Akhir yang akan dilakukan:

1. Dataset penelitian ini menggunakan dataset pada *Mobile-TrojanMetasploit Traffic*, terutama pada skenario 2 *Victim Reverse* HTTPS yang akan dianalisis.
2. Penelitian ini berfokus secara *Dynamic Analysis* dan *Decision Tree* dalam mendeteksi serangan pada *Reverse Victim* HTTPS dari Aplikasi pada dataset *Network Traffic Mobile-TrojanMetasploit* untuk menganalisis pola-pola karakteristik serangan.
3. Menggunakan *Random Oversampling* untuk menangani masalah dataset yang imbalance pada *Reverse Victim* HTTPS.
4. Nilai performa yang diukur adalah accuracy, precision, recall dan f1-score.

1.4 Tujuan Penelitian

Berikut ini merupakan tujuan dari penelitian Tugas Akhir yang dilakukan:

1. Melakukan ekstraksi pada dataset yang awalnya format .pcap menjadi .csv dengan menggunakan *CICFlowMeter.*
2. Menerapkan model Decision Tree untuk mendeteksi *Exploit Reverse* HTTPS pada Aplikasi melalui *Network Traffic.*
3. Melakukan analisa hasil kinerja dari proses deteksi yang dihasilkan menggunakan *Dynamic Analysis* dan Decision Tree untuk memperoleh model terbaik.

1.5 Manfaat Penelitian

Berikut ini merupakan manfaat dari penelitian Tugas Akhir yang dilakukan:

1. Menambah wawasan mengenai ekstraksi proses dataset dengan *CICFlowMeter.*
2. Dapat mengetahui *Behavior Exploit Reverse* HTTPS dari *Network Traffic* dengan cara *Dynamic Analysis* dan *Decision Tree.*

Hasil penelitian ini dapat menjadi dasar untuk pengembangan lebih lanjut dalam perlindungan data dan keamanan di dunia digital.

1.6 Metodologi Penelitian

Metodologi penelitian yang diterapkan pada penelitian Tugas Akhir ini mencakup beberapa tahapan sebagai berikut:

1.6.1 Studi Pustaka (Literature)

Pada tahapan ini mencari dan mengumpulkan referensi berupa literature yang berkaitan dengan *Behavior Exploit Reverse HTTPS, Dynamic Analysis, Decision Tree, Random Oversampling* dan lainnya yang diperlukan dalam proses penelitian.

1.6.2 Pengumpulan Data

Tahap ini merupakan tahapan awal dalam pengumpulan data dengan tahapan sebagai berikut:

a. Dynamic Analysis

Melakukan *Dynamic Analysis* untuk mengetahui serangan atau aktivitas yang mencurigakan di lalu lintas jaringan pada dataset *Mobile-TrojanMetasploit Traffic* skenario percobaan ke 2 yaitu *Victim Reverse* HTTPS.

b. Identifikasi Sumber Data

Menentukan sumber, jenis, dan karakteristik data bahwa analisis tersebut relevan dengan dataset *Mobile-TrojanMetasploit Traffic* pada skenario *Victim Reverse* HTTPS.

c. Ekstraksi Data

Ekstraksi data dari sumber yang teridentifikasi, hal ini melibatkan ektraksi pada dataset *Victim Reverse HTTPS* untuk dianalsis.

1.6.3 Pemeriksaan

Tahap selanjutnya adalah pemeriksaan dengan melakukan ekstraksi data yang telah dilakukan dengan tahapan berikut:

a. Membuat Label

Melabeli data untuk diklasifikasikan bahwa data tersebut termasuk kedalam *Benign* atau *ReverseHTTPS.*

b. Exploratory Data Analysis

Exploratory Data Analysis adalah proses analisis data awal untuk memahami karakteristiknya, menemukan pola, mengidentifikasi anomali, dan memverifikasi hipotesis dengan cara statistik dan visualisasi.

c. Preprocessing

Mengubah data mentah menjadi format yang lebih bersih sebelum dianalisis seperti nilai yang hilang, normalisasi, dan label encoder.

1.6.4 Analisis

Metode ini dilakukan dengan menganalisa hasil deteksi yang didapat dari hasil proses pada dataset *Victim Reverse* HTTPS.

a. Pembangunan Decision Tree

Menggunakan dataset *Victim Reverse* HTTPS yang telah disiapkan dengan menyesuaikan parameternya dan kriteria pemilihan node.

b. Evaluasi Model

Tahapan ini menggunakan metrik seperti *Accuracy, Precision, Recall,* dan *F1-Score* untuk mengukur kinerja model.

1.6.5 Kesimpulan dan Saran

Tahap ini merupakan langkah akhir setelah menganalisa penelitian secara keseluruhan untuk membuat suatu kesimpulan dan saran yang dibutuhkan bagi para peneliti selanjutnya.

a. Dokumentasi Hasil

Mencatat dan menyusun hasil analisis data dengan metode Decision Tree yang disertai deskripsi pada model, aturan keputusan, dan hasil evaluasi.

b. Interpretasi Kesimpulan

Memberikan hasil analisis yang diperoleh dari analisa data dalam penelitian ini kemudian di tulis ke dalam kesimpulan.

1.7 Sistematika Penulisan

Berikut ini merupakan sistematika yang digunakan dalam penelitian Tugas Akhir ini:

BAB I PENDAHULUAN

Bab ini terdapat Latar Belakang penelitian yang dilakukan, Rumusan Masalah, Batasan Masalah, Tujuan Penelitan, Manfaat Penelitian, Metodologi Penelitian dan Sistematika Penelitian.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan mengenai HTTPS, Dynamic Analysis, Metode Decision Tree, Dataset yang digunakan, review literatur tentang penggunaan terkini dalam proses Dynamic Analysis Malware dan Decision Tree dalam Keamanan Jaringan.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan mengenai Langkah-langkah (Metodologi) penelitian, diagram alur (FlowChart) dan tahapan perancangan sistem pada tugas akhir ini.

BAB IV HASIL DAN ANALISA

Bab ini menjelaskan hasil dari proses pengolahan data yang sudah dilakukan, dan dari hasil tersebut akan dilakukan analisa supaya mendapatkan data terbaik dan akurat.

BAB V KESIMPULAN DAN SARAN

Bab ini menjelaskan kesimpulan yang didapatkan berdasarkan hasil dan analisa yang diperoleh setelah melakukan penelitian, kemudian memberikan saran agar dapat dilakukan pengembangan untuk penelitian kedepannya.

DAFTAR PUSTAKA

[1] J. Carrillo-Mondejar, H. Turtiainen, A. Costin, J. L. Martinez, and G. Suarez-Tangil, "HALE-IoT: Hardening Legacy Internet of Things Devices by Retrofitting Defensive Firmware Modifications and Implants," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8371–8394, 2023, doi: 10.1109/JIOT.2022.3224649.

[2] S. Lee, C. Lee, K. G. Mun, and D. Kim, "Decision Tree Algorithm Considering Distances between Classes," *IEEE Access*, vol. 10, no. April, pp. 69750–69756, 2022, doi: 10.1109/ACCESS.2022.3187172.

[3] I. Shhadat, B. Bataineh, A. Hayajneh, and Z. A. Al-Sharif, "The Use of Machine Learning Techniques to Advance the Detection and Classification of Unknown Malware," *Procedia Comput. Sci.*, vol. 170, no. 2019, pp. 917–922, 2020, doi: 10.1016/j.procs.2020.03.110.

[4] "Mobile-TrojanMetasploit Traffic Dataset Sebagai bentuk upaya untuk melakukan penelitian pada kasus," pp. 2–5.

[5] N. Yuvaraj *et al.*, "Automatic detection of cyberbullying using multi-feature based artificial intelligence with deep decision tree classification," *Comput. Electr. Eng.*, vol. 92, no. September 2020, 2021, doi: 10.1016/j.compeleceng.2021.107186.

[6] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade," *IEEE Access*, vol. 8, pp. 222310–222354, 2020, doi: 10.1109/ACCESS.2020.3041951.

[7] J. H. Joloudari, M. Haderbadi, A. Mashmool, M. Ghasemigol, S. S. Band, and A. Mosavi, "Early detection of the advanced persistent threat attack using performance analysis of deep learning," *IEEE Access*, vol. 8, pp. 186125–186137, 2020, doi: 10.1109/ACCESS.2020.3029202.

[8] Z. Ma, Y. Huang, and J. Lu, "Trojan Traffic Detection based on Machine

Learning," *2020 17th Int. Comput. Conf. Wavelet Act. Media Technol. Inf. Process. ICCWAMTIP 2020*, pp. 157–160, 2020, doi: 10.1109/ICCWAMTIP51612.2020.9317515.

[9] B. Urooj, M. A. Shah, C. Maple, M. K. Abbasi, and S. Riasat, "Malware Detection: A Framework for Reverse Engineered Android Applications Through Machine Learning Algorithms," *IEEE Access*, vol. 10, no. February, pp. 89031–89050, 2022, doi: 10.1109/ACCESS.2022.3149053.

[10] Z. Azam, M. M. Islam, and M. N. Huda, "Comparative Analysis of Intrusion Detection Systems and Machine Learning-Based Model Analysis Through Decision Tree," *IEEE Access*, vol. 11, no. August, pp. 80348–80391, 2023, doi: 10.1109/ACCESS.2023.3296444.

[11] J. Jeon, J. H. Park, and Y. Jeong, "Dynamic Analysis for IoT Malware Detection With Convolution Neural Network Model," vol. 8, pp. 96899–96911, 2020, doi: 10.1109/ACCESS.2020.2995887.

[12] S. K. Smmarwar, G. P. Gupta, and S. Kumar, "Android malware detection and identification frameworks by leveraging the machine and deep learning techniques: A comprehensive review," *Telemat. Informatics Reports*, vol. 14, no. November 2023, p. 100130, 2024, doi: 10.1016/j.teler.2024.100130.

[13] K. Hynek, D. Vekshin, J. A. N. Luxemburk, A. Wasicek, and S. Member, "Summary of DNS Over HTTPS Abuse," *IEEE Access*, vol. 10, pp. 54668–54680, 2022, doi: 10.1109/ACCESS.2022.3175497.

[14] D. O. Sahin, S. Akleylek, and E. Kilic, "LinRegDroid: Detection of Android Malware Using Multiple Linear Regression Models-Based Classifiers," *IEEE Access*, vol. 10, pp. 14246–14259, 2022, doi: 10.1109/ACCESS.2022.3146363.

[15] G. Karatas, O. Demir, and O. K. Sahingoz, "Increasing the Performance of Machine Learning-Based IDSs on an Imbalanced and Up-to-Date Dataset," *IEEE Access*, vol. 8, pp. 32150–32162, 2020, doi: 10.1109/ACCESS.2020.2973219.

[16] J. Velasco-Mata, V. Gonzalez-Castro, E. F. Fernandez, and E. Alegre, “Efficient Detection of Botnet Traffic by Features Selection and Decision Trees,” *IEEE Access*, vol. 9, pp. 120567–120579, 2021, doi: 10.1109/ACCESS.2021.3108222.

[17] S. D. Alotaibi *et al.*, “Bioinspired artificial intelligence based android malware detection and classification for cybersecurity applications,” *Alexandria Eng. J.*, vol. 100, no. March, pp. 142–152, 2024, doi: 10.1016/j.aej.2024.05.038.

[18] N. Gregório, J. Bispo, J. P. Fernandes, and S. Queiroz de Medeiros, “E-APK: Energy pattern detection in decompiled android applications,” *J. Comput. Lang.*, vol. 76, no. May, p. 101220, 2023, doi: 10.1016/j.cola.2023.101220.

[19] G. Kale, G. E. Bostancı, and F. V. Çelebi, “Evolutionary feature selection for machine learning based malware classification,” *Eng. Sci. Technol. an Int. J.*, vol. 56, no. July 2024, p. 101762, 2024, doi: 10.1016/j.jestch.2024.101762.

[20] R. Kumar, X. Zhang, W. Wang, J. A. Y. Kumar, and A. Sharif, “A Multimodal Malware Detection Technique for Android IoT Devices Using Various Features,” 2020.

[21] E. Chatzoglou, V. Kouliaridis, G. Kambourakis, G. Karopoulos, and S. Gritzalis, “A hands-on gaze on HTTP/3 security through the lens of HTTP/2 and a public dataset,” *Comput. Secur.*, vol. 125, p. 103051, 2023, doi: 10.1016/j.cose.2022.103051.

[22] L. F. Sikos, “Packet analysis for network forensics: A comprehensive survey,” *Forensic Sci. Int. Digit. Investig.*, vol. 32, p. 200892, 2020, doi: 10.1016/j.fsidi.2019.200892.

[23] K. Mahmud, S. Azam, A. Karim, S. Zobaed, B. Shanmugam, and D. Mathur, “Machine Learning Based PV Power Generation Forecasting in Alice Springs,” *IEEE Access*, vol. 9, pp. 46117–46128, 2021, doi: 10.1109/ACCESS.2021.3066494.

[24] D. M. Rodríguez, M. P. Cuéllar, and D. P. Morales, “On the fusion of soft-decision-trees and concept-based models,” *Appl. Soft Comput.*, vol. 160, no. March 2023, p. 111632, 2024, doi: 10.1016/j.asoc.2024.111632.

[25] G. Phillips *et al.*, “Setting nutrient boundaries to protect aquatic communities: The importance of comparing observed and predicted classifications using measures derived from a confusion matrix,” *Sci. Total Environ.*, vol. 912, no. July 2023, 2024, doi: 10.1016/j.scitotenv.2023.168872.