Profiling Attack Surface Safe Exam Browser (Seb)

1st Refsi Gusniarti
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
refsig@student.telkomuniversity.ac.id

2nd Yudha Purwanto
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
omyudha@telkomuniversity.ac.id

3rd Muhammad Faris
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
muhammadfaris@telkomuniversity.ac.id

***Abstrak* — Ujian daring merupakan perkembangan dari era teknologi yang awalnya ujian itu harus bertatap muka namun kini bisa dilakukan dimana saja dengan menggunakan platform *e-learning*, namun disisi lain dengan adanya ujian daring ini akan mendapati titik celah rentan keamanan sehingga bisa didapati beberapa celah untuk melakukan tindak kecurangan selama ujian. Safe Exam Browser (SEB) merupakan browser ujian yang aman dan paling sering digunakan, aplikasi tersebut memungkinkan penggunanya untuk dibatasi hak akses kepada situs web, sistem, dan aplikasi eksternal.**

Solusi alternatif yang ditawarkan pada penelitian ini adalah melakukan pengujian keamanan terhadap aplikasi Safe Exam Browser untuk diuji keamanannya melalui beberapa aplikasi untuk diketahui celah keamanannya dan menjadi bahan evaluasi terhadap penggunaan Safe Exam Browser. Sehingga dapat meminimalisir tindak kecurangan selama ujian pada penggunaan Safe Exam Browser

Sistem yang diimplementasikan adalah melakukan eksekusi penyerangan terhadap aplikasi Safe Exam Browser pada aplikasi perangkat *virtual*, aplikasi *mirroring*, dan aplikasi yang dapat menangkap *packet traffic*. Hasil pengujian didapati kesimpulan bahwa Safe Exam Browser dapat dijalankan pada aplikasi *virtual machine*, dapat melakukan *mirroring* melalui aplikasi AnyDesk, dan dapat menangkap informasi selama penggunaan Safe Exam Browser melalui aplikasi Wireshark.

***Kata kunci :* Safe Exam Browser, virtual machine, AnyDesk, Wireshark. System, Study Program Accreditation 4.0, Lecturer, SAW**

I. PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan mengajar dan pembelajaran khususnya pada jarak edukasi dengan kehadirannya World Wide Web (WWW) telah meningkatkan metode pembelajaran atau mengajar yang baru dengan konsep pembelajaran online atau biasa disebut dengan *e-learning*, metode e-learning ini banyak digunakan dan sering digunakan pada tingkat studi yang lebih tinggi dan banyak penelitian yang digunakan untuk mencari kelebihan dan kekurangan dari metode e-learning ini. Sejak e-learning ini diterapkan ada kelemahan yang didapatkan seperti kurangnya sosialisasi tatap muka antar individu [1].

Ujian daring merupakan perkembangan dari era teknologi yang awalnya ujian itu harus bertatap muka namun kini bisa dilakukan dimana saja dengan menggunakan fasilitas internet, platform *e-learning* digunakan untuk mengadakan ujian daring ini dapat dilakukan ketika pengawas dan peserta mempunyai lokasi yang berbeda. Namun disisi lain dengan adanya ujian daring ini akan mendapati titik celah rentan keamanan sehingga bisa didapati beberapa celah untuk melakukan tindak kecurangan selama ujian [2].

Tantangan terbesar dalam sistem ujian daring adalah tindak kecurangan yang sangat rentan, para peneliti menyatakan bahwa 52,27% siswa berpendapat bahwa tidak ada perbedaan dalam kemudahan kecurangan antara ujian tradsional dengan ujian daring [3], begitu juga menyatakan bahwa lebih sulit mencegah kecuragan dalam lingkungan daring daripada lingkungan konvesional. Hasil penelitian menunjukan bahwa ketidakjujuran dalam penggunaan ujian daring lebih banyak di kalangan mahasiswa baru daripada mahasiswa pascasarjana [4].

Safe Exam Browser (SEB) merupakan browser ujian yang aman dan *open source*, *software* tersebut memungkinkan anda untuk membatasi akses ke situs web eksternal, fungsi sistem atau aplikasi lainnya saat mengikuti ujian secara daring. Program ini menjadikan ujian daring lebih aman [5].

Maka berdasarkan latar belakang tersebut, pada penelitian ini mencoba untuk melakukan *penetration testing* terhadap aplikasi Safe Exam Browser yang sedang ramai digunakan dalam proses ujian secara daring, dengan mencari beberapa celah yang dapat dilakukan oleh peserta ujian dalam melakukan tindak kecurangan selama proses pengerjaaan soal ujian.

II. KAJIAN TEORI

A. Spesifikasi Produk

Adapaun spesifikasi produk berdasarkan CD-1 pada tugas akhir ini dijelaskan sebagai berikut :

1. Dapat menajalankan aplikasi Safe Exam Browser pada virtual machine.
2. Dapat melakukan analisis traffic penggunaan jaringan oleh Wireshark ketika membuka Safe Exam Browser.

Spesifikasi tersebut dapat dijabarkan menjadi karakteristik produk dengan fitur utama, fitur dasar. Berikut adalah fitur yang akan dibuat :

Fitur utama :

1. Layar pada virtual machine dapat di split atau di minimize sehingga dapat menjalankan aplikasi lain ketika Safe Exam Browser dijalankan.
2. Aktivitas penggunaan Safe Exam Browser dapat dibaca pada perangkat lain

Fitur Dasar :

1. Safe Exam Browser dapat dijalankan pada virtual machine.
2. Wireshark dapat tetap berjalan ketika Safe Exam Browser dijalankan.

No	Hal	Rincian
1	Virtual machine	Safe Exam Browser dapat berjalan pada *virtual machine* tanpa aplikasi Safe Exam Browser membaca sedang dijalankan pada aplikasi *virtual*.
2	Wireshark	Aplikasi ini digunakan untuk menganalisis log aktivitas pada penggunaan jaringan di Safe Exam Browser

Spesifikasi 1

Pada aplikasi virtual machine yang dipakai merupakan VMware versi 17, versi ini merupakan versi keluaran terakhir yang rilis pada tahun 2022. Virtual machine ini merupakan sebuah aplikasi yang dapat menduplikat seperti perangkat keras sehingga dapat di instalasi dengan operasi sistem seperti windows ataupun linux.

Spesifikasi 2

Aplikasi Wireshark merupakan sebuah aplikasi yang dapat menangkap *packet traffic* dengan *open source* pada lintasan jaringan yang sedang dipakai, untuk dilakukan analisis terhadap jaringan tersebut.

B. Verifikasi

Hal	Sistem
Rincian	Safe Exam Browser akan diuji coba pada virtual machine untuk dapat dilihat apakah Safe Exam Browser dapat dijalankan atau tidak
Metode Pengukuran	Keberhasilan Safe Exam Browser untuk dijalankan pada virtual machine
Prosedur Pengujian	Virtual machine akan dibuka lalu akan di install Safe Exam Browser, mengunduh file Eprt setelahnya membuka file eprt dan mengerjakan tes eprt pada Safe Exam Browser melalui virtual machine

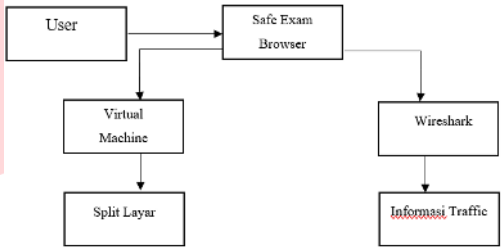
Hal	Sistem
Rincian	Wireshark akan dijalankan sebelum melakukan pengerjaan soal melalui Safe Exam Browser, sehingga Wireshark dapat menganalisis aktivitas ketika pengerjaan soal ujian sedang berlangsung
Metode Pengukuran	Wireshark dapat menganalisis hasil *traffic* ketika pengerjaan soal ujian.
Prosedur Pengujian	Aplikasi Wireshark akan melakukan analisis terhadap aktivitas selama penggunaaan aplikasi Safe Exam Browser sehingga didapatkan informasi yang relevan terhadap aktivitas Safe Exam Browser tersebut

III. METODE

A. Konsep Sistem

Dokumen ini menjelaskan tentang mengnalisis rentan keamanan pada konfigurasi Safe Exam Browser dan fungsi tersebut dilakukan untuk mengetahui apakah ada celah keamanan dari Safe Exam Browser dengan menggunakan virtual machine serta kami menggunakan Wireshark untuk menganalisis log aktivitas pada jaringan Safe Exam Browser.

B. Pilihan Sistem



Pada gambar diatas terdapat bahwasannya *user* akan mencoba untuk membuka Safe Exam Browser melalui aplikasi *virtual machine*, Wireshark. Pada sistem tersebut akan menghasilkan salah satu pengeluarannya masing masing seperti pada *virtual machine* ketika Safe Exam Browser dapat dijalankan maka Safe Exam Browser tersebut dapat dibagi layarnya sehingga memungkinkan untuk bekerja pada dua layar, maka fungsi layar kesatu adalah untuk membuka Safe Exam Browser sedangkan layar kedua membuka aplikasi lain. Selanjutnya pada Wireshark akan menangkap *packet traffic* pada aktivitas internat yang sedang melintas.

C. Analisis

Pada tahap analisis kali ini ada kriteria yang dapat dijelaskan yaitu sebagai berikut :

1. Kriteria Virtual Machine

Pada virtual machine akan dilakukan uji coba pembukaan aplikasi Safe Exam Browser, namun sebelum membuka kami memberikan *command* pada .vmx agar Safe Exam Browser membaca *virtual machine* tersebut sebagai model utama. Sehingga Safe Exam Browser dapat dijalankan dan layar pun dapat dibagi.

2. Kriteria Wireshark

Pada aplikasi Wireshark akan membaca *packet traffic* data yang terlintas pada jaringan yang digunakan, sehingga dapat dianalisis segala aktvitas *traffic* yang terlintas tersebut untuk diketahui informasi apa saja yang bisa didapatkan oleh aplikasi Wireshark pada aplikasi Safe Exam Browser.

D. Sistem Yang Akan Dikembangkan

Pada sistem yang akan dikembangkan terhadap pencarian celah aplikasi Safe Exam Browser pada virtual machine,

Wireshark, dan penggunaan aplikasi mirroring yang tidak dapat dilakukan ketika Safe Exam Browser terbuka, ini digunakan untuk melakukan pengamanan ketika ada sesuatu tindakan kecurangan dalam pembelajaran atau saat menjalankan ujian online.

E. Rencana Desain Sistem

Keterangan	Laptop	Smartphone
Gambar		
Tipe	Msi cyborg 15 a12ve	Iphone 13 pro max
Sistem Operasi	Windows 11	iOS 16.6

Perangkat Lunak

Perangkat lunak	Versi	Keterangan
Windows	11	Sistem Operasi untuk menjalankan aplikasi lainnya seperti virtual machine, AnyDesk, Wireshark.
AnyDesk	7.1.13	Digunakan untuk melakukan mirroring pada perangkat keras yang dituju sehingga didapatkan hak akses.
Wireshark		Digunakan untuk mendapatkan packet traffic pada jaringan yang digunakan.
Safe Exam Browser	3.0.1	Digunakan untuk melakukan pengujian pengerjaan soal tes pada browser yang tidak bisa membuka aplikasi tertenu.

F. Pengujian Komponen

Hal	Sistem
Rincian	Virtual machine
Metode Pengujian	Membuka aplikasi Safe Exam Browser pada virtual machine
Prosedur Pengujian	Virtual machine akan dibuka lalu akan di install Safe Exam Browser, mengunduh file Eprt setelahnya membuka file eprt dan mengerjakan tes eprt pada Safe Exam Browser melalui virtual machine

G. Pengujian Wireshark

Hal	Sistem
Rincian	Wireshark akan dijalankan sebelum melakukan pengerjaan soal melalui Safe Exam Browser, sehingga Wireshark dapat menganalisis aktivitas ketika pengerjaan soal ujian sedang berlangsung
Metode Pengukuran	Wireshark dapat menganalisis hasil *traffic* ketika pengerjaan soal ujian.
Prosedur Pengujian	Aplikasi Wireshark akan melakukan analisis terhadap aktivitas selama penggunaaan aplikasi Safe Exam Browser sehingga didapatkan informasi yang relevan terhadap aktivitas Safe Exam Browser tersebut

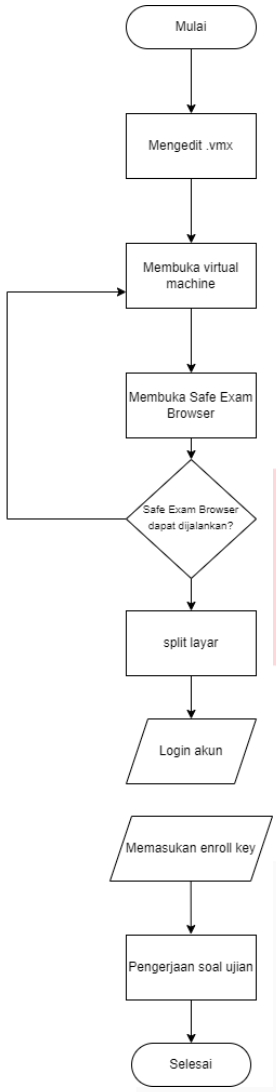
IV. HASIL DAN PEMBAHASAN

A. Implementasi sistem

Pada implementasi sistem ini ada beberapa tahap yang dilakukan seperti Instalasi kebutuhan aplikasi lalu konfigurasi terhadap beberapa aplikasi yang akan digunakan serta ada eksekusi terhadap aplikasi yang akan digunakan untuk berfokus pada pencarian celah terhadap aplikasi Safe Exam Browser.

B. Virtual Machine

Cara Kerja



Virtual machine akan digunakan sebagai sistem operasi tiruan pada perangkat keras untuk dilakukan pemasangan Safe Exam Browser agar diketahui Safe Exam Browser dapat berjalan pada virtual machine, sehingga ketika menjalankan pengujian pada Safe Exam Browser dapat terbagi layar sehingga bisa untuk membuka aplikasi lain yang dapat membantu pengejerjaan soal ujian. Namun agar Safe Exam Browser tidak dapat membaca sedang dibuka pada virtual machine maka perlu untuk merubah konfigurasi pada file .vmx yang terdapat pada folder instalasi virtual machine

C. Implementasi

Pengujian Komponen (Kalibrasi)

A. Pengujian AnyDesk

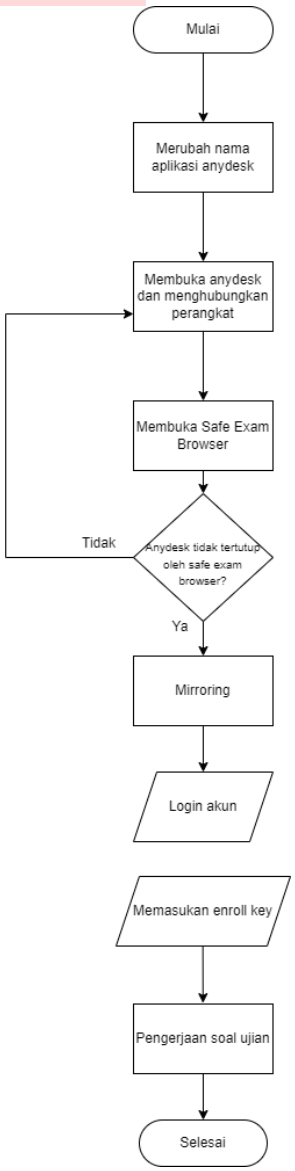
TABEL 3.1
Pengujian AnyDesk

Hal	Sistem
Rincian	AnyDesk
Metode Pengukuran	Berjalannya aplikasi Safe Exam Browser dan AnyDesk tanpa aplikasi AnyDesk tertutupi
Prosedur Pengujian	Aplikasi AnyDesk akan di *rename* menjadi nama lain, lalu menjalankan aplikasi AnyDesk tersebut dengan nama yang sudah di ganti serta menghubungkannya dengan device lain setelah terhubung lalu membuka file config Safe Exam Browser.

A. Implementasi Sistem

Pada implementasi sistem ini ada beberapa tahap yang dilakukan seperti Instalasi kebutuhan aplikasi lalu konfigurasi terhadap beberapa aplikasi yang akan digunakan serta ada eksekusi terhadap aplikasi yang akan digunakan untuk berfokus pada pencarian celah terhadap aplikasi Safe Exam Browser.

B. Rename Aplikasi
Cara Kerja

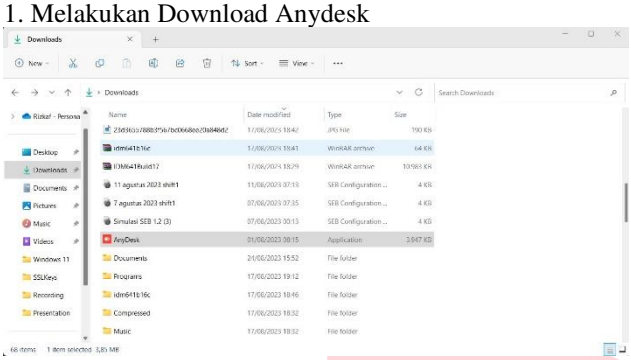


Aplikasi AnyDesk akan dirubah namanya sehingga tidak dapat dibaca sebagai aplikasi terlarang yang dapat di proses oleh Safe Exam Browser, ketika sudah merubah namanya maka proses selanjutnya adalah membuka Safe Exam Browser tersebut dan melihat kondisi apakah AnyDesk akan dipaksa tutup oleh Safe Exam Browser atau tidak. Proses selanjutnya ketika AnyDesk tidak terbaca sedang dijalankan

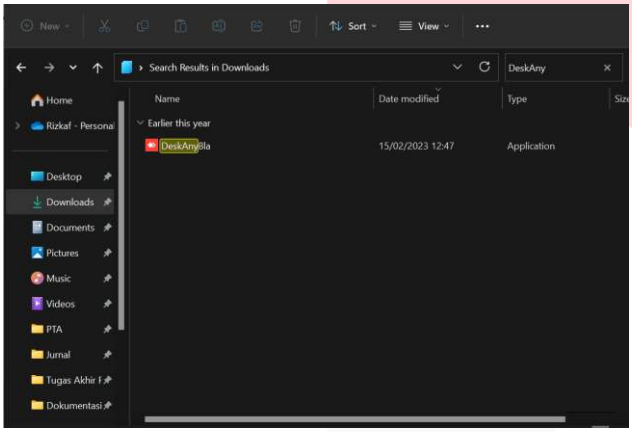
maka proses *mirroring* terhadap perangkat tersebut dapat berjalan sampai pengerjaan soal ujian diselesaikan.

A. Impelementasi

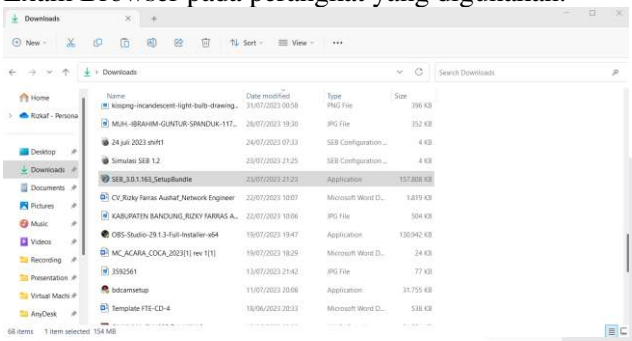
1. Melakukan Download Anydesk



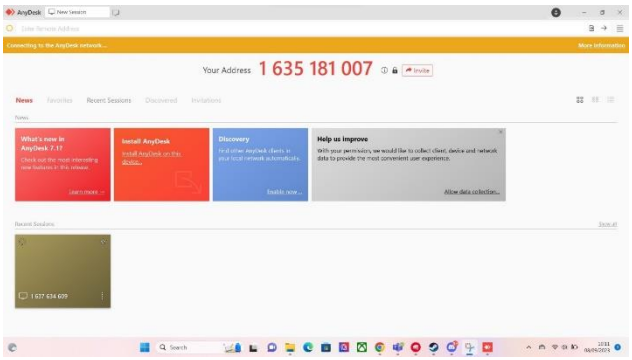
2. Merubah nama aplikasi AnyDesk.exe menjadi DeskAnyBla.exe agar tidak dapat terbaca oleh aplikasi Safe Exam Browser.



Melakukan pengunduhan dan instalasi aplikasi Safe Exam Browser pada perangkat yang digunakan.



Menjalankan aplikasi AnyDesk yang sudah dirubah namanya dan hubungkan dengan perangkat lain melalui *address* yang tertera pada aplikasi tersebut.



a. Skema Pengujian Sistem

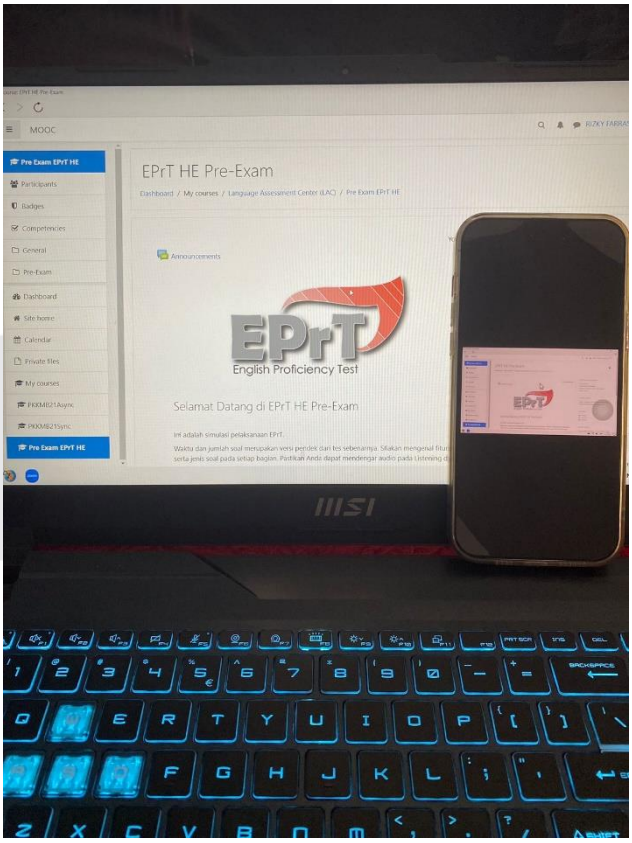
Pada skenario pengujian tugas akhir kali ini kami mencoba melalui beberapa sistem seperti melalui virtual machine, aplikasi *mirroring*, dan aplikasi Wireshark

b. Proses Pengujian

Pengujian sistem dilakukan secara keseluruhan sesuai dengan spesifikasi yang dicantumkan di CD2

c. Proses Pengujian 2

Pada pengujian kedua dilakukan perubahan nama terhadap aplikasi AnyDesk menjadi nama lain agar tidak terdeteksi oleh aplikasi Safe Exam Browser sebagai aplikasi yang diblokir atau di indikasi berpotensi kecurangan, pada aplikasi AnyDesk ini memungkinkan proses *mirroring* terhdap *device* yang saling terhubung



Pada pengujian ini kedua device sudah saling terhubung nomor alamt yang dinputkan sehingga terjadi proses mirroring dan device yang menginputkan alamat tersebut

dapat mengkontrol hak akses terhadap device yang dihubungkan

A. Langkah Pengujian

1. Mencari aplikasi AnyDesk.exe
2. Merubah nama aplikasi AnyDesk.exe menjadi DeskAnyBla.exe
3. Menjalankan aplikasi tersebut dan membuka juga pada device lain
4. Menghubungkan antar device melalui alamat remote yang tersedia pada aplikasi AnyDesk.
5. Setelah kedua device saling terhubung, pada salah satu device membuka file konfigurasi Eprt.
6. Maka device yang sedang membuka Safe Exam Browser dapat di mirroring dan dapat dikontrol melalui device yang terkoneksi pada device yang sedang menjalankan Safe Exam Browser.

a. Hasil Pengujian

Didapati hasilnya bahwa Safe Exam Browser dapat dijalankan tanpa harus menutup aplikasi AnyDesk sehingga perangkat keras yang terhubung melalui AnyDesk dapat di kontrol secara jarak jauh melalui perangkat lain, ini dapat menjadi tindakan kecurangan sebab peserta ujian bisa menyerahkan kendali pada orang lain untuk mengerjakan soal ujian tersebut.

b. Analisis dan Kesimpulan Hasil Pengujian 2

Pada pengujian kedua ketika aplikasi AnyDesk dirubah namanya menjadi DeskAnyBla pada aplikasi Safe Exam Browser tidak akan membaca DeskAnyBla hal tersebut disebabkan karena konfigurasi pada Safe Exam Browser hanya dapat membaca aplikasi yang bernama AnyDesk.

Sehingga ketika aplikasi AnyDesk tersebut dirubah namanya Safe Exam Browser menganggap aplikasi tersebut bukan sebagai aplikasi mirroring atau aplikasi yang diindkasi menjadi tindak kecurangan. Meskipun aplikasi AnyDesk sudah dijalankan dan pada tampilan aplikasi pun tetap bernama AnyDesk bukan nama yang sudah dirubah.

Pengujian keamanan melalui aplikasi AnyDesk terhadap aplikasi Safe Exam Browser ini merupakan celah keamanan pada aplikasi Safe Exam Browser tersebut dikarena peserta ujian EPRT dapat memanfaatkan hal tersebut untuk melakukan pengerjaan soal jarak jauh yang dikerjakan oleh orang lain melalui perangkatnya sendiri, hal tersebut didukung ketika pengerjaan soal ujian *listening audio* dapat keluar pada perangkat yang sedang mengontrol perangkat yang sedang membuka Safe Exam Browser.

REFERENSI

[1] M. Tayebinik and M. Puteh, “Blended Learning or E-learning?”

[2] T. Langenfeld, “Internet-Based Proctored Assessment: Security and Fairness Issues,” vol. 39, pp. 24–27, 2020, [Online]. Available: https://doi.org/10.1111/emip.12359

[3] S. D. C. and J. F. C. Y. Chuang, “Detecting probable cheating during online assessments based on time delay and head pose,” *High. Educ. Res. Dev.*, vol. 36, 2017, [Online]. Available: https://doi.org/10.1080/07294360.2017.1303456

[4] J. Golden and M. Kohlbeck, “Addressing cheating when using test bank questions in online Classes,” *J. Account. Educ.*, vol. 52, 2020, [Online]. Available: https://doi.org/10.1016/j.jaccedu.2020.100671

[5] C. Anglano, M. Canonico, and M. Guazzone, “Forensic analysis of Telegram Messenger on Android smartphones,” *Digit. Investig.*, vol. 23, no. December, pp. 31–49, 2017, doi: 10.1016/j.diin.2017.09.002.

[6] J. T. Informatika, U. Asahan, J. Jend, A. Yani, and S. Utara, “SISTEM APLIKASI UJIAN DARING BERBASIS LEARNING MANAGEMENT SYSTEM (LMS) MENGGUNAKAN MOODLE Adi Widarma , 2 Yustria Handika Siregar I . PENDAHULUAN Pendidikan merupakan sebuah proses akademik yang tujuannya untuk meningkatkan nilai sosial , budaya , moral,” pp. 813–821, 2020.

[7] Thea Marie Søgaard, “Cheating Threats in Digital BYOD Exams: A Preliminary Investigation,” vol. 2015.

[8] H. M. Mohammed and Q. I. Ali, “Cheating Prevention in E-proctoring Systems Using Secure Exam Browsers: A Case Study,” *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 8, no. 4, p. 634, 2022, doi: 10.26555/jiteki.v8i4.25094.

[9] Thea Marie Søgaard, “Mitigation of Cheating Threats in Digital BYOD exams,” no. June, 2016, [Online]. Available: https://brage.bibsys.no/xmlui/handle/11250/2410735

[10] A. Heintz, “Cheating at Digital Exams Vulnerabilities and Countermeasures,” no. June, 2017, [Online]. Available: https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2460113/12292_FULLTEXT.pdf?sequence=1