

BAB 1

USULAN GAGASAN

1.1 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 didapatkan 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 tradisional dengan ujian daring [3], begitu juga menyatakan bahwa lebih sulit mencegah kecurangan dalam lingkungan daring daripada lingkungan konvensional. Hasil penelitian menunjukkan 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 pengerjaan soal ujian.

1.2 Informasi Pendukung Masalah

E-Learning atau pembelajaran elektronik merupakan pembelajaran yang memanfaatkan teknologi informasi dan komunikasi untuk kepentingan dalam pembelajaran yang dapat diakses kapan saja dan dimana saja [6]. Studi mengatakan bahwa pembelajaran jarak jauh pada tahun yang sama ditemukan bahwa Sebagian besar siswa berperilaku curang dan mereka cenderung lebih curang secara pembelajaran atau ujian daring [7].

Pada penelitian pertama, yaitu penelitian dengan judul “Cheating Prevention in E-proctoring Systems Using Secure Exam Browsers; A Case Study” pada tahun 2022. Membahas tentang skema pengujian pada aplikasi Safe Exam Browser dengan menggunakan berbagai cara yang dapat di indikasi sebagai tindak kecurangan dalam pengerjaan soal ujian melalui aplikasi Safe Exam Browser, dan membandingkan pengerjaan soal ujian dengan aplikasi Safe Exam Browser, *respondus lockdown browser*, dengan browser selain SEB. Didapatkan bahwasannya Safe Exam Browser dapat membatasi atau mencegah cara – cara yang dapat di indikasi sebagai tindak kecurangan seperti *screen recording, print screen, virtual machine, minimizing exam window* [8].

Pada penelitian kedua, yaitu penelitian dengan judul “Mitigation of Cheating Threats in Digital BYOD exams” pada tahun 2016, pada penelitian ini peneliti tersebut mencoba untuk mencari celah terhadap aplikasi Safe Exam Browser yang bisa digunakan untuk tindak kecurangan dalam mengerjakan soal ujian pada aplikasi Safe Exam Browser, penelitian tersebut mencoba dengan merubah config pada aplikasi Safe Exam Browser, menjalankan melalui *virtual machine*, dan menyebarkan video dan audio melalui aplikasi skypea [9].

Pada penelitian ketiga, yaitu penelitian dengan judul “Cheating at Digital Exams Vulnerabilities and Countermeasures” pada tahun 2017, penelitian tersebut menjelaskan tentang celah terhadap aplikasi Safe Exam Browser yang dapat ditandai sebagai tindak kecurangan salah satunya dengan metode *man in the middle attack* dengan cara mendapatkan

akses pada perangkat keras yang berada pada seseorang yang mengakses dengan server yang dicoba aksesnya [10].

1.3 Analisis Umum

1.3.1 Aspek Keberlanjutan

Pada penelitian ini diharapkan dengan ditemukannya titik celah terhadap aplikasi Safe Exam Browser dapat menjadi bahan evaluasi kedepannya dalam penggunaan safe exam browse untuk pengerjaan soal ujian secara daring, sehingga dapat meminimalisir peserta ujian dalam melakukan tindak kecurangan.

1.3.2 Aspek Keamanan

Penelitian ini merupakan evaluasi dari penelitian sebelumnya dalam mencari celah untuk melakukan tindak kecurangan pada aplikasi Safe Exam Browser, karena pada beberapa jurnal penggunaan *virtual machine* tidak dapat dilakukan sebab aplikasi Safe Exam Browser membaca sebagai virtual machine, dan belum dilakukannya perubahan nama pada aplikasi *mirroring*.

1.4 Kebutuhan yang Harus Dipenuhi

Berdasarkan hasil analisis yang telah dilakukan, kebutuhan yang harus dipenuhi adalah menginstalasi beberapa software dan mengkonfigurasi dari beberapa aplikasi tersebut untuk mendapatkan hasil yang diinginkan, sebagai berikut :

1. Menginstalasi software seperti virtual machine, Wireshark, AnyDesk.
2. Merubah nama pada aplikasi AnyDesk.
3. Melakukan analisis terhadap hasil tangkap aktivitas pada Wireshark

Tujuan penelitian mengacu pada permasalahan yang telah dikemukakan, diharapkan pada penelitian ini dapat mencapai tujuan sebagai berikut :

1. Dapat melakukan pengujian keamanan agar diketahui celah keamanan pada aplikasi Safe Exam Browser.
2. Dapat menjalankan tes ujian pada aplikasi Safe Exam Browser melalui aplikasi virtual machine.
3. Melakukan tindak *mirroring* dengan mendapatkan akses terhadap perangkat keras peserta ujian yang terhubung dengan server tes ujian Safe Exam Browser.

4. Dapat melakukan perekaman aktivitas melalui aplikasi Wireshark.

1.5 Solusi Sistem yang Diusulkan

1.5.1 Karakteristik Produk

Solusi yang ditawarkan pada penelitian ini berlandaskan dasar pada referensi yang telah dicantumkan pada kebutuhan beserta tujuan. Pada penelitian ini disebutkan ada beberapa skema yang dapat dilakukan dalam percobaan pengujian keamanan pada aplikasi Safe Exam Browser dalam pengerjaan soal ujian EPRT, skema tersebut dijelaskan sebagai berikut :

A. Safe Exam Browser dibuka melalui *virtual machine*

Pada percobaan ini aplikasi Safe Exam Browser akan dibuka melalui virtual machine yang telah dijalankan, sehingga fitur yang ada pada produk ini adalah :

1. Safe Exam Browser dapat dijalankan pada virtual machine.
2. Layar pada virtual machine dapat di *minimize* atau di *split* sehingga dimungkinkan untuk menjalankan aplikasi selain virtual machine seperti browser, aplikasi yang dapat melakukan *mirroring*, dan aplikasi yang dapat melakukan pembagian layar.

B. Safe Exam Browser dapat menjalankan aplikasi AnyDesk

Pada percobaan ini aplikasi Safe Exam Browser tidak dapat melakukan *terminate* pada aplikasi AnyDesk sebab aplikasi tersebut telah dirubah namanya, sehingga konfigurasi pada Safe Exam Browser tidak dapat membaca aplikasi AnyDesk yang telah dijalankan. Sehingga fitur yang ada pada produk ini adalah :

1. Safe Exam Browser tidak dapat melakukan penutupan aplikasi AnyDesk.
2. AnyDesk dapat berjalan beriringan dengan Safe Exam Browser sehingga perangkat yang sedang mengerjakan ujian dapat dihubungkan dengan perangkat lain ketika ujian sedang berlangsung.
3. Perangkat yang terhubung dengan perangkat yang sedang menjalankan Safe Exam Browser dapat melakukan *control* terhadap perangkat terhubung yang sedang menjalankan aplikasi Safe Exam Browser.
4. Merubah konfigurasi Safe Exam Browser.

C. Safe Exam Browser dapat menjalankan aplikasi Wireshark

Pada percobaan ini aplikasi Safe Exam Browser akan dilakukan perubahan konfigurasi yang diharapkan dapat membuka aplikasi yang dilarang oleh Safe Exam Browser, sehingga fitur yang ada pada produk ini adalah :

1. SEB configuration tool akan dibuka.
2. Masuk pada menu prohibited processes.
3. Menghilangkan tanda centang pada aplikasi yang dilarang oleh Safe Exam Browser.
4. Menyimpan konfigurasi.
5. Membuka aplikasi yang telah dihilangkan tanda centang pada konfigurasi sebelumnya.
6. Membuka aplikasi Safe Exam Browser.
7. Menjalankan aplikasi Wireshark

Pada percobaan ini aplikasi Safe Exam Browser akan dijalankan beriringan dengan membuka aplikasi Wireshark, sehingga fitur yang ada pada produk ini adalah :

1. Wireshark dibuka dan aplikasi Safe Exam Browser akan dijalankan.
2. Wireshark akan menangkap aktivitas perangkat berdasarkan terhubung dengan jaringan yang sama.
3. Jalur aktivitas pengguna jaringan dapat ditangkap oleh Wireshark sehingga diharapkan dapat membaca isi pada aplikasi Safe Exam Browser.

1.6 Skenario Penggunaan

Penggunaan aplikasi Safe Exam Browser dapat dilakukan dengan beberapa skenario yang dapat dilakukan, berikut beberapa skenario yang akan dilakukan sebagai berikut :

1.6.1 Skema A

Menggunakan *virtual machine* untuk dapat dilihat apakah Safe Exam Browser dapat dijalankan pada virtual machine :

- Safe Exam Browser akan dibuka melalui *virtual machine*.
- Layar pada virtual machine akan di *minimize* atau di *split* sehingga.
- Membuka aplikasi selain virtual machine seperti google chrome, AnyDesk, aplikasi yang dapat melakukan pembagian layar.

1.6.2 Skema B

Merubah nama pada aplikasi AnyDesk sehingga Safe Exam Browser tidak membaca aplikasi AnyDesk sebagai aplikasi yang dilarang, maka langkah yang akan dilakukan sebagai berikut :

- Merubah nama aplikasi AnyDesk melalui *file explorer* menjadi DeskAnyBla.
- Menjalankan aplikasi AnyDesk yang telah dirubah namanya.
- Menghubungkan dengan perangkat lain.
- Membuka aplikasi Safe Exam Browser.
- Melakukan kontrol terhadap perangkat terhubung yang sedang menjalankan Safe Exam Browser.

1.6.3 Skema C

Pada skenario ini akan dilakukan perubahan konfigurasi melalui SEB Configuration Tool dengan menghilangkan tanda centang pada aplikasi yang dituju pada tab *prohibited processes*. Maka langkah yang dilakukan sebagai berikut :

- Membuka SEB Configuration Tool.
- Masuk pada menu *prohibited processes*.
- Menghilangkan tanda centang pada aplikasi yang dituju.
- Melakukan penyimpanan konfigurasi dengan meng-klik *configuration client*.
- Membuka aplikasi yang dituju dan membuka Safe Exam Browser.

1.6.4 Skema D

Membuka aplikasi Wireshark untuk membaca *traffic* pada jaringan yang sama sehingga dapat di analisis apa saja yang dilakukan pada perangkat lain dengan terhubung kepada jaringan yang sama, maka pada skema ini dilakukan sebagai berikut :

- Membuka aplikasi Wireshark dan memilih pada jaringan terhubung yang sama pada perangkat yang akan di analisis.
- Membuka aplikasi Safe Exam Browser dan melakukan pengerjaan soal ujian.
- Menutup aplikasi Safe Exam Browser dan membaca hasil analisis yang didapatkan oleh aplikasi Wireshark.

1.7 Solusi yang Dipilih

Berdasarkan latar belakang dan solusi yang telah dipaparkan untuk melakukan pengujian keamanan pada aplikasi Safe Exam Browser untuk diketahui celah keamanannya dalam pengerjaan soal ujian EPRT, maka telah dipilih solusi yang akan dilakukan yaitu solusi pertama, kedua, dan keempat, pada solusi yang dipilih tersebut maka fitur yang ada produk tersebut adalah :

- Safe Exam Browser dapat dijalankan melalui aplikasi *virtual machine*.
- AnyDesk dapat dijalankan tanpa harus di *terminate* oleh Safe Exam Browser karena dibaca sebagai aplikasi yang tidak diizinkan ketika membuka Safe Exam Browser.
- Wireshark dapat membaca aktivitas yang dilakukan oleh perangkat lain dengan terhubung kepada jaringan yang sama.

1.8 Kesimpulan dan Ringkasan CD-1

Ringkasan dari dokumen CD-1 adalah solusi yang dipilih berdasarkan latar belakang yang ditambahkan dengan informasi pendukungnya. Solusi yang dipilih adalah pengujian keamanan pada penggunaan aplikasi Safe Exam Browser melalui *virtual machine*, menjalankan aplikasi AnyDesk ketika akan menjalankan aplikasi Safe Exam Browser, dan melakukan analisis aktivitas perangkat melalui aplikasi Wireshark. Sehingga aplikasi Safe Exam Browser dapat diketahui celah keamanannya selama pengerjaan soal ujian EPRT maka dapat dilakukan untuk menjadi bahan pertimbangan dan evaluasi terhadap pembelajaran ataupun ujian yang dilakukan secara daring agar mengantisipasi tindak kecurangan yang dilakukan oleh peserta ujian daring.