MINI PROPOSAL TUGAS AKHIR

Program Studi
Fakultas Keguruan dan Ilmu Pendidikan - Universitas Sebelas Maret Surakarta

---

Identitas Mahasiswa

Nama Mahasiswa	:	Aji Nur Rohman
NIM	:	K3515006
Nomor Handphone / WA	:	089698606075
IPK Terakhir	:	3.66
Jumlah SKS Kumulatif	:	121

Deskripsi Rencana Tugas Akhir

Judul Rencana Tugas Akhir

EVALUASI TERHADAP MEDIA PEMBELAJARAN CYBERSECURITY DARING BERBASIS CAPTURE THE FLAG DITINJAU DARI ASPEK ETHICAL HACKING DAN ASPEK GAMIFIKASI

Jenis Penelitian [v] Kualitatif [ ] Kuantitatif [ ] PTK [ ] Research and Development

[ ] Lain-Lain (Sebutkan: .....)

Latar Belakang

Dengan meningkatnya tingkat perkembangan internet, keamanan komputer menjadi konsentrasi utama untuk sebuah bisnis dan pemerintahan. Mereka berharap bisa mengambil keuntungan dari berbagai keuntungan yang disediakan internet tapi mereka juga menghawatirkan kemungkinan ter-"*hacked*" (C.C Palmer). Oleh karena itu dibutuhkan suatu sistem keamanan cyber.

Keamanan cyber atau keamanan dunia maya atau yang biasa disebut dengan *cybersecurity* merupakan kegiatan atau perlakuan yang diberikan untuk memproteksi suatu sistem, jaringan, dan program dari serangan digital. Serangan dunia maya atau *cyberattack* ini biasanya ditujukan untuk mengakses, mengubah atau menghancurkan informasi dan data sensitif, memeras uang dari pengguna atau mengganggu proses bisnis.

Untuk melindungi data dan informasi yang sensitif tersebut diperlukan sistem keamanan yang baik sehingga diharapkan dapat melindungi data dan informasi tersebut. Hal yang perlu dilakukan untuk melindungi data dan informasi yang ada adalah dengan pemasangan sistem keamanan jaringan komputer. Hal ini dikarenakan keamanan jaringan merupakan sistem pertahanan yang digunakan untuk melindungi ancaman dari serangan dari luar jaringan.

Setelah dilakukan pemasangan sistem keamanan tersebut tidak langsung keamanan terjamin serangan dari luar. Untuk lebih menguatkan sistem pertahanan tersebut maka diperlukan pengujian untuk mengetahui seberapa kuat sistem pertahanan tersebut dan apabila dalam pengujian terdapat celah yang masih bisa dimasuki maka bisa diperbaiki untuk mengingkatkan keamanan sistem dari ancaman luar jaringan.

Bentuk pengujian terhadap sistem keamanan jaringan ini bisa menggunakan cara meng-*hack* sistem sendiri atau *ethical hacking*. *Ethical hacking* atau juga diketahui sebagai penetrasi tes atau *white hat hacking*, menggunakan alat-alat, trik, dan teknik yang biasa digunakan peretas, yang membedakan adalah *ethical hacking* ini dilakukan secara legal dengan persetujuan dari target. Tujuan utama dari *ethical hacking* adalah untuk mencari celah sistem dari sudut pandang peretas sehingga keamanan bisa lebih baik. (Sonali Patil, 2017)

Tahap-tahap yang dilakukan ethical hacking terbagi menjadi 5 blok atau bagian (Sonali Patil, 2017), terdiri dari:

Reconnaissance, dimana peretas secara sembunyi-sembunyi mencari informasi sistem yang menjadi target

Scanning and Enumeration, scanning sendiri merupakan teknik umum yang digunakan penguji untuk menemukan pintu terbuka dari sebuah sistem. Sedangkan enumeration adalah proses serangan awal menuju target untuk mendapatkan informasi dari mesin target dan secara aktif tetap terkoneksi.

Gaining Access, dari sini peretas mulai mencoba mendapatkan akses ke dalam sistem dengan bantuan tools. Disini peretas mulai mencari dan berusaha mendapatkan password dari mesin sistem.

Maintaining Access, setelah bisa masuk kedalam mesin sistem, peretas

sudah melakukan peretasan bukan hanya pada sistem tapi juga pada sumber daya pada mesin.

Clearing Tracks, setelah peretas mendapatkan apa yang diinginkan atau sudah selesai peretasan maka tahap selanjutnya adalah menghapus keberadaan dirinya dari sistem yang telah diretas.

Dari pemaparan masalah diatas, untuk mempelajari cara kerja *ethical hacking* secara menyeluruh masih kurang baik. Meskipun sudah ada materi-materi yang yang bisa dipelajari mengenai ethical hacking melalui buku dan video tutorial, dirasa masih belum cukup untuk mengingkatkan kemampuan ethical hacking.

Buku-buku teks yang digunakan untuk pembelajaran cybersecurity ini sudah sangat banyak dan bermacam-macam seperti **CEH, CompTIA, Security+, Cisco Cyberops Course Materials, Linux Security**, dan lain-lain. Buku-buku ini tentunya sangat menunjang dalam memahami cybersecurity. Akan tetapi, buku teks saja masih dirasa kurang untuk menignkatkan kemampuan ethical hacking dan cybersecurity, karena siswa atau mahasiswa hanya bisa membayangkan atau mengimajinasikan teks dalam buku dan tidak bisa mempraktekkan secara langsung.

Selain itu materi mengenai cybersecurity juga bisa didapatkan atau bisa diperoleh dalam video-video tutorial yang bisa di temukan di internet baik secara gratis maupun secara berbayar. Video-video tutorial ini juga bisa ditonton atau diperoleh melalui website-website tertentu, misalnya di website **UDEMY, Netacad-InPurchase, Cybrary IT**, dan lain-lain. Keunggulan dari video tutorial daripada buku teks diatas adalah dalam bentuk audio dan visual, dimana siswa atau mahasiswa bisa lebih mudah mengerti materi cybersecurity dan ethical hacking. Kekurangan dari bentuk media pembelajaran bentuk video tutorial ini adalah masis sama seperti buku teks yaitu siswa atau mahasiswa belum bisa mempraktekkan secara langsung.

Selain kedua media pembelajaran diatas masih bentuk media lain yang bisa digunakan yaitu independen lab untuk praktek, ini merupakan simulasi kecil dari sebuah sistem nyata. Menggunakan independen lab ini sangat mengasah kemampuan siswa atau mahasiswa dalam mengerti materi dan mempraktekkan materi cybersecurity dan ethical hacking secara langsung sesuai dengan keadaan di lingkungan nyata. Akan tetapi kekurangan penggunaan independen lab ini adalah dibutuhkan biaya yang cukup besar untuk membuatnya.

Selain ketiga media pembelajaran diatas masih ada satu solusi alternatif yang bisa digunakan untuk mempelajari dan mempraktekkan cybersecurity dan ethical hacking secara lebih bebas dan menyenangkan yaitu menggunakan laboratorium virtual secara online untuk pelajaran cyber security. Dengan adanya virtual lab ini lebih memudahkan dalam mempraktekkan cyber security dan ethical hacking karena lebih sesuai dengan lingkungan nyata dan tidak membutuhkan biaya yang besar serta bisa diakses kapan saja dan dimana saja asalkan ada koneksi internet.

Dengan media atau alat bantu mengajar berupa virtual lab yang sesuai dengan lingkungan riil akan mampu menambah perhatian dan motivasi siswa

dalam kegiatan pembelajaran. Media belajar berupa virtual lab ini memberikan kelebihan lain dibanding media belajar konvensional lain yaitu dapat membantu memahami suatu pembelajaran secara lebih baik karena menggunakan sistem simulasi yang didasarkan pada lingkungan riil. Berdasarkan permasalahan yang sudah dijabarkan, akan diadakan penelitian yang berjudul "**INVESTIGASI TERHADAP APLIKASI-APLIKASI DARING MEDIA PEMBELAJARAN KEAMANAN KOMPUTER DAN JARINGAN**"

Rumusan Masalah

Bagaimana hasil evaluasi media pembelajaran cybersecurity online terhadap kesesuaian dengan proses audit keamanan komputer?

Tujuan Penelitian

1. Melakukan ulasan secara komprehensif terhadap media pembelajaran cybersecurity