Pengujian dan Penilaian Kerentanan E-Learning Universitas Langlangbuana Menggunakan Metode STRIDE dan DREAD

Mokhamad Hendayun[1], Hadi Prasetyo Utomo[2], Dandi Pardamean Nababan[3]

Program Studi Informatika, Fakultas Teknik, Universitas Langlangbuana[1,2,3]

[1]hendayun@unla.ac.id

[2]hadi@informatika.unla.ac.id

[3]dandinababan@gmail.com

Abstrak—***Sistem e-learning Universitas Langlangbuana Bandung merupakan platform pembelajaran berbasis web, yang proses kegiatan belajar mengajarnya dilakukan secara online dan memberi kemudahan layanan kepada dosen dan mahasiswa yang dapat diakses dimana saja dan kapan saja. Namun karena kemudahannya, layanan tersebut masih terdapat banyak beberapa masalah pada celah keamanan. Oleh karena itu peneliti melakukan identifikasi mengenai celah keamanan web elearning.unla.ac.id serta melakukan pengujian dan penilaian menggunakan metode STRIDE dan DREAD untuk meminimalisir risiko keamanan yang mungkin kembali terjadi. Berdasarkan hasil penelitian yang sudah dilakukan, didapatkan hasil security report yang berisikan tentang deskripsi ancaman, tingkat ancaman, target ancaman, jenis serangan yang terjadi, serta pencegahannya..***

Kata kunci **- penilaian risiko, e-learning, STRIDE, DREAD**

I. PENDAHULUAN

Saat ini sudah banyak perguruan tinggi melakukan inovasi pembelajaran menggunakan teknologi informasi dan komunikasi [1]. Kemudahan akses internet dan murahnya perangkat membuat pengguna sistem *e-learning* terus bertambah. Dengan pembelajaran yang dilakukan secara *online* maka materi pembelajaran tidak lagi terbatas oleh jarak, ruang dan waktu. Begitupun pada sistem informasi *e-learning* Universitas Langlangbuana Bandung yang merupakan *platform* pembelajaran berbasis *web* yang membantu proses kegiatan belajar mengajar secara *online* [2]. *Platform* ini menyajikan seluruh materi, kuis, atau bahan pembelajaran lainnya yang memberikan kemudahan layanan kepada dosen dan mahasiswa yang dapat diakses dimana saja dan kapan saja. Namun karena kemudahannya, layanan tersebut masih mungkin terdapat beberapa masalah pada celah keamanan.

Keamanan dalam informasi ada berbagai prinsip yang harus dipenuhi agar sistem tersebut handal. Prinsip yang dimaksud untuk mencapai kerahasiaan, integritas, dan ketersediaan di dalam sumber informasi yang ada [3]. Keamanan juga harus dapat menjamin informasi dapat terlindung dari berbagai ancaman yang mungkin timbul atau juga setidaknya mampu mengurangi kerugian yang diderita apabila terjadi ancaman pada sistem informasi [4].

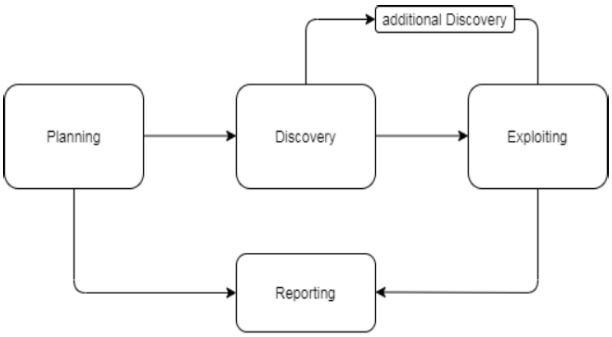
Berdasarkan informasi yang didapat dari penelitian terdahulu, ada yang berhasil meretas domain utama *web* tersebut sehingga mengakibatkan *down* selama beberapa waktu dan tidak bisa diakses [5].

II. METODE

Metode penelitian yang digunakan adalah metode kuantitatif. Penelitian kuantitatif adalah upaya seorang peneliti menemukan pengetahuan menyuguhkan data dalam bentuk angka. Angka-angka yang diperoleh inilah yang digunakan untuk melakukan analisis [6]. Proses yang akan dilakukan untuk mendapatkan angka dan analisis adalah sebagai berikut:

- *Penetration testing* berdasarkan STRIDE.
- Menilai jenis ancaman berdasarkan DREAD.
- Mengakumulasikan nilai jenis ancaman secara keseluruhan guna untuk mengetahui apakah keamanan tersebut berada di *level* yang rendah, menengah, atau *level* tinggi.

Tahapan dalam melakukan *penestration testing* tersaji dalam Gambar 1.



Gambar 1. Tahapan Pentest [7]

Microsoft telah mengembangkan metode klasifikasi ancaman yaitu STRIDE, yang dapat diterapkan pada jaringan, host, dan aplikasi. Dengan menerapkan model STRIDE memungkinkan untuk mengetahui karakterisasi ancaman sesuai dengan tujuan [8]. Singkatan STRIDE sendiri dibentuk dari huruf pertama dari masing-masing kategorinya, yaitu

Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, dan Elevation of privilege.

Metode DREAD merupakan suatu model dari Microsoft yang digunakan untuk menghitung risiko yang dapat menghasilkan informasi peringkat risiko untuk sebuah ancaman yang terjadi [8].

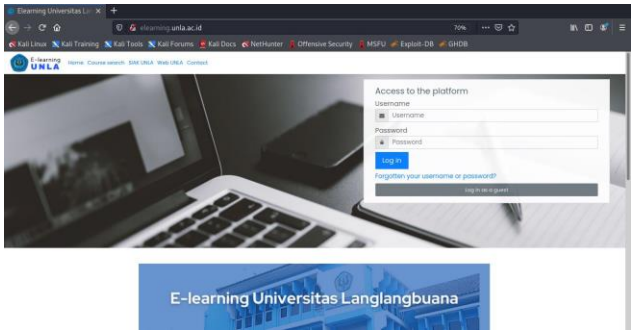
Penilaian peringkat dengan model DREAD tidak harus menggunakan skala besar karena dapat mempersulit menilai tingkatan konsisten ancaman antar satu dengan yang lain. Skala dapat menggunakan skema sederhana seperti tinggi (3), sedang (2), dan rendah (1).

III. HASIL DAN PEMBAHASAN

Dalam pembahasan akan dilakukan identifikasi celah keamanan yang terdapat pada *e-learning*. Setelah melakukan identifikasi tahap selanjutnya melakukan penilaian pada celah keamanan yang didapat dari hasil identifikasi ancaman tersebut.

A. Planning

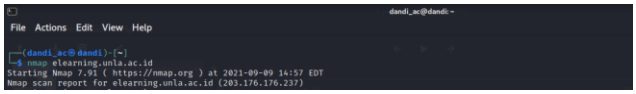
Dalam rencana menggunakan *web* elearning.unla.ac.id sebagai objek penelitian dan sudah berdasarkan izin dari pihak yang berwajib sebagai target pengujian kerentanan atau celah keamanannya. Tampilan halaman utama *web* elearning.unla.ac.id terdapat pada Gambar 2.



Gambar 2. Halaman Utama e-learning.unla.ac.id

B. Discovery

Dalam tahap ini melakukan pengumpulan berbagai informasi yang bertujuan untuk merencanakan jenis serangan apa saja yang akan dilakukan. Alat yang digunakan adalah berupa *tools* bernama Nmap. Nmap untuk menampilkan IP dan beberapa *port* yang terbuka pada *web server*. Alasan menggunakan *tools* Nmap dikarenakan mampu digunakan sebagai *network inventory tools* dan *mapping* atau pemetaan IP, *port* dan *services* juga mampu mendeteksi *vulnerability* di *network port scanning* dan relatif mudah digunakan [9]. Perintah yang digunakan untuk proses pengumpulan informasi dapat dilihat pada Gambar 3.



Gambar 3. Perintah Nmap

Setelah perintah dijalankan, maka akan terlihat hasil yang didapat yang berupa informasi IP dan beberapa *port* yang terbuka dan dapat dilihat pada Gambar 4.

Gambar 4. Hasil *scan* Nmap

C. Exploiting dengan Metode STRIDE

Pada tahap ini melakukan exploitasi melalui celah atau bug yang ada pada sistem dengan melakukan tahap pengujian diantaranya:

a) *Spoofing* untuk mengakses sistem dengan menggunakan identitas orang lain dengan bantuan *tools* Setoolkit dan Ettercap [10].
b) *Tampering* tanpa mempunyai hak akses namun dapat mengubah data yang ada di dalam database dengan bantuan *tools* Burp Suite dan Backdoor [11].
c) *Repudiation* membuat sebuah sistem dan sengaja menyisipkan *bugs*, atau menyertakan virus tertentu di dalam aplikasi sehingga dapat digunakan untuk mengakses sistem pada suatu saat.
d) *Information disclosure* membuka atau membaca sebuah informasi tanpa memiliki hak akses atau membaca sesuatu tanpa mempunyai hak otoritas.
e) *Denial of Service* membuat sebuah sistem tidak bekerja atau tidak dapat digunakan orang lain dengan bantuan *tools* Pentmenu.
f) *Elevation of privilage* menyalahgunakan wewenang yang dimiliki untuk mengakses sebuah sistem untuk kepentingan pribadi.

D. Reporting dengan Metode DREAD

Tahap *reporting* merupakan tahap yang dilakukan untuk mendokumentasikan kerentanan atau celah keamanan yang sudah dieksploitasi pada sistem, kemudian akan menghitung tingkat risiko kerentanan atau celah keamanan dapat dilihat pada tahap penilaian berikut:

a) *Damage Potensial* (potensi kerusakan) seberapa besar kerusakan kelemahan tersebut di exploitasi.
b) *Reproducibility* (reproduktifitas) seberapa mudah untuk reproduktifitas serangan itu.
c) *Exploitability* (eksploitasi) seberapa mudah untuk melalui serangan.
d) *Affected User* (terkena pengguna) seberapa besar persentase kasar, berapa banyak pengguna terpengaruh.
e) *Discoverability* (dapat ditemukan) seberapa mudah untuk menemukan kerentanan.

E. Identifikasi Ancaman

Dari hasil pengujian ancaman yang telah dilakukan, didapatkan hasil identifikasi jenis ancaman seperti pada Tabel I.

TABEL I
JENIS ANCAMAN STRIDE

No	Jenis Ancaman	Hasil	Asset
1.	*Spoofing*	Setelah melakukan pengujian Dns *Spoofing* pada learning.unla.ac.id menggunakan jaringan lokal yang terdapat pada sistem, saat berhasil melakukan dns *spoofing* dan mendapatkan *username* dan *password*.	Data mahasiswa, jaringan di dalam kampus dan diluar kampus.
2.	*Tampering*	Ketika menemukan salah satu celah keamanan pada file upload foto pada akun mahasiswa dan melakukan pengujian tamper data pada upload file yang berupa file backdoor yang bertujuan masuk pada sistem melalui jalan belakang. Namun pada tahap ini tidak berhasil melakukan tamper data dikarenakan keamanan pada elearning.unla.ac.id sangat ketat.	Tidak Ada
3.	*Repudiation*	Ketika mencoba melakukan upload file backdoor yang berupa gambar dengan tujuan agar bisa masuk pada sistem administrator sehingga dapat membuat sebuah vulnerability di dalam sistem. Namun tidak berhasil masuk kedalam sistem.	Tidak Ada
4.	*Information Disclosure*	Dengan hasil pengujian yang dilakukan dengan memanfaatkan celah keamanan dengan menggunakan dns spoofing dan berhasil mendapatkan informasi penting yang berupa data diri mahasiswa.	Data Mahasiswa
5.	*Denial of Service*	Dengan hasil pengujian discovery memanfaatkan celah keamanan pada port-port yang maka dilakukan serangan DoS pada web server dengan hasil membuat sistem sibuk dan tidak bisa diakses untuk beberapa waktu.	Web Server
6.	*Elevation Privilege*	Ketika mencoba masuk pada sistem agar bisa mendapat hak akses admin namun tidak berhasil dilakukan.	Data Mahasiswa

F. Tingkat Ancaman

Setelah melalui tahap identifikasi ancaman, selanjutnya akan dilakukan penilaian dengan menggunakan metode DREAD. Untuk mengetahui rumusan dan penilaian menggunakan metode DREAD dapat dilihat pada Tabel II.

TABEL III
PENILAIAN ANCAMAN DREAD

	Penilaian	Tinggi (3)	Medium (2)	Rendah (1)
D	Damage Potential	Penyerang dapat menumbangkan sistem keamanan, mendapatkan otorisasi kepercayaan penuh, berjalan sebagai administrator,meng-upload konten.	Membocorkan informasi sensitif.	Membocorkan informasi sepele.
R	Reproducibility	Serangan dapat direproduksi setiap saat dan tidak memerlukan jendela waktu.	Serangan dapat direproduksi, tetapi hanya jendela waktu dan situasi ras tertentu.	Serangan sangat sulit mereproduksi, bahkan dengan pengetahuan dari lubang keamanan.
E	Exploitability	SeorangProgrammer pemula biasa membuat serangan dalam waktu singkat.	Seorangprogrammer yang terampil bisa membuat serangan, kemudian ulangi langkah langkah.	Serangan itu membutuhkan orang yang sangat terampil dan pengetahuan yang mendalam setiap kali untuk mengeksploitasi.
A	Affected User	Semua pengguna,konfigurasi default, pelanggan utama.	Beberapapengguna,non konfigurasi default.	Persentase yangsangat kecil.
D	Discoverability	Informasi diterbitkan menjelaskan serangan. Kerentanan ditemukan dalam fitur yang paling umum digunakan dan sangat terlihat.	Kelemahan tersebut di bagian yang jarang digunakan.	Bug tidak jelas.

Dari tabel penilaian ancaman metode DREAD tersebut digunakan untuk menghitung risiko yang dapat menghasilkan informasi peringkat risiko untuk sebuah ancaman yang terjadi. Untuk mengetahui peringkat risiko dengan model DREAD, beberapa hal yang perlu diperhatikan berhubungan dengan kepanjangan dari DREAD yaitu:

1) Damage Potential: seberapa besar kerusakan jika kelemahan tersebut di-eksploitasi?
2) Reproducibility: seberapa mudah untuk reproduktifitas serangan itu?
3) Exploitability: seberapa mudah untuk melalui serangan?
4) Affected User: berapa banyak pengguna terpengaruh?

5) Discoverability: seberapa mudah untuk menemukan kerentanan?

Dari hasil identifikasi ancaman, dari setiap pertanyaan yang terdapat pada atribut DREAD, bila pada setiap atribut pertanyaannya yang diajukan telah dijawab untuk risiko yang rendah diberi nilai (1), untuk risiko sedang diberikan nilai (2), dan untuk nilai yang tinggi diberikan nilai (3). Setelah mendapatkan nilai tersebut hasilnya dibagi dari banyaknya atribut pada DREAD yaitu 5. Setelah pertanyaan-pertanyaan dijawab, hasil dari setiap ancaman dilakukan proses menghitung dengan pemberian nilai dengan skala 1-3 dari setiap atribut DREAD. Hasil dari berbagai pertanyaan-pertanyaan yang sudah diajukan memiliki rentang nilai 5 hingga 15. Untuk mengetahui tingkat ancaman dengan peringkat dapat dilihat pada Tabel III.

TABEL IIIII
PERINGKAT PENILAIAN RISIKO METODE DREAD

No	Rentang Penilaian	Peringkat	Keterangan Risiko
1.	5 hingga 7	3	Rendah
2.	8 hingga 11	2	Sedang
3.	12 hingga 15	1	Tinggi

Setelah mendapatkan rumusan, langsung membuat tingkat penilaian dari setiap ancaman yang telah dihasilkan dari identifikasi ancaman pada metode STRIDE dapat dilihat pada tabel-tabel di bawah ini.

TABEL IVV
HASIL PENILAIAN *SPOOFING*

Ancaman	D	R	E	A	D	Jumlah	Peringkat	Risiko
Spoofing	2	3	2	2	3	12	1	Tinggi

Berdasarkan hasil identifikasi ancaman *spoofing* yang telah dilakukan, didapatkan hasil nilai risiko seperti yang terlihat pada Tabel IV di atas.

TABEL V
HASIL PENILAIAN *TAMPERING DATA*

Ancaman	D	R	E	A	D	Jumlah	Peringkat	Risiko
Tampering Data	1	1	1	1	3	7	3	Rendah

Berdasarkan hasil identifikasi ancaman *tampering data* yang telah dilakukan, didapatkan hasil nilai risiko seperti yang terlihat pada Tabel V di atas.

TABEL VI
HASIL PENILAIAN *REPUDIATION*

Ancaman	D	R	E	A	D	Jumlah	Peringkat	Risiko
Repudiation	1	1	1	1	3	7	3	Rendah

Berdasarkan hasil identifikasi ancaman *repudiation* yang telah dilakukan, didapatkan hasil nilai risiko seperti yang terlihat pada Tabel VI di atas.

TABEL VII
HASIL PENILAIAN *INFORMATION DISCLOSURE*

Ancaman	D	R	E	A	D	Jumlah	Peringkat	Risiko
Information Disclosure	2	3	2	2	3	12	1	Tinggi

Berdasarkan hasil identifikasi ancaman *information disclosure* yang telah dilakukan, didapatkan hasil nilai risiko seperti yang terlihat pada Tabel VII di atas.

TABEL VIII
HASIL PENILAIAN *DENIAL OF SERVICES*

Ancaman	D	R	E	A	D	Jumlah	Peringkat	Risiko
Denial of Services	3	3	1	3	1	11	2	Sedang

Berdasarkan hasil identifikasi ancaman *denial of services* yang telah dilakukan, didapatkan hasil nilai risiko seperti yang terlihat pada Tabel VIII di atas.

TABEL IX
HASIL PENILAIAN *ELEVATION PRIVILEGE*

Ancaman	D	R	E	A	D	Jumlah	Peringkat	Risiko
Elevation Privilege	1	1	1	2	1	6	3	Rendah

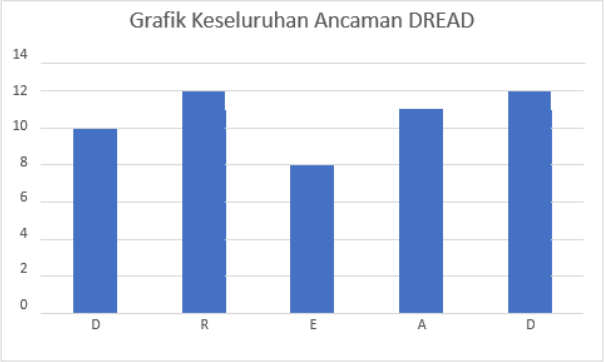
Berdasarkan hasil identifikasi ancaman *elevation privilege* yang telah dilakukan, didapatkan hasil nilai risiko seperti yang terlihat pada Tabel IX di atas.

Dari hasil perhitungan setiap identifikasi ancaman yang sudah dilakukan, kemudian akan menghitung keseluruhan dan mengelompokkan hasil penilaian yang sudah dihitung sebelumnya, dapat dilihat pada Tabel X.

TABEL X
HASIL PENILAIAN KESELURUHAN ATRIBUT DREAD

No.	Ancaman	D	R	E	A	D	Jumlah	Rata-rata	Tingkat Risiko
1.	*Spoofing*	2	3	2	2	3	**12**	**2.4**	Tinggi
2.	*Tampering*	1	1	1	1	3	**7**	**1.4**	Rendah
3.	*Repudiation*	1	1	1	1	1	**5**	**1**	Rendah
4.	*Information Disclosure*	2	3	2	2	3	**12**	**2.4**	Tinggi
5.	*Denial of Service*	3	3	1	3	1	**11**	**2.2**	Sedang
6.	*Elevation Of Privilege*	1	1	1	2	1	**6**	**1.2**	Rendah
Total		**10**	**12**	**8**	**11**	**12**	**53**	**10.6**	Sedang

Dari hasil perhitungan nilai total keseluruhan ancaman didapatkan nilai 10,6 yang berarti dari total keseluruhan ancaman mendapatkan nilai 10,6 dengan tingkatan risiko yang sedang. Dari hasil nilai ancaman tersebut dapat dibuatkan grafik keseluruhan ancaman dengan metode DREAD, grafik dapat dilihat pada Gambar 5.



Gambar 5. Grafik Penilaian Keseluruhan Ancaman

IV. SIMPULAN

Berdasarkan hasil penelitian yang sudah dilakukan, didapatkan beberapa celah keamanan sesuai metode STRIDE yaitu pada *spoofing, information disclosure, dan denial of service*. Hasil penilaian terhadap keamanan *web* elearning.unla.ac.id menggunakan model DREAD, didapat nilai tertinggi 12 dan nilai terendah 8. Untuk secara keseluruhan, tingkat ancaman terhadap *web* elearning.unla.ac.id adalah sedang dengan nilai 10,6 yang artinya masih diperlukan beberapa perbaikan.

REFERENSI

[1] T. N. Azis, "Strategi pembelajaran era digital." *The Annual Conference on Islamic Education and Social Science*. Vol. 1. No. 2. 2019.

[2] "Elearning Universitas langlangbuana," *Elearning Universitas Langlangbuana*. [Online]. Tersedia: http://elearning.unla.ac.id/. [Diakses: 14-Mar-2021].

[3] I. Y. Sari, dkk. *Keamanan Data dan Informasi*. Yayasan Kita Menulis, 2020.

[4] A. Ramadhani, "Keamanan Informasi." *Nusantara Journal of Information and Library Studies (N-JILS)* 1, no. 1 (2018): 39-51.

[5] P. Wiguna, "*Penilaian Risiko Celah Keamanan Pada Sistem Informasi Akademik Menggunakan Metode Stride dan Dread (Studi Kasus: www.unla.ac.id)*", Skripsi Sarjana, Program Studi Teknik Informatika, Universitas Langlangbuana, 2017.

[6] M. Kasiran, *Metodologi Penelitian Kualitatif-Kuantitatif*, Malang: UIN Maliki Press, 2010.

[7] K. Scarfone, dkk. "Technical guide to information security testing and assessment." *NIST Special Publication* 800.115, 2008.

[8] A. Shostack, "Experiences Threat Modeling at Microsoft", *MODSEC@ MoDELS*, 2008.

[9] S, Mujahid, dkk, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool." *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*. IEEE, 2019.

[10] K. Barta, "Creation of Pentesting Labs." PhD diss., University of Cincinnati. College of Education, Criminal Justice, and Human Services, 2013.

[11] S. Wear, *Burp Suite Cookbook: Practical recipes to help you master web penetration testing with Burp Suite*. Packt Publishing Ltd, 2018.