Jurnal Ilmiah Informatika (JIF)
| ISSN (Print) 2337-8379 | ISSN (Online) 2615-1049 |
Jurnal online di akses di http://ejournal.upbatam.ac.id/index.php/jif

Peran *Ethical Hacking* dalam Memerangi *Cyberthreats*

Qorry Aina Fitroh[1], Bambang Sugiantoro[2]

[1, 2] Universitas Islam Negeri Sunan Kalijaga, Jl. Laksda Adisucipto Depok, Sleman, Daerah Istimewa Yogyakarta, 55281, Indonesia

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Redaksi: 27 Desember 2022
Revisi Akhir: 02 Februari 2023
Diterbitkan *Online*: 10 Maret 2023

KATA KUNCI

Hacker
Ethical hacking
Cyberthreats
Black hat hackers
White hat hackers

KORESPONDENSI

E-mail: qorryafitroh@gmail.com

A B S T R A C T

The efforts to digitize and optimize various things in the modern world will certainly highlight issues related to cybersecurity such as data breaches, security breaches, and so on. Ethical hacking and its need in the future cannot be avoided. Ethical hacking technology is spreading in almost every aspect of life, especially the computer industry, which requires protection of important data and must be handled with the right technology. Ethical hacking aims to find vulnerabilities in security systems and discover potential data breaches. This contrasts with the common understanding of hacking, which is black hat hackers who damage systems with malicious intent and steal data and infect viruses. Ethical hacking is a way to combat and neutralize black hat hackers. Teaching ethical hacking is preparing professionals in the information security field with the tools and skills to combat and prevent cybersecurity threats. Teaching inexperienced people in information security with aggressive methods can be viewed as both beneficial and harmful. This is because the same methods are used by malicious hackers hence educating professionals in information security may be perceived as enhancing malicious hackers. Using the literature study method, this article discusses various issues related to ethical hacking.

1. PENDAHULUAN

Kemajuan teknologi informasi dan meningkatnya ketergantungan terhadap teknologi semakin berkembang dalam masyarakat. Era digitalisasi ini membawa manfaat besar dan memudahkan kehidupan. Meskipun demikian, terdapat risiko terkait dengan penggunaan teknologi informasi, diantaranya risiko *cybernetic* yang dapat menyebabkan kerusakan pada sistem teknologi pada suatu instansi atau organisasi. Dampak negatif lainnya yaitu terjadi peningkatan peretasan atau *hacking*, baik pada akun media sosial, akun bank, pencurian data, dan sebagainya. Hal tersebut menuntut instansi atau organisasi untuk memprioritaskan dalam melindungi aset digital dari ancaman dunia maya atau *cyber threat*. Kegagalan instansi atau organisasi dalam menerapkan langkah-langkah keamanan dasar dalam mengamankan data dapat membuat organisasi rentan terhadap serangan siber [1].

Berdasarkan penilaian *E-Governance Academy* (EGA) tahun 2020 [2], Indonesia memiliki nilai indeks kemanan siber nasional sebesar 38,96 yang menempati peringkat 84. Hal ini jauh dibawah nilai indeks keamanan siber nasional milik negara tetangga, Malaysia dan Singapura yang menempati posisi 20 dan 28 dengan nilai indeks 79,22 dan 71,43. Akan tetapi, nilai indeks keamanan siber nasional Indonesia tidak jauh dengan Brunei Darussalam yang menduduki peringkat 82 dengan nilai 41,56. Nilai indeks tersebut menunjukkan bahwa keamanan siber Indonesia masih tergolong lemah dengan menempati posisi 84 sehingga keamanannya dapat ditembus oleh *hacker* dengan cukup mudah. Hal ini ditunjukkan dari salah satu kasus dalam keamanan siber yaitu kasus kebocoran data yang paling sering dilaporkan oleh BSSN [3].

Adanya teknologi informasi memberi jalan kepada pengguna jahat untuk merusak dengan cara menembus keamanan. Untuk memerangi *hackers* dengan niat jahat, dibutuhkan *ethical hacking* untuk mengidentifikasi kelemahan dalam keamanan dan membantu memperkuat dan mencegah peretasan. *Ethical hackers* menggunakan alat yang sama dengan *hackers* jahat atau yang biasa disebut dengan *black hat hackers* tetapi dengan berbagai auran yang ketat dan hanya diperuntukkan bagi yang sudah memiliki sertifikasi untuk menjadi *ethical hacker* yang diakui secara hukum [4].

Meskipun *ethical hacking* bersifat baik, terkadang *ethical hackers* menjelajah ke dunia illegal dan berubah menjadi *black hat hackers* yang menggunakan pengetahuannya untuk kejahatan. Oleh karena itu, *ethical hacking* harus dilakukan oleh seseorang yang sudah tersertifikasi, harus mematuhi kode etik, dan sadar hukum dalam menjalankan tugasnya. Seseorang yang akan menjadi *ethical hacker* harus diajarkan strategi dan metode yang

dilakukan oleh *black hat hackers*. Dengan demikian, mengajari seseorang berbagai taktik tersebut berpotensi untuk menambah jumlah *hacker* jahat, bukan hanya untuk memperbaiki. Keputusan dari orang tersebutlah yang akhirnya menentukan apakah dia akan menggunakan kemampuan dan pengetahuannya secara jahat atau etis. Selain pengetahuan dan kemampuan yang mapan, moral yang kuat dan baik juga perlu diajarkan kepada seseorang yang akan belajar menjadi *ethical hacker*.

Penelitian ini memberikan ulasan dan analisa singkat mengenai *ethical hacking*, kaitannya dengan keamanan informasi, dan dampak bagi seseorang yang diajarkan *ethical hacking*.

2. TINJAUAN PUSTAKA

2.1 *Hacking*

Hacking atau peretasan oleh sebagian orang dipandang sebagai akses tidak sah ke dalam sistem dan jaringan komputer. Padahal seharusnya tidak demikian. Awalnya, *hacking* mengenai mempelajari bahasa pemrograman dan sistem komputer dengan tujuan agar dapat menciptakan inovasi dan kode program dalam menyelesaikan permasalahan. Hal tersebut terkait dengan memahami komputer secara menyeluruh, membuat inovasi, dan terobosan teknologi. *Ethical hacking* tidaklah melanggar hukum karena memiliki otorisasi sehingga sejalan dengan peraturan.

Saat ini beberapa orang yang memiliki keahlian dalam bidang *hacking* terlibat dalam peretasan yang berbahaya. Mereka mengidentifikasi kelemahan dalam sistem komputer dan mendapatkan akses lalu mengeksploitasi kelemahan tersebut. *Hacking* tidak sah ini dilakukan oleh *hacker* jahat. Mereka adalah agen ancaman yang terlibat dalam peretasan berdasarkan motivasi, peluang, dan kemampuan. Agen *hacker* memiliki kemampuan untuk meretas serta memiliki alat peretasan sehingga mereka sangat lihai dan dapat melakukan ancaman. Agen ini bertindak berdasarkan motivasi dan motif yang berbeda-beda, motivasi tersebut dapat berupa keuntungan, kekuasaan, balas dendam, rasa ingin tahu, atau bahkan politik. Sementara motif di balik tindakan yang dilakukan dapat berupa terorisme, agama, dan sebagainya. Selain motivasi, agen ini juga melakukan ancaman berdasarkan peluang. Sebelum agen mengeksploitasi target, peluang harus muncul dengan sendirinya [5].

2.2 Tipe *Hacker*

Istilah *hacker* pertama kali diperkenalkan pada tahun 1960 oleh programer MIT untuk mendeskripsikan seseorang yang memiliki kemampuan untuk memahami dan memanipulasi teknologi [6]. Tipe *hackers* dapat dilihat dari motif, target, pengalaman, dan strateginya. Perbedaan singkat antara *hackers* dan *ethical hackers* dari segi tindakan dan serangan adalah *hackers* bersifat ofensif dan *harmful* sedangkan *ethical hackers* bersifat defensif dan *simulated*. Tujuannya *hacker malicious* atau dapat dikatakan jahat dan menyerang, sementara *ethical hackers* tujuannya *non-malicious* dan melindungi.

Lebih lengkapnya, *hackers* digolongkan dalam tiga belas kelas [7], yaitu *newbie*, *students*, *thugs*, *online sex offenders*, *old guards*, *insiders*, *petty thieves*, *hacktivist*, *digital pirates*, *professionals*, *crime facilitators*, *crowdsources*, dan *nation states*. Setiap kategori *hacker* tersebut memiliki motivasi dan strateginya masing-masing. Sementara itu, [8] membagi *hackers* dalam tujuh tipe utama, yaitu *white-hat*, *black-hat*, *grey hat*, *green hat*, *red hat*, *script kiddle*, dan *blue hat*. Tipe *hackers* juga diklasifikasikan dalam sembilan kelas, yaitu *state/nation sponsored*, *hacktivist*, *whistle blower*, *cyber spy*, *cyber heist*, *botnet master*, *cyber criminals*, *cyber terrorists*, dan *suicide hackers*. Untuk motivasi atau alasan dalam melakukan *hacking* [7], [8] dibedakan menjadi dua belas, yaitu keingintahuan, rekreasi, ketenaran, keuangan, dorongan seksual, balas dendam, ideologi, politik, patriotisme, religiusitas, rasis, dan sosial.

Sementara itu, secara umum, *hacker* dikategorikan dalam tiga kelas. Ketiga kategori *hacker* tersebut adalah *white hat*, *black hat*, dan *grey hat*. Kategori ini dibagi berdasarkan niat dan tindakan orang-orang yang berada di dalamnya. *White* dan *black* merupakan dua kategori yang paling sering muncul karena kedua kategori tersebut dibagi berdasarkan niatnya, baik ataukah buruk. Sementara kategori *grey* merupakan *hacker* yang tidak termasuk golongan *black* ataupun *white hat*.

White hat hackers biasanya seorang profesional dalam kemanan informasi yang memiliki perangkat *hacker* yang digunakan untuk menemukan titik lemah yang berpotensi dapat dieksploitasi oleh *hacker* jahat. Selain itu, mereka juga merekomendasikan tindakan pencegahan yang dapat dilakukan. *White hat hacker* seharusnya dapat dipercaya dan tidak mengeksploitasi informasi sensitif apapun yang didapatkannya[9]. Mereka akan mendapatkan otorisasi dari organisasi yang memiliki hak pada sistem yang akan dibobolnya sehingga pemilik sistem sepenuhnya sadar saat adanya upaya *hacking* yang akan dilakukan.

Berbeda halnya dengan *white hat hackers*, *black hats* memiliki niat yang jahat. Jenis *hacker* ini paling terkenal dan biasanya dikaitakn dengan istilah *hacker* itu sendiri. Meskipun kedua *hackers* tersebut menggunakan alat yang serupa untuk mengakses sistem, hal utama yang membedakan adalah niatnya. Selain itu, *black hats* juga tidak memiliki otorisasi untuk mengakses sistem. *Black hats* menggunakan keahliannya untuk mengacaukan, merusak, dan mencuri dari sistem komputer dan pemiliknya. Mereka mencari keuntungan pribadi dari tindakan yang dilakukannya seperti dengan menjual data curian, menghancurkan data untuk menimbulkan masalah bagi pengguna yang berwenang ke depannya, mereka juga bisa merusak komputer dengan menanam ancaman seperti virus, *spyware*, *malware*, dan sebagainya.

Grey hat hackers bisa disebut perpaduan anatara *white hat* dan *black hat hackers*. Sebagian besar dari *grey hats* bertindak secara ilegal dan tidak mendapatkan otorisasi untuk mengakses sistem. Akan tetapi, *grey hats* tidak sepenuhnya jahat sebab yang dilakukannya tidak untuk mengeksploitasi ataupun membantu pemiliknya, mereka melakukan *hacking* hanya untuk bersenang-senang [9]. beberapa *grey hats* berawal dari *black hats* yang kemudian menggunakan keahliannya sesuai dengan persepsi mereka tentang kebaikan[6]. Kasus umum dalam ranah non-pemerintahan yang dilakukan *grey hats* adalah membobol situs web atau sistem komputer suatu organisasi tanpa izin. Kemudian mereka menghubungi organisasi terkait untuk meminta kompensasi sebagai imbalan atas detail kelemahan keamanan yang ditemukan. Meskipun tindakan mereka mungkin memiliki niat baik, mereka tetap dikatakan ilegal sebab tidak mendapat izin untuk melakukannya.

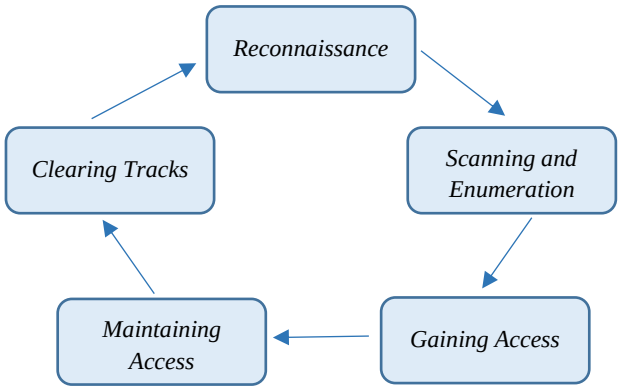
White hat dan *grey hat hackers* tergolong *old guards* dalam kategori yang dijabarkan oleh Samuel Chang dan rekan-rekannya. Sementara, *black hat hackers* tergolong *professionals*. Kategori *old guards* memiliki alasan untuk melakukan *hacking*, diantaranya karena keingintahuan, ketenaran, rekreasi atau bersenang-senang sebagai hiburan, dan ideologi. Sedangkan *professional* dalam melakukan *hacking* didasari alasan balas dendam dan finansial.

2.3 *Ethical Hackers*

Ethical hackers termasuk kategori *white hat hackers*. Seorang *ethical hacker* profesional harus bersertifikasi yang mengharuskan mereka untuk memiliki pengalaman dalam keamanan informasi dan lulus ujian. Organisasi yang menggunakan *ethical hacker* biasanya menanyakan keselamatan dan keamanan data sensitif. Jika *ethical hacker* mendapatkan akses kepada informasi atau data tersebut, mereka harus dipercaya untuk tidak mencuri atau memanfaatkan data untuk kepentingan pribadi. Perbedaan *ethical hacker* dengan *white hat* ada pada kode etik yang harus selalu diikuti oleh *ethical hacker*. Melalui kode etik ini, mereka mendapatkan kepercayaan dan kredibilitas lebih banyak daripada *white hat hackers* biasanya. *Ethical hacker* penting untuk melakukan *update* informasi terkait metode penetrasi baru, walaupun mereka harus tetap berpegang kepada kode etik.

Sementara itu, proses dalam melakukan *ethical hacking* secara umum meliputi lima tahapan [10] seperti yang ditunjukkan oleh Gambar 1. Tahapan pertama adalah *reconnaissance* yang merupakan serangkaian prosedur dan teknik untuk mendapatkan informasi atau data mengenai sistem yang ditargetkan dengan rahasia. Pada tahap ini mencakup identifikasi mesin aktif dan setiap *port service*, pengumpulan informasi awal, pemetaan jaringan, identifikasi *port* terbuka dan titik akses, serta sidik jari OS. Tahap kedua adalah *scanning and enumeration*. *Scanning* digunakan untuk mencari kelemahan yang dapat disalahgunakan pada *port*. Sementara *enumeration* merupakan serangan jaringan utama. Melalui *enumeration*, dilakukan aktivitas menghubungkan untuk mengumpulkan informasi tentang target mesin.

Tahapan selanjutnya adalah *gaining access* menggunakan bantuan beberapa alat dan teknik. Hal ini pada dasarnya berfokus pada pengambilan *password* sehingga *hacker* dapat menyimpulkan beberapa alternatif untuk mengakses sistem. Tahap keempat adalah *maintaining access*. Setelah *hacker* berhasil mengakses sistem, sistem dan sumber dayanya dapat dimanfaatkan dan digunakan sebagai landasan untuk menguji dan merusak sistem lain serta mengeksploitasi tanpa pemilik sistem mengetahuinya. Tahapan terakhir adalah *clearing tracks*. Proses ini pada dasarnya dapat dikatakan sebagai aktivitas tidak etis. Dengan tujuan seperti menghindari deteksi, *hacker* akan menghapus konfirmasi aktivitas dan keberadaannya dalam sistem. Menghilangkan jejak atau bukti merupakan persyaratan untuk setiap *hacker* agar menjaga identitasnya untuk tetap anonym dan mencegah deteksi balik.



Gambar 1. Langkah-langkah *Ethical Hacking*

3. METODOLOGI

Penelitian ini menggunakan metode kualitatif melalui studi literatur yang dikaji dari berbagai sumber. Penulisan artikel ini bersifat deksriptif untuk menggambarkan analisis dari fenomena *ethical hacking*. Artikel ini membahas tentang (1) Pentingnya *ethical hacking*; (2) Kode etik dalam *ethical hacking*; (3) Pro dan kontra adanya *ethical hacking*; dan (4) Mengajarkan *ethical hacking* kepada siswa.

4. HASIL DAN PEMBAHASAN

4.1. Pentingnya *Ethical Hacking*

Meningkatnya kejahatan dalam dunia maya seperti *black hat hackers* dan berbagai serangan siber yang dilakukannya, seperti serangan web, aplikasi, jaringan, maupun serangan infrastruktur [8]. Organisasi perlu melakukan langkah untuk memerangi serangan ilegal yang mungkin terjadi pada sistemnya. Hal ini dilakukan oleh profesional yang direkrut untuk memberikan analisis yang tidak bias tentang struktur dan keamanan organisasi tersebut [9]. *Ethical hackers* memastikan bahwa semua sistem dilindungi dan tidak dapat diakses oleh *black hat hackers*. Profesional keamanan informasi biasanya bersikap defensif. Sering kali, mereka hanya dapat melakukan tindakan pencegahan untuk menghalangi *hackers* jahat memasuki sistem. Ketika *hackers* jahat mendapatkan akses ke sistem atau jaringan yang dibatasi, profesional keamanan informasi menjalankan tugasnya untuk mengendalikan kerusakan. *Ethicak hacker* memberikan kesempatan bagi profesional keamanan informasi untuk melakukan tindakan yang lebih ofensif dalam melindungi sistem dan jaringan dari organisasi yang merekrutnya [11].

Penelitian tahun 2013 [12] menunjukkan bahwa 206 profesional keamanan siber dengan lugas menjawab cara terbaik untuk mencegah *hackers* jahat yaitu dengan melibatkan *hacking* secara instruksional dalam organisasi. Penting bagi profesional *cybersecurity* untuk memahami berbagai teknik *hacking* untuk melindungi sistem secara efisien. Sebagian besar organisasi saat ini memiliki profesional *cybersecurity* di dalamnya. *Ethical hacker* yang bersertifikasi dipandang sebagai keamanan ekstra atau sebagai auditor *cybersecurity* dalam suatu organisasi. Tujuan dari adanya ekstra keamanan adalah untuk meningkatkan keamanan sistem atau jaringan, bukan untuk merusak atau mencuri data dari organisasi tersebut [11]. Mereka akan menyampaikan setiap risiko keamanan atau kerentanan yang ditemukan, serta tingkat keparahannya kepada organisasi yang merekrut dan kemudian memberikan solusi potensial yang dapat digunakan untuk menghilangkan atau mengurangi risiko yang mungkin terjadi. Adanya *ethical hacking* diperlukan dalam suatu organisasi sebagai jaminan bahwa organisasi tersebut kredibel sehingga dapat menjaga reputasinya [13].

4.2. Kode Etik

Terdapat beberapa kode etik yang berlaku dalam industri keamanan informasi yang diakui oleh dunia dan dijalankan oleh organisasi atau instansi. Beberapa kode etik tersebut [6] adalah yang dibuat oleh *Australian Computer Society* (ACS) pada industri informasi, komunikasi, dan teknologi (ICT). Meskipun berfokus pada bidang ICT, ACS membuat sertifikasi khusus dalam bidang *cyber security* untuk profesional ICT pada tahun 2017. Selain itu, ada kode etik yang diluncurkan oleh CREST yang berasal organisasi nirlaba dari Inggris. Meskipun demikian,

sudah ada cabang-cabanya di seluruh Eropa, Timur Tengah, Afrika, India, Amerika, Asia, Australia, dan Selandia Baru. Kode etik CREST relatif mendetail yang meliputi persyaratan seperti memastikan kewajiban peraturan, manajemen proyek yang memadai, kompetensi, kepentingan klien, kerahasiaan, dan etika. Kode etik lain adalah yang diadakan oleh *The International Council of E-Commerce Consultants* atau yang biasa dikenal dengan EC-Council yang membuat sertifikasi *Certified Ethical Hacker* (CEH), ada juga *Global Information Assurance Certification* (GIAC) yang berdiri sejak 1999, ISACA, dan ISC2 yang juga menyediakan sertifikasi untuk kode etik.

Di antara berbagai sertifikasi kode etik tersebut, sebagian besar industri di Indonesia menerapkan sertifikasi yang berasal dari EC-Council yang telah didirikan sejak 2001. Sertifikasi CEH yang dimilikinya telah diakui oleh *Department of Defense* (DoD) Amerika Serikat. Kode etik EC-Council menysaratkan kerahasiaan informasi yang ditemukan, memastikan bahwa proses atau *software* apapun yang digunakan adalah legal dan etis, memastikan otorisasi yang tepat, manajemen proyek yang memadai, pengembangan profesional berkelanjutan, perilaku etis, dan tidak dihukum karena kejahatan apapun [6].

Adanya sertifikasi tersebut, mengharuskan seorang *ethical hackers* atau seorang profesional keamanan informasi harus lulus ujian sertifikasi yang dilakukan oleh EC-Council. Namun, untuk mempertahankan kepemilikan sertifikasi, *ethical hacker* harus mengikuti kode etik EC-Council. Meskipun sebagian besar aturan ini bergantung pada akal sehat, beberapa tetap ambigu dan mungkin berbeda artinya dalam situasi yang berbeda. Ambiguitas dalam kode etik *ethical hackers* yang dapat mempertanyakan etika profesional yang dimilikinya.

Salah satu hal umum yang ada dalam kode etik EC-Council adalah tidak mencuri atau merusak informasi klien, tidak melibatkan diri dalam praktik keuangan yang menipu, dan harus mendapatkan otorisasi yang tepat sebelum mengakses sistem atau jaringan. Walaupun *ethical hacker* menggunakan metode dan alat yang mirip dengan *hacker* jahat, kode etik EC-Council mengharuskan *ethical hackers* untuk menghindari kontak dan afiliasi dengan *black hat hackers* ataupun komunitasnya karena hal tersebut dapat menimbulkan masalah dengan *ethical hacker* ketika mereka mencoba untuk tetap mengikuti perkembangan metode dari *black hat hackers* [6].

Sebelum melakukan *ethical hacking*, *hackers* harus memahami karakteristik dari sistem, jaringan dan *framework* keamanan. Selain itu, *hacker* harus mengenali tingkat sensitivitas dan kerahasiaan informasi atau data yang akan dihadapi agar tidak melanggar hukum, aturan, dan regulasi dari organisasi tersebut. Seorang *ethical hacker* dalam praktiknya harus memelihara transparansi dengan klien dan menjaga kepercayaan setiap waktu. Setiap informasi resmi yang relevan harus dikomunikasikan dengan jelas untuk memastikan pemahaman terhadap prosedur dan penemuan yang dilakukan oleh *hacker*.

Saat menjalankan *ethical hacking*, *hacker* harus berhati-hati agar tidak mengakses sistem atau *software* selain yang didaftarkan oleh klien. Setelah *ethical hacking* dan perjanjian dengan klien selesai dijalankan, *hacker* tidak diperbolehkan untuk membeberkan informasi atau data yang ditemukannya kepada pihak lain. *Ethical hacking* dilakukan untuk menjamin keamanan sistem. Membocorkan informasi akan membuat proses yang telah dilakukan menjadi tidak berlaku dan tidak efektif. Data privat dan rahasia harus tetap dijaga privasi dan kerahasiaannya [9].

4.3. Pro dan Kontra

Pro dan keuntungan adanya *ethical hacker* dalam suatu organisasi di antaranya dapat memberikan bukti yang meyakinkan dan menentukan ancaman dari jaringan atau sistem secara nyata melalui bukti akses. Temuan dapat bersifat negatif, tetapi hal itu akan membantu mengungkapkan potensi celah dan kelemahan dalam keamanan sistem secara keseluruhan. Hasilnya aka nada gambaran secara jelas tentang kekuatan proses deteksi dan mekanisme respon. Selain itu, adanya *ethical hacker* juga dapat mengidentifikasi keamanan sistem administrator atau manajemen yang tidak diperhatikan karena mungkin tidak *up to date* pada teknologi terbaru dan metode yang digunakan oleh *hackers* atau potensi adanya *cyberthreat*. *Ethical hackers* juga memiliki peran yang besar dalam melindungi sebagian besar rahasia berharga negara.

Sementara itu, ada beberapa hal yang membuat kontra dari adanya *ethical hackers* ini. Mendidik dan mengedukasi seseorang untuk menjadi *ethical hacker* dapat terbukti kontraproduktif karena kebenaran niat dari seseorang tidak dapat dijabarkan dan mereka berkemungkinan menggunakan kemampuannya untuk menjadi *black hat hackers*. Selain itu, merekrut *ethical hackers* membutuhkan dana yang tidak sedikit. Organisasi yang menggunakan *ethical hacker* juga tidak mengetahui apa saja informasi yang telah diambil dari sistemnya. Setiap kesalahan yang dilakukan oleh *hacker* amatir ketika melakukan tes tertentu dapat berbahaya karena mungkin merusak data dan menghambat sistem operasi. Dengan demikian, organisasi harus berhati-hati dalam merekrut *ethical hacker* dan memastikan mereka memiliki sertifikat professional untuk melakukan *ethical hacking* [9].

4.4. Mengajarkan *Ethical Hacking*

Ide dibalik mengajarkan metode *hacking* pada tingkat universitas adalah mengajarkan bagaimana melindungi aset data calon organisasi yang akan merekrut. Perdebatan mengenai mengajarkan *hacking* kepada siswa selalu ada karena mereka mungkin menggunakan kemampuannya untuk memperkuat keamanan jaringan dan berbagai keuntungan serta kebaikan lainnya bagi organisasi perekrut, atau menggunakan kemampuannya secara negatif atau dengan cara ilegal [14]. Siswa berpotensi untuk menggunakan teknik yang telah dipelajari secara tidak bertanggung jawab, tidak tepat atau dengan cara ilegal yang dapat dianggap oleh pengajar keamanan sebagai hal yang tidak etis dan tidak bertanggung jawab secara sosial [6].

Siswa harus diberikan pelatihan secara tepat dalam etika dan hukum. Tujuan dari mengajarkan *hacking* adalah untuk menanamkan pengetahuan dan cara mengaplikasikannya. Tujuan tersebut akan menjadi lebih jelas ketika dihubungkan dengan kemampuan seorang auditor. Melalui kemampuan tersebut, siswa dapat menguji sistem untuk menunjukkan kekurangan dari desain sistem serta masalah keamanan. Dengan memahami cara untuk meretas, siswa tidak hanya mengetahui bagaimana sistem dilanggar, tetapi dapat mengidentifikasi tanda-tanda sistem dilanggar dan dapat menentukan bagian sistem yang mungkin diserang oleh *hacker*. Dengan memiliki keahlian yang sama dengan *hacker* jahat, siswa dapat lebih baik dalam melindungi sistem. Agar siswa dapat menggunakan kemampuannya di masa depan, kuncinya adalah dengan mengajarkan etika dan implikasi legal dari kemampuan yang dimilikinya serta dampak dari penyalahgunaan keahlian yang mereka miliki.

Perhatian terhadap cara terbaik yang ditawarkan untuk mempersiapkan keamanan profesional di masa depan adalah dengan praktik yang menekankan pendekatan langsung dan penggabungan *soft skills*. Kurikulum untuk mengajarkan teknik *ethical hacking* harus cukup mempersiapkan siswa untuk

memiliki karir pada bidang keamanan. Kurikulum yang tidak memberikan siswa kesempatan untuk praktik eksperimen dengan berbagai teknik keamanan berpotensi menyebabkan siswa kurang mampu dipersiapkan untuk karir di masa depan. Mereka harus ditanamkan keahlian dan rasa percaya diri dengan keahlian tersebut bahwa mereka dapat memerangi penyerang sistem nantinya. Jika siswa tidak memiliki kesempatan untuk bereksperimen dengan "*real hacking*", mungkin mereka akan kurang mampu dan siap untuk menggagalkan serangan di masa mendatang [11]. Pendidikan atau pelatihan yang biasa dilakukan oleh siswa secara formal belum tentu cocok dengan "*real hackers*". Hal ini perlu penelitian lebih lanjut, termasuk untuk menguji keefektifan sertifikasi *ethical hacking* yang telah diperoleh [6].

5. KESIMPULAN DAN SARAN

Penting bagi organisasi atau instansi menerapkan *ethical hacking*. Meskipun memiliki kekurangan tersendiri, adanya *ethical hacking* berpotensi melakukan hal yang baik jika dilakukan dengan benar. Hampir setiap aktivitas keseharian manusia berkaitan dengan dunia digitalisasi seperti *e-commerce*, kelas dan *meeting online*, serta perbankan. Selain itu, komputer dan teknologi terus melakukan pembaharuan yang berkelanjutan yang membuatnya mengharuskan adanya *ethical hacking*. Untuk melindungi dari *black hat hackers* yang menyalahgunakan *hacking* dengan tujuan mendapatkan keuntungan pribadi dan juga menjaga keamanan serta mencegah *cyberthreats*, diperlukan *ethical hackers*. Setiap organisasi atau instansi membutuhkan *ethical hacker* untuk memeriksa sistem keamanan dan menemukan kerentanan di dalamnya dan kemudian memperbaikinya. *Ethical hackers* yang direkrut tentunya harus sudah memiliki sertifikat profesional dari EC-Council dan mematuhi kode etiknya. Selain itu, mereka juga harus dapat dipercaya oleh organisasi baik di masa lalu, saat ini, ataupun mendatang. Sementara itu, mengajarkan *ethical hacking* kepada siswa dapat dipandang sebagai hal yang kontraproduktif sebab kelak di masa mendatang tidak menutup kemungkinan keahlian yang dimilikinya akan digunakan untuk hal yang jahat dan dengan cara yang ilegal. Oleh karena itu, selain mengajarkan keahlian dan praktik nyata, siswa harus dibekali dengan moral yang matang agar tidak melanggar kode etik dan hukum.

DAFTAR PUSTAKA

[1] A. M. AL Hawamleh, A. S. M. Alorfi, J. A. Al-Gasawneh, dan G. Al-Rawashdeh, "Cyber Security and Ethical Hacking: The Importance of Protecting User Data," *Solid State Technol.*, vol. 63, no. 5, hal. 7894–7899, 2020, [Daring]. Tersedia pada: http://solidstatetechnology.us/index.php/JSST/article/view/7202.

[2] "National Cyber Security Index," 2020. https://ncsi.ega.ee/ncsi-index/.

[3] K. R. Ramadhan dan C. Wijaya, "The Challenges of Personal Data Protection Policy in Indonesia: Lesson learned from the European Union, Singapore, and Malaysia," *Tech. Soc. Sci. J.*, vol. 36, hal. 18–28, 2022.

[4] L. A. Smith, M. M. Chowdhury, dan S. Latif, "Ethical hacking: Skills to fight cybersecurity threats," *Epic Ser. Comput.*, vol. 82, hal. 102–111, 2022, doi: 10.29007/vwww.

[5] B. O. Omoyiola, "The Legality of Ethical Hacking," *IOSR J. Comput. Eng.*, vol. 20, no. 1, hal. 61–63, 2018, doi: 10.9790/0661-2001016163.

[6] G. Thomas, O. Burmeister, dan G. Low, "Issues of implied trust in ethical hacking," *ORBIT J.*, vol. 2, no. 1, hal. 1–19, 2018, doi: 10.29297/orbit.v2i1.77.

[7] T. Sutikno dan D. Stiawan, "Cyberattacks and data breaches in Indonesia by Bjorka: hacker or data collector?," *Bull. Electr. Eng. Informatics*, vol. 11, no. 6, hal. 2989–2994, 2022, doi: 10.11591/eei.v11i6.4854.

[8] J.-P. A. Yaacoub, H. N. Noura, O. Salman, dan A. Chehab, "A Survey on Ethical Hacking: Issues and Challenges," hal. 1–46, 2021, [Daring]. Tersedia pada: http://arxiv.org/abs/2103.15072.

[9] G. Vishnuram, K. Tripathi, dan A. K. Tyagi, "Ethical Hacking: Importance, Controversies and Scope in the Future," *Int. Conf. Comput. Commun. Informatics*, 2022, doi: 10.1109/ICCCI54379.2022.9740860.

[10] P. K. Sahu dan B. Acharya, "A Review Paper on Ethical Hacking," *Int. J. Adv. Res. Eng. Technol.*, vol. 11, no. 12, hal. 163–168, 2020, doi: 10.34218/IJARET.11.12.2020.018.

[11] R. Hartley, D. Medlin, dan Z. Houlik, "Ethical Hacking: Educating Future Cybersecurity Professionals," *Proc. EDSIG Conf.*, hal. 1–10, 2017, [Daring]. Tersedia pada: http://proc.iscap.info/2017/pdf/4341.pdf%0Ahttp://iscap.info.

[12] R. E. Pike dan S. S. Curl, "The 'ethics' of teaching ethical hacking," *2013 Proc. ISECON Inf. Syst. Educ. Conf. CONISAR 2013, Conf. Inf. Syst. Appl. Res.*, vol. 22, no. 4, 2013.

[13] A. R. Kelrey dan A. Muzaki, "Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan," *Cyber Secur. dan Forensik Digit.*, vol. 2, no. 2, hal. 77–81, 2019, doi: 10.14421/csecurity.2019.2.2.1625.

[14] B. A. Pashel, "Teaching Students to Hack : Ethical Implications in Teaching Students to Hack at the University Level," *InfoSecCD Conf.*, hal. 197–200, 2006.

BIODATA PENULIS

Qorry Aina Fitroh
Mahasiswa Magister di Program Studi Informatika Universitas Islam Negeri Sunan Kalijaga Yogyakarta.

Bambang Sugiantoro
Dosen di Program Studi Informatika Universitas Islam Negeri Sunan Kalijaga Yogyakarta.