Jurnal Layanan Masyarakat (*Journal of Public Service*), vol 6 no 2 Tahun 2022, halaman 385-394
ISSN 2580-8680, e-ISSN 2722-239X

TRAINING & SIMULATION CRACK VS HACK 1.0 AT SMA NEGERI 3 SEMARANG

PELATIHAN & SIMULASI CRACK VS HACK 1.0 DI SMA NEGERI 3 SEMARANG

Sendi Novianto[1], Setyo Budi*[2], Farrikh Al Zami [3], Sasono Wibowo[4], Achmad Wahid Kurniawan[5], Budi Widjajanto[6]

[1,5]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
[*2,3,4,6]Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
*e-mail: setyobudi@dsn.dinus.aci.id[2]

Abstract

Of all the high schools in the city of Semarang, there is one high school which is the best high school in this city, namely SMA Negeri 3 Semarang. However, this high school is still trying to advance the skills and knowledge of students and teachers, namely by collaborating with other agencies by holding training in the field of information technology whose contents include crack, hack, social media, innovative industry, data mining, and others. This collaboration is held with the aim that the high school can be on par with other best high schools in facing the development of world information technology which is growing rapidly. One way to deal with global technological developments is to require training, counseling, and simulations. In this training, crack vs hack is knowledge that needs to be taught to students so that there is a significant increase in competence. Cracking is destruction that is done and harms others. While hacking, although it can also damage and manipulate data, it is done without harming other people. The service activity begins with interviews and surveys at SMA Negeri 3 Semarang, then determines the material to be delivered, followed by training and simulation activities as well as activity evaluation. The result of this community service is that teachers and students will understand crack vs hack and the materials presented have been selected in such a way that they are in accordance with the needs of SMA Negeri 3 Semarang.

***Keywords**: Crack, Hack, Simulation, Case Study, Implementation.*

Abstrak

Dari seluruh SMA yang ada di Kota Semarang, ada salah satu SMA yang merupakan SMA terbaik di kota ini, yaitu SMA Negeri 3 Semarang. Namun demikian SMA ini tetap berusaha memajukan keterampilan dan pengetahuan siswa dan guru, yaitu dengan cara berkolaborasi dengan instansi lain dengan mengadakan pelatihan dibidang teknologi informasi yang isi materinya meliputi crack, hack, sosial media, industri inovatif, data mining, dan yang lainnya. Kolaborasi ini diadakan dengan tujuan agar SMA tersebut dapat sejajar dengan SMA terbaik lainnya dalam menyongsong perkembangan teknologi informasi dunia yang semakin pesat perkembangannya. Salah satu cara untuk menghadapi perkembangan teknologi global adalah diperlukan pelatihan, penyuluhan, dan simulasi. Pada pelatihan ini, crack vs hack merupakan pengetahuan yang perlu diajarkan kepada siswa agar terjadi peningkatan kompetensi secara signifikan. Cracking adalah perusakan yang dilakukan dan merugikan orang lain. Sedangkan hacking, meski juga bisa merusak dan memanipulasi data, tapi dilakukan tanpa merugikan orang lain. Kegiatan pengabdian diawali dengan wawancara dan survei di SMA Negeri 3 Semarang, kemudian menentukan materi yang akan disampaikan, dilanjutkan kegiatan pelatihan dan simulasi serta evaluasi kegiatan. Hasil dari pengabdian masyarakat ini adalah guru dan siswa akan memahami crack vs hack dan materi-materi yang dihadirkan sudah dipilih sedemikan rupa sehingga sesuai dengan kebutuhan dari SMA Negeri 3 Semarang.

***Kata kunci:** Crack, Hack, Simulasi, Studi kasus, Implementasi*

10.20473/jlm.v6i2.2022.385-394

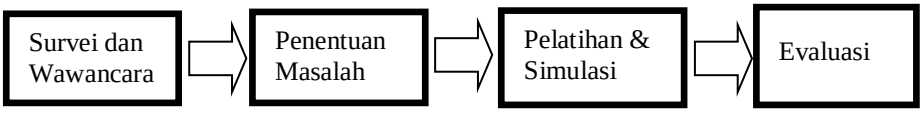
PENDAHULUAN

Dari seluruh SMA yang ada di Kota Semarang, ada salah satu SMA yang merupakan SMA terbaik di kota ini, yaitu SMA Negeri 3 Semarang. Namun demikian SMA Negeri 3 Semarang tetap berusaha memajukan keterampilan dan pengetahuan siswa/i dan guru-gurunya, yaitu dengan cara berkolaborasi dengan instansi lain dengan mengadakan pelatihan dibidang teknologi informasi yang isi dari materi tersebut meliputi *crack, hack* sosial media, industri inovatif, *data mining*, dan yang lainnya. Kolaborasi ini diadakan dengan tujuan agar SMA Negeri 3 Semarang dapat sejajar dengan SMA terbaik lainnya dalam menyongsong perkembangan teknologi informasi dunia yang semakin pesat perkembangannya. Topik yang sangat diperlukan dalam hal peningkatan kemampuan sumber daya manusia berbasis *information technology*, antara lain: (1) Pemahaman tentang dasar-dasar *crack* vs *hack* dan dampaknya bagi kehidupan kita dan orang lain. Pada bagian ini siswa/i dan guru akan mampu memahami apa yang harus dipahami dan diketahui tentang *crack* vs *hack* secara mendalam; (2) *Crack vs hack*, pada bagian ini siswa/i akan dapat memahami bagaimana *crack* vs *hack* diterapkan dan apa solusinya mengatasi hal tersebut, (3) Pemahaman yang mendalam bagaimana *crack vs hack* dapat diterapkan disertai contoh studi kasus, (4) Bagaimana implementasi *crack* vs *hack* dan bagaimana cara mengatasi kendala-kendala yang ada, (5) Bagaimana *crack* vs *hack* dapat memiliki pengaruh yang signifikan terhadap perkembangan teknologi informasi.

Dari hasil diskusi dengan guru SMA Negeri 3 Semarang di ditemukan permasalahan yang harus di selesaikan SMA Negeri 3 Semarang yaitu dibutuhkannya peningkatan keterampilan dan pengetahuan peserta didik dan pendidiknya dalam menghadapi perkembangan teknologi dunia yang semakin pesat, lebih rinci permasalahannya adalah: SMA Negeri 3 Semarang memerlukan wawasan lebih luas lagi, sebelum peserta didiknya tersebut lulus, dengan memperbanyak pengetahuan-pengetahuan yang lebih dalam di bidang teknologi informasi, terutama dalam bidang *crack, hack,* sosial media, industri inovatif, penggalian data *(data mining)*, bisnis online, menciptakan usaha dan lain sebagainya. Tujuan dari kegiatan pengabdian ini adalah: (1) meningkatkan keterampilan dan pengetahuan siswa/i dan guru dalam bidang *crack* vs *hack*, (2) Pemahaman yang mendalam tentang *crack* vs *hack* dan contoh penerapannya, (3) Mampu mengimplementasikan *crack* vs *hack* ke dalam kehidupan sehari-hari.

METODE PENGABDIAN MASYARAKAT

Metode yang digunakan didalam kegiatan pengabdian masyarakat ini secara umum terdiri dari 4 tahap, yaitu 1) survei dan wawancara, 2) menentukan masalah, 3) pelatihan dan simulasi, dan ke 4) evaluasi. Tahapan tersebut kalau diilustrasikan dalam bentuk gambar dapat dilihat pada gambar 1.



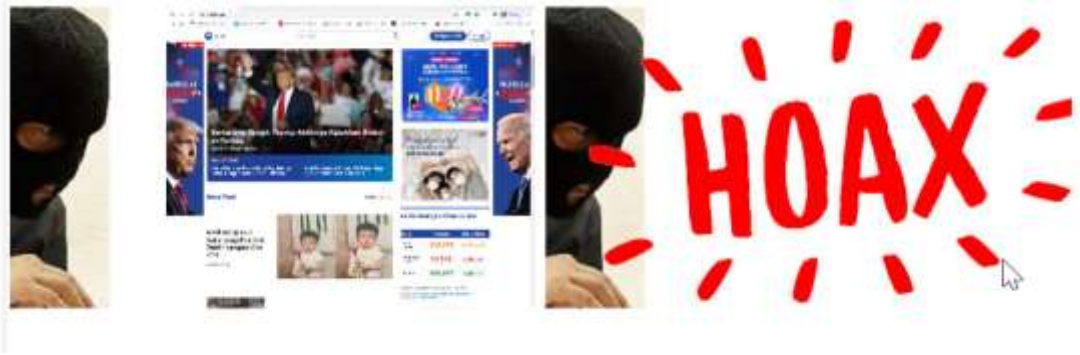
Gambar 1. Tahapan kegiatan pelatihan

Pada gambar 1 dapat dijelaskan bahwa metode pelaksanaan dari kegiatan ini adalah dalam bentuk pelatihan berupa tutorial, yaitu memilih salah satu anggota tim pengabdian untuk menyampaikan tentang materi *hack* vs *crack* secara umum terlebih dahulu, baru kemudian dilanjutkan dengan penjabaran dan penerapannya. Dari 4 tahapan umun diatas secara detail dijelaskan menjadi beberapa tahap. Berikut merupakan tahapan-tahapan yang dilakukan: (1) Melakukan diskusi dengan guru mitra. Diskusi ini dilakukan dengan tujuan untuk menetapkan peserta yang akan mengikuti

kegiatan dan mengevaluasi permasalahan yang lebih rinci lagi, (2) Membuat materi yang akan disampaikan di pelatihan, (3) Menetapkan waktu dan lokasi pelatihan. Jam kegiatan pelatihan disesuaikan dengan waktu kosong peserta dan pemberi materi, (4) Membuat undangan bagi guru dan peserta pelatihan. Undangan berisi pemberitahuan jam pelaksanaan, lokasi dan susunan acara, (5) Menyiagakan alat-alat yang dibutuhkan pada saat pelatihan, antara lain laboratorium komputer, konsumsi, laptop, dan LCD apabila nanti kegiatan dilaksanakan secara *offline*, tetapi jika dilakukan secara *online*, maka akan dipersiapkan link untuk pertemuan baik melalui google meet, zoom, maupun lewat *live* youtube. Hal ini dimaksudkan agar nanti acaranya dapat berlangsung baik dan sukses, (6) Penyediaan waktu khusus untuk bimbingan dan konsultasi apabila ada peserta yang kesulitan didalam mengikuti pelatihan, (7) Mengadakan arsip dan dokumentasi pelatihan, antara lain undangan peserta, surat menyurat, dokumentasi foto, dan daftar hadir, nantinya yang akan digunakan untuk pembuatan laporan, (8) Menyusun laporan kegiatan, guna memberikan uraian kegiatan kepada instansi bahwa pelatihan telah dilaksanakan, (9) Mempersiapkan petugas khusus untuk monitoring, yaitu kegunaannya untuk mengamati kemajuan peserta setelah mengikuti pelatihan. Metode atau cara yang dilakukan oleh tim dalam penyampaian materi adalah sebagai berikut: (1) Menerangkan tentang dasar-dasar *hack* vs *crack*, (2) Memberikan langkah-langkah praktis secara detail dalam memulai aktivitas *hack* maupun *crack*, (3) Membuka sesi tanya jawab untuk menjelaskan lebih detail mengenai kegiatan yang sedang berlangsung agar dapat memperjelas materi.

HASIL DAN PEMBAHASAN

Lokasi pengabdian masyarakat yaitu di SMA Negeri 3 Semarang yang berlokasi di Jl. Pemuda No.149, RT.5/RW.3, Sekayu, Kecamatan Semarang Tengah, Kota Semarang, Jawa Tengah 50132. Kegiatan dimulai dengan penjelasan awal tentang hoax yang disampaikan olah pemateri, seperti pada gambar 2.



Gambar 2. Materi penjelasan tentang hoax

Pada gambar 2 dijelaskan bahwa kegiatan pelatihan dan simulasi diawali dengan penjelasan tentang hoax, sebagai pengetahuan dasar untuk siswa/siswa di SMA Negeri 3 Semarang. Pengetahuan dasar tentang hoax penting untuk disampaikan agar siswa/i mengetahui atau membedakan antara berita yang benar dan yang tidak. Berikut dibawah ini adalah simulasi dan pelatihan yang kami lakukan, antara lain menjelaskan tentang *Crack* vs *Hack* yang disampaikan oleh tutor. Pada gambar 3 dapat dijelaskan bahwa tutor menyampaikan tentang perbedaan antara *hacker* dan *cracker*.

Gambar 3. Pemateri menjelaskan tentang *hacker* dan *cracker*

Gambar 4. Contoh *hacker* Indonesia

Pada gambar 4 ditampilkan dua contoh *hacker* terbaik di Indonesia. Sebenarnya keberadaan *hacker* dapat menjadi ancaman dari pembangun situs internet, akan tetapi disisi lain pada jaman sekarang ini yang serba *cyber*, *hacker* juga dibutuhkan untuk menjadikan teknologi internet semakin maju dan minimal kebocoran, sebab *hacker* dapat menggunakan kemampuan dan keahliannya untuk memperbaiki kelemahan sistem keamanan dalam semuah sistem komputer.

Berita tentang pelanggaran data meningkat dengan cepat, media memberitakan hal tersebut hampir di seluruh dunia. Banyak organisasi, perusahaan dan lainnya yang menjadi sasaran eksploitasi data dan hal ini melonjak dengan drastis pada dekade ini. Resiko tereskposnya data seharusnya menjadi *concern* kita semua untuk meningkatkan kewaspadaan terhadap penggunaan *social media* dan hal-hal yang berhubungan dengan *online* serta data(Jang-jaccard, Julian, 2014; Kott, 2011). Pemahaman mengenai *cybersecurity* dan dasar-dasar tentang *hacker*, *cracker* dan lain sebagainya merupakan hal yang mutlak perlu diketahui dan dipahami secara gambaran besar. Contoh-contoh studi kasus mengenai hal itupun harus kita pahami agar kita dapat meningkatkan kehati-hatian dalam melakukan sesuatu yang bersifat *online*(Alotaibi, 2019). Beberapa hal

yang harus kita pahami adalah: (1) apa itu *hacker* dan motifnya, (2) apa itu *cracker* dan motifnya, (3) dasar-dasar *cybersecurity*. Ketiga hal ini sangat penting dan di sisi lain, studi kasus serta hal-hal yang terjadi mengenai hal tersebut juga harus dipahami. Perbedaan antara memahami dan mengerti adalah, jika mengerti, kita hanya sekilas mendengar dan melihat kemudian secara cepat masuk ke dalam pikiran kita kemudian kita bisa mengingatnya dan juga bisa tidak mengingatnya di kemudian hari, tetapi memahami adalah kita mengerti secara lebih mendalam hal-hal yang perlu kita ketahui secara gambaran besar dan contohnya, hal ini berguna untuk menambah pengetahuan kita serta meningkatkan kemampuan kita dalam mengambil keputusan dengan tepat(Böhme et al., 2019; Rugge, 2018). Dibawah ini dijelaskan lebih jauh tentang *hacker* dan *cracker* yang akan menambah pengetahuan untuk peserta pelatihan.

Apa itu *Hacker*?

Hacker adalah seseorang atau beberapa orang yang melakukan kegiatan pembobolan atau memaksa masuk(Diskominfo, 2018). Istilah ini sering disalahgunakan dalam konteks yang kurang tepat. Dalam istilah yang lebih sederhana, seorang *hacker* adalah seseorang yang menggunakan keterampilan dan pengetahuannya untuk menemukan kerentanan dalam sistem komputer dan membantu meningkatkan dan menambal kerentanan tersebut. Pengetahuan yang mereka miliki tentang pemrograman, berbagai bahasa komputer, kode, dan keamanan komputer umum dikembangkan dan digunakan untuk tujuan yang baik secara moral. Mereka biasanya adalah profesional keamanan yang dapat dipekerjakan oleh organisasi untuk mencoba masuk ke sistem mereka, untuk mengaudit DNS (Domain Name Server) dan jaringan mereka sehingga mereka dapat mengidentifikasi kekurangan yang mungkin mereka miliki. Mereka sering dipekerjakan sebagai bagian dari tim merah dan tim biru. Ketika peretas menemukan kerentanan atau ancaman, mereka mendokumentasikan proses tersebut dan memberi tahu organisasi yang mempekerjakan mereka, atau vendor perangkat lunak yang membangun sistem, sehingga kerentanan dapat diperbaiki sebelum dieksploitasi oleh pelaku jahat. Kita sering melihat istilah *white hat*, atau *ethical hacker*, dikaitkan dengan orang-orang baik yang menggunakan keterampilan mereka untuk tujuan pertahanan(Ghadi et al., 2020; I. Gamayanto, 2020; Sandar et al., 2019).

Motivasi Peretas

Hacker adalah mereka yang membangun dan menciptakan. Mereka belajar dan menemukan berbagai sistem komputer, jaringan, dan sering kali memiliki pengalaman sebelumnya dalam pemrograman yang hanya menambah pengetahuan mereka yang luas. Mereka membangun lingkungan yang aman(Jelen, 2021). Pepatah "kenali penyerang Anda" tidak pernah lebih tepat daripada saat berbicara tentang peretas dan pekerjaan mereka; mereka menggunakan alat, perangkat lunak, dan bahkan teknik yang sama seperti *cracker*. Peretas tahu apa yang dicari penyerang ketika mereka merencanakan serangan, sehingga mereka dapat melindungi mereka secara proaktif. Mereka membangun perangkat lunak dan alat yang bahkan mungkin sama dengan yang digunakan para *cracker*, tetapi mereka menggunakannya untuk meningkatkan keamanan, bukan merusaknya. Pendekatan yang diambil peretas juga mirip dengan yang digunakan para *cracker*, mereka masuk ke sistem dan jaringan untuk menemukan celah dalam keamanan, tetapi motivasi di balik tindakan mereka murni tidak berbahaya dan etis. Mereka bekerja dengan izin dari perusahaan yang memiliki sistem yang mereka coba hancurkan, dan yang selalu diberi tahu tentang hasil akhirnya. Karena peretas, kerentanan dapat ditambal dan ancaman dihindari. Praktik peretas tidak

melibatkan sesuatu yang ilegal dan tidak merusak data apa pun yang berhubungan dengan mereka, mereka memanfaatkan keterampilan mereka untuk keuntungan positif(Kuparinen-koho, 2020; Naumovski & Taneski, 2019).

Apa itu *Cracker*?

Cracker adalah individu atau seseorang yang mencoba untuk masuk ke dalam suatu jaringan komputer(Diskominfo, 2018). Orang-orang ini sering kali jahat, bukan peretas, dan memiliki banyak cara untuk membobol suatu sistem. *Cracker* juga disebut "topi hitam". Mereka mencari pintu belakang dalam program dan sistem, mengeksploitasi pintu belakang itu, dan mencuri informasi pribadi untuk digunakan dengan cara yang jahat. Sementara peretas bekerja untuk membantu organisasi dan individu mengamankan sistem dan jaringan mereka, *cracker* memiliki tujuan yang berbeda. Saat mereka merusak keamanan jaringan, mereka melakukannya secara ilegal tanpa izin pemilik dan mereka melakukannya untuk keuntungan pribadi. Keterampilan dan pengetahuan yang mereka miliki digunakan secara jelas untuk melanggar keamanan dengan niat jahat. Tujuan mereka mungkin untuk mencuri informasi kartu kredit, untuk mendapatkan data pribadi yang dapat dimanfaatkan untuk aktivitas ilegal, untuk mendapatkan data pribadi dan menjualnya, atau hanya untuk menghancurkan data.

Apa yang Memotivasi *Cracker*?

Cracker sering kali didorong oleh keuntungan finansial: sebagian besar akrab dengan serangan *ransomware* di mana *cracker* membobol sistem melalui email *phishing* dan lampiran berbahaya, kemudian memblokir akses ke komputer atau data dan mengancam korban dengan mengekspos data pribadi mereka jika tebusan tidak dibayarkan(Jelen, 2021). Beberapa *cracker* juga akan mencuri informasi kartu kredit, atau informasi pribadi lainnya yang dapat mereka gunakan, untuk mengakses rekening bank korban dan mencuri uang dari mereka. Tentu saja ada motivasi lain yang mendorong para *cracker* melakukan aktivitas ilegal. Ada beberapa kasus di mana *cracker* telah menembus jaringan hanya untuk pamer dan mendapatkan publisitas. Dengan banyaknya media yang meliput pelanggaran, tidak mengherankan jika banyak yang ingin menggunakannya untuk membuat diri mereka "terkenal", terutama karena beberapa jenis kejahatan dunia maya tidak memerlukan keahlian tingkat tinggi. Kita juga bisa menemukan *cracker* yang ingin membobol *software* dengan *reverse engineering*, untuk mengeksploitasi kelemahannya. Dan ada juga sebagian yang melakukannya hanya untuk iseng.

Perbedaan antara *Hacker* dan *Cracker*

Perbedaan etis: *Hacker* adalah orang-orang baik yang membobol jaringan untuk menemukan celah, dan memulihkan keamanan jaringan yang rusak untuk membangun sistem yang aman. Mereka tidak pernah melakukannya secara ilegal dan selalu memberi tahu organisasi perekrutan atau individu tentang tindakan mereka. Mereka adalah senjata ampuh dalam berburu dan menangkap *cracker*. *Cracker*, bagaimanapun, akan membobol sistem yang sama untuk keuntungan pribadi, keuangan atau jenis lainnya tanpa sepengetahuan atau izin dari pemilik sistem, untuk tujuan terlibat dalam aktivitas illegal. Perbedaan keterampilan: *Hacker* memiliki kemampuan untuk membuat program dan perangkat lunak; mereka terampil dalam berbagai kode dan bahasa dan memiliki pengetahuan tingkat lanjut tentang berbagai bahasa komputer pilihan. *Cracker*, di sisi lain, tidak perlu memiliki pengetahuan yang dalam, kecuali tentang cara benar-benar merusak sistem, dan biasanya tidak melihat mereka cukup terampil untuk membuat program mereka sendiri. Bahkan dengan begitu sedikit *cracker* yang cukup terampil

untuk membuat alat dan perangkat lunak untuk membantu mereka mengeksploitasi kelemahan yang mereka temukan, kita tidak boleh mengabaikan ancaman mereka(Newhouse et al., 2017).

Empat Keamanan Cyber Pribadi

"Empat Dasar Keamanan Siber Pribadi" adalah pendekatan yang relevan untuk individu, namun dapat juga diterapkan langsung kepada karyawan di tempat kerja yaitu untuk: **1) Lindungi perangkat**. Ponsel cerdas, laptop, tablet, dan tentang apa pun yang terhubung secara *online* harus dilindungi menggunakan solusi perlindungan perangkat yang canggih. Untungnya, inovasi terbaru telah menghadirkan sistem perlindungan berkualitas tinggi dan efektif yang dulunya hanya tersedia untuk jaringan besar yang berpusat pada server, dan membuatnya tersedia untuk individu dan perangkat mereka agar berfungsi dengan aman di semua lingkungan dan melalui jaringan apa pun. Perlindungan perangkat harus menyertakan fitur manajemen jarak jauh yang menghilangkan kebutuhan untuk masukan pengguna atau modifikasi perilaku. **2) Lindungi koneksi**. Setelah masing-masing perangkat terhubung secara *online*, lebih banyak pertahanan diperlukan untuk melindungi informasi yang dikirimkan melalui internet. Selain perlindungan perangkat, setiap perangkat harus memiliki VPN (virtual private network), atau jaringan pribadi maya, untuk enkripsi otomatis lalu lintas internet. VPN yang baik akan melindungi identitas pengguna, lokasi, penjelajahan, belanja, perbankan, dan semua informasi yang ditransaksikan secara *online,* termasuk melalui jaringan WiFi publik. Layanan VPN tingkat konsumen atau "eceran" sampai saat ini sangat kaku untuk digunakan dan tidak dapat diprediksi dalam pengoperasiannya. Inovasi terkini dan model distribusi baru memberikan kinerja dan pengalaman yang jauh lebih baik, dan peningkatan tersebut diharapkan terus meningkat dalam waktu dekat(Brown, 2012). **3). Lindungi komunikasi email**. Dalam banyak kasus, email adalah "pintu gudang" untuk informasi pribadi. Gunakan layanan yang secara otomatis menghapus lokasi IP (Internet Protocol) dan informasi metadata dari email individu saat mereka menjelajah internet. Gunakan layanan yang menggunakan perangkat lunak sumber terbuka untuk keamanan tertinggi, portabilitas, dan kompatibilitas di seluruh arsitektur dan *platform* teknologi. Akun email pribadi dapat berfungsi sebagai domain digital multi-generasi untuk penggunanya, dan menyediakan ruang keamanan dunia maya selama beberapa dekade mendatang. **4) Lindungi dan cadangkan dokumen dan file elektronik**. Layanan pencadangan jarak jauh itu mudah dan murah, dan kenyamanan *cloud* sangat bagus, tetapi dokumen penting layak mendapatkan brankas digital. Dokumen penting termasuk *scan* paspor, kartu jaminan sosial, akta kelahiran, surat wasiat, perwalian, pengembalian pajak, dan dokumen lain yang merupakan inti kehidupan pribadi kita. Brankas digital mudah digunakan tetapi sangat aman berfungsi sebagai brankas untuk dokumen sensitif. Semua solusi ini sangat terjangkau, tidak mengganggu privasi siapapun, dan akan memberikan ROI (*Return on Investment*) yang membayar dengan mengurangi risiko dan meningkatkan produktivitas selama bertahun-tahun yang akan datang. Selain itu, pendekatan strategi keamanan siber ini memposisikan perusahaan untuk mendapatkan manfaat optimal dari percepatan inovasi yang mengganggu dalam industri keamanan TI(Medovarschi, 2018).

Evaluasi

Dari hasil kegiatan pelatihan ini, untuk mengukur tingkat keberhasilan pelatihan dapat dilihat dari antusias seluruh peserta dalam mengikuti pelatihan. Pada saat kegiatan berlangsung ada beberapa peserta yang mengajukan pertanyaan baik terkait dengan *hacker* dan *cracker*. Dari pertanyaan tersebut pemateri dapat memberi jawaban yang

memuaskan bagi peserta yang bertanya. Disamping antusias didalam bertanya, sebaliknya pemateri juga memberikan beberapa pertanyaan kepada peserta dengan maksud untuk megetahui sejauh mana materi dapat di mengerti oleh peserta. Dari beberapa pertanyaan yang diberikan, peserta juga dapat menjawab pertanyaan dengan baik dan benar sesuai yang diharapkan pemateri. Untuk mengetahui indikator tingkat kepuasan tingkat peserta dapat dilihat dari hasil qusioner yang teringkas didalam tabel 1, dan hasilnya terdapat pada tabel 2.

Tabel 1. Indikator tingkat kepuasan siswa dalam pengabdian ini

No	Pertanyaan	1	2	3	4	5
1	Apakah anda memahami dasar-dasar *cracker* dan *hacker* secara baik?					
2	Apakah contoh-contoh yang diberikan dapat membantu anda dalam memahami cara kerja *cracker* dan *hacker*?					
3	Apakah studi kasus yang dijelaskan dapat memotivasi anda untuk dapat mengembangkan diri dalam bidang komputer?					
4	Apakah pelatihan ini dapat membantu anda mengembangkan pengetahuan dalam teknologi informasi?					
5	Apakah pelatihan ini akan dapat berdampak pada masa depan anda?					

Catatan:

1: Sangat tidak memahami

2: Tidak memahami, penjelaskan dirasa kurang menjelaskan dan hanya konteks tetapi secara mendalam belum mencapai hal tersebut

3: Ragu-ragu dalam menjawab, hal ini dikarenakan masih banyak hal yang harus dipahami mengenai *cracker* dan *hacker*

4: Cukup dapat memahami, tetapi ada beberapa contoh dan studi kasus yang mungkin dapat dijelaskan lebih mendetails agar kami dapat memahami lebih mendalam mengenai dunia *cracker* dan *hacker*. Pelatihan iini memberikan dampak yang positif kepada kami, sehingga kami ingin melanjutkan karier di bidang teknologi informasi

5: Ya, kami sangat memahami setelah mengikuti pelatihan ini, dimana contoh dan studi kasus yang diberikan dapat membantu kami dalam memahami secara mendalam mengenai *cracker* dan *hacker*. Pelatihan ini juga memiliki dampak bagi masa depan kami untuk dapat mengembangkan diri dalam teknologi informasi dan di sini kami dapat mengetahui serta memahami lebih jauh bahwa dunia *cracker* dan *hacker* sangatlah luas dan layak untuk didalami.

Indikator ini dibagikan kepada 100 siswa yang mengikuti pelatihan ini, dan hasilnya adalah sebagai berikut:

Tabel 2. Hasil indikator

Q	1	2	3	4	5	Hasil
1	5	5	10	40	40	100

2	2	1	18	9	70	100
3	1	1	12	6	80	100
4	0	0	20	47	33	100
5	0	0	1	34	65	100

Pada tabel 2, dijelaskan, hasil dari indikator tingkat kepuasan siswa dalam mengikuti pengabdian ini.

PENUTUP

Kegiatan pelatihan dan pengabdian masyarakat di SMA Negeri 3 Semarang sudah berjalan dengan baik. Dilihat dari hasil indikator pada tabel 2, dapat di jelaskan bahwa setelah mengikuti pelatihan dan simulasi, pemahaman peserta tentang materi yang disampaikan sangat meningkat. Dari kegiatan tersebut dapat diambil tiga kesimpulan adalah sebagai berikut: 1) Meningkatkan kemampuan dan pemahaman siswa/i dan guru dalam bidang *crack* vs *hack* dan bagaimana menjadi seorang *crack* vs *hack*. 2) Mampu mengimplementasikan *crack* vs *hack* dalam kehidupan sehari-hari. 3) Mampu mengimplementasikan *crack* vs *hack* pada bidang TI.

Kegiatan pengabdian kepada masyarakat ini akan dilakukan secara *continue*, artinya ini adalah pengabdian masyarakat dalam jangka panjang, dimana pelatihan-pelatihan akan terus dilakukan guna meningkatkan kompetensi khususnya di bidang teknologi informasi di SMA Negeri 3 Semarang.

UCAPAN TERIMA KASIH

Kami berterima kasih kepada SMA Negeri Kota 3 Semarang yang telah memberikan kesempatan dan kerjasama dalam hal meningkatkan kreativitas dalam rangka menghadapi persaingan di tingkat globalisasi pada saat ini.

DAFTAR PUSTAKA

Alotaibi, F. F. G. (2019). *Evaluation and Enhancement of Public Cyber Security Awareness*.

Böhme, R., Laube, S., & Riek, M. (2019). A Fundamental Approach to Cyber Risk Analysis. *Variance. Advancing the Science of Risk*, *12*(2), 161–185.

Brown, N. W. (2012). *Cybersecurity Foundations : An Interdisciplinary Introduction*. *000*.

Diskominfo. (2018). *Hacker adalah seseorang atau beberapa orang yang melakukan aktifitas hacking (pembobolan / memaksa masuk)*. Https://Diskominfo.Badungkab.Go.Id/Artikel/18221-Perbedaan-Hacker-Dengan-Cracker. https://diskominfo.badungkab.go.id/artikel/18221-perbedaan-hacker-dengan-cracker

Ghadi, M., Sali, Á., Szalay, Z., & Török, Á. (2020). A new methodology for analyzing vehicle network topologies for critical hacking. *Journal of Ambient Intelligence and Humanized Computing*, *2010*. https://doi.org/10.1007/s12652-020-02522-w

I. Gamayanto, F. A. and S. N. (2020). Guidelines of Influencer Intelligence: Positive &

Negative Impact of Influencer to Community. *2020 International Conference on Decision Aid Sciences and Application (DASA)*, 90–94. https://doi.org/10.1109/DASA51403.2020.9317236

Jang-jaccard, Julian, S. N. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Jelen, S. (2021). *Hacker vs Cracker: Main Differences Explained*. SECURITYTRAILS BLOG. https://securitytrails.com/blog/hacker-vs-cracker

Kott, A. (2011). *Science of Cyber Security as a System of Models and Problems*. *Lemnios 2011*.

Kuparinen-koho, T. (2020). *RISKS IN USER INTERACTION OF ALARM FUNCTIONALITY*.

Medovarschi, D. M. (2018). *HACKERS : CYBERCRIMINALS OR NOT ?*

Naumovski, T., & Taneski, N. (2019). Social engineering in the context of cyber security. *... The Great Power Influence on the ...*. http://eprints.ugd.edu.mk/22241/

Newhouse, W., Scribner, B., & Witte, G. (2017). *Cybersecurity Workforce Framework National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*.

Rugge, F. (2018). *" MIND HACKING " : INFORMATION WARFARE IN THE CYBER AGE*. *319*, 1–8.

Sandar, A. M., Min, Y., Myat, K., & Win, N. (2019). Fundamental Areas of Cyber Security on Latest Technology. *International Journal of Trend in Scientific Research and Development (IJTSRD)*, *3*(5), 3–5.