

SEC²Story

presented by NGESEC





Daftar Isi

Kata Pengantar	4
Tentang Kami Komunitas NGESEC	5
Aan	
Belajar Secara Otodidak Meraih Mimpi Besar	7
Eryk	
Semangat Menulis, Semangat Berbagi	11
Deutan	
More Silent to Listen More	18
Dirga	
Komputer adalah Kehidupan	22
Eko	
Parallel Hands On	26
– Trust dan Pengendalian di Dunia Internet	31
Edo Maland	
Learning is Everywhere and Anytime	35
Febrian	
Kata si Bocah IT, Prinsip Belajar Komputer “Membangun Logika dan Learning by Doing”	58
Galuh	
Perjalanan Mendalami IT Security	68
Loader	
“Keep learn and share”	74

Pataka	79
Berpetualang dan Berprofesi di Dunia IT Security	
Priyadi	86
Pengalaman di Bidang Security	
Rootbakar	91
'Newbie' Bug Bounty Hunter	
Rungga	111
Mac Gyver, Inspirasi Mengenal Komputer Lebih Dalam	
– Strategi Keamanan Informasi di Organisasi Anda	116
Shulkhan	127
Terus Belajar, Bergaul Dan Bertukar Ilmu NGESEC	
Y3dips	133
More U feel Stupid. More clever U're Now	
– Penetration Testing is Dead?	137
Yuga	149
Anda Menguasai dan Mengenalnya Dengan Baik, Komputer Mempermudah Pekerjaan Anda	
Zet	157
Keterbatasan Tidak Membuatmu Lemah, <i>Keep Fight!</i>	

Presented by NGESEC

Penanggung Jawab: **NGESEC**

Tukang Ramu Buku : **Shinta K Sari**

Bagian Ngecek Editan : **Handoko**

Juru Kompor: **M. Prasodjo**

Yang nge-Desain : **Agus Roch Cahyono**

(cahyono.agus61@gmail.com, mobile: +62 812-9917-381

Juru Tagih Tulisan : **Rony Lantip**

Tukang Poto : Tangtungan Project, Shinta, Pras, Ngesec, dracos dan
koleksi pribadi penulis

Kata Pengantar

Assalamu'alaikum Warahmatullahi Wabarakatuh,
Salam Damai Sejahtera untuk kita semua,
Om Swastiastu,
Namo Buddhaya,
Salam kebajikan.

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 Sec Story 2 yang merupakan kependekan dari Security Story 2.

Buku ini adalah buku kedua Sec Story (Security Story) yang berisi kumpulan donasi cerita. Ditulis oleh 17 donatur pemangku kepentingan keamanan siber (praktisi, dosen, pembicara, pembuat kebijakan, penegak hukum, penggiat komunitas, dan pengusaha) di Indonesia. Sebuah buku yang merupakan hasil karya dan kolaborasi komunitas keamanan siber dalam rangka menyambut Hari Buku Nasional pada tanggal 17 Mei 2019. Seperti buku pertama, buku ini bebas dibagikan dan diunduh secara gratis.

Selama proses penyusunan, kami mendapatkan banyak bantuan, dorongan, serta dan masukan dari teman-teman komunitas, tanpa ada imbalan sedikitpun. Untuk itu 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 dan bermanfaat bagi yang membacanya. Akhir kata: Selamat Merayakan Hari Buku Nasional 17 Mei 2019.

Wassalamu'alaikum warahmatullahi wabarakatuh.
Om Shanti Shanti Om,
Namo Buddhaya.

Tim Editor

TENTANG KAMI KOMUNITAS NGESEC

**Jogja Jogja tetap istimewa
Istimewa negerinya istimewa orangnya
Jogja Jogja tetap istimewa
Jogja istimewa untuk Indonesia
(Lagu Jogja Istimewa - Jogja Hip Hop Foundation)**

Itulah lagu tentang Yogyakarta yang menggambarkan keistimewaan kota ini. Yogyakarta dikenal sebagai kota pelajar, dimana setiap tahun ribuan pelajar/mahasiswa datang dan pergi. Bagi mereka, Yogyakarta adalah rumah singgah sementara. Menyadari sepenuhnya hal ini, kami berusaha untuk menjadi komunitas yang cair, komunitas persinggahan sementara yang istimewa. Sebuah tempat dimana mereka mendapat sesuatu untuk diri mereka dan untuk kehidupan yang lebih luas. Tempat dimana kami bisa saling belajar dan berbagi ilmu pengetahuan terutama tentang dunia computer dan Cyber. Kami, sekelompok orang yang memiliki minat yang sama berkumpul dan mengembangkan diri, membentuk sebuah komunitas yang kami beri nama NGESEC. Atau Nge-Rumpi SECurity.

Dengan latar belakang yang sederhana, kami berkumpul dengan beberapa tujuan dan harapan. Kami berharap NGESEC dapat:

- Menjadi wadah diskusi dan silaturahmi seputar keamanan Cyber,
- Mendampingi pelajar/mahasiswa menyelesaikan studi terkait keamanan Cyber

Dalam berkomunitas, NGESEC memiliki 3 nilai utama yang kami pegang teguh yaitu:

- NgeLab : Semua kegiatan dilakukan dalam ekosistem yang legal
- NgeRumpi : model komunikasi yang digunakan adalah diskusi
- Ngangkring: NgeLab dan NgeRumpi dilakukan dengan suasana yang ringan dan santai seperti di angkringan.

Sejak 5 April 2017, komunitas NGESEC (Nge-Lab & Nge-Rumpi SECurity) memegang komitmen untuk berkumpul seminggu sekali, setiap hari rabu pukul 19:00 WIB di Kelas Pagi Yogyakarta Creative Space (<http://s.id/k17>).

URL: <https://ngesec.id>

Aan Wahyu

Belajar Secara Otodidak Meraih Mimpi Besar

Ada sebuah pepatah yang mengatakan “Keterbatasan tak selamanya melahirkan sesuatu yang terbatas, namun terkadang itu yang menjadikan kita menjadi sesuatu.” Pepatah ini baru aku ketahui kemudian hari. Jangan tanya ya pastinya kapan, tapi bukan sejak aku kecil. Namun secara perlahan, pemahaman seperti ini masuk sedikit demi sedikit dalam kepalaiku sejak aku kecil.

Aku, seorang anak kampungan yang tidak mengerti dunia IT dan komputer. Seorang anak kecil yang memiliki pengetahuan terbatas, tapi memiliki mimpi besar. Awal kenal komputer pas sekolah. aku belajar *office* waktu itu. Keren ya, padahal ngetiknya aja masih 11 jari :P. Keliatan bodoh sih memang, tapi nggak apalah daripada minta bantuan nggak direspon --*hiks sedih akutuh*--.

Dari rasa sedih dan bodoh itu, motivasiku muncul --*ajegile*-- buat nggak pernah bolos pelajaran TIK. Sebentar, TIK singkatannya apa ya..... ah iya, pelajaran Teknologi Informasi dan Komputer, eh bukan Komunikasi. Belajar di rumah? Ya pasti nggak lah. Boro-boro punya komputer, uang jajanku aja cuma bisa buat beli cilok doang hahaha. Semua keadaan ini ternyata justru membuat aku mau terus belajar dan terus, otodidak dan otodidak. Ngerasa ketinggalan jauh, ngerasa nggak bisa apa-apa jadi mesti lari terus. Itulah pemikiranku. Tanpa kusadari, aku ternyata sudah tidak lagi mengetik 11 jari. Ternyata aku tidak hanya belajar *office* lagi. Mulai deh aku belajar yang

lain yang aku temui. Saat itu sekolahku masih pakai Freezy system yang menjengkelkan. Nah mulai deh penasaran dan kenal LINUX.

Saat kenal LINUX, aku langsung tertarik. Bela-belain install (bukan live cd) ubuntu ke flashdisk biar cuman bisa belajar 'cd, ls, ps aux, dan lain lain. Biar ingat, pake bela belain sampe dicatet di note hahahaha. Sampe akhirnya sekarang sudah punya mesin sendiri yang bisa diinstall ArchLinux yeyyy~

Kalau penasaran terhadap sesuatu, langsung mbah gugel. Otodidak, otodidak dan otodidak. Selebihnya belajar sambil berjalan, maksudnya sesuai dengan yang dibutuhkan ya bukan sambil olahraga :P Itulah cara terbaik belajar komputer, menurutku. Dan itulah yang aku jalani sampai sekarang.

Hal teraneh yang pernah aku ketahui adalah komputer. Dari satu buah komputer itu terlahir banyak hal. Dan komputer bisa melakukan banyak hal. Keren kan. Makanya komputer kemudian menjadi pilihan gidupku. Satu keputusan yang kuakui nggak salah pilih untuk bisa berdiri sampai sekarang :D

Secara sederhananya, aku seorang penyuka Wayang dan penggiat Open Source. Tertarik dengan Research Development dan Non-Profit Organization yang bersifat Open Source. Tertarik dengan hal yang berkaitan OSINT, Reverse Engineering, Exploit Development dan Security. Sedangkan bidang ilmu komputer yang paling kusukai Software Development, Exploit, Reverse engineering. Membuat Automation tools dan tools yang menunjang untuk kerja/kegiatan lain sangat aku suka. Soalnya kadang aku itu pemalas gituh lohh. Aku malas untuk mengulang sesuatu terus-terusan.

Sebagai penggiat open source, aku kadang ditanya apa itu? Menurutku opensource adalah tempat di mana kita bisa belajar dengan bebas dan berkontribusi kembali untuk kemajuan open source tersebut. Ya, tempat belajar dan membangun sesuatu di dunia komputer. Sangat keren dan bermanfaat kan. Makanya aku bercita cita membuka tempat atau wadah belajar bersama di Indonesia. Aku ingin mendirikan organisasi untuk menampung orang-orang belajar, develop, eksperimen di bidang ilmu komputer. Seharusnya pemerintah lebih serius dalam menangani dan memberikan dukungan terhadap perkembangan opensource di Indonesia. Memang si sudah lebih baik, meskipun open source masih dipandang sebelah mata, apalagi pas lagi tender wkwkwkwkwkw

Selain cita-cita besarku itu, aku sih tetep pingin jadi manusia biasa yang punya resolusi tahunan. Seperti orang-orang lah. Mencoba hal baru, menjadi bagian resolusi di suatu tahun kehidupan aku. Saat itu, rasanya aku juga ingin memperdalam apa yang selama ini cuman jadi bahan bacaan tanpa

diberikan kesempatan untuk terjun langsung ke dunia security. Nah, saat ada kesempatan ya *I take it.*

Security adalah sesuatu hal yang seharusnya menjadi bagian dalam setiap pengambilan keputusan dalam hidup ini. Security harus selalu diikutsertakan. Tidak hanya dipakai ketika dibutuhkan saja dan dilupakan saat seolah-olah tidak ada masalah. Dan jangan pernah merasa bahwa kita aman, karena itu adalah saat terlelah dalam hidup kita. Itu terjemahan aku akan security.

Sesuai dengan moto kesukaan aku yang membuka tulisan ini, belajar dan belajar, otodidak dan otodidak. Saat pertama kali berkenalan dengan dunia security, aku benar-benar baru. Dasar pengetahuanku adalah developer. Aku bukan praktisi security saat itu. Aku menemukan sebuah hal yang menarik yang menuntutku untuk terjun bebas. Pilihannya kan antara hidup atau mati, kalau terjun bebas. Namun aku memutuskan untuk berani ambil resiko dengan hanya berbekal otodidak. Kembali lagi, aku mengambil sebuah keputusan yang tepat menurutku. Ilmunya dapat, bisa buat mencari hidup dan jadi kenal banyak orang-orang hebat yang dulu sempet diidolakan. Sekarang ternyata lingkaran kita bisa jadi sama. Nah loh. Tapi bukan tokoh tokoh yang aku kagumi karena pemikiran-pemikiran yang cemerlang :D seperti Oscar Wilde, Socrates, Confucius, Carl C Jung dan sebagainya ya. Aku terus belajar dan akhirnya bisa bergabung ke komunitas-komunitas IT dan security di Indonesia. Komunitas komunitas IT di Indonesia yang terus berkembang dan terus melahirkan orang-orang baru yang berbakat. Aku harap *No more kiddos, no more you-know-who generation*, di dunia security Indonesia. Oh iya semakin banyak conference lokal dong~. Biar aku dan teman teman makin bisa terus berkembang dan menjadi bagian dari dunia security tingkat dunia. Ngimpi sih bisa ngomong di conference global, tapi nggak apa-apalah. Semoga ada kesempatan :P

Profil:

1. Nama : Aan Wahyu
2. Panggilan sehari hari : Aan
3. Handle/nick : petruknisme
4. Tempat/Tanggal lahir : Lupa, adanya di KTP :P
5. Alamat : Jakarta
6. Handle origin : petruk-n-isme (<https://petruknisme.com/tentang/>)
7. Mobile :
 - Telegram : @petruknisme
 - Lain lain : <https://medium.com/@petruknisme>
 - Urls : <https://petruknisme.com>
8. Sosial Media : twitter.com/petruknisme
9. Komputers spec :
 - Pertama : Komputer warnet pentium 3 sama komputer sekolah pentium 4 CRT wkwkw
 - Sekarang : Masih barang rongsok yang bisa dipake kerjalah (Dell Latitude)
 - Yang diidamkan : Dell Latitude/Thinkpad Military Grade
10. Member of :
 - Community : di manapun aku berada, tetap remahan mie instan :(
 - Projects : github.com/aancw
11. What I like to do? : Seeing others when they can't see me.
12. What I dislike : Distracted and too much talking a sh*t
13. Favorite / Kesukaan :
 - Makanan/Foods : apa ya, banyak si :P
 - Minuman/Drinks : Susu Jahe Merah sama Wedang Ronde
 - Warna/Colours : Biru
 - Jenis/genre Music : Classic Instrumental s/d Metal
 - Band / penyanyi : Foo Fighter, Offspring, Cranberries,
 - Movies/TV : A Beautiful Mind
 - Books & Authors : Anak Bajang Menggiring Angin, Cantik itu Luka, Retorika
 - Place : Nowhere
 - Time : When
 - OS : ArchLinux -- Karena ditanya akutuh, kalau ga ditanya juga ga bakal ngasih tau. suka dibully :--
 - Software : Telegram, karena di sana aku bisa nge-junk sepantasnya hahaha
 - Bahasa programing : Python & C/C++



Eryk



Semangat Menulis, Semangat Berbagi

Saya adalah insan yang terlahir di bumi Indonesia untuk kelak menjadi pemimpin bangsa, melalui segala hal yang bisa saya kontribusikan selama hidup. Sejak sekolah dulu, saya mengidolakan Bill Gates. Seorang engineer yang juga pengusaha sukses dan filantropi. Banyak duit, banyak beramal (Semoga kelak saya bisa sesukses dia juga.) Terlahir dari keluarga yang biasa, dengan segala keterbatasan yang ada, saya berusaha mengembangkan diri semaksimal mungkin dan memanfaatkan segala peluang/kesempatan yang ada untuk kebaikan banyak pihak, baik untuk saya sendiri, keluarga, rekan-rekan, komunitas, dan semua orang yang saya kenal.

Saya menghabiskan masa sekolah di Surabaya. Di sana, adopsi pelajaran IT cukup baik. Sejak SD kelas 3, siswa sudah dikenalkan dengan komputer. Saat itu pelajaran yang diberikan lebih banyak tentang penggunaan DOS (padahal sudah ada Windows 95). Saat SMP pun saya masih belajar menggunakan Wordstar, meskipun sudah ada MS Word.

Saat SD, nilai saya yang paling rendah adalah pelajaran komputer. Dapat nilai E pun pernah. Hambatan saat itu adalah saya hanya belajar di sekolah, karena tidak punya komputer di rumah. Menjelang kelulusan SD, baru ada komputer di rumah sehingga dari situ saya bisa banyak ngoprek software-software. Saya masih ingat saat SD dulu sempat coba-coba Microsoft FoxPro. Dari sinilah saya menyimpulkan bahwa belajar komputer itu harus

menyempatkan diri untuk membaca dan ngoprek. Dengan membaca minimal kita paham teorinya, dengan ngoprek, minimal kita paham *implementasinya*.

Dari semula yang tidak seberapa suka pelajaran komputer karena selalu dapat nilai jelek (saat SD), hingga akhirnya memiliki *passion* yang tinggi khususnya di bidang IT security. Bagi saya saat ini, komputer sudah merupakan sumber inspirasi dan media dalam menghasilkan karya-karya yang dapat saya kontribusikan untuk masyarakat. Dengan komputer, Alhamdulillah dapat membantu meningkatkan rejeki dan taraf hidup keluarga dan memudahkan saya dalam menyebarkan kebaikan, khususnya dalam bentuk tulisan.

Kalau ditanya tentang *security* yang menjadi *passion* saya sekarang, jawabannya adalah sebuah proses, bukan hasil akhir atau target yang harus kita capai di ujung. *Security* tidak akan ada ujungnya karena tidak ada 100% sistem yang aman. *Security* juga tidak hanya berbicara perihal teknologi, namun juga orang dan proses. Seperti kata pepatah: "*Human is the weakest link in cybersecurity*". *Security* juga lebih berbicara perihal "*how to protect the crown jewels*" alias bagaimana melindungi aset terpenting kita. Namun, dengan semakin berkembangnya *threat* yang ada, *security* tidak cukup hanya "*protecting the crown jewels*". Penjaga (*defender*) butuh banyak cara untuk melindungi banyak titik akses ke aset mereka, namun penyerang (*attacker*) kadang hanya butuh satu titik/celah untuk mendapatkan akses ke aset yang ditarget. Dunia IT khususnya *Security* itu perkembangannya cukup pesat. Banyak sekali yang harus dipelajari. Hal inilah yang membuat saya memiliki *passion* di bidang tersebut.

Saya mulai belajar *security* sejak SMP. Saat saya SMA, ekstrakurikuler robotika yang saya ikuti sempat mengadakan seminar tentang IT dan Robotika untuk siswa SMP. Saat itu saya menjadi narasumber untuk topik pengenalan dasar keamanan informasi. Itulah pengalaman saya memberikan *public speaking*. Saat kuliah, saya sempat memberikan *sharing session* namun tidak hanya tentang IT Security. Saat itu selain tentang IT Security & networking, saya juga tertarik belajar tentang *Big Data* dan *IT Governance & Management*. Saat sudah kerja, Alhamdulillah saya diberikan kesempatan untuk sharing session dalam beberapa *event/meetup*.

Saya mengawali karier formal sebagai pentester di salah satu *global consulting firm*. Jika saat awal-awal belajar ngoprek di IT Security itu saya jalankan dengan tanpa arah, saat pertama kali bekerja secara formal, saya belajar bagaimana melakukan pentest yang professional. Hal yang harus diperhatikan adalah pentester selain membutuhkan skill untuk aktivitas

pentest itu sendiri, juga butuh *skill* dalam hal *reporting* dan *presentation*. Hal ini yang saya pelajari selama mengerjakan project pentest secara formal. At the end, klien kita pasti berharap laporan yang kita hasilkan dapat dipahami.

Dunia hacking saya kenal saat SMP. Hacker menurut saya adalah *innovator* dalam dunia IT. Tanpa hacker, perkembangan dan peningkatan kemampuan IT tidak berkembang dengan pesat juga. Saat awal-awal masuk SMP, bahkan saya sendiri baru menggunakan Google, setelah diperkenalkan oleh teman saya yang hobinya main game online. Saya hobi membeli dan membaca buku. Justru hal inilah yang memperkenalan saya dengan ilmu hacking. Saat itu saya menemukan buku "Seni Internet Hacking" yang ditulis oleh Sto (Jasakom). Sejak saat itulah saya membeli buku-buku yang diterbitkan Jasakom dan mencobanya langsung di warnet dan sekolah. Saat itu banyak sekali website lokal yang *vulnerable*. Bahkan dengan modal Google Dork saja, saya dapat mengakses *database target*. Kegiatan semacam *defacing* dan *carding* pun juga tidak terhindarkan.

Dari aktivitas-aktivitas yang merugikan tersebut saya jadi berpikir, harusnya saya bisa memberikan manfaat dengan ilmu yang saya pelajari. Untuk itulah, saat SMA, saya lebih banyak berfokus pada dunia pervirusan dan pemrograman web dengan PHP. Di sekolah saya, pemrograman web dengan PHP dan database (MySQL) sudah dikenalkan. Saat SMA saya sempat belajar tentang pembuatan virus dan antivirus. Dari belajar membuat virus, saya jadi memiliki banyak ide iseng yang dapat saya terapkan ke teman-teman saya saat itu. Manfaat yang benar-benar saya rasakan adalah saat membuat antivirus. Antivirus yang saya kembangkan sempat digunakan untuk semacam kompetisi inovasi di sebuah perusahaan. Alhamdulillah menjadi pemenang dan dapat duit. Tapi yang membuat saya bangga, antivirus saya waktu itu digunakan di kantor-kantor cabang.

Saat kuliah, pengetahuan dan pengalaman di bidang IT security yang saya dapat semakin luas. Dibekali dengan mata kuliah yang berhubungan dengan programming (Java, C++, .NET), networking (mengacu ke kurikulum CCNA), dan juga IT Security (mengacu ke kurikulum CEH). Mengingat di Jakarta banyak kegiatan yang gratis, selain mengembangkan ilmu dan skill teknis, saya juga berusaha meningkatkan relasi dengan hadir dalam berbagai macam kegiatan IT dan komunitas. Tidak bisa dipungkiri bahwa menguasai hal teknis saja tidak cukup. Banyak hal-hal non-teknis yang perlu kita perhatikan karena justru faktor keberhasilan karier kita menurut saya lebih didominasi oleh hal-hal non-teknis tersebut.

Ketika lulus kuliah dan memulai karier sebagai praktisi IT Security, awal-awal dan sampai sekarang, saya banyak terlibat dalam proyek terkait dengan penetration testing dan *configuration review*. Target dari penetration testing cukup beragam yang mencakup aplikasi berbasis web, aplikasi berbasis mobile (Android & IOS), infrastruktur (mencakup host/server dan perangkat jaringan), dan wifi. Selain *assessment* yang bersifat teknis, saya juga mendapatkan pengalaman dalam proyek keamanan informasi yang bersifat non-teknis, misalnya penyusunan strategi IT security. Tidak dapat dipungkiri bahwa mengelola dan meningkatkan kapabilitas IT Security sama dengan IT pada umumnya. Perlu adanya perencanaan, identifikasi kebutuhan, pemantauan, dan peningkatan yang berkelanjutan dimana hal ini dapat dicapai jika perusahaan dapat menyelaraskan aspek *People, Process, and Technology*.

Dalam Pentest Tools Saja Tidak Cukup

Jika berbicara tentang tools, saat sekolah dulu penggunaan tools di Windows dan Linux bisa dibilang seimbang. Tools macam Cain and Abel dan Havij mungkin jadi pegangan wajib bagi script kiddies saat itu. Saya pun dulu juga script kiddies ☹ Namun saat ini saya lebih banyak menggunakan tools di Linux, khususnya yang sudah ada di Kali Linux (dulu Backtrack). Hanya tools semacam Acunetix (web vulnerability scanner) saja yang saya gunakan di windows. Untuk web application pentest, tools wajib yang harus digunakan seperti Burpsuite Pro, OWASP ZAP, dan nikto. Masih banyak tools yang dapat digunakan. Jika ingin praktis, cukup pakai Kali Linux karena disitu sudah banyak *pre-installed tools*.

Penguasaan tools dan teknik dalam melakukan pentest saja tidak cukup. Untuk itulah, saya mulai memberanikan diri untuk aktif di beberapa komunitas IT, khususnya IT Security. Pada beberapa kesempatan, saya menyempatkan diri untuk memberikan sharing session baik saat kopdar/meetup maupun kegiatan yang diadakan oleh lembaga/perusahaan lain. Keterlibatan dalam komunitas ini sangat penting karena dari situ kita dapat mengenal dan menimba ilmu dari rekan-rekan yang lebih berpengalaman. Selain itu komunitas dapat menjadi media untuk memberikan kontribusi kita bagi dunia keamanan informasi di Indonesia.

Alhamdulillah, sampai saat ini saya masih dapat menjaga passion saya untuk mempelajari dan berkontribusi bagi dunia keamanan informasi, minimal melalui tulisan dan sharing session pada acara kopdar/meetup komunitas. Sebagai konsultan IT Security, selain dituntut untuk selalu update

dengan perkembangan IT yang nantinya akan mempengaruhi secara teknis kemampuan yang harus saya latih, juga dapat memberikan security awareness dan menjaga relasi dengan stakeholder terkait IT Security agar saya dan komunitas dapat berkembang bersama dalam memajukan dunia IT Security di Indonesia. Komunitas IT di indonesia itu LUAR BIASA. Banyak sekali komunitas-komunitas iT yang usernya aktif juga, baik melalui media sosial maupun melalui kopdar.

Dunia IT Security sangat luas, sehingga menjaga passion agar selalu haus dalam menuntut dan berbagai ilmu pengetahuan di bidang IT Security ini menjadi sangat penting. Dari sisi SDM, komunitas IT security Indonesia, mungkin jumlahnya masih jauh di bawah SDM di bidang software development. Namun dengan aktifnya komunitas-komunitas IT Security, peningkatan SDM di bidang IT Security semakin terlihat. Banyak juga praktisi IT Security yang dengan senang hati meluangkan waktu untuk diskusi.. Saat ini sumber belajar untuk IT Security dapat diakses dengan mudah (cukup googling). Saya berharap semoga semakin banyak kegiatan di bidang IT Security sehingga dapat meningkatkan awareness dan minat orang-orang dalam mempelajari IT Security. Harapannya, kemajuan dunia IT Security di Indonesia tidak kalah juga dengan negara lain, minimal bisa bersaing dengan negara di ASEAN.

Selain itu ada peran penting dari *open source*. Tanpa adanya *open source*, perkembangan dunia IT tidak akan sepesat saat ini. Selain itu tanpa *open source*, kesempatan belajar menjadi sangat terbatas juga. Sejauh yang saya tahu, secara teori pemerintah khususnya kominfo mendukung gerakan *open source*. Cuma pada praktiknya, di pemerintahan itu sendiri masih tergantung dengan *proprietary software*. Disini perlu pengembangan dari semua pihak bersama sama.

Maju terus untuk dunia IT Security Indonesia !!!
Eryk Budi Pratama (@proferyk)
Konsultan Keamanan Informasi
proferyk@gmail.com



Profil

1. Nama (real name) : Eryk Budi Pratama
2. Panggilan sehari hari : Eryk
3. Handle/nick : proferyk
4. Tempat/Tanggal lahir : Jakarta
5. Alamat : Jakarta
6. Mobile : @proferyk
7. Sosial Media : @proferyk
8. Computers spec :
 - Pertama : Asus
 - Sekarang : Macbook Pro & Asus ROG
 - Yang diidamkan : Macbook Pro
9. Member of :
 - Community : Berbagai komunitas IT Security
 - Projects : Berbagai project di bidang IT Security, mencakup penetration testing, cybersecurity program development, technology implementation, dll. (ada di linkedin saya)
10. What I like to do? : Membaca, menulis, menyanyi, mendengarkan music
11. What I dislike : Menganggur
12. Favorite / Kesukaan :
 - Makanan/Foods : Gado-gado
 - Minuman/Drinks : Air mineral
 - Jenis/genre Music : Pop, nostalgia, & dangdut modern
 - Movies/TV : Die Hard, Olympus has fallen, London has fallen
 - Hobby : Membaca, menulis, menyanyi, mendengarkan music (sedang coba rajin olahraga)
 - OS (kenapa?) : Linux (kali linux & ubuntu) & Windows. Alasan: penggunaan sehari-hari baik untuk pekerjaan kantor maupun saat pentest
 - Software (kenapa?) : Python, R, & PHP
 - Bahasa programing :

Deutan

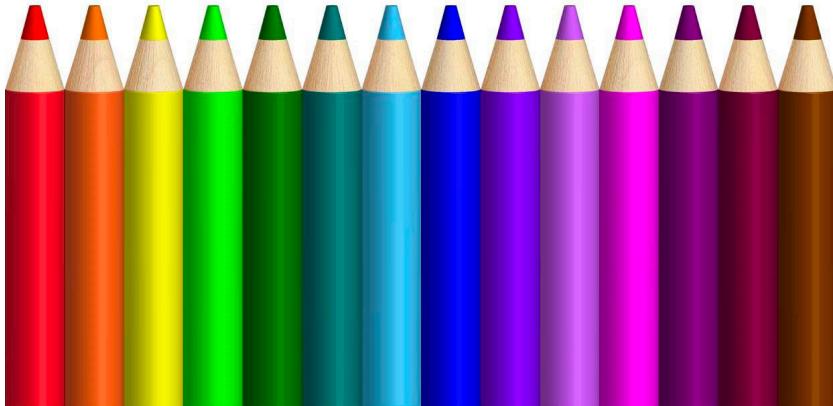


More Silent to Listen More

So just call me Deutan. I am no body, just friend of computer. Oh no, computer even more than a friend for me.

Ya komputer adalah *tool* yang membuat saya menjadi seseorang. Salah satu *tool* menuju cita cita saya menjadi *Chief Information Officer*. Sesuatu yang sangat saya kenal dan menjadi sahabat terbaik. Sejak awal, saya “bergaul” dengan komputer dengan cara *READ – DO IT*. Buka, cari tahu, baca lalu lakukan. Jika kamu sudah menemukan cara mengerti komputer maka kamu akan menjadikannya sahabat terbaik. Saya sendiri nggak pernah bikin aplikasi, *don't code anymore*. Karena saat ini sedang asyik dengan bidang ilmu *Risk Management*. Bicara soal *risk*, saya kira penggunaan *open source* juga merupakan *risk management*. Mengurangi faktor resiko, menghindari api neraka. Sesuatu yang baik kan. Sayangnya dukungan pemerintah terhadap *open source* belum serius. Hal ini terbukti dengan belum banyak RnD yang didukung pemerintah dalam pengembangan *open source*.

Hal yang menarik lainnya adalah *security*. Karena para pelaku *security* ini *cool* banget. Sukses tidak dipuji, gagal dicaci maki, mati tidak dicari. *Security* dan dunia IT itu merupakan barang langka yang belum banyak disadari oleh semua orang, namun banyak dibutuhkan. Dengan *security* saya bisa banyak



membantu orang lain. Dan itu sangat menarik. Sedangkan perkenalan saya dengan *security* yang paling menarik adalah saat saya melakukan *hacking access door*.

What? Arti hacker menurut saya? Pastinya, semua orang yang menggunakan perangkat atau proses yang tidak sesuai dengan panduannya adalah seorang *hacker*. Termasuk dengan penggunaan dan pengetahuan tentang hardware. Seiring dengan perkembangan IoT, menurut saya, *hardware hacking* akan menjadi salah satu yang akan menjadi tren dimasa depan.

Sebagai seseorang yang mempelajari *security* dan IT, tentu saya juga mencari tau tentang komunitas *Security* dan IT di Indonesia. Komunitas IT di negeri ini masih terlalu mengandalkan implementasi. Belum berani menyentuh kepada ide-ide besar. Mereka belum mampu menjabarkan ide besar dalam bentuk narasi yang persuasif. Saat ini, Indonesia memiliki sumber daya manusia yang potensial di bidang *Security* dan IT. Namun sayangnya, sumber daya manusia yang besar tersebut, saat ini terlalu underconfident untuk tampil menjadi seorang *security* profesional. Itulah mengapa, menjaring para pelaku *security* menjadi profesional, adalah harapan personal saya. Dengan demikian, para

profesional ini mampu menjadi profesional handal yang tampil sebagai dirinya sendiri. Bukan sebagai ajang ladang politis. Dengan demikian mereka akan dapat memberikan dampak positif terhadap kehidupan umat manusia yang lebih baik



Profil:

1. Nama : (cukup) Deutan
2. Panggilan sehari hari : Deutan
3. Handle/nick : Deutan
4. Alamat : Jakarta
5. Sosial Media : deutan, the_deutan
6. Computers spec:
 - Pertama : Jetway 7zxan pentium III
 - Sekarang : MacbookPro, HP Elitebook 840 G3
 - Yang diidamkan : Apple Macbook Pro Custom 15" Core i9 2.9 GHz 32GB 1TB SSD Retina
7. Member of:
 - Community : IT Security Audit, CDEF, Pentester ID, TataKelola, DevSecOps, HackTheBox, IHP, AFDI
8. What I like to do? : *couching people*
9. What I dislike : *assLicker* a.k.a penjilat lol
10. Favorite / Kesukaan:
 - Makanan/Foods : Kangkung, tempe dan sambal hantu keeper
 - Minuman/Drinks : Macchiato
 - Warna/Colours : hitam dan abu
 - Jenis/genre Music : cello, jazz
 - Books & Authors : *Ghost in the wires - Kevin Mitnick, The Dancing Wu Li Master - Gary Zukav*
 - Place : *home*
 - Time : *sleep time*
 - Hobby : *gardening*
 - OS : MacOS, karena UNIX based yang klo dicompile dengan benar jadi senjata ampuh
 - Software : PowerPoint, menyalurkan ide melalui sebuah narasi
 - Bahasa programing : *I don't code anymore, but if has to choose, Python will be the answer.*



Dirga

The word "Dirga" is written in a bold, red, sans-serif font. The letter "D" is stylized with a white circular cutout containing a blue gear icon. The letters "i", "r", and "g" are stacked vertically, with "i" being white, "r" being red, and "g" being white. The letter "a" is red and has a small blue gear icon at its bottom right corner.

Komputer adalah Kehidupan

Apakah saya seorang pelupa? Entahlah. Tapi kalau yang namanya komputer, saya nggak akan lupa. Karena memang itu kesukaan dan hobby saya. Komputer adalah bagian dari kehidupan ini. Saya sendiri sebenarnya suka lupa sama orang, makanya saya suka dengan quote "Selama Saya tidak lupa hari ini, Kita akan bisa bertemu lagi. Jangan nanya ya itu quote siapa, karena saya lupa. Yang pasti saya nggak lupa diri lho ya.

Siapa saya? Saya hanya pria biasa, yang ingin menggapai cita-cita. Kehidupan saya tidak jauh dari yang namanya komputer dan pemrograman. Bahasa yang menjadi favorit saya adalah PHP. Tapi bukan PHP ini anu ya...

Sejak awal belajar komputer dan pemograman, modal utamanya adalah tertarik dan rasa penasaran yang tinggi. Dari sanalah saya banyak mendapatkan keilmuan yang sangat bermanfaat dan mengasyikan. Hasilnya saat ini, yahhhh.... adalah beberapa aplikasi kecil untuk membantu keseharian yang saya buat. Aplikasi-aplikasi sederhana namun membantu. Seperti saya bilang tadi kan, komputer dan aplikasi itu bagian dari kehidupan, untuk kehidupan dan harus digunakan untuk kehidupan itu sendiri.

IT Sec Ada Untuk Membantu Kita

Mungkin bagi saya semuanya menarik kalau sudah tentang dunia komputer, karena setiap sudutnya penuh dengan kesan. Kalau ditanya “Apa yang membuat Anda tertarik dengan security, atau dunia IT?” Mungkin akan saya jawab naluri. Saya tidak pernah memperhitungkan prospek, hanya mengikuti alur dan memuaskan rasa penasaran.

Ada satu bidang komputer yang menurut saya sangat menarik. Bisa dibilang kalau bidang inilah yang paling saya sukai saat ini, di dunia komputer. IT Sec pastinya. Kalau menurut Wikipedia sih, IT sec adalah: *Keamanan komputer (bahasa Inggris: computer security) atau dikenal juga dengan sebutan cyber security atau IT security adalah keamanan informasi yang diaplikasikan kepada komputer dan jaringannya. Computer security atau keamanan komputer*



bertujuan membantu user agar dapat mencegah penipuan atau mendeteksi adanya usaha penipuan di sebuah sistem yang berbasis informasi. Informasinya sendiri memiliki arti non fisik. ([Wikipedia.id](#)) Kalau menurut saya pribadi ya seperti di Wikipedia itu hehee. Nah mungkin karena naluri pembantu saya ya, jadi ya suka sama IT Sec. Jadi alasan sukanya sih sepertinya hanya naluri saja. Yang pasti security itu adalah sebuah bahasan menarik di dunia komputer. Tidak ada habisnya kalau kita membahas security. Selalu ada yang baru dan selalu bikin penasaran. Itulah yang membuat saya sangat terkesan dengan dunia security ini. Itu kenapa saya bercita cita untuk menjadi *IT Sec Pro* hehe (Aamiin). Pinginnya sih saya bisa jadi orang yang kerjanya seputaran *attack and defense*. Tapi jangan tanya kayak siapa ya, karena saya belum bisa ngasih tau beliau itu siapa. Ada 1 orang yang saya kagumi, namun belum diberi kesempatan bertemu. Siapa? Ntar aja ya kalau sudah ketemu.

Berbeda dengan keilmuan sekolah, di dunia IT Sec, kita bisa belajar dari siapa saja dan dimana saja. Itulah mengapa saya berusaha untuk selalu membuka “mata” dan “telinga”. Saya banyak mencari dan melihat komunitas IT di manapun, terutama di Indonesia, yang ternyata memang sangat banyak. Pergaulan di komunitas ini sangat membantu proses belajar dan pengembangan keahlian saya di bidang *IT Sec*. Selain komunitas, keberadaan *open source* juga banyak membantu proses belajar saya.

IT sec dan *hacker* sering dihubungkan, tapi itu bukan saya. Kalau ditanya *hacker* itu apa, saya agak agak gimana gitu..... Mungkin bisa bertanya pada yang lain? Pokoknya bukan saya. Tapi bukan berarti saya nggak mau belajar ya. Sebenarnya *hacking* dan *hardware hacking* itu menarik juga, mungkin suatu saat saya akan belajar.

Dunia *IT sec* Indonesia saat ini menurut saya sudah sangat luas dan maju. Kita tidak kalah dengan negara tetangga, atau dunia luar. Dan semoga akan terus begini. Meski begitu, saya juga yakin bahwa dunia *IT sec* diluar sana juga akan terus berkembang. Semoga dunia *IT Sec* memberikan seorang Dirga, tempat untuk berkontribusi dan belajar :)

Profil

1. Nama (real name) : Ikhwan D Pratama
2. Panggilan sehari hari : Bermacam macam, ada yang ikhwan, dirga, tama,
3. Handle/nick : Djenova
4. Alamat : Yogyakarta
5. Handle origin : Belum ada yang manggil Handle origin, padahal pengen di panggil nova, tapi ada 1 orang sih yang manggil DJ dari Djenova
6. Mobile :
 - Telegram : djenova
7. Urls : idpratama.com
8. Sosial Media : twitter/idirgap
9. Komputers spec :
 - Pertama : Seingat saya core2duo
 - Sekarang : MBP MD101
 - Yang diidamkan : baru teripikirkan memberi nama setelah ada pertanyaan ini, mungkin akan saya kasih nama 'Athena'
 - Nama komputermu :
10. Member of :
 - Community : NgeSEC
11. What I like to do? : Research
12. What I dislike : Gapunya duit kwkwkw
13. Favorite / Kesukaan :
 - Makanan/Foods : Tempe
 - Minuman/Drinks : Air putih
 - Warna/Colours : Hitam
 - Jenis/genre Music : All
 - OS : Linux / Mac / Windows semua OK
 - Bahasa programing : PHP

50.5

55.40. 002

EKO



Parallel Hands On

Dalam hidup ini banyak hal yang bisa kita sepadankan dengan anime. Halah... ngomong apa ya saya.... Saya memang salah satu penggemar anime. Makanya saya menggunakan nama Ryo Saeba sebagai *nickname* saya. Bahkan sampai sekarang banyak yang memanggil saya om Ryo. Padahal nama saya Eko, dari nama asli saya Eko Juniarto.

Jaman chat di MSN, saya suka dengan komik anime berjudul City Hunter, dengan tokohnya Ryo Saeba. Kemudian saya ngobrolin anime ini dengan Matias Prasodjo. Dia sedang membahas soal cewe butuh cowo itu seperti ikan butuh sepeda. Sebuah quote yang cukup keren.

Dia sendiri punya *nickname* "sigantengkalem". Sebuah nickname yang tampaknya bisa jadi alternatif yang cukup bagus. Maklumlah, saat itu sudah terlalu banyak orang lain yang menggunakan "ryosaeba" sebagai nickname. Jadi sigantengkalem itu saya "curi" dari Pras.

Saya pengagum Steve jobs, seorang manusia yang *disruptive, know what he's doing, know what people needs*. Saya sendiri seorang technologist yang mempunyai cita cita terbesar menjadi pensiunan bahagia. Sebagai *technologist*, saya tidak bisa jauh dari komputer. Kalau ditanya apa itu komputer menurut saya, jawabannya adalah sesuatu yang jika diberikan perintah dengan benar, *would do anything for you*.

Tentunya jika bicara soal benar dan salah, kita harus mempelajarinya kan. Nah kalau menurut saya lagi nih, cara belajar komputer itu *Paralel hands on. Parallel hands on sendiri* seperti kata pepatah 'Sambil menyelam, minum air'. Belajar tapi agar lebih menarik ada target yang memang disukai, seperti *problem solving* misalnya. Jadi belajar

dan langsung praktek. Kita harus tahu konsep di belakangnya. Kita juga harus punya target tertentu yang akan kita capai, seperti *problem solving* misalnya. Cerita saya jaman dulu mungkin bisa menjadi contoh. Cerita tentang *how do I play Doom multiplayer*, di jaman belum ada internet? Bahkan saat itu network ethernetpun belum umum. Dengan belajar secara pararel dan tahu konsepnya maka saya bisa menghubungkan dua komputer dengan serial port. Saya mengulur kabel serial dan menyolder kabel RS232. Dan masalahpun terpecahkan, saya bisa main Doom multiplayer.

Automation, dan Security IT

Dari begitu banyak bidang di ilmu komputer, *automation* menjadi pilihan saya. Hal ini karena dengan ilmu ini, saya bisa membuat komputer yang bisa bereaksi dengan minimal manual input dari manusia. Automation itu seperti melakukan geofencing. Saat udah dekat rumah, komputer akan otomatis menyalakan AC, dan sebaliknya jika sudah di luar geofencing, komputer otomatis mematikan AC. Karena pilihan saya inilah maka aplikasi yang saya garap adalah aplikasi *home brew automation*. Tentu saja yang berhubungan dengan hobby saya, yaitu mengumpulkan film dan TV series

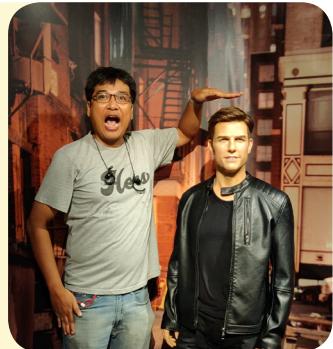
Karena dari kecil sudah mengenal komputer (Atari PC), maka saya sangat tertarik pada komputer. Menurut saya jika diberikan perintah atau input yang benar, banyak sekali yang bisa dilakukan oleh komputer, termasuk penjabarannya ke dunia IT dan *security*, yang menarik bagi saya. Bidang lain yang saya pelajari di dunia komputer adalah bidang *security*, yaitu sebuah proses atau bisa dikatakan sebagai sebuah perspektif dalam keilmuan komputer. Semacam disiplin seseorang, supaya tidak mudah dikerjain oleh orang lain

Pengalaman pertama saya dengan *security* sebenarnya adalah saat saya berhadapan dengan virus *Brain*. Namun pada waktu itu (jaman SMP) komputer hanyalah tempat untuk bersenang-senang bagi saya. Jadi konsep *security* masih belum masuk di kepala. Barulah ketika duduk di bangku kuliah dan mengenal *Back Orifice*, *broken TCP stack*, saya mulai mengerti mengenai apa itu *security*. Saya baru menyadari bahwa *security* bukan sekedar pasang firewall atau antivirus. Melainkan disiplin pribadi untuk tidak membuka kesempatan buat orang lain iseng. Misalnya hacker. Seseorang yang punya waktu, punya kemampuan dan cukup sabar mencari celah dan membuat sebuah sistem melakukan sesuatu yang di luar spesifikasi. Berbeda dengan hardware hacking atau open hardware. Menurut saya *Hardware hacking could be great, as long as there is a sustainable business model than can supports it*.

Disisi lain, ada opensource yang merupakan sebuah perkembangan luar biasa di dunia komputer. *Great movement, enabling great softwares being created: high performance webservers (apache, nginx), multimedia processors (ffmpeg, mkvtoolnix, imagemagick), and startups growing depending on them*. Sepertinya pemerintah harus lebih pro aktif ya. Harusnya ada standarisasi, pemanfaatan dan dukungan penuh.

Profil:

1. Nama (real name) : Eko Juniarso
2. Panggilan sehari hari : Eko. Kadang ada yang manggil Oom Ryo.
3. Handle/nick : ryosaeba/ sigantengkalem
4. Alamat : Apartemen Kebagusan City, Jakarta Selatan
5. Urls : ryosaeba.wordpress.com
6. Sosial Media (Facebook, Instagram, Twitter, dll) : ryosaeba/sigantengkalem
7. Computers spec :
 - Pertama : Atari 800
 - Sekarang : old faithful, Macbook Air 2014, 256 GB SSD 8 GB RAM. Tapi ini kebanyakan cuma buat remote box2 lain (Windows, Linux, cloud instances).
 - Yang diidamkan : belum ada yang real. Mau cari yang batere tahan lama (lebih dari satu hari), konektivitas internet, ringan, dan mudah buat jalanin RDP & ssh.
8. Member of :
 - Community : Mafindo, Masyarakat Anti Fitnah Indonesia
9. What I like to do? :
 - : knowledge sharing, also learning something new. That's why I hang out at ABSM, Anda Bertanya Sains Menjawab FB group.
 - : not owning mistakes.
 - : anything that tastes great. From nasi goreng to sushi.
 - : es teh manis atau coca-cola
 - : mix & match. Lately red.
 - : easy listening
 - : U2
 - : Kung Fu Hustle. Band of brothers.
 - : tom clancy. Herge.
 - : somewhere familiar. Love & hate relationship with jakarta.
 - : alone
 - : hoarding movies & TV series.
 - : nothing partial, anything that works. If I had to choose, probably linux, probably because it supports my hobby.
 - : ffmpeg, mkvtoolnix, plex: supporting my current hobby
 - : bash scripting
10. What I dislike :
11. Favorite / Kesukaan :
 - Makanan/Foods
 - Minuman/Drinks
 - Warna/Colours
 - Jenis/genre Music
 - Band / penyanyi
 - Movies/TV
 - Books & Authors
 - Place
 - Time
 - Hobby
 - OS (kenapa?)
 - Software (kenapa?)
 - Bahasa programing



Trust dan Pengendalian di Dunia Internet

Pada suatu ketika, ada seorang guru yang menghubungi ke saya melalui Telegram. Saya tidak kenal dengan orang ini. Saya hanya tahu profesinya guru. Itupun karena dia yang memberitahu saya diawal pembicaraan. Saat itu Dia bertanya, bagaimana cara login ke modem ADSL. Ya ... ya... kira-kira beginilah nasib seseorang yang sudah telanjur dikenal sebagai "orang IT". Mungkin saya dianggap sebagai *helpdesk* gratisan 24 jam. Saat itu sudah larut malam.

Sebagai bagian dari rangkaian pertanyaan, Dia mengirimkan foto stiker konfigurasi dari modem tersebut. Isinya berupa alamat IP dan user/password-nya. Problem dia adalah, walau sudah mengisikan alamat IP di browser, hanya pesan error yang muncul. Bukan layar login ke *control panel*. Dari sini saya menduga kalau konfigurasi modem tersebut sudah dimodifikasi. Hal ini menyebabkan konfigurasi yang baru sudah tidak sesuai dengan keterangan dalam stiker konfigurasi tersebut. Berbekal dugaan sementara tersebut, saya menanyakan alamat IP komputer yang dia pergunakan, untuk bisa mendapatkan gambaran, berapa kira-kira alamat IP lokal dari modem yang dipertanyakan. Alih-alih mendapatkan alamat IP, jawaban yang datang malah membuat dahi saya berkerut,

"Saya sudah mengubah alamat IP komputer yang saya pakai. Sudah saya sesuaikan dengan informasi pada stiker yang menempel pada modem tersebut," katanya. Waduh, muncul lagi dong problem baru. Sekarang komputer dia

terputus dari internet. Kami masih bisa berkomunikasi karena menggunakan handphone. Saya mulai berkeriyit kesal. Ini orang kenapa melakukan hal yang jauh berbeda dengan yang saya minta ya. Maksud saya, kalau dia sampai perlu bertanya minta tolong ke saya, artinya dia memang tidak tahu apa-apa soal jaringan IP. Namun alih-alih menjawab pertanyaan saya, dia malah berinisiatif sendiri. Dia melakukan hal yang sama sekali berbeda dan bukan merupakan solusi.

Efek Dunning-Kruger, adalah penjelasan sebuah fenomena ketika seseorang yang tidak tahu bahwa dia tidak banyak tahu tentang sesuatu hal, malah sok tahu dan yakin akan pengetahuan dia tentang hal tersebut. Dan sekarang tampaknya saya sedang menyaksikan efek DK ini sedang beraksi. Untuk bisa melanjutkan penyelesaian masalah, dengan sedikit kesal saya minta dia untuk membatalkan perubahan yang telanjur dilakukan. Saya minta dia mengubah setting dengan menggunakan DHCP.

Segera setelah setting DHCP dipergunakan, komputer sudah kembali bisa berinternet. Kali ini saya meminta dia mengirimkan hasil perintah ipconfig. Dia menggunakan Windows.

Dari informasi yang dia kirimkan, terlihat IP gateway yang semestinya juga merupakan IP dari modem tersebut. Saya minta dia untuk membuka IP tersebut di *browser*. Apakah masalahnya selesai?

Tentu saja belum, dan membuat saya masih harus terbangun walau sudah menjelang tengah malam. Kali ini dia tidak bisa login, karena sepertinya kata sandinya sudah diubah. Tidak sesuai dengan stiker konfigurasi yang ditempelkan di modem tersebut. Lalu dia minta tolong saya untuk bisa me-reset password.

Saya sebenarnya tahu jika modem direset, maka kemungkinan besar modem tidak bisa lagi login ke DSLAM. Hal ini disebabkan informasi login tersebut ikut hilang kena reset. Namun jiwa iseng saya muncul, akibat kekesalan yang bertumpuk. Sudah dianggap helpdesk gratisan oleh orang yang tidak saya kenal, lalu sok tahu walau tidak mengerti soal jaringan, dan kini masih minta tolong reset password walau sudah hampir tengah malam. Jadi saya putuskan untuk memberitahu cara reset modem tanpa memberitahu bahwa itu akan mengakibatkan internet terputus. Toh dia juga tidak minta internetnya tidak putus.

Selang beberapa lama kemudian, dia memberitahu saya bahwa kali ini dia sudah bisa login ke modem, sesuai dengan alamat IP dan kredensial yang tertulis di stiker, namun malah tidak bisa terkoneksi ke internet.

Oh iya, kali ini dia kontak ke saya melalui Telegram di HP. Saya sarankan agar dia menghubungi call center dari penyedia layanan internet yang dia pakai, untuk minta dikirimkan teknisi untuk setting ulang modem tersebut. Kekesalan saya kini jauh berkurang, karena saya bisa melakukan *denial of service*. Saya memutuskan sambungan internet di depan mata dia, tanpa dia menyadarinya. Saya bisa melakukan hal tersebut karena *trust* atau kepercayaan yang berlebihan dari orang yang tidak saya kenal ke saya.

Bercerita soal *trust*, hingar-bingar soal Pemilu 2019 mengedepankan berbagai isu. Salah satunya adalah banyaknya kartu yang dijanjikan untuk kepentingan dan kesejahteraan rakyat. Bermunculan video PoC, atau *Proof of Concept* di media sosial, bahwa dengan hanya modal eKTP, berbagai kartu yang dijanjikan tadi tidak diperlukan. Seperti mesin otomatis yang mengeluarkan beras, atau palang pintu tol.

Konsep penggunaan NFC ini sebenarnya bukan hal baru. Sejak munculnya NFC di ponsel pintar, sudah banyak yang memanfaatkan untuk kendali rumah pintar, seperti membuka kunci pintu, menyalakan AC atau lampu secara otomatis, dan lain sebagainya. KRL, jalan tol, dan MRT juga menggunakan NFC melalui kartu KRL dan juga uang digital (eMoney, Flazz, dan lain-lain). Semua ini bekerja dengan konsep yang sama: saldo tercatat di kartu. Bukan



disimpan pada sebuah sistem terpusat di cloud. Ini akan menjamin *robustness* atau ketahanan sistem: ratusan gerbang bisa berfungsi independen terhadap koneksi jaringan, karena proses debit dilakukan secara lokal langsung pada saldo yang tersimpan di kartu.

Kembali ke PoC di atas, memang benar eKTP yang merupakan kartu NFC bisa dimanfaatkan untuk membuka gerbang tol misalnya. Namun karena tidak didesain sebagai uang digital, saldo mau tidak mau harus disimpan terpusat. Ini tentu saja membuat tiap gerbang menjadi bergantung pada kesediaan jaringan; jika terjadi gangguan sehingga tidak bisa memeriksa saldo, maka praktis ratusan gerbang tol juga turut tidak bisa berfungsi.

Jadi mana yang dimaksud berhubungan dengan *trust*? Bayangkan jika benar terjadi bisa menggunakan eKTP untuk gerbang tol/KRL/MRT, semuanya itu harus tersambung ke jaringan agar bisa cek saldo, yang berarti *seluruh pergerakan pemilik eKTP* yang menggunakan jalan tol/KRL/MRT, bisa dipantau secara *real time*. Hal ini tidak terjadi di sistem yang menggunakan uang digital yang sekarang sudah berjalan. Benar menggunakan uang digital memang tetap bisa dipantau jika diinginkan. Namun kartu uang digital tidak ada korelasi langsung dengan identifikasi diri (NIK). Berbeda dengan eKTP yang juga menyimpan NIK di kartu. Kemungkinan kartu uang digital dipergunakan oleh lebih dari satu orang lebih besar ketimbang eKTP. Sistem yang tidak terhubung ke jaringan membuat pemantauan tidak bisa *real time*, harus mengambil dulu data yang tersimpan di tiap gerbang.

Jadi kalau memang mau pakai eKTP untuk keperluan transportasi, maka pemerintah bisa memantau gerak-gerik rakyatnya sendiri. Seperti yang sudah terjadi di Cina yang memantau warganya melalui CCTV dan alat pengenalan wajah. Yakin menempatkan *trust* pada sistem seperti ini?

The background features a dense field of glowing blue fiber optic strands radiating light in various directions, creating a sense of depth and connectivity. In the foreground, four network cables with clear plastic RJ45 connectors are bundled together. The connectors are illuminated from behind, casting a bright glow and creating sharp highlights on their metallic contacts and plastic housing. The cables themselves are dark, contrasting with the bright background.

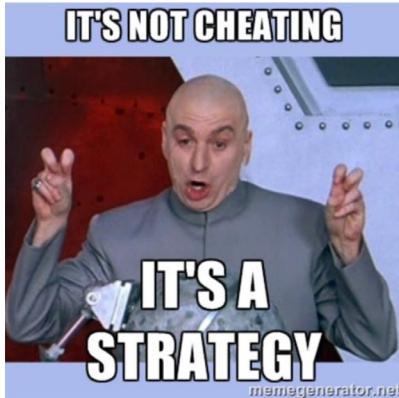
Edo Maland

Learning is Everywhere and Anytime

Siapa saya? Saya adalah *hackerman* wakwakwak. Tidak, tidak saya bercanda. Saya hanyalah orang penggiat IT yang suka ngoprek saja dan memiliki penasaran yang tinggi terhadap dunia it terutama IT Sec. Bersama dengan teman-teman, saya juga mendevelop beberapa tools dan distro pentest yang asli dari Indonesia. Distro ini bernama draCos Linux tidak turunan tapi *Linux From scratch*. Di tahun ini kita juga akan merelase versi dracOs linux Versi 4 dengan Codename santet. Ditunggu ya teman teman kehadiranya dan tetap dukung karya anak bangsa



Dulu waktu tahun 2012/2013 jaman jaman saya smp itu saya dulunya hobby main game dan tidak tau dunia security-security an itu apaan yang saya tau hanya Cheat,. Maybe



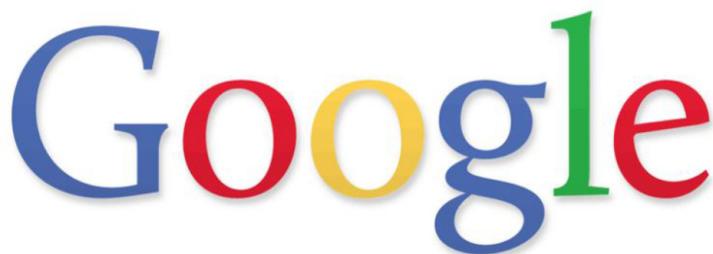
Wkwkwk, Jadi pertama itu game yang mainin adalah game Grand Chase, kira kira penampakan dari gamenya tu gambar gim dibawah ada dibawah ini



Jadi seiring dengan perjalanan, saya itu penasaran sama alur dari game ini. Banyak pertanyaan yang muncul saat itu. Kok bisa ya ada muncul *damage critical* (meskipun dalam hati saya menjawab sendiri “oo ini tergantung, point critical kita seberapa besar”). Kok darah kita bisa berkurang yang kalau kena pukul dan MP (Mana) kita kok bisa abis ya kalau digunakan untuk skill.

Nah disini sayanya penasaran dan mencoba untuk berandai-andai ajaa dulu. Seandainya bisa kita ganti darah kita menjadi 9999999 mungkin kita ga akan mati-mati. Seandainya kita ganti dan setting MP kita *Delay* terisi otomatis maka MP ga akan habis habis.

Dari sini saya lalu mencoba, iseng iseng melakukan pencarian dan bertanya kepada "**suhu para suhu**"



Nah saat "**suhu para suhu**" ini memberikan referensi untuk masuk ke sebuah forum luar yang membahas *cheat*, disana lah saya mendengar beberapa tools seperti Kernel Detective, Charles Proxy, Fiddler dan lain-lain sebagainya.

Dengan adanya beberapa tools diatas saya udah coba bongkar file executable menggunakan PE Explorer. "Nggak ngerti cuy isi nya x0x0x0x gitu" Jadi waktu itu saya cuma baca stringnya aja wakwakwakw. Saya bongkar sub folder"nya kemudian melihat isi file satu persatu. Saya mencari value-value yang digunakan dalam game tersebut. Saat itu saya belum tau kalau apa yang saya lakukan itu adalah metode Reverse Engineering, p. Nah disitu lah saya menemukan beberapa nilai penting dan *end point*. Saya menemukan kapan firewall game itu berjalan dan mematikan process firewallnya menggunakan tools kernel detective dan lain-lainya untuk mengganti valuenya (kek burpsuite gitu laa wkwk).

Seiring perjalanan saya malah "**tidak menikmati game yang saya mainkan**". Kemudian saya menyadari bahwa saya malah mencari game-game yang ada untuk, *saya cheat*. Saya merasa tertantang saja wkwk. Misalnya penggunaan *fiddler* dan *charles proxy* untuk menangkap dan mengubah *traffic* yang saya gunakan untuk game-game yang berbasis Web seperti game yang ada difacebook maupun game MMPORG lainya

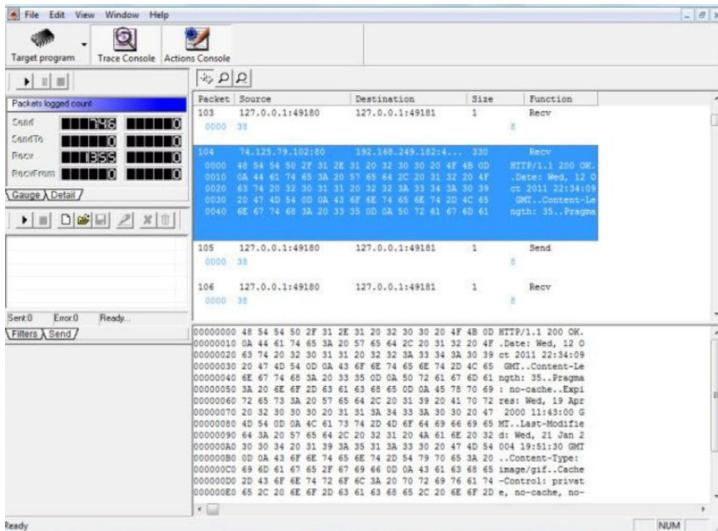
Selang 6 bulan kemudian, ada game serupa yang muncul. Game yang bernama Elsword dari Netmarble,



Perbedaan dengan game sebelumnya, game ini lebih bagus graphicnya. Lebih menariknya lagi, game ini bisa memperjual belikan ED (GOLD).



Sesuatu yang mampu membuat saya tertarik dan mulai berpikir keras. Muncul dalam pemikiran saya, bagaimana kalau saat kita mendapatkan (ED+) ataupun EXP,kita coba tangkap paket yang masuk lalu kita repeat ulang. Mungkin bisa dikatakan dengan *diburpsuite di intercept* terus dikirim ke *intruder*. Sayapun mencoba browsing" apa sih tools yang bisa dipakai. Saya menemukan beberapa tools yang cukup keren. Namanya "WPE (Winsock Packet Editor)



Ready

Winsock packet editor ini memungkinkan kita untuk:

- memodifikasi data pada level TCP,
- dapat memilih proses yang berjalan dari memori,
- memodifikasi data yang dikirim sebelum mencapai tujuan dan,
- merekam paket dari proses tertentu, kemudian mengirimkan dan menganalisis informasinya kembali

Ternyata tools ini terdeteksi oleh firewall dan program langsung exit saat kita menjalankannya. Saya mencoba searching kembali untuk mengakalinya. Akhirnya saya menemukan dan menggunakan Proxy Server (**CCProxy**). Jadi semua packet yang akan kita tangkap, akan melalui proxy server. Nah disinilah kita mulai masuk menggunakan wpe. Saya menjalankan wpenya beda Mesin *Gunain Virtual machine. biar process wpenya ga terdeteksi sama firewallnya. Karena saat itu komputer saya hanya satu, saya berusaha mencari solusi lain.



Kemudian saya coba menangkap packet saat proses mendapatkan ED dan EXP. Saya coba mencari-cari, dimana proses tersebut hingga mendapatkan repeat packetnya pada game tersebut. Dan ternyata berhasil, duit dan exp saya bertambah meskipun hanya tinggal duduk saja wkwkwkw.

Dari Game Pindah Ke Film

Di tahun 2014 an saya mulai bosan bermain game. Rasanya sudah tidak ada rasa "hilang selera" terhadap dunia game. Saya beralih ke film. Kerjaan saya hanya menonton film saja. Ada beberapa film yang membuat saya tertarik ke dunia hacker-hacker gitu gan, rasanya kek pengen bisa aja kek gitu wkwkw.

Film yang pertama yaitu berjudul Bloody Monday



Ini film dulu gan, dah jadul banget tapi keren banget. Film ini menceritakan tentang seorang hacker bernama Fujiyama. Dia yang membantu menyelamatkan dunia. Seperti motto hacker (save the world). Dalam film ini ada beberapa teknik yang merupakan real teknik. Seperti penggunaan Live USB (dulu itu tenar banget pada jamanya), Exploitasi windows menggunakan gambar yang telah disisipin virus untuk ngehack gurunya dan juga ngehack komputer lalu mengunci komputer tersbut dan mengantinya dengan wallpaper burung falcon. Hal ini membuat saya terinspirasi dan mencoba tirukan dari sebuah film wkwk.

Mungkin ada yang mencemooh “Haalah kebanyakan nonton film”. Tapi ya gimana ya, kalau saya, semua itu harus mencoba dulu, apakah itu mustahil atau tidak, baru kemudian mencari refensinya. Beberapa Teknik yang saya lakukan juga mungkin terinspirasi dari sebuah film. Lalu dengan kepenasaran itu saya langsung kembali bertanya ke **“suhu para suhu”, GOOGLE**. Dari sinilah saya mulai terjun dan membaca baca artikel/engine apapun itu yang ada disana. Kemudian dari beberapa hal yang bermunculan, seperti forum forum sesepuh, saya mendapatkan banyak hal yang menjadi bahan bacaan saya yang masih serapuh indomie ini forum-forum itu diantaranya forum echo.or.id :



Kecoak elektronik



Indonesianbactrack

The screenshot shows the profile page for 'THJC' on the 'indonesianbactrack.com' forum. At the top, there's a navigation bar with links for Home, Forum, Portal, Mirror, Search, Member List, Calendar, and Help. A search bar is also present. Below the navigation, it says 'Profile of THJC'. The profile information includes a small profile picture of a person with a red and yellow logo, a bio section with a 'LinuxUser' badge, and a registration date of 18-05-2011. It also shows a 'Status: Online' message.

Dan masih banyak lagi forum-forum hebat lainnya. Sayapun harus mengucapkan terimakasih banyak kepada mereka yang telah membagi ilmunya.

Dari Film Bloody Monday, saya berhasil menginstall linux backtrack di live usb. Saat itu rasanya sudah kaya haker tingkat dunia gan. Bagaimana ngga coba, kita bisa menggunakan sistem operasi lain di tempat orang lain dimana saja secara portable. Sayapun menjadi



Saya Masih Newbie dan Akan Selalu Menjadi Newbie

Lalu setelah install linux di live usb saya coba mengimplementasikan "ngehack windows", gan. Saya mencoba untuk bisa meremote pc korban dari jauh seperti di film Bloody Monday. Kemudian saya mencoba menanamkan virus di gambar.

Ternyata tidak mudah wkwk, setiap malam saya membaca artikel yang tidak saya paham sama sekali wkwk. Saya hanya mengikuti instruksi youtube dan artikel yang ada. Maklum saya masih newbie dan *scriptkiddies* kala itu (dan sekarang pun saya masih tetap **newbie – I'm always newbie** om, karena ilmu berkembang pesat dan setiap orang mendapatkan informasi yang berbeda dan sumber yang berbeda pula), Coba lihat tampang saya aja seperti ini. Lihat lingkaran bewarna merah dan itu adalah saya wkwk

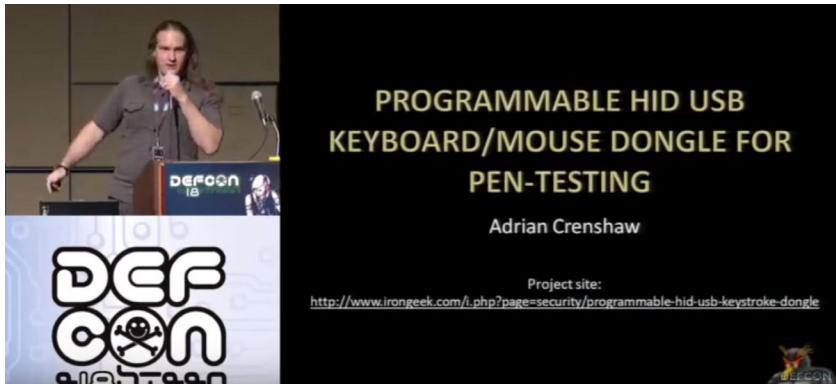


Setelah mencoba beberapa kali saya tetap gagal. Tapi menurut saya, itu lebih baik “ **mencoba lalu gagal dari pada gagal mencoba** ”. Kemudian sayapun mencari referensi lain dan mencoba mengkombinasikan referensi yang ada agar bisa mencari titik masalah yang ada itu dibawa ke **suhu para suhu**.



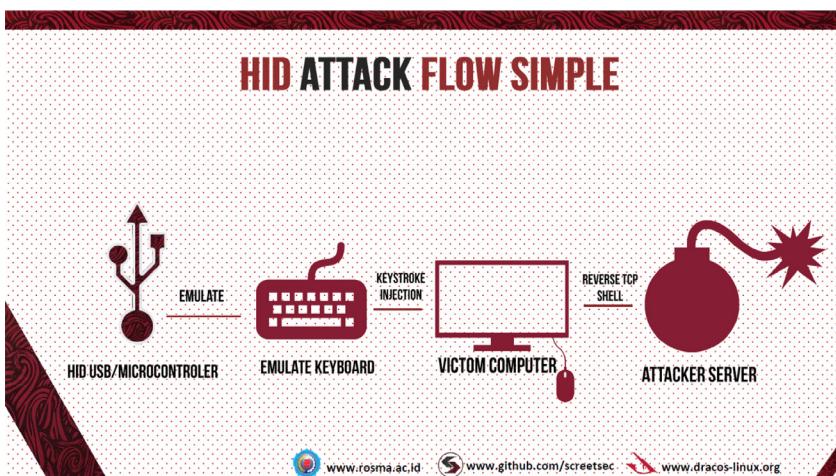
Dan akhirnya setelah mencoba lagi sayapun berhasil. Meskipun hanya bisa antar jaringan jaringan local dan rasanya itu seneng bangeet dan rasanya terbalaskan.

Pada tahun 2014/2015 saya beralih ke youtube dan menonton channel-channel conference seperti defcon / blackhat dan lain lain yang membahas tentang security. Disana ada satu materi yang bener bener menarik yaitu tentang "Programmable HID USB keystroke Dongle" yang dibawakan sama om Adrian Crenshaw (irongeek),



Jadi yang dibahas disini adalah kita bisa memasukan sebuah kode jahat kedalam sebuah microcontroller / device yang berbentuk seperti USB Drive atau Flashdisk maupun hardware yang, namun berfungsi layaknya mouse, joystik dan keyboard. (USB = Keyboard)

Mungkin proses alurnya seperti ini secara sederhananya



Lalu dengan adanya referensi dari om Irlonegeek, saya mencoba melakukan research, “mencoba menggunakan teensy 3.0 dan mencoba membuat script” payload, untuk menginjeksikan kode tersebut ke dalam teensy, dan mencoba menjalankannya ke komputer orang. Lagi-lagi rasanya saya seperti

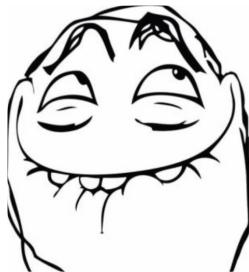


Berkembang Dengan Membuat Tools “Brutal”

Kemudian di tahun selanjutnya saya mencoba membuat Tools “Brutal” untuk membantu kita dalam pembuatan payload. Tools ini akan membuat beragam payload dengan cepat seperti,powershell attack, virus attack and lain lain

```
V  
Brutal Created By : Edo Maland ( Sreetsec )  
Version : 1.0  
Codename : Reaper  
Follow Me on Github : https://github.com/Sreetsec  
Dracos Linux : dracos-linux.org  
  
[01] Meterpreter Reverse TCP Injection using Powershell  
[02] Download and Execute Backdoor  
[03] Get Credential information With Mimikatz [ Send to gmail ]  
[04] Retrieve lots of passwords stored on a local computer [ gmail ]  
[05] Exploit Local Admin Privilege [ Fun with Windows ]  
[06] Payload to Manage Windows [ add user,up,enable,tele ]  
[07] Attacking Windows [ At your Own Risk ]  
[08] Help and Tutorials  
[09] Credits  
[10] Exit  
  
Sreetsec@Brutal: >> |
```

Kalian bisa mencoba dan mendownloadnya di
<https://github.com/Sreetsec/Brutal>



Dari metode penyerangan diatas saya memiliki sebuah cerita yang lucu dan gregetan banget. Saya coba implementasikan penyerangan tersebut ke guru saya sendiri. Its really cool bro

Saat itu posisinya, saya sedang duduk dan membuka laptop kecil sambil asik "ngoprek". Ketika bu guru selesai menjelaskan, dia mengatakan sebuah kalimat yang indah

"Hai anak anak Besok kita ulangan "



Saya terkejut dan spontan bilang “wuanjirr kok dadakan sihh dan besok pula!”. Maklum ya, namanya masih pelajar, rada sebel dengan yang dadakan wkwkw. Kemudian munculah itikad baik saya



Lalu saya mencoba menggali informasi (*Social engineering*) ke ibuknyaa

Saya : “Buk Kisi kisi ada gak”

Ibuk : “Adaa naak”

Saya: “Dikasih tau ga buk kisi kisinya kekita “

Ibuk : “Iya nanti ibuk bacain kisinya “

Saya : “Wooh berarti soalnya udah selesai ya bu“

Ibuk : “Iya udah nanti ibuk kasih gambaran dari soal yang ibu bikin ini”

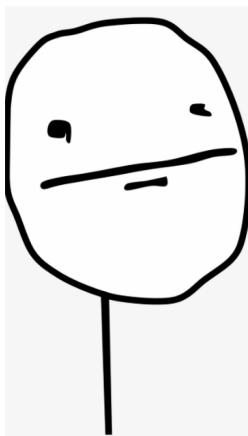
Dalem hati saya, waaah ini sepertinya bisa deeh kalau kita coba ambil soalnyaaa wkwkwkw. Kebetulan posisi laptop bu guru sedang berada di depan meja dan saya juga sedang duduk didepan deket meja guru. Kira kira gambaranya seperti ini



Naah disini saya ada niatan untuk memasukan badUSB ini ke laptop ibu guru. Tetapi sebelum itu saya harus membuat sebuah *payload* untuk melakukan *take over laptop* ibu guru. Saya menggunakan brutal untuk lebih cepat dalam pembuat *payload*. Setelah *payload* berhasil dimasukin ke Teensy, saya bersiap-siap menunggu ibu guru berjalan keliling *posisinya kita sedang membahas soal latihan.

Saat si ibu berkeliling dan menuju ke meja belakang bagian ujung. Saya langsung maju dengan membawa buku LKS (Lembar kerja siswa) dan BadUSB ini dengan kabel yang Panjang dan diletakan di kantong teensynya. Saat ibu itu menunduk dan menjelaskan ke bagian kelompok belakang, saya langsung memasukan usb tersebut kelaptop ibu guru. Disini saya meminta bantuan temen saya untuk menutupinya dari depan bersama dengan saya agar tidak terlihatnya kabel yang sedang menjulur sedikit.

Setelah badUSB dimasukin saya menunggu sekitar 10-15 detik agar kode tereksekusi secara otomatis tanpa adanya perantara lagi dari kita. Saat kode tereksekusi, di hitungan kelima ibu guru menoleh ke arah depan secara tiba-tiba dan menatap seperti ini wkwkwk



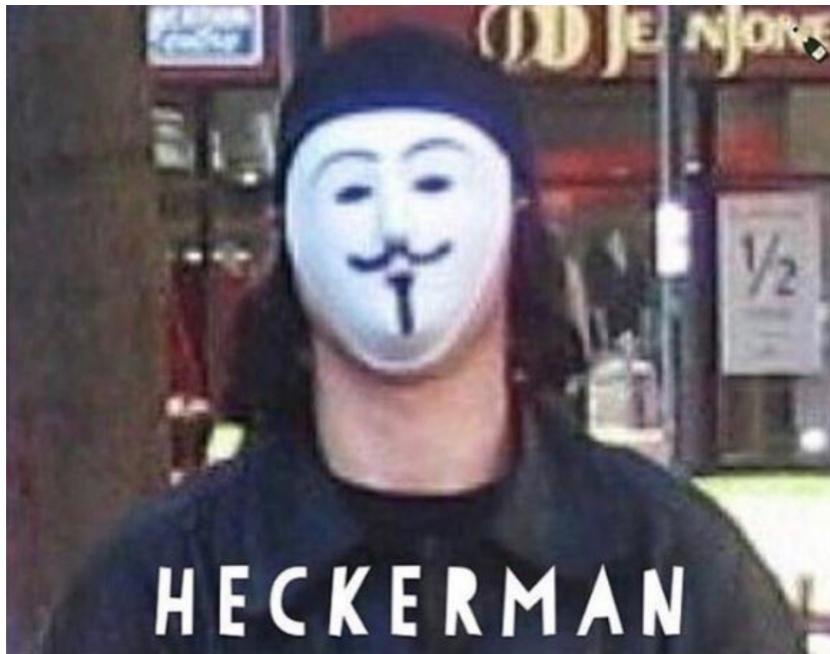
Namun kita tetap terlihat santai. Kita tetap memegang LKS dengan kedua tangan. Dan saya berpura-pura menjelaskan materi kepada teman saya. Tidak berapa lama perhatian si ibu kembali ke bagian belakang dan melepaskan pandangannya dari kami. Mungkin ibunya berpikir, selama kita tidak ada interaksi langsung, tanpa adanya sentuhan seperti memegang laptopnya, maka laptopnya akan tetap aman. Mungkin dia berpikir apabila mahasiswa mencoba untuk mengambil sebuah file, akan membutuhkan waktu yang lama.

Setelah berjalan kurang lebih 15 detik dan kode telah berjalan, kita langsung melepaskannya usb tersebut dari laptop bu guru. Saya pun berhasil mendapatkan akses dari komputer Ibu guru itu hanya dalam ±15 detik saja.

```
msf exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.43.1:4444
msf exploit(multi/handler) > [*] Sending stage (70071 bytes) to 192.168.43.100
[*] Meterpreter session 1 opened (192.168.43.1:4444 -> 192.168.43.100:60904) at 2018-09-28 16:48:51 +0500
msf exploit(multi/handler) > 
```

Setelah mendapatkan sesi, lalu saya bisa mengontrol laptop ibuk itu secara penuh. Saya kemudian mencari file ulangan berada dan berhasil menemukannya. Dan sekali lagi *I like*



Mungkin itu cerita awal mula saya, kenapa bisa terjun dan berkecimpung di dunia IT Sec. Sebenarnya sih masih banyak cerita-cerita memorable lainnya yang tidak sempat saya ceritakan. Apabila ada waktu kita dapat bertemu kita bisa *sharing* dan bertukar sudut pandang.

Profile

1. Nama (real name) : Redho Maland
2. Panggilan sehari hari : Edo Maland / Edo
3. Handle/nick : screetsec
4. Alamat : Pekanbaru, Pelalawan
5. Handle origin : Yogyakarta
6. Mobile :
 - Telegram
 - Lain lain
 : screetsec
7. Urls : <https://www.linkedin.com/in/edomaland/>
8. Sosial Media (Facebook, Instagram, Twitter, dll) : <https://www.github.com/sreetsec>
9. Computers spec :
 - pertama : Asus x401u & Thinkpad x240
 - Sekarang : Asus ROG 553VD
 - Yang diidamkan : Asus ROG Zephyrus & Dell xps 15
10. Member of :
 - Community : dimana ada komunitas disitu ada wkwkw
 - Projects : dracOs Linux & dev some tools (github.com/sreetsec)
11. Favorite / Kesukaan :
 - Makanan/Foods : Enak semua sih, tapi paling di utamain daging & seafood
 - Minuman/Drinks : Kopi & Susu (Biar hitam dan putih)
 - Warna/Colours : Hitam / Putih
 - Jenis/genre Music : Indie, Pop & Classical Music Instrumental Guitar
 - Band / penyanyi : Kalo Film Hacker Hacker gitu sih (Mr. Robot, Bloody Monday, Phantom Ghost, Sword Fish dan lain lain). Kalo Film Super hero Avengers dong
 - Movies/TV : Jarang baca melalui buku sih, lebih sering dari artikel / twitter (lebih progressive perkembangan informasinya cepett gan)
 - Books & Authors : 127.0.0.1
 - Place : 8.8.8.8
 - Time : Ngoprek, Lukis (art), Fingerstylee, Music,
 - Hobby : dracOs Linux & Kali Linux & Windows
 - OS (kenapa?) : Software yang Open Source Lebih diutamain, ga punya duit bang
 - Software (kenapa?) : Python & Bash
 - Bahasa programing : Bergabunglah dengan komunitas karena komunitas itu menentukan kualitas dan kita akan menjadi sama dengan siapa kita Bersama
 - Words/Quote :

Penjabaran Istilah

Di sini saya coba jabarkan beberapa istilah tersebut :
Kernel Detective :

Tools gratis yang membantu Anda mendekripsi, menganalisis, memodifikasi secara manual, dan memperbaiki beberapa modifikasi kernel Windows NT. Kernel Detective memberi Anda akses ke kernel secara langsung sehingga tidak berorientasi untuk pemula

Kernel Detective v1.2.1 - System						
File	Settings	Help	Handlers	Kernel-Mode Drivers	Disassembly	Debug New
Index	Sel	Current ISR	Real ISR	Type	Access Level (OPK)	Module
0x00	0x0000	0x00001F80	0x00001F80	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x01	0x0000	0x00054C0C	0x00054C0C	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x02	0x0000	0x00054C10	0x00054C10	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x03	0x0000	0x00054C10	0x00054C10	32bit Interrupt	Accessible from ring 3	D:\WINDOWS\system32\kernel32.exe [test]
0x04	0x0000	0x00054C90	0x00054C90	32bit Interrupt	Accessible from ring 3	D:\WINDOWS\system32\kernel32.exe [test]
0x05	0x0000	0x00054C90	0x00054C90	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x06	0x0000	0x00054C94	0x00054C94	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x07	0x0000	0x00054C94	0x00054C94	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x08	0x0000	0x00054C94	0x00054C94	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x09	0x0000	0x00054C30	0x00054C30	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x0A	0x0000	0x00054C50	0x00054C50	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x0B	0x0000	0x00054C50	0x00054C50	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x0C	0x0000	0x00054C80	0x00054C80	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x0D	0x0000	0x00054C80	0x00054C80	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x0E	0x0000	0x00054C80	0x00054C80	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x0F	0x0000	0x00054C50	0x00054C50	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x10	0x0000	0x00054C60	0x00054C60	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x11	0x0000	0x00054C60	0x00054C60	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x12	0x0040	0x00054C50	0x00054C50	16bit Task	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x13	0x0000	0x00054C80	0x00054C80	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x14	0x0000	0x00054C80	0x00054C80	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x15	0x0000	0x00054C80	0x00054C80	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x16	0x0000	0x00054C80	0x00054C80	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x17	0x0000	0x00054C80	0x00054C80	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x18	0x0000	0x00054C80	0x00054C80	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x19	0x0000	0x00054C80	0x00054C80	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x1A	0x0000	0x00054C80	0x00054C80	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x1B	0x0000	0x00054C50	0x00054C50	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x1C	0x0000	0x00054C50	0x00054C50	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x1D	0x0000	0x00054C50	0x00054C50	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]
0x1E	0x0000	0x00054C50	0x00054C50	32bit Interrupt	Accessible from ring 0	D:\WINDOWS\system32\kernel32.exe [test]

Charles proxy :

Charles adalah proxy HTTP / monitor HTTP / Reverse Proxy yang memungkinkan pengembang melihat semua lalu lintas HTTP dan SSL / HTTPS antara mesin mereka dan Internet

The screenshot shows the Charles proxy application interface. The title bar reads "Charles 2.7.04 - Session 3". The main window has several tabs: "Structure", "Sequence", "Overview", "Request", "Response", "Summary", "Chart", and "Notes". The "Request" tab is currently selected. In the left sidebar, there's a tree view of network traffic. The first item is a request to "<http://localhost:16080/>". Below it, under "Content", are requests for "<http://www.google-analytics.com>" and "<http://rcn.syndication.twimg.com>". Under "Default", there's a request for "<http://rcn.twitter.com>". Under "HTTP", there's a request for "<http://syndication.twitter.com>". The "Request" tab displays detailed information for the first request to localhost:

Name	Value
URL	http://localhost:16080/
Method	GET
Response Code	200 OK
Protocol	HTTP/1.1
Host	localhost
Keep-Alive	No
Content-Type	text/html; charset=UTF-8
Content-Length	1277 bytes
Remote Address	localhost:16080

The "Timing" section shows the following times for this request:

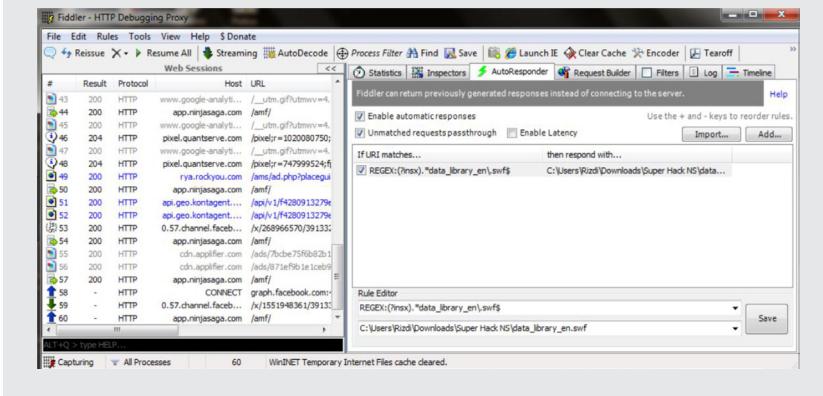
- Request Start Time: 11/02/13 13:44:02
- Request End Time: 11/02/13 13:44:02
- Response Start Time: 11/02/13 13:44:02
- Response End Time: 11/02/13 13:44:02
- Duration: 5.18 ms
- DNS: 113 ms
- Forward: 97 ms
- TLS Handshake: 0 ms
- Request: 120 ms
- Latency: 106 ms
- Speed: 15.12 kB/s
- Response Speed: 176.06 kB/s

The "Headers" section lists the following:

Name	Value
Request Header	692 bytes
Request-Header	342 bytes
Request	17.27 KB (17667 bytes)
Response	18.19 KB (18661 bytes)
Request Compression	98.8% (gzip)
Response Compression	98.8% (gzip)

Fiddler :

proksi yang dibuat untuk men-debug masalah lalu lintas HTTP antara komputer Anda dan internet

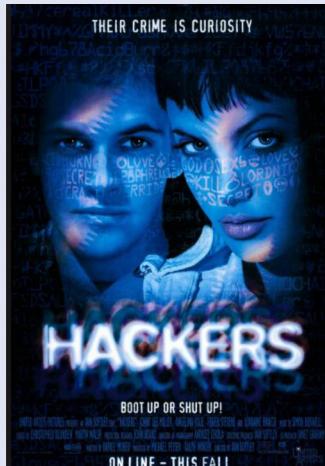


Film Yang Berkisah Tentang hacker

Ada beberapa film lain yang serupa dengan Bloody Monday yang berbau tentang hacker juga seperti film:

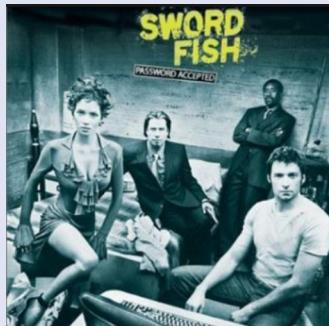
1. Hackers

Film jadul banget, keren deh pokoknya, tonton aja. Film ini diperankan sama wanita cantik Angelina Jolie wew



2. Swordfish

Film drama tentang hacker dan mata-mata. Dalam film ini, sepertinya sang tokoh menggunakan nmap untuk men-scanning dan mencari vulnerability pada service yang berjalan



3. Snowden

Membahas tentang intelligence, CIA dan lain-lain ini keren banget dia sampai membocorkan rahasia ini itu



4. Whoami

Film ini lebih membahas tentang social engineering. Ada beberapa film lain yang juga berkisah tentang Kevin Mitnick.

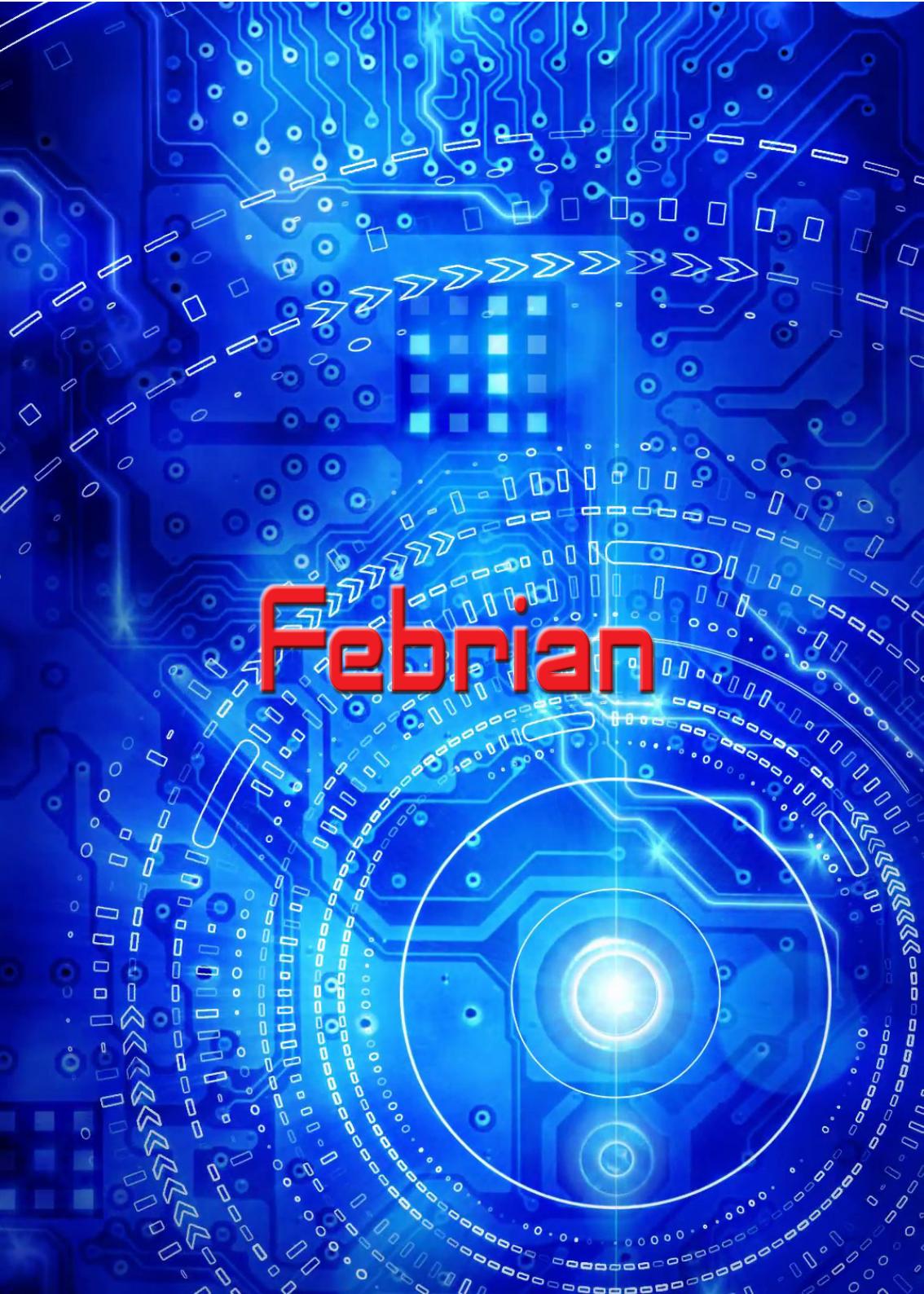


5. MR. ROBOT

Film ini bagus banget, jalan ceritanya tidak mudah untuk diprediksi. Hampir semua teknik yang digunakan pada film ini adalah metode yang teruji dan benar-benar asli, seperti penggunaan tools dan algoritma.



Dan masih banyak film-film yang keren dan tidak bisa saya sebutkan satu-satu, kalau ingin melihat listnya kalian bisa lihat disini <https://github.com/k4m4/movies-for-hackers>



Febrian

Kata si Bocah IT, Prinsip Belajar Komputer “Membangun Logika dan Learning by Doing”

“ **K**erjakan apa yang jadi bagianmu dan Tuhan akan mengerjakan apa yang jadi bagian-Nya” itulah quote yang saya jalani dan merupakan cerminan dari hidup saya. Seorang anti sosmed, alias tidak punya akun sosmed ditengah maraknya trend bersosmed yang luar biasa. Anda bisa memanggil saya Febri atau Rian atau bayi tabung atau unyil, atau nama saya Febrian. Nama yang diberikan oleh orang yang paling saya kagumi di dunia ini, ayah saya. Seorang laki-laki yang tidak pernah mengeluh dan selalu tersenyum hingga ajal menjemputnya. Kalau ditanya siapa saya, jawaban yang saya suka adalah hanya manusia mungil yang menjadi satpam server. Sebagai satpam server, komputer merupakan bagian terpenting dari hidup saya. Disinilah rejeki mengalir dengan bantuan seglondong komponen yang unik ini.

Terlahir dari keluarga sederhana di sebuah kota kecil yang masih masuk daerah Jawa Tengah dengan perawakan yang pendek dan berkacamata sedikit tebal. Orang-orang sering menyebut saya “bocah IT” dan muka laptop karena mayoritas waktu saya banyak di depan komputer mini itu. Saat ini status saya sudah resmi suami orang dengan 1 istri serta dikaruniai 2 malaikat kecil yang membuat hidup saya bahagia banget. Terlebih bahagia lagi istri dan anak saya bisa mengerti pekerjaan dan hobi ayahnya yang memang mengharuskan standby serta lebih banyak waktu di depan laptop. Berbicara tentang hobi, hobi saya banyak banget dari olahraga karate, lari,

mengajar dan main musik serta satu hobi yang mungkin sudah mendarah daging yaitu belajar IT. Namun kalau ditanya tentang sosmed, saya hanya punya WA dan telegram saja.

Dari awal belajar mengenal komputer yang kemudian menjadi sumber rejeki ini ada beberapa prinsip belajar komputer yang saya ikuti. Membangun logika dan *learning by doing*. Semua harus dilakukan dan dicoba dengan selalu membangun logika. Dari sinilah saya menemukan bidang kesukaan saya *cyber security & networking*. Kata security dalam benak saya memunculkan sosok polisi yang mencari lubang unik yang bikin penasaran.

Kecintaan saya akan dunia IT bermula ketika saya bisa membeli komputer dengan hasil jerih payah saya sendiri ketika memenangkan kejuaraan daerah atletik se-Jawa Tengah pada tahun 2004. Dengan bermodalkan uang itu saya dapat membeli komputer desktop dengan spesifikasi low-end yaitu processor intel celeron pentium IV, 128MB RAM, 20GB HDD ATA, VGA dan LAN Card onboard serta monitor tabung 14". walau low spek tapi lumayan deh untuk belajar. Pada saat itu pengennya yang canggih komputernya tapi apa daya uang tidak cukup.

Karena segitu cintanya saya dengan komputer itu maka tanpa sadar waktu saya habiskan untuk belajar komputer. Dimulai dari dasar pengoperasian software seperti microsoft office, ACDSee,dll hingga ketika SMK lebih mendalami lagi karena mengambil jurusan teknik komputer dan jaringan sehingga pada tahun 2006/2007 mulai kenal dengan komunitas cyber security seperti jasakom dan pertama kali belajar XSS dan itulah awal saya mengenal serta mengerti konsep security (ini masih dalam pemahaman konsep maling bekerja/konsep menyerang). Saya ingat ketika masih duduk di bangku SMK, ada salah satu guru yang bernama Bapak Soepracihno sering memberikan motivasi kepada saya dengan berkata : "Jangan hanya mempunyai skill yang biasa tapi ambillah spesialis karena tidak banyak orang yang tahu apa keuntungan menjadi spesialis". Nah, dari situ saya mencoba fokus pada dunia security yang dikala tahun 2007 masih sangat jarang ditemui dan ilmunya masih "tabu". Sebenarnya dulu mau masuk di SMA Taruna Nusantara di Magelang karena cita-cita dulu pengen jadi TNI. Namun apa daya takdir mengarahkan ke jalan yang lebih asyik hingga menjadi seperti sekarang yaitu satpam server.

Mengenang kisah pengenalan saya dengan bidang security saya kembali mengingat beberapa kenangan yang indah. Pengalaman pengalaman yang membuat saya ketagihan. Saya pernah *ngerjain* komputer teman-teman

dengan Metasploit di lab kom. Waktu itu OS yang digunakan masih win XP bug MS08-067 netapi. Saat itu kita sedang main dota. Nah pas mau menang, saya shutdown deh. Nakal ya wkwkwkwkk. Inilah pertama kali saya bisa ngehack dan rasanya seperti pertama kali makan durian, nagih cuy,,,!

Pernah suatu ketika, saya lagi nongkrong di sebuah kafe. Setelah duduk dan buka laptop, saya mulai deh searching target dengan metasploit. Nah disinilah saya mendapat file "menarik". Tidak hanya melihat, saya kemudian membuat orang itu panik dengan melakukan shutdown with message "**Hai cantik, video kamu asik"**.

Pada suatu saat, saya pernah magang di sebuah perusahaan Mining Contractor. Pada suatu hari, saya ngehack web portal tempat saya magang (Mining contractor). Nah karena sebuah tindakan bloop yang saya lakukan, kelakuan saya ini ke gap. Tentunya saya tau dan lumayan deg deg an, apalagi nggak lama kemudian saya dipanggil ke HO. Wah kena deh nih. Disidang deh saya. Itu pikiran saya saat disuruh menghadap. Tapi ternyata pikiran saya meleset jauh. Saya malah disuruh presentasi didepan owner. Setelah itu, saya malah ditawari pekerjaan disana. Alhamdulillah kan, belum lulus sekolah udah langsung kerja. Dari situlah akhirnya, saya mendapat tugas mulia dari sekolah untuk mengajar cyber security adek-adek yunior. Dan dari situlah kecintaan saya pada dunia Security makin menjadi. Apalagi setelah kenal sama om Bimo, dan dikenalkan dengan komunitas NgeSEC. Saya makin nakal jadinya, tapi positif lho. Selain pengalaman diatas, Skill yang unik, butuh rasa penasaran yang tinggi untuk cari "lobang" serta effort luar biasa biasa untuk mengerti dan memanfaatkan merupakan hal yang membuat saya tertarik dunia IT, khususnya Security. Dari security akhirnya saya mengerti akan arti sabar.

Pengalaman yang Tak terlupakan

Mendengar kata security sekilas terbayang seperti mantan maling yang jadi polisi dan Tetap mencari lubang unik untuk dieksekusi. Banyak hal yang menarik dan saya temukan ketika sudah masuk di dunia security, dari perubahan pola pikir, iseng yang intelektual (istilah ini diberikan oleh guru saya) serta ilmu yang jarang orang bisa. Jika anda mau belajar security cukup bermodal kegigihan dan membangun logika yang kuat dengan belajar *basic hardware, logic programming dan networking* kemudian tentunya belajar bukan hanya teori namun learn by doing is the best way. Berbagai pengalaman menarik dan lucu yang terjadi dalam hidup saya diseputaran IT Security yaitu :

1. Isengin teman ketika main game di lab.komputer. Ini terjadi saat awal-awal belajar hacking dengan menggunakan metasploit. Ketika udah bisa pakai metasploit dan windows XP masih menjadi OS andalan saat itu, dengan mudah saya isengin teman yang asik masih dota. Satu-satu saya *hack* komputernya dan *shutdown with message*, apa yang terjadi? seketika mereka teriak "aseeeemmm", hahaha.
2. Iseng yang membawa berkah. ini cerita ketika magang di sebuah perusahaan pertambangan batubara. Awalnya berjalan dengan biasa aja namun ketika itu saya sedang belajar *web hacking* dan saya menemukan potensi SQLi pada web portalnya sehingga dengan polos saya meminta ijin ke supervisor untuk mencoba meretasnya. Alhamdulillah karena supervisor saya juga penasaran sehingga beliau mengijinkan dan membackup saya. Dengan percaya diri saya retas web itu dan hingga sampai ke rooting dan tidak berhenti pada root di web server itu saja namun saya mencoba dengan meretas server yang terhubung dengan web server itu. Alhasil 5 server critical saya takeover. Ya karena saya masih cupu sehingga saya masih meninggalkan jejak dan dengan mudah mereka trace di log dan dapatkan IP site saya. Terjadilah investigasi dan akhirnya saya mengaku. Langsung pada saat itu juga saya disuruh ke jakarta. Woh., perasaan pada waktu itu campur aduk antara takut, khawatir, dsb. Mengingat saya itu magang dan takut dipulangkam. Oiya waktu itu saya magang penempatan di Kaltim. Keesokan paginya saya berangkat ke jakarta. Benar saja, sesampainya di jakarta saya langsung ketemu manager IT dan langsung diinterrogasi tentang motive kenapa saya melakukan itu dan bagaimana caranya. Saya bercerita panjang lebar dan dengan perasaan pasrah saja. Ternyata beliau menghendaki untuk saya presentasi dihadapan owner dan petinggi-petinggi lainnya. Setelah melewati presentasi yang cukup melelahkan batin karena banyak sekali pertanyaan yang menurut saya cukup kritis dimana waktu itu masih saya masih newbee, ya saya jawab saja sebisanya (hahaha), saya langsung dipanggil oleh manager IT di sebuah ruangan yang kemungkinan ruangan itu memang diperuntukkan untuk interview, dan saya langsung ditembak mau tidak kerja disini, woo dengan semangat 45 dan lantang saya menjawab "mau banget Pak". Namun kerjaan saya waktu itu menjadi *IT Representatif Site* dengan tambahan tugas sebagai security analyst. Senang sekali rasanya. Dan ternyata benar kata guru saya bahwa : "jangan jadi orang yang hanya mempunyai pengetahuan yang bisa namun jadilah spesialis karena tenaga ahli masih sangat kurang

dan menjadi potensial." Begitulah pesan dan wejangan yang masih saya ingat hingga saat ini.

3. Iseng di cafe yang membuat saya lebih sadar akan *security awareness*. Cafe atau angkringan yang tempatnya enak dan terdapat wifi masih menjadi ciri khas tongkrongan mahasiswa yang ekonomis untuk mengerjakan tugas di daerah samarinda. Dan disitulah saya selalu nongkrong juga. Bukan untuk mengerjakan tugas atau sebagai *co-working* namun untuk melampiaskan keisengan saya yang berlebihan dengan mencari file yang menarik tentunya. Dibantu dengan metasploit dengan mudah saya menyelinap masuk ke komputer korban dan berselancar asik bak mencari file di windows explorer. Banyak yang saya dapat dari file dengan nama *password.txt* hingga foto dan video yang harusnya itu privasi. :p

Kalau ditanya cita-cita yang belum tercapai di bidang IT Security adalah mengikuti sertifikasi CEH,OSCP,dll karena sertifikasi itu duit yang dibutuhkan aduhai mahal jadi tetap berharap dan mencari sponsor untuk ikut sertifikasi (curcol dikit ya,,hahaha). Maklum ya motivasi ini ada karena saya selalu sedih ketika ada project yang mengharuskan punya sertifikasi IT Security dan saya tidak ada, akhirnya project berlalu begitu saja.

Hacker dan Satpam Server

Kalau bicara tentang satpam, orang akan ngomongin maling dan siskamling. Kalau satpam server, maka banyak yang menghubungkan sama hacker. Sebenarnya nggak gitu juga sih. Menurut saya Hacker adalah orang yang banyak akal dan bisa mengakali sistem. Dia masuk seperti semut yang se bisa mungkin menyelinap tanpa ketahuan untuk mengintip sedikit informasi yang asik. Itu kalau masuknya lewat system. Akan berbeda dengan yang namanya hardware hacking atau open hardware. Sebuah kegiatan yang butuh banyak modal dan kecerdasan untuk masalah oprek mengoprek. Namun, hanya orang yang bener-bener "selo" waktunya yang melakukan itu.

Hacker adalah istilah yang simple yang diberikan pada orang yang fokus pada dunia security dan lebih familier dan pada umumnya sebutan ini diberikan kepada orang yang bisa meretas situs maupun sesuatu yang online seperti mengakali system ataupun pengamanan yang dibangun bak semut yang mencari lubang dan kemudian masuk untuk mengintip atau mengambil sesuatu yang bermanfaat tanpa disadari oleh pemiliknya. Jadi membayangkan adegan di film yang saya suka berjudul Firewall yang dimana musuhnya sampai mencari informasi di bak sampah dan kemudian mendapatkan info



password disebuah sobekan dokumen, kemudian mengelabui satpam untuk bisa masuk ke kantornya dan meretas data center. Belakangan ini orang dan media masih salah kaprah menggunakan istilah hacker dimana hacker selalu dipakai untuk oknum yang melakukan kejahatan yang merugikan padahal ada 2 istilah yaitu Hacker dan Cracker. Hacker sendiri mempunyai arti membangun yang bisa diartikan pula seseorang yang membangun system kemudian mencoba meretasnya dan dari sisi internal memperbaiki dimana terdapat security hole. Dan Cracker artinya merusak dengan tujuan menjatuhkan atau tujuan tertentu.

Meski hobi banget sama yang namanya komputer, ada juga lho bidang yang bikin saya mual *kalau* disuruh menghadapinya. Programing dan bikin aplikasi, paling tidak bisa. Jadi programing bukan cita cita saya. Cita cita terbesar saat ini adalah bisa ambil sertifikasi CEH dan OSCP. Mahal coiiiiiii #nunggu sponsor yang baik hati :D. Makanya saya juga bergabung dengan komunitas IT. Siapa tahu bisa nemu sponsor.

Dunia *cyber security* tak lepas dengan namanya open source dimana dari open source-lah terlahir tools yang keren. Saya sendiri belajar dari OS dan tools yang open source seperti : Backtrack (sebelum namanya berganti dengan Kali Linux), nmap, metasploit, SQLMaps,dsb.

Saya selalu berpikir bagaimana orang bisa menciptakan OS dan membagikan tools yang mereka buat sendiri dengan cuma-cuma. Disini terbukti dedikasi

yang sangat tinggi untuk orang-orang yang berkontribusi di open source. Satu kata yang bisa saya ungkapkan pada mereka adalah Genius. Pengen rasanya bisa seperti mereka namun sayang saat ini otak dan waktu masih belum mengijinkan saya untuk beranjak mempelajari akan hal itu.

Sama halnya dengan belajar hardware hacking, woh butuh *effort*, banyak belajar seperti elektronika dasar, bahasa *assembly*, dsb serta yang utama adalah modal yang cukup untuk beli hardwarenya kemudian hanya orang yang punya waktu "selo" yang bisa oprek hardware.

Pemerintah dalam hal dukungan *open source* di Indonesia masih belum bergaung keras dan bisa dikatakan belum mendukung secara penuh. Dengan bukti dikalangan pemerintahan sendiri masih menggunakan produk yang berlisensi seperti Microsoft Windows padahal ada banyak distro OS *open source* yang diciptakan oleh masyarakat Indonesia sendiri. Harapannya kedepan pemerintah dapat mensupport secara nyata dan mengapresiasinya dengan cara menggunakan OS *open source* Indonesia dan menghidupkan komunitas serta dapat membantu secara materiil untuk komunitas atau pegiat di *open source*.

Menemukan komunitas yang hits dan tidak ada matinya

Bericara tentang komunitas ternyata sudah banyak komunitas IT berkembang pesat di Indonesia terlebih sekarang Indonesia menyambut industri 4.0 dimana komunitas IT security mulai muncul dipermukaan dan mengambil bagian dari fungsinya. Bagus namun masih dianak-tirikan itulah ungkapan yang bisa saya gambarkan untuk komunitas IT security. Melaporkan kerentanan tapi terkadang mendapat respon yang menyedihkan. Jika pemerintah lebih peka dan terbuka, di dalam komunitas tersebut banyak potensi yang dapat digali bak simbiosis mutualisme, kerja sama yang epic antara komunitas dan pemerintah dapat terjalin. Dan itulah harapan saya ke pemerintah yaitu keterbukaan pemerintah dan menerima komunitas yang unik ini kemudian bersinergi untuk membangun Indonesia maju dan tetap dalam konteks profesional dalam bekerja sama. Bukan hanya pemerintah dengan komunitas saja yang saling kerja sama namun antar komunitas perlu dijaga komunikasinya sehingga dapat saling sharing ilmu dan informasi secara cepat.

Namun kemudian saya menemukan komunitas hits dan tidak ada matinya. NgeSEC, begitulah nama komunitas tersebut. Jangan berpikir negatif dulu ketika mendengar nama komunitas itu. Komunitas tersebut bukanlah komunitas yang suka dengan film vulgar lho namun itu mempunyai kepanjangan yaitu Nge-

Lab & Ngerumpi Security.. Awal saya mengenal komunitas itu ketika bertemu dengan om *bimosaurus* pada saat meeting dan setelah meeting kami ngobrol dan kita mempunyai hobi yang sama di bidang cyber security sehingga beliau mengajak untuk join di komunitas NgeSEC. Ditambah pula bertemu dengan om *djenova* di gamatechno ketika event jagongan IT yang pada saat itu beliau menjadi narasumber. Dari komunitas itulah saya lebih mendalamai pengetahuan di bidang *cyber security*. Di dalam komunitas tersebut saya bertemu orang-orang hebat yang mempunyai good personality dan low profile dimana orang-orang tersebut membagikan ilmunya dengan gratis dan tanpa meminta imbalan serta mempunyai rasa kekeluargaan yang cukup tinggi. Luar biasa pokoknya.



Di Indonesia sendiri, menurut saya, komunitas IT itu sangat luar biasa banyaknya. Sayangnya tidak terkoordinir dengan baik, terutama oleh pemerintah. Andai saja pemerintah lebih aware dengan komunitas komunitas ini, mungkin akan berbeda hasilnya. Akan lebih terasa lah manfaatnya. Terhadap dunia security Indonesia saat ini saya mengharapkan Bersatunya para komunitas dan pegiat IT untuk berbagi ilmu dan sambutan hangat dari pemerintah dengan terjalinnya kerjasama yang epik dan saling menguntungkan. Hacker juga butuh makan dan hidup jadi tidak hanya butuh 2M (Makasih Mas). Tetapi juga jangan mau ya kalau dimanfaatkan orang yang hanya *money oriented* saja, tanpa memikirkan kemajuan IT khususnya dibidang security. Harapan untuk security di dunia adalah tidak melulu berpikir tentang materi yang kita dapat di dunia security ini namun semoga ada banyak orang yang peduli akan perkembangan dan mau berbagi ilmu serta "*don't do stupid think*", karena jika dilihat saat ini security di dunia masih dimanfaatkan orang yang berduit untuk menjatuhkan reputasi atau merugikan seseorang demi kepentingan pribadinya

Nah saya rasa, Itu saja cukup, karena sudah banyak cuap-cuap dan akhir kata selamat tidur.

Profil

1. Nama (real name) : Febrian
2. Panggilan sehari hari : Febri atau Rian atau bayi tabung atau unyil
3. Handle/nick : cyberbean
4. Tempat/Tanggal lahir : Desa kecil di Jateng dengan ultah yang dirayakan sedunia
5. Alamat : Baru aja hijrah dari desa ke kota istimewa
6. Handle origin : Masih bangga jadi orang Indonesia
7. Urls : sedang membuat web tunggu tanggal publishnya ya
8. Computers spec :
 - pertama : Intel celeron P4 RAM 128MB VGA onboard #Menyediakan ;(
 - Sekarang : Intel i5 7th Gen RAM 8GB VGA 1GB #Lumayan :p
 - Yang diidamkan : Gak pernah mengidamkan spek tinggi karena gak mungkin beli
9. Member of :
 - Community : NgeSEC (Ngerumpi & Ngelab Security)
 - Projects : Gak ada saya hanya tukang ketik
10. What I like to do? : Minum kopi sambil sharing sambil ketawa guling-guling
11. What I dislike : Ketika dihadapkan pada suatu kondisi tidak bisa berbuat apa-apa
12. Favorite / Kesukaan :
 - Makanan/Foods : Nasi goreng & sayur lodeh buatan bini
 - Minuman/Drinks : Cukup dengan jahe hangat penghangat jiwa
 - Warna/Colours : Biru
 - Jenis/genre Music : Jazz
 - Band / penyanyi : Semua band dan penyanyi jazz
 - Movies/TV : Firewall, Die Hard 4 and Swordfish
 - Books & Authors : CEH 100% - 500% Ilegal, Author S'to
 - Place : Singgasana panas disudut pojok kamar #remote_kerjaan
 - Time : 00.00 tengah malah yang hening sambil main piano
 - Hobby : Berbagi ilmu, jalan-jalan sama anak istri, ngoprek sampai rasa penasaran terpuaskan
 - OS (kenapa?) : Kali linux karena alasan yang masih mainstream "Kerjaan"
 - Software (kenapa?) : SQLMap karena belum bisa move on
 - Bahasa programing : HTML dan PHP



Galuh

Perjalanan Mendalam IT Security

Perkenalkan nama saya Galuh Muhammad Iman Akbar, ini kedua kalinya saya berkontribusi dalam penulisan NgeSec, tahun lalu saya bercerita mengenai pengalaman pertama kali terjun di dunia IT Security dalam tulisan tersebut saya menggunakan nickname Human_Error.

Bercerita mengenai IT security emang tidak ada habis-habisnya selalu saja muncul hal-hal yang baru yang belum diketahui oleh orang banyak, terlebih lagi sekarang Indonesia sudah memasuki revolusi industry 4.0 yang dimana semua orang menggunakan alat komunikasi salah satunya untuk pengiriman data. Sekitar 7 bulan yang lalu saya mengikuti seminar H@dfex (*Hacking and Digital Forensic Exposed*) se-nasional yang di selenggarakan di Hotel Santika Premiere Yogyakarta saya mendapatkan sangat banyak ilmu terutama dalam bidang digital forensic, dan juga mendapatkan banyak teman baru.

Setelah itu selang sekitar 3 bulan saya mengikuti workshop *Capture The Flag* yang diselenggarakan di Universitas Brawijaya, saya mendapatkan ilmu-ilmu baru dalam mengerjakan CTF dan ini sangat berarti buat saya. Selang beberapa bulan tepatnya pada 20 oktober 2018 saya mengikuti lomba CTF yang diselenggarakan oleh Universitas Brawijaya, disini kami dari Universitas Islam Negeri Maulana Malik Ibrahim Malang mengirimkan 2 tim delegasi untuk mengikuti lomba, terdapat sekitar beberapa universitas

di jawa timur juga yang mengikuti lomba tersebut, seperti Institut Teknologi Surabaya, Universitas Brawijaya, Universitas Narotama dan masih banyak lagi. Untuk babak penyisihan di laksanakan secara online, waktu itu saya sempat pesimis di benak saya, apakah saya pantas untuk masuk final? Masuk final saja sudah cukup menurut aku. maka beberapa hari yang lalu saya berusaha secara maksimal dan gigih untuk belajar mengenai CTF. Setelah tiba waktunya kualifikasi saya berusaha secara maksimal dan kami pun membagi tugas masing-masing dari tim kami untuk menyelesaikan soal CTF jeopardy. Selang beberapa jam kami sudah bisa menyelesaikan soal-soal yang di beri panitia, dan soal-soal tersebut beragam ada yang gampang, sedang, dan sulit.

Setelah waktu selesai seluruh tim yang mengikuti lomba CTF harus membuat sebuah *WriteUp* ibarat langkah-langkah yang terperinci dalam mengerjakan setiap soal yang diberikan hingga menemukan sebuah flag, setelah itu kami pun mengirimkan laporan tersebut ke panitia. Selang 2-3 hari kami pun mendapat pesan bahwa kami berhak untuk masuk ke final, dan disitu saya sangat bersyukur sekali, ternyata saya berhak untuk masuk ke final dan oleh panitia memberitahukan final akan dilaksanakan pada 18 November 2018.

Beberapa hari sebelum saya memasuki final, saya sudah menyiapkan semuanya dengan lumayan matang baik itu psikis dan mental. Hal ini yang sangat menyenangkan dan juga menegangkan, dimana hal yang menyenangkannya bisa melihat muka-muka orang yang biasanya kenal di sosial media akhirnya kelihatan juga rupa-rupanya pada waktu final itu wokwokwok, dan hal yang menegangkan kita harus bersaing antara satu dengan yang lainnya untuk memperebutkan gelar juara 1,2, dan 3. Yang masuk final ada dari Universitas Brawijaya, Institut Teknologi Surabaya, Universitas Narotama, dan dari Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Persaingan sangat sengit dari awal sampai akhir perlomba, dibeberapa jam UIN pernah menduduki posisi 1 dalam scoreboard tapi lama kelamaan disusul oleh yang lain sehingga UIN menduduki posisi ke-3 hingga akhir perlomba, setelah perlombaan berakhir semua tim wajib mengumpulkan *WriteUp* kepada panitia. Dan setelah itu kami di berikan nasi kotak Assikkkk :v. Setelah itu kami pun langsung balik ke rumah masing-masing, dan berharap semoga kami yang mendapatkan juara, untuk pengumuman juaranya akan diberikan pada saat malam Exhibition & Awarding Night.

Pada hari H nya saya bersama temen saya yang bernama mas Adib

berangkat ke award night tersebut, sedangkan untuk temen saya mas Naufal tidak dapat mengikuti acara tersebut di karenakan mempunyai acara lain yang tidak bisa ditinggalkan. Setelah sampai disana saya melakukan registrasi dulu, dan mendengarkan beberapa sambutan, dan di penghujung acara adalah hal yang ditunggu-tunggu oleh banyak orang yaitu pengumuman pemenang lomba karena sangat banyak yang dilombakan pada acara HOLOGY tersebut seperti : *App Innovation, Business IT Case, Business Plan, Smart Device, Game, Capture The Flag, dan Programming*. Ketika pembawa acara membacakan pemenang lomba CTF, saya sangat tidak menyangka dan terkejut, bahwa kami menang pada lomba tersebut dan menduduki peringkat ke 3, dan kemudian kami naik ke podium untuk mendapatkan plakat dan hadiah berupa uang.



Saya yang memegang plakat dan disebelah saya temen saya mas Adib

Event HOLOGY tahun kemarin emang paling berkesan menurut saya pribadi, karena saya mendapatkan banyak pengalaman yang tak terlupakan dan juga teman-teman yang super duper pokoknya *the best* dah...

Setelah itu saya juga mengikuti seminar dan lomba CTF jeopardy dalam acara IDSECCONF (Indonesia IT Security Conference) pada tanggal 1-2 Desember 2018 bertempat di Universitas Muhammadiyah Malang (UMM) Dome, pada acara seminar sangat banyak materi-materi yang dibahas seperti: IoT Security and Hacking, Big Data Security and Hacking, DevOps Security and SOAR, Cloud Computing Security and Hacking, Machine Learing and

Blockchain. Materi yang di bawakan sangat menarik dan ahli dalam bidangnya.

Pada acara tersebut saya ketemu juga sama anak-anak Surabaya Hacker Link (SHL), baik itu yang udah sesepuh, maupun yang masih muda pokoknya mereka semua kerennnn dehh...., Setelah itu tim kami memasuki ruangan yang dimana disana adalah tempat untuk perlombaan CTF dan satu tim maksimal terdiri dari 3 orang. Disana aku sangat gugup bukannya gimana-gimana karena pesertanya hampir semuanya anak SHL, dan bukan main mereka semua sudah pernah mengikuti event Born To Protect yang di adakan oleh KOMINFO. Lomba CTF ini diselenggarakan selama 2 hari onsite (ditempat), soal yang diberikan untuk CTF IDSECCONF tahun 2018 hanya soal berupa Web dan Reversing Engineering (RE). Dihari ke 2 kami memasuki ruang tersebut untuk menyelesaikan soal-soal kemarin yang belum terselesaikan dan ditambah soal-soal yang baru.

Setelah waktu habis kami pun keluar dari ruangan tersebut dan menunggu pengumuman pemenang lomba CTF dari panitia. Dan untuk juara satu jatuh pada anak-anak muda dari Reversing Engineering, juara dua jatuh pada anak-anak muda dari SHL, dan juara 3 jatuh pada mahasiswa dari Universitas Brawijaya.



Lomba CTF IDSECCONF 2018 di hari pertama

Event IDSECCONF 2018 sangat membekas di hati saya pribadi yang dimana saya mendapatkan ilmu yang cukup banyak dan ilmu-ilmu yang pastinya tidak di dapatkan dibangku perkuliahan, terlebih lagi mendapatkan temen-temen baru yang sesuai dengan *passion* itu sangat menyenangkan.



Lomba CTF IDSECCONF 2018 di hari kedua



Penyerahan hadiah bagi para pemenang IDSECCONF 2018

Akhir-akhir tahun 2018 saya mulai belajar mendalami mengenai bug bounty, memang membutuhkan proses yang cukup lama, harus setahap demi setahap mulai dari membaca Open Web Application Security Project (OWASP), dan membaca Write Up bug bounty. Semua itu butuh proses, tidak ada yang instan. Percayalah semua akan indah pada waktunya ☺

Nama : Galuh Muhammad Iman Akbar

Fakultas : Sains dan Teknologi

Jurusan : Teknik Informatika

Loader

[HTTP://2-DESIGN.DEVIANTART.COM](http://2-design.deviantart.com)
[HTTP://2-DESIGN.DEVIANTART.COM](http://2-design.deviantart.com)

“Keep learn and share”

Hallo semua, perkenalkan namaku loader13, lahir pada tanggal 13 oktober 1998. Pada saat ini aku sedang menjadi mahasiswa tingkat akhir disalah satu sebuah perguruan tinggi swasta. Kalau ada yang tau, namanya Institut Teknologi Del. jurusan yang sedang saya geluti saat ini adalah Teknik Komputer. Sebelum mengenal dunia siber aku hanya seorang penggelut game onlen yang hobinya ngecet :v, dan sering menghabiskan waktu diwarnet.

Semua bermula ketika aku menjadi Maba (mahasiswa baru) dikampus ITDel. Dikampusku setiap Maba akan diperkenalkan dengan yang namanya UKM-UKM (unit kegiatan mahasiswa) yang ada dikampus. Tiba saatnya ketika sebuah UKM diberi waktu untuk memperkenalkan UKMnya, sebut saja namanya di cyber army :v. Dalam kesempatan itu, para senior anggota UKM itu memperkenalkan diri secara singkat. Mereka juga memperkenalkan dunia siber (network security, dll). Sebagian besar Maba langsung tertarik ketika mendengar penjelasan demi penjelasan mengenai dunia siber.

Tidak lama setelah kegiatan pengenalan itu, ternyata UKM yang menggeluti dunia siber tadi mengadakan workshop dengan topik “Hacking Kipotrix Server”. Begitu mengetahui hal tersebut, aku mengajak beberapa teman untuk mendaftar pada kegiatan workshop tersebut. Bayar cuy 50k :v. *But it's okay, knowledge is more important.*

Tiba hari workshop, kami hadir dengan semangat. Kami belajar step by step untuk melakukan penyerangan. Tetapi masih terlalu sulit kami pahami. Maklumlah, kami masih awam wkwk. Pada saat melakukan *hacking* kami melakukan setiap langkah menggunakan konsep *etikal hacking*. Saat memasuki tahapan *maintaining access*, hampir semua Maba yang ikut pada kegiatan workshop tidak ada yang berhasil untuk melakukan *privileges escalation*. Entah kenapa hanya saya yang berhasil (bangga sedikit) :v. Akibat waktu yang telah disediakan sudah habis, akhirnya workshop diakhiri, walaupun belum semua tahapan selesai. Kemudian, salah satu anggota UKM senior Bang Bernal, memberikan kesempatan pada saya untuk melanjutkan ketahapan *hacking* selanjutnya, yaitu *covering tracks*. Beliau menyuruh saya, untuk menentukan jadwal untuk kami. Yes, saya mendapat akses VIP :v dan bisa melanjutkan tahapan yang belum terselesaikan.

Apa yang terjadi ternyata tidak sesuai ekspektasi. Setelah mencoba beberapa kali mengirim email pada senior untuk mengingatkan jadwal dan janji tersebut, ternyata aku di PHPin :(. Setelah berlama-lama kecewa, akhirnya aku memutuskan untuk mencari buku yang related dengan topik yang kami bahas. Kebetulan setelah mencari di perpustakaan kampus, aku menemukan buku yang membahas topik yang sama (hmmm ternyata ada bukunya toh :v). Tanpa pikir panjang aku langsung memutuskan untuk explore sendiri. Dari pada berharap sama yang gak pasti. Inilah yang menjadi pengalaman pertamaku dalam dunia siber.

Bergabung dengan IBT

Cerita selanjutnya adalah moment yang menentukan. Saya baru tahu bahwa ternyata dikampus kami ada sebuah komunitas yang bernama Indonesian Backtrack Team, yang juga merupakan penggiat dunia siber. Kebetulan mereka juga mengadakan workshop yang pembicaranya adalah Ketua Umum Indonesian Backtrack Team, Bang Dimas Kusuma. Bang Dimas menampilkan topik “Ransomware”. Namun yang menjadi inti pentingnya adalah, setelah workshop IBT sub regional Tobasa mengadakan recruitment (kebetulan pengurusnya mahasiswa itdel). Aku dan beberapa temanku langsung mendaftarkan diri tanpa perlu mikir lama-lama. Secara pribadi, aku benar-benar mempersiapkan diri dengan baik. Tiba-tiba hari test, ternyata semua soal yang diujikan sudah kupersiapkan dan pelajari. Dan akupun lolos untuk bergabung menjadi anggota IBT sub regional Tobasa.

Setelah bergabung dengan IBT aku memang belum bisa langsung menjadi seorang yang pro. Tapi didalam komunitas ini aku belajar banyak. Kebetulan ada senior yang begitu baik selalu membimbing dan mensupport apa yang kulakukan. Sebut saja namanya Dragz. Selain itu, di komunitas aku memiliki banyak teman yang bisa diajak kerja sama seperti Babiboo, Zleetch, dll.

Selang beberapa waktu aku dan teman-teman yang baru bergabung sering mengikuti kompetisi (*Capture The Flag*). Walaupun belum berhasil mendapatkan prestasi, setidaknya ada niat dan kemauan kami untuk bisa lebih baik lagi. Untuk media belajar sendiri aku sering menggunakan platform dalam maupun luar negeri seperti *shelterlabs*, *root-me*, *ctfs.me*, *vulnhub*, *picoCTF*, *liveoverflow*, dll. Kebetulan aku juga dipercayai untuk memimpin komunitas IBT sub regional Tobasa. Masa jabatanku diakhiri dengan sebuah prestasi (mungkin hanya kebanggaan pribadi sih), kami mengikuti kompetisi yang diakan kominfo dan xynexis namanya Born To Protect (BTP) dan berhasil lolos untuk mengikuti Digital Camp. Mungkin ini pengalaman pertamaku bisa berhasil sejauh ini, dan disana aku bertemu dengan orang-orang yang kuanggap sudah pro dibidang siber. Pada acara digitalcamp kami dipersiapkan untuk mengikuti ujian sertifikasi (*Certified Network Defender*). Beruntungnya lagi kami mendapatkan pembicara yang sangat hebat, sebut saja namanya Om Belly dan Kak Aan. Setiap materi yang diberikan sangat mudah untuk dipahami.

Pada saat *digitalcamp* kami mengadakan *weekend challenge*. Kegiatan ini juga merupakan pengalaman pertamaku untuk melakukan pentest live target. Berhubung ini pengalaman pertama, aku sendiri sedikit kebingungan. Namun stelah mencoba memaksakan diri dengan melakukan googling akhirnya aku berhasil mendapatkan akses shell menggunakan celah *druppageddon2*.

Selanjutnya tibalah saatnya untuk melakukan ujian sertifikasi. Sebelumnya kami sudah diberikan kisi-kisi. Beruntungnya aku pribadi berhasil mendapatkan top 10 setelah melakukan ujian dan menerima hadiah laptop. Yang paling penting aku bisa menambah relasi dengan teman-teman yang berasal dari tempat yang berbeda denganku. Sekarang aku juga sudah menjadi mahasiswa tingkat akhir yang masih juga tertarik dengan dunia siber karena judul Tugas Akhir yang aku ambil adalah

“Analysis of SIEM Implementation in Open Source SIEM Tools Study Case: Wazuh and OSSIM (Alien Vault)”. Dan aku juga memiliki junior-

junior (kylex, difnet,dll) yang kuberi harapan besar untuk bisa memajukan komunitas kami ini untuk menjadi lebih baik dan berguna kedepannya.



Mungkin sekian yang bisa saya ceritakan tentang pengalaman pribadi saya mengenal dunia siber. Bagi yang sudah membaca cerita ini saya mengucapkan terima kasih banyak. Jika ada perkataan maupun penyampaian saya yang kurang berkenan, saya mohon maaf.

"The quieter you become, the more you can hear"

PataKa

Desoxyribonucleic acid (DNA) is a nucleic acid that contains the genetic instructions used in the development and functioning of known living organisms, and serves as a template for their replication. DNA molecules are the long chains of nucleotides that store information. DNA is often compared to a set of blueprints or a recipe. After being transcribed, DNA provides the instructions needed to construct other macromolecules, such as proteins and RNA molecules. The DNA sequences that carry this genetic information are called genes, but other DNA sequences have structural purposes, or are involved in regulating the use of genetic information.

Chemically, DNA consists of two long polymers of simple units called nucleotides, with a backbone of sugars and phosphate groups joined by ester bonds. These two strands are oriented in opposite directions to each other and are therefore antiparallel. After being transcribed, sugar is one of four types of molecules found in DNA, it is the sequence of these four bases along the backbone that encodes information. This information is read using the genetic code, which specifies the sequence of the amino acids within proteins. The code is read by copying stretches of DNA into the related template strand RNA, in a process called transcription.

Within cells, DNA is organized into long structures called chromosomes. These chromosomes are duplicated before cells divide, in a process called DNA replication. Eukaryotic organisms (animal, plants, fungi), and protists) store most of their DNA inside the cell nucleus and some of their DNA in organelles, such as mitochondria and chloroplasts. [1] In contrast, prokaryotes (bacteria and archaea) store their DNA only in the cytoplasm. Within the chromosomes, chromatin proteins such as histones compact and organize DNA. These compact structures include the interaction between DNA and other proteins, helping control which parts of the DNA are transcribed.

DNA exists in many possible conformations that include the A-DNA, B-DNA, and Z-DNA forms, although only A-DNA and B-DNA have been directly observed in living organisms.^[2] The conformation of DNA sequence and the hydration level, DNA sequence, the amount and direction of supercoiling, chemical modifications of the bases, the type and concentration of metal ions, as well as the presence of polyamines in solution,^[29]

The first published reports of A-DNA X-ray diffraction patterns were from DNA used analyses based on paracrystalline DNA. The results provided only a limited information for oriented fibres of DNA. The orientation for oriented fibres of DNA was then proposed by the *in vivo* B-DNA X-ray analysis of highly hydrated DNA in the journal *Watson and Crick presented their molecular modelling analysis of the DNA X-ray diffraction patterns to suggest that the structure was a right-handed helix with a zig-zag pattern*.^[32] In the same journal, Watson and Crick presented their molecular modelling analysis of the DNA X-ray diffraction patterns to suggest that the structure was a right-handed helix with a zig-zag pattern.^[32]

Although the "B-DNA form" is most common under the conditions found in cells, it is not a well-defined conformation but a family of related DNA conformations^[34] that occur at the high hydration environment in living cells. Their corresponding X-ray diffraction and scattering patterns are characteristic of disordered^{[35][36]}

Compared to B-DNA, the A-DNA form is a wider right-handed spiral, with a shallow, wide minor groove and a deeper, deeper major groove. The A form occurs under non-physiological conditions. The A form dehydrated samples of DNA, while in the cell it may be produced in living through of DNA and RNA strands, Segments of DNA which are bound to proteins, such as in enzyme-DNA complexes,^{[37][38]} chemically modified DNA bases have been shown to undergo a large change in conformation and adopt the Z form.^[39]

Berpetualang dan Berprofesi di Dunia IT Security



Sorang kawan senior dulu pernah berkata “**kalau cari pekerjaan, pilih yang kamu sukai saja**”. Kelak di kemudian hari saya baru paham maksud sebenarnya dari kalimat tersebut. Pertama kali bekerja – dalam arti menghasilkan uang sendiri, dimulai ketika masih SMP. Hasil dari hobi merakit aneka perangkat elektronik bergeser menjadi jasa menyelesaikan tugas keterampilan elektronika untuk kawan-kawan yang “kurang ahli”. Tidak lama jasa tersebut meningkat, menerima pesanan perakitan power supply, VOX mic, echo, hingga antena radio amatir. Ketika itu, sedang trend “geng radio gelap lokal” alias tak berijin.

Pekerjaan saya berikutnya adalah *trainer Search And Rescue (SAR)*, gara-gara hobi *Caving* (penelusuran gua) dan menjadi aktivis Pecinta Alam. Suatu pengetahuan dan keterampilan yang kelak ternyata akan sangat berguna – khususnya dalam hal disiplin, manajemen dan kemampuan mengelola situasi darurat yang kemudian digabungkan dengan keahlian IT.

Ketika saya bergabung di Yayasan Air Putih sebagai relawan IT dan Internet di Aceh pasca bencana tsunami, saya sengaja merekrut relawan yang diutamakan punya kualifikasi SAR dan Pecinta Alam – mengingat tantangan kondisi serba terbatas pada saat itu. Terbukti, ketika ada relawan IT yang bergabung tanpa latar belakang SAR dan Pecinta Alam, shock balik kanan pulang ke Jakarta karena tidak sanggup bekerja diantara tumpukan jenazah.

Keterampilan IT, jaringan dan Internet diajarkan sambil jalan langsung di lokasi mulai dari nol. Yang punya hobi elektronika, komunikasi radio berbagi keahlian dengan temannya yang “gaptek total”. Bagaimana merakit antena darurat dari material rongsok, berburu motor butut dan aki bekas untuk catu daya laptop dan VSAT. Atau pointing dish ke satelit dengan meminjam peralatan navigasi Pecinta Alam, peta, kompas, GPS, *klinometer*. Mengajari partner relawan lainnya mendirikan “tower” untuk radio komunikasi ataupun *wireless internet* darurat dengan peralatan seadanya. Dibarter keahlian memasak “mie kembung”. Saya sering menyebut kombinasi keahlian unik berbeda ini sebagai “survival networking”.

Bahkan di malam hari ditambah “kursus bahasa Inggris” dengan tutor relawan juga tetapi lewat *chatting*. Karena sehari-hari harus bergaul dengan relawan manca negara. Relawan dengan “keahlian khusus” ini melanjutkan petualangannya di titik bencana besar lainnya seperti di Nias, Jogja, Mentawai, Tasikmalaya dan lain lain. Bahkan saya berpetualang sampai ke Wasior di Papua. Berlangsung sampai sekarang meski telah berganti generasi ke generasi. Semua menjadi mungkin terjadi karena satu hal yang sama mengikat mereka, yaitu sama-sama mencintai apa yang mereka kerjakan.

Sedangkan awal mula saya sudah bergelut di dunia IT baru dimulai ketika kuliah di Jurusan (Diploma) Komputer yang baru buka di Fakultas MIPA Universitas Brawijaya. Ketika itu lagi trend “komputer cap jangkrik” sebagai “the next thing” bagi para penghobi elektronika dan ternyata “keasyikan” yang dialami di bidang ini sangat menantang. Berburu koleksi aplikasi dan mencobanya menjadi “hobi baru”. Lalu nekat kita membangun sendiri jaringan



dengan komponen yang ketika itu sangat mahal harganya dan juga langka. Untuk mendukung hobi yang mewah itu, saya dan sejumlah kawan patungan membuka usaha persewaan dan juga jasa pengetikan komputer. Modal awal yang disetorkan adalah PC jangkrik masing-masing. Bisnis lalu berkembang menjadi jasa service, jual beli *peripheral* dan perakitan PC, menjual disket hingga tinta, kertas dll. Lalu ketika punya printer laser, nekat buka jasa untuk desain percetakan. Sampai kemudian mulai mengenal layanan BBS dan akhirnya : Internet.

Ketika itu saya juga bekerja sebagai Kepala Teknisi di sebuah toko komputer lokal. Untuk melengkapi dan memperbaharui koleksi aplikasi – tentu saja kebanyakan ‘bajakan’, mesti rajin berburu keluar masuk toko komputer yang punya ‘koleksi’ aplikasi. Ketika itu, saya kemana-mana sudah selalu membawa harddisk untuk meng-copy aplikasi. Suatu hal yang tidak lazim ketika itu ketika semua orang masih menggunakan disket. Maka perburuan itu dengan cepat berujung pada keranjingan langganan layanan *Bulletin Board System* (BBS) – kalau jaman sekarang, BBS itu mirip dengan FORUM seperti KAS-KUS. BBS menawarkan *download* koleksi aplikasi, games, ensiklopedia dll. bagi para pelanggannya. Namun masa jaya BBS tidak bertahan lama karena kemudian Internet masuk ke kota saya, Malang.

ISP pionir yang punya jaringan atau cabang di banyak kota ketika itu adalah Mega Net yang didukung group media terbesar di Jawa Timur yaitu Jawa Pos dan Wasantara Net yang juga anak usaha PT Pos Indonesia. Untuk mengurangi biaya “dial up” yang sangat mahal, saya dan beberapa kawan mempraktekkan teknik “blue box” untuk membajak saluran telepon umum kartu yang kebetulan ditempatkan persis di bawah jendela kamar rumah saya.

Untuk mendapatkan “unlimited access” dial-up ke ISP tanpa dibatasi kuota jam, kami melakukan “trashing”. Nekat pura-pura menjadi teknisi, kemudian menyusup ke kantor-kantor yang diperkirakan punya akun dial up ISP dengan kuota akses yang besar. Seperti di kantor cabang Jawa Pos sendiri, security awareness sangat rendah. Username/password sharing account unlimited yang digunakan bersama untuk keperluan tugas wartawan, ternyata sudah lama diketahui oleh banyak orang tanpa susah payah mengorek informasi.

Sejak saat itu, mindset saya jadi berubah. Pekerjaan yang keren itu adalah menjadi teknisi ISP. Tak terduga, impian itu terwujud tidak lama kemudian. Tahun 1996/1997, Yayasan Widya Caraka Nusantara (YWCN) – satu-satunya ISP dengan lisensi/ijin non komersil untuk pendidikan yang bekerjasama dengan proyek AI3 (Asian Internet Interconnection Initiatives) dari Jepang. YWCN

membuka kantor di Malang dan melayani akses Internet untuk kampus, termasuk almamater saya ITN, UB dan UMM serta sejumlah perguruan tinggi lainnya.

Saya melamar ke YWCN dan diterima sebagai teknisi jaringan. Di tempat inilah sebenarnya belajar tentang Internet dengan “teori dan praktek” yang benar. Bukan hanya pasang kabel dan konfigurasi tapi juga “diwajibkan” membaca referensi dan *manual book* yang tebalnya alaihim gambreng serta dalam bahasa Inggris. Karena orang-orang yang ada di YWCN juga “tukang oprek elektronika” sekaligus “DX-ers gaek” – sebutan untuk penggiat amatir radio, saya juga harus mengulang praktek serta menerapkan etika dengan cara yang benar bukan serampangan ala radio gelap yang semau gue. Aturan batasan power, tenggang rasa dalam pemanfaatan bersama (*frequency sharing*), berlatih teknik instalasi yang rapi dan aman dst.

Beberapa tahun kemudian, YWCN mendapat kiriman perangkat Wireless LAN dari Al3ITB, produk Inggris berjudul Karl Net yang bekerja di frekuensi UHF 900 MHz dengan kapasitas throughput 2 Mbps. *Fantastis* untuk ukuran waktu itu. Tapi tak lama kemudian datang para aparat TNI dari Badan Koordinasi Bantuan Pemantapan Stabilitas Nasional (Bakorstanas) yang menegur dan akan men-segел perangkat karena dianggap mengganggu operator selular GSM XL, frekuensi yang digunakan bertabrakan dan Karl Net belum punya ijin maupun sertifikasi – sebenarnya ketika itu memang belum ada aturan dan standarnya. Kelak, Wireless LAN ini yang menjadi cikal bakal WiFi sebagaimana kita kenal sekarang.

Prestasi fenomenal Karl Net adalah menjadi “backbone” yang menghubungkan YWCN Malang ke YWCN Surabaya via repeater di Gunung Penanjakan, kawasan Taman Nasional Bromo Tengger Semeru TNBTS. Pengalamannya instalasinya “penuh penderitaan”. Memanjat tower milik TNI di subuh buta, mengangkat PC ke “rumah burung” di ujung menara. Jemari kram terkena serangan angin dingin suhu nol derajat karena harus buka sarung tangan untuk mengoperasikan kunci pas mengencangkan mur dan baut. Satu-satunya hiburan hanya masakan “mie kembung” dan “musik dugem” dari Jeep Hardtop yang mengantar. Tetapi pengalamannya itu justru senang hati saya ceritakan kembali, seperti sekarang ini.

Pengalamannya membuktikan, ketika seseorang bekerja karena menyukai apa yang dikerjakan, secara alamiah akan tumbuh kecintaan. Kemudian berlanjut menjadi motivasi personal yang kuat. Orang seperti ini, tidak pernah kehabisan semangat dan kreativitas. Menjadi teladan karena punya dedikasi dan integritas yang lebih baik dibandingkan dengan pekerja lainnya. Mungkin ada jeda ketika



dia perlu beristirahat, tapi pada akhirnya akan selalu kembali.

Inilah yang menurut teori manajemen SDM disebut dengan “passion”, syarat pertama dan utama bagi seorang profesional khususnya di bidang IT security. Kini, setiap kali bertemu orang yang menggeluti profesi ini, saya selalu merasakan suasana antusias dan bergairah. Karena memang tingkat kesulitan dan kerumitan di dunia IT security, menurut saya hanya mungkin ditangani oleh orang yang memiliki “passion”. Mereka yang berpeluang sukses.

Modal berikutnya yang juga akan berperan besar mendukung karir profesional praktisi IT security adalah berjejaring (*peer network*). Aktif dan berkontribusi di tengah komunitas. Di dalam cerita perjalanan saya pribadi di atas, tergambar jelas bagaimana komunitas menjadi “ruang berlatih” dan menambah “jam terbang”. Bahkan update pengetahuan dan ilmu bisa didapatkan cuma-cuma termasuk seringkali juga “bantuan”. Aktivitas non profesional akan membantu anda tetap antusias “ngoprek”, mencoba hal baru, menguji ide dan kreativitas.

Di tengah persahabatan ini “eksistensi” anda mendapatkan pengakuan yang jujur tanpa harus melalui “kompetisi”. Dalam banyak hal, seorang praktisi IT security tabu melakukan “eksposure” karena profesi ini memang jalan sepi. Sebaiknya anda membiasakan diri tidak banyak dikenal, bekerja di belakang layar. “Stay LOW” memberikan kredit poin, prestasi kerja kepada atasan atau orang lain. Kalau pun terpaksa harus muncul di permukaan, adalah sebagai kawan atau dalam rangka melakukan edukasi publik. Tidak memancing permusuhan atau persaingan. Orang yang ingin selalu menonjolkan diri, tidak cocok di profesi ini. Tidak ada yang mau menggunakan jasa “selebritis security” karena

pasti musuh yang iri banyak. Maka resiko keamanan justru akan meningkat bila menyewa praktisi yang semacam ini. Para “pendekar” paling dicari, seperti legenda. Dikenal karyanya, ketimbang pribadinya.

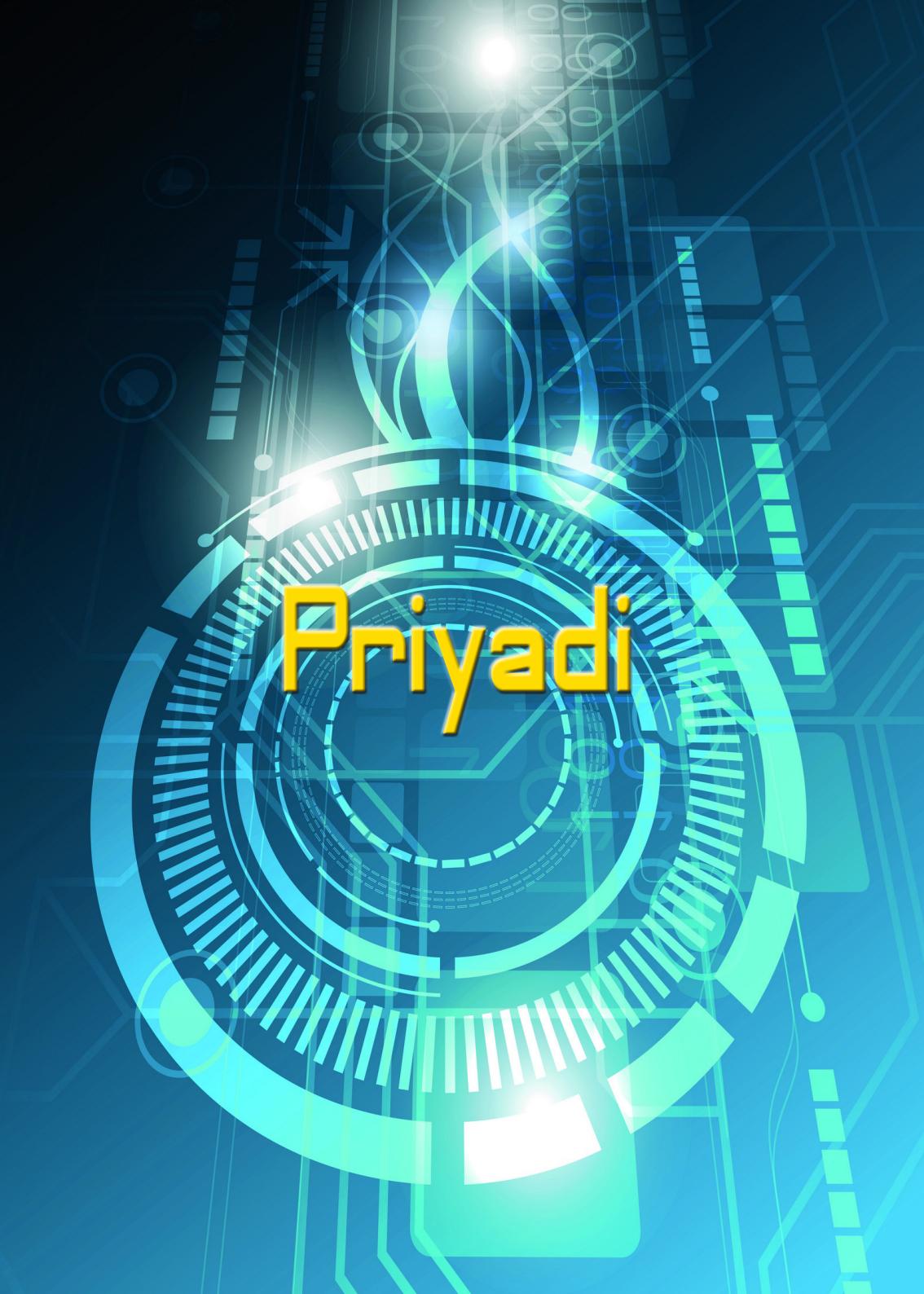
Pada akhirnya, dari komunitas pula jalannya aliran rejeki. Banyak orang yang membutuhkan jasa IT security, tidak mencari dari “bursa kerja” yang terbuka. Mereka lebih mengandalkan “endorsement” – istilah jaman now, dari senior atau “prominent people” yang “establish” dan DIPERCAYA untuk mereferensikan seseorang yang sesuai dengan pekerjaan tersebut.

Di atas segalanya, pergaulan di komunitas IT security dilandasi oleh rasa saling percaya yang terbentuk karena relasi sosial dan interpersonal yang intensif. Bahkan seperti keluargaan.

Punya CV dan portofolio serta track record yang bagus dan sempurna, tentu saja sangat penting di dunia profesional. Tetapi di IT security, ribuan orang memiliki sertifikasi serupa atau bahkan lebih mentereng, bergengsi. Ketika membaca CV, semua orang akan tampak sama. Yang dicari untuk membedakan mereka satu sama lain, adalah reputasi dan jam terbangnya. Keahlian paling impresif, bisa dipelajari. Teknologi mudah dikuasai kalau punya uang, tapi reputasi tidak dapat dibeli atau dipalsukan. Pengalaman juga tidak diajarkan di sekolah yang mana pun. Yang bisa menunjukkan dan meyakinkan reputasi dan pengalaman anda tentu saja adalah senior di komunitas yang mengenal dan mau merekomendasikan.

Ketika saya “direkrut” untuk membentuk, membangun dan menjalankan ID-SIRTII/CC, yang terjadi adalah seperti itu. Beberapa senior di komunitas, “prominent people” memberikan rekomendasi dan memperkenalkan sekaligus memberikan jaminan bedasarkan TRUST.

Di tingkat organisasi regional seperti APCERT dan global di FIRST atau National CSIRT Forum, ID-SIRTII/CC tidak serta merta “diterima” walaupun kami membawa “supporting letter” dari Menteri dan perwakilan Pemerintah RI yang resmi. Baru ketika ada organisasi counterpart yang lebih senior dan telah “established” dan dihormati di komunitas itu, misalnya JPCERT (Jepang) dan MYCERT (Malaysia) mau memberikan “endorsement” untuk ID-SIRTII/CC (atau istilahnya sponsor), pintu mulai terbuka lebar. Sampai kemudian di kawasan ASEAN dan di komunitas OIC (organisasi kerjasama negara islam) ID-SIRTII/CC ditunjuk dan diberikan kepercayaan sebagai mentor untuk program edukasi di kawasan indochina dan Timor Leste. Maka, ketika kepercayaan telah terbentuk, rejeki pun ikut lancar. Terbukti. Cintai yang kamu kerjakan, jangan lupa bersyukur, terus memberi dan bersikap rendah hati.



Priyadi

Pengalaman di Bidang Security



Saya bukan ahli security dalam arti ahli security pada umumnya. Namun pekerjaan menuntut kompetensi dalam bidang security. Jika biasanya seorang ahli security bermula dari sisi ‘penyerang’ saya bermula dari ‘pemain bertahan.’ Pekerjaan membuat saya perlu memikirkan security untuk segala hal yang saya implementasikan di Internet.

Kunci utama sebagai ‘pemain bertahan’ sebenarnya hanya tiga:

1. Update terus menerus,
2. Konfigurasi yang benar,
3. Backup.

Walaupun tentunya di lapangan tidaklah sesederhana itu.

Insiden Serangan Antar Negara

Akhir tahun 1990-an terjadi saling serang antara Indonesia & Portugal mengenai masalah politik Timor Timur. Cracker dari Indonesia menyerang situs-situs Portugal, dan juga sebaliknya, cracker dari Portugal juga menyerang situs-situs Indonesia. Umumnya mereka melakukan deface dalam rangka hacktivism, atau menyelipkan ujaran-ujaran politik pada situs web targetnya.

Pada situasi ini, saya yang mengoperasikan layanan hosting berada di tengah-tengah baku hantam antara kedua belah pihak. Di satu sisi, teman-

teman sebangsa dan senegara banyak yang memiliki akun di server-server yang saya operasikan. Di sisi lain, akun-akun yang saya kelola menjadi target serangan mereka.

Satu server saya pernah menjadi korban deface, karena pihak penyedia jaringan menyambungkan server saya menggunakan hub, karena kebetulan switch yang biasanya dipakai sedang rusak dan menunggu penggantinya. Penyerang berhasil mendapatkan akses root dari server milik pihak lain. Dan karenanya, sniffer yang mereka pasang bisa menjaring banyak akun dari server saya. Jaman dahulu, SSH atau SFTP belum populer, dan kebanyakan pengguna masih menggunakan protokol yang tidak terenkripsi seperti telnet dan FTP. Walaupun demikian, saya selaku admin sudah menggunakan SSH sehingga akses root tidak berhasil mereka dapatkan.

Singkatnya, bukan salah saya, tetapi tetap menjadi tanggung jawab saya. Pekerjaan terbesar saat itu bukan hanya masalah teknis membersihkan server dari deface dan me-restore backup, tetapi yang lebih sulit adalah menangani masalah emosi dari user-user saya. User-user yang menjadi korban cenderung menjadi ofensif dan melibatkan diri dalam pertikaian tersebut. Mereka ikut menyerang situs-situs Portugal karena mereka merasa sudah berada dalam medan pertempuran.

Menurut hemat saya sebenarnya tidak perlu begitu. Masalah keamanan adalah risiko yang perlu dihadapi secara profesional. Kemampuan teknis perlu dibarengi dengan kecerdasan emosi, agar kita tidak dapat fokus pada pekerjaan utama kita dan memperbaiki masalah semampu kita dengan kepala dingin. Penjahat di luar sana akan tetap ada, dan bukan sesuatu yang dapat kita kontrol. Ikut-ikutan menjadi penjahat bukanlah solusi. Kita hanya dapat berusaha untuk meminimalkan efek dari keberadaan mereka.

Pentester Taqlid Buta

Tahun 2016, tim saya mendapat tugas untuk mengelola sistem *super legacy*: sistem operasi keluaran lebih dari satu setengah dasawarsa yang lalu, dengan CMS dengan beberapa celah keamanan, dan yang sudah tidak ada update untuk beberapa tahun. Ditambah bahwa tidak ada yang mengelola sistem tersebut selama bertahun-tahun selain dari tim yang menambah konten.

Lebih buruk lagi, sistem tersebut adalah web server publik dan dimiliki oleh lembaga keuangan yang memiliki standar keamanan yang tinggi.



Karena itu, pihak klien juga menggunakan jasa konsultan keamanan dari pihak ketiga, yang akan mengevaluasi sistem tersebut dari sudut pandang keamanan.

Pendekatan yang kami lakukan adalah melakukan P2V (*physical to virtual*) karena diduga kami akan kesulitan jika sistem operasi keluaran jaman dahulu dipakai menggunakan server bare metal dengan spesifikasi jaman sekarang & tidak ada jaminan CMS bisa berfungsi pada sistem operasi versi terbaru. Selain itu kami memasang *frontend web server* agar sistem *legacy* ini tidak terekspos langsung ke Internet seperti sebelumnya.

Saya menggunakan berbagai macam rule di web server *frontend* untuk mengatasi masalah keamanan yang berhubungan dengan aplikasi, karena tidak mungkin memperbaharui aplikasi tersebut. Informasi didapatkan dari situs-situs *security* dan hal ini tidak sulit dilakukan. Untuk pengelolaan, saya memasang sebuah server VPN dan SSH. Tim pengelola CMS kini harus masuk ke dalam VPN sebelum dapat mengelola konten.

Walaupun implementasinya sedikit sulit, namun semuanya berjalan dengan baik. Masalah justru ada pada ‘tim *security*’ yang dipekerjakan pihak klien. Jadi ‘tim *security*’ ini melakukan analisis sistem kami hanya

dengan cara memasukkan *IP address* kami ke *software scanner* yang mereka gunakan. Jika *software* tersebut melakukan ‘komplain’, maka mereka hanya akan meneruskan ‘komplain’ tersebut ke kami dan pihak klien.

Tim saya menyebutnya ‘pentester taqlid buta’. Salah satu yang dilakukan *software* tersebut sepertinya mengecek versi *software* yang digunakan oleh server. Jika versi *software* yang dideteksi di bawah versi *software* terakhir yang tidak memiliki celah keamanan, maka *scanner* mereka akan ‘komplain’ dan menganggap server kami tidak aman.

Masalahnya di sini adalah bahwa sistem operasi yang kami gunakan, CentOS, melakukan backport perbaikan dari versi terbaru ke versi yang digunakan pada sistem operasi tersebut. Akibatnya *software* tidak menggunakan versi terbaru, walaupun celah keamanan tersebut diperbaiki. Hal ini yang tidak dipahami oleh ‘tim security’ tersebut. Mereka bersikeras bahwa kami harus melakukan update *software* seperti OpenSSH ke versi terbaru secara manual, dan tidak mengandalkan update yang disediakan vendor sistem operasi.

Moral of the story di sini adalah bahwa menjadi profesional di bidang *security* perlu dibarengi dengan pengalaman dan pengetahuan mengenai apa yang terjadi di lapangan. Pengetahuan bagaimana siklus penanganan celah keamanan ditangani oleh vendor sistem operasi adalah hal yang perlu diketahui. Begitu pula pengetahuan mengenai desain arsitektur sistem juga merupakan hal yang wajib diketahui. *Software scanner* hanyalah alat bantu. Tetapi yang lebih penting adalah pengetahuan dari orang-orang yang terkait itu sendiri.



Rootbakan

'Newbie' Bug Bounty Hunter

Sebelum saya mulai menulis sebuah catatan sederhana terkait awal mula saya bermain Bug Bounty dan menjadi seorang **'Newbie' Bug Bounty Hunter** sampai bisa mendapatkan sebuah bug di salah satu sosial media ternama di dunia yaitu Facebook. Izinkan saya menuliskan sedikit list tahapan yang biasa saya gunakan sebelum dan sesudah mencari sebuah bug pada platform penyedia program-program **'Bug Bounty'** atau website yang menyediakan program Bug Bounty, berikut ulasannya:

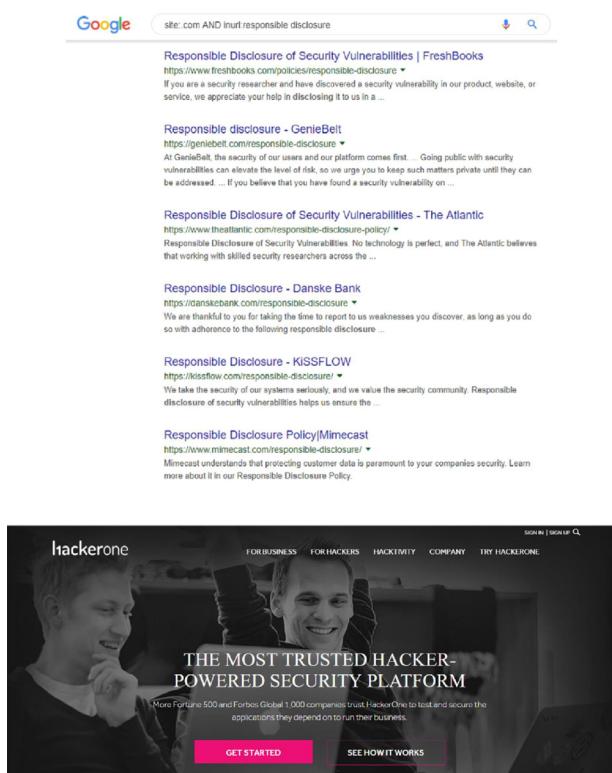
1. *Finding a Target*
2. *Recon a Target*
3. *Creating Report*
4. *Sending Report*
5. *Getting the Bounty*

Hal-hal diatas tidak akan berhasil dilakukan jika kita mengerjakannya tidak dengan tenang. Selain itu, selalu lakukan sesuatu dengan tujuan bahwa dirimu selalu ingin bergerak selangkah lebih maju dari orang lain (*jika mereka bisa kenapa kita tidak*). Kata-kata itu yang selalu menjadi acuan saya dalam memulai sesuatu atau dalam mencari sebuah bug. Jika kita mampu memotivasi diri kita sendiri maka kita juga mampu memotivasi orang lain, percayalah bahwa hal kecil yang kita lakukan jika itu dapat bermanfaat bagi orang lain, maka hal positif yang dapat kau peroleh dalam kehidupanmu akan jauh lebih banyak dari yang orang lain dapatkan. Selalu pegang teguh bahwa rezeki sudah ada yang mengatur dan takkan pernah tertukar (*karena rezeki itu tidak selalu berbentuk uang atau barang*).

Lakukanlah sebuah hal yang ingin kau lakukan dengan sebaik-baiknya sesuai dengan kemampuan yang kau punya, jangan paksakan dirimu untuk menjadi orang lain tapi coba arahkan dirimu untuk bisa mempunyai kemampuan yang setara atau melebihi orang lain. Baiklah tanpa pajang lebar mari kita ulas 5 hal diatas dalam sebuah rangkuman sederhana berikut ini

1. Finding a Target

Pada tahapan ini seorang Bug Hunter akan mencari website atau platform yang menyediakan program Bug Bounty, cara yang dilakukan sangat bervariatif mulai dari menggunakan google dorking, informasi dari sesama rekan bug hunter dan mengunjungi langsgung platform penyedia bug bounty seperti Hackerone, Bugcrowd, Zerocopter, AntiHack, CyberArmyID, RedStrom dan masih banyak lagi



site: com AND inurl responsible disclosure

Responsible Disclosure of Security Vulnerabilities | FreshBooks
<https://www.freshbooks.com/policies/responsible-disclosure> ▾
 If you are a security researcher and have discovered a security vulnerability in our product, website, or service, we appreciate your help in disclosing it to us in a ...

Responsible disclosure - GenieBelt
<https://geniebelt.com/responsible-disclosure> ▾
 At GenieBelt, the security of our users and our platform comes first. Going public with security vulnerabilities can elevate the level of risk, so we urge you to keep such matters private until they can be addressed ... If you believe that you have found a security vulnerability on ...

Responsible Disclosure of Security Vulnerabilities - The Atlantic
<https://www.theatlantic.com/responsible-disclosure-policy/> ▾
 Responsible Disclosure of Security Vulnerabilities. No technology is perfect, and The Atlantic believes that working with skilled security researchers across the ...

Responsible Disclosure - Danske Bank
<https://danskebank.com/responsible-disclosure> ▾
 We are thankful to you for taking the time to report to us weaknesses you discover, as long as you do so with adherence to the following responsible disclosure ...

Responsible Disclosure - KISFLOW
<https://kisflow.com/responsible-disclosure/> ▾
 We take the security of our systems seriously, and we value the security community. Responsible disclosure of security vulnerabilities helps us ensure the ...

Responsible Disclosure Policy|Mimecast
<https://www.mimecast.com/responsible-disclosure/> ▾
 Mimecast understands that protecting customer data is paramount to your companies security. Learn more about it in our Responsible Disclosure Policy.

hackerone

FOR BUSINESS FOR HACKERS HACKTIVITY COMPANY TRY HACKERONE

THE MOST TRUSTED HACKER-POWERED SECURITY PLATFORM

More Fortune 500 and Forbes Global 1,000 companies trust HackerOne to test and secure the applications they depend on to run their business.

GET STARTED SEE HOW IT WORKS



Zerocopter

Features Researchers Pricing Blog Company Demo [Sign Up](#)

Work with Hackers

Zerocopter enables you to confidently leverage the skills of the world's most knowledgeable ethical hackers to secure your applications.

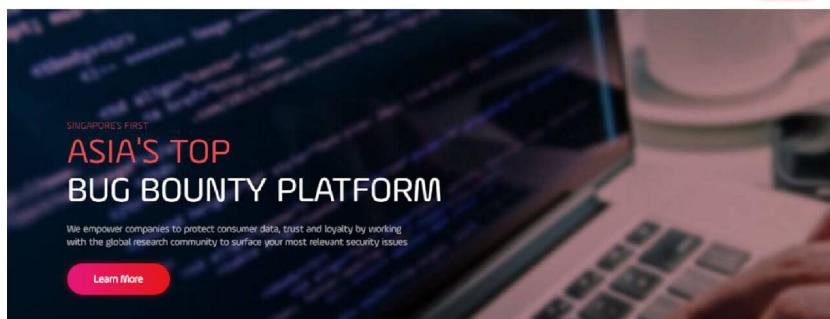
[Start Today](#)

AntiHACK^{.me}

About Us Our Services Our Courses How It Works Programs Email Spoof Checker Contact

Sign In

[Sign Up](#)





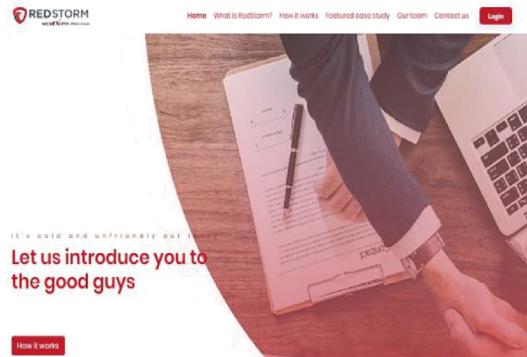
CyberArmy

LAYANAN PROGRAM TENTANG MASUK DAFTAR

#1 CROWDSOURCED CYBER SECURITY PLATFORM IN INDONESIA

Uji Keamanan Aplikasi Bisnis Anda Bersama Bug Hunter Terbaik Disini.

Mulai Sekarang



2. Recon a Target

Setelah mendapatkan salah satu target saya biasa melakukan recon dengan menggunakan beberapa tools berikut ini:

- Recon subdomain

```
root@BUG-BOUNTY:~/TOOLS# knockpy progress28.web.id
```

```
[!] [!] 4.1.1
[!] [!]
[!] [!]
[!] [!]
[!] [!]

+ checking for virustotal subdomains: YES
[
    "www.progress28.web.id"
]
+ checking for wildcard: NO
+ checking for zonetransfer: NO
+ resolving target: YES
- scanning for subdomain...

Ip Address      Status   Type     Domain Name          Server
-----          -----
31.170.161.27  200      host     ftp.progress28.web.id  openresty
```

- Recon file and folder

```
root@BUG-BOUNTY:~/TOOLS# aquatone-discover -d progress28.web.id
[!] discover v0.5.0 - by @michenriksen
Identifying nameservers for progress28.web.id... Done
Using nameservers:
- 31.170.163.241
- 173.192.183.247
- 31.170.164.249
- 31.220.23.1
```

```
root@BUG-BOUNTY:~/TOOLS# knockpy progress28.web.id
```

```
[!] 4.1.1
+ checking for virustotal subdomains: YES
[
    "www.progress28.web.id"
]
+ checking for wildcard: NO
+ checking for zonetransfer: NO
+ resolving target: YES
- scanning for subdomain...
Ip Address      Status  Type   Domain Name          Server
-----  -----  ----  -----
31.170.161.27  200     host   ftp.progress28.web.id  openresty
```

```
root@BUG-BOUNTY:~/TOOLS# aquatone-discover -d progress28.web.id
[!] discover v0.5.0 - by @michenriksen
Identifying nameservers for progress28.web.id... Done
Using nameservers:
- 31.170.163.241
- 173.192.183.247
- 31.170.164.249
- 31.220.23.1
```

- Recon parameter

```
root@BUG-BOUNTY:~/TOOLS/XSStrike# python3.6 xsstrike.py -u http://vulnweb28.hol.es/?tampil=artikel_detail&id=85
[2] 432
root@BUG-BOUNTY:~/TOOLS/XSStrike#
XSStrike v3.1.2

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: tampil
[!] No reflection found
```

```
root@BUG-BOUNTY:~/TOOLS/xsscrappy# ./xsscrappy.py -u http://vulnweb28.hol.es/?tampil=artikel_detail&id=85
[2] 454
root@BUG-BOUNTY:~/TOOLS/xsscrappy# 2019-04-14 12:00:01 [scrapy] INFO: Scrapy 1.1.0rc3 started (bot: xsscrappy)
2019-04-14 12:00:01 [scrapy] INFO: Overridden settings: {'NEWSPIDER_MODULE': 'xsscrappy.spiders', 'DUPEFILTER_CLASS': 'xsscrappy.bloomfilters.BloomURLDupeFilter', 'SPIDER_MODULES': ['xsscrappy.spiders'], 'CONCURRENT_REQUESTS': '30', 'BOT_NAME': 'xsscrappy', 'DOWNLOAD_DELAY': '0'}
2019-04-14 12:00:01 [scrapy] INFO: Enabled extensions:
['scrapy.extensions.logstats.LogStats',
 'scrapy.extensions.telnet.TelnetConsole',
 'scrapy.extensions.corestats.CoreStats']
2019-04-14 12:00:01 [scrapy] INFO: Enabled downloader middlewares:
['xsscrappy.middlewares.InjectedDupsFilter',
 'xsscrappy.middlewares.RandomUserAgentMiddleware',
 'scrapy.downloadermiddlewares.httpauth.HttpAuthMiddleware',
 'scrapy.downloadermiddlewares.downloadtimeout.DownloadTimeoutMiddleware',
 'scrapy.downloadermiddlewares.useragent.UserAgentMiddleware',
 'scrapy.downloadermiddlewares.retry.RetryMiddleware',
 'scrapy.downloadermiddlewares.defaultheaders.DefaultHeadersMiddleware',
 'scrapy.downloadermiddlewares.redirect.MetaRefreshMiddleware',
 'scrapy.downloadermiddlewares.httpcompression.HttpCompressionMiddleware',
 'scrapy.downloadermiddlewares.redirect.RedirectMiddleware',
 'scrapy.downloadermiddlewares.cookies.CookiesMiddleware',
 'scrapy.downloadermiddlewares.chunked.ChunkedTransferMiddleware',
 'scrapy.downloadermiddlewares.stats.DownloaderStats']
2019-04-14 12:00:01 [scrapy] INFO: Enabled spider middlewares:
```

Contents								
Host	Method	URL	Params	Status	Length	MIME type	Title	Comm
http://vulnweb28.hol.es	GET	/		200	4976	HTML	VULNWEB28	
http://vulnweb28.hol.es	GET	?tampil=artikel_detail&id=83	✓	200	29907	HTML	VULNWEB28	
http://vulnweb28.hol.es	GET	?tampil=artikel_detail&id=83	✓	200	4798	HTML	VULNWEB28	
http://vulnweb28.hol.es	GET	?tampil=artikel_detail&id=83	✓	200	5120	HTML	VULNWEB28	
http://vulnweb28.hol.es	GET	?tampil=galeri	✓	200	3258	HTML	VULNWEB28	
http://vulnweb28.hol.es	GET	?tampil=halaman&i=1	✓	200	5612	HTML	VULNWEB28	
http://vulnweb28.hol.es	GET	?tampil=halaman&i=1	✓	200	3798	HTML	VULNWEB28	
http://vulnweb28.hol.es	GET	?tampil=halaman&i=1	✓	200	4004	HTML	VULNWEB28	

Request	Response
<input type="button" value="Raw"/> <input type="button" value="Params"/> <input type="button" value="Headers"/> <input type="button" value="Hex"/>	<pre>GET /?tampil=artikel_detail&id=83 HTTP/1.1 Host: vulnweb28.hol.es Accept-Encoding: gzip, deflate Accept: /* Accept-Language: en User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0) Connection: close Referer: http://vulnweb28.hol.es/?tampil=artikel_detail&id=83 Cookie: PHPSESSID=fedcec8a128f809e3bd06552312cf50</pre>

Not secure | view-source:vulnweb28.hol.es

```
1
2
3 <html>
4 <head>
5 <title>VULNWEB28</title>
6 <link rel="stylesheet" href="css/style.css">
7 <link rel="shortcut icon" href="img/FIX.jpg" />
8 </head>
9 <body>
10 <style type="text/css">
11 body,td,th {
12   font-family: "Times New Roman", Times, serif;
13   font-size: 16px;
14 }
15 </style>
16 <div id="container">
17 <div id="header">
18 
19 </div>
20 <div id="menu">
21 <p>
22
23 <ul class="nav">
24
25   <li><a href="index.php"> HOME </a></li>
26
27   <li><a href="?tampil=halaman&id=78"> HACKING </a></li>
28
29   <li><a href="?tampil=halaman&id=79"> TUTORIAL </a></li>
30
31   <li><a href="?tampil=halaman&id=80"> CHEAT SHEET </a></li>
32
33   <li><a href="?tampil=halaman&id=81"> JAVA </a></li>
34
35   <li><a href="?tampil=galeri"> GALERI </a></li>
36
37   <li><a href="?tampil=kontak"> KONTAK </a></li>
38
39 . . .
```

Recon sendiri berfungsi untuk menemukan bermacam-macam kemungkinan jenis bug, exploit, dan serangan yang mungkin bisa dilakukan oleh seorang bug hunter dari mulai XSS, LFI, RCE, SQL Injection, Bypass Admin, Logic Error, Path Disclosure atau berbagai jenis serangan yang terdapat pada **OWASP Top 10 2017**. Karena dari berbagai testing yang dilakukan baik active, passive, manual maupun auto testing akan menemukan jenis celah keamanan yang berbeda-beda tergantung dari kekuatan tiap website.

3. Creating Report

Hal terpenting lainnya dari melaksanakan kegiatan perburuan bug yaitu pembuatan sebuah laporan, karena laporan yang menarik dan lengkap akan menjadikan nilai lebih pada sebuah temuan seorang bug hunter, semakin lengkap dan terstruktur laporan tersebut akan membuat seorang bug hunter menghasilkan jumlah bounty yang berbeda-beda (

terkadang diberikan bonus) atau terkadang report yang sederhana saja sudah bisa mendapatkan bounty berupa rewards yang besar atau hanya sekedar diberikan swag / goodie, bahkan terkadang report yang lengkap tidak mendapatkan rewards sama sekali melainkan hanya sebuah ucapan '2M'(makasih mas). Berikut beberapa contoh report yang pernah saat buat:



NAMA TEMUAN

11 Desember 2018

Oleh RootBakar

Laporan Bug Bounty Qualitiva | 2

Deskripsi	
URL / Aplikasi	https://qualitiva.id/PT1BYnBaMmJSQjg=PT1BYzY2C0ckx6DE3Yml2NWU3OD.
Dampak	
Langkah-langkah	<ol style="list-style-type: none"> 1. Atta http 2. Tarç 3. Rek 4. Kort
Bukti Temuan	<p>_____</p> <p>_____</p> <p>_____</p> <p style="text-align: center;">Simpan</p> <p style="text-align: center;"><i>Sebelum perubahan</i></p>

Sebuah report biasanya berisikan beberapa poin inti diantaranya **Nama Temuan, Tanggal Temuan, Nama Bug Hunter, Deskripsi Temuan, URL / Aplikasi, Dampak, Langkah-langkah, Bukti Temuan, Remediasi / Rekomendasi** serta **Referensi Temuan**.

Karena semua poin-poin diatas normalnya akan membantu seorang *IT Security* maupun *Developer* pemilik *program* dalam memahami dan mereproduksi ulang serta memperbaiki celah keamanan / bug yang dilaporkan oleh seorang *Bug Hunter*.

4. Sending Report

Setelah laporan dibuat maka seorang bug hunter akan mengirimkan ke email tim *security* (*security@blablabla.com*) atau bahkan hanya sekedar ke email *customer service* yang biasanya akan dilanjutkan ke tim *IT Security* dari pemilik program tersebut, atau mengirimkannya secara langsung pada menu *submitting platform* seperti *Hackerone*, *Bugcrowd*, *AntiHack*, *Zerocopter*, *CyberArmyID* dan *RedStorm* yang sudah menyediakan secara langsung dengan template. Biasanya laporan akan dilihat dan diolah dalam jangka waktu yang berbeda-beda terkadang 2 hari, 5 hari, 7 hari, 14 hari atau bahkan 1 bulan lamanya sampai dengan sebuah bug dilakukan fixing.

- **report**
- **triaged**
- **resolved / fixing**
- **rewards**

5. Getting the Bounty

Ini merupakan sebuah proses yang ditunggu oleh seorang *bug hunter* dan merupakan hal yang paling di nanti-nantikan yaitu pemberian hadiah atau *rewards*. Nantinya jika temuan seorang bug hunter dikatakan *eligible* terhadap sebuah *bounty* maka *rewards* tersebut akan diberikan baik dalam bentuk *uang*, *swag*, *certificate* atau bahkan hanya sebuah ucapan terimakasih (*jangan dongkol hehehehe, insyaallah ada rezeki lain kok*). Hadiah biasa dikirim dan diproses dalam waktu yang berbeda-beda, kadang 2 hari sudah kirim, kadang nunggu sampai 1-2 minggu lamanya atau bahkan 1-2 bulan, semua tergantung kebijakan yang diterapkan oleh perusahaan pemberi bounty dan kebijakan pajak dari masing-masing negara. Biasanya *rewards* yang diperoleh dari luar negeri akan meminta seorang *bug hunter* untuk mengisi dokumen pajak dalam bentuk sebuah formulir **W-8BEN**.

Form W-8BEN (Rev. July 2017) <small>Department of the Treasury Internal Revenue Service</small>	Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding and Reporting (Individuals) • For use by individuals. Entities must use Form W-8BEN-E. • Go to www.irs.gov/FormW8BEN for instructions and the latest information. • Give this form to the withholding agent or payer. Do not send to the IRS.	<small>OMB No. 1545-1621</small>
Do NOT use this form if: <ul style="list-style-type: none"> • You are NOT an individual • You are a U.S. citizen or other U.S. person, including a resident alien individual • You are a beneficial owner claiming that income is effectively connected with the conduct of trade or business within the U.S. (other than personal services) • You are a beneficial owner who is receiving compensation for personal services performed in the United States • You are a person acting as an intermediary 		Instead, use Form: W-8BEN-E W-9 W-8ECI 8233 or W-4 W-8IMY
Note: If you are resident in a FATCA partner jurisdiction (i.e., a Model 1 IGA jurisdiction with reciprocity), certain tax account information may be provided to your jurisdiction of residence.		
Part I Identification of Beneficial Owner (see instructions)		
1 Name of individual who is the beneficial owner ROHOLESI TALAOHU		2 Country of citizenship INDONESIA
3 Permanent residence address (street, apt. or suite no., or rural route). Do not use a P.O. box or in-care-of address.		
City or town, state or province. Include postal code where appropriate.		Country INDONESIA

Berikut ini adalah daftar temuan Bug, Rewards beserta Hall of Fame yang pernah saya dapatkan:

* **Tokopedia**

tokopedia

Sertifikat

Apresiasi

Tokopedia mengucapkan terima kasih atas kerjasama dari

ROHOLESI TALAOHU

yang telah menemukan dan melaporkan *Vulnerability Bug "Blind Stored XSS"* kepada kami sehingga dapat kami tangani dengan cepat dan baik.

Traveloka

Traveloka Bug Bounty Program

[Overview](#)[Rules & Eligibility](#)[Scope](#)[Reward & Bounty](#)[Wall of Thanks](#)

Wall of Thanks

Traveloka bug bounty program appreciate and gratitude security researchers for helping us to make our products and services safer. We are happy to present the list of researchers who have participated in this program:

2018 ^

- Nosa Shandy
- Tomi Ashari
- Roholesi Talaohu (RootBakar)
- Yoshua Kristanto

* CodePolitan

<https://www.codepolitan.com/credit-to-bug-reporter>**Choirur Rizal****/Mr. Security_system****Syahrul Akbar R****RootBakar**

* Envato

Honor Roll - Envato Systems

Name	Dates of reports
Fabergé — hackerone.com/faberge	20 Mar 2019
Shady Gamal	21 Jan 2018
Sakhavat Ismayilov — fs-code.com	01 Oct 2018
RootBakar — Roholesi Talaohu	19 Sep 2018

* Gitlab

username

The username field contained an input validation issue which resulted in HTML content injection on several pages and could lead to phishing attacks. The issue is now resolved in the latest release.

Thanks to @talaohu28 for responsibly reporting this vulnerability to us.

Versions Affected

Affects GitLab CE/EE 4.1 and later.

Remediation

We strongly recommend that all installations running an affected version above to be

* Sony

The screenshot shows the Sony Vulnerability Disclosure Program website. At the top, there's a logo with the word 'SONY' and the text 'Sony Vulnerability Disclosure Program www.sony.com Launched on February 26th, 2018'. Below the header, there are navigation links: Policy, Hacktivity, Thanks (which is underlined), and Updates (0). The main content area is titled 'Sony - 2019' and displays a grid of user profiles. There are two rows of four profiles each. The profiles are numbered 1 through 8. Profile 8, which belongs to the user 'keretasenja...', has a QR code icon next to it and is highlighted with a red border. The other profiles show various user photos and their names and reputations.

User ID	User Name	Reputation
1	lordjerry0x01	Reputation: 88
2	Oxd0m7	Reputation: 28
3	udhayalsro...	Reputation: 26
4	zayn1337	Reputation: 23
5	kingagnar	Reputation: 21
5	ggabarin	Reputation: 21
7	yujitounai	Reputation: 16
8	amalyoman	Reputation: 14
8	keretasenja...	Reputation: 14
8	Oang3el	Reputation: 14

* Redstorm

3 bulan terakhir

Sepanjang masa

Peringkat	Nama peneliti	Poin
1	 zetcode	800
2	 noobSecurity	480
3	 Eka Syahwanh	255
4	 Akun pribodi	180
5	 rootbakar	175

* KhanAcademy

 Khan Academy
Start learning now. Completely free, forever.
Vulnerability Disclosure Program
www.khanacademy.org/ • Launched on April 8th, 2014

Policy Hacktivity Thanks Updates (0) Insights

Khan Academy - 2018

 1 tomoh Reputation: 61	 2 keretasenja... Reputation: 21	 3 co0nan Reputation: 16	 4 na5ne3t Reputation: 14	 5 abdilahrf_ Reputation: 7
 5 aaron_coste... Reputation: 7	 5 hanno Reputation: 7	 5 yddmat Reputation: 7	 5 jaimakali Reputation: 7	 5 avileox Reputation: 7

* Private Program CyberArmyID

Reward CyberArmyID [Inbox](#)

 Cyber Army Indonesia <hello@cyberarmy.id>
to me ▾

 Indonesian ▾ > Igbo ▾ Translate message

Dear RootBakar,

Terimakasih telah menjadi Dedicated BugHunter untuk Program

Sebagai apresiasi kami, kami telah mengirimkan reward senilai Rp. 10.000.000.

Terima kasih telah menjadi bagian dari Bug Hunter "The First Crowdsourced Cyber Security Platform in Indonesia"

Best Regards,
Cyber Army Indonesia

PT Global Inovasi Siber Indonesia
Office 1 - Jl. Naripan No.43, Ks. Pasang.
Semen Bandung, Kota Bandung, Jawa Barat 40113.
Office 2 - Menara Bandung Digital Valley Lantai 4.
Jl. Gegerkalong Hill No.47 Kota Bandung
Website: www.cyberarmy.id

* HaloDoc



Security <security@halodoc.com>
to me, security, security ▾

 English ▾ > Igbo ▾ Translate message

Dear RootBakar,

Untuk pembayaran bounty lebih lanjut. Tolong sertakan informasi berikut

- Nama sesuai yang tertera di bank
- Nama bank
- Cabang dimana akun bank terdaftar
- Nomor akun

Terima kasih

Salam,

Halodoc Security Team

* Shopify

 HackerOne, Inc. [US] | <https://hackerone.com/shopify/thanks/2018>



55



keretasenja28

SEC 2 STORY

* Massdrop

Hi RootBakar,

Thank you for your continued reports. Both this iframe XSS report and your email HTML injection report are eligible for \$500 rewards each. This is on top of your previously confirmed reward of \$500 for your original XSS report.

I think we have already requested W-9 and W-8BEN from you. Reward will be paid after that information is provided to us.

* IKEA

REPORTED BY



rootbakar

PROJECT

[IKEA.com - Responsible Disclosure](#)

PROGRAM

[IKEA.com - Responsible Disclosure](#)

CATEGORY

Injection

SEVERITY LEVEL

⚠️ High

REWARD AMOUNT

€ 250

PAYMENT STATUS

Paid

CLOSED AS

Resolved

* Facebook

 16 Feb

Hi Robin Talaohu,

After reviewing this issue, we have decided to award you a bounty of \$500. Below is an explanation of the bounty amount. Facebook fulfills its bounty awards through Bugcrowd.

This could have allowed a malicious user to tag users to posts which victims could then not untag themselves.

Note that we are awarding this submission because it helped us identify the second instance of the same issue despite the same fix.

Thank you again for your report. We look forward to receiving more reports from you in the future!

== Claim Your Bounty ==



*** AntiHack**

ASRC Rewards for January 2019 Inbox x X Print Email

AlibabaSecurity <security@service.alibaba.com> Fri, Feb 15, 6:33 PM Star Reply More

to me ▾

Hi,

Thanks very much for the report(s) you have posted to ASRC (<https://security.alibaba.com/en/>). We will follow the "Vulnerability Rewards Program" and give you the reward.

From 2019.1.1 to 2019.1.31, 4 report(s) is eligible and rewarded for **60** USD. You can visit [ASRC website](#) for more details.

Currently we only support Bank Transfer and [Alipay](#). If you have an Alipay account, please provide your Alipay account number and name.

For Bank Transfer, the reward will be transfer to your bank account as you provided in your profile at "Profile | Payment Information" (<https://security.alibaba.com/en/information.htm>). Bank Transfer transnationally may take a little longer time. **If this information is correct, please reply this mail as soon as possible.** Or if you need to fill in or modify this information, also mail us after you changed it.

If you haven't provided your Payment information in your profile, we need ALL the **following information** to continue our financial processes.

- Your Country
- Your Name
- Your Bank Name
- Your Bank Account No.
- Your address
- SWIFT CODE
- And special info for different country
 - Routing No. (United States of America)
 - Contacts and Tel No. (Republic of Korea)
 - IBAN (Europe)
 - Bank Code & Bank Branch Code (Hong Kong, Singapore, Korea)
 - BSB (The Commonwealth of Australia)
 - Sort Code (The United Kingdom of Great Britain and Northern Ireland)

Please feedback your information to us. We are committed to protecting your privacy.

Thank you very much for your support!

*** Alibaba**

Chip Benson (Edmodo)
Apr 10, 2013 4:00 AM EDT

Hello,

Thank you for reporting this issue. More than anything we want Edmodo to meet and surpass the needs of our teachers, and your input is truly invaluable as Edmodo continues to grow and develop.

After talking with our internal security team, we have reviewed your request in detail and prioritized it accordingly. Rather than have you wait until the fix is live (since it may be a while) we would like to show you our appreciation now by sending you some Edmodo "gadgets" as a token of our appreciation. If you are interested in receiving those goodies, please let us know your shirt size and how we can send them to you, and we'll take care of the rest. When giving us your address please include a phone number which we need for the shipping documentation.

Please format your address for us below so we are sure to enter it correctly on the shipping documents (please put your info after the title words on each line).

Name:
Street address (please include house, apartment, or building number).
City:
State, province, etc.:
Country:
Postal code:
Phone number:
Shirt size:

Thanks again for your help and we look forward to your reply.

* Edmod

 **SimonJ Smith** <Simon.J.Smith@autotrader.co.u... Thu, Apr 11, 6:27 PM (3 days ago)   

to me ▾

 English ▾ > Igbo ▾ Translate message Turn off for: English ×

Hi,
Thanks for your message. The issue has been raised with the relevant development team for remediation.

As a token of thanks we would be glad to add you to our hall of fame at www.autotrader.co.uk/hall-of-fame. If this is of interest to you, please supply the details that you would like us to use (twitter/linkedin etc). If at any point you would like us to then remove those details please contact customersecurity@autotrader.co.uk and we will be glad to assist.

We would also like to purchase a voucher for an online store of your choice. Please ensure the site that you suggest are able to take payment by virtual credit card from the UK.

Thanks again for taking the time to help maintain the security of our site.
Best regards,
Simon.

This e-mail is sent on behalf of Auto Trader Group Plc, Registered Office: 1 Tony Wilson Place, Manchester, Lancashire, M15 4FN (Registered in England No. 9439967). This email and any files transmitted with it are confidential and may be legally privileged, and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the sender. This email message has been swept for the presence of computer viruses.

* Auto Trader

   Inloggen *

- Jineesh AK
- Robert Villalon
- Mark de Groot
- Florian Kunushevci
- @mcorral74
- UMESH B. PATIL
- Tarun Mahour
- Roholesi Talaohu (rootbakar)

PostNL

Pada bagian penutup ini saya lampirkan link **Proof of Concept** dari temuan saya pada sebuah *platform social media* terkenal di dunia yaitu **Facebook**

<https://progress28.web.id/bug-bounty-facebook-how-i-hack-facebook-and-get-1000-using -simple-technique/>

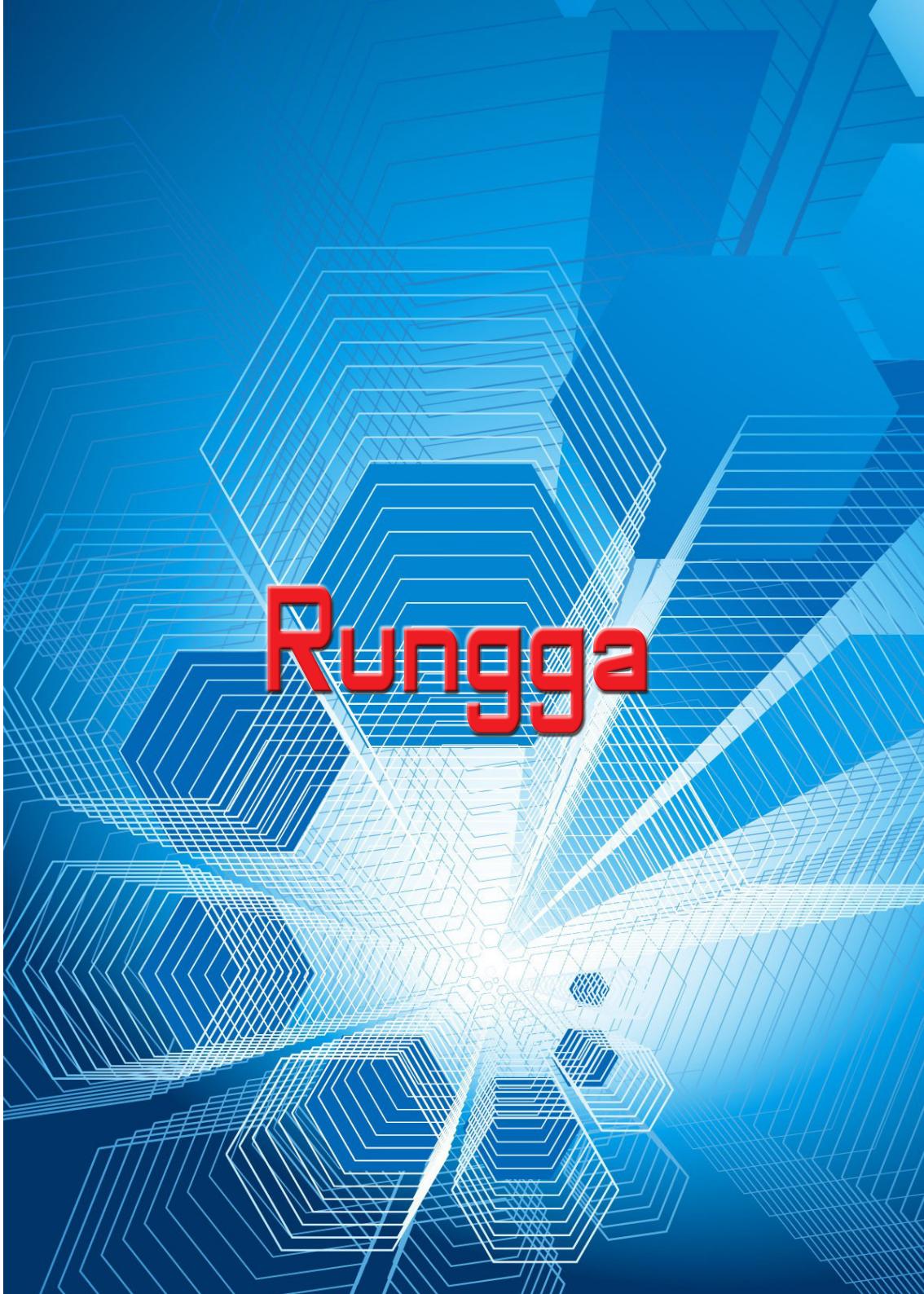
Alhamdulillah pada temuan ini saya diberikan rewards **1000\$** oleh pihak **Facebook** karena menemukan bug pada **2 endpoint** yang berbeda dan rewards dikirimkan melalui Bugcrowd. Semoga tulisan kecil ini dapat menginspirasi diri saya khususnya dan orang lain pada umumnya terkait kegiatan Bug Hunting atau untuk menjadi seorang '**Newbie' Bug Bounty Hunter**'.

Terimakasih sudah menyempatkan untuk membaca tulisan sederhana saya ini. Saya tak pandai dalam menulis dan merangkai kata, namun kritik dan saran akan sangat membantu membangun dan memperbaiki tulisan saya pada kesempatan berikutnya. Jadikanlah ilmu yang kau punya sebagai lentera dunia yang selalu memberikan manfaat bagi orang banyak. Saya hanya orang beruntung yang diberikan amanah untuk memiliki ilmu tersebut dan saya akan terus mencoba untuk mempergunakan dengan sebaik-baiknya (*Dari timur untuk Indonesia*).

Reference:

<https://hackerone.com/>
<https://bugcrowd.com/>
<https://app.zerocopter.com/>
<https://www.antihack.me/>
<https://www.cyberarmy.id/>
<https://www.redstorm.io/>

https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf <https://progress28.web.id/bug-bounty-facebook-how-i-hack-facebook-and-get-1000-using-simple-technique/>



A 3D-style background featuring a perspective view of a space filled with numerous blue hexagonal outlines. These hexagons are arranged in layers, creating a sense of depth and movement. Overlaid on this geometric pattern is a large, bold, red 3D-style text that reads "Rungga". The text is centered and stands out prominently against the blue and white background.

Rungga

Mac Gyver, Inspirasi Mengenal Komputer Lebih Dalam

Nama saya Runga, Meskipun nama saya unik tapi saya bukan orang penting di Indonesia. Coba aja googling nama saya, yang Anda temukan adalah sosmed saya tapi bukan jabatan penting di Indonesia. Salah satu yang istimewa dalam hidup saya adalah komputer. Kalau ditanya apasih komputer bagi saya, bisa saya bilang ya seperti “dia”, sulit dilupakan dan ditinggalkan, meski dia hanya sebuah perangkat. Awal kenalan sama si komputer ini, saya main kerumah tetangga. Numpang kenalan ceritanya. Komputer Pentium IV pertama saya yang boleh kredit sama koperasi. Dan setelah itu, saya beberapa kali ganti pacar, eh maksud saya ganti komputer sampai sekarang ini saya mencoba si Mac. Tapi bukan MacGyver ya.

Ngomong soal MacGyver, ada yang berkesan buat saya dari film ini. Mac Gyver adalah film yang saya kenal sejak pohon mangga berbuah lagi setelah berbuah pertama yang menandai kelahiran saya. Nah dari si Mac inilah saya terinspirasi untuk mengenal lebih jauh tentang si komputer ini. Saya terus mempelajarinya dengan prinsip *“Learning by doing.”*. Harus terjerumus dikesalahan agar bisa tau jalan keluarnya yg benar kaya apa. Dari si komputer saya kenal banyak dunia. Saya menemukan bidang ilmu komputer yang paling saya sukai, yaitu semua hal yang berbau serangan. Nah disinilah saya berkenalan dengan kata security. Menurut saya, security adalah Bahasa keren dari hansip, satpam dan bodyguard. Tapi sekarang

saya mulai memiliki arti lain, nyambung dengan kesukaan saya dari jaman sekolah, suka ngoprek dan terinspirasi dari Macgyver.

Kalau ditanya pengalaman menarik dalam bidang security saya teringat saat bertemu dengan klien dan berhasil mengembalikan kata sandi secara plaintext lalu memaparkannya di depan seluruh user. Tapi kemudian ada beberapa orang yang senyum-senyum dan langsung ngasih kode agar cepat-cepat di skip saja urusan kata sandi tersebut. Setelah selesai presentasi, saya langsung didatangi oleh beberapa user yang mengatakan bahwa itu ternyata kata sandi sysadmin adalah nama selingkuhannya (a.k.a calon bini muda). Disinilah keseruan pada bidang jebol menjebol. Kadang kita dihadapkan dengan situasi sulit yang semuanya serba terbatas. Ketika satu sistem sudah diambil alih, maka tugas belum berhenti sampai disitu dan masih ada perjalanan panjang lainnya. Paling lucu itu jika bisa membaca pola kata sandi yang ada di organisasi tersebut dan memaparkannya seperti contoh di atas.

Beberapa perangkat lunak untuk melakukan serangan bersifat open source dan inilah salah satu kenikmatan dunia ketika ada yang gratisan seperti jaman sekolah numpang makan siang dan sore di rumah kawan. Dikalangan pemerintah saat ini masih mencanangkan penggunaan perangkat lunak yang bersifat opensource dan menurut gue pribadi cukup bagus jika bisa menyamakan fitur dengan yang berlisensi (takut salah ucapan nih, hehehe). Eh ada tapinya loh, ketika nyari produk teknologi keamanan informasi khususnya untuk lini pertahanan, disinilah yang akan membuat kita galau seperti jomblo akut yang ditinggal TTM nya (ga berani komentar banyak karena takut kena sentil). Intinya mau fitur yg seimbang dengan berbayar tapi ah sudahlah.

Hacker itu Kayak Jagoan Pilem: Jago Bengbeng Nembus Semua Sistem Tapi Bukan Hati

Bicara soal hansip pasti bicara soal maling, kalau bicara soal security, kita bicara penjahatnya. Katanya sih hacker namanya. Tapi buat saya, hacker itu orang yg seperti di pilem-pilem barat gitu, jago bengbeng bisa nembus semua sistem tapi terkadang si hacker sulit nembus hati orang yg disukai. Nah Kalau ditanya soal hardware hacking, maka gue akan jawab "Orang gilak yg suka oprek itu", karena hanya orang unik yang suka berbicara dengan perangkat keras apalagi sampai jatuh cinta mengobrak abrik si perangkat itu. Soalnya kan berbeda Bahasa perangkat keras dengan Bahasa manusia (awas dilempar bata ngeledek terus).

Sebagai orang yang banyak berhubungan dengan komputer dan dunia nya, tentu saya juga bergaul dengan orang-orang seperti saya. (saya ikut komunitas yang berbau teknis keamanan dan manajemen keamanan walau cuman silent rider karena saya cupu banget). Menurut saya, dunia komunitas IT dan komputer di Indonesia sendiri sangat banyak. Makin lama makin luar biasa ramainya, baguslah. Semoga ya dunia security Indonesia saat ini lebih berkualitas secara SDM. Oh iya, orang orang di dunia security juga jangan ngartis karena nanti bisa digosipin sama Lambe turah dan masuk ke acara Hitam Putih lagi, hehehe. Terus berkembang tanpa sikut-sikutan antar teman di dunia keamanan informasi. Semua saling kolaborasi untuk meningkatkan ilmu di negeri ini dan bukan MONEY ORIENTED, apalagi sampai memeras atau ngancam.

Aduhhh jangan ditanya ya cita cita terbesar saya yang belum dipenuhi saat ini. Karena jawabannya "bisa masuk surga dan punya anak-anak yg Sholeh dan Sholehah, apalagi didukung sama para isteri yg sholehah" (eh awas dibaca orang rumah).



Profil

1. Nama : Rungga
2. Panggilan sehari hari : Rungga
3. Handle/nick : Bukan Hacker Kaya Om Matias, Jadi Ndak Punya Nick
4. Tempat/Tanggal lahir : Indonesia, Tanggal lupa klo ndak salah pas pohon mangga berbuah pertama kali di depan rumah
5. Alamat : Masih di Pulau Jawa
6. Handle origin : KTP sih dari Indonesia
7. Mobile : - Telegram : rungga
8. Urls : rungga.blogspot.com
9. Sosial Media : nama saya tinggal di gugling langsung ketemu dah semua akun medsos (nama ane unik)
10. Computers spec :
 - Pertama : Pentium IV (boleh kredit sama koperasi) sebelumnya numpang tetangga
 - Sekarang : Lagi mencoba pakai Mac
 - Yang diidamkan : Ga ada sih karena enakan ngidam rujak
11. Member of :
 - Community : Bukan CIA yang jelas
 - Projects : Ane cuman Calo ajah
12. What I like to do? : Berbagi apapun baik derita maupun suka
13. What I dislike : Dibohongi dan dikhianati oleh sahabat (maka akan downgrade jadi TEMAN bukan SAHABAT lagi)
14. Tokoh yang paling Anda kagumi, mengapa? Nabi Muhammad SAW dan Kedua orang tua
15. Favorite / Kesukaan :
 - Makanan/Foods : Semua makanan kolesterol
 - Minuman/Drinks : Teh PANAS bukan Hangat
 - Warna/Colours : Apapun kecuali Pink
 - Jenis/genre Music : Asal bukan koplo
 - Band / penyanyi : Sheila on 7 bukan sheila majid loh
 - Movies/TV : Agent of Shield, Avenger, Intelligence (U.S. TV series), Macgyver
 - Books & Authors : Jarang baca buku klo ga terpaksa
 - Place : Kamar Tidur (tempat paling enak untuk remote kerjaan)
 - Time : 04.30 (sebelum subuh karena itu waktu utk mulai kehidupan setiap hari)
 - Hobby : Martial Arts, Liat berita otomotif, Ngoprek dikala senggang, Main PS (PES & FIFA), Bersihin mobil, Nyuci, Nyapu, Ngepel, Nongkrong sama temen sekolah, Main sama anak dan yang pasti main sama isteri (Khusus Dewasa)
 - OS : Windows XP karena paling Legend
 - Software (kenapa?) : Firefox (termasuk perangkat lunak) karena IE sudah ga enak
 - Bahasa programing : PHP, .Net, C#, tapi semua itu bukan kesukaan
 - Words/Quote : Belajarlah mencintai seni bela diri karena anda akan mengerti kapan harus menyerang dan bertahan. Mirip di dunia Keamanan Informasi

Strategi Keamanan Informasi di Organisasi Anda

Aktivitas kejahatan siber (*cybercrime*) adalah salah satu tantangan terbesar yang akan dihadapi oleh setiap Organisasi di dunia. Baik dari sisi kerugian yang ditimbulkan, kemunculannya yang selalu baru dan tiba tiba sampai penanganan yang harus terus berkembang. Kasus yang muncul seperti *WannaCry* dan *Petya/NotPetya*, bisa kita jadikan contoh ancaman keamanan digital yang datang dari sumber baru dan bersifat tidak terduga. Dengan demikian, makin bertambahnya waktu, lansekap ancaman pun tidak berhenti pada bentuk yang sama. Tetapi telah menjadi lebih beragam. Para *Attacker* (Penyerang) terus menerus bekerja untuk menemukan cara baru, agar dapat melakukan serangan serta menutupi jejak mereka saat melakukannya.

Menurut dokumen “*Internet Security Threat Report Volume 23*” yang dikeluarkan oleh *Symantec*, penjahat siber yang selama ini telah fokus pada ransomware untuk menghasilkan pendapatan, mulai menjelajahi peluang lain. Selama setahun terakhir, kenaikan astronomi dalam nilai-nilai *cryptocurrency* telah menginspirasi penjahat siber untuk beralih ke penambangan koin. Hal ini merupakan alternatif sumber pendapatan bagi mereka. *Gold rush* pertambangan koin ini menghasilkan sebuah peningkatan 8.500 persen dalam pendekripsi koinminer komputer *endpoint* pada tahun 2017.



Jika melihat eksloitasi *EternalBlue* yang mendatangkan malapetaka pada tahun 2017, muncul fakta bahwa kerentanan yang ada telah menyulitkan penyerang untuk mengidentifikasi dan mengeksloitasi. Dari kasus tersebut, kita dapat melihat peningkatan penyerang yang menyuntikkan implan *malware* ke dalam rantai pasokan, untuk menyusup ke organisasi yang tidak curiga. Jika secara prosentasi peningkatan ini mencapai 200 persen. Sebuah angka yang sangat signifikan dibandingkan dengan tahun sebelumnya. Sementara itu pada saat kita melakukan kegiatan seperti *penetration testing* (*pentest*), terkadang hasil temuan yang didapatkan mirip antara aplikasi satu dengan yang lain. Disinilah timbul pertanyaan, mengapa bisa demikian? Padahal proses *pentest* rutin dilakukan setiap tahunnya !?@#\$%. Disinilah muncul permasalahan yang membutuhkan solusi, yaitu strategi keamanan informasi.

Tujuan Strategi Keamanan Informasi sendiri merupakan perencanaan strategis dalam konteks pemanfaatan Teknologi Informasi (TI). Pemanfaatan yang dimaksud disini, bersifat menyeluruh, terpadu, serta terkoordinasi yang secara dinamis dan realistik, memperhitungkan serta mengaitkan aspek keamanan informasi. Hal ini guna mengatur proses manajemen Organisasi TI,

perangkat keras, perangkat lunak, sumber daya manusia, jaringan komunikasi data dan lain-lain.

Keamanan Informasi Seperti Permainan Sepak Bola

Keamanan informasi di dalam organisasi, menurut saya terlihat seperti pertandingan sepak bola. Setiap orang memiliki peran dan tanggung jawab yang berbeda tetapi memiliki tujuan bersama. Tujuannya adalah untuk mengamankan data dan informasi organisasi dari tingkat teknis hingga tingkat strategis. Konsep ini saya mulai tuangkan di awal tahun 2017. Kemudian ada beberapa orang yang menggunakan serta mengembangkannya.

Sebagaimana permainan sepak bola, keamanan informasi dalam organisasi ini memiliki peran sebagaimana yang ada dalam sepak bola, untuk setiap anggota tim keamanan TI, seperti:

- Penjaga gawang dan bek, mereka adalah sysadmin dan tim jaringan infrastruktur. Melindungi aset di semua lini. Pertahanan solid mereka disumbangkan tidak hanya oleh keterampilan dan pengetahuan mereka, tetapi juga dari dukungan alat-alat seperti firewall, SIEM, dll.
- Gelandang, atau orang yang menyeimbangkan tim. Posisi mereka sangat penting untuk mempertahankan permainan. Mereka dapat berada di posisi mundur dan di posisi maju di lain waktu. Contoh penamaan aslinya adalah Petugas Keamanan Informasi (*Information Security Officer*), Divisi Internal Manajemen Risiko, dan Divisi Kepatuhan.
- Striker, atau pria yang memainkan bagian serangan. Mereka adalah Konsultan Keamanan Informasi dan Pentester. Tujuan tunggal mereka adalah untuk menembus lini pertahanan musuh dan mencetak gol.
- Pelatih adalah manajemen puncak (*top management*) atau senior executive level. Mereka mengawasi permainan dan bertanggung jawab atas semua hasil. Memberi semangat, membimbing tim, dan memutuskan taktik apa yang harus digunakan dalam permainan.
- Taktik itu seperti kerangka kerja keamanan informasi. Kerangka kerja mengatur posisi dan tugas untuk setiap orang dalam tim. Hal ini juga digunakan untuk memutuskan proses ketika permainan sedang berlangsung, baik menjadi defensif, ofensif, atau memperkuat posisi tengah untuk menjaga keseimbangan. Setiap taktik memiliki kelebihan dan kekurangan.
- *Last but not least*, pendukung. Mereka adalah pemangku kepentingan yang memiliki minat dan kepedulian terhadap organisasi. Mereka akan mendukung tim untuk menjadi sukses dalam menjalankan proses bisnis di dalam organisasi.



Figure 1 Information Security is Like Football

Membangun Strategi Keamanan Informasi dalam Organisasi

Setelah kita memahami latar dan tujuan kenapa sebuah keamanan strategi dibuat, maka kita mulai membuat Strategi Keamanan Informasi itu sendiri. Dalam pembuatannya, kita dapat menggabungkan seluruh framework (kerangka kerja) seperti TOGAF, ISO/IEC 27001, CyberSecurity Framework, NIST, SABSA dan bahkan COBIT sebagai Arsitektur Keamanan Enterprise nya.

Sebagaimana didefinisikan oleh Decker, Arsitektur Keamanan Enterprise adalah “menggabungkan semua aspek keamanan untuk organisasi, termasuk kepemimpinan, strategi, struktur organisasi, perencanaan, desain, implementasi, dan operasional. Ini mencakup orang, proses, dan aspek teknologi keamanan” (Tipton & Krause, 2007, p.1425).

Sherwood dalam bukunya menyatakan “Arsitektur keamanan adalah seni dan ilmu perancangan serta pengawasan konstruksi sistem bisnis, biasanya sistem informasi bisnis, yang bebas dari bahaya, kerusakan, dan lain-lain, serta bebas dari rasa takut, peduli, tidak mungkin gagal, dapat diandalkan, aman dari instalasi” (Sherwood, 2005, p.2).

Menurut saya, kerangka kerja dan metodologi yang telah terbukti untuk Arsitektur Keamanan dan Manajemen Layanan Organisasi adalah SABSA (*Sherwood Applied Business Security Architecture*). SABSA telah digunakan oleh sejumlah besar Organisasi di seluruh dunia, untuk memenuhi berbagai kebutuhan termasuk Manajemen Risiko, Jaminan Informasi, Tata Kelola, dan

Manajemen Keberlangsungan. Berdasarkan ide yang pertama kali dikembangkan oleh John Sherwood pada tahun 1995 dan diterbitkan pada tahun 1996 sebagai "SABSA: Sebuah Metode untuk Mengembangkan Arsitektur dan Strategi Keamanan Enterprise", SABSA saat ini merupakan pendekatan yang valid untuk kedua Organisasi komersial dan pemerintah. SABSA bertujuan untuk memenuhi kebutuhan target Organisasi dan memastikan bahwa layanan keamanan dirancang, disampaikan dan didukung sebagai bagian integral dari bisnis proses dan infrastruktur Manajemen TI (SABSA Institute, 2013).

Model SABSA terdiri dari enam lapisan yang tertera pada tabel 1 di bawah ini dan pada awalnya mengacu kepada model arsitektur organisasi yang dibuat atau dikembangkan oleh Zachman. Model SABSA telah disesuaikan dengan pandangan keamanan informasi dunia. Setiap lapisan dirancang untuk mewakili pandangan pemain yang berbeda dalam proses menentukan, merancang, membangun, dan menggunakan sistem bisnis.

Tabel 1. Model SABSA

NO	View	Architecture
1	<i>The Business View</i>	<i>Contextual Security Architecture</i>
2	<i>The Architect's View</i>	<i>Conceptual Security Architecture</i>
3	<i>The Designer's View</i>	<i>Logical Security Architecture</i>
4	<i>The Builder's View</i>	<i>Physical Security Architecture</i>
5	<i>The Tradesman's View</i>	<i>Component Security Architecture</i>
6	<i>The Facilities Manager's View</i>	<i>Operational Security Architecture</i>

SABSA menganalisis setiap lapisan dengan menggunakan enam pertanyaan yang sama, dimana pada awalnya digunakan dalam Kerangka Zachman:

- a) Apa yang coba lakukan di lapisan ini? (Aset yang akan dilindungi oleh arsitektur keamanan);
- b) Mengapa melakukannya? (Motivasi untuk ingin menerapkan keamanan, dinyatakan dalam ketentuan lapisan ini);
- c) Bagaimana mencoba melakukannya? (Fungsi-fungsi yang diperlukan untuk mencapai keamanan pada lapisan ini);
- d) Siapa yang terlibat? (Sumber daya manusia dan aspek organisasi keamanan di lapisan ini);

- e) Di mana melakukannya? (Lokasi tempat menerapkan keamanan yang relevan dengan lapisan ini); dan
- f) Kapan melakukannya? (Aspek keamanan terkait waktu yang relevan dengan lapisan ini).

Tabel 2. Lapisan Model SABSA

	<i>Assets (What)</i>	<i>Motivation (Why)</i>	<i>Process (How)</i>	<i>People (Who)</i>	<i>Location (Where)</i>	<i>Time (When)</i>
Contextual	The Business	Business Risk Model	Business Process Model	Business Organization and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Atributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetimes and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices and Procedures	Security Mechanism	Users, Application and The User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions and ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Supports	Application and User Management and Support	Security of Sites, Networks and Platforms	Security Operations Schedule

Sebagai hasil untuk konsep keamanan arsitektur pada area konseptual adalah menentukan kerangka kerja untuk mendukung tata kelola keamanan informasi. Contoh yang bisa kita lihat adalah

- COBIT untuk Tata Kelola TI,
- ISO 31000 untuk Manajemen Risiko,
- ISO/IEC 27001 & NIST SP 800-53 untuk Keamanan Informasi,
- OWASP untuk teknis keamanan aplikasi berbasis web dan aplikasi perangkat bergerak,
- TOGAF dan SABSA untuk menentukan arsitektur keamanan informasi.

Jika kerangka kerja telah terbentuk, juga diperlukan komitmen pimpinan untuk mendukung semua proses tersebut serta membuat kebijakan, organisasi dan ruang lingkup keamanan informasi. Disamping itu juga diperlukan sumber daya yang cukup dengan dukungan kompetensi dan kesadaran seluruh pendukung proses keamanan informasi. Setiap kebijakan atau proses yang baru harus selalu dikomunikasikan.

Setelah semua siap maka akan didapatkan hasil untuk konsep keamanan arsitektur. Pada area logic, hasil yang didapat dengan menentukan kontrol keamanan informasi, adalah:

- a) *Mobile Device Management;*
- b) *Teleworking;*
- c) *Access Control;*
- d) *Cryptographic;*
- e) *Protection from Malware;*
- f) *System Acquisition, Development & Maintenance;*
- g) *Control of Operational Software;*
- h) *Vulnerability Management;*
- i) *Communication Security;* dan
- j) *Backup.*

Hasil untuk konsep keamanan arsitektur pada area fisik dengan menentukan kontrol keamanan informasi, yaitu:

- a) *Asset Management;*
- b) *Secure Areas;*
- c) *Equipment Security;* dan
- d) *Supplier Relationship.*

Sedangkan hasil untuk konsep keamanan arsitektur pada area komponen, disini diberikan contoh, sampai ke produk yang ada di pasaran, akan tetapi

sebelum mengimplementasikan diperlukan landasan dalam menentukan proses tersebut.

Contoh Arsitektur dan Desain Infrastruktur Untuk Aplikasi Berbasis Web dan Mobile

Aplikasi web dan perangkat bergerak menghadirkan desain serta pengembangan dengan banyak tantangan. Sifat tanpa status HTTP sendiri berarti pelacakan status sesi setiap pengguna menjadi tanggung jawab aplikasi. Sebagai pendahulu untuk hal ini, aplikasi harus dapat mengidentifikasi pengguna dengan menggunakan beberapa bentuk otentikasi. Mengingat bahwa semua keputusan otorisasi berikutnya didasarkan pada identitas pengguna, penting bahwa proses otentikasi secara aman dan mekanisme penanganan sesi yang digunakan untuk melacak pengguna yang terautentikasi juga terlindung dengan baik. Merancang autentikasi secara aman dan mekanisme manajemen sesi hanyalah beberapa masalah yang dihadapi para desainer dan pengembang aplikasi web.

Tantangan lain terjadi karena data input dan output melewati jaringan publik. Mencegah manipulasi parameter dan pengungkapan data sensitif adalah masalah utama lainnya. Dari serangkaian risiko tersebut maka dapat disimpulkan minimal aplikasi web yang sifatnya dapat diakses melalui jaringan internet harus menggunakan protokol yang aman seperti menerapkan HTTPS (*Hypertext Transfer Protocol Secure*).

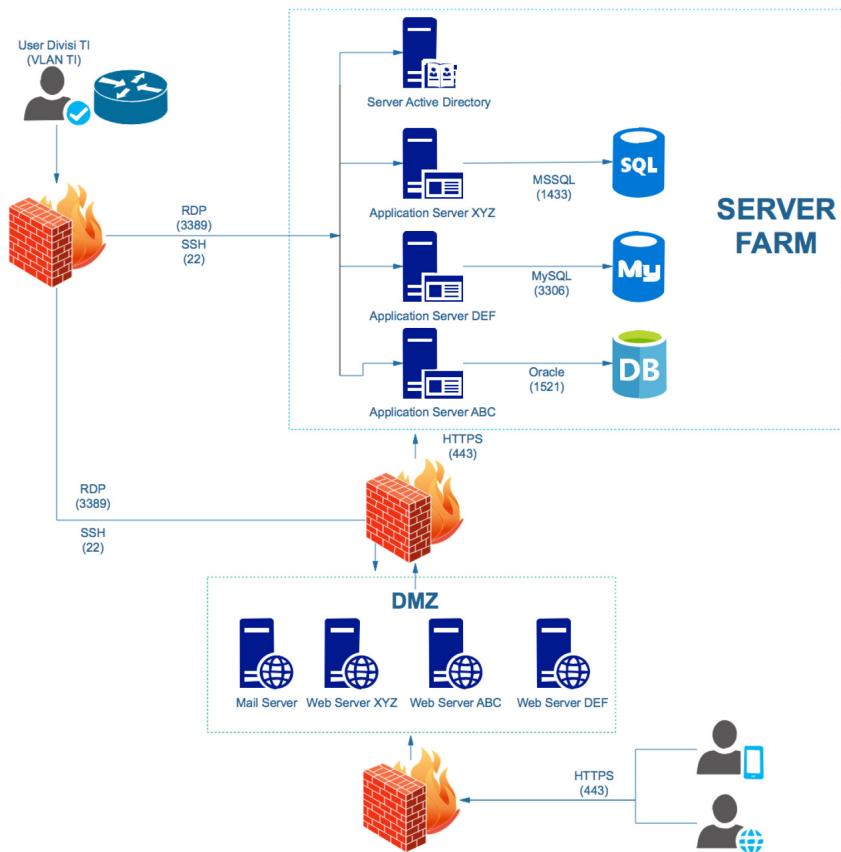
HTTPS bukanlah protokol yang terpisah, tetapi HTTPS mengacu pada kombinasi dari interaksi HTTP normal melalui *Secure Socket Layer* (SSL) atau *Transport Layer Security* (TLS). Hal ini menjamin keamanan dari para penyadap informasi.

Dalam hal ini, ada dua jenis umum lapisan enkripsi diantaranya *Transport Layer Security* (TLS) dan *Secure Socket Layer* (SSL). TLS adalah protokol pada jaringan komputer yang dapat menjaga kerahasiaan data yang dikirim oleh *client* ke *server* ataupun sebaliknya. Dengan itu, pihak ketiga tidak dapat menyadap data yang dikirim ke *server* atau ke *client*.

Sedangkan SSL adalah sebuah teknologi enkripsi untuk mengamankan HTTP sehingga terjaga pengiriman data antara *server* dengan *client*. Penggunaan SSL biasanya dapat dilihat pada *address bar browser* yang digunakan. Web yang sudah terpasang SSL akan menjadi <https://contohnamadomain.com>.

Kemudian setiap aplikasi web yang dapat diakses melalui jaringan internet, aplikasi web server harus berada di *Demilitarized Zone* (DMZ).

Persyaratan minimal topologi jaringan komputer dapat dilihat pada gambar di bawah ini:



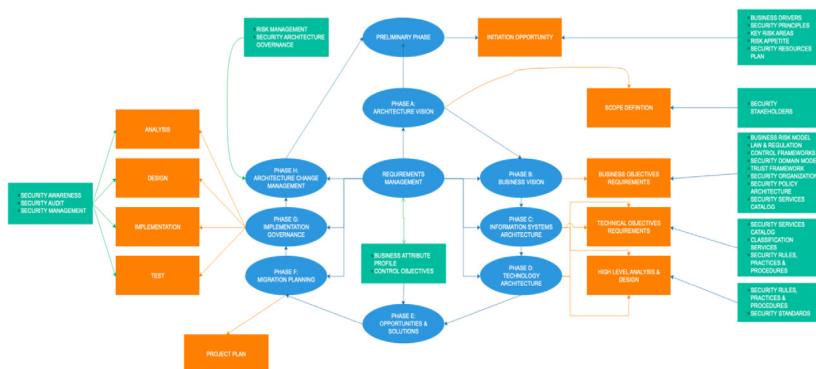
Gambar 1. Persyaratan Minimal Topologi Infrastruktur

Peningkatan Efektivitas dan Keamanan Dari SDLC

Meskipun TOGAF dan SABSA telah ada, kesamaan budaya dan filosofi keduanya didorong oleh bisnis dan keduanya memiliki visi arsitektur Organisasi, asal-usul dan sejarah mereka yang berbeda membedakan kedua kerangka

tersebut. Akibatnya ketika seorang mencoba untuk menghubungkan satu dengan yang lain adalah mungkin untuk menghadapi tingkat perselisihan tertentu pada pilihannya, oleh orang-orang dengan pola pikir atau sudut pandang yang berbeda. Oleh karena itu penting untuk memperjelas pada tahap ini, bahwa tidak ada pemetaan universal tunggal antara dua kerangka kerja tersebut dan bisa saja dikombinasikan dengan kerangka kerja yang lain seperti OWASP, ISO/IEC 27001 dan lain-lain. Prinsip-prinsip untuk kerangka terpadu ini sebagaimana didefinisikan adalah sebagai berikut:

- Ketika sebuah artefak muncul di berbagai tingkat arsitektur, artefak dipetakan menggunakan tingkat abstraksi tertinggi, untuk menjaga fokus utamanya pada tingkat Organisasi;
- Ketika di mana dua atau lebih pemetaan dapat diterima, salah satu yang lebih jelas lebih disukai, karena kepraktisan yang berasal dari kemungkinan penerimaan yang lebih besar; dan
- Hanya konsep yang paling penting dan berguna yang dimaksudkan untuk diintegrasikan.



Gambar 2. Mapping Untuk SDLC-TOGAF-SABSA

Dapat disimpulkan bahwa penyusunan strategi keamanan informasi adalah upaya yang menantang yang memerlukan koordinasi di antara berbagai pemangku kepentingan. Meskipun ada banyak metodologi, strategi keamanan informasi telah terbukti menjadi instrumen untuk membantu dalam mengelola risiko yang terkait dengan keamanan informasi.

Hal yang patut diperhitungkan dalam membuat strategi keamanan informasi sebagai berikut:

- a. Menetapkan visi, ruang lingkup, tujuan dan prioritas pada aspek keamanan informasi di Organisasi;
- b. Mengikuti pendekatan penilaian risiko;
- c. Memperhatikan kebijakan, peraturan, dan kemampuan yang ada;
- d. Mengembangkan struktur tata kelola keamanan informasi yang jelas;
- e. Mengembangkan rencana kontinjensi keamanan informasi;
- f. Mengorganisasi pelatihan keamanan informasi, dan hal lainnya.

Diharapkan dengan membuat strategi keamanan informasi, terdapat standar di Organisasi dalam mengimplementasikan keamanan informasi sehingga hasil pentest diharapkan tidak ada yang berulang di sistem lainnya di Organisasi dan memang butuh peningkatan secara berkesinambungan.





A close-up photograph of numerous fiber optic cables. The cables are thin, translucent rods that catch light, appearing as bright points of light or small lines of light. They are densely packed and radiate outwards from the center of the frame. The color palette is primarily shades of blue and green, with some white highlights where light reflects off the fibers. The background is a deep, dark blue, making the glowing fibers stand out.

Shulkhan

Terus Belajar Bergaul Dan Bertukar Ilmu

NGESEC

Hai, perkenalkan, nama Saya Shulkhan. Jadi ya panggil saja Shulkhan. Pakai H ya. Saya adalah orang biasa, yang terlahir dari keluarga biasa. Sebuah keluarga yang tidak memiliki latar belakang IT. Makanya Saya juga bukan anak yang terbiasa dengan Komputer dan teknologi internet sejak kecil.

Awal main komputerpun Saya masih mengetik pake 2 telunjuk wakkawak. Waktu itu Saya masuk ke sebuah SMP. Di hari pertama Saya diperkenalkan dengan silabus pelajaran. Yes, Saya langsung seneng karena ada pelajaran baru yang diberi nama TIK atau Teknologi Informasi dan Komunikasi. Senang sama pelajarannya? Nggak sepenuhnya benar sih. Saya senang karena disitu jadi sering bisa main Komputer. Dan sejak SMP inilah Saya jadi mau fokus ke dunia IT. Oh ya waktu itu Saya berpikir tentang IT nya cetek bener.

"Halah palingan cuman ngetik gini doang, main word, excel, ppt " kata Saya waktu itu.

Selain belajar TIK (baca saja main Komputer ya), ternyata pengetahuan mengetik dengan 11 jari (dua jari telunjuk bergantian seperti angka sebelas kan) berkembang. Saya belajar mengetik dengan benar di bangku SMP. Meskipun tidak ada yang ngajarin sih wakkawak. Mungkin karena insting ya, Saya jadi bisa nulis pake 10 jari (anjer sok"an bahas insting wakkawakwak). Komputer bagi Saya adalah salah satu hal menarik yang pernah Saya sentuh. Nah begitu nyentuh Komputer di SMP itu, jadi deh sampe sekarang. Karena

menurut Saya cara belajar komputer yang baik itu ya belajar langsung praktek. Jadi harus berani salah biar belajar gimana solved nya. Itulah mengapa Saya harus terus berdekatan dengan Komputer.

Singkat cerita Saya lulus SMP dengan nilai yang lumayan. Saya langsung mendaftar kesalah satu sekolah yang katanya salah satu yang terbaik di Yogyakarta. Oh ya, tempat Saya mendaftar ini bukan SMA lho tapi STM bos. Alhamdulillah Saya bisa masuk ke jurusan TKJ (Teknik Komputer dan Jaringan). Dari sinilah Saya mulai ada sedikit gambaran tentang dunia IT. Jadi dunia IT bukan hanya ketak ketik Saya seperti pemikiran Saya saat SMP, kelas 7 & 8.

Saya baru terbuka pemikiran dunia IT setelah mengikuti banyak pelajaran programming. Alhasil muncul keinginan Saya untuk menjadi programmer/ developer. Namun entah kenapa, saat masuk ke kelas 3 Saya tiba tiba merasa "wah ga ada feel ni di coding" saya berubah pikiran. Apalagi kebanyakan teman, fokus ke programmer juga membuat Saya berpikir "wah kebanyakan teman-teman udah mau jadi programmer ni, kenapa ga jadi yang beda aja? toh nanti juga dibutuhin". Dan Sayapun pindah fokus ke Sysadmin dikelas 3., dari situ belajar banyak hal dari siapin requirement server, instalasi, troubleshoot & maintenance (*regards to guru - guru SMK yang udah sabar ngajar anak didikmu yang satu ini :D wkwakkawwka*).

foto by Tangtungan Project



Masuk tahun ke 4 di SMK, Saya harus melakukan PKL atau magang atau nama kerennya intern. Saya daftar deh ke perusahaan Kelana Idea Sahabat atau Kelana Indonesia sebagai sysadmin. Sebuah pengalaman yang menarik dari situ belajar juga banyak hal - hal baru seperti *hardening server*, *optimasi*, *cloudflare*, dan sebagainya. selain kerjaan jadi sysadmin/devops diajarin juga *pentest* (thanks suhu @bernadsatriani) dari gimana *information gathering* yang optimal sampe *exploitnya + nulis report*. Akhirnya pernah sampe dapat report yang katanya *pentest* tapi pas dibaca kok kayak *report VA* doang, dan pas validasi bareng ternyata tidak ada yang valid :))

Pada suatu masa, ada sebuah event yang disebut "JAGONGAN IT". Event ini diselenggarakan oleh PT Gamatechno (Maturnuwun GT udah membuat event yang menarik dan berguna untuk semua), Kenapa Saya bilang pada suatu masa? Karena Saya lupa tanggalnya kapan itu, tapi yang ngisi ga bakal lupa, jadi coba tanya pada yang mengisi wkwkwk. Yang mengisi acara ini adalah salah satu teman *sharing*, ngopi, dan guru Saya, yang punya id telegram @bimosaurs. Dia saat itu membawakan materi *sql injection* dengan target bwapp. Dari mengikuti acara inilah akhirnya Saya sedikit tau tentang security. Saya juga kemudian disenggol sama om @DyanGalih.

"Di Yogyakarta ada lho komunitas security. Sering tu ngumpul tiap Rabu, di Kelas Pagi Yogyakarta (KPY). Namanya NgeSEC." ujar beliau sambil ketawa saat ngomong NgeSEC. Karena tertarik dengan materi yang dibawakan, begitu selesai pemaparan, Saya coba deh kenalan dan minta kontak pemateri. Setelah itu langsung coba deh dateng ke KPY, kenalan sama teman-teman



di NgeSEC. Orang-orangnya asik & baik, membuat Saya betah di komunitas. Dari sini Saya banyak mendapat ilmu baru. Pandangan Saya akan security makin terbuka. (*Regards to teman - teman NgeSEC, thanks buat teman - teman yang tidak bisa disebut satu persatu*). Kalau Anda tanya ke Saya "Jadi security itu apa?" Saya rasa jawabannya adalah.... Satpam wak wak wak

Oke dari cerita pengalaman kenal security pertama kali tadi, Saya juga ada kenangan kenalan sama ilmu satpam ini. Yaitu saat testing website punya salah satu teman NgeSEC, @djenova, bareng-bareng (thanks Hu, sudah dikasih tempat buat ngeraba-raba webnya wakwakwak). Setelah kenal, Saya juga main-main VM kloptrix, dvwa, sampai benar - benar hapal bug-bug yang ada disitu. Walaupun hapal doang, paham tidak wakwakwak.

Semua ilmu dan bidang IT dan computer, menurut Saya menarik sebenarnya. Tetapi mungkin Saya ingin fokus bagaimana menyerang dulu, sebelum belajar cara bertahan. Menurut Saya "*I need to learn how thief think before i learn how to defense*". Saat ini saja, kalau ditanya apa itu hacker, Saya akan jawab tidak paham. Sedangkan hardware hacking atau kata orang *open hardware*, Saya cukup tertarik. Risetnya itu lho, gila-gilaan. Mungkin nanti kali ya Saya akan coba melihat kesana. Mungkin sekarang belum waktunya kearah sana.

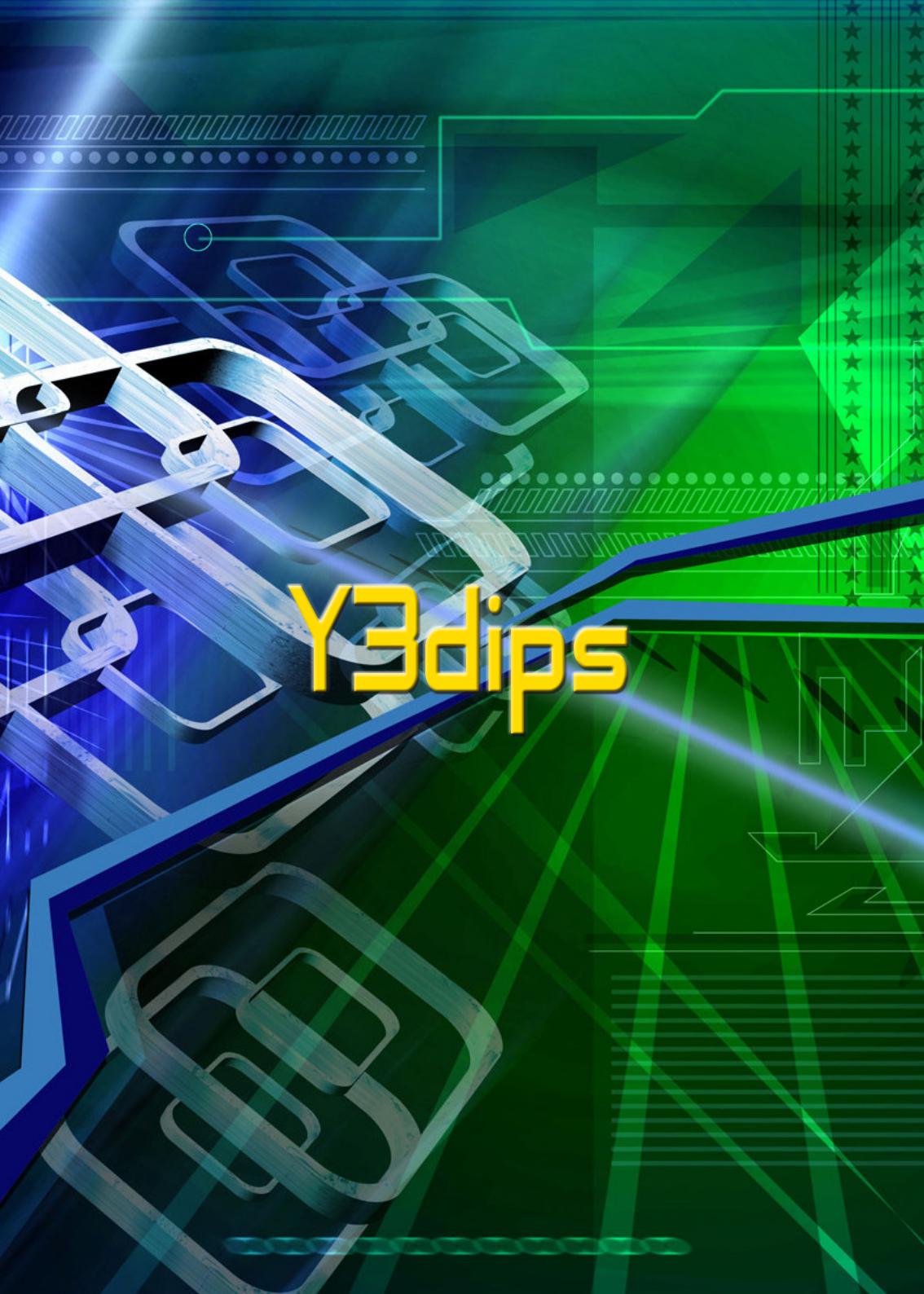
Selain itu, sudah banyak developer atau programmer membuat Saya dulu berpikir untuk memilih bidang security. Entah *blue team*, *red team* atau yang lainnya. Mereka masih sedikit. Jadi Saya putuskan untuk coba deh fokus di security. Sekarang waktunya Saya untuk lebih mendalami koding.

"Rejeki iku ora iso ditiru. sanajan padha lakumu, sanajan padha dodolanmu, sanajan padha kerjamu, hasil sing ditampa bakal beda. Isa beda ning akehe bandha, isa uga ana ing rasa lan ayeme ati". Kata kata inilah yang pada akhirnya membuat Saya memutukan untuk serius dan meraih cita-cita Saya, punya usaha sendiri, dan mungkin kuliah sampai mentok.

Terus belajar, bergaul dengan orang-orang pintar untuk bisa bertukar ilmu. Bergabung dengan beberapa komunitas IT di Indonesia yang lumayan banyak. Selama ini komunitas IT di Indonesia (kalau melihat dari grup yang Saya ikuti) cukup ramai. Meskipun kebanyakan di setiap grup hampir ketemu orang yang sama. Saya harap dunia IT dan security Indonesia saat ini makin aware tentang security, saling mendukung untuk hal yang lebih baik, "*keep low profile*" ini kalo kata salah satu suhuku. Seperti pepatah favorit Saya mengatakan "hidup kaya atau miskin itu takdir, namun kesederhanaan adalah sebuah pilihan (mas-mas top hunter)". Saya juga berharap, makin banyak orang baik yang share ilmunya di dunia IT dan security dunia.

Profil

1. Nama (real name) : Shulkhan
2. Panggilan sehari hari : Shulkhan
3. Tempat/Tanggal lahir : wah pas ga bawa ktp :3
4. Alamat : Yogyakarta
5. Handle origin : Epic Indonesia
6. Mobile :
 - Telegram : @tanpausernamee
7. Sosial Media (Facebook, Instagram, Twitter, dll) : gugling namaku dapet semua
8. Komputers spec :
 - Pertama : Toshiba satellite lupa serinya (Core i3 2310M -4 GB RAM - 500 GB HDD)
 - Sekarang : Asus Vivobook pro n580v (Core i7-7700HQ - 4 GB RAM - 1 TB HDD - 128 SSD)
9. Member of :
 - Community : NgeSEC
 - Projects : tidak ada. Bagi proyek om :(
10. What I like to do? : apapun asal senang dan baik untuk sekitar
11. What I dislike : Doesn't has respect for others
12. Favorite / Kesukaan :
 - Makanan/Foods : banyak :| angkringan & burjo utama wkwk
 - Minuman/Drinks : es teh + air bening idolaquee
 - Warna/Colours : biru, hijau, coklat
 - Jenis/genre Musik : Tergantung mood wakwakwak, bisa jazz, hiphop, pop, rock, instrumental
 - Band / penyanyi : Kebanyakan genre jadi gaada yang spesific fav band/ penyanyi :(
 - Movies/TV : The Shawshank Redemption, The Good Doctor(TV Series)
 - Place : tergantung situasi
 - Time : anytime asal kondusif
 - Hobby : nongkrong sama teman" sekolah, ngoprek/learn a new things waktu senggang, main game(PES, DOTA2, CSGO), olahraga
 - OS : windows 10, bawaan dari komputernya:(kan sayang kalau tidak dipake
 - Software : Burpsuite(karena multifungsi), telegram(karena banyak group, teman & guru baru buat belajar)
 - Bahasa programing : Python # belum bisa, proses belajar



Y3dips

More U feel Stupid. More clever U're Now.

Jangan tanya saya siapa. Karena saya manusia. Nama saya Ammar atau biasa juga dipanggil Y3dips. Saya suka belajar dan belajar. Quote "More you feel stupid, more clever you are" saya anggap tepat. Karena ketika kita merasa bodoh kita makin berusaha untuk menjadi tahu dan pintar. Ketika kita sudah merasa paling tahu, kita akan berhenti mencari tau. Yang lebih bodoh adalah orang yang tahu kalau tidak tau tapi tidak mau belajar dan mencari tahu.

Hal ini juga berlaku dalam bidang saya. Komputer. Perangkat 'bodoh' yang bisa membantu pekerjaan manusia. Perangkat yang seharusnya digunakan untuk membantu manusia, bukan menggantikan manusia. Sebagai sesuatu yang baru, computer adalah sesuatu yang menarik untuk kita terus cari tau. Menurut saya, belajarnya dengan mencari tau, membaca, menguji coba apa yang kita abaca atau kita praktikan, baca lagi, terus seperti itu.

Dalam bidang computer yang saya geluti, Security IT yang menjadi pilihan. Security sendiri sering menjadi bagian ilmu computer yang diandalkan dan diharapkan 100% namun tidak selalu bisa memuaskan. Karena Security IT tidak bisa diandalkan 100%. Nah kalau mau tahu lebih banyak atau lengkap tentang kesukaan saya di bidang Security IT, sudah saya ceritakan sebagian besar pada artikel SECSTORY 1, mungkin bisa membaca disana atau di <https://www.linkedin.com/pulse/me-pen-test-short-story-ahmad-muammar/>. Sedikit saya buka disini, awal tertarik dengan security, atau dunia IT saat

tahun 2000-an awal. Kala itu komputer masih menjadi hal baru. Security IT, (tahun 1999/2000-an) merupakan hal yang baru, sedikit yang berminat, sangat sedikit yang mengerti dan lebih sedikit lagi yang menguasai, suatu hal yang membanggakan bisa menguasainya lebih dulu dan menjadi bagian dari yang sedikit itu. Dan sayapun mulai mendalaminya.

Hacker atau seseorang yang sangat ahli dibidangnya (dalam hal ini komputer) sempat menjadi pembicaraan dikalayak saat kita bicara tentang security IT. Saat ini juga muncul istilah baru *hardware hacking* (*open hardware*). Ini adalah salah satu ide yang akan mempercepat pemerataan kemampuan dibidang hardware yang kita ketahui Indonesia sudah sangat-sangat tertinggal baik dari SDM, industri, dsb.

Dalam perkembangan dunia komputer, Open Source mulai muncul. Open source adalah salah satu jenis ide yang membuat pemerataan kemampuan serta target/kemajuan yang ingin dicapai di bidang teknologi bisa terwujud dengan relatif lebih cepat. Sayangnya dukungan pemerintah masih sedikit, dan masih kurang, mungkin karena ketidaktahuan, ketidakpedulian dan ketidakmampuan.

Yang mendukung perkembangan security IT di Indonesia sendiri, selain para pelaku juga munculnya komunitas komunitas IT. Di awal awal kemunculan, komunitas IT memang sempat sangat heboh. Saat ini sudah tidak seramai, seheboh, dan sebermanfaat dahulu untuk mengejar ketertinggalan. Saat ini anda bisa belajar secara langsung ke sumbernya lewat media audio video bahkan, tetapi tetap komunitas sangat amat berguna. Saya sih berharap akan banyak bermunculan generasi muda yang benar-benar belajar untuk kemajuan industri IT security di Indonesia. Selain itu, saya juga berharap semakin banyak dukungan pemerintah terhadap penciptaan ekosistem khususnya peningkatan sumber daya manusia, pembukaan lapangan kerja di bidang IT khususnya security di segala sektor khususnya di pemerintahan. Kalau secara skala besar, saya berharap munculnya inovasi dan teknologi-teknologi baru yang bermanfaat khususnya di bidang IT security.

Profil

1. Nama (real name) : Ahmad Muammar
2. Panggilan sehari hari : Ammar
3. Handle/nick : y3dips
4. Tempat/Tanggal lahir : Jakarta/198*
5. Alamat : Republik Indonesia
6. Handle origin : reverse spidey, gunakan substitusi pada huruf 'e' jadi '3'
7. Mobile : -
- Telegram : y3dips
- Lain lain : <https://linkedin.com/in/ammarwk>
- 8.Urls : <http://y3dips.echo.or.id>
9. Sosial Media (Facebook, Instagram, Twitter, dll) : twitter.com/y3dips
10. Computers spec :
 - Pertama :
 - Arachnids - Personal Computer (AMD 750 MHz, 1MB of SDRAM, 20 GB of Hardisk,
 - Dualboot OS with RedHat 7.3 Operating system && XP Ops sys
 - Sekarang : Raiser - Macbook Pro, Intel Core i7 2,6GHz, 16 GB of RAM, 250GB SSD, Mojave OS
 - Yang diidamkan : Macbook Pro 2019
11. Member of :
 - Community : echo, idseccnf
 - Projects : Membesarkan seclab.id :-)
12. What I like to do? : Reading, Discuss, Sharing
13. What I dislike : Debate
14. Favorite / Kesukaan :
 - Makanan/Foods : pempek, gado-gado
 - Minuman/Drinks : air putih
 - Warna/Colours : hitam
 - Jenis/genre Music : Currently not listening to any music.
 - Band / penyanyi : Currently not listening to any music.
 - Movies/TV : marvel movies occasionally/not watching tv anymore.
 - Books & Authors : Qur'an
 - Place : In front of Computer.
 - Time : 03:13:37
 - Hobby : Observe and Learn
 - OS (kenapa?) : Semua sistem operasi ok, tergantung kebutuhannya
 - Software (kenapa?) : Nmap, bahkan saat ini bisa melakukan aktifitas pentest dengan nmap saja
 - Bahasa programing : python

Penetration Testing is Dead?

Tema yang saya angkat kali ini mengenai materi yang saya sampaikan pada acara Infosec Awareness Night. Sebuah acara yang diselenggarakan oleh Bank Mandiri pada November tahun lalu. Materi saya saat itu berjudul "**pen-testing is dead?**"[0]. Saya rasa tema ini masih cukup relevan untuk saat ini, cukup menarik dan bermanfaat untuk teman-teman penggiat Keamanan Teknologi Informasi.

Saya mendapatkan ide untuk menyampaikan tema "Pen-Testing is Dead?" setelah terlebih dahulu saya berselancar di google. Saya menemukan bahwa tema ini sudah pernah dibawakan oleh pemateri lain di dunia Internasional. Ok, ternyata tema ini bukan hal baru yang sedang ramai di bicarakan orang. Bahkan sudah beberapa kali dibahas oleh orang lain. Setidaknya, saya berhasil menemukan 2 buah materi presentasi dengan tema yang sama, dengan mempergunakan google engine. Judul nya "Pen-Testing is Dead, Long Live the Pen Test"[1] dan "Penetration Testing Is Dead! (Long Live Penetration Testing!)"[2]

Tema ini pertama kali di sampaikan (setidaknya itu yang saya temukan via google) dalam konferensi keamanan komputer terbesar di dunia, "DEFCON 16", pada tahun 2008. Pembicara menyoroti awal-awal aktifitas penetration-testing yang lama-kelamahan menjadi kepada aktifitas yang hanya mengandalkan *tools vulnerability assessment* bahkan dia menyebutnya "scan now" pentest,

evolusi pentest, dan bagaimana pen-test pada abad 21, untuk lengkapnya dapat di lihat pada tautan diatas. Sedangkan pada 2014, Katie Moussouris yang merupakan Chief Policy Officer HackerOne pada kala itu menjelaskan mengenai pasar celah keamanan sampai kepada bug-bounty dan kesimpulan bahwa Bug Bounty tidak dapat menggantikan Penetration Testing. (untuk lengkapnya pun dapat di lihat pada tautan diatas).

Melihat fakta diatas, saya lalu berpikir mengapa pemikiran “Pen-Testing is Dead” ini adalah anggapan yang pernah (seringkali?) saya temui akhir-akhir ini. Mungkin penetration Testing bisa jadi dianggap Mati atau lebih tepatnya di anggap ‘tidak berguna’ oleh sebagian individu atau perusahaan. Setidaknya ada beberapa hal yang saya pribadi anggap menjadi alasan sehingga anggapan seperti itu ada. Saya sendiri mencoba melakukan kesimpulan berikut inilah penyebabnya:

1. Misconception
2. Bug Bounty Programs
3. Red Team
4. Agile Development
5. Industry 4.0 Technology

Sekarang mari kita bahas satu-persatu mengapa hal-hal yang membuat banyak individu, instansi ataupun perusahaan menganggap bahwa *penetration testing* sudah mati? atau tidak berguna, diatas.

1. Misconception – Kesalahan Persepsi

Individu (khususnya mereka yang tidak bekerja dibagian teknis teknologi informasi) sampai instansi dan perusahaan beranggapan bahwa percuma melakukan kegiatan *penetration testing*. Sebuah tes yang harus mereka bayar relatif mahal, sedangkan hasil dari kegiatan pen-test yang mereka lakukan tidak terlihat, tidak cukup membantu mereka menemukan isu keamanan yang berdampak kritikal. Mereka mungkin merasa telah rutin untuk setiap tahun melakukan kegiatan pen-test tetapi isu keamanan yang ditemukan bahkan hampir tidak ada, dan insiden keamanan atau *fraud* tetap saja terjadi bahkan setelah pen-test itu dilakukan. Hal Inilah yang menjadi alasan pertama kegiatan *penetration testing* yang seharusnya merupakan kegiatan yang paling mendekati aktifitas *attack* yang dilakukan oleh *attacker* di anggap tidak berhasil, tidak berguna, bahkan di anggap mati.

Saat ini hampir **tiap-tiap perusahaan penjual jasa keamanan IT merasa**

mampu dan yakin dapat melakukan kegiatan Penetration-Testing. Ditambah dengan persepsi dari perusahaan yang membutuhkan, bahwa **siapapun yang melakukan pen-test hasilnya akan sama.** Hal ini menyebabkan perusahaan akan memilih perusahaan penyedia jasa yang menawarkan harga ‘paling murah’ untuk kegiatan pen-test. Hal inilah yang akhirnya menyulitkan mereka sendiri untuk mendapatkan hasil yang maksimal, karena perusahaan jasa juga akan kesulitan untuk dapat men-deliver hasil yang memuaskan, dikarenakan harga *mandays* seorang *pen-tester professional* tidak akan dapat dibayar. Akibatnya, aktifitas yang dilakukan bukanlah pen-test tetapi hanya melakukan kegiatan *vulnerability assessment* mempergunakan tools dengan hasil yang kebenaran isu keamanannya belum di validasi.

Aktifitas *Vulnerability Assessment* yang mempergunakan aplikasi *scan* otomatis tentunya akan menghasilkan output yang sama siapapun yang mengerjakannya. Padahal kegiatan *penetration Testing* adalah kegiatan yang seharusnya dapat menggambarkan aktifitas yang dilakukan oleh *real attacker*. Tujuan dari *penetration testing* adalah mendapatkan akses setinggi-tingginya dan mengambil alih infrastruktur sebanyak-banyaknya dengan celah keamanan yang ditemukan. Sehingga tenaga *professional penetration tester* yang mengerjakan adalah menjadi pembanding.

Kesalahan persepsi lainnya, terkadang **penetration testing diharapkan untuk menemukan seluruh isu keamanan.** Ideal-nya, aktifitas *penetration testing* hanya peduli dengan isu keamanan yang dapat memungkinkan pen-tester untuk masuk (*gaining access*) dan melakukan eskalasi hak akses (*privilege escalation*). Jadi apabila ada 10 isu keamanan, tetapi dengan 1 isu keamanan pen-tester sukses masuk dan mengambil alih target, maka 9 isu lainnya tidaklah menjadi hal yang “penting” bagi pen-tester untuk di tindak lanjuti. Karena fokus selanjutnya adalah mendapatkan informasi sensitif/kritisikl dan mencoba masuk ke server/segmen lainnya. Dan juga aktifitas pen-test tidak akan bisa ideal untuk sama persis dengan aktifitas *Attacker* di karenakan keterbatasan *scope* & keterbatasan waktu. Sehingga kegiatan pen-test harus menyeluruh dan tetap harus di barengi dengan kegiatan *vulnerability assessment* dan *IT Security Audit*.

Meskipun ada persepsi-persepsi lain, tetapi setidaknya, hal diatas adalah 2 kesalahan persepsi terhadap aktifitas Penetration Testing yang cukup kritisikl menurut saya dan memicu anggapan bahwa aktifitas Penetration Testing itu tidak berguna.

2. Bug Bounty Program

Selanjutnya yang membuat banyak orang menganggap aktivitas *penetration-testing* ‘mati’ atau setidaknya menjadi tidak berguna adalah semakin maraknya program ‘bug-bounty’ akhir-akhir ini. Sebagian orang bahkan menganggap ‘bug-bounty’ dapat menggantikan aktifitas *penetration-testing* yang dilakukan oleh seorang *professional penetration tester*. Sehingga banyak perusahaan berlomba-lomba untuk membuat program bug-bounty dan menghilangkan aktifitas *IT Security Assessment* khususnya *penetration testing*. Bug bounty adalah salah satu aktifitas yang sedang marak di dunia Keamanan Teknologi Informasi khususnya baik di sektor swasta dan pemerintah. Kegiatan ini ‘diharapkan’ dapat membantu perusahaan untuk menemukan isu keamanan dengan relatif lebih cepat dan relatif lebih ‘murah’ serta mengarahkan para penggiat keamanan teknologi informasi untuk melakukan aktifitas yang positif.

Saya pribadi, menganggap bahwa bug bounty ini sebenarnya dapat disebut sebagai *evolusi* dari “*responsible disclosure*”. Sebuah aktifitas yang sudah sejak dulu dilakukan oleh para penggiat keamanan teknologi informasi, dimana para penemu isu keamanan menahan publikasi terkait isu yang mereka temukan sebelum menghubungi pihak yang memiliki isu keamanan.

Terdapat banyak hal positif dari program *bug bounty*. Salah satu yang bisa saya sebutkan atau *highlight* dari maraknya program ini adalah **Ikon membantu perkembangan sumber daya manusia**. Tidak adanya syarat professional atau edukasi, banyak penggiat keamanan baik yang sudah berpengalaman atau yang baru ingin mulai (bahkan pelajar) dapat langsung berkecimpung dan aktif melakukan aktivitas bug-bounty ini tanpa harus memiliki berapa tahun pengalaman, dan sertifikasi tertentu yang berbeda dengan professional penetration tester. Untuk negara kita yang memiliki pengguna internet dalam jumlah besar, serta banyaknya sumber daya manusia yang berminat terhadap pemanfaatan teknologi informasi, sudah di pastikan bahwa program seperti ini akan memberikan banyak manfaat khususnya bagi pengembangan sumber daya manusia dan ekonomi. Namun, saya juga ingin menyampaikan bahwa program bug-bounty ini juga memiliki beberapa kekurangan. Mungkin juga inilah yang menjadi alasan saya pribadi dan juga Katie (lihat gambar di bawah) untuk mengatakan bahwa Program Bug-bounty tidak dapat menggantikan Pen-test

Why Bounty?

Bounties are **not one size** fits all

Finding the **right approach** for customers

Creating a **win-win** for hackers & Orgs

Cannot Replace Penetration Testing!!

l1ckerone

14

Katie[2] menjelaskan kelebihan program *bug-bounty* terlebih dahulu kemudian berkesimpulan bahwa program ini “Cannot Replace Penetration Testing!!”. Berbeda dengan Katie, Saya mengemukakan beberapa batasan dari program Bug-bounty ini secara umum (meskipun ada beberapa program yang berusaha ‘mengakali’ batasan ini)

- Yang pertama adalah, **Bug Bounty terbatas pada target yang online.** Umumnya target program bug-bounty adalah infrastruktur aplikasi yang bisa di akses di internet seperti aplikasi web (publik) dan aplikasi mobile, sehingga infrastruktur lain sulit untuk termasuk, seperti infrastruktur network (wifi, wire, voip, dsb), infrastruktur physical, infrastuktur private dsb.
- Yang kedua adalah, **Bug Bounty umumnya dilakukan pada production state**, sedangkan umumnya terkait regulasi suatu infastuktur baru yang membutuhkan izin agar dapat beroperas, maka harus sudah di lakukan kegiatan pemeriksaan Keamanan Teknologi Informasinya, sehingga umumnya kegiatan pemeriksaan keamanan TI dilakukan di fase development seperti UAT, SIT.

- Yang ketiga adalah, **Bug Bounty tidak cocok untuk melakukan test terhadap private system.** Tentunya hal ini akan sulit di penuhi, sebagai contoh test terhadap perangkat HSM, mesin ATM, atau core-banking atau hanya sekedar akun e-banking yang mempergunakan token akan tidak mungkin memenuhi kebutuhan perangkat/token terhadap semua bug bounty hunter.

Selain beberapa hal diatas, ada beberapa hal yang menurut saya bisa menjadi mimpi buruk apabila perusahaan atau instansi belum siap ikut program bug-bounty. **Program Bug-bounty yang belum matang hanya akan menghancurkan brand perusahaan** yang membuat program bug bounty itu sendiri. Program ini juga dapat merusak hubungan dengan komunitas keamanan dan bisa jadi menghancurkan industri bug-bounty itu sendiri. Sebagai contoh, permasalahan yang umum terjadi adalah perusahaan yang memaksakan mengadakan program bug-bounty tidak memiliki sumber daya untuk mem-validasi dan memproses laporan yang diterima sehingga laporan yang masuk menumpuk dan tidak bisa di validasi dan di proses.

Permasalahan lain adalah dengan **membuka program Bug Bounty seperti mengundang perusahaan anda untuk diserang**, karena akan sangat sulit untuk membedakan mana Kriminal sesungguhnya dan mana *bounty hunters*, bayangkan betapa pusingnya tim SOC perusahaan anda menentukan hal tersebut, belum lagi apabila serangan yang banyak itu dapat membuat sistem perusahaan terganggu atau down.

Meskipun seperti saya sebutkan di atas, bahwa ada beberapa program bug-bounty yang ternyata bisa melakukan hal diatas dengan mempergunakan pihak ketiga, mengadakan program undangan, atau mekanisme lain untuk mengatasi keterbatasan tersebut tetapi sangat langka dan tidak umum.

Perlu diketahui bahwa aktifitas *bug hunting* yang tanpa izin atau tanpa adanya kesepakatan atau untuk situs/server yang tidak mengadakan program *bug bounty* sama saja dengan aktifitas kriminal dan sah-sah saja jika pihak tersebut melaporkan karena dijamin oleh Undang-undang ITE. Mungkin banyak terjadi kesalahan pahaman dalam melakukan aktifitas *bug bounty* khususnya di negara kita adalah dengan mencari target sendiri tanpa peduli instansi atau perusahaan tersebut memiliki program bug bounty atau tidak.

Seharusnya, *bug bounty* dapat mengurangi akses/aktivitas illegal peretasan, tetapi dengan tanpa adanya komunikasi dan informasi serta tidak maunya para *bug bounty hunter* ini mencari informasi terlebih dahulu, hal ini akan dapat merugikan banyak pihak, bahkan diri mereka sendiri, serta tren yang terjadi di negeri kita tercinta ini, **Bug Bounty bahkan mengarah kepada**

pemerasan (blackmail) dan pencemaran nama baik apabila tidak diberikan bounty atau bounty tidak sesuai. Hal ini sangatlah disayangkan dikarenakan malah akan merusak industri bug bounty itu sendiri serta komunitasnya.

Dengan berbagai alasan yang saya kemukakan diatas maka menurut saya **bug-bounty tetaplah tidak dapat menggantikan kegiatan Penetration Testing**, bahkan sebaiknya perusahaan yang ingin membuat program bugbounty sebaiknya terlebih dahulu melakukan kegiatan *IT Security Assessment* seperti *vulnerability assessment*, *security audit* dan *penetration testing* sebelum membuka program bug bounty.

Bug bounty sangat membantu peningkatan keamanan teknologi informasi, juga sumber daya manusia. Para bounty hunter dapat menjadikan aktifitas bug bounty-nya sebagai referensi untuk masuk ke dunia professional, disamping melalui jalur pendidikan formal dan sertifikasi.

3. Red Team

Hal yang ketiga yang membuat banyak individu, instansi dan perusahaan beranggapan bahwa kegiatan penetration testing tidak diperlukan adalah dengan adanya Red Team di instansi/perusahaan tersebut. Red Team adalah satu tim khusus yang terdapat di suatu perusahaan dan bertujuan untuk menemukan isu keamanan secara khusus serta mensimulasikan serangan. Memang banyak yang beranggapan red-team sama seperti pen-tester tetapi sebenarnya merupakan 2 hal yang berbeda, tentu saja karena istilah/namanya saja beda 😊.

Sebuah artikel menarik dari Rapid7 pada tahun 2016 (dan saya cukup sepandapat dengan artikel ini) bahkan membandingkan pen-tester dengan red-team seperti “pirates” vs “ninja”, hal ini dengan catatan bahwa para ninja ini juga melakukan kegiatan seperti penetration testing tetapi dengan tujuan lebih spesifik atau *targeted* untuk mensimulasikan serangan *Advanced persistent threat (APT)*.

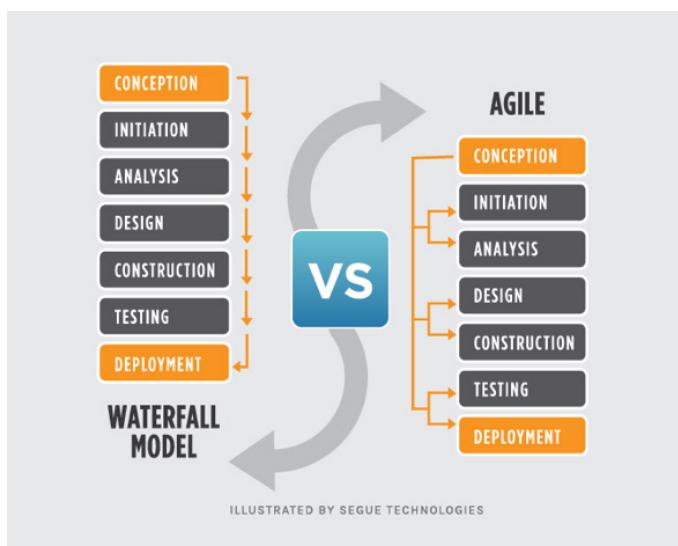
Kemudian tujuannya adalah untuk melakukan test terhadap kemampuan deteksi dan kemampuan respon dari perusahaan, dan sebaiknya perusahaan atau instansi sudah rutin dilakukan kegiatan penetration testing dengan hasil yang baik, telah melakukan patch dan perbaikan dari isu keamanan terlebih dahulu barulah di lakukan *red team assessment*.

Dan ada kata-kata menarik dari artikel tersebut adalah “*You would not want to use a Penetration Test to judge how well your incident response is and you would not want to perform a Red Team assessment to discover vulnerabilities.*”

4. Agile Development

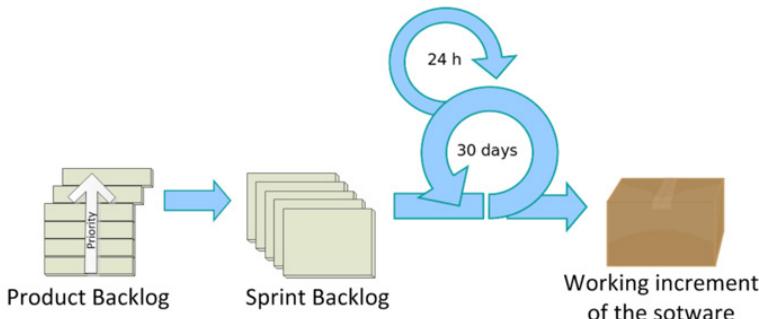
Yang keempat adalah metode development yang sedang berkembang dan menjadi tren saat ini adalah "Agile Methodology". Menurut Wikipedia Bahasa Indonesia, adalah metodologi pengembangan perangkat lunak yang didasarkan pada prinsip-prinsip yang sama atau pengembangan sistem jangka pendek yang memerlukan adaptasi cepat dari pengembang terhadap perubahan dalam bentuk apapun.

Jika kita melihat diagramnya yang saya ambil dari internet [4] yang membandingkan dengan metode waterfall yang umum dipergunakan dan umum dilakukan pen-test pada saat fase testing atau deployment. Sehingga munculah anggapan bahwa pen-test tidak dapat di gunakan pada metode 'agile development' dikarenakan fase-fase yang cepat.

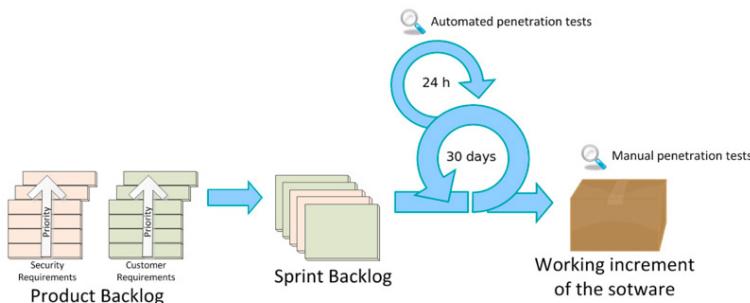


Meskipun saya pribadi sudah pernah melakukan pen-test untuk aplikasi yang mempergunakan metode agile development, tetapi untuk menjelaskan secara detail saya juga menemukan sebuah paper yang diterbitkan dalam sebuah jurnal internasional yang membahas hal ini[5].

Pada paper tersebut mereka memperlihatkan bagaimana dan kapan kegiatan penetration testing dilakukan pada metode "agile development" dalam hal ini mereka mencontohkan implementasi pada framework SCRUM. Berikut ini adalah gambar "scrum framework"



Dan berikut ini adalah gambar Kegiatan Penetration Testing pada “agile development” dalam hal ini pada framework scrum.



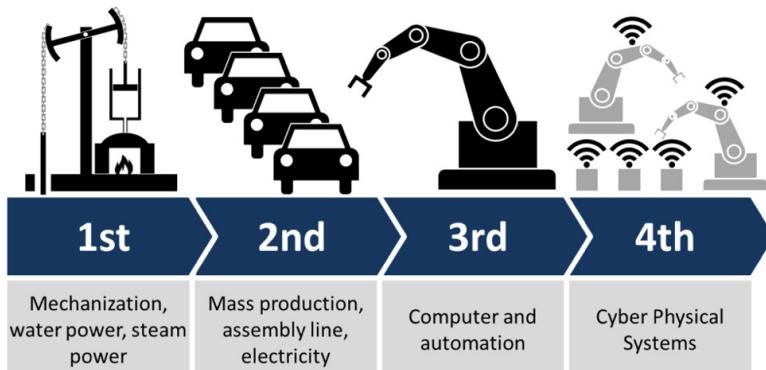
Mereka melakukan aktivitas Automated Penetration testing pada cycle yang kecil (tiap 1 hari/24 jam) untuk memproses setiap sprint, dan melakukan manual penetration testing untuk tiap release (30 hari/1 bulan)

Metode ini akan membantu mendeteksi isu keamanan khususnya saat masih dalam masing-masing sprint sehingga dapat langsung diperbaiki sesuai dengan sprint yang memiliki isu keamanan sekaligus sudah memastikan security best practices di implementasikan pada cycle development.

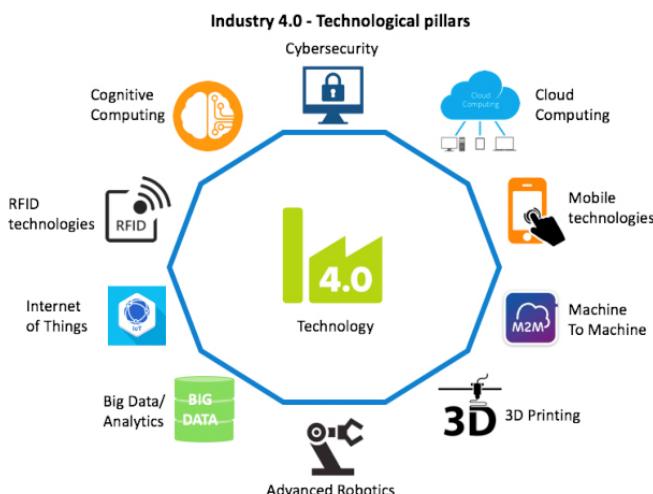
5. Industry 4.0

Industri 4.0 menjadi alasan bagi sebagian orang atau instansi/perusahaan yang selanjutnya memiliki anggapan bahwa penetration testing kedepannya atau pada industry 4.0 akan menjadi tidak berguna atau sudah tidak dibutuhkan lagi. Industri 4.0 adalah nama yang saat ini disematkan terhadap

tren proses otomatisasi dan pertukaran data pada teknologi manufaktur. Menurut Wikipedia[6] juga ini termasuk didalamnya adalah *cyber physical system*, *internet of things* (IOT) dan *cloud-computing*. Industri 4.0 umumnya direferensikan sebagai revolusi industry 4.0.



Industri 4.0 yang sudah menggunakan teknologi canggih dengan mempergunakan otomatisasi ini mungkin dianggap sebagian orang akan menghilangkan "the weakest link" yaitu manusia, sehingga nantinya teknologi ini akan lebih matang dan tidak memiliki isu-isu keamanan, kalaupun iya pastinya akan di monitor dan deteksi lebih baik di karenakan sudah terhubung secara terus-menerus.



Tetapi ternyata *cyber security* tidak dapat di hilangkan dari pilar teknologi di industry 4.0[7] itu sendiri. Hal ini terbukti untuk banyaknya publikasi terkait isu keamanan dari produk-produk IOT yang sudah banyak. Diantaranya adalah Mesin cuci piring berbasis IOT yang memiliki isu keamanan yang kritis.

Title:
Miele Professional PG 8128 - Web Server Directory Traversal
Author:
Jens Regel, Schneider + Wulf EDV-Beratung GmbH & Co., KG
CVE-ID:
CVE-2017-7240
Risk Information:
Severity: High
Risk Factor: Medium
CVSS Base Score: 5.0
CVSS Temporal Score: 4.0 CVSS3 Metrics: AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Vector: CVSSVF#(POC/G1/OF/N/C)
CVSS Environmental Score: 3.0
Timeline:
2016-11-16 Vulnerability discovered
2016-11-18 Asked for security contact
2016-11-20 Received response from product representative
2016-12-03 Send details to the Miele product representative
2017-01-03 Received response from product representative
2017-02-03 Asked for update, no response
2017-02-23 Public disclosure
Status:
Published
Affected Products:
Miele Professional PG 8128 (washer-disinfector) with ethernet interface.
Vendor Homepage:
https://www.miele.co.uk/professional/large-capacity-washer-disinfectors-560.htm?partno=PG_8128
Details:
The corresponding embedded webserver "PT10 WebServer" typically listens to port 80 and is prone to a directory traversal attack, therefore an unauthenticated attacker may be able to exploit this subsequent attacks.
Proof of Concept:
-F telnet 192.168.3.1 80
Trying to connect...
Connected to 192.168.3.1.
Device: PT10 WebServer
GET /..../etc/shadow HTTP/1.1
HTTP/1.1 200 OK
Date: Mon, 27 Feb 2017 11:09:50 GMT
Server: PT10 WebServer
Content-Type: application/octet-stream
Last-Modified: Fri, 22 Feb 2013 10:04:40 GMT
Content-Disposition: attachment; filename="";/etc/shadow"
Accept-Ranges: bytes
Content-Length: 52
root@192.168.3.1:~\$./shp...|[2001:10932:0:99999977:
File:
We are not aware of an actual fix.

Sebagai Pilar dari Industri 4.0 yang masih dan akan terus berkembang maka sudah dapat di pastikan bahwa produk-produk industry 4.0 sangatlah membutuhkan untuk dilakukan tes uji keamanan (IT Security Assessment), khususnya *penetration testing*.

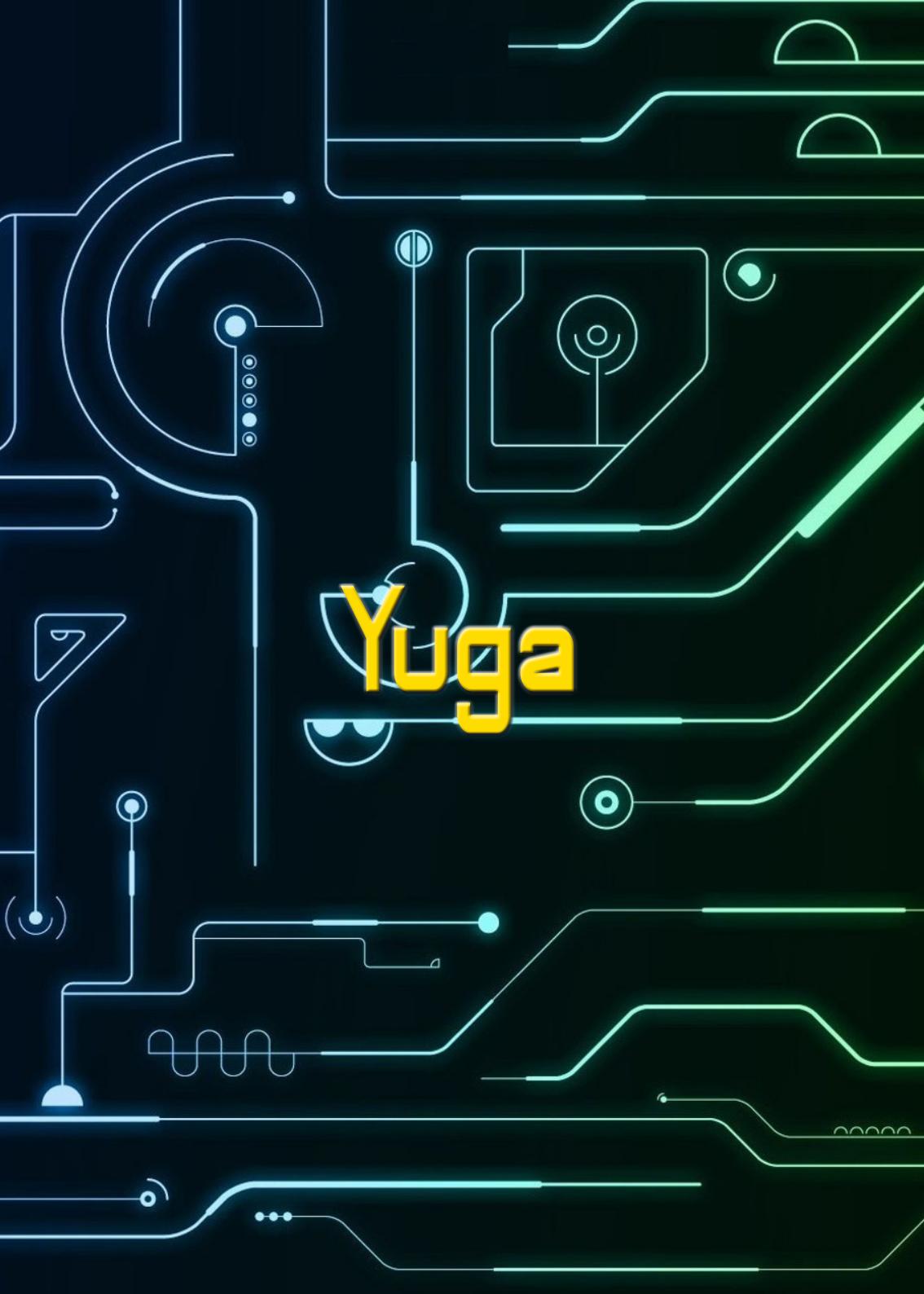
Penetration Testing is not Dead!

Akhirnya, kita atau setidaknya saya sampai kepada suatu kesimpulan bahwa kegiatan *penetration testing* tidaklah mati, bahkan masih sangat di perlukan dan masih terus harus ber-evolusi untuk mampu beradaptasi dan menjadi sesuai dengan harapan untuk dapat tetap membantu meningkatkan dan memberikan rasa aman dan nyaman bagi pengguna.

Saya juga optimis bahwa kegiatan *penetration testing* akan menjadi lebih baik lagi, disertai dengan peningkatan jumlah sumber daya manusia, peningkatan kemampuan dari tiap-tiap individu sebagai *professional penetration tester*, keseriusan perusahaan penyedia jasa IT Security yang tidak hanya mengedepankan keuntungan dan khususnya dengan pemahaman yang semakin meningkat dari user, instansi dan perusahaan mengenai kegiatan *Penetration Testing* itu sendiri. Jadi, sekali lagi saya katakan bahwa "**Penetration Testing tidaklah Mati!**".

Referensi :

1. "Pen-testing is dead?" – Ahmad Muammar WK - <https://www.slideshare.net/y3dips/pentesting-is-dead>
2. "Pen-Testing is Dead, Long Live the Pen Test" - Taylor Banks & Carric - Defcon 16 (2008) - <https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-banks-carric.pdf> - diakses terakhir 29 April 2019
3. "Penetration Testing Is Dead! (Long Live Penetration Testing!)" - Katie Moussouris (Chief Policy Officer - HackerOne) - Pen Test Hackfest Summit & Training (November 2014) - <https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1493862762.pdf> - diakses terakhir 29 April 2019
4. "Penetration Test vs. Red Team Assessment: The Age Old Debate of Pirates vs. Ninjas Continues" dapat dibaca di <https://blog.rapid7.com/2016/06/23/penetration-testing-vs-red-teaming-the-age-old-debate-of-pirates-vs-ninja-continues/> - diakses terakhir 29 April 2019
5. "Diagram Waterfall vs Agile Development Methodology" - <https://www.seguetech.com/waterfall-vs-agile-methodology/> -diakses terakhir 29 April 2019
6. "Penetration Testing in Agile Software Development Cycle (scrum framework)" (International Journal on Cryptography and Information Security (IJCIS), Vol. 5, No. 1, March 2015) membahas hal ini berjudul - Martin Tomanek and Tomas Klima dan dapat diakses di <https://arxiv.org/ftp/arxiv/papers/1504/1504.00942.pdf> - diakses terakhir 29 April 2019
7. Industry 4.0 - https://en.wikipedia.org/wiki/Industry_4.0 - diakses terakhir 29 April 2019
8. Technologies for industry 4.0.Image - https://www.researchgate.net/figure/Technologies-for-industry-40_fig1_319944621 - diakses terakhir 29 April 2019
9. Miele Professional PG 8528 - Directory Traversal - <https://www.exploit-db.com/exploits/41718> - diakses terakhir 29 April 2019



Yuga

Anda Menguasai dan Mengenalnya Dengan Baik, Komputer Mempermudah Pekerjaan Anda

Salah satu yang saya suka dari komputer adalah bisa memudahkan pekerjaan seseorang yang menggunakan. Tanpa memandang siapa Anda dan bagaimana Anda. Selama Anda menguasai dan mengenalnya dengan baik, komputer dapat mempermudah pekerjaan Anda. Itulah komputer dimata saya.

Oh ya, kita belum berkenalan. Nama saya Muhammad Yuga Nugraha. Biasa dipanggil Yuga. Saat membuat tulisan ini, saya duduk di bangku kuliah kampus saya di sebuah kota kecil yang menarik, Yogyakarta. Ya, saya sedang kuliah di semester 4 di sebuah kampus. Semua ini bisa saya capai dengan cara yang berbeda dari teman teman saya pada umumnya. Saya bisa disini karena komputer.

Saya sejak lama tertarik dan belajar komputer. Dari pengenalan sekilas, saya amati dengan dan akhirnya saya menemukan hal hal menarik yang akirnya membuat saya menjadi sahabat. Jadi jika kalian bingung apa yang ingin kalian pelajari, cobalah semua terlebih dahulu secara sekilas, pasti ada salah satu materi atau bidang yang menarik perhatian kamu. Setelah itu berusahalah untuk mencari tahu dan memperdalam materi atau bidang tersebut. Seperti yang dikatakan oleh quote favorite saya, “*Learn by doing and explore more what you want but fokus on one goal*”, belajar sambil melakukan, selalu eksplorasi dan mengembangkan kan pengetahuan tapi tetap fokus pada tujuan awal. Quote ini saya terapkan dalam kehidupan

sehari hari, terutama jika berhubungan dengan komputer dan ilmunya. Saya memiliki ketertarikan didunia keamanan informasi terutama aplikasi web dan berfokus dibidang infrastruktur salah satunya *cloud*. Bidang dari ilmu komputer yang paling saya sukai adalah *Cloud*. Bahkan cita-cita terbesar saya adalah mengikuti sertifikasi disalah satu *Cloud* maupun infrastruktur seperti aws, *google cloud*, *docker* dan sebagainya. Memang sih tidak harus, tapi itu merupakan bukti formal akan kemampuan saya. Keinginan saya yang lebih besar adalah bisa belajar lebih banyak lagi dari orang-orang yang piawai terutama yang ada diluar indonesia serta menambah relasi.

Sesuai dengan pengertian komputer sebagai alat yang digunakan seseorang untuk mempermudah pekerjaannya, dengan membuat program yang berguna dalam aspek tertentu, maka ada beberapa hal yang sudah saya buat. Untuk saat ini saya lebih sering menggunakan docker sebagai media development environment pada local komputer dengan membuat beberapa image seperti Web server, CMS dan lain-lain agar mudah digunakan dalam tahap development.

Security IT, Sangat Penting Bagi Kita

Tentu saya juga tertarik dengan *IT Security*. *Security* adalah hal yang sangat penting untuk diperhatikan oleh masyarakat sekitar. Seperti kita ketahui, *security* menyangkut keamanan informasi berbagai data apalagi privasi dalam dunia maya. Awal ketertarikan saya ke dunia IT adalah bahasa pemrograman. Saat itu, saya masih duduk di bangku SMP. Di bangku sekolah menengah pertama ini saya mempelajari html, css dan php. Entah kenapa, saat itu saya merasa kurang belum puas. Saya mulai melirik dan mencoba mempelajari dunia lain (selain windows). Dunia GNU/Linux. Disinilah pertama kalinya saya kenal dengan dunia komunitas. Sebuah dunia dimana orang-orang saling berbagi informasi yang mereka miliki. Saling membantu menyelesaikan permasalahan dengan informasi-informasi tersebut. Mereka juga menyelesaikan masalah bersama-sama melalui diskusi dan mencoba hal-hal baru.

Kenikmatan bergabung dengan komunitas ini membuat saya terus eksplor. Saya banyak bergabung dengan beberapa komunitas. Meskipun hanya sebagian komunitas yang saya ikuti dengan aktif didalamnya. Hal ini lebih dikarenakan keterbatasan waktu yang saya miliki. Tentu akan sangat sulit dalam me-manage waktu, ketika kita mengikuti banyak komunitas.



Setelah beberapa bulan saya mempelajari mengenai GNU/Linux dengan mencoba remastering, customizing desktop dan sebagainya, tahun 2017 saya mulai mengenal dunia baru. Saat itu barulah saya mengenal dunia security melalui sebuah projek sistem operasi yang bernama “dracOs”.

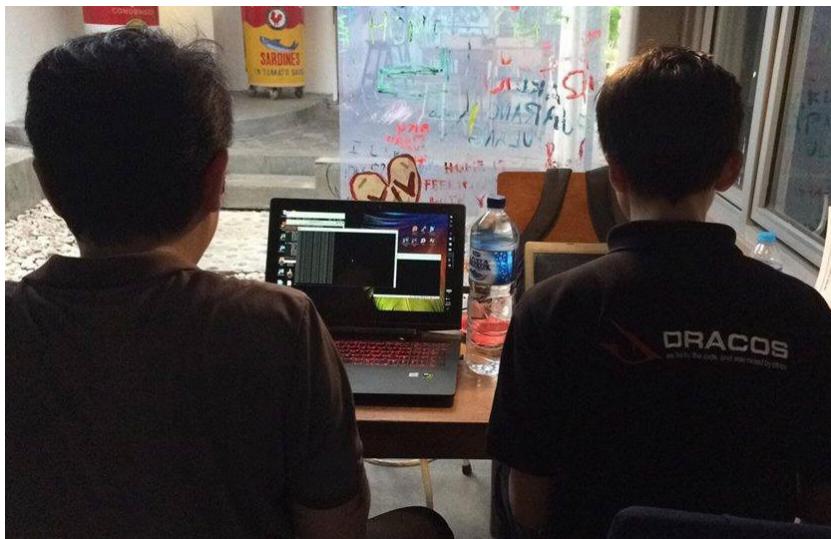
Awal saya melihat sistem operasi “dracOs” ini sangat menarik. Karena meskipun dari sisi tampilannya *old style*, tetapi *cool* ketika digunakan. Saat itu saya sama sekali belum tahu mengenai security dan ilmunya. Saya hanya terpikirkan untuk bisa tergabung ke projek tersebut. Saya sangat bersemangat dan ingin menambah pengalaman.

Saya kemudian mencoba mengikuti tesnya. Meskipun saat itu tidak ada respon mengenai tes tersebut tapi saya tetap menunggu. Hasilnya setelah bersabar beberapa lama, saya akhirnya diajak bergabung kedalam tim dracOs. Saat itu saya tahu, karena status saya disini, masih belum bisa berbuat banyak. Namun saya juga berusaha melakukan yang terbaik yang saya bisa. Meskipun hanya sekedar menjawab pertanyaan untuk troubleshooting maupun yang lainnya. Atau mungkin bisa disebut sebagai *Technical Support*. Disinilah saya dituntun untuk belajar mengenai security perlahan-lahan.

Karena saya terlalu fokus dalam sebuah komunitas membuat saya jadi malas belajar padahal saat itu mau menjelang ujian akhir atau kelulusan SMA, ketika ujian pun saya tidak benar benar belajar justru saya malah asyik belajar GNU/Linux dengan mengekplorasi sendiri dan berdiskusi dibeberapa komunitas ketika ada masalah, alhasil sayapun tidak masuk perguruan tinggi negeri yang diinginkan. Sebenarnya kalau mau jujur sayapun tidak sungguh-sungguh berniat perguruan tinggi negeri.

Namun Tuhan memberi jalan kepada saya. Gagal di perguruan tinggi negeri saya diterima di sebuah perguruan tinggi di Yogyakarta Mungkin inilah yang dimaksud rejeki lain yang Tuhan berikan. Saya sendiri menyadari kalau tidak termasuk orang-orang cerdas (yang masuk PTN). Bahkan tidak terpikirkan sama sekali di kepala saya untuk kuliah di kota pelajar Yogyakarta. Saya bersyukur ada jalan lain untuk menempuh kesuksekan. Menurut saya, kesuksesan tidak harus melulu dari kuliah PTN ataupun pendidikan diatasnya lagi. Saya masih bisa kuliah di Yogyakarta, meskipun swasta tapi tidak masalah.

Ketika sudah datang dan mengenal yogya, baru terpikirkan alasan saya kenapa tiba tiba ingin sekali merantau ke Yogyakarta. Ya... karena "Komunitas". Disini saya tidak punya kerabat maupun teman dari tempat asal saya sendiri. Jadi bisa dibilang modal nekat ke Yogyakarta dengan alasan yang tidak masuk akal yang akan saya simpan sendiri. Namun justru disinilah



perjalanan saya dimulai dengan bergabung disebuah komunitas bernama Ngesec. Saya berkenalan dengan teman-teman baru dari wilayah yang berbeda, apa ini membuat saya senang? ya justru bisa dibilang seperti ini "enaknya merantau bisa kenal orang yang berbeda dari daerah yang berbeda juga. Ini lebih menyenangkan dibandingkan tinggal dan gaul dikota asal yang orangnya itu-itu saja. Suasana tidak berubah mungkin juga ilmu yang didapat tidak sebanyak seperti merantau". Di Yogyakarta saya kuliah bersama salah satu rekan developer dracOs yang belum pernah saya kenal dekat. Hanya pernah bertemu sekali ketika dracOs meetup Jakarta diakhir tahun 2016.

Komunitas Ngesec yang baru saya kenal ini, tidak hanya membahas seputar security tetapi bidang lainnya pun ada. Kalau menurut saya sih bisa disebut sebagai komunitas all in one. Disana, meski tidak secara keseluruhan, ada orang-orang dengan kemampuan sebagai *Pentester, Programmer, Sysadmin, Network engineer* dan lain-lain.

Meskipun berstatus sebagai mahasiswa, saya tetap aktif dalam mengikuti komunitas ngesec ini. Dan dengan kemampuan saya, akhirnya saya mendapat kesempatan untuk bekerja disebuah perusahaan *Solution Provider* sebagai *System Administrator* secara *remote*. Dengan pekerjaan baru ini, tentu saya harus tetap update berita mengenai keamanan informasi dari luar maupun lokal. Apalagi saat ini, diperusahaan saya bekerja baru akan menerapkan penetration testing pada aplikasi yang dipakai. Mungkin kalian tidak tau bahwa masih banyak sampai sekarang beberapa institusi maupun perusahaan yang belum memperdulikan pentingnya pentest dalam mengamankan data user maupun client.

Nah, yang menarik dalam dunia security adalah bagaimana seorang IT Security dapat menerobos masuk ke sebuah sistem yang bukan miliknya dengan melakukan penetration testing. Sebuah pekerjaan yang ternyata memiliki metodenya sendiri dan juga langkah-langkah yang harus dilakukan serta aturan mainnya tersendiri. Dan disinilah saya mulai memahami pentest. Saya bekerja dengan mempelajari jenis metode-metode didalamnya dan mencobanya serta update informasi seputar tools maupun berita mengenai hacking/dunia security.

Jika ditanya apa sih *Hacker*? Saya akan menjawab *Hacker* adalah seseorang yang melakukan pengujian keamanan sebuah system. Menurut saya, masyarakat sering kali salah beranggapan mengenai hacker karena dari awal sudah ada yang mendoktrin bahwa *hacker* adalah orang jahat

di dunia maya. Selain itu ada *hardware hacking* (*open hardware*). Sebuah hal yang sangat menarik. Terutama jika dilakukan pada beberapa alat yang sering digunakan dalam kegiatan sehari hari. Karena ini menyangkut *hardware* dan *IoT*, *hardware hacking* juga akan menambah resiko keamanan sangat tinggi. Bukan lagi software yang didapatkan aksesnya tetapi hardwarenya secara penuh dapat dikendalikan. Jika sudah demikian bisa jadi kan operasional pekerjaan Anda juga dikendalikan.

Begitu banyaknya aplikasi seringkali membuat orang bingung. Nah salah satunya *opensource*. Buat saya *opensource* adalah software yang sangat fleksibel. Hal ini disebabkan oleh tidak banyak aturan yang mengikat software tersebut. Karena sifatnya terbuka, setiap orang dapat dengan mudahnya mengembangkan aplikasi yang sudah ada. Sehingga aplikasi ini akan berkembang lebih cepat dibandingkan aplikasi yang dikembangkan *vendor* dan tidak di-share secara terbuka. Tapi dari hal ini ada juga sisi buruknya yaitu, dari segi managemen project aplikasi serta *source code* yang mungkin bisa saja disisipi code iseng (yang berfungsi untuk merusak).

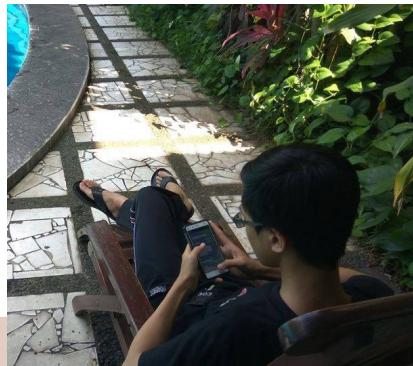
Saya sendiri pengguna dan pengagum Archlinux, karena customizable dari awal instalasi sistem operasi ini masih clean. Cocok untuk menginstal aplikasi yang dibutuhkan walau terkadang ada beberapa dependensi yang belum terpasang. Karena itu saya mengagumi Linux Torvald dan Richard Stallman. Merekalah yang menciptakan projek yang sampai sekarang digunakan banyak orang diseluruh dunia dan akan terus berkembang dari masa kemasa. Merekalah pelopor kernel Linux dan sistem operasi baru GNU/Linux yang tidak akan pernah berhenti berkembang secara code maupun donasi dari orang-orang yang peduli akan *opensource*.

Di Indonesia sendiri *opensource* tidak terlalu mendapat dukungan dari pemerintah. Hal ini karena masih ada keraguan dari pemerintah pada komunitas. Tapi hal ini sangat jelas karena pemerintah tidak mau jika ada hal-hal yang tidak diinginkan terjadi. Menurut saya ini menjadi hal penting yang perlu didiskusikan antara pemerintah dan komunitas dengan berdiskusi untuk mencari jalan tengahnya seperti apa.

Komunitas IT di Indonesia saat ini, bisa dikatakan sudah lebih maju. Sudah banyak komunitas yang mampu mengadakan event seperti seminar dan workshop kepada masyarakat secara gratis maupun berbayar, untuk membagikan ilmu yang diperlukan oleh masyarakat, seperti security awareness. Hal seperti ini menurut saya harus banyak dilakukan karena

banyaknya masyarakat yang belum tahu mengenai keamanan privasi mereka sama sekali setidaknya dapat menjaga.

Saya sendiri berharap, pemerintah dapat bekerja sama dengan komunitas untuk menyelenggarakan *security awareness* kepada masyarakat yang diera ini sudah serba instan dengan menggunakan internet. Dan untuk tingkat dunia, saya mengharapkan berkembangnya teknik teknik baru dalam melakukan hacking serta pengamanannya atau mengurangi resiko.



Profil

1.	Nama (real name)	:	Muhammad Yuga Nugraha
2.	Panggilan sehari hari	:	Yuga
3.	Handle/nick	:	jerukitumanis
4.	Tempat/Tanggal lahir	:	Bandung, 28 Januari 2000
5.	Mobile	:	
	- Telegram	:	jerukitumanis
6.	Komputers spec	:	
	- Pertama	:	ASUS i3-4010U RAM 8Gb SSD 256Gb Nvidia 740M
	- Sekarang	:	MacBook Air 2017 RAM 8Gb SSD 128Gb Intel HD Graphic 6000
	- Yang diidamkan	:	Thinkpad X1 Carbon
7.	Member of	:	
	- Community	:	NgeSEC, Docker
	- Projects	:	Anisble and Docker
8.	What I like to do?	:	Mengeksplor hal baru
9.	What I dislike	:	Kebosanan
10.	Favorite / Kesukaan	:	
	- Minuman/Drinks	:	Jus jeruk
	- Warna/Colours	:	Biru
	- Jenis/genre Music	:	Pop
	- Movies/TV	:	Pirates of Carribean
	- Hobby	:	Berenang
	- OS	:	Archlinux
	- Bahasa programing	:	Python, Bash, Javascript, C++

Zet

Keterbatasan tidak membuatmu lemah, *keep fight!*

Bermain kucing-kelingan, *hide and seek*, memasuki satu warnet ke warnet lain, *menonaktifkan online mode* pada facebook, hampir menjadi kegiatan rutin bagi kami para santri 'nakal' yang penasaran dengan internet dan teknologi. Internet menjadi barang yang terlarang di lingkungan pesantren kami. *Rolling diatas tanah, push-up, sit-up, gundul, diguyur*, menjadi makanan keseharian buat mereka yang melanggar, yang ketahuan ☺. Di luar sana, teknologi begitu dikedepankan. Hampir diseluruh lini kehidupan menggunakan teknologi komputer dan internet. Disini kami berbeda.

Jika teman-teman sebayaku sibuk bermain facebook, chatting dengan perempuan, bermain game online (2014 masih *boming* game PointBlank), berbeda dengan santri yang lain, aku lebih tertarik dengan membaca dan diskusi di group" facebook maupun forum online yang dikenalkan oleh temanku. Mendapat cerita-cerita tentang *hacking* dan *hacker* menjadikanku penasaran. Aku lebih tertarik untuk mencari tahu tentang *hacking* ketika ada kesempatan menggunakan internet.

Walaupun internet terlarang di pesantren, tapi tidak dengan buku. Karena keterbatasan, aku juga bukan termasuk orang yang dengan mudah bisa membeli buku. Jujur aku 'iri' dengan mereka yang mampu memiliki buku-buku itu. Walau begitu, aku berusaha mempelajari komputer dengan meminjam buku ke teman-teman yang ada. Tentu dengan keterbatasan pengetahuan,

saat itu aku nggak paham blassssssss, nggak ngerti maksud ini dan itu. Tapi aku yakin suatu saat nanti pasti akan mengerti dengan sendirinya.

Salah satu ustazku sangat mendukung niatku untuk mempelajarinya, saat mengetahui keingintahuanku tentang komputer dan *hacking*. Aku sangat berterimakah kepadanya. Saat para santri tidak boleh mengakses internet, aku dibolehkan mengakses internet. Beliau percaya jika aku menggunakan internet untuk belajar. Aku tidak menyia-nyikan kesempatan ini, aku banyak belajar di warnet-warnet setempat. Sewajarnya belajar tanpa mentor, aku belajar *hacking* dan komputer secara serabutan. Hehe..

Suatu ketika, saat sedang asik berselancar di dunia maya, aku menemukan ada *exploit RCE* baru yang keluar. Akupun mulai coba-coba *exploit* itu di web-web yang bertebaran di google. Aku coba-coba report terkait celah keamanan tersebut. Tanpa disangka, salah satu website kamera terkenal di Indonesia merespon baik, setelah aku laporan celah keamannya. Aku diundang ke Jakarta, diajak jalan-jalan, menginap di hotel, dan diberi uang saku dari atasannya. Kejadian ini menjadi pengalaman yang 'nampol' buatku, agar terus selalu belajar dan menyebarkan kebaikan kepada orang lain ☺.

Berangkat dari pengalaman diatas, aku jadi lebih interest pada dunia IT Security. Walaupun aku baru lulus dari pesantren dan tidak memiliki dasar-dasar IT atau *programming*, aku berniat untuk bisa. Aku tidak menyerah dengan keadaan ini. Aku tidak menyalahkan diri ini karena belajar di pesantren. Walaupun sejurnya aku 'iri' dengan mereka yang mempelajari IT di sekolah-sekolahnya, anak-anak SMK yang sudah bisa ini itu. Tapi ya sudahlah. Aku jalani saja peran hidupku saat ini, dan aku selalu yakin untuk bisa terus melangkah. ☺

Berkat Ijin Khusus Dari Ustadz, Aku Bisa

Oh iya, namaku Habiburrohman, teman-teman memanggilku dengan nama itu, atau Rohman, atau di komunitas dan lingkungan kampus saat ini dipanggil Zet. Terlahir dari lingkungan pesantren yang tidak ada hubungannya dengan dunia internet apalagi dunia IT Security. Bermula ketika ustazku mengizinkanku mengakses internet, aku banyak belajar di internet. Tahun 2017 aku memutuskan untuk kuliah di Yogyakarta, dengan satu alasan "aku ingin bergabung dengan komunitas IT". Aku yakin pasti ada komunitas IT di kota pelajar itu. Mengikuti berbagai acara gratis, workshop ini dan itu, sampai akhirnya bertemu dengan komunitas bernama NgeSEC pada acara Jogja Rembug waktu itu:



Jogja Rembug, 17 November 2017



Foto NgeSEC waktu Jogja Rembug, dan aku belum join 😊

Aku Menemukan Diriku di NGESEC

Awalnya aneh sih, katanya kumpul di Kelas Pagi Yogyakarta, aku fikir kalau ngumpulnya itu pagi hari, ahahaha. Ternyata KPY (Kelas Pagi Yogyakarta) itu adalah nama tempat buat belajar, ada yang belajar photography, menari, ada coffee, dan lain-lain. Komunitas NgeSEC menggunakan salah satu ruangan untuk ngumpul rutin setiap rabu. Diajak @orangmiliter di telegram, dengan modal muka tembok, aku coba ikut gabung ngesec hari rabu malam. Di komunitas ini aku menemukan jati diri, sesuatu yang kucari-cari ada disini. Hampir setiap rabu malam berkumpul, bercanda, bercengkrama, curhat, belajar, menjadikan komunitas ini seperti keluarga ke-2 dihidupku. Suasana keakraban ini menjadikan jogja semakin istimewa 😊.



Aku bertemu dengan orang-orang hebat di komunitas ini, menggali pengalaman-pengalaman mereka, menimba ilmu dari mereka, menjadikan aku banyak belajar dan berkembang di komunitas. Tak henti sampai disini, aku juga banyak belajar dari komunitas lain, seperti Surabaya Hacker Link (SHL). Di komunitas SHL aku juga banyak belajar tentang security dan ctf. Bertemu langsung dengan member SHL memperkaya keilmuan dan pengalaman, dan aku sangat berterimakasih dengan mereka yang tentunya tidak bisa aku sebutkan namanya satu persatu.

Februari 2018, aku diajak oleh teman dunia maya ku untuk mengikuti kompetisi CTF (*Capture The Flag*) Born To Protect (<https://www.borntoprotect.id/>). Born To Protect adalah sebuah program dengan aktifitas terpadu untuk menjaring *gladiator-gladiator* muda dibidang *Cyber Security*. Program ini digagas oleh Xynexis dan didukung penuh oleh KOMINFO. Dengan senang hati aku menyambut ajakan temanku itu, berbekal sedikit pengalaman dan bantuan teman-teman, aku berhasil masuk 100 besar gladiator yang dipilih untuk dididik menjadi Jagoan *Cyber Security* pada event DIGITAL CAMP selama 2 minggu.

September 2018, muncul sebuah *platform Bug Bounty* asli dari Indonesia bernama *Cyber Army ID*, lseng-iseng aku mendaftarkan diri, meski tanpa pengalaman mengikuti Bug Bounty Program. Aku coba-coba untuk mencari *vulnerability* dan mereport terkait temuan. Kalau melihat *history* awal-awal ngereport itu, ya ampun report-report receh pun ⚡. Hampir setiap hari aku menanti program-program di *Cyber Army*, mencoba dan terus mencoba. Awal 2019 aku termasuk 5 top bug hunter di *Cyber Army* dan mendapatkan penghargaan dari CA.

Februrari 2019, tepat satu tahun aku bergabung dengan komunitas ini, banyak pelajaran dan pengalaman yang aku dapatkan, mengikuti kompetisi CTF, mengikuti Bug Bounty Program, dan lebih mendapatkan pengalaman-pengalaman di dunia professional. Aku sadar aku masih n000b dan masih perlu banyak belajar lagi.



Profil

1. Nama (real name) : Muhammad Khabiburrohman
2. Panggilan sehari hari : Zet,Rohman,Habiburrohman
3. Handle/nick : zetcOde
4. Alamat : Yogyakarta
5. Handle origin : zet
6. Mobile :
 - Telegram : @zetcOde
 - Urls : <https://zetalab.pw>
7. Sosial Media :
 - Facebook : zetcOde
 - Instagram : @zetcode
 - Twitter : @zetcOde
8. Computers spec :
 - pertama : Lenovo Ideapad 100-14IBD
 - Sekarang : Macbook Pro Retina
 - Yang diidamkan : Macbook Pro
9. Member of Community : NgeSEC
10. What I like to do? : Belajar, Research, Bug Hunting
11. What I dislike : Nggak suka nganggur
12. Favorite / Kesukaan :
 - Makanan/Foods : Seafood
 - Minuman/Drinks : Es The
 - Warna/Colours : Black
 - Place : Yogyakarta
 - Hobby : Olah raga, Ngenet
 - OS (kenapa?) : Linux (Fleksibel,customable,secure), Mac (Easy to use,secure,like a pro wkwkwk)
 - Software (kenapa?) :
 - Bahasa programing : Python,Bash
 - Words/Quote : "Dari n00b semua bermula, try harder!"