CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 2, No. 1, Mei 2019, hlm. 8-15

ETHICAL HACKING

Galih Aryo Utomo

Mahasiswa Magister Teknik Informatika Forensika Digital UII
Email: galih.a.utomo@gmail.com

Abstrak

Ethical Hacking dilakukan oleh perusahaan sebagai antisipasi celah keamanan system. Ethical hacking dilakukan oleh seorang yang memiliki kemampuan layaknya hacker yang mampu menyerang suatu system namun memiliki motivasi untuk membantu perusahaan menemukan celah keamanan yang akan digunakan perusahaan untuk mengevaluasi system mereka. Paper ini menjelaskan pentingnya informasi dan mengapa harus dijaga serta bagaimana seorang ethical hacker melakukan pekerjaanya.

Kata kunci: *ethical, hacking, hacker, informasi, keamanan, sistem*

ETHICAL HACKING

Abstract

Ethical Hacking is done by companies in anticipation of system security loopholes. Ethical hacking is done by someone who has the ability like a hacker who is able to attack a system but has the motivation to help companies find security gaps that companies will use to evaluate their systems. This paper explains the importance of information and why it must be maintained and how an ethical hacker does his work.

Keywords: *ethical, hacking, hacker, information, security, system*

1. PENDAHULUAN

Berkembangnya komputer dan sistem informasi yang pesat memanjakan penggunanya dalam kecepatan akses informasi dan pertukaran data. Banyak aplikasi dan sistem informasi manajemen dibuat untuk keperluan pribadi hingga profesional seperti sekolah, perusahaaan, rumah sakit dan banyak lagi. Banyak lembaga sudah menerapkan sistem informasi manajemen untuk menunjang proses bisnis perusahaannya. Namun banyak pengembang sistem informasi melupakan faktor keamanan dan lebih berfokus kepada fungsional sistem informasi sehingga tambal sulam sistem, kehilangan data dan ancaman dari pencuri dan perusak data semakin tak terelakan.

Mudahnya melakukan hacking juga disebabkan oleh semakin mudahnya mendapatkan *tools* dan pelatihan gratis di internet. *Tools* yang lebih modernpun membuat pelaku *hacking* (*hacker)* dapat dilakukan oleh orang yang baru belajar sekalipun. Sehingga kualitas *hacker* sebenarnya semakin menurun namun dampak ancaman yang ditimbulkannya semakin besar.

Dalam laporan tahunan Cybersecurity (Cisco 2018 Annual Cybersecurity Report) menyebutkan bahwa tempat kerja yang modern menciptakan kondisi yang mendukung *hacking*. Mobilitas karyawan dan adopsi IoT *(Internet of Things)* memberi peluang baru bagi *hacker*.

Kemudahan seseorang melakukan hacking tidak diimbangi oleh etika dan pemahaman yang baik sehingga mengakibatkan angka *cybercrime* semakin meningkat. Etika hacking yang baik akan membantu pengembang sistem untuk menemukan celah atau ancaman sistem dan menguatkan kualitas sistem informasi

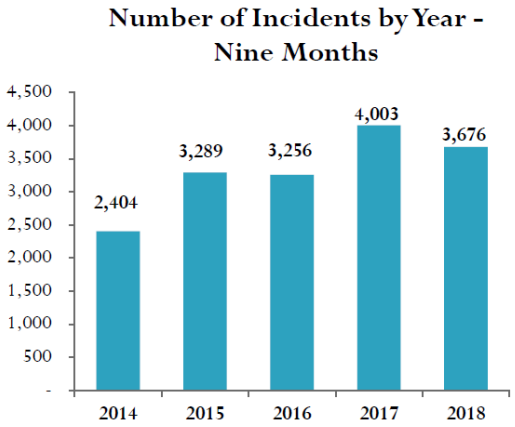
Ethical Hacking ditujukan sebagai aktivitas peretasan dengan metode serangan/ penetrasi untuk mengetahui tingkat keamanan sistem komputer dan cara penanggulangan terhadap kelemahannya.

2. STATISTIK KEAMANAN INFORMASI

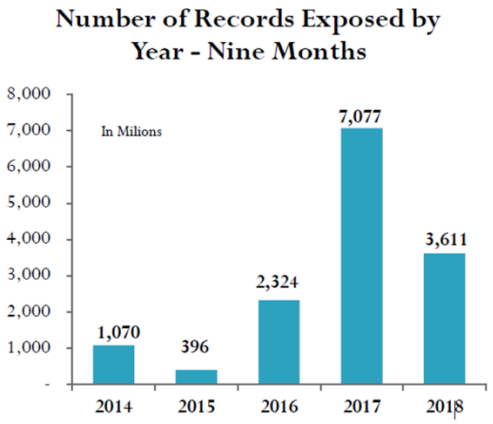
Berdasarkan situs breachlevelindex.com terkait kebocoran atau kehilangan data sejak tahun 2013 hingga paper ini dibuat pada Januari 2019 menunjukkan angka yang fantastic yaitu 13.443.149.623 data yang bocor atau hilang dimana 4% dari data tersebut adalah data yang terenkripsi.

Gambar 1. Data Breach Statistic breachlevelindex.com

Data Loss Statistics dari website *www.cyberriskanalytics.com* Ada 3676 insiden yang dilaporkan selama 2018 memperlihatkan 3611 juta records.

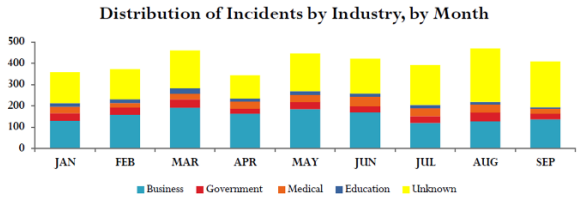


Gambar 2. Graphic Incidents www.cyberriskanalytics.com



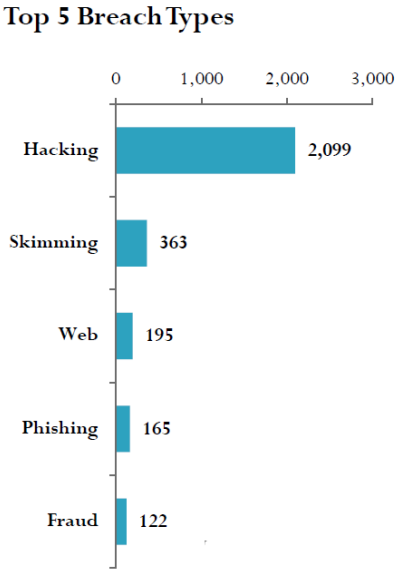
Gambar 3. Graphic Records Exposed
www.cyberriskanalytics.com

Masih dari sumber yang sama menunjukkan distribusi insiden pencurian data di beberapa industry terbanyak diduduki oleh Business sebagaimana ditunjukkan pada gambar dibawah ini.



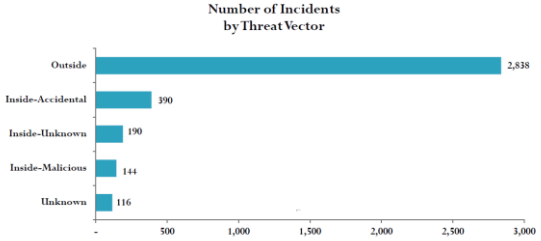
Gambar 4. Graphic Distribution of Incidents by Industry
www.cyberriskanalytics.com

Sedangkan Breach Types (tipe pelanggaran) yang dilakukan untuk melakukan pencurian data terbanyak adalah dengan hacking yaitu 2.099 kasus sebagaimana ditunjukkan dalam grafik dibawah ini.



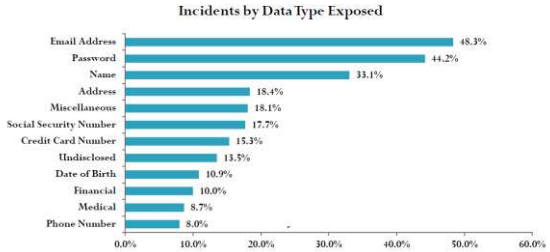
Gambar 5. Graphic Top 5 Breach Types
www.cyberriskanalytics.com

Data vector ancaman menunjukkan bahwa ancaman dari luar mencapai angka 2.838 kasus. Angka tertinggi dibanding yang lain. Terbesar kedua adalah ancaman dari dalam secara sengaja angkanya mencapai 390 kasus. Selengkapnya dapat dilihat pada gambar dibawah.



Gambar 6. Graphic Number of Incidents by Threat Vector
www.cyberriskanalytics.com

Data Type Exposed (tipe data yang terkena) yang terbanyak adalah alamat email dan password sebagaimana disajikan dalam gambar dibawah ini.



Gambar 7. Graphic Incidents by Data Type Exposed
www.cyberriskanalytics.com

3. PENTINGNYA KEAMANAN INFORMASI

Informasi menjadi asset penting dalam sebuah perusahaan. Dengannya mampu memberikan support untuk mengatur strategi dalam menjaga kestablian perusahana dan menunjang pengambilan keputusan. Olehnya selayaknya informasi harus dijaga dari pihak-pihak yang tidak berkepentingan. Menurut G. J. Simons, keamanan informasi adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik. Keamanan informasi adalah proses melindungi/ menjaga informasi serta sistem informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran yang tidak sah. Sedangkan tujuan pengelolaan keamanan informasi adalah untuk memastikan kelangsungan bisnis dan meminimalkan dampak insiden keamanan.

Prinsip keamanan informasi merupakan perlindungan terhadap aspek-aspek berikut:

a. *Confidentiality* (kerahasiaan) yaitu aspek yang menjamin kerahasiaan data atau informasi, dan memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima, dan disimpan.
b. *Integrity* (integritas) yaitu aspek yang menjamin bahwa data tidak dilakukan perbuahan tanpa ijin dari pihak yang berwenang (*authorized*), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.
c. *Availability* (ketersediaan) yakni aspek yang menjamin bahwa data tersedia ketika dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait.

Aspek ancaman terhadap keamanan informasi diantaranya adalah:

a. *Interruption* yaitu data dan informasi dalam sistem komputer dirusak dan dihapus data atau informasi tersebut tidak dapat diakses saat dibutuhkan.
b. *Interception* yaitu Informasi disadap oleh orang yang tidak berhak.
c. *Modifikasi* yaitu aktivitas menyadap lalu lintas informasi yang sedang dikirim dan mengubah data atau informasi yang melintas tersebut tanpa ijin.
d. *Fabrication* yaitu orang yang meniru pemberi informasi, sehingga pihak yang menerima menyangka informasi tersebut berasal dari orang yang benar/ dikehendaki oleh si penerima informasi.

4. HACKING

Hacking adalah teknik yang dilakukan oleh seseorang (hacker, cracker, penyusup, atau penyerang) untuk menyerang suatu sistem, jaringan, dan aplikasi dengan cara mengkesploitasi kelemahan dengan maksud untuk mendapatkan hak akses atas data dan sistem.

Beberapa motivasi seseorang melakukan *hacking* diantaranya adalah karena kesenangan, keuntungan dengan cara memeras korban, bisnis seperti dengan menguji keamanan sistem, bisa juga karena ingin mendapatkan pengakuan/ pamer. Sangat banyak motivasi atau tujuan dari aktivitas hacking, dan bisa dikatakan ada niat positif dan negatif. Meskipun memiliki tujuan yang berbeda, intinya adalah untuk menemukan kelemahan dalam sistem dan memanfaatkannya. Seorang yang melakukan tindakan *hacking* mereka disebut *hacker*.

Hacker dapat diklasifikasikan dalam kategori yang berbeda, secara umum terdapat tiga kategori yakni :

a. *Black Hat Hacker*
   Tipikal *hacker* yang berbahaya dan jahat, biasanya dimotivas oleh uang, balas dendam, kriminal, dll. Mereka mendapatkan akses tidak sah kedalam sistem, merusaknya dan atau mencuri informasi yang sensitif.
b. *White Hat Hacker*
   Dikenal sebagai *Ethical Hacker*. Mereka tidak pernah bermaksud untuk merusak suatu sistem, namun mereka mencoba untuk mengetahui kelemahan dalam komputer atau sistem jaringan sebagai bagian dari *penetration* testing dan/atau *vulnerability assessments*.
c. *Grey Hat Hacker*
   Perpaduan dari *Black Hat* dan *White Hat Hacker*. Tidak diketahui dengan jelas batasan baik atau jahat, terkadang melakukan penyerangan dengan memanfaatkan kelemahan sistem yang dilakukan untuk kesenangan. Namun terkadang menjadi konsultan keamanan, bisa saja dikarenakan butuh uang, atau tergantung permintaan.

Selain dari klasifikasi Hacker diatas, masih banyak lagi jenis hacker yang diklasifikasikan berdasarkan tujuan meretas sistem, seperti :

a. *Script Kiddies*

Hacker pemula yang memiliki sedikit pengetahuan dan menggunakan tools buatan orang lain, biasanya tidak dapat mengembangkan serangan dan pertahanan.

b. *Red Hat Hackers*
Agen pemerintah, sebagai hub top-secret information, dan segala sesuatu yang berhubungan dengan informasi sensitif.
c. *Blue Hat Hackers*
Konsultan keamanan komputer yang terbiasa melakukan bug-test sistem sebelum diluncurkan. Mereka mencari celah yang bisa dimanfaatkan dan mencoba menutup celah ini.
d. *Elite* Hackers
Status sosial dikalangan *hacker*, yang digunakan untuk menggambarkan yang memiliki skill paling hebat. Eksploitasi yang baru ditemukan ataupun *ZeroDay Vulnerability* akan beredar di antara para hacker ini.
e. *Cyber Terrorist*
Tipikal hacker jahat, biasanya secara organisasi/group, mereka menyebarkan ancaman-ancaman untuk tujuan tertentu (agama, politik, nasionalis, atau aktivis)
f. *State-sponsored Hackers*
Hacker terlatih yang dibiayai oleh negara atau pemerintah biasanya bertujuan untuk mata-mata dan perang *cyber* (*cyberwarfare*). Mereka adalah hacker yang memiliki kemampuan tinggi dan banyak uang karena disponsori oleh negara.
g. *Hacktivist*
Salah satu *black hat*, mereka menyerang sambil menyebarkan suatu pesan khusus. Melalui *deface* website, serangan DoS, dll.
h. *Corporate Hackers*
Tipikal *hacker* yang menyerang properti intelektual dan data penting suatu perusahaan. Tujuan mereka adalah untuk mendapatkan informasi mengenai kompetitor suatu perusahaan.

5. ETHICAL HACKING

Ethical Hacking merupakan suatu aktifitas melakukan penetrasi ke suatu sistem, jaringan, dan aplikasi dengan cara mengkesploitasi kelemahan dengan maksud untuk mendapatkan hak akses atas data dan sistem, yang bertujuan untuk membantu perusahaan menguji keamanan system dan jaringan mereka karena kemungkinan celah dan kerentanan. Orangnya yang melakukan *ethical hacking* disebut sebagai *Ethical Hacker*.

Pada dasarnya, teknik yang digunakan oleh *Ethical Hacker* sama dengan teknik yang digunakan oleh *Hacker*, namun yang berbeda adalah pada tujuan melakukan aktivitas *hacking*.

Selain memiliki kemampuan teknis, seorang *Ethical Hacker* juga harus memiliki kemampuan non teknis seperti:

a. Memiliki kemampuan untuk belajar dan beradaptasi dengan cepat terhadap teknologi baru,
b. Memiliki kemampuan bekerja dengan etika tinggi, memiliki kemampuan dalam menyelesaikan masalah dan kemampuan mengkomunikasikannya dengna pihak client dalam hal ini organisasi/perusahaan,
c. Memiliki komitmen yang kuat terhadap kebijakan keamanan dari sebuah organisasi (client),
d. Peduli dengan standar dan aturan yang ada dalam organisasi.

Jasa dari Ethical Hacker sangat diperlukan perusahaan yang ingin melakukan pengamanan system. Alasan lainnya seorang Ethical Hacker juga dapat melakukan pengungkapan *vulnerability* yang ada pada sistem, dan dapat mengeksploitasi lebih dalam sehingga menemukan risiko apa saja yang ditimbulkan dari vulnerability yang ditemukan.

Seorang Ethical Hacker dalam mengevaluasi sistem yang dimiliki oleh perusahaan, harus mampu mencari jawaban dari tiga pertanyaan dasar yakni:

a. Apa yang dilihat oleh penyerang terhadap sebuah target sistem?
Seorang *Ethical Hacker* harus mampu memikirkan tentang apa yang dilihat oleh seorang penyerang selama penyerang itu melakukan *fase reconnaissance* atau *fase scanning*.
b. Apa yang akan dilakukan oleh seorang penyerang dengan informasi dari fase tersebut?
Seorang *Ethical Hacker* harus memiliki kemampuan satu langkah di depan dari seorang penyerang dalam memanfaatkan informasi yang diperoleh dari fase sebelumnya sampai dengan fase mendapatkan akses dan melakukan meintenance akses pada sistem target.
c. Apakah upaya penyerang diperhatikan pada sistem target?
Terkadang penyerang akan mencoba melakukan penyerangan selama berhari-hari, atau berminggu-minggu, atau bahkan berbulan-bulan. Selama periode tersebut, seorang *Ethical Hacker* harus mampu mendeteksi dan menghentikan adanya serangan tersebut.

Jenis-jenis test/percobaan yang biasa dilakukan oleh seorang *Ethical Hacker* terhadap sebuah sistem diantaranya adalah:

a. *Vulnerability Testing*
Melakukan scan terhadap sistem (manual atau dengan tools), dengan tujuan untuk mengetahui apakah sistem tersebut memiliki kelemahan, apa solusi untuk menambal kelemahannya, apa konfigurasi sistem yang mereka pakai, kemudian dihasilkan sebuah laporan keamanan. Dalam testing ini tidak dilakukan tindakan eksploitasi atau penetrasi ke dalam sistem, namun hanya

melaporkan temuan/hasil scan yang telah dilakukan.

b. Full Penetration Testing.
Pada testing ini akan dilakukan ujicobad. penyerangan dari berbagai vektor, seperti penyerangan aplikasi web, *sql injection, firewall, wireless network, OS.*

c. Targeted Testing.
Prosesnya sama seperti *full penetration testing*, hanya saja penyerangan difokuskan ke satu vektor serangan saja.

Adapun jenis-jenis test/percobaan berdasarkan informasi dan lokasi seorang *Ethical Hacker* dalam melakukan pengujian dapat dikategorikan sebagai berikut:

a. *Black Box*
Seorang *Ethical Hacker* tidak memiliki informasi mengenai infrastruktur atau jaringan sebuah organisasi yang sedang dilakukan test. Dalam pengujian penetrasi ini, *Ethical Hacker* mencoba mencari informasinya sendiri.

b. Grey Box
Seorang *Ethical Hacker* hanya memiliki sedikit informasi (*partial information*) mengenai infrastruktur atau jaringan sebuah organisasi yang sedang dilakukan test

c. White Box
Seorang *Ethical Hacker* memiliki informasi (walaupun itu informasi rahasia) mengenai infrastruktur atau jaringan sebuah organisasi yang sedang dilakukan test.

d. External Penetration Testing
Seorang *Ethical Hacker* mencoba menyerang menggunakan jaringan publik melalui internet

e. Internal Penetration Testing
Seorang *Ethical Hacker* berada di dalam jaringan organisasi dan melakukan uji penetrasi dari dalam.

Selain berdampak positif, pengujian penetrasi yang dilakukan oleh seorang *Ethical Hacke*r juga dapat menyebabkan masalah seperti kerusakan sistem, sistem crash, atau kehilangan data. Oleh karena itu, perusahaan harus mengambil risiko yang diperhitungkan sebelum melanjutkan pengujian penetrasi. Ada beberapa batasan yang perlu diketahui dalam melakukan uji penetrasi. *Ethical Hacker* harus mengikuti aturan dalam rangka memenuhi kewajiban moral dan etika dalam menjalankan profesinya. Adapun hal-hal yang perlu diperhatikan seperti:

a. Mendapatkan otorisasi dan izin dari organisasi dalam bentuk kontrak tertulis.

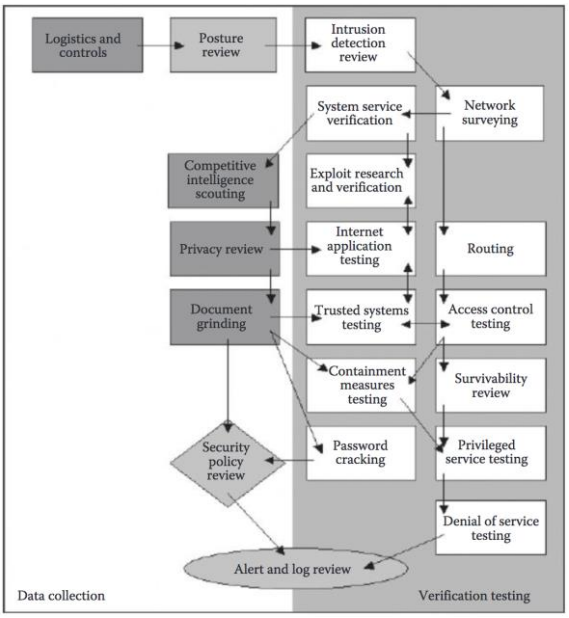
b. Ethical Hacker harus mengikuti aturan seperti *Non Disclosure Agreement (NDA*) karena dalam melakukan uji penetrasi, seorang *Ethical Hacker* bisa saja mendapatkan atau mengungkapkan informasi yang bersifat rahasia dan *sensitive*.

c. Harus tetap mempertahankan kerahasiaan saat melakukan uji penetrasi. Informasi yang bersifat *confidential* tidak boleh disebarkan ke pihak lain.

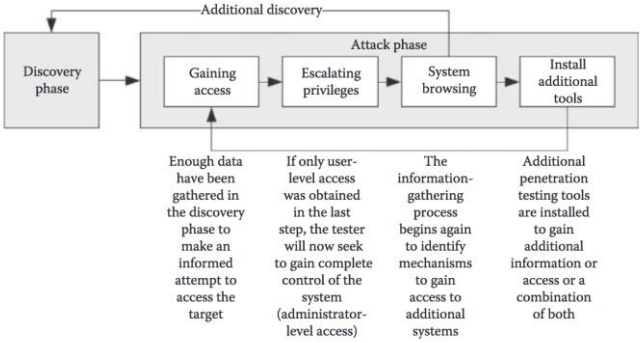
Uji penetrasi tidak boleh melampaui batas yang telah disepakati. Misalnya ketika seorang *Ethical Hacker* akan melakukan tindakan *Denial of Services (DoS),* harus melihat kondisi dari sebuah organisasi. Jangan sampai ketika melakukan uji penetrasi hanya dapat mengakibatkan kerugian pada organisasi tersebut dengan tidak dapat berjalannya system yang diakibatkan oleh tindakan DoS.

6. METODE HACKING

Ethi*cal Hacking* memiliki metode dalam melakukan aktivitasnya. Hal ini membantu proses pengujian sistem menjadi terstruktur. Banyak standar yang bisa diikuti dalam melakukan proses pengujian sistem. Seperti yang dikeluarkan oleh *Open Source Security Testing Methodology Manual (OSSTMM) dan National Institute of Standards and Technology (NIST)* seperti pada gambar berikut.



Gambar 8. Metode Hacking OSSTMM



Gambar 9. Metode Hacking NIST

Proses atau metode hacking secara sederhana dapat dilakukan dalam enam fase seperti pada gambar berikut:

Gambar 10. Metode Hacking

Reconnaissance

Reconnaissance adalah fase dimana penyerang mengumpulkan informasi tentang target dengan cara aktif atau pasif. Tools yang sering digunakan digunakan dalam proses ini seperti NMAP, Hping, Maltego, dan Google Dorks.

Selama melakukan proses reconnaissance, seorang *Ethical Hacker* mencoba mengumpulkan informasi sebanyak mungkin dengan mengikuti 7 hal berikut:

- Mengumpulkan informasi awal
- Menentukan range atau rentang dari jaringan komputer
- Mengidentifikasi mesin atau server yang aktif
- Menemukan port dan titik akses yang terbuka
- Menemukan informasi mengenai sistem operasi server
- Mengungkap service apa saja yang berjalan
- Memetakan jaringan komputer.

Proses *recconnaissance* dapat dilakukan secara aktif yakni sebuah kondisi dimana *Ethical Hacker* akan langsung berinteraksi dengan sistem komputer untuk mendapatkan informasi, sedangkan cara pasif yakni dimana kondisi seorang *Ethical Hacker* tidak berinteraksi secara langsung dengan sistem target.

Scanning

Dalam proses ini, *Ethical Hacker* mulai secara aktif menyelidiki mesin target atau jaringan kerentanan yang bisa dimanfaatkan. Tools yang digunakan dalam proses ini adalah Nessus, Nexpose, dan NMAP.

Gaining Access

Dalam proses ini, ketika kerentanan ditemukan, maka *Ethical Hacker* akan memanfaatkan kerentanan tersebut untuk mendapatkan akses ke sistem target. Tools yang populer digunakan dalam proses ini seperti Metasploit.

Maintaining Access

Ini adalah proses dimana *Ethical Hacker* telah mendapatkan akses ke sistem. Setelah mendapatkan akses, *Ethical Hacker* akan menginstal beberapa *backdoor* yang bisa digunakan kedepannya untuk melakukan akses ke sistem.

Clearing Tracks

Proses ini sebenarnya adalah kegiatan yang tidak etis. Ini berkaitan dengan penghapusan log dari semua aktivitas yang terjadi selama proses *hacking* sebelumnya.

Reporting.

Pelaporan merupakan langkah terakhir dalam menyelesaikan proses *hacking* etis. Disini *Ethical Hacker* menyusun sebuah laporan dengan temuannya dan penggunaan alat yang digunakan, tingkat keberhasilan, kerentanan yang ditemukan, dan proses eksploitasi.

7. REPORTING (PELAPORAN)

Sebuah laporan yang baik harus memperhatikan hal sebagai berikut:

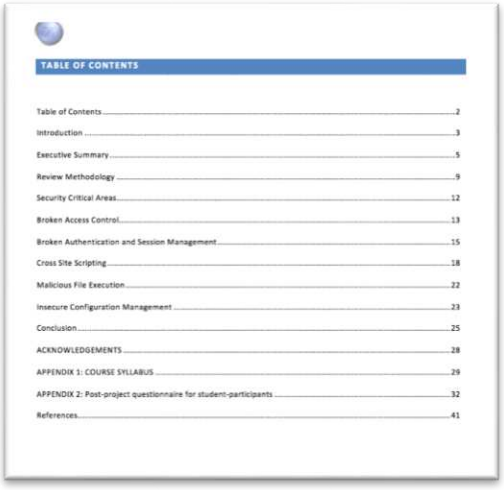
- Laporan harus sederhana, jelas, dan mudah dimengerti.
- Presentasi laporan juga penting.
- Laporan harus terstruktur dengan baik.
- Selalu pastikan menggunakan gaya penulisan yang konsisten dalam penulisan laporan.
- Pastikan untuk meminimalisir hasil temuan yang bersifat false-positive.
- Laporan merupakan hasil analisis terperinci tentang kerentanan, hal ini untuk mengetahui
- akar penyebabnya.

Beberapa contoh laporan :

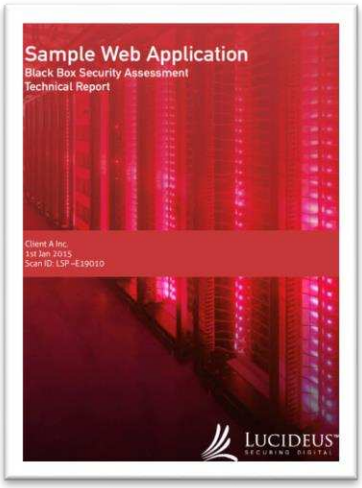
Gambar 11. Contoh Laporan

Gambar 12. Contoh Laporan

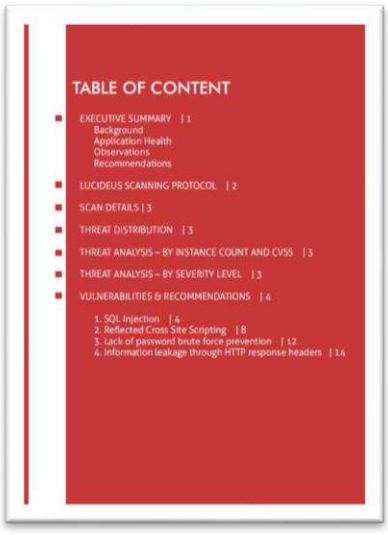
Gambar 13. Contoh Laporan



Gambar 14. Contoh Laporan



Gambar 15. Contoh Laporan



Gambar 16. Contoh Laporan

Gambar 17. Contoh Laporan

8. CONTOH KASUS KERAWANAN SISTEM

Dalam laporan www.cyberriskanalytics.com salah satu industry yang terkena dampak pencurian data atau informasi adalah industri kesehatan. Pencurian yang dilakukan bisa jadi dilakukan oleh pihak eksternal dengan memanfaatkan kelemahan-kelamahan system dan dari pihak internal yaitu pengguna system secara tidak sengaja maupun sengaja membocorkan informasi penting akses ke sistem.

Penyerangan kepada sistem informasi rumah sakit oleh pihak eksternal harus diwaspadai oleh pihak rumah sakit yang menggunakan system gratis dan mudah untuk diperoleh sebagai contoh SIM RS Khansa yang dikembangkan oleh komunitas SIM RS dan SIM RS GOS yang dikembangkan oleh Kemkes. Secanggih apapun system yang dibuat namun jika dapat diperoleh dengan gratis dan bebas bisa jadi dapat dimanfaatkan oleh pihak yang tidak bertanggungjawab untuk menganalisa celah keamanannya. Kecerobohan yang dilakukan oleh pihak internal rumah sakit dalam berbagi data dengan komunitas juga merupakah celah keamanan system yang harus segera disadari.

Hal yang harus diperhatikan pula jika menggunakan SIM RS gratis sebaiknya segera mengganti system keamanan standar berupa koneksi database dan password administrator serta sebaiknya pihak internal rumah sakit mengganti system enkription datanya.

Bagi RS yang mengembangkan system dengan pihak ke 3 atau vendor baiknya juga melakukan MOU kerahasiaan data dan informasi. Sebagai contoh kasus penggunaan Cons ID BPJS yang seharusnya menjadi rahasia suatu rumah sakit digunakan oleh vendor untuk uji coba system di rumah sakit lainnya kerap kali terjadi.

Dapat disimpulkan bocornya data dan informasi di Rumah Sakit sering terjadi karena kecerobohan user dan ketidakpedulian vendor dalam kerahasiaan data.

Penyalahgunaan aksespun kerap terjadi di lingkungan rumah sakit. Malasnya user seperti dokter spesialis mengingat/ mengganti password melakukan login atau logout membuat password yang semestinya dijaga sebagai privasi malah disebarluaskan ke pihak lain/ perawat. Hal ini jelas membuat data tidak lagi memiliki integritas.

DAFTAR PUSTAKA

Data Breach StatisticsData Records Lost or Stolen Since 2013, breachlevelindex.com, diakses pada tanggal 16 Januari 2019

Ethical Hacking, tutorialspoint.com, diakses pada tanggal 16 Januari 2019

Gurpreet K. Juneja,"Ethical hanking :A technique to enhance information security" international

journal of computer applications (3297: 2007), vol. 2, Issue 12, December 2013

Laporan Tahunan Cybersecurity Cisco 2018, https://www.cisco.com/c/en/us/products/security/security-reports.html?CCID=cc000160&DTID=esootr000875&OID=anrsc005983#~download-the-report, diakses pada tanggal 16 Januari 2019

Technical Guide toInformation Security Testingand Assessment, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf, diakses pada tanggal 5 Desember 2018

The Open Source Security Testing Methodology Manual, Contemporary Security Testing and Analysis, http://www.isecom.org/mirror/OSSTMM.3.pdf, diakses pada tanggal 16 Januari 2019