Analisa Keamanan Situs Terhadap Serangan SQL Injection Di Universitas Kristen Maranatha

Marvin Chandra Wijaya

Program Studi Sistem Komputer, Fakultas Teknik, Universitas Kristen Maranatha
marvinchw@gmail.com

Abstrak

Sebuah situs resmi (*official website*) bukan hanya sebagai tempat promosi suatu institusi, tetapi situs resmi merupakan sebuah identitas dari instutusi tersebut. Situs resmi merupakan jati diri atau merupakan cermin dari citra institusi tersebut. Dalam situs tersebut akan berisi identitas diri dari instiutusi tersebut, profil, kegiatan-kegiatan, berita, dan masih banyak lagi.

Oleh karena itu sebuah situs resmi harus dijaga sedemikian rupa terhadap serangan-serangan di dalam dunia maya. Situs resmi tersebut dapat ditempat dan dikelola oleh pihak ketiga. Yaitu pihak yang menyediakan jasa *hosting website*. Selain itu juga sebuah institusi dapat mengelola sendiri situs resmi tersebut. Dengan pengelolaan sendiri maka akan banyak sekali kebebasan dan fasilitas yang dapat diberikan dalam sistem tersebut. Namun dengan pengelolaan sendiri, maka tantangan untuk menjaga situs dan sistem informasi yang dibuat menjadi hal sangat krusial.

Universitas Kristen Maranatha sudah sejak lama mempunyai sistem informasi yang dikelola oleh Departement Informasi Maranatha dalam pengelolaan trafik data keluar dan masuk melalui saluran internet.

Kata Kunci: Keamanan Informasi, Situs, SQL Injection

1. Pendahuluan

Situs resmi merupakan sebuah identitas dari sebuah instutusi yang merupakan jati diri atau merupakan cermin dari citra institusi tersebut. Situs resmi berisi :

- Identitas diri dari instiutusi tersebut,
- Profil institusi,
- Kegiatan-kegiatan,
- Berita internal
- Berita eksternal
- dan lain-lain

Oleh karena itu sebuah situs resmi harus dijaga sedemikian rupa terhadap serangan-serangan di dalam dunia maya.

Ada dua cara pengelolaan suatu situs :

- Situs resmi tersebut dapat ditempat dan dikelola oleh pihak ketiga. Yaitu pihak yang menyediakan jasa hosting website.
- Selain itu juga sebuah institusi dapat mengelola sendiri situs resmi tersebut. Dengan pengelolaan sendiri maka akan banyak sekali kebebasan dan fasilitas yang dapat diberikan dalam sistem tersebut. Namun dengan pengelolaan sendiri, maka tantangan untuk menjaga situs dan sistem informasi yang dibuat menjadi hal sangat krusial.

Universitas Kristen Maranatha sudah sejak lama mempunyai sistem informasi yang dikelola oleh Departement Informasi Maranatha dalam pengelolaan trafik data keluar dan masuk melalui saluran internet.

Universitas Kristen Maranatha mempunyai beberapa situ resmi yaitu :

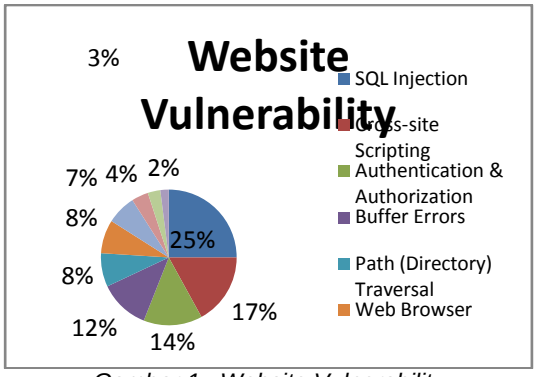
- sebuah situs beralamatkan www.maranatha.edu yang dapat diakses dari internal dan eksternal.
- Serta memiliki situs noc.maranatha.edu yang hanya dapat diakses secara internal dari jaringan kampus.
- Selain itu juga terdapat sat.maranatha.edu yang berfungsi sebagai situs pengelolaan akademik dari Universitas Kristen Maranatha.

2. Metode

Keamanan website merupakan topik yang menarik. Masalah dengan keamanan Web merupakan suatu masalah yang sangat kompleks. Sebagai contoh adanya pengiriman pesan spam tanpa disadari. Email dan password telah yang dibajak dan dijual kembali kepada orang-orang untuk memesan suatu barang secara online.

Analisis dari banyaknya penyerangan pada Webiste di kelompokkan pada beberapa kelas yaitu :

- Command Injection
- Expression Language Injection
- Default Login
- Local File Include
- Remote Code Injection
- Remote File Include
- SQL Injection
- Vanilla SQL Injection
- Weak Session Management
- Cross-site Scripting
- LDAP Injection
- Persistent Cross-site Scripting
- Reflected Cross-site Scripting
- XML Injection
- XPATH Injection
- Cross-site Request Forgery
- Open Cross Domain Policy
- CRLF Injection
- Directory Traversal
- Frame Injection
- Inadequate Session Revocation
- .NET Tracing Capabilities
- Open Redirect
- Response Splitting
- Admin Page Discovered
- Session Cookie not Flagged as HTTPOnly
- Session Cookie not Flagged as Secure
- Session Fixation
- Autocomplete Enabled
- Directory Listing Enabled
- Discovered SOAP Service
- Path Disclosure
- Source Leakage
- Additional Applications
- Common Files
- Dangerous Methods Enabled
- Debug Methods Enabled
- Directory Listing Denied
- File Upload
- Microsoft Office Document
- Open Cross-Origin Resource Sharing
- Password Via GET
- Permissive Cross-Origin Resource Sharing
- Redirect Response With Body
- Referer Leakage
- Strict Transport Security
- Version Control Files
- ViewState Not Encrypted
- ViewState not Signed
- X-Frame-Options Not Used
- Permissive X-Frame Options Used
- XSS Protection Disabled
- XSS Protection Error
- CVE Finding
- OSVDB Finding
- Virtual Host Discovery



Gambar 1. Website Vulnerability
Sumber : www.smashingmagazine.com

Dari hasil penelitian pada gambar 1. terlihat bahwa penyerangan bersifat SQL Injection merupakan penyerangan yang paling banyak dilakukan dibandingkan dengan penyerangan-penyerangan tipe lainnya.

SQL Injection

SQL injection adalah serangan yang memanfaatkan kelalaian dari website yang mengijinkan user untuk menginputkan data tertentu tanpa melakukan filter terhadap malicious character. Inputan tersebut biasanya di masukan pada box search atau bagian-bagian tertentu dari website yang berinteraksi dengan database SQL dari situs tersebut. Perintah yang dimasukan para attacker biasanya adalah sebuah data yang mengandung link tertentu yang mengarahkan para korban ke website khusus yang digunakan para attacker untuk mengambil data pribadi korban.

Untuk menghindari link berbahaya dari website yang telah terinfeksi serangan SQL injection, dapat menggunakan aplikasi tambahan seperti NoScript yang merupakan Add-ons untuk aplikasi web browser Firefox.

Dengan SQL Injection, seorang penyerang dapat mengakses database dengan mengirimkan perintah ke server melalui URI atau form fields. Sebagai contoh kerawanan pada pengaksesan username:

```
statement = "SELECT * FROM
users WHERE name = '" +
userName + "';"
```

Kode SQL didesain untuk menarik record dengan username tertentu dari tabel user, tetapi variable “UserName” dapat digunakan oleh pengguna yang tidak bertanggungjawab. Pemecahannya dengan melakukan setting variable “userName” sebagai :

```
' or '1'='1
```

Lalu lakukan pengubahan SQL command dengan:

```
SELECT * FROM users WHERE
name = '' OR '1'='1';
```

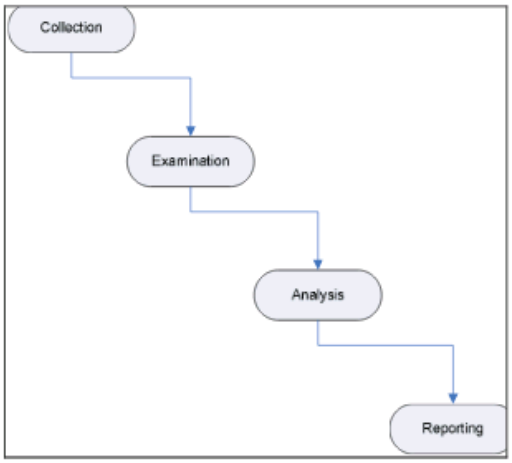
Tabel 1 merupakan daftar dari kumpulan SQL Injection yang dapat digunakan untuk penyerangan-penyerangan.

Tabel 1. Kumpulan SQL Injection

inurl:index.php?id=	inurl:productinfo.php?id=
inurl:trainers.php?id=	inurl:showimg.php?id=
inurl:buy.php?category=	inurl:view.php?id=
inurl:article.php?ID=	inurl:website.php?id=
inurl:play_old.php?id=	inurl:hosting_info.php?id=
inurl:declaration_more.php?decl_id=	inurl:gallery.php?id=
inurl:Pageid=	inurl:rub.php?idr=
inurl:games.php?id=	inurl:view_faq.php?id=
inurl:page.php?file=	inurl:artikelinfo.php?id=
inurl:newsDetail.php?id=	inurl:detail.php?ID=
inurl:gallery.php?id=	inurl:index.php?=
inurl:article.php?id=	inurl:profile_view.php?id=
inurl:show.php?id=	inurl:category.php?id=
inurl:staff_id=	inurl:publications.php?id=
inurl:newsitem.php?num=	inurl:fellows.php?id=
inurl:readnews.php?id=	inurl:downloads_info.php?id=
inurl:top10.php?cat=	inurl:prod_info.php?id=
inurl:historialeer.php?num=	inurl:shop.php?do=part&id=
inurl:reagir.php?num=	inurl:Productinfo.php?id=
inurl:forum_bds.php?num=	inurl:collectionitem.php?id=
inurl:game.php?id=	inurl:band_info.php?id=
inurl:view_product.php?id=	inurl:product.php?id=
inurl:newsone.php?id=	inurl:releases.php?id=
inurl:sw_comment.php?id=	inurl:ray.php?id=
inurl:news.php?id=	inurl:produit.php?id=
inurl:avd_start.php?avd=	inurl:pop.php?id=
inurl:event.php?id=	inurl:shopping.php?id=
inurl:product-item.php?id=	inurl:productdetail.php?id=
inurl:sql.php?id=	inurl:post.php?id=
inurl:news_view.php?id=	inurl:viewshowdetail.php?id=
inurl:select_biblio.php?id=	inurl:clubpage.php?id=
inurl:humor.php?id=	inurl:memberInfo.php?id=
inurl:aboutbook.php?id=	inurl:section.php?id=
inurl:fiche_spectacle.php?id=	inurl:theme.php?id=
inurl:communique_detail.php?id=	inurl:page.php?id=
inurl:sem.php3?id=	inurl:shredder-categories.php?id=
inurl:kategorie.php4?id=	inurl:tradeCategory.php?id=
inurl:news.php?id=	inurl:product_ranges_view.php?ID=
inurl:index.php?id=	inurl:shop_category.php?id=
inurl:faq2.php?id=	inurl:transcript.php?id=
inurl:show_an.php?id=	inurl:channel_id=
inurl:preview.php?id=	inurl:item_id=
inurl:loadpsb.php?id=	inurl:newsid=
inurl:opinions.php?id=	inurl:trainers.php?id=
inurl:spr.php?id=	inurl:news-full.php?id=
inurl:pages.php?id=	inurl:news_display.php?getid=
inurl:announce.php?id=	inurl:index2.php?option=
inurl:clanek.php4?id=	inurl:readnews.php?id=
inurl:participant.php?id=	inurl:top10.php?cat=
inurl:download.php?id=	inurl:newsone.php?id=
inurl:main.php?id=	inurl:event.php?id=
inurl:review.php?id=	inurl:product-item.php?id=
inurl:chappies.php?id=	inurl:sql.php?id=
inurl:read.php?id=	inurl:aboutbook.php?id=
inurl:prod_detail.php?id=	inurl:review.php?id=
inurl:viewphoto.php?id=	inurl:loadpsb.php?id=
inurl:article.php?id=	inurl:ages.php?id=
inurl:person.php?id=	inurl:material.php?id=
inurl:productinfo.php?id=	inurl:clanek.php4?id=
inurl:showimg.php?id=	inurl:announce.php?id=
inurl:view.php?id=	inurl:chappies.php?id=
inurl:website.php?id=	inurl:read.php?id=
inurl:hosting_info.php?id=	inurl:viewapp.php?id=
inurl:gallery.php?id=	inurl:viewphoto.php?id=
inurl:rub.php?idr=	inurl:rub.php?idr=
inurl:view_faq.php?id=	inurl:galeri_info.php?l=
inurl:artikelinfo.php?id=	inurl:review.php?id=
inurl:detail.php?ID=	inurl:iniziativa.php?in=
inurl:index.php?=	inurl:shopping.php?id=
inurl:profile_view.php?id=	inurl:productdetail.php?id=
inurl:category.php?id=	inurl:post.php?id=
inurl:publications.php?id=	inurl:viewshowdetail.php?id=
inurl:fellows.php?id=	inurl:clubpage.php?id=
inurl:downloads_info.php?id=	inurl:memberInfo.php?id=
inurl:prod_info.php?id=	inurl:section.php?id=
inurl:shop.php?do=part&id=	inurl:theme.php?id=
inurl:Productinfo.php?id=	inurl:page.php?id=
inurl:collectionitem.php?id=	inurl:shredder-categories.php?id=
inurl:band_info.php?id=	inurl:tradeCategory.php?id=
inurl:product.php?id=	inurl:product_ranges_view.php?ID=
inurl:releases.php?id=	inurl:shop_category.php?id=
inurl:ray.php?id=	inurl:transcript.php?id=
inurl:produit.php?id=	inurl:channel_id=
inurl:pop.php?id=	inurl:item_id=
inurl:event.php?id=	inurl:newsid=
inurl:product-item.php?id=	inurl:trainers.php?id=
inurl:sql.php?id=	inurl:news-full.php?id=
inurl:aboutbook.php?id=	inurl:news_display.php?getid=
inurl:review.php?id=	inurl:index2.php?option=
inurl:loadpsb.php?id=	inurl:readnews.php?id=
inurl:ages.php?id=	inurl:top10.php?cat=
inurl:material.php?id=	inurl:newsone.php?id=
inurl:clanek.php4?id=	inurl:announce.php?id=
inurl:announce.php?id=	inurl:rub.php?idr=
inurl:chappies.php?id=	inurl:galeri_info.php?l=
inurl:read.php?id=	inurl:tekst.php?idt=
inurl:viewapp.php?id=	inurl:newscat.php?id=
inurl:viewphoto.php?id=	inurl:newsticker_info.php?idn=
inurl:rub.php?idr=	inurl:rubrika.php?idr=
inurl:galeri_info.php?l=	inurl:rubp.php?idr=
inurl:review.php?id=	inurl:offer.php?idf=
inurl:iniziativa.php?in=	inurl:art.php?idm=
inurl:curriculum.php?id=	inurl:title.php?id=
inurl:labels.php?id=	
inurl:story.php?id=	
inurl:look.php?ID=	
inurl:newsone.php?id=	
inurl:aboutbook.php?id=	
inurl:material.php?id=	
inurl:opinions.php?id=	

2.1 Metode Pengumpulan Data

Penelitian ini menggunakan metodologi yang digunakan pendekatan proses forensik untuk menganalisa teknis keamanan website dan studi pustaka sebagai referensi kajian. Selain itu juga menggunakan teori-teori dalam melakukan observasi terkait tema penelitian.



Gambar 2. Diagram Alir Penelitian
Sumber : Baryamureeba dan Tushabe, 2004

2.1.1.Collection

Pada tahap ini dilakukan identifikasi terhadap kebutuhan-kebutuhan, baik kebutuhan fungsional sistem maupun identifikasi kondisi jaringan websiteUniversitas Muria Kudus. Pada tahapan identifikasi ini tim peneliti
berhasil mengidentifikasi kebutuhan alat dan bahan,identifikasi veriabel yang diteliti, jangka waktu penelitian dan tempat penelitian.

- Satu buah komputer sebagai IDS Snort Server
- Tools IDS Snort
- Tools Wiresark

2.1.2. Examintaion

Pada tahap ini mulai dilakukan pengujian terhadap keamanan website Universitas Kristen Maranatha. Dilakukan SQL Injection terhadap website Universitas Kristen Maranatha. Serangan disini hanya dilakukan untuk melihat apakah penyerang dapat memasuki database website Universitas Kristen Maranatha.

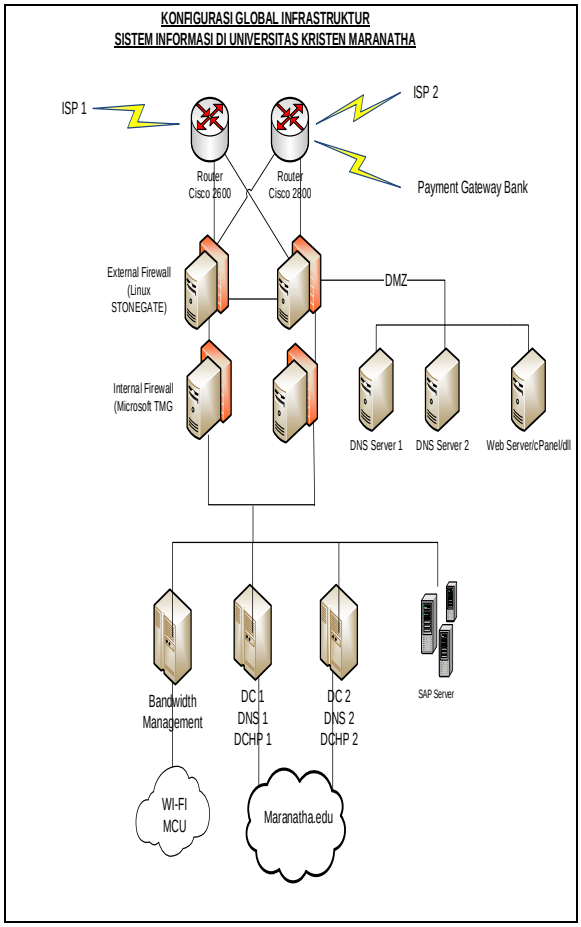
2.13. Analysis

Pada tahapan ini, dilakukan analisa terhadap hasil serangan SQL Injection, hal ini berguna untuk menemukan kelemahan-kelemahan pada website Universitas Kristen Maranatha. Berdasarkan hasil analisa, juga diharapkan dapat diperoleh solusi untuk pengembagan keamanan sistem.

2.1.4.Reporting

Pada tahap pelaporan, mulai dilakukan dokumentasi terhadap hasil penelitian beserta analisisnya.

3. Hasil dan Pembahasan



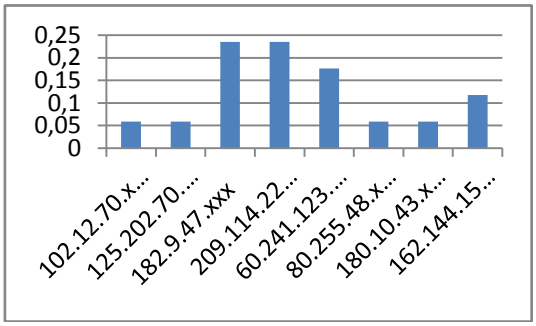
Gambar 3. Topologi Jaringan Kampus Universitas Kristen Maranatha
Sumber : Departement IT Maranatha

Gambar 3 adalah topologi awal jaringan kampus Univesitas Kristen Maranatha.

Untuk kebutuhan analisa, maka dilakukan penambahan server portal dengan IDS Snort untuk melihat dan mencatat setiap serangan yang ada. Intrusion Detection System (IDS) adalah sejenis perangkat lunak yang berfungsi untuk mendeteksi penyerangan sistem. Instrusi disini adalah menganalisa segala macam serangan yang mungkin terjadi dari luar sistem.

Prosentase IP Penyerang

Hal pertama yang dilakukan adalah dengan melihat prosentasi IP Penyerang dalam kondisi pengamatan selama 2 bulan.



Gambar 4. Prosentasi IP penyerang
Sumber : Pribadi

Parsing File Log Pcap

Implementasi dilakukan pada server forensik jaringan untuk membaca file log. Dilakukan analisis terhadap file log tersebut yang berguna melihat aliran header paket yang melewati jaringan

```
dataku@dataku:~$perl   parsingpcap.pl
|less

Time: 09-12 18:41:12.152693
IP Address Source: xxx.xxx.xxx.xxx
Mac Address Source: 03144f607983
Port Numbers: 45601
IP        Address        Destination:
xxx.xxx.xxx.xxx
Mac       Address        Destination:
003462758dda
Port Numbers: 80

Time: 09-11 20:17:32.123546
IP Address Source: xxx.xxx.xxx.xxx
Mac Address Source: 00134a40f475
Port Numbers: 123703
IP        Address        Destination:
xxx.xxx.xxx.xxx
Mac Address Destination: 0009dfd3343
Port Numbers: 80
```

Port Scanning

Program port scanning merupakan sebuah alat untuk mengetahui port mana saja yang terbuka maupun tertutup pada sebuah server atau host. Cara menjalankannya adalah dengan cara mengetikkan perl portscan.pl lalu ip address sebuah server atau host yang ingin di ketahui setelah itu nomot port yang diinginkan

```
root@dataku:/home/dataku#        perl
portscan.pl xxx.xxx.xxx.xxx 21-25

Hasilnya adalah...

Target xxx.xxx.xxx.xxx : Port 21 is
closed
Target xxx.xxx.xxx.xxx : Port 22 is
open
Target xxx.xxx.xxx.xxx : Port 23 is
closed
Target xxx.xxx.xxx.xxx : Port 24 is
closed
Target xxx.xxx.xxx.xxx : Port 25 is
closed
```

Analisis File Log

Parsing log dan port scan digunakan untuk menganalisis file log yang telah diambil dari IDS, sehingga dapat digunakan untuk melihat jawaban pertanyaan forensik seperti berapa ip address yang menyerang suatu server, penyerang menggunakan port apa saja untuk memasuki suatu sistem, dan beberapa hal lainnya. Skrip ketiga ini menggunakan SQLite untuk melakukan analisis terhadap file log.

Proses file log menjadi sebuah basis data adalah dengan memanggil skrip pkts2db.pl diikuti dengan membuka file (-read) logfileall.pcap yaitu file log yang akan dieksekusi, lalu –d(untuk membuat basis data) dan nama file log basis data yang baru.

.

```
data@dataku:~$       perllogkedb.pl-r
datalog.pcap-d datalog.db

sqlite>    select    saddr,    daddr,
count(*) as count
...> from ip
...> group by saddr, daddr
...> order by count desc;
Saddr           daddr count
------------ - ---------- ----------
-
xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx 512
xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx 82
xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx 70
xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx 40
xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx 39
xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx 25
xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx 15
xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx 4
```

Analisis Tool Penyerang

Analisis tool yang digunakan oleh penyerang akan dianalisis beberapa IP address saja.

Penyerang dengan IP Adress 125.202.70.xxx melukiskan penyerang yang diketahui berada di asia pasifik.

Penyerang tersebut menggunakan sqlmap untuk melakukan penyerangan ke Universitas Kristen Maranatha

```
sqlite>   select   strftime('%Y-%d-%d
%H:%M', time) as time, saddr, daddr
   ...> from tcp,ip
   ...>   where   tcp.id=ip.id   and
saddr='125.202.70.xxx';

time                              saddr
daddr
```

```
---------------  -------------  ----
----------
2014-11-11    11:47    125.202.70.xxx
xxx.xxx.xxx.xxx
2014-11-11    11:47    125.202.70.xxx
xxx.xxx.xxx.xxx
2014-11-11    11:48    125.202.70.xxx
xxx.xxx.xxx.xxx



125.202.70.xxx     xxx.xxx.xxx.xxx
sqlmap/1.0-dev (rNone)
(http://www.sqlmap.org)
```

Penyerang dengan IP Adress 80.255.48.xxx melukiskan penyerang yang diketahui berada di Eropa.
Penyerang tersebut menggunakan python untuk melakukan penyerangan ke Universitas Kristen Maranatha

```
sqlite>   select   strftime('%Y-%d-%d
%H:%M', time) as time, saddr, daddr
   ...> from tcp,ip
   ...>   where   tcp.id=ip.id   and
saddr='80.255.48.xxx';

time             saddr          daddr
---------------  -------------  -----
----------
2014-09-09    10:41    80.255.48.xxx
xxx.xxx.xxx.xxx
2014-09-09    10:41    80.255.48.xxx
xxx.xxx.xxx.xxx
2014-09-09    10:41    80.255.48.xxx
xxx.xxx.xxx.xxx



86.127.220.36  10.13.254.43  Python-
urllib/2.7
86.127.220.36  10.13.254.43  Python-
urllib/2.7
```

Laporan Hasil Investigasi Forensik Jaringan

Investigasi forensik jaringan dilakukan untuk melakukan penelursuran jejak-jejak dari penyerang. Pencarian jejak dari tindakan illegal pada jaringan dapat dilihat dari file log.

Data diambil pada IDS Snort yang merupakan sistem pendeteksi penyusup pada jaringan. Pada IDS Snort terdapat beberapa aturan (rule) yang digunakan dalam mendeteksi penyusup pada jaringan, pembuatan aturan tersebut merupakan hal yang penting dalampendeteksian penyerangan.

Pada server forensik jaringan digunakan script perl untuk menganalisis kejadian, script parsing pcap digunakan untuk memecah file log berdasarkan waktu penyerangan, ip address, mac address dan port. Lalu script portscanning digunakan untuk mengetahui port yang terbuka pada suatu server dan script untuk analisis file log dengan menggunakan SQLite. Kegunaan script port scan adalah jika penyerang berhasil memasuki suatu sistem dengan menggunakan SQL Injection atau mengekploitasi kelemahan web dengan basis data, maka penyerang akan melakukan port scan untuk mengetahui port mana saja yang terbuka. Kemudian script SQLite digunakan sebagai alat untuk menganalisis file log tersebut. Ketiga script tersebut diletakkan pada server forensik jaringan beserta
dengan modul yang digunakan.
Dengan adanya penelitian forensik jaringan di Universitas Kristen Maranatha diharapkan dapat menjadi kesadaran bahwa cukup sulit untuk melindungi sebuah jaringan dari tindakan serangan. Hal yang dapat dilakukan adalah mencegahnya agar kejadian tersebut tidak terjadi kembali atau mengurangi kerusakan akibat dari serangan tersebut.

4. Kesimpulan

Dari hasil analisa forensik di Universitas Kristen Marnatha, terjadi beberapa serangan dalam dunia maya diantaranya dengan menggunakan sqlmap dan phyton. Dari penelitian ini diharapkan adanya kesadaran dalam setiap insan di sivitas akademika kampus akan banyak serangan dalam dunia maya.

Daftar Pustaka

Anley, C., (2002), Advanced SQL Injection in SQL Server Applications. An NGSSoftware Insight Security Research (NISR) Publications: Next Generation Security Software Ltd.

Baryamureeba,V., Tushabe, F.,(2004), The Enhanced Digital Investigation Process Model. Proceedings of the Fourth Digital Forensic Research Workshop, May 27.

Clarke, J., 2009, SQL Injection Attacks and Defense. Burlington: Syngress Publishing and Elseiver.