# METRIK DAN INDEKS KESELAMATAN LAMAN SESAWANG: SATU KAJIAN KES TERHADAP INSTITUSI PENGAJIAN TINGGI AWAM DI MALAYSIA

MUHAMMAD NIZAM OMAR
MOHD. ZAMRI MURAH

Fakulti Teknologi dan Sistem Maklumat Universiti Kebangsaan Malaysia
muhammadnizam.omar@gmail.com, zamri@ukm.edu.my

**ABSTRAK**

Dunia pada hari ini bergantung kepada laman sesawang sebagai medium utama bagi menguruskan perkhidmatan yang ditawarkan kepada pelanggan. Penggunaan laman sesawang adalah bagi memudahkan dan mempercepatkan pengurusan dan pengedaran kepada pelanggan, tanpa memerlukan mereka hadir secara fizikal ke premis organisasi. Oleh yang demikian, organisasi seharusnya mempunyai cara yang praktikal dan berkesan dalam menilai keselamatan laman sesawang mereka, kerana perkhidmatan yang ditawarkan mengandungi data sensitif seperti nombor kad kredit dan maklumat peribadi pelanggan. Untuk itu, kajian ini mencadangkan satu metodologi bagi menilai keselamatan laman sesawang dengan menggunakan pelbagai jenis pengimbas. Penilaian keselamatan dilakukan dengan membina satu metrik keselamatan yang menggabungkan laporan daripada kesemua pengimbas. Daripada metrik keselamatan ini, satu indeks keselamatan akan dibina bagi membandingkan tahap keselamatan di antara laman sesawang. Perbandingan ini akan digunakan bagi melakukan penarafan ke atas laman sesawang walaupun ia berlainan sistem operasi, perisian dan konfigurasi. Untuk itu, kertas kerja ini mengambil sejumlah 98 laman sesawang utama institusi pengajian tinggi awam di Malaysia sebagai kajian kes.



## 1. PENGENALAN

Terdapat pelbagai teknik dan cara yang dilakukan bagi meningkatkan tahap keselamatan terhadap laman sesawang sesebuah organisasi. Menurut Cavusoglu et al. (2004), antara teknik yang biasa digunakan sesebuah organisasi adalah dengan meletakkan tembok api dan sistem pengesanan pencerobohan (*intrusion detection system*). Namun begitu, bagi memastikan bahawa tahap keselamatan laman sesawang berada pada tahap terbaik adalah dengan membuat penilaian keselamatan secara berkala.

Penilaian keselamatan ini boleh dilakukan menggunakan pelbagai peralatan dan perisian yang terdapat di pasaran seperti *NMAP* dan *Nessus*. Menurut Im et al. (2016), pengimbas seperti *NMAP* dan *Nessus* menggunakan teknik pengesanan cap jari bagi mengenal pasti perkhidmatan yang dijalankan oleh pelayan. Namun laporan hasil imbasan tidak memberikan gambaran secara keseluruhan terhadap tahap keselamatan sesebuah organisasi. Sebagai contoh, hasil imbasan daripada perisian *NMAP* akan memberikan gambaran terhadap port yang dibuka di sesebuah pelayan, manakala imbasan menggunakan *Nessus* akan hanya memberikan gambaran hanya kepada tahap kerentanan pelayan pangkalan data.

Bagi mendapatkan gambaran keselamatan secara menyeluruh, kesemua laporan daripada pelbagai pengimbas sepatutnya diletakkan di bawah satu metrik keselamatan. Namun begitu, penilaian keselamatan sedia ada tidak mengumpulkan kesemua hasil laporan di bawah satu metrik keselamatan. Tanpa satu metrik keselamatan yang menggabungkan kesemua laporan, penilaian keselamatan secara menyeluruh adalah sukar untuk dilakukan.

Menurut Mendes et al. (2014), penggunaan pengimbas yang berlainan tanpa strategi untuk mengukur metrik keselamatan global, akan hanya memberikan pandangan secara berpecah-pecah.

Penilaian keselamatan perlu dilakukan secara berkala. Ini kerana infrastruktur IT dan kod terhadap sistem berubah mengikut masa, dan ini memungkinkan terdapatnya kelemahan baru. Apa yang selamat pada hari semalam, mungkin tidak lagi pada hari ini. Penilaian keselamatan ini tidak menjadikan sesebuah laman sesawang itu lebih selamat, tetapi ia membolehkan pentadbir sistem sedar tentang kelemahan yang terdapat pada infrastruktur IT dan sistem mereka sebelum penyerang menyedari dan mengeksploitasi kelemahan tersebut.

Kajian ini mencadangkan metodologi untuk menilai keselamatan laman sesawang dengan menggabungkan kesemua laporan daripada pengimbas-pengimbas yang berbeza di bawah satu metrik keselamatan. Untuk itu, kajian ini mengambil laman sesawang utama institusi pengajian tinggi awam di Malaysia sebagai kajian kes.

## 2. KAJIAN BERKAITAN

Mohammed et al. (2015) telah melakukan kajian mengenai evolusi keselamatan terhadap 150 laman sesawang di Arab Saudi dengan menggunakan perisian dengan lesen sumber terbuka. Antara laman sesawang yang termasuk di dalam kajian ini adalah daripada sektor kerajaan, pendidikan, kewangan dan juga daripada pihak organisasi berasaskan komersial. Hasil kajian mereka mendapati bahawa 17.5% laman sesawang mempunyai kelemahan terhadap suntikan SQL. 13.5% laman sesawang pula mempunyai kelemahan terhadap suntikan *Shell* dan sebanyak 61% lagi mempunyai kelemahan terhadap *clickjacking*. Kajian mereka juga menyatakan bahawa laman sesawang daripada organisasi komersial lebih selamat daripada laman sesawang milik kerajaan.

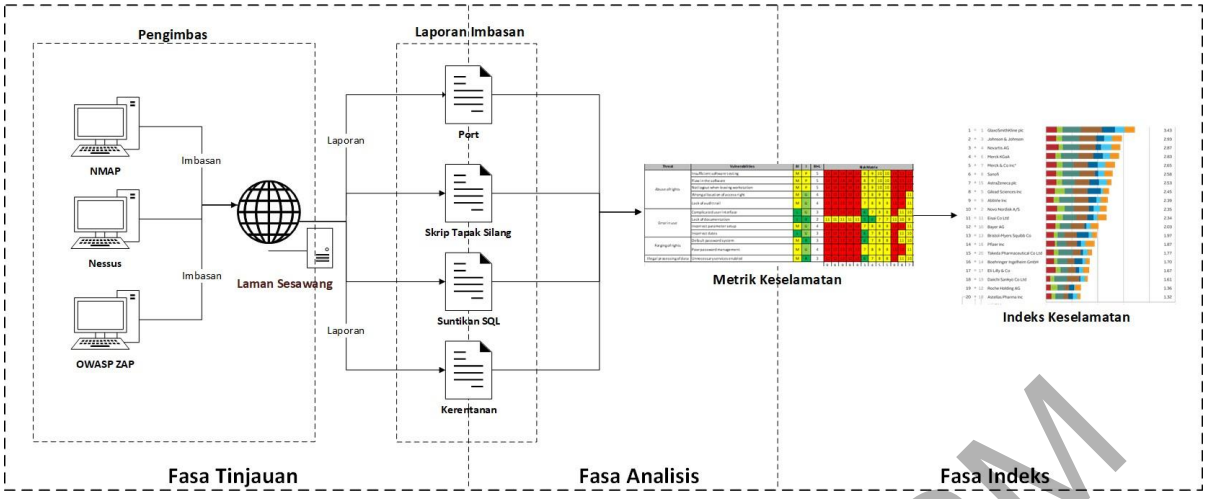
Menurut Tupper et al. (2008), metrik keselamatan merupakan sesuatu yang boleh diukur, sama ada ia berbentuk kualitatif atau kuantitatif. Metrik keselamatan ini mengukur tahap kawalan keselamatan, dasar dan prosedur. Kajian mereka menggunakan perisian *VEA-bility* bagi mendapatkan nilai kuantitatif metrik keselamatan bagi konfigurasi rangkaian. Maklumat ini kemudiannya digunakan oleh pentadbir sistem untuk meneroka konfigurasi alternatif bagi rangkaian.

Wang et al. (2009) mengetengahkan pendekatan bagi menentukan metrik keselamatan perisian berdasarkan kelemahan yang dapat dieksploitasi oleh penyerang. Wang menyatakan bahawa indikasi terpenting keselamatan adalah bilangan kerentanan dan impak kerentanan ini apabila berjaya dieksploitasi.

Menurut DBP, indeks membawa makna laporan secara statistik yang digunakan sebagai petunjuk untuk mengukur prestasi harga, jumlah atau perkembangan sesuatu kumpulan barang atau aset, atau keadaan ekonomi pada suatu masa atau tempoh masa tertentu. Menurut Mudgil et al. (2013), pengindeksan adalah proses penyusunan rekod secara sistematik. Penyusunan indeks membolehkan pengguna mencari rekod dengan lebih cepat.

## 3. CADANGAN METRIK DAN INDEKS KESELAMATAN LAMAN SESAWANG

Terdapat tiga fasa di dalam kajian ini. Fasa pertama adalah fasa tinjauan, diikuti dengan fasa analisis dan diakhiri dengan fasa indeks.




## a. FASA TINJAUAN

Di bawah fasa tinjauan ini, pengimbas akan mengimbas infrastruktur IT dan sistem yang telah dipilih. Pengimbas akan mengimbas port, kerentanan terhadap sistem operasi dan perisian bagi pangkalan data dan kelemahan pada kod yang membolehkan serangan skrip tapak silang dijalankan. Kemudiannya, pengimbas akan mengeluarkan laporan keselamatan mengenai laman sesawang yang diimbas

Pada fasa imbasan ini, setiap jenis pengimbas akan melakukan sebanyak tiga kali imbasan dengan waktu yang berbeza. Ini adalah untuk melihat sekiranya terdapat perubahan konfigurasi keselamatan yang dilakukan oleh pentadbir sistem pada waktu yang berlainan. Ini kerana terdapat pentadbir sistem yang merendahkan tahap konfigurasi keselamatan terhadap laman sesawang bagi melihat sama ada tembok api menghalang aplikasi atau kod yang baru dibina daripada berfungsi dengan sepatutnya. Waktu yang dipilih bagi melakukan imbasan adalah:

a. Waktu Pejabat : 8 Pagi sehingga 5 Petang [Isnin – Jumaat]
b. Selepas Waktu Pejabat : 8 Malam sehingga 5 Pagi [Isnin – Jumaat]
c. Hari Minggu : 1 Pagi sehingga 11 Malam [Sabtu dan Ahad]

Imbasan yang dijalankan terhadap laman sesawang IPTA ini adalah menggunakan metodologi kotak hitam (*black box*) dengan hanya alamat URL sahaja yang diketahui. Imbasan ini juga akan dilakukan daripada luar rangkaian IPTA, yakni secara jauh (*remote*). Pemilihan metodologi begini adalah untuk meniru tindakan yang diambil oleh penyerang di dalam mencari kelemahan terhadap laman sesawang.

## b. FASA ANALISIS

Fasa analisis ini akan mengumpulkan kesemua laporan hasil imbasan yang dijalankan pada infrastruktur IT dan sistem. Setiap laporan imbasan akan dianalisis bagi membolehkan

klasifikasi terhadap data tersebut dilakukan. Klasifikasi dilakukan bagi membolehkan satu nilai kuantitatif diletakkan bagi membina nilai metrik keselamatan.

### i. Analisis Data Imbasan Port

Pengimbas NMAP digunakan untuk mencari port yang dibuka pada pelayan laman

sesawang. Perisian NMAP akan mengimbas keseluruhan pelayan bagi menentukan perkhidmatan yang ditawarkan oleh pelayan tersebut. Kesemua port yang dilaporkan dibuka oleh pengimbas akan direkodkan. Nilai 1 akan diberikan kepada setiap port yang dibuka ($P_b$), ini termasuklah port http ($P_{HTTP}$) dan port https ($P_{HTTPS}$). Bagi mendapatkan metrik keselamatan port, port yang dibuka akan ditolak dengan port 80 dan port 443. Persamaan 3.1 di bawah adalah contoh pengiraan bagi mendapatkan nilai metrik keselamatan port.

Persamaan 3.1 Pengiraan metrik keselamatan bagi port

$$\boldsymbol{MP = P_b - P_{HTTP} - P_{HTTPS}}$$

**ii. Analisis Data Imbasan Kerentanan**

Pengimbas *Nessus* akan digunakan bagi mencari kerentanan terhadap laman sesawang. Laporan yang dikeluarkan oleh pengimbas *Nessus*, membahagikan kerentanan yang didapati pada laman sesawang kepada lima jenis, iaitu kritikal, tinggi, sederhana, rendah dan info.

Namun jenis-jenis kerentanan yang terdapat di dalam *Nessus* tidak membawa nilai kuantitatif, nilai yang boleh dikira secara matematik. Untuk itu, kajian ini memberikan nilai 4 bagi kerentanan kategori kritikal ($K_k$) dan nilai 3 bagi kerentanan kategori tinggi ($K_t$). Kerentanan kategori sederhana ($K_s$) akan diberikan nilai 2 dan nilai 1 diberikan kepada kerentanan kategori rendah ($K_r$). Bagi kategori info ($K_i$), tiada nilai akan diberikan kepada kerentanan tersebut. Ini kerana info adalah maklumat yang tidak berkait dengan kerentanan. Bagi mendapatkan metrik keselamatan kerentanan, kesemua jenis kerentanan akan dikira dengan menggunakan persamaan 3.2 di bawah:

Persamaan 3.2 Pengiraan metrik keselamatan bagi kerentanan

$$\boldsymbol{MV = (K_k * 4) + (K_t * 3) + (K_s * 2) + (K_r * 1) + (K_i * 0)}$$

**iii. Analisis Data Imbasan Skrip Tapak Silang dan Suntikan SQL**

Data daripada pengimbas *OWASP ZAP* akan digunakan bagi mencari kelemahan laman sesawang terhadap serangan skrip tapak silang dan juga suntikan SQL. Namun pengimbas ini tidak mengimbas kesemua halaman yang terdapat di dalam laman sesawang IPTA. Ini kerana terdapat isu pada masa dan storan untuk kajian ini.

Untuk itu, bagi setiap laman sesawang yang dikesan mempunyai kelemahan skrip tapak silang (MX) atau pun suntikan SQL (MS), nilai pemberat satu akan diletakkan. Nilai 1 diberikan tanpa mengambil kira berapa banyak kelemahan tersebut dijumpai. Nilai pemberat 0 akan diletakkan sekiranya tiada kelemahan yang dikesan. Berikut adalah persamaan yang digunakan bagi metrik keselamatan suntikan SQL dan skrip tapak silang.

Persamaan 3.3 Pengiraan metrik keselamatan bagi suntikan SQL

$$\boldsymbol{MS = 1\ atau\ 0}$$

Persamaan 3.4 Pengiraan metrik keselamatan bagi skrip tapak silang

$$\boldsymbol{MX = 1\ atau\ 0}$$

**iv. Nilai Metrik Keselamatan**

Nilai metrik keselamatan dibina dengan mengikut waktu imbasan yang dijalankan.

Bermakna, terdapat tiga nilai metrik yang berbeza mengikut waktu imbasan dijalankan bagi setiap pengimbas. Ini bagi melihat sama ada terdapatnya perbezaan konfigurasi keselamatan yang dilakukan oleh pentadbir sistem. Seharusnya tiada perbezaan konfigurasi keselamatan pada bila-bila masa.

Metrik keselamatan ini dibina dengan kesemua hasil pemberat daripada laporan imbasan port (MK), skrip tapak silang (MX), suntikan SQL (MS) dan kerentanan (MV) akan ditambah bagi mendapatkan jumlah akhir (rujuk persamaan
3.5 – 3.7) nilai metrik keselamatan. Terdapat tiga nilai bagi metrik keselamatan ini, iaitu nilai pada waktu imbasan waktu pejabat (JWP), selepas waktu pejabat (JSP) dan hari minggu (JHM).

Semakin besar hasil tambah jumlah akhir ini, menunjukkan laman sesawang tersebut mempunyai risiko keselamatan yang tinggi untuk digodam. Kesemua jumlah akhir ini akan digunakan pada fasa indeks bagi mendapatkan nilai indeks keselamatan laman sesawang.

Persamaan 3.5 Nilai metrik keselamatan pada waktu pejabat

$$JWP=MP+MV+MS+MX$$

Persamaan 3.6 Nilai metrik keselamatan pada selepas waktu pejabat

$$JSP=MP+MV+MS+MX$$

Persamaan 3.7 Nilai metrik keselamatan pada hari minggu

$$JHM=MP+MV+MS+MX$$

### c. FASA INDEKS

Hasil pengiraan jumlah akhir daripada metrik keselamatan akan mengujudkan indeks keselamatan. Indeks ini membolehkan penarafan dilakukan terhadap infrastruktur IT dan sistem sesebuah organisasi. Penarafan ini dilakukan adalah bagi membolehkan perbandingan keselamatan dilakukan terhadap infrastruktur IT dan sistem walaupun ia berlainan jenis dan konfigurasi, asalkan ia membawa fungsi yang sama.

Persamaan 3.8 digunakan bagi mendapatkan indeks keselamatan. Bagi mendapatkan indeks keselamatan (I), jumlah metrik pada imbasan yang dilakukan pada waktu pejabat (JWP) akan ditambah dengan jumlah metrik pada selepas waktu pejabat (JSP) dan jumlah metrik pada hari minggu (JHM). Nilai ini kemudiannya akan dibahagikan kepada tiga bagi mendapatkan nilau purata untuk ketiga-tiga waktu imbasan.

Daripada nilai purata inilah, indeks keselamatan akan dibina. Susunan pada indeks ini adalah daripada nilai terkecil sehingga kepada yang terbesar. Semakin tinggi nilai indeks untuk laman sesawang tersebut, bermakna semakin tinggi risiko untuk laman sesawang tersebut diserang dengan jayanya oleh penyerang.

Persamaan 3.8 Pengiraan indeks keselamatan

$$I=(JWP+JSP+JHM)/\ 3$$

## 4. METRIK KESELAMATAN LAMAN SESAWANG

Metrik keselamatan adalah gabungan daripada metrik individu bagi:

1. Port
2. Kerentanan
3. Skrip tapak silang
4. Suntikan SQL

Jadual 4.1 adalah contoh bagi jadual metrik keseluruhan. Nilai metrik keseluruhan adalah hasil tambah daripada keseluruhan nilai metrik individu, iaitu daripada metrik port (P), kerentanan (K), suntikan SQL (S) dan skrip tapak silang (X). Setiap IPTA diimbas sebanyak tiga kali pada waktu yang berlainan iaitu pada waktu bekerja (WB), bukan waktu bekerja (BWB) dan juga pada hari minggu (HM).

Jadual 4.1 Contoh metrik keseluruhan

| Entiti | *Waktu | Nilai Metrik Individu | | | | Nilai Metrik Keseluruhan |
|---|---|---|---|---|---|---|
| | | P | K | S | X | |
| U01 | WB | 0 | 0 | 0 | 0 | 0 |
| | BWB | 0 | 17 | 0 | 0 | 17 |
| | HM | 0 | 15 | 0 | 0 | 15 |
| U02 | WB | 0 | 7 | 0 | 0 | 7 |
| | BWB | 0 | 7 | 0 | 0 | 7 |
| | HM | 0 | 5 | 0 | 0 | 5 |
| U03 | WB | 2 | 19 | 0 | 0 | 21 |
| | BWB | 2 | 19 | 0 | 0 | 21 |
| | HM | 2 | 23 | 0 | 0 | 25 |

Jadual 4.2 di bawah merupakan nilai metrik yang diperolehi oleh IPTA berdasarkan persamaan yang digunakan pada fasa analisis di atas. Nilai metrik port bagi keseluruhan IPTA yang membuka selain daripada port HTTP dan HTTPS adalah sebanyak 1697 dengan 1093 daripada nilai tersebut datang daripada kolej dan institut.

Sejumlah 8208 nilai metrik kerentanan dikesan untuk keseluruhan IPTA. 4606 daripadanya datang daripada keterukan sederhana. Ini diikuti oleh keterukan kritikal dengan nilai metrik sebanyak 1620 dan 1120 daripadanya dikesan daripada kolej dan institut.

Jadual 4.2 Nilai metrik bagi keseluruhan IPTA

| IPTA | Jumlah Nilai Metrik | | | | | | |
|---|---|---|---|---|---|---|---|
| | Port | Kerentanan | | | | SQL | XSS |
| | | K | T | S | R | | |
| Universiti | 142 | 100 | 159 | 794 | 78 | 1 | 9 |
| Politeknik | 462 | 400 | 477 | 1588 | 78 | 1 | 17 |
| Kolej dan Institut | 1093 | 1120 | 867 | 2224 | 323 | 0 | 4 |
| **Jumlah Keseluruhan IPTA** | **1697** | **1620** | **1503** | **4606** | **479** | **2** | **30** |

Kritikal (K) / Tinggi (T) / Sederhana (S) / Rendah (R)

## 5. INDEKS KESELAMATAN LAMAN SESAWANG

Pengiraan indeks ini dilakukan dengan mengambil purata hasil tambahan nilai metrik pada waktu imbasan dijalankan pada waktu pejabat, waktu selepas pejabat dan hari minggu. Hasil purata bagi nilai indeks ini dibundarkan kepada dua titik perpuluhan sahaja.

Jadual 5.1 adalah indeks keselamatan keseluruhan IPTA ini menggabungkan kesemua universiti, politeknik, kolej dan institut. Kesemua IPTA telah disusun dengan

kedudukan menaik berdasarkan jumlah indeks keselamatan yang diperolehi.

Jadual 5.1 Indeks keselamatan bagi keseluruhan IPTA

| Posisi | Entiti | Indeks | Posisi | Entiti | Indeks |
|---|---|---|---|---|---|
| 1 | K01 | 0.00 | 50 | K39 | 22.67 |
| 2 | P15 | 0.33 | 51 | K22 | 23.00 |
| 3 | U14 | 1.00 | 51 | K30 | 23.00 |
| 3 | P04 | 1.00 | 53 | U13 | 23.33 |
| 3 | P14 | 1.00 | 54 | K23 | 23.33 |
| 3 | P16 | 1.00 | 55 | K24 | 25.00 |
| 7 | K07 | 2.00 | 56 | U04 | 25.67 |
| 8 | P24 | 2.67 | 57 | P30 | 28.00 |
| 9 | K03 | 3.00 | 58 | K05 | 29.00 |
| 10 | U05 | 3.33 | 59 | U15 | 30.67 |
| 11 | U23 | 5.33 | 60 | K31 | 32.00 |
| 11 | K26 | 5.33 | 61 | P20 | 38.00 |
| 13 | U21 | 6.00 | 61 | K35 | 38.00 |
| 13 | P11 | 6.00 | 63 | P07 | 41.67 |
| 13 | K36 | 6.00 | 64 | K11 | 44.67 |
| 16 | U02 | 6.33 | 65 | K12 | 45.67 |
| 17 | K25 | 6.67 | 66 | K10 | 46.33 |
| 17 | K27 | 6.67 | 67 | P29 | 48.33 |
| 17 | K32 | 6.67 | 68 | P18 | 49.67 |
| 20 | U20 | 7.33 | 69 | K21 | 55.67 |
| 21 | P26 | 8.00 | 70 | P10 | 56.00 |
| 21 | K09 | 8.00 | 71 | K17 | 56.67 |
| 23 | U18 | 8.33 | 71 | K37 | 56.67 |
| 23 | P06 | 8.33 | 73 | P02 | 57.00 |
| 25 | U19 | 8.67 | 74 | P03 | 60.33 |
| 25 | K15 | 8.67 | 75 | P28 | 66.33 |
| 27 | U10 | 9.00 | 76 | P05 | 68.00 |
| 27 | U17 | 9.00 | 77 | P25 | 68.33 |
| 27 | P12 | 9.00 | 78 | K38 | 72.00 |
| 27 | K40 | 9.00 | 79 | K16 | 73.00 |
| 31 | P08 | 10.33 | 80 | K19 | 73.33 |
| 32 | U01 | 10.67 | 81 | P17 | 73.67 |
| 33 | U07 | 11.00 | 82 | U22 | 75.33 |
| 33 | K33 | 11.00 | 83 | K18 | 76.33 |
| 35 | U24 | 12.00 | 84 | P21 | 77.00 |
| 36 | K14 | 13.00 | 85 | U06 | 79.67 |
| 37 | P27 | 14.00 | 86 | K44 | 82.67 |
| 38 | K13 | 14.33 | 87 | P22 | 83.00 |
| 39 | P23 | 16.67 | 88 | K34 | 92.00 |
| 40 | U16 | 17.00 | 89 | P19 | 103.33 |
| 41 | U11 | 17.33 | 90 | K43 | 106.00 |
| 42 | U09 | 18.00 | 91 | P13 | 107.33 |
| 42 | K08 | 18.00 | 92 | K41 | 112.00 |
| 44 | K02 | 18.67 | 93 | K42 | 135.67 |

bersambung...

...sambungan

| | | | | | |
|---|---|---|---|---|---|
| 45 | U08 | 20.33 | 94 | K28 | 137.00 |
| 45 | K06 | 20.33 | 95 | P01 | 146.67 |
| 47 | K29 | 22.00 | 96 | K20 | 161.00 |
| 48 | U03 | 22.33 | 97 | P09 | 176.00 |
| | K04 | 22.33 | | U12 | 65518.67 |

48 98

Jadual 5.2 di bawah adalah merupakan kesimpulan bagi nilai indeks keselamatan, median, kekerapan, purata dan risiko bagi keseluruhan IPTA

Jadual 5.2 Kesimpulan nilai indeks keselamatan, median, kekerapan, purata dan risiko bagi keseluruhan IPTA

| IPTA / Jumlah | Nilai Indeks | Median | Kekerapan / Ulangan | Purata | Risiko | | |
|---|---|---|---|---|---|---|---|
| | | | | | Rendah | Sederhana | Tinggi |
| Keseluruhan / 97 | 3475.33 | 22.33 | 1.00 / 4 | 38.13 | 62 | 22 | 13 |
| Universiti / 24 | 427.67 | 11.50 | 9.00 / 2 | 18.59 | 16 | 5 | 2 |
| Politeknik / 30 | 1427.00 | 45.00 | 1.00 / 3 | 47.57 | 15 | 11 | 4 |
| Kolej dan Institut / 44 | 1844.33 | 23.17 | 6.67 / 3 | 41.92 | 27 | 10 | 7 |

## 6. PENILAIAN RISIKO KESELAMATAN

Berikut adalah penilaian risiko keselamatan laman sesawang bagi IPTA di Malaysia. Penilaian ini dilakukan melalui imbasan yang dilakukan menggunakan pengimbas *NMAP*, *Nessus* dan *OWASP ZAP*.

### a. PORT

Sebanyak 60 buah IPTA hanya membuka port HTTP dan HTTPS sahaja pada pelayan laman sesawang mereka. Jumlah terbesar adalah datang daripada kolej dan institut dengan sebanyak 30 buah, iaitu 68% daripada jumlah keseluruhan kolej dan institut. Ini diikuti dengan 14 buah universiti, iaitu 58% daripada 24 buah universiti. Akhir sekali, sebanyak 16 buah politeknik, bersamaan dengan 53% daripada sejumlah 30 buah politeknik (rujuk jadual 6.1).

Jadual 6.1 Jumlah IPTA yang mengubah konfigurasi dan menjalankan perkhidmatan selain daripada perkhidmatan HTTP dan HTTPS.

| IPTA | Konfigurasi | | Port | |
|---|---|---|---|---|
| | Ubah | Sama | 80 / 443 | Lain-lain |
| Universiti | 1 | 23 | 14 | 10 |
| Politeknik | 5 | 25 | 16 | 14 |
| Kolej dan Institut | 7 | 37 | 30 | 14 |
| Keseluruhan | 13 | 85 | 60 | 38 |

### b. SUNTIKAN SQL DAN SKRIP TAPAK SILANG

Tiada kelemahan suntikan SQL dikesan pada kolej dan institut, namun 4 daripadanya dikesan mempunyai kelemahan skrip tapak silang. Yang paling membimbangkan adalah politeknik dengan 17, yakni lebih daripada separuh politeknik yang diimbas mempunyai kelemahan ini. Ini diikuti dengan sebanyak 9 buah universiti dan 4 buah kolej dan institut (rujuk jadual 6.2).

Jadual 6.2 Jumlah IPTA yang mempunyai kelemahan suntikan SQL dan skrip tapak silang

| IPTA | SQL | XSS |
|---|---|---|
| Universiti | 1 | 9 |

| | | |
|---|---|---|
| Politeknik | 1 | 17 |
| Kolej dan Institut | 0 | 4 |
| | 2 | 30 |
| Keseluruhan | | |

## c. KERENTANAN

Data daripada imbasan kerentanan adalah paling membimbangkan dengan sebanyak 4245 kerentanan yang mempunyai keterukan bernilai kritikal (484), tinggi (668), sederhana (2402), dan rendah (691) dijumpai (rujuk rajah 6.3). Daripada 484 kerentanan dengan keterukan kritikal ini, 25 daripadanya datang dari 6 buah universiti. Sejumlah 179 keterukan kritikal datang daripada 15 buah politeknik. Bakinya datang daripada 18 kolej dan institut dengan sejumlah 280 kerentanan kritikal dijumpai.

668 keterukan bernilai tinggi dijumpai pada 52 buah IPTA. 9 buah universiti mempunyai keterukan tinggi sebanyak 53. Ini diikuti dengan 17 buah politeknik dengan sebanyak 326 dikesan. Bakinya, sebanyak 289 keterukan tinggi dikesan pada kolej dan institut (rujuk rajah 6.3).

Jadual 6.3 Jumlah kerentanan per jumlah IPTA

| IPTA | Jumlah Kerentanan / Jumlah IPTA | | | | |
|---|---|---|---|---|---|
| | Kritikal | Tinggi | Sederhana | Rendah | Info |
| Universiti | 25 / 6 | 53 / 9 | 397 / 23 | 78 / 14 | 3501 / 24 |
| Politeknik | 179 / 15 | 326 / 17 | 893 / 26 | 290 / 22 | 6197 / 30 |
| Kolej dan Institut | 280 / 18 | 289 / 26 | 1112 / 42 | 323 / 37 | 12834 / 44 |
| Keseluruhan | 484 / 39 | 668 / 52 | 2402 / 91 | 691 / 73 | 22532 / 98 |

## d. SISTEM OPERASI

Sistem operasi berasaskan Linux menjadi pilihan dan kegemaran pentadbir sistem bagi IPTA dengan 53% daripada mereka memilih untuk menggunakannya. Ini diikuti oleh Windows dengan 15% laman sesawang menggunakannya sebagai sistem operasi. Sebanyak 4 buah IPTA yang mengubah sistem operasi mereka. 6 buah IPTA menggunakan sistem operasi Forti. (rujuk jadual 6.4).

Jadual 6.4 Pecahan sistem operasi laman sesawang mengikut IPTA

| IPTA | Sistem Operasi Laman Sesawang | | | | | |
|---|---|---|---|---|---|---|
| | Windows | Linux | Forti | Mac | Tidak Diketahui | Ubah |
| Universiti | 2 | 11 | 6 | 2 | 2 | 1 |
| Politeknik | 6 | 16 | 0 | 0 | 6 | 2 |
| Kolej dan Institut | 7 | 25 | 0 | 0 | 11 | 1 |
| Keseluruhan | 15 | 52 | 6 | 2 | 19 | 4 |

## 7. KESIMPULAN

Kajian ini mengetengahkan metodologi bagi melakukan penilaian keselamatan terhadap laman sesawang. Metodologi kajian ini adalah berdasarkan laporan imbasan yang dikeluarkan oleh pengimbas. Daripada laporan tersebut, satu metrik keselamatan dibina dengan meletakkan

suatu nilai pemberat berdasarkan keterukan yang dijumpai. Semakin tinggi nilai keterukan,

bermakna semakin tinggi nilai metrik yang didapati oleh laman sesawang tersebut.

Berdasarkan metrik keselamatan ini, satu indeks keselamatan dibina bagi memudahkan penarafan dan perbandingan keselamatan laman sesawang. Perbandingan di antara laman sesawang ini boleh dilakukan walaupun laman sesawang tersebut menggunakan sistem operasi, konfigurasi dan perisian yang berlainan antara satu sama lain. Bagi membuktikan bahawa metodologi ini boleh digunakan dalam dunia sebenar, laman sesawang institusi pengajian tinggi awam di Malaysia diangkat sebagai kajian kes.

Kajian yang dijalankan masih boleh dilakukan penambahbaikan pada masa hadapan. Berikut adalah cadangan bagi menjalankan kajian lanjutan pada masa hadapan:

1. Imbasan yang dilakukan adalah tidak terhad kepada laman sesawang utama sahaja. Seharusnya kesemua sub domain dimasukkan sekali ke dalam imbasan yang dijalankan. Ini supaya, penilaian keselamatan secara menyeluruh dapat dilakukan terhadap keseluruhan laman sesawang organisasi.
2. Kesemua anak halaman (*child*) pada setiap kedalaman (*depth*) perlulah diimbas bagi mengelakkan terdapatnya kelemahan suntikan SQL dan skrip tapak silang yang terlepas pandang.
3. Menggunakan pengimbas versi terkini. Ini kerana pengimbas dengan lesen sumber terbuka ini tidak mengemas kini perisian, *plugin* dan pangkalan data mereka secara automatik.
4. Imbasan dilakukan untuk bulan yang berlainan pada sepanjang tahun.
    a. Awal tahun : Ini bagi melihat sama ada terdapatnya perubahan konfigurasi dilakukan oleh pentadbir sistem apabila mendapat peruntukan kewangan bagi menaik taraf laman sesawang.
    b. Akhir tahun : Bagi melihat sama ada pentadbir sistem mengemas kini sistem operasi dan perisian yang digunakan bagi menutup kerentanan yang dijumpai pada tahun tersebut.

## 8. RUJUKAN

Cavusoglu, H., Mishra, B., & Raghunathan, S. 2004. Communications of the ACM. A Model for Evaluating IT Security Investments 7(47):87-92

Im, S.Y., Shin, S.H., Ryu, K.Y., & Roh B.H. 2016. Eighth International Conference on Ubiquitous and Future Networks (ICUFN). Performance Evaluation of Network Scanning Tools with Operation of Firewall 876-881

Mendes, N., Duraes, J. & Madeira, H. 2014. IEEE 25th International Symposium on Software Reliability Engineering. Security Benchmarks for Web Serving Systems. 1-12

Mendes, N. 2015. Security Benchmarks for Web Serving Systems. Tesis Doctoral Program of Science and Information Technology, Faculty of Science and Technology, University of Coimbra.

Mohammed S. AL-Sanea & Ahmad A. Al-Daraiseh. 2015. First International Conference on Security Anti-Cybercrime (ICACC). Evaluation of Saudi Arabia's Websites Using Open Source Tools. 5-9

Mudgil, P., Sharma, A.K. & Gupta, P. 2013. 5th International Conference on Computational Intelligence and Communication Networks. An Improved Indexing Mechanism to Index Web Documents. 460-464

Pamula, J., Jajodia, S., Ammann, P. & Swarup, V. 2006. Proceedings of the ACM Workshop on Quality of Protection. Weakest Adversary Security Metric for Network Configuration Security Analysis. 31-38

Tupper, M. & Zincir-Heywood, A.N. 2008. Third International Conference on Availability, Reliability and Security. VEA-bility Security Metric: A Network Security Analysis Tool. 950 – 957

Wang, L., Singhal, A. & Jajodia, S. 2007. Proceedings of the ACM Workshop on Quality of Protection. Toward Measuring Network Security Using Attack Graphs. 49-55