# IMPLEMENTASI KEAMANAN JARINGAN MENGGUNAKAN *INTRUSION DETECTION SYSTEM* (IDS) PADA PT. MEGA ESA FARMA

Veren Prisscilya[1], Tri Santoso[2]
[12]Jurusan Teknik Informatika, Sekolah Tinggi Manajemen Informatika dan Komputer Nusa Mandiri Jakarta

***Abstract.*** *In the current global era, Information Technology (IT) has developed rapidly, especially with the existence of an internet network that makes it easy to communicate and exchange data with other parties. Because of the easy access to this information, security issues have become a major focus in the world of computer networks. This causes a new problem that is important information or data can be used by parties who are not responsible for their own benefits. So that a network security system becomes an important aspect. PT. Mega Esa Farma is an industrial company engaged in the field of Pharmacy. This company is one of the many companies in Indonesian that has obstacles in network security, the absence of monitoring on a company's computer network is very bad for data security. Therefore, we need a system that can be used to monitor and proctect the network from threats that will occur. By using the Intrusion Detection System (IDS) with snort to follow up on the generated snort alerts. A DDOS attack and port scanning attempt has been conducted on a computer that has a snort installed and the results are obtained that the snort is able to detect the attack and directly send alert to the administrator.*
***Key Words:*** *IDS, Snort, Network, Security*

***Abstrak.*** *Pada era global saat ini, Teknologi Informasi (TI) telah berkembang dengan pesat, terutama dengan adanya jaringan internet yang memudahkan dalam melakukan komunikasi dan pertukaran data dengan pihak lain. Karena mudahnya pengaksesan terhadap informasi tersebut, masalah keamanan telah menjadi fokus utama dalam dunia jaringan komputer. Hal ini menyebabkan timbulnya masalah baru yaitu informasi atau data-data penting dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mendapatkan keuntungan sendiri. Sehingga suatu sistem keamanan jaringan menjadi salah satu aspek yang penting. PT. Mega Esa Farma merupakan perusahaan industri yang bergerak dalam bidang Farmasi, Perusahaan ini merupakan salah satu dari banyak perusahaan yang ada di Indonesia yang mempunyai kendala dalam keamanan jaringan, tidak adanya pemantauan pada jaringan komputer suatu perusahaan sangat berdampak buruk bagi keamanan data. Oleh karena itu, dibutuhkan suatu sistem yang dapat digunakan untuk memantau dan melindungi jaringan dari ancaman yang akan terjadi. Dengan menggunakan Intrusion Detection System (IDS) dengan Snort untuk menindak lanjuti alert snort yang dihasilkan. Telah dilakukan percobaan serangan DDOS dan Port Scanning pada komputer yang telah dipasang snort dan diperoleh hasil bahwa snort mampu mendeteksi adanya serangan tersebut dan secara langsung mengirimkan alert kepada administrator.*
***Kata Kunci:*** *IDS, Snort, Network, Security*

## 1. Pendahuluan

Seorang pengelola *server* jaringan dan internet (*system administrator*) memiliki tanggung jawab yang besar terhadap keamanan sistem dari waktu ke waktu, memastikan bahwa sistem dan jaringan yang dikelola terjaga dari berbagai peluang ancaman. Perusahaan merupakan salah satu tempat dimana penggunaan jaringan internet terbuka terhadap pemakai-pemakainya. Penggunaan tersebut bisa dipergunakan dengan benar dan tidak pula disalahgunakan pemakaiannya. Selain itu *administrator* harus mengetahui sesuatu *log* yang mengidentifikasi adanya serangan atau penyalahgunaan jaringan. Oleh karena itu, dibutuhkan suatu sistem dalam menangani penyalahgunaan jaringan atau ancaman yang akan terjadi yaitu dengan menggunakan *Intrusion Detection System* (IDS) [1].

PT. Mega Esa Farma merupakan perusahaan industri yang bergerak dalam bidang Farmasi. Perusahaan ini merupakan salah satu dari banyak perusahaan yang ada di Indonesia yang mempunyai

 ISSN: 2579-566X (Online)
ISSN: 2477-5274 (Print)

kendala dalam keamanan jaringan, tidak adanya pemantauan jaringan computer suatu perusahaan sangat berdampak buruk bagi kemanan data.

Pentingnya nilai dari sebuah informasi menjadikan informasi tersebut dibatasi hanya untuk orang-orang tertentu. Bocornya suatu informasi ke pihak yang tidak bertanggung jawab dapat menimbulkan kerugian bagi pemilik informasi [2]. *Intrusion Detection System* (IDS) akan melakukan pemberitahuan saat mendeteksi sesuatu yang dianggap mencurigakan atau tindakan *ilegal* [3].

## 2. Tinjauan Pustaka

bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktivitas jaringan komputer. Menurut Steven A. Hofmeyr dalam jurnalnya yang berjudul "*Intrusion Detection using Sequences of System Calls*", salah satu mekanisme keamanan IDS adalah dengan melakukan asumsi bahwa sistem dalam keadaan tidak aman, dengan begitu IDS dapat melakukan pendeteksian dengan pola yang aneh pada sistem tersebut [4].

*Snort* merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu menganalisis paket yang melintasi jaringan secara *real time traffic* dan *logging* ke dalam *database* serta mampu mengidentifikasi berbagai serangan yang berasal dari luar jaringan [1].

*Snort* dapat diimplementasikan dalam jaringan yang *multiplatform*, salah satu kelebihannya adalah mampu mengirimkan *alert* dari mesin Unix ataupun Linux ke *platform* Microsoft Windows dengan melalui *Server Message Box* (SMB). *Snort* dapat bekerja dalam 3 mode, yaitu *Sniffer Mode* (mode penyadap), *Packet Logger Mode* (mode perekam paket) dan *Network Intrusion Detection Mode* (mode memonitor jaringan) [5]

## 3. Metode Penelitian

Terdapat dua metode penelitian yang digunakan, yaitu:

### 3.1 Metode Pengumpulan Data

Metode yang digunakan dalam melakukan penelitian yang dijadikan informasi untuk menganalisa, yaitu:

### 3.2 Observasi

Melakukan pengamatan secara langsung pada PT. Mega Esa Farma untuk mendapatkan gambaran mengenai sistem jaringan komputer yang sedang berjalan.

### 3.3 Wawancara

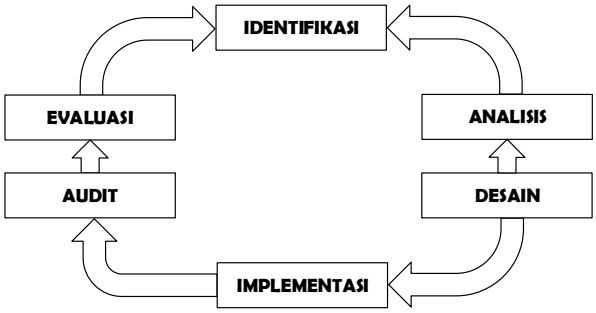
Melakukan tanya jawab terhadap karyawan PT. Mega Esa Farma terutama pada divisi Teknik untuk mendapatkan informasi akurat sehingga menunjang penelitian yang akan dilakukan.

### 3.4 Studi Pustaka

Mencari dan mengumpulkan segala informasi yang berkaitan dengan penelitian yang bersumber dari jurnal, *ebook* dan internet. Seluruh informasi tersebut dikumpulkan dan akan digunakan sebagai pedoman dalam pencarian solusi yang sesuai untuk menyelesaikan permasalahan yang sedang dihadapi pada PT. Mega Esa Farma.

### 3.5 Analisa Penelitian

Metode yang digunakan dalam melakukan penelitian ini adalah *Security Policy Development Life Cycle* (SPDLC).




**Gambar 1. Metode *Security Policy Development Life Cycle* (SDPLC)**

Berikut penjelasan tentang tahapannya, yaitu:

### 3.6 Identifikasi

Melakukan identifikasi terhadap masalah keamanan jaringan dan sistem yang sedang berjalan pada PT. Mega Esa Farma.

### 3.7 Analisis

Menganalisa data yang telah diperoleh pada tahap identifikasi untuk menentukan metode apa yang dapat digunakn untuk mengamankan jaringn pada PT. Mega Esa Farma.

### 3.8 Desain

Membuat sebuah skema topologi sistem keamanan yang tepat dan membuat alur sistem autentikasi serta menentukan kebutuhan sistem yang diperlukan oleh PT. Mega Esa Farma.

### 3.9 Implementasi

Menerapkan semua rancangan yang telah didesain dan direncanakan, selanjutnya dilakukan pengujian apakah hasil yang diperoleh dapat berjalan dan digunakan oleh *user* atau *administrator*.

### 3.10 Audit

Melakukan pemeriksaan untuk memastikan bahwa sistem keamanan yang diterapkan sudah sesuai dengan tujuan awal dan dapat digunakan oleh PT. Mega Esa Farma.

### 3.11 Evaluasi

Melakukan evaluasi dari hasil yang telah diperoleh pada tahap-tahap sebelumnya. Hal tersebut bertujuan untuk mengetahui apakah keamanann yang telah dirancang dapat berjalan sesuai dengan tujuan awal yang telah direncanakan serta mendapatkan *feedback* dari *user*.

## 4. Hasil Dan Pembahasan

### 4.1 Permasalahan

Setelah melakukan penelitian telah diperoleh masalah yang terjadi pada PT. Mega Esa Farma yaitu kurangnya keamanan jaringan komputer, dimana PT. Mega Esa Farma hanya menggunakan antivirus saja dan tidak adanya komputer *server* yang dapat digunakan untuk mengatur keamanan jaringannya.

### 4.2 Alternatif Pemecahan Masalah

Alternatif pemecahan masalah yang dapat ditempuh pada sistem jaringan yang terdapat pada PT. Mega Esa Farma adalah:

 ISSN: 2579-566X (Online)
ISSN: 2477-5274 (Print)

Pentingnya komputer *server* untuk mengawasi data-data yang keluar masuk dalam suatu jaringan

Mengamankan jaringan dengan cara mengusulkan keamanan tambahn dengan melakukan konfigurasi IDS menggunakan *Snort* untuk memperkuat keamanan jaringan agar dapat mendeteksi atau mencegah serangan.

### 4.3 Topologi Jaringan

Topologi jaringan pada PT. Mega Esa Farma tidak mengalami perubahan, dimana topologi yangn digunakan masih menggunakan topologi *tree.*

### 4.4 Skema Jaringan

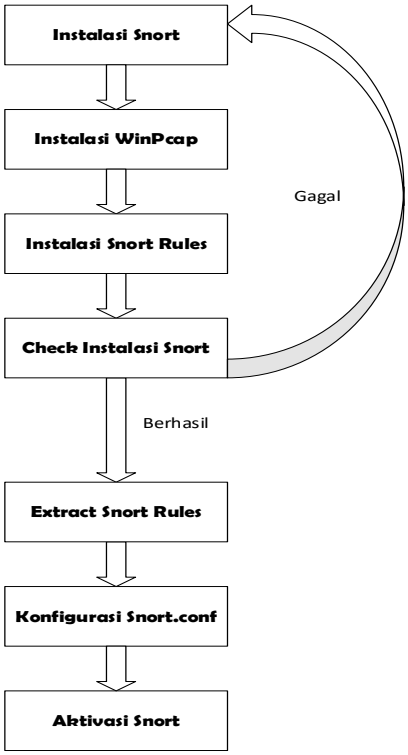
Setelah melakukan penelitian penulis tidak banyak merubah skema jaringan yang sudah berjalan pada PT. Mega Esa Farma, hanya menambahkan PC *Server* yang akan digunakan sebagai pusat untuk mengamankan jaringan, dimana PC *Server* akan digunakan untuk meng-*install* IDS menggunakan *snort* yang dapat berguna untuk memantau, melindungi dan memperkuat keamanan jaringan yang terdapat pada PT. Mega Esa Farma.

### 4.5 Keamanan Jaringan

Pada keamanan jaringan penulis mengusulkan keamanan jaringan menggunakan IDS *Snort*, dimana telah dibahas sebelumnya bahwa PT. Mega Esa Farma hanya menggunakan *antivirus* saja untuk keamanannya. Penulis memilih IDS untuk keamanan jaringan yang dapat digunakan sebagai sebuah alarm/peringatan keamanan yang dikonfigurasi untuk mengamankan dan melindungi informasi atau aset yang berharga pada sebuah perusahaan dari serangan dan kegiatan penyusup. IDS yang digunakan adalah *snort* untuk mendeteksi sistem jaringan. *Snort* merupakan salah satu program *Network-based Intrusion Detection System*, yaitu sebuah program yang dapat mendeteksi suatu usaha penyusupan pada suatu sistem jaringan komputer. *Snort* bersifat *Open Source* dengan lisensi *GNU General Purpose License* sehingga *software* ini dapat digunakan untuk mengamankan *system server* secara gratis.

### 4.6 Rancangan Aplikasi

Berikut ini beberapa rancangan aplikasi yang dapat diusulkan untuk mengatasi permasalahan yang telah dibahas sebelumnya, yaitu:




**Gambar 2. Flowchart Rancangan Aplikasi**

### 4.7 Manajemen Jaringan

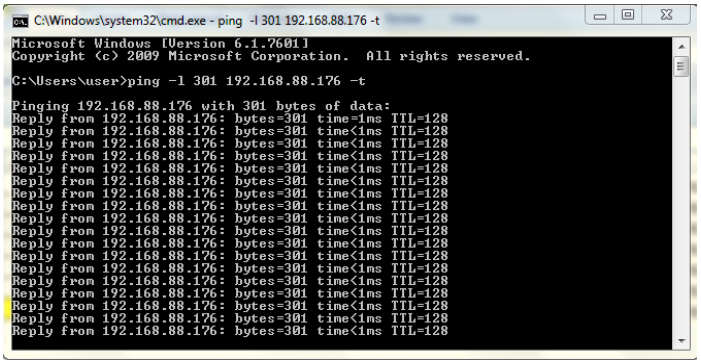
Dengan mengusulkan IDS untuk keamanan jaringan penulis berharap agar dapat memudahkan pekerjaan *administrator* dalam manajemen sebuah keamanan jaringan, karena IDS dapat melakukan pemantauan atau pendeteksian terhadap jaringan dan juga memberikan peringatan dari hasil pemantauan atau pendeteksian kepada *administrator* apabila terdeteksi suatu serangan.

### 4.8 Pengujian Jaringan

Pada tahapan pengujian jaringan disini kita akan melakukan berbagai macam serangan mulai daari DDOS, DoS dan Nmap. Pengujian penyerangan tersebut dilakukan untuk melihat apakah IDS *Snort* dapat mendeteksi adanya serangan atau tidak**.**

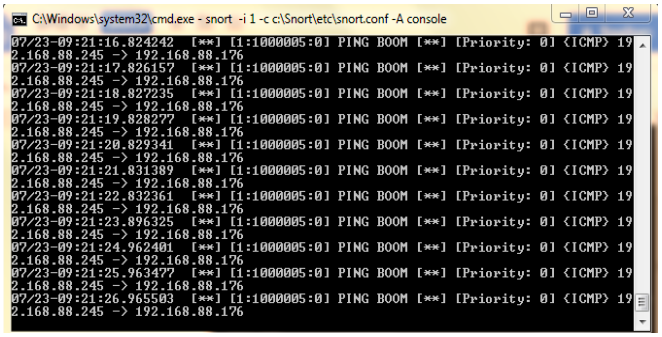
### 4.9 Serangan DDoS

Percobaan serangan yang melibatkan 1 komputer atau lebih yang terkoneksi internet yang digunakan untuk membanjiri sebuah server dengan paket ICMP, TCP, UDP. Tujuannya untuk membuat *bandwith server* menjadi *overload* atau *server down (Zombie).*



ISSN: 2579-566X (Online)
ISSN: 2477-5274 (Print)

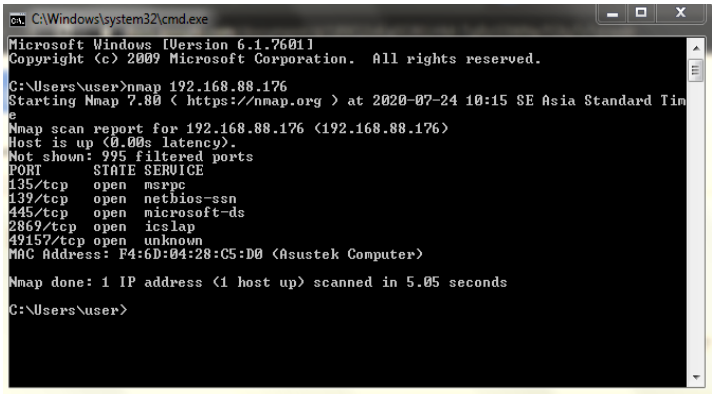
Gambar 3. Serangan DdoS dari PC *Client*



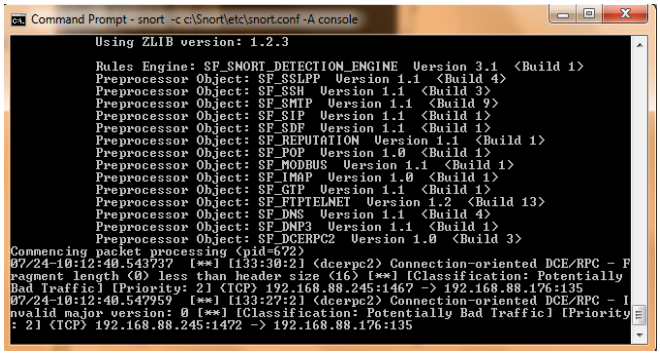

Gambar 4. Pemberitahuan serangan DDOS dari PC *Server*

### 4.10 Nmap (*Network Mapper*)

Merupakan sebuah *tools open source* untuk *explorasi* dan audit keamanan jaringan, dimana *Nmap* berfungsi sebagai aplikasi untuk melihat *port* mana saja yang terbuka atau bisa disebut sebagai *Port Scanner*, dapat juga digunakan untuk serangan lain seperti DOS.

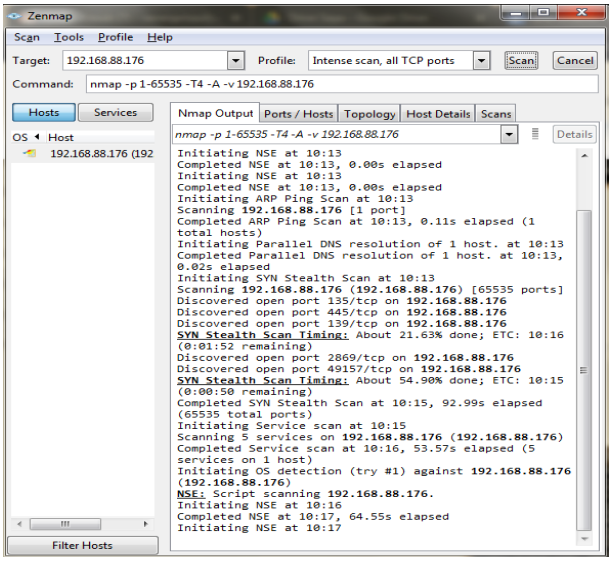



Gambar 5. Serangan *Nmap* dari PC *Client*

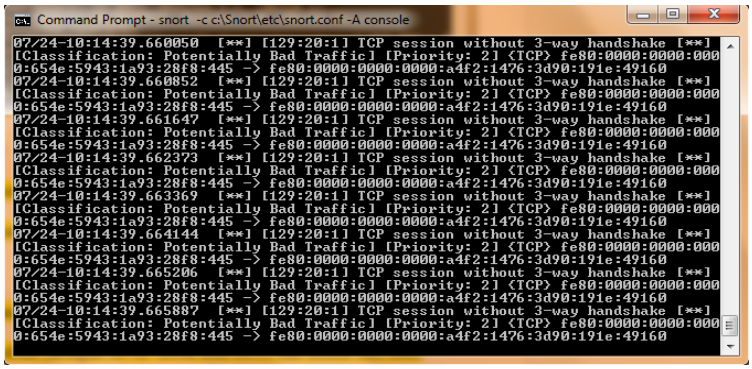



Gambar 6. Pemberitahuan Serangan *Nmap* dari PC *Server*

### 4.11 Serangan *Nmap DOS*



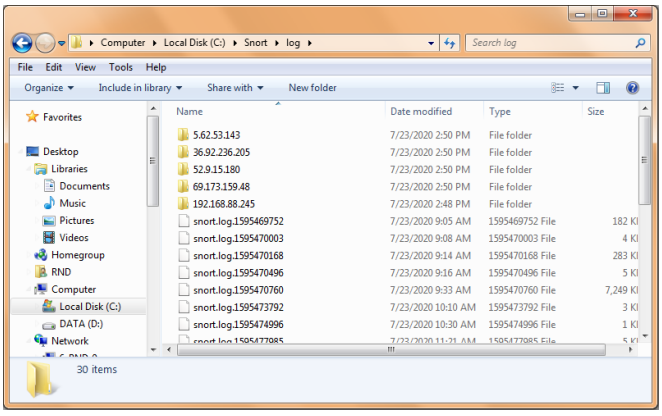

Gambar 7. Serangan *Nmap DOS* dari PC *Client*




Gambar 8. Pemberitahuan Serangan *Nmap DOS* dari PC *Client*

### *4.12 Report IDS Snort Log*

*Snort* melakukan pencatatan laporan dari hasil serangan yang telah dilakukan dan catatan tersebut akan disimpan pada *folder log*, yang akan digunakan untuk menyimpan berbagai macam aktivitas jaringan maupun ancaman yang terdeteksi dalam bentuk *file* dengan nama *folder* IP dari jaringan yang melaluinya untuk memudahkan *administrator* untuk menganalisa masalah yang terjadi pada jaringan.




Gambar 9. *Snort Log Report*

 ISSN: 2579-566X (Online)
ISSN: 2477-5274 (Print)

## 5. Penutup

### 5.1 Kesimpulan

Dengan meng-*install snort* pada PC *Server*, PC *Server* dapat digunakan sebagai pusat untuk memantau dan melindungi keamanan jaringan yang berada pada jaringan yang sama dan tidak perlu lagi melakukan instalasi *snort* pada komputer lain, IDS *snort* dapat mendeteksi adanya serangan seperti *DDOS* dan *Nmap,* dengan menggunakan *snort* dapat membantu *administrator* dalam memantau jaringan secara *realtime,* karena *snort* dapat memberikan peringatan secara langsung apabila terdeteksi sebuah serangan, sehingga *administrator* dapat langsung menindaklanjuti peringatan tersebut.

### 5.2 Saran

Perlunya pengembangan *rules* atau konfigurasi pada *snort* agar dapat mendeteksi serangan selain *DDOS* dan *Nmap,* untuk memudahkan *administrator* dalam mendapatkan peringatan ada baiknya *snort* dapat dikembangkan lagi dalam bentuk *SMS gateway,* karena *snort* tidak bisa menindaklanjuti *alert* yang terdeteksi, ada baiknya menambahkan keamanan jaringan yang lain untuk melindungi keamanan jaringan.

## Referensi

Sutarti, P. Pancaro, Adi, and I. Saputra, Fembi, "Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal," *J. PROSISKO*, vol. 5, no. 1, 2018, [Online]. Available: http://e-jurnal.lppmunsera.org/index.php/PROSISKO/article/download/584/592.

M. S. H. S.S, L. F. Aksara, and N. Ransi, "Implementasi Keamanan Server Pada Jaringan Wireless Menggunakan Metode Intrusion Detection and Prevention System (Idps) (Studi Kasus : Techno'S Studio)," *semanTIK*, vol. 4, no. 2, pp. 11–20, 2018, doi: 10.5281/zenodo.1407864.

A. Elanda and D. Tjahjadi, "Analisis Manajemen Resiko Sistem Keamanan Ids (Intrusion Detection System) Dengan Framework Nist (National Institute of Standards and Technology) Sp 800-30," *Infoman's*, vol. 12, no. 1, pp. 1–13, 2018, doi: 10.33481/infomans.v12i1.45.

E. Risyad, M. Data, and E. S. Pramukantoro, "Perbandingan Performa Intrusion Detection System ( IDS ) Snort Dan Suricata Dalam Mendeteksi Serangan TCP SYN Flood," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 9, pp. 2615–2624, 2018.

Y. Arta, "Implementasi Intrusion Detection System Pada Rule Based System Menggunakan Sniffer Mode Pada Jaringan Lokal," *It J. Res. Dev.*, vol. 2, no. 1, pp. 43–50, 2017, doi: 10.25299/itjrd.2017.vol2(1).979.