ANALISIS KEAMANAN ATAS SERANGAN HEARTBLEED PADA ANDROID YANG DIGUNAKAN UNTUK AKSES LOKAL

Makalah

Program Studi Informatika

Fakultas Komunikasi dan Informatika

Diajukan oleh :

Arifin

Bana Handaga,S.T.,M.T.,P.h.D

PROGRAM STUDI INFORMATIKA

FAKULTAS KOMUNIKASI DAN INFORMATIKA

UNIVERSITAS MUHAMMADIYAH SURAKARTA

JULI 2015

HALAMAN PERSETUJUAN

Makalah dengan judul

ANALISIS KEAMANAN ATAS SERANGAN HEARTBLEED

PADA ANDROID YANG DIGUNAKAN UNTUK AKSES LOKAL

Telah diperiksa, disetujui dan disahkan pada :

Hari : Rabu

Tanggal : 29 juli 2015

Pembimbing

Bana Handaga,S.T.,M.T.,P.h.D

NIK : 793

HALAMAN PENGESAHAN

Publikasi ilmiah dengan judul :

ANALISIS KEAMANAN ATAS SERANGAN HEARTBLEED PADA ANDROID YANG DIGUNAKAN UNTUK AKSES LOKAL

Dipersiapkan dan disusun oleh :

ARIFIN

NIM : L200110083

Telah disetujui pada :

Hari : Rabu

Tanggal : 29 Juli 2015

Pembimbing I

Bana Handaga,S.T.,M.T.,P.h.D

NIK : 793

Publikasi ini telah diterima sebagai salah satu persyaratan untuk memperoleh gelar sarjana

Tanggal 4 Juli 2015

Mengetahui,

Ketua Program Studi Informatika

Dr. Heru Supriyono, M.Eng.

NIK : 970

UNIVERSITAS MUHAMMADIYAH SURAKARTA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
PROGRAM STUDI INFORMATIKA
Jl. A Yani Tromol Pos 1 Pabelan Kartasura Telp. (0271)717417, 719483 Fax (0271) 714448
Surakarta 57102 Indonesia. Web: http://informatika.ums.ac.id. Email: informatika@fki.ums.ac.id

SURAT KETERANGAN LULUS PLAGIASI

/A.3-II.3/INF-FKI/VIII/2015

Assalamu'alaikum Wr. Wb

Biro Skripsi Program Studi Informatika menerangkan bahwa :

Nama	:	ARIFIN
NIM	:	L200110083
Judul	:	ANALISIS KEAMANAN ATAS SERANGAN HEARTBLEED PADA ANDROID YANG DIGUNAKAN UNTUK AKSES LOKAL
Program Studi	:	Informatika
Status	:	**Lulus**

Adalah benar-benar sudah lulus pengecekan plagiasi dari Naskah Publikasi Skripsi, dengan menggunakan aplikasi Turnitin.

Demikian surat keterangan ini dibuat agar dipergunakan sebagaimana mestinya.

Wassalamu'alaikum Wr. Wb

Surakarta, 4 Agustus 2015

Biro Skripsi
Informatika

Adjie Sapoetra, S.Kom

Turnitin Originality Report

ANALISIS KEAMANAN ATAS SERANGAN HEARTBLEED PADA ANDROID YANG DIGUNAKAN UNTUK AKSES INTERNET
by Arifin .

From publikasi september 2015 (publikasi)

Similarity Index	Similarity by Source	
10%	Internet Sources:	4%
	Publications:	0%
	Student Papers:	8%

Processed on 09-Jul-2015 16:58 WIB
ID: 554819437
Word Count: 2759

sources:

1 3% match (student papers from 07-Jul-2015)
Class: publikasi
Assignment:
Paper ID: 554455546

2 1% match (student papers from 25-Nov-2014)
Class: publikasi
Assignment:
Paper ID: 482301347

3 1% match (student papers from 26-Nov-2014)
Class: publikasi
Assignment:
Paper ID: 482841172

4 1% match (student papers from 16-Mar-2015)
Class: publikasi
Assignment:
Paper ID: 516773507

5 1% match (Internet from 17-Feb-2015)
http://blog.skerta.com/?author=1

6 1% match (student papers from 10-Mar-2015)
Class: publikasi
Assignment:
Paper ID: 514615059

7 1% match (Internet from 28-Apr-2015)
http://dblp.dagstuhl.de/db/conf/cloudcom/cloudcom2014.html

8 < 1% match (student papers from 04-Feb-2014)
Class: publikasi maret 2014
Assignment:
Paper ID: 393366363

ANALISIS KEAMANAN ATAS SERANGAN HEARTBLEED PADA ANDROID YANG DIGUNAKAN UNTUK AKSES LOKAL

Arifin, Bana Handaga

Program Studi Informatika, Fakultas Komunikasi dan Informatika

Universitas Muhammadiyah Surakarta

Email : arifin.harusbisa@gmail.com, banahandaga@gmail.com

ABSTRACT

There are kinds of vulnerabities in OpenSSL extentions, one of them is heartbleed. Heartbleed exploit security system by encrypt inputed text such as username and password. Input text attacked by heartbleed script which runing with command prompt or terminal in operating system. Therefore, hackers or attackers can record and exploit the informations.

This Research did by 3 steps, first step by setup and configuration server sysem and client system. Second step by tested heartbleed vulnerability and third step by tested heartbleed using Heartbleed Detector and Heartbleed Scanner.The result said that problems not come from operating system but come from OpenSSL vulnerabilitiess.The problems from system could be overcame by upgrade to the last version OpenSSL 1.0.1i

Keywords: *Android, Client, Heartbleed, Heartbleed Detector, Heartbleed Scanner, Heartbleed Script, Server.*

ABSTRAKSI

Terdapat banyak kerentanan pada ekstensi OpenSSL, salah satunya adalah heartbleed. Heartbleed meretas sistem keamanan dengan mengenkripsi teks yang di inputkan misalnya username dan password. Teks yang diinputkan diserang oleh *skript heartbleed* yang dijalankan menggunakan *command promt* atau *terminal* pada sistem operasi. Sehingga, penyerang dapat merekam dan mengeksploitasi informasi.

Penelitian ini dilakukan dengan 3 langkah pertama dengan mengatur konfigurasi sistem *server* dan *sistem client*. Langkah kedua dengan menguji kerentanan heartbleed, langkah ketiga menguji *heartbleed* menggunakan *Heartbleed detector* dan *heartbleed scanner*. Hasil dari penelitian menunjukkan bahwa permasalahan bukan dari sistem operasi melainkan dari kerentanan OpenSSL. Masalah ini dapat diatasi dengan meng*upgrade* ke versi terbaru yaitu OpenSSL 1.0.1i

Kata kunci : *Android,Client, Heartbleed, Heartbleed Detector, Heartbleed Scanner, Heartbleed Script, Server.*

PENDAHULUAN

Adanya informasi yang menjadikan seorang penulis ingin menganalisis terjadinya kegagalan enkripsi bernama Heartbleed yang telah berhasil membaca salah satu celah keamanan yang memungkinkan pencurian informasi yang sewajarnya dilindungi oleh enkripsi SSL/TLS sebagai enkripsi pengamanan internet. Sistem yang akan digunakan dalam penelitian ini mengunakan *Android* pada akses internet. Akibat dari heartbleed ini, beberapa perusahaan dengan rahasia besar kawatir atas data-data pribadi mereka yang kemungkinan akan dapat diakses oleh kracker yang menggunakan "kunci Digital" untuk dapat mengambil data root seperti *username* dan *password* yang menggunakan OpenSSL.

Dalam hal ini bertujuan untuk menganalisa terjadinya Heartbleed yang menyerang *Android* dan layanan sosial lainnya dimana hampir setiap hari berjuta-juta orang menggunakan internet yang digunakan untuk bersosialisasi, bisnis dan bisa juga sebagai penunjang pekerjaan seperti *Google* yang digunakan banyak orang sebagai tempat mencari informasi, hampir apa saja yang kita inginkan terdapat pada *Google* begitu juga *Gmail* yang biasa kita gunakan untuk sarana informasi pribadi dengan teman, rekan, serta sebagai bahan komunikasi yang bersifat rahasia yang tidak semua orang dapat mengetahuinya, kemudian *facebook* yang hampir semua orang telah menggunakan situs media sosial ini sebagai media komunikasi yang dianggap aman karena *facebook* termasuk media sosial yang berbasis *security*, tapi ternyata disitus yang dilengkapi dengan keamanan seperti enkripsi SSL/TLS sebagai enkripsi pengamanan internet data pribadi kita seperti *username* dan *password* dan masih dapat terlihat oleh pihak-pihak tertentu. Yang dapat disalah gunakan seperti mecuri data pribadi maupun kelompok yang dapat merugikan banyak pihak.

TINJAUAN PUSTAKA

Menurut *Ghafoor*(2014), pada penelitiannya yang berjudul “Analysis of OpenSSL Heartbleed Vulnerability for Embedded Systems”. Perubahan *system embedded*yang banyak digunakan pada jaringan internet seperti perangkat medis yang menggunakan sinar untuk dijadikan data informasi, dimana informasi yang terhubung pada jaringan internet di dunia membutuhkan saluran komunikasi yang aman agar data yang di dapat dari proses *system embedded* menjadi informasi *valid* yang dipastikan oleh keamanan data salah satunya openssl. Openssl adalah standar kamanan yang nyata untuk komunikasi jaringan internet.

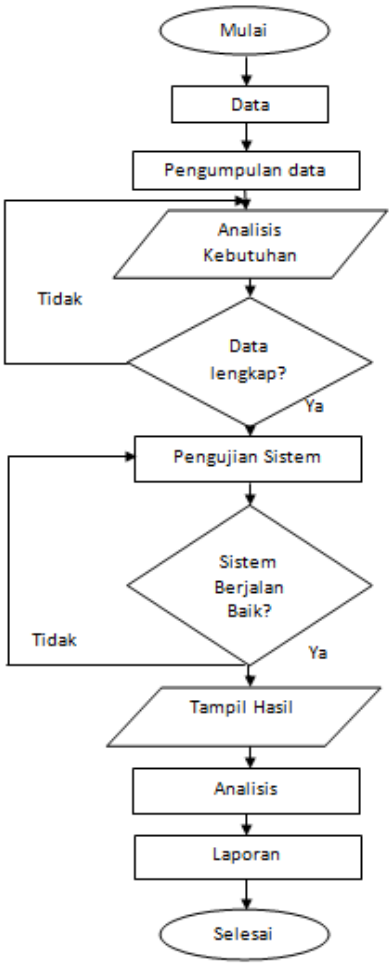
Dalam penelitian ini menjelaskan cek kerentanan CEV-2014-0160 ditemukan kegagalan encripsi pada openssl, temuan kegagalan *enkripsi* pada openssl yaitu pada tanggal 7 Februari 2014, yang menjelaskan kerentanan ini terjadi desebut dengan Bug Heartbleed yang mengakibatkan lebih dari 16% dari total *web server* rentan terhadap heartbleed.

Bug heartbleed dapat menyebabkan kebocoran pada 64KB memori *plaintext* (teks asli) yang memungkinkan berisi kunci keamanan, sertifikat dan data pribadi pengguna. Openssl juga digunakan untuk mengamankan *system embedded* yang tehubung pada jaringan internet. Bug heartbleed memiliki dampak yang lebih besar pada sistem embedded karena beberapa KB atau MB yang tertanam pada memori perangkat dapat bocor di beberapa detik ketika serangan heartbleed sedang berlangsung. Penelitian ini menunjukkan serangan heartbleed serta mengembangkan sistem keamanan untuk menambal kerentanan atas serangan heartbleed. Dan juga mengusulkan update patch RFC-6520 yang digunakan sebagai heartbleed patch.

Menurut *Chonho Lee Sch*(2014). Penelitiannya yang berjudul "A Case Study of Heartbleed Vulnerability". Pada penelitian yang tertulis dalam sebuah *paper*yaitu proses menyelidiki lalu lintas jaringan sebelum dan sesudah kerentanan yang disebut dengan Bug Heartbleed, bug ini menjadi isu publik antara pada bulan Maret dan Mei 2014. Untuk mendeteksi kerentanan dan potensi atas ancaman heartbleed menggunakan sistem berbasis *entropy wavelet.* Metode deteksi perubahan diusulkan dan dibandingkan dengan tiga metode lain : seperti metode berbasis prediksi, metode berbasis *clustering*dan metode berbasis Fourier transform.

METODE

Metode penelitian ini dapat diinformasikanmelalui Gambar 1



Gambar1*Flowchart* Penelitian

Data

Informasi yang didapatkan dari beberapa sumber yang menjelaskan bahwa adanya gegagalan *enkripsi* yang disebut dengan *Bug Heartbleed*. Dalam informasi tersebut menunjukkan salah satu celah keamanan yang memungkinkan *hacker*mencuri informasi yang seharusnya dilindungi oleh data *enkripsi* SSL/TLS sebagai keamanan *internet.*

Akibat dari *Bug Heartbleed* yang memungkinkan *hacker*untuk mengambil data pribadi yang semestinya dilindungi dengan keamanan SSL seperti *username* dan *password*. Dalam kenyataanya data pribadi tersebut masih terlihat dengan menggunakan kunci digital. Adanya isu yang didapatkan, maka timbulah rasa ingin menganalisa terjadinyaproses serangan *heartbleed*,*tools* yang digunakan, hingga rekomendasi penanggulangannya.

Seperti yang telah dilaporkan oleh pihak *google* yang mengatakan bahwa masih jutaan perangkat *android* dengan *versi Android Jelly Bean* 4.1.1 yang telah dirilis pada tahun 2012 yang terdeteksi rentan atau *vulnerable* terhadap *heartbleed*. Seperti kata Michael Shoulov, CEO dan *CO-Founder* dari *Lacoon Mobile Security* mengatakan yaitu untuk memudahkan perangkat dapat terdeteksi rentan terhadap *heartbleed.* begitu juga dijelaskan proses pengambilan data seperti *password*dan informasi sensitif lainnya dapat diekspos dengan cara menunjukkan halaman data yang di tarik dari memori perangkat ke target yang di tampilkan kelayar. (Jordan Robertson, Mei 2014).

Pengumpulan Data.

Pada tahap ini peneliti mengumpulkan data-data yang diperlukan untuk melakukan penelitian, dimana data yang telah dianalisa sebelumnya dalam kebutuhan apa saja yang diperlukan dengan teknik pengumpulan yang sudah dijelaskan.

Analisa data.

Pada tahap ini peneliti menganalisa kebutuhan apa aja yang diperlukan untuk melakukan penelitian ini, baik itu *hardware, software* dan materi apa saja yang berkaitan dengan penelitian ini.

Setup dan Konfigurasi Sistem

Pada tahap ini peneliti melakukan proses yang lebih detail dalam melakukan Setup dan Konfigurasi penelitian. Adapun tahapan yang harus dilakukan sebagai berikut:

1. Sistem Operasi Linux Backbox.
2. Instalasi Xampp.
3. Wifi Portable dari Android.
4. Script Heartbleed.

Pengujian Sistem

Dalam tahap pengujian yang akan lakukan,bertujuan untuk mengetahui bagaimana cara untuk mendeteksi jalannya *system heartbleed* dengan beberapa *tools* yang dibutuhkan antara lain sebagai berikut :

1. Testing Scan Ip dengan Nmap atau Ping alamat web.
2. Testing Heartbleed dengan Heartbleed Script.
3. Hasil dan penentuan Username dan Password.

Dalam pengujian sistem hanya menggunakan wifi lokal dan website lokal.

Analisa.

Pada tahap ini peneliti melakukan analisa dari pengujian yang sudah dilakukan, dengan maksud mencari data-data yang diinginkan sesuai dengan tujuan penelitian.

Penyusunan Laporan.

Pada tahap terakhir, peneliti menyusun laporan dari hasi penelitian dengan data-data yang sudah dilakukan dengan menarik sebuah kesimpulan dari semua kegiatan penelitian.

HASIL DAN PEMBAHASAN

Hasil dari penelitian yang dilakukan sebagai tugas akhir progdi informatika, yang dikerjakan kurang lebih 8 (delapan) bulan adalah dapat mengetahui cara kerja heartbleed yang dimulai dari tools yang digunakan dalam serangan, proses pengambilan host/ip yang digunakan oleh client, sehingga proses kerja heartbleed dapat berjalan sebagai mana yang diharapkan sesuai dengan tujuan. Kemudian dengan adanya tools *heartbleed script* yang disebutkan sebagai alat untuk *testing* serangan *heartbleed*. Disimulasikan dengan bantuan *server* lokal dan jaringan *wifi* lokal yang dibuat untuk menghubungkan antara *smartphone* dan *netbook* yang digunakan.

Untuk mewujudkan hasil yang diharapkan sebagai mana yang menjadi tujuan an ini, yaitu hasil dari tahap *testing heartbleed vulnerable*, hasil tahap*testing scan host*, hasil tahapIdentifikasi *heartbleed script* yang pengambilan data pribadi seperti *username* dan *password*.

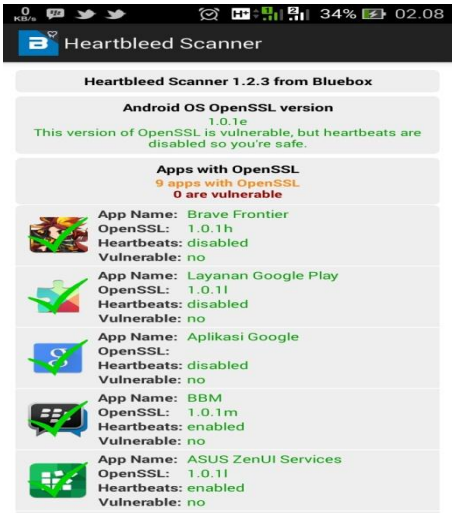
Dari hasil pengujian yang sudah dilakukan dengan melakukan berapa tahap yaitu tahap scanning, Identifikasi dan Record maka dihasilkan data pada tabel 1

Tabel 1 Data yang didapatkan dari hasil analisa sebuah permasalahan dan hasil pengujian secara simulasi.

No	Tahap	Input	Output
1.	Testing	Versi Openssl 1.0.1	Vunerable
2.	Scan Host	Client & Server	IP Adress
3.	Scan Heatbleed	Heartbleed Script	Vulnerable
4	Record	Heartbleed Script	Username & Pasword

Dari tabel 1 dapat dijelaskan bahwa pada tahap *Testing* dengan menggunakan beberapa *tools* yakni *Heartbleed Detector, Heartbleed Scanner*, dan juga *Heartbleed Script* yang gunakan untuk mengetahui bahwa beberapa versi sistem operasi android rentan terhadap heartbleed. Namun setelah tahap testing menggunakan beberapa tools yang telah di sebutkan dapat dijelaskan bahwa memang beberapa versi sistem android diketahui menggunakan openssl yang rentan terhadap *heartbleed*. yaitu Openssl 1.0.1e diketahui *Vulnerable* terhadap heartbleed. Namun juga mendapatkan pengetahuan lebih setelah tahap testing telah selesai dilakukan.

Walaupun versi sistem android dari 4.2 hingga kitkat 4.4 menggunakan Openssl 1.0.1e *vulnerable* dengan heartbleed, dapat dinyatakan kebal dari serangan heartbleed karena dari pihak android telah memperbaiki kebocoran sistem enkripsi yang disebut dengan heartbleed menggunakan patch sistem. yaitu dengan cara mengapgrade seluruh aplikasi yang masih menggunakan openssl 1.0.1e menjadi 1.0.1h atau openssl 1.0.1i. dapat dibuktikan dengan melihat hasil dari *Heartbleed Scanner*yang penulis informasikan dengan gambar 2.

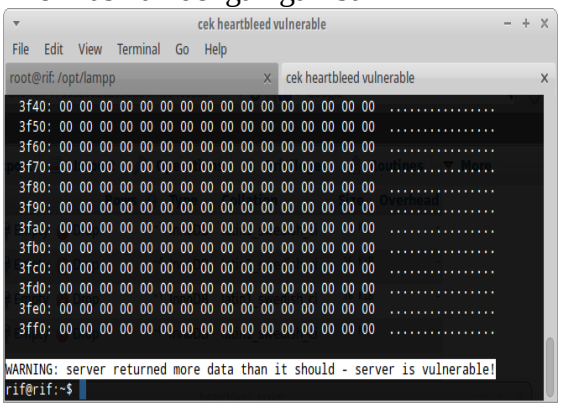


Gambar 2 Hasil Scan Heartbleed Scanner

Dari gambar 2 dapat dijelaskan dengan gamblang yaitu pada sistem operasi android yang menggunakan Openssl 1.0.1e yang dikenal Vulnerable oleh heartbleed ternyata kebal oleh heartbleed karena dari keseluruhan aplikasi telah mengapgrade Opensslnya menjadi Openssl 1.0.1h sampai dengan Openssl 1.0.1m bahwa dari openssl tersebut tidak rentan oleh heartbleed.

Kemudian melanjutkan penelitiannya untuk mengetahui bagaimana proses *heartbleed* menyerang Openssl 1.0.1e, pada tahap ini menggunakan simulasi serangan heartbleed yaitu dimulai dengan tahap Scan Host. Tujuan dari tahap *scan host*yaitu untuk mengetahui bawah adanya hubunga antara client dengan server yang didalamnya mendapatkan hasil proses serangan heartbleed. yaitu dengan mengambil ip server sebagai alamat tujuan serangan.

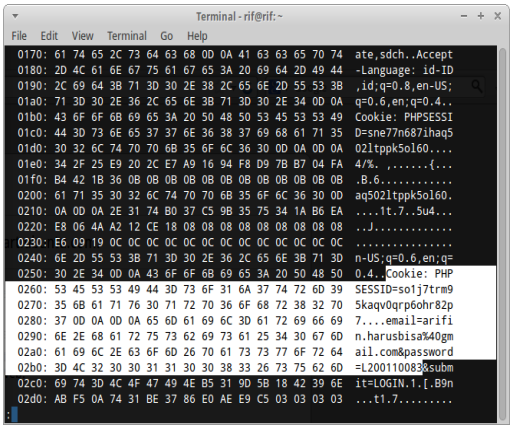
Setelah ip server diperoleh kemudian mulai untuk cek apakah openssl yang digunakan dalam website tersebut Vulnerable dengan heartbleed atau tidak. Dengan menggunakan heartbleed script peneliti dapat menunjukkan bahwa openssl yang digunakan menggunakan openssl yang Vulnerabled dengan Heartbleed di informasikan dengan gambar



Gambar 3 Versi Openssl

Dengan gambar 3 dapat di informasikan bahwa openssl yang gunakan untuk simulasi serangan heartbleed menggunakan versi *openssl* yang *vulnerable* dengan *heartbleed*.

Kemudia setelah diketahui Openssl yang digunakan Vulnerable maka dapat melanjutkan penelitianya yaitu dengan tahap Record, yaitu menggabil informasi pribadi client seperti *Username*dan *Password* dengan menggunakan *Heartbleed Script*. Dengan pengujian beberapa kali percobaan maka didapatkan hasil yaitu menangkap informasi penting seperti *username* dan *password* yang *Clientinput*-kan, diinformasikan pada gambar 4.



Gambar 4 Hasil Record Username Password

Dengan gambart 4 dapat dijelaskan bahwa dalam hasil uji menggunakan heartbleed script mendapatkan data yang dikirm oleh server yaitu berupa aktifitas client yang sedang mengakses kepada server berupa login kedalam website. Data yang didapatkan berupa *Username* dan *Password* yang seharrusnya menjadi data privasi seorang Client.

Interpretasi Hasil Penelitian

Dari hasil penelitian maka dapat memberikan beberapa interpretasi hasil penelitian yang dilakukan melalu pengujian secara langsung dan juga simulasi. Untuk pengujian langsung yaitu dapat menginformasikan bahwa beberapa versi android masih rentan terhadap serangan heartbleed, karena masih menggunakan Openssl 1.0.1e yang ternyata dari hasil testing meggunakan beberapa tools seperti heartbleed detector, heartbleed scanner dan heartbleed script bahwa Openssl tersebut Bulnerable dengan

heartbleed. Sehingga jika aplikasi yang terdapat pada android yang menggunakan Openssl 1.0.1e masih menggunakan versi Openssl 1.0.1e segera mengapgrade dengan versi openssl yang lebih dari 1.0.1e yaitu seperti 1.0.1h atau 1.0.1i yang diketahui tidak vulenerable dengan seragan heartbleed.

Dan yang menjadi hasil utama dari penelitian ini ialah bukan sistem Operasi android yang menjadi target serangan heartbleed namun dari kelemahan Openssl yang digunakan oleh beberapa sistem android yang mengakibatkan kerentan terhadap sestem android.

Kemudian pada pengujian secara simulasi dapat diinformasikan bahwa cara kerja heartbleed yaitu mengambil beberapa aktifitas client yang terhubunga dengan server. Dan aktifitas tersebut dapat termonitoring oleh tools yang sebut heartbleed script, dari *heartbleed script*yang gunakan maka dapat mendapatkan sebuah aktifitas seorang *client* yaitu seperti saat *client* sedang *login* kesebuah *website* maka *heartbleed script* akan mengambil informasi yang *clientinput*-kan pada halaman *login*berupa paket data seperti Cookies dan SESSID dan juga *Username*dan *Password.*

Ketika *Username* dan *Password* telah diketahui orang lain, maka sudah dapat dipastikan data yang ada dalam website tersebut tidak lagi aman. Jika sudah terjadi, maka sebaiknya mengganti *Username*, *Password* dan yang terpenting meng-*upgrade* Openssl yang digunakan dalam website tersebut dengan Openssl yang tidak *Vulnerable* dengan *heartleed.* Jika hanya mengganti *Username* dan *Password* saja kemungkinan besar masih dapat terkena dampak heartbleed.

KESIMPULAN

Berdasarkan dari hasil analisa data dan beberapa percobaan dengan melakukan pengujian secara langsung dan pengujian secara simulasi, maka dapat diambil beberapa kesimpulan yaitu sebagai berikut :

1. Setelah dilakukan pengujian secara langsung terhadap beberapa sistem Operasi Android dengan menggunakan *tools* seperti Heartbleed Detector dan Heartbleed Scanner maka dihasilkan sebuah data yang menginformasikan bahwa yang menjadi permasalahan yakni bukan dari sistem Androidnya melainkan Openssl yang digunakan pada sistem Operasi Android.
2. Kemudian peneliti juga melakukan pengujian secara simulasi bahwa bagaimana proses Heartbleed mengambil informasi penting yang sedang dilakukan oleh*client* dimana informasi penting tersebut berupa data privasi *client* seperti Username dan Password milik *Client* yang digunakan untuk Login kesebuah *website*.

Saran

Dengan adanya permasalahan yang terjadi pada kebocoran data pribadi yang biasa disebut dengan heartbleed maka perlu adanya perhatian khusus yakni :

1. Jika mengalami beberapa gejala seperti data dalam *website* hilang, atau juga adanya perubahan dalam data maka dapat dimungkin kan itu terjadinya heartbleed dan yang harus dilakukan yaitu mengganti *Username* dan *Password* karena dapat disimpulkan ketika *username* dan *password* tidak bocor atau hanya *client* sendri yang mengetahui maka data akan dianggap aman dan tidak akan berubah sebelum pemiliknya yang merubahnya.
2. Jika dalam menggunakan sebuah smartphone yang berbasis android khususnya, dan yang masih menggunakan aplikasi dengan Openssl versi 1.0.1c dan Openssl versi 1.0.1e maka segeramengapgrade ke-Openssl versi yang tidak lagi Vulnerable dengan heartbleed seperti Openssl versi 1.0.1h atau 1.0.1i dan untuk mengetahui apakah sistem yang digunakan Vunerable atau tidak maka dari hasil penelitian ini merekomendarikan menggunakan *tools* Heartbleed Detector untuk mengetahui Versi Openssl Pada *device*, dan Heartbleed Scanner yang digunakan untuk mengetahui versi Openssl pada Aplikasi yang terinstal pada Smartphone yang berbasis Android khususnya.
3. Untuk penelitian selanjutya dapat lebih mengembangkan gejala-gejala apa saja yang dialami atas serangan heartbleed.

DAFTAR PUSTAKA

Ghafoor, I. dkk. (2014).*"Analysis of OpenSSL Heartbleed vulnerability for embedded systems"*. IEEE, Nat. Univ. of Sci. & Technol. (NUST), Islamabad, Pakistan, pp 314 – 319.

Jared Stafford (2014).*Quick and dirty demonstration of CVE-2014-0160*.jspenguin@jspenguin.org.

Lee, Chonho. dkk. (2014).*"A Wavelet Entropy-Based Change Point Detection on Network Traffic: A Case Study of Heartbleed Vulnerability "*. Cloud Computing Technology and Science (CloudCom), IEEE 6th International Conference. pp 995 - 1000.

BIODATA PENULIS

Nama	: Arifin
NIM	: L200110083
Tempat lahir	: Kab. Temanggung
Tanggal Lahir	: 09Mei 1992
Jenis Kelamin	: Laki-laki
Agama	: Islam
Pendidikan	: S1
Jurusan/Fakultas	: Informatika / Komunikasi dan Infromatika
Perguruan Tinggi	: Universitas Muhammadiyah Surakarta
Alamat	: Dusun Sido Makmur RT 011 RW 004 Desa Jairan Jaya Kec. Sungai Melayu Rayak, Kab. Ketapang, Kalimantan Barat
No. Hp	: 085246818508
Email	: arifin.harusbisa@gmail.com