Investigasi *Email Spoofing* dengan Metode *Digital Forensics Research Workshop* (DFRWS)

Andri Lesmana Suryana[#1], R. Reza El Akbar[#2], Nur Widiyasono[#3]

[#]*Teknik Informatika, Universitas Siliwangi*
Jl. Siliwangi No. 24, Kota Tasikmalaya

[1]andri.l@student.unsil.ac.id

[2]reza@unsil.ac.id

[3]nur.widiyasono@unsil.ac.id

***Abstrak*—Email spoofing merupakan kegiatan melakukan manipulasi data pada header email. Serangan yang paling terkenal dari email spoofing adalah serangan phishing, Tujuan dilakukan penelitian ini adalah untuk memberi wawasan tentang cara kerja melakukan pengiriman email spoofing dan mampu melakukan identifikasi email spoofing dengan melakukan analsis pada header email yang diterima. Metodologi yang digunakan pada penelitian ini adalah DFRWS (Digital Forensics Research Workshop), karena setiap langkah yang dilakukan dapat memberikan penjelasan yang lengkap. Hasil dari penelitian ini adalah email spoofing dapat dikirimkan dengan memanfaatkan layanan web hosting yang menyediakan layanan untuk pengiriman email dengan menggunakan bahasa pemrograman PHP dan hasil selanjutnya adalah mengetahui perbedaan antara email spoofing dan email asli, perbedaan tersebut akan diketahui dengan jelas ketika membuka header email rinci.**

***Kata kunci* : DFRWS, Email, Investigasi , Phishing, Spoofing**

I. PENDAHULUAN

Email spoofing dianggap sebagai tindakan membahayakan, karena melakukan manipulasi data pada *header email* untuk menyamar sebagai orang atau organisasi yang sah, contohnya seperti melakukan pengiriman *email* dengan nama pengirim seolah dari administrator suatu organisasi. Pengirim email spoofing menyerang dengan berbagai macam isi pesan untuk membuat percaya korban yang menerima email tersebut.

Serangan yang paling terkenal dari *email spoofing* adalah serangan *phishing*. Para penyerang dalam kategori ini biasanya tertarik pada informasi yang bersifat rahasia yang dimiliki oleh korban. Salah satu contoh dari *email phishing* adalah dengan melakukan penyamaran sebagai email resmi dari bank [1].

Hasil dari laporan yang dipaparkan oleh [2], *Email Phishing* memang mengalami penurunan pada bulan sepetember 2016, namun penurunan tidak terlalu signifikan dari bulan agustus 2016. Penurunan tingkat aktifitas *email phishing* yang signifikan terjadi pada bulan januari, bulan maret dan bulan Juli 2016, namun setiap bulan setelah penurunan tingkat *email phishing* yang signifikan, justru terjadi pula peningkatan yang signifikan pada bulan selanjutnya.

Gambar. 1 Aktifitas Email Phishing

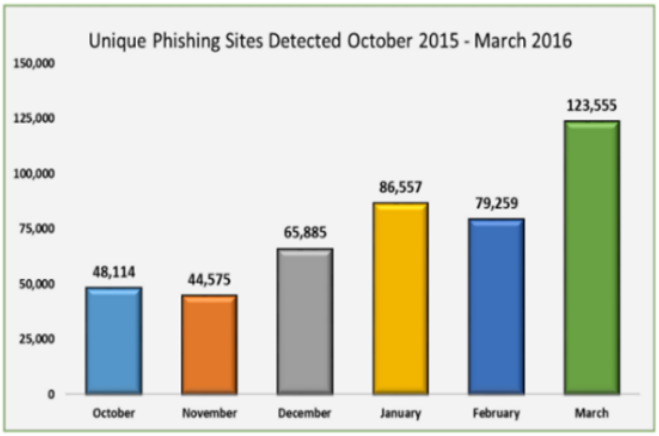
(Sumber: Symantec, Security Response Publications)

Gambar 1 menunjukkan aktifitas serangan *email phisihing* dari bulan oktober 2015 sampai bulan september 2016

Hasil dari laporan yang dipaparkan oleh [3], "jumlah situs *phishing* berjumlah 289.371. Jumlah situs *phishing* diamati setiap bulan terus meningkat dari bulan oktober 2015 ada 48.114 situs *phishing* terdeteksi. Bulan maret 2016 ada 123.555 situs *phishing* yang terdeteksi, situs *phishing* meningkat 250% selama enam bulan. Peningkatan terjadi pada bulan desember tahun 2015, karena biasanya ada serentetan *spamming* dan penipuan online selama musim belanja liburan. Hasil dari laporan yang dipaparkan oleh [3] menyinggung pengiriman *email spamming* sebagai awal dari serangan halaman *web phishing*. Email Spamming biasanya dikirimkan menggunakan teknik *email spoofing* dengan jenis serangan berupa *email phishing*, karena melakukan pengiriman email dengan tujuan untuk mengunjungi halaman *web phishing* milik penyerang.

Gambar 2 menunjukkan aktifitas serangan phishing pada kuartal akhir tahun 2015 sampai dengan kuartal awal pada tahun 2016.

ISSN 2460-0741



Gambar. 2 Aktifitas *Phishing* 2015- 2016

(*Sumber: Phishing Activity Trends Report, 2016*)

II. KAJIAN PUSTAKA

A. Penelitian Sebelumnya

Penelitian *email spoofing* juga dilakukan oleh [1], hasil dari penelitainnya adalah " Serangan *email spoofing* dapat digunakan sebagai awal dari serangan *phishing* untuk mendapatkan informasi dari pengguna (korban)". Pembedaan penelitiannya adalah penelitian ini melakukan identifikasi *email spoofing* dimulai dari pemahaman tentang cara kerja *email spoofing*, sedangkan penelitian yang dilakukan oleh [1] adalah pengenalan dan pemahaman tentang *email spoofing* tanpa melakukan identifikasi secara rinci pada *email spoofing* seperti melakukan analisis *header email* rinci.

Penelitian sebelumnya yang mengambil tema yang sama yaitu *email spoofing* dilakukan oleh [4], hasil dari penelitiannya adalah "Pemahaman tentang berbagai jenis *email* akan meningkatkan pengguna supaya lebih sadar tentang pola pada berbagai jenis *email*". Pembeda dalam penelitiannya adalah penelitian oleh [4] memberikan pemaparan tentang berbagai jenis *email* tanpa melakukan analisis pada *header email* sedangkan pada penelitian ini melakukan analisis pada *header email* dan tanpa menjelaskan kategori email lain selain *email spoofing*.

Penelitian *email spoofing* juga dilakukan oleh [5], hasil dari penelitiannya adalah "Analisis dilakukan pada isi pesan *email* untuk menentukan legitimasinya". Pembeda penelitiannya adalah penelitian oleh [5] melakukan analisis *header email* namun tanpa mengetahui asal usul email dikirimkan dan tidak membahas cara kerja *email spoofing*, hal itu memungkinkan analisis *email spoofing* tidak dapat dengan mudah dipahami oleh semua orang, sedangkan pada penelitian ini dilakukan simulasi pengiriman *email spoofing* dengan tujuan mempermudah pemahaman tentang *email spoofing*.

B. *Email (Electronic Mail)*

Electronic Mail atau dapat disebut dengan *email*, merupakan salah satu layanan internet yang sangat populer dan paling banyak digunakan oleh orang banyak, baik di lingkungan organisasi maupun perusahaan. Secara harfiah email dapat di definisikan sebagai metode pengiriman, penerimaan, dan penyimpanan pesan melalui sistem komunikasi elektronik berupa internet. Definisi tersebut menjelaskan bahwa email mulai dari ditulis, dikirim, diterima sampai dengan dibaca dilakukan secara elektronis[6].

C. Penyalahgunaan *Email*

Penyalahgunaan dalam penggunaan *email* yang sering ditemukan salah satunya bertujuan mencuri informasi pribadi dari pengguna (korban) atau mendapatkan akses tidak sah ke rekening korban. Banyak serangan memiliki efek buruk pada pengguna (korban) seperti kerugian finansial[4].

Berbagai penggunaan negatif pada *email* adalah sebagai berikut[4]:

a. Spam

Spam adalah *mail* yang tidak diinginkan, *email spam* dikirim kepada *inbox mail* seseorang dan pesan tersebut tidak ada gunanya untuk penerima. *Spam* dikirim pada jaringan untuk meningkatkan konsumsi sumber daya, dengan kata lain untuk meningkatkan lalu lintas jaringan.

a. Penipuan (*Scam*)

Penipuan (*Scam*) adalah kategori *email* yang dimaksudkan untuk memikat seseorang ke dalam transaksi yang palsu dan benar-benar penipuan. *Email Scam* terkadang digabungkan dengan *phishing*.

b. Penyebaran *URL Phishing*

Situs *phishing* adalah situs palsu, yang hampir identik dengan beberapa situs-situs jaringan sosial, situs *email* atau situs *online banking*, yang memerlukan pengguna untuk *login*.

c. *Email spoofing*

Email Spoofing adalah teknik yang biasa digunakan oleh *spammer* dan *scammer* untuk menyembunyikan asal usul pesan email. *Email spoofing* dapat mengubah sifat tertentu dari *email*, seperti pada bidang "From" yang merupakan informasi pengirim email. Pengirim *email spoofing* ini dapat membuat *email* tampak dari seseorang selain pengirim sebenarnya.

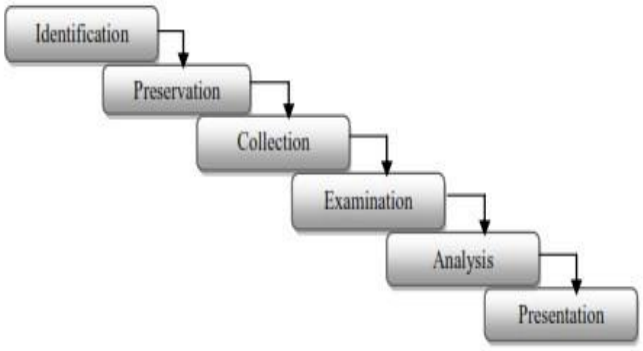
D. *Phishing*

Phishing adalah bentuk pencurian identitas *online* yang bertujuan untuk mencuri informasi sensitif seperti *password* dan informasi kartu kredit. Serangan *phishing* menggunakan kombinasi teknik *social engineering* dan teknik *spoofing* untuk membujuk pengguna agar memberikan informasi sensitif yang dapat digunakan untuk membuat keuntungan, contohnya keuntungan finansial. *Pisher* biasanya membajak sebuah halaman *web* dari bank, kemudian mengirim *email* kepada korban untuk mengelabui korbannya supaya mengunjungi situs berbahaya dengan tujuan untuk mengumpulkan informasi rekening bank dan nomor kartu milik korban[7].

ISSN 2460-0741

III. METODOLOGI PENELITIAN

Metodologi yang digunakan dalam penelitian ini adalah *DFRWS (Digital Forensics Research Workshop)*, metode *DFRWS* membantu mendapatkan bukti dan mekanisme terpusat untuk merekam informasi yang dikumpulkan [8].



Gambar. 3 Metodologi Penelitian *DFRWS* (*Digital Forensics Research Workshop*)

(*Sumber: Patil, 2015*)

Gambar 3 menunjukkan tahapan yang dilakukan berdasarkan metode yang digunakan yaitu *DFRWS* (*Digital Forensics Research Workshop*). Pemaparannya adalah sebagai berikut:

A. Identifikasi (*Identification*)

Identifikasi dilakukan untuk melakukan penentuan kebutuhan yang diperlukan pada penyelidikan dan pencarian bukti.

B. Pemeliharaan (*Preservation*)

pemeliharaan dilakukanan untuk menjaga bukti digital agar memastikan keaslian bukti dan membantah klaim bukti telah dilakukan sabotase.

C. Pengumpulan (*Collection*)

Pengumpulan merupakan tahap untuk melakukan identifikasi bagian tertentu dari bukti digital dan melakukan identifikasi sumber data

D. Pemeriksaan (*Examination*)

Pemeriksaan dilakukan untuk menentukan filterisasi data pada bagian tertentu dari sumber data, filterisasi data dilakukan dengan melakukan perubahan bentuk data namun tidak melakukan perubahan pada isi data karena keaslian data merupakan hal yang sangat penting.

E. Analisis (*Analysis*)

Analisis merupakan tahap untuk melakukan penentuan tentang dimana data tersebut dihasilkan, oleh siapa data tersebut dihasilkan, bagaimana data tersebut dihasilkan dan kenapa data tersebut dihasilkan

F. Presentasi (*Presentation*)

Presentasi dilakukan dengan menyajikan informasi yang dihasilkan dari tahap analisis.

IV. HASIL DAN PEMBAHASAN

Berdasarkan pada metodologi penelitian yang digunakan, maka tahapan yang dilakukan untuk melakukan *investigasi email spoofing* adalah sebagai berikut:

A. Tahap Identifikasi

Tahap identifikasi dilakukan dengan mencari informasi dari kasus yang terjadi sebelumnya untuk dijadikan sebagai rujukan tentang pemahaman pada barang bukti yang sedang dilakukan pencarian. Tahap identifikasi ini juga melakukan identifikasi tentang cara kerja email spoofing dapat dipergunakan. Simulasi pengiriman email spoofing dilakukan untuk mendapatkan bukti digital, karena dengan mendapatkan barang bukti yang dicari, maka tahap identifikasi dapat dilanjutkan pada tahap pemeliharaan sesuai dengan kerangka kerja pada metodologi DFRWS.

TABEL I.

LAPORAN SERANGAN EMAIL SPOOFING

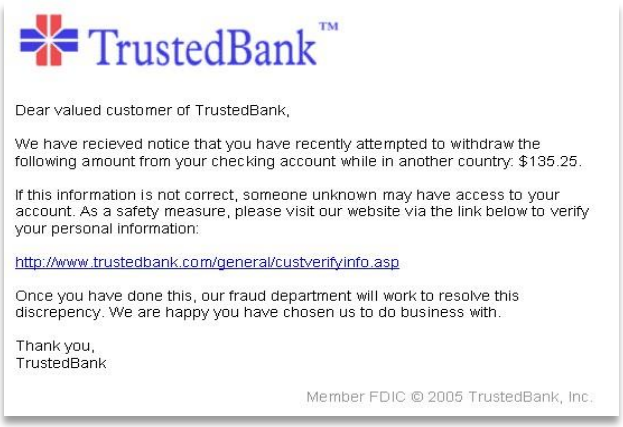
Company	Email Content
Visa	*"Attention! Several VISA Credit Card bases have been LOST!"*
NCUA	*"*** WARNING: Security Issues ***"*
LaSalle Bank	*"IMPORTANT - Account Verification"*
PayPal	*"Unauthorized Account Access"*
PayPal	*"Update Your Account"*
SouthTrust	*"Important Security Issue!!!"*
Marshall & Ilsley Bank	*"Security Update!"*
Citizens Bank	*"Citizens Bank Instant 5 USD reward survey"*
Ameritrade	*"Ameritrade Online Application"*
Regions Bank	*"Notification about your Regions online account"*
Bank Of America	*"Online Banking Alert (Change of Email Address)"*
eBay	*"eBay Verify Accounts"*
Associated Bank	*"Online Alert: online account is blocked"*
Huntington Bank	*"Huntington Bank Email Verification"*

Tabel I memaparkan tentang laporan email spoofing yang terjadi sebelumnnya, data diambil dari [9].

Bukti digital yang didapatkan saat melakukan persiapan untuk melakukan analisis email spoofing, berupa tampilan *email spoofing* yang menjadi kasus sebelumnya. [1] memaparkan penjelasan untuk gambar 4, "Sebuah contoh dari *email spoofing*, menyamar sebagai email resmi dari Bank.

ISSN 2460-0741

Pengirim mencoba untuk mengelabui penerima untuk mengungkapkan informasi rahasia oleh "konfirmasi" di *website phisher*. Catat, bahwa meskipun URL dari halaman *web* bank tampaknya sah, sebenarnya link ke halaman *web phishing*. *Phisher* ditujukan untuk memperoleh informasi rahasia mengenai pengguna. Email tersebut membawa pengguna ke *URL* yang merupakan situs palsu yang diselenggarakan oleh penyerang dan berpura-pura menjadi orang asli untuk mendapatkan beberapa informasi pribadi.

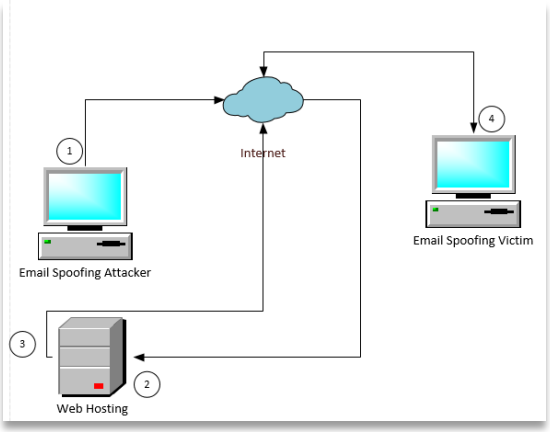


Gambar. 4 Tampilan *email spoofing* pada kasus sebelumnya

(*Sumber: Kumar 2010*)

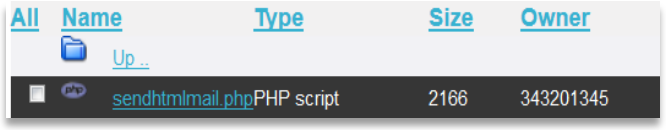
Gambar 4 menunjukkan *email spoofing* yang ditemukan pada penelitian sebelumnya.

Identifikasi tentang cara kerja *email spoofing* dilakukan dengan melakukan simulasi penyerangan menggunakan teknik pengiriman *email spoofing* memanfaatkan fitur yang disediakan oleh bahasa pemrograman *PHP*, Pengunggahan *script php* dilakukan untuk melaksanakan eksekusi pengiriman *email* dengan memanfaatkan layanan *web hosting* yang menyediakan fasilitas pengiriman *email* dengan menggunakan bahasa pemrograman *PHP*.



Gambar. 5 Alur Simulasi Penyerangan email spoofing

Merujuk pada gambar 5, gambar tersebut merupakan alur simulasi penyerangan menggunakan teknik email spoofing dengan memanfaatkan layanan *web hosting* sebagai *mail-server* pengirim email.



Gambar. 6 *Script PHP* untuk *email spoofing* terunggah pada *web hosting*

Merujuk pada gambar 6, gambar tersebut menjelaskan bahwa *script* dengan bahasa pemrograman *PHP* untuk pengiriman *email spoofing* sudah terunggah pada layanan *web hosting* yang menyediakan fasilitas pengiriman *email* menggunakan bahasa pemrograman *PHP*.

Gambar. 7 Pengiriman *Email Spoofing*

Merujuk pada gambar 7. gambar tersebut menunjukkan *email spoofing* telah siap untuk dikirimkan kepada korban, isi *email* yang dikirimkan merupakan *email* dengan konten *HTML* dan telah di selipkan sebuah tautan (*link*) menuju ke halaman *web phishing* yang bertindak sebagai serangan kedua

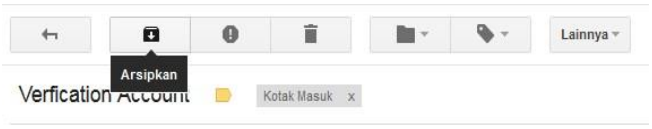
Gambar. 8 Email Spoofing ditemukan.

ISSN 2460-0741

Merujuk pada gambar 8, gambar tersebut menunjukkan bahwa barang bukti digital berupa sebuah penyalahgunaan email dengan kategori *email spoofing* ditemukan pada kotak masuk *email*.

B. Tahap Pemeliharaan

Tahap yang dilakukan adalah melakukan pemerikasaan email pada kotak masuk *email* dan kotak masuk *email spam*, kemudian melakukan pengarsipan *email* untuk menjaga dan memelihara barang bukti yang didapat.



Gambar. 9 pengarsipan barang bukti berupa email spoofing

Merujuk pada gambar 9, gambar tersebut menampilkan bahwa *email spoofing* tersebut dipindahkan pada arsip *email* yang disediakan oleh layanan penyedia *email*. Pengarsipan *email* dilakukan untuk melakukan penjagaan dan pemeliharaan pada barang bukti digital yang didapatkan.

C. Tahap Pengumpulan

Tahap yang dilakukan adalah membuka bagian header email untuk memperkuat alasan tentang mengapa email tersebut dianggap sebagai email spoofing.

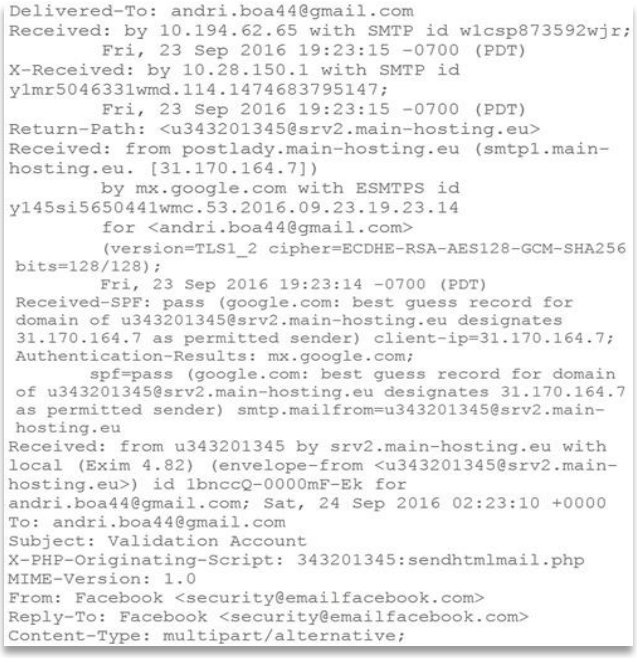
Gambar. 10 Penentuan bagian tertentu pada bukti digital

Merujuk pada gambar 10, Gambar tersebut menjelaskan bahwa adanya kejanggalan dari pesan email. Alamat email dikirim oleh facebook namun melalui srv2.main-hosting.eu. Pengumpulan bagian tertentu dari bukti digital adalah dengan membuka header email yang ditampilkan secara rinci.

Merujuk pada gambar 11, gambar tersebut menampilkan header email rinci, data tersebut merupakan data yang sangat diperlukan untuk tahap-tahap selanjutnya.

D. Tahap Pemeriksaan

Tahap yang dilakukan adalah melakukan perubahan bentuk data tanpa merubah isi data. Data yang dihasilkan dari tahap pengumpulan dilakukan perubahan bentuk data menjadi sebuah tabel dan menentukan bagian terpenting dari data.



Gambar. 11 Header Email Rinci

TABEL II

EMAIL HEADER ANALISIS

Return-Path	<u343201345@srv2.main-hosting.eu>
Received-SPF	pass (google.com: best guess record for domain of u343201345@srv2.main-hosting.eu designates 31.170.164.6 as permitted sender) client-ip=31.170.164.6;
Received	from srv2.main-hosting.eu (unknown [31.170.164.17]) by postlady.main-hosting.eu ([Hostinger Sendmail System]) with ESMTP id C9DE480C6E for <andri.boa44@gmail.com>; Thu, 22 Sep 2016 05:27:18 +0100 (BST)
X-PHP-Originating-Script	343201345:sendhtmlmail.php
From	Facebook <security@emailfacebook.com>
Reply-To	Facebook <security@emailfacebook.com>
Sender	<u343201345@srv2.main-hosting.eu>
Date	Thu, 22 Sep 2016 04:27:18 +0000

Merujuk pada tabel II, tabel tersebut merupakan perubahan bentuk data tanpa mengubah isi data yang dikumpulkan pada tahap pengumpulan.

E. Tahap Analisis

Tahap yang dilakukan adalah melakukan analisis dari data yang dihasilkan oleh tahap pemeriksaan. Proses analisis melakukan pencarian informasi penting dari hasil pemeriksaan, seperti dimana email tersebut dihasilkan, siapa yang menghasilkan *email* tersebut, bagaimana email tersebut dihasikan dan kenapa *email* tersebut dihasilkan.

Merujuk pada tabel 2, tabel tersebut menjelaskan *email* tidak dikirimkan dari orang ataupun perusahaan sesungguhnya pada bagian sender terlihat jelas bahwa salah satu pengguna *web hosting* dengan *ID* pengguna "u343201345" yang

ISSN 2460-0741

mengirimkan *email* dan email tersebut dikirim dengan meggunakan bahasa pemrograman *PHP*, bukti pengiriman email dilakukan dengan menggunakan bahasa pemrograman *PHP* terdapat pada bagian "X-PHP-Originating-Script" disana terdapat nama file yang di unggah ke *web hosting* yaitu 'sendhtmlmail.php'.

Bagian "Received-SPF" menjelaskan email diizinkan masuk SPF record, karena nama domain "srv2.main-hosting.eu" sudah terdaftar pada SPF record di *mail-server* gmail, jika *mail-server* yang mengirimkan *email* tidak terdaftar pada SPF record maka email tidak akan sampai pada kotak masuk email penerimanya

F. Tahap Presentasi

Tahap yang dilakukan adalah melakuan penyajian dari hasil analisis pada *header email spoofing* dan kemudian membandingkan dengan email yang asli, sehingga memberikan penjelasan tentang kesimpulan.

TABEL III

PERBANDINGAN ANTARA EMAIL SPOOFING DAN EMAIL ASLI

	Email Spoofing	Email Asli
Return-Path	<u343201345@srv2.main-hosting.eu>	<password+zj4o==_4jccy@facebookmail.com>
Received-SPF	pass (google.com: best guess record for domain of u343201345@srv2.main-hosting.eu designates 31.170.164.6 as permitted sender) client-ip=31.170.164.6;	pass (google.com: domain of password+zj4o==_4jccy@facebookmail.com designates 66.220.144.146 as permitted sender) client-ip=66.220.144.146;
X-PHP-Originating-Script	343201345:sendhtmlmail.php	-
From	Facebook <security@emailfacebook.com>	Facebook <password+zj4o==_4jccy@facebookmail.com>
Sender	<u343201345@srv2.main-hosting.eu>	-
Received	from srv2.main-hosting.eu (unknown [31.170.164.17]) by postlady.main-hosting.eu ([Hostinger Sendmail System]) with ESMTP id C9DE480C6E for <andri.boa44@gmail.com>; Thu, 22 Sep 2016 05:27:18 +0100 (BST)	from facebook.com (Bmemxis1Iv9d8Ck1S1XRY2R2jLIjxx2+SHxWhUc/GJ4KpB30OMPbgaiu3/hpW2Gu 10.103.99.65) by facebook.com with Thrift id 306851a2808311e68ec50002c9ae8cac-151fba50; Wed, 21 Sep 2016 22:12:42 -0700

Merujuk pada tabel III, data pada tabel tersebut sepenuhnya berbeda antara pengirim *email spoofing* dan pengirim *email* asli. *Email* asli selalu memberikan informasi yang sah, seperti *server email* yang digunakan akan selalu sama dengan nama domain yang ada pada alamat *email*, sedangkan pada *email spoofing* tidak akan memberikan informasi yang sah, seperti adanya perbedaan antara server email yang digunakan dengan nama domain pada alamat email pengirim.

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan hasil penelitian yang dilakukan mengenai analisis *email spoofing*, maka dapat ditarik dua kesimpulan sebagai berikut:

1) *Email spoofing* dapat dikirimkan dengan memanfaatkan layanan *web hosting* yang menyediakan fasilitas pengiriman *email* menggunakan bahasa pemrograman *PHP*. *Email spoofing* dapat dikirimkan pada semua layanan *email* yang dominan digunakan, seperti gmail, yahoo mail, outlook atau hotmail dan mail.com.
2) Identifikasi *email spoofing* dapat dilakukan dengan melakukan analisis pada pesan yang diterima dan mencari kejanggalan dari pesan yang mencurigakan, seperti kejanggalan tautan (*link*) yang akan mengantarkan pada halaman *web phishing*. Identifikasi *email spoofing* harus dilakukan dengan melihat header email yang rinci pada email yang diterima, karena jika melakukan identifikasi hanya dari pesan tidak akan cukup untuk meyakinkan bahwa email tersebut merupakan *email spoofing*.

B. Saran

Berdasarkan dari kesimpulan yang didapatkan maka dapat diajukan beberapa saran untuk mencegah penerimaan *email spoofing*, menangani penerimaan *email spoofing* dan saran untuk penelitian selanjutnya tentang *email spoofing* adalah sebagai berikut:

1) Pengguna *email* seharusnya tidak melakukan publikasi alamat email, seperti pada media sosial, melakukan *subscribe* pada halaman *web* yang menyediakan fasilitas *subscribe* dan lain sebagainya yang merupakan tindakan melakukan publikasi alamat email, karena dengan banyak melakukan publikasi email maka kemungkinan mendapatkan *email spoofing* akan semakin besar.
2) Pengguna layanan *email* yang menerima *email spoofing*, diharapkan untuk melakukan pemblokiran pada alamat *email* yang mencurigakan dan melaporkan *email* yang diterima sebagai *email phishing* kepada layanan *email* yang digunakan.
3) Ketelitian saat menerima *email* mencurigakan pada kotak masuk ataupun kotak masuk *email* jenis *spam* sangat diperlukan, karena akan mencegah pengguna layanan *email* untuk masuk pada alur penyerangan yang diinginkan oleh penyerang.

ISSN 2460-0741

4) Serangan dari *email spoofing* tidak hanya digunakan sebagai pengelabuhan korban agar mengunjungi halaman *web phishing*, akan tetapi *funciton mail* pada bahasa pemrograman *PHP* memungkinkan pengirim untuk mengirin berkas (*file*). Penelitian selanjutnya dapat melakukan identifikasi *email spoofing* yang melampirkan berkas *(file*).

REFERENSI

[1]. Kumar, Rajinder. "*Email Spoofing*". International Journal of Computer Applications, vol. 5, no. 1, 0975 – 8887. 2010.

[2]. Symantec. "*Security Response Publications*". [online], 2016 https://www.symantec.com/security_response/publications/monthlythreatreport.jsp#Phishing, diakses pada tanggal 30 Oktober 2016).

[3]. APWG. 2016. "*Phishing Activity Trends Report, 1st Quarter* 2016". https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf, diakses pada tanggal 22 september 2016.

[4]. Ojha, Gaurav & Gaurav Kumar Tak. "*Novel Approach Against E-Mail Attacks Derived from User-Awareness Based Techniques*". International Journal of Information Technology Convergence and Services, Vol.2, No.4. 2012.

[5]. Banday, Tariq M. "*Analysing E-Mail Headers for Forensic Investigation*". Journal of Digital Forensics, Security and Law, Vol. 6, No. 2, Article 5. 2011.

[6]. Kakunsi, Olivia. "Penipuan Penawaran Pekerjaan Melalui *E-Mail*". Lex Crimen, Vol.1, No.2. 2012.

[7]. Banu, M.N., & Banu, Munawara S. "*A Comprehensive Study of Phishing Attacks*". International Journal of Computer Science and Information Technologies, Vol. 4, no. 6, 783-786. 2013.

[8]. Tanner, April & David Dampier, "Concept Mapping for Digital Forensic Investigations". Advances In Digital Forensics, vol 5. 2014.

[9]. Joshi, Nivedita. "*Counter-Measures to Prevent Spoof E-Mail Tracking*". International Journal of Advanced Technology & Engineering Research. 2014.

ISSN 2460-0741