Prosiding
Seminar Nasional Sains Antariksa
Homepage:http//www.lapan.go.id

KAJIAN *VULNERABILITY SPOOFING* PADA SISTEM PENGELOLAAN DATA SAINS ANTARIKSA

(STUDY OF VULNERABILITY SPOOFING FOR SPACE SCIENCE DATA MANAGEMENT SYSTEM)

Siti Maryam
Pusat Sains Antariksa – LAPAN
email : siti.maryam@lapan.go.id

Riwayat Artikel:

Diterima:
25 Oktober 2017
Direvisi:
16 April 2018
Disetujui:
28 September 2018
Diterbitkan:
19 Nopember 2018

Kata kunci:
Kerentanan Keamanan, *Local Host, Public host*

ABSTRAK

Pusat Sains Antariksa telah membangun sistem pengelolaan data sains antariksa dengan memanfaatkan teknologi HTML (*Hyper Text Markup Language*) dan DNS (*Domain Name Server*). Sistem ini mengelola data hasil pengamatan dari Balai Pengamatan Dirgantara yang tersebar di seluruh wilayah Indonesia. Sistem pengelolaan data sains antariksa dibangun untuk mendukung riset cuaca antariksa. Saat ini sistem pengelolaan data sains antariksa berstatus *local host*. Tahun 2018 akan ditingkatkan menjadi *public host*. Kajian *Vulnerability Spoofing* diperlukan untuk mengetahui kerentanan keamanan pada sistem pengelolaan sains antariksa pada saat menjadi status *public host*. Dengan melakukan kajian *vulnerability spoofing* diharapkan dapat mengantisipasi gangguan keamanan dan menjaga ketersediaan data sains antariksa.

Keywords:

Vulnerability Spoofing, Local Host, Public host

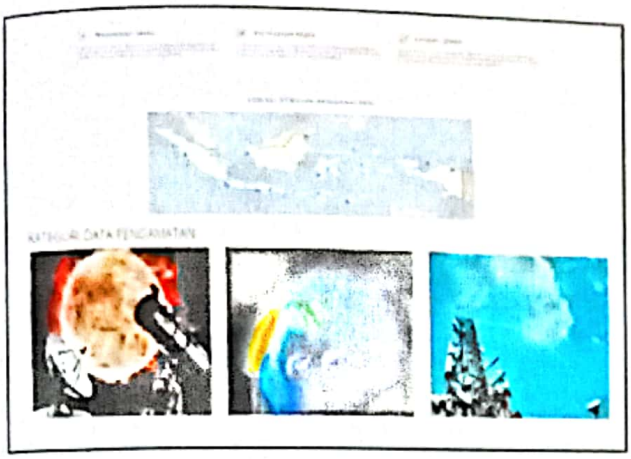
ABSTRACT

Space Science Center has built space science data management system by using HTML (Hyper Text Markup Language) and DNS (Domain Name Server). The space science data management system is a set of observational data management from the Aerospace Observation Center to support space weather research. All space science data stored in a dedicated server. Currently the space science data management system is local host status. 2018 will be upgraded to public host. Vulnerability Spoofing Study is required to find out the security vulnerabilities of the space science management system while it becomes a public host status. By applying vulnerability spoofing study is expected to anticipate security disturbances and maintain the availability of space science data.

1. PENDAHULUAN

Vulnerability spoofing adalah kerentanan yang muncul akibat kelemahan program dan terjadi karena kesalahan dalam merancang, membuat atau mengimplementasikan sebuah sistem. *Vulnerability spoofing*

memungkinkan terjadinya exploitasi pada jaringan komputer. Sekitar 48% situs web di Indonesia rentan terhadap serangan fiksasi (simar et.al., 2011). Penyerang memperoleh kontrol penuh atas akun situs web korban tanpa harus menggunakan kredensial korban yaitu *username* dan *password*

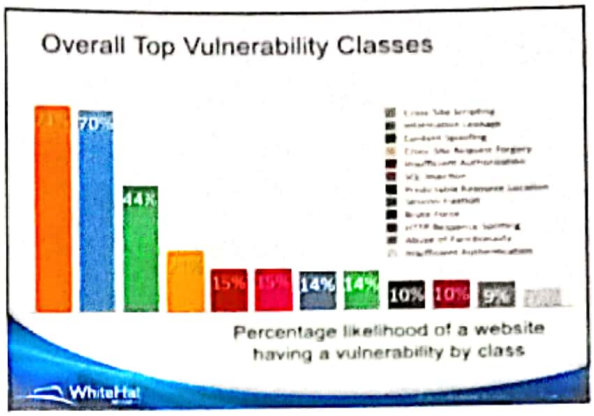


Gambar 1-1 Halaman Sistem Pengelolaan Data Sains Antariksa
(Sumber : badas/localhost)

Pusat Sains Antariksa LAPAN telah membangun sistem pengelolaan data sains antariksa dengan memanfaatkan teknologi *Hyper Text Markup Language* (HTML) dan *Domain Name Server* (DNS). Sistem ini mengelola data pengamatan dan memonitor status operasional alat penelitian 12 balai dan loka pengamatan yang tersebar di seluruh wilayah Indonesia. Sistem pengelolaan data sains antariksa terdiri dari kelompok pengelolaan aktivitas matahari, geomagnet dan ionosfer. Sistem ini dibangun untuk mendukung kebutuhan riset cuaca antariksa. Saat ini sistem pengelolaan data sains antariksa masih dalam status *local host* dengan nama domain *localhost/badas* (maryam, 2017). Tahun 2018 akan ditingkatkan menjadi *public host*. Perhatian yang serius terhadap kasus *vulnerability spoofing* merupakan tahapan dalam persiapan pembaharuan sistem pengelolaan data sains antariksa menuju *public host*. Kajian *vulnerability spoofing* diperlukan untuk mengetahui titik rawan celah keamanan pada sistem pengelolaan data sains antariksa. Tujuan pembahasan agar pengelola dapat mengantisipasi jika terjadi gangguan keamanan pada sistem pengelolaan data sains antariksa, dengan harapan agar sistem dapat beroperasi dan menjamin ketersediaan data untuk kebutuhan riset cuaca antariksa.

2. LANDASAN TEORI

Content spoofing menempati ranking ke-3 Kelas *vulnerability* yaitu sebesar 44%. *Spoofing* melibatkan berbagai representasi informasi palsu. Karena beratnya serangan *spoofing*, jika dibiarkan dapat menimbulkan kerugian yang besar.

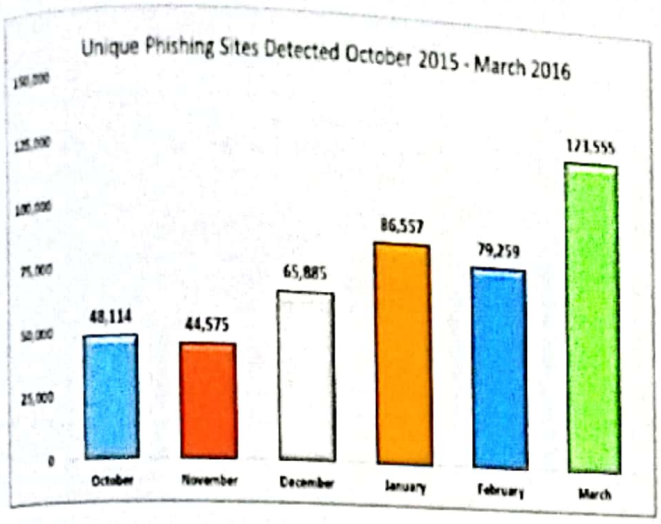


Gambar 2-1 Grafik Spoofing
Sumber https//slideshare.net

Efek serangan *spoofing* menyebabkan pengguna diarahkan ke situs web dan e-mail yang salah (surat non-resmi). Sepertiga dari semua *server* DNS pada internet rentan terhadap *spoofing* (Abisheket.al., 2012). Serangan *spoofing* dapat menyebabkan masalah keamanan serius bagi *server* DNS. Terdapat lima celah keamanan pada DNS yaitu jaringan lokal, ISP DNS *Services*, DNS *Global Services*, *Corporate Domain*, *Related Resolution Services* (Panchabi et.al,2014). Ancaman lain dari serangan DNS *Spoofing* adalah pemanfaatan serangan *phishing*, yaitu suatu cara penipuan untuk mendapatkan rincian informasi akun tertentu melalui cara yang tidak sah, seperti melalui website tiruan maupun *pop-up* yang menyerupai website resmi instansi atau perusahaan (Steinho et.al., 2013).

3. DATA DAN METODE

Data yang digunakan pada kajian *vulnerability* spoofing pada sistem pengelolaan data sains antariksa adalah data kasus phising yang terjadi pada tahun 2016.



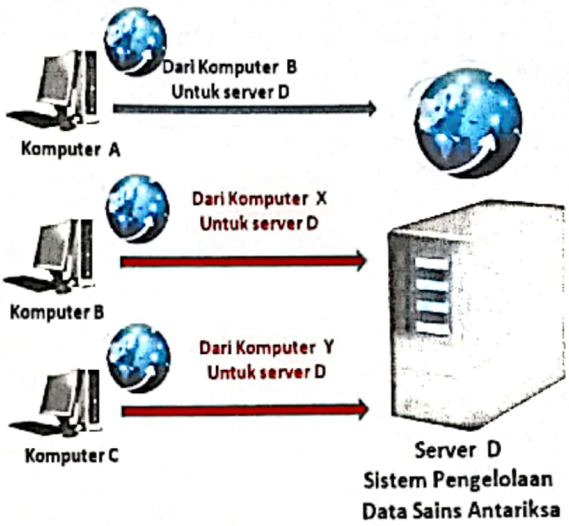
Gambar 3-1 Laporan Kasus *Phishing (Andri et.al, 2016*

Sumber data Anti *Phising Working Group* (APWG) menunjukan jumlah situs *phishing* terus meningkat setiap bulan. Laporan kasus *phishing* meningkat pada periode Oktober 2015 – Maret 2016 (Savita et.al., 2013). Pada bulan Oktober 2015 berjumlah 48.114 kasus. Dan mencapai puncaknya pada bulan maret 2016, yaitu sejumlah 123. Peningkatan yang luar biasa hingga mencapai 250% dalam kurun waktu enam bulan.

Metode kajian *vulnerability spoofing* pada sistem pengelolaan data sains antariksa dilakukan melalui kegiatan identifikasi *vulnerability spoofing* yaitu mengkaji jenis *vulnerability spoofing* serta mekanismenya. Pada sistem pengelolaan data sains antariksa, memungkinkan terdapatnyan tiga jenis *vulnerability spoofing*, yaitu IP *spoofing*, web *spoofing* dan DNS *spoofing*.

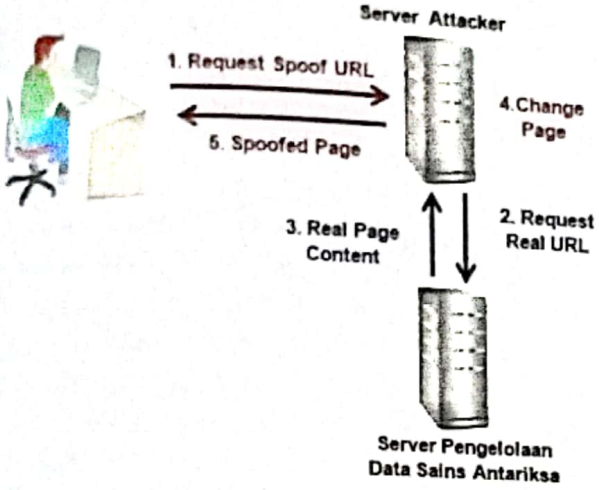
4. PEMBAHASAN

Gambar 4-1 adalah skema IP *spoofing* pada sistem pengelolaan data sains antariksa. IP *spoofing* digunakan untuk mendapatkan akses tidak sah ke komputer. Komputer X dan Y akan berusaha mendapatkan akses ke *server* sistem pengelolaan data sains antariksa dengan memanfaatkan IP milik komputer B dan C. *IP Spoofing* mengirim label yang dipalsukan (*spoofed)* untuk menyesatkan sehingga *server* akan mengirimkan balasan paket informasi pada komputer yang salah. Pengelola harus waspada, bila pada *server* sistem pengelolaan data sains antariksa terjadi pengiriman paket sampah dalam jumlah besar, maka server mengalami *overload*. Dan ini merupakan tujuan dari IP *spoofing*. Pada kondisi normal, komunikasi dalam suatu jaringan komputer harus menyertakan label pengirim dari sumber ke tujuan (Ramesh, 2010). Pada komunikasi normal, komputer pengirim menggunakan informasi yang benar tentang dirinya sebagai pengirim, dan *server* akan mudah untuk merespon komunikasi tersebut.



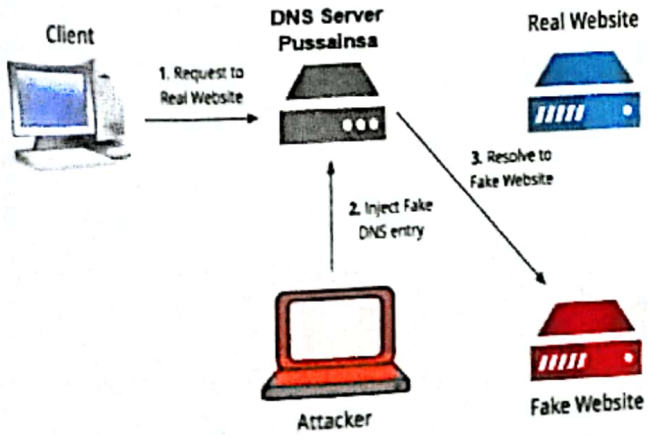
Gambar 4-1 Skema *IP spoofing*
Pada Sistem Pengelolaan Data Sains Antariksa

Gambar 4-2 adalah *web spoofing* atau *hyperlink* pada sistem pengelolaan data sains antariksa. *Web spoofing* merupakan serangan yang memungkinkan pelaku dapat melihat dan memodifikasi semua halaman situs web(Adam et.al., 2014). Pelaku dapat memonitor, mengambil, atau mengubah informasi pengguna ke *server* atau sebaliknya. *Web spoofing* membahayakan informasi pengguna situs web dan memungkinkan pelaku membuat duplikat seluruh situs web (Syarif, 2008). Akses ke duplikat situs web akan menuju ke komputer pelaku, sehingga dengan leluasa pelaku dapat memonitor aktifitas korban pada situs web. Pelaku memantau dan mengendalikan semua yang dilakukan korban melalui situs web. Lalu lintas situs web berjalan antara *browser* korban, *web server* dan pelaku. Pada *web spoofing*, pelaku membuat halaman palsu yang meyakinkan sehingga korban merasa mendapatkan yang asli. Pelaku pada web *spoofing* dapat mengawasi, mengubah serta menulis ulang tautan URL.



Gambar 4-2 Skema *Web Spoofing Pada Pengelolaan Data Sains Antariksa*

Gambar 4-3 : adalah skema DNS *spoofing* pada sistem pengelolaan data sains antariksa. DNS *Spoofing* merupakan kesalahan pada saat *server* DNS menerima dan menggunakan informasi yang salah dari *host* akibat *malicious application* (malware, virus) atau kesalahan konfigurasi nama server sehingga tidak dapat diakses secara normal karena permintaan *resolve* diubah dan pengguna disalurkan menuju situs web yang berbeda dengan situs web yang dituju[(Amala et.al., 2013). DNS *spoofing* melakukan serangan dengan cara masuk ke DNS *server*, mengedit *file host* yang terdapat di DNS *Server* (*poisoning file host*) dan mengubah *IP address* dari suatu situs web. Pada saat pengguna mengakses situs web, maka alamat situs lain yang diperoleh, yaitu situs peralihan yang dibuat oleh pelaku kemudian memanfaatkannya untuk melakukan tindakan kejahatan lain seperti *phising* dan menyelipkan virus.



Gambar 4-3 Skema DNS *Spoofing Pada Sistem Pengelolaan Data Sains Antariksa*

5. KESIMPULAN

Kajian *vulnerability spoofing*, memberikan pemahaman kepada pengelola betapa pentingnya mengetahui celah keamanan pada sistem pengelolaan data sains antariksa. Tahapan persiapan keamanan sistem pengelolaan data sains antariksa perlu dilakukan sebelum memperbaharui ke tahap *public host*. Tiga bagian penting pengetahuan tentang celah keamanan pda sistem pengelolaan data sains antariksa, yaitu IP, Situs Web dan DNS. Dengan mengetahui celah keamanan pada ketiganya diharapkan menjaga ketersediaan data sains antariksa dan mengantisipasi gangguan keamanan selama sistem beroperasi.

UCAPAN TERIMA KASIH

Ucapan terima kasih disampaikan kepada Ibu Elyyani, Bapak. Ahmad Zulfiana, Bapak Yoga Andrian beserta tim jaringan dan pengelolaan basis data sains antariksa.

DAFTAR RUJUKAN

Abhishek Khumar, K., B., & Manoj, C. (2012). Prevention Of Session Hijacking And IP spoofing With Sensor Nodes And Cryptographic Approach. International Journal of Sciences: Basic and Applied Research (IJSBAR).

Adam Ali, Z., & Esra'a Ali, Z., H.(2014). DNS Advanced Attacks and Analysis. International Journal of Computer Science and Security (IJCSS): Volume (8), Issue (2).

Andri, L. S., Reza El, A., & Nur, W.(2016). Investigasi Email Spoofing dengan Metode Digital Forensics Research Workshop (DFRWS). Jurnal Edukasi dan Penelitian Informatika (JEPIN): Vol. 2, No. 2, ISSN 2460-0741.

Amala, G., & Chinappanjayakumar.(2013). Identifying and locating multiple spoofing attackers using clustering in wireless network. International Journal of Wireless Communications and Mobile Computing 2013; 1(4): 82-90 Published online September 30, 2013.

Maryam, S.(2017). Sistem Pengelolaan Basis Data Sains Antariksa. Laporan Kegiatan Inhouse: Pusat Sains Antariksa, LAPAN.

Panchabi, K., & Ramesh, K.(2014). Detection of Spoofing Attack and Localization of Multiple Adversaries in WSN. International Journal of Innovative Research in Computer and Communication Engineering.

Ramesh Babu, & Lalitha, B.(2010). A Comprehensive Analysis of Spoofing. (IJACSA) International Journal of Advanced Computer Science and Applications: Vol. 1, No.6, December.

Savita, B., Chavan, & Meshram.(2013). Classification of Web Application Vulnerabilities. International Journal of Engineering Science and Innovative Technology (IJESIT): Volume 2, Issue 2, March.

Simar, P. S., & Raman, M., (2011), Spoofing Attacks of Domain Name System Internet, International Journal of Computer Applications® (IJCA).

Steinho, Wiesmaier, & Araújo.(2013). The State of the Art in DNS Spoofng. Department of Cryptography and Computeralgebra Technische Universität Darmstadt Hochschulstr: 10; D-64283 Darmstadt, Germany.

Syarif, H.(2008). Konsep Solusi Keamanan Web Pada Pemograman PHP. Jurnal Computech & Bisnis: Vol. 2, No. 2, Desember, ISSN 1978-9629.

Siti Maryam, ST, Lahir di kota Tasikmalaya (Jawa Barat), 18 Juni 1973. Menyelesaikan pendidikan strata 1 (S1) di Jurusan Teknik Informatika Fakultas Teknik Universitas Islam Nusantara Bandung pada tahun 1996. Bekerja sebagai Pegawai Negeri Sipil di Lembaga Penerbangan dan Antariksa Nasional mulai tahun 1997. Saat ini menjabat sebagai Peneliti Bidang sistem Informasi di Pusat Sains Antariksa LAPAN.