Implementasi IP-Tables Firewall pada Linux sebagai Sistem Keamanan Jaringan yang Handal

Qurrotul Aini[a] dan Victor Amrizal[b]

[a]*Staf Pengajar Fakultas Sains dan Teknologi*
Universitas Islam Negeri Syarif Hidayatullah Jakarta
Tel : (021) 7493547 Fax : (021) 7493315
e-mail : atafamily@yahoo.com

[b]*Staf Pengajar Fakultas Sains dan Teknologi*
Universitas Islam Negeri Syarif Hidayatullah Jakarta
Tel : (021) 7493547 Fax : (021) 7493315
e-mail : ersebros@yahoo.com

ABSTRACT

Effloresce computer network technology considerably quick, even with its attending internet *which technically doesn't be stymied by distance and time, so communication process and data interchange can be done squashy. It cans be big problem if not handled aright, since with being exploited its security hole, therefore user that don't deserve to get squashy do crimes in world cyber that recognized with the title Cyber Crime, as sniffing, spoofing, Attack's pack and another one gets Category as criminological as deep world virtual, about the problem on firewall's implemented analysis as one computer network security system. Analysis process is done through steps which systematic and there is three parameter that become base in gleans from which is port in a state stealth, close and open. From analysis result that gets to be pulled a conclusion by applying IP-Tables as firewall can secure computer network system***.**

Keywords: *Cyber crime, sniffing, spoofing, Dos Attack, Stealth, PORT, IP-tables and Firewall.*

1. PENDAHULUAN

Teknologi jaringan komputer berkembang dengan sangat pesat, bahkan dengan hadirnya internet yang secara teknis tidak terhalang oleh jarak dan waktu, sehingga proses komunikasi dan pertukaran data dapat dilakukan dengan mudah. Tetapi akibat dari perkembangan teknologi tersebut telah mengarah kepada suatu eksploitasi lubang keamanan sistem jaringan komputer. Hal ini dapat menjadi masalah yang besar apabila tidak ditangani dengan benar, karena dengan tereksploitasinya lubang keamanan, maka pengguna yang tidak berhak dapat dengan mudah melakukan kejahatan-kejahatan dalam dunia *cyber* yang dikenal dengan sebutan *Cyber Crime*, seperti *sniffing*, *spoofing*, DoS *Attack* dan lainnya yang dapat dikategorikan sebagai kejahatan dalam dunia maya.

Permasalahan pada analisis penerapan *firewall* sebagai sebuah sistem keamanan jaringan komputer. Diharapkan dapat memberikan suatu pengertian tentang peranan *firewall* dalam mengamankan jaringan lokal terhadap kemungkinan serangan dari pihak-pihak yang tidak bertanggung jawab. Proses analisis dilakukan melalui langkah-langkah yang sistematis dan ada tiga parameter yang menjadi landasan dalam menarik kesimpulan yaitu port dalam keadaan *stealth*, *close* dan *open*. Prosesnya dilakukan melalui situs-situs internet yang menyediakan layanan *probing* dan *scanning* port seperti grc.com, Symantec.com dan veniceflorida.com, sehingga dihasilkan suatu analisis yang dapat menggambarkan suatu sistem keamanan komputer secara deskriptif dan menyeluruh.

Hasil *probing* dan *scanning* yang telah dilakukan didapatkan hasil *port-port* yang sangat penting dan rawan akan terjadinya penerobosan oleh para *cracker* berada dalam kondisi *stealth*, yang berarti bahwa *port-port* tersebut dalam keadaan sangat baik dan sulit bagi para *cracker* untuk menembusnya. Dari hasil analisis, dapat ditarik suatu kesimpulan bahwa dengan menerapkan Iptables sebagai firewall sudah dapat mengamankan sistem jaringan komputer. Tetapi hal ini juga tergantung dari kecakapan Administrator jaringan dalam mengkonfigurasikan *firewall*. Untuk lebih meningkatkan keamanan jaringan, sebaiknya Administrator jaringan harus sering memperbaharui sistem keamanan jaringan yang telah ada serta menambahkan beberapa aplikasi keamanan jaringan, terus memantau serta mencari kelemahan-kelemahan

yang terdapat pada sistem keamanan jaringan yang dikelolanya, sehingga akan didapat sistem keamanan jaringan yang benar-benar handal.

2. LANDASAN TEORI

2.1 Karakteristik dan Jenis Firewall yang digunakan

Dalam proses implementasi sistem keamanan jaringan digunakan *firewall* yang mempunyai karakteristik dan jenis yang disesuaikan dengan kebutuhan perusahaan dilihat dari berbagai segi keamanan data perusahaan.

2.2 Karakteristik Firewall

Firewall yang digunakan sebagai sistem pengaman jaringan dan *Firewall* ini terdapat pada Linux dengan kernel versi 2.4x

1. Hanya dapat bekerja di sistem operasi linux
2. *Firewall* ini tidak memerlukan lisensi khusus karena telah terdapat dalam satu paket linux
3. *Firewall* diletakkan di antara internet dengan jaringan internal
4. Informasi yang keluar atau masuk harus melalui *firewall* ini
5. Bekerja dengan mengamati paket IP (internet *protocol*) yang melewatinya
6. Dapat melakukan fungsi *filtering* dan fungsi *proxy*

2.3. Jenis Firewall yang digunakan

Sesuai dengan sistem operasi yang digunakan sebagai server maka firewall yang digunakan adalah Iptables yang sudah terdapat satu paket dalam Linux dengan kernel versi 2.4x ke atas.

2.4 Analisis Efektifitas Penerapan Iptables sebagai Sistem Pengamanan Jaringan Komputer

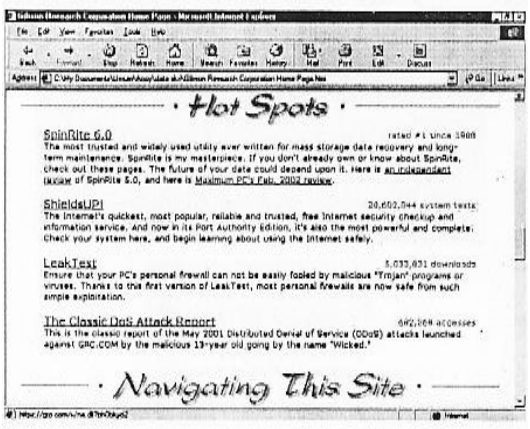
Pada proses analisis sistem keamanan jaringan, agar mendapatkan hasil yang benar-benar akurat, metode yang dilakukan adalah dengan melakukan probing dan *scanning port* melalui *webtools* yang disediakan oleh situs-situs yang menyediakan layanan tersebut.

Ada beberapa situs yang menyediakan layanan probing port di antaranya adalah:
http://www.grc.com/,
http://www.veniceflorida.com/,
http://www.dwam.com/, dan
http://www.symantec.com/.

2.5 Analisis Sistem Keamanan Jaringan menggunakan Webtools grc.com

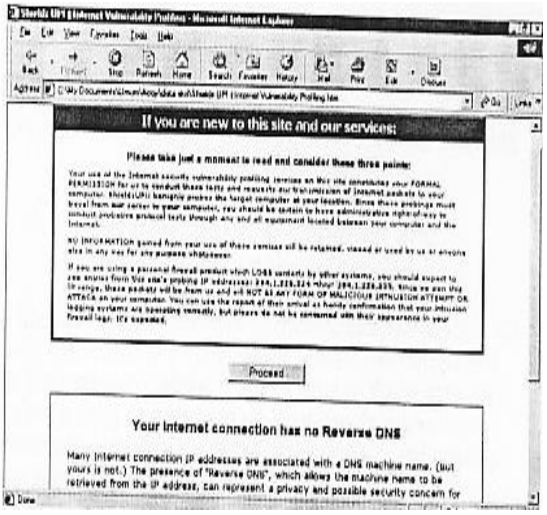
Langkah-langkah teknis proses analisis yang dilakukan pada situs grc.com adalah sebagai berikut:

1. Pertama masuk ke halaman muka dari situs grc.com, yang mempunyai alamat: http://www.grc.com/default.htm, kemudian klik ShieldUP!!
2. Kemudian klik *online* internet security test atau klik *shields up*.



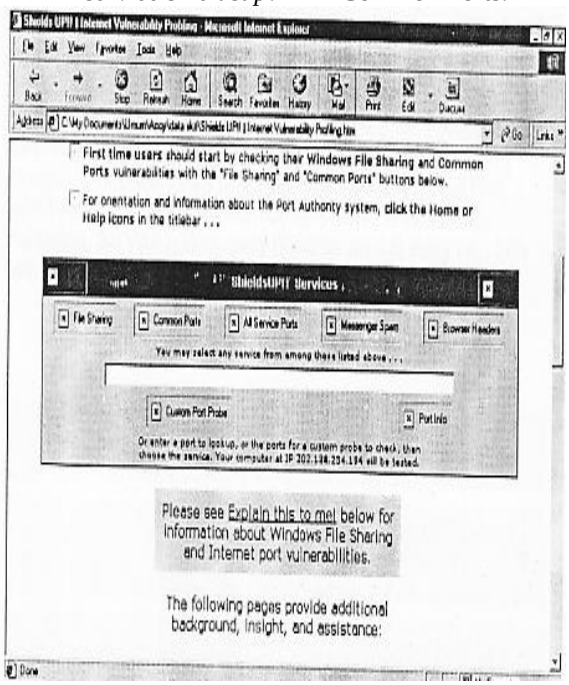
Gambar 1. Halaman *Security Test*

3. Langkah selanjutnya akan ada dua pilihan proses, klik *command button Proceed* pertama untuk proses selanjutnya.



Gambar 2. Halaman Autentifikasi Proses

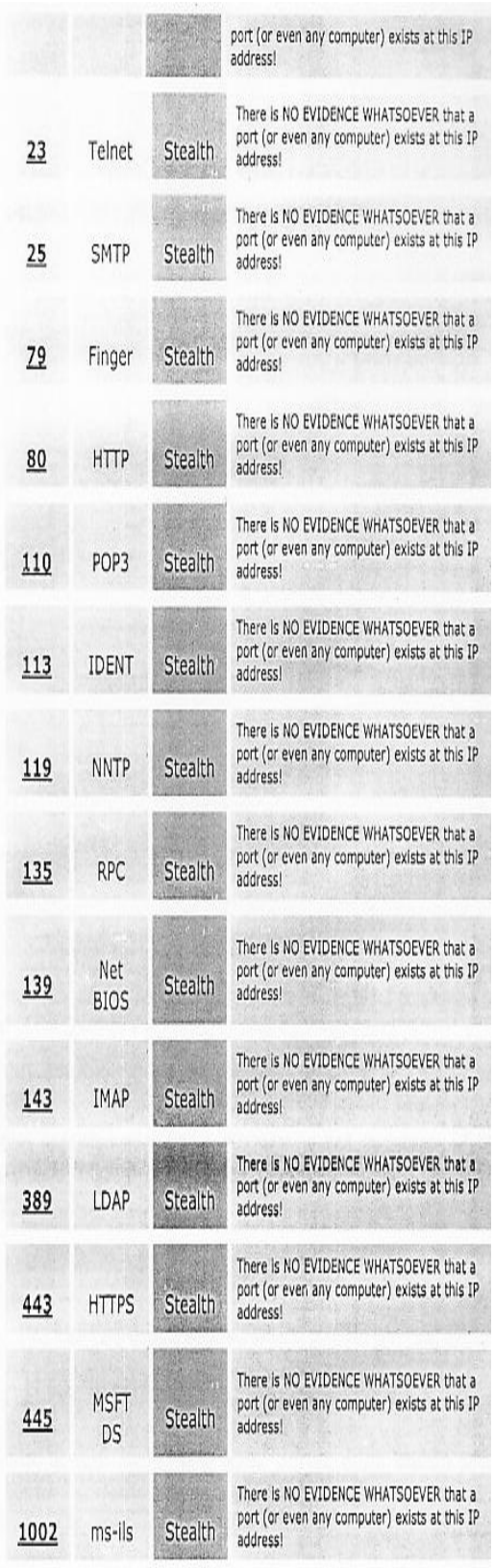
4. Kemudian akan ada beberapa pilihan proses *service shieldsup*! Pilih Common Ports.



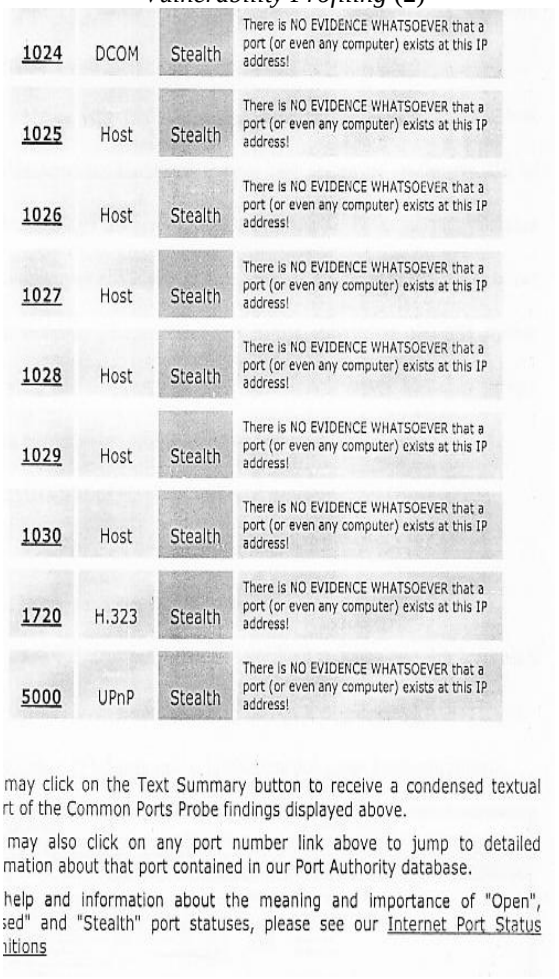
Gambar 3. Halaman Pemilihan *Port*

5. Tunggu dalam beberapa menit maka akan ditampilkan hasil proses analisis yang telah dilakukan, sebagai berikut:

Gambar 4. Halaman Hasil Proses *Probing Port Authority Edition* - Internet *Vulnerability Profiling* (1)



Gambar 5. Halaman Hasil Proses *Probing Port Authority Edition* - Internet *Vulnerability Profiling* (2)



Gambar 6. Halaman Hasil Proses *Probing Port Authority Edition* - Internet *Vulnerability Profiling* (3)

Dari hasil yang didapat tidak ada satupun port dari *port* yang didefinisikan yaitu *port* 21, 23, 25, 79,80 yang berindikator *closed* ataupun *open*. Semua port memiliki nilai *Stealth*, yang berarti jaringan dalam keadaan aman dari *sniffing*, prqfflng, DoS *Attack* dan gangguan lainnya.

3. PEMBAHASAN

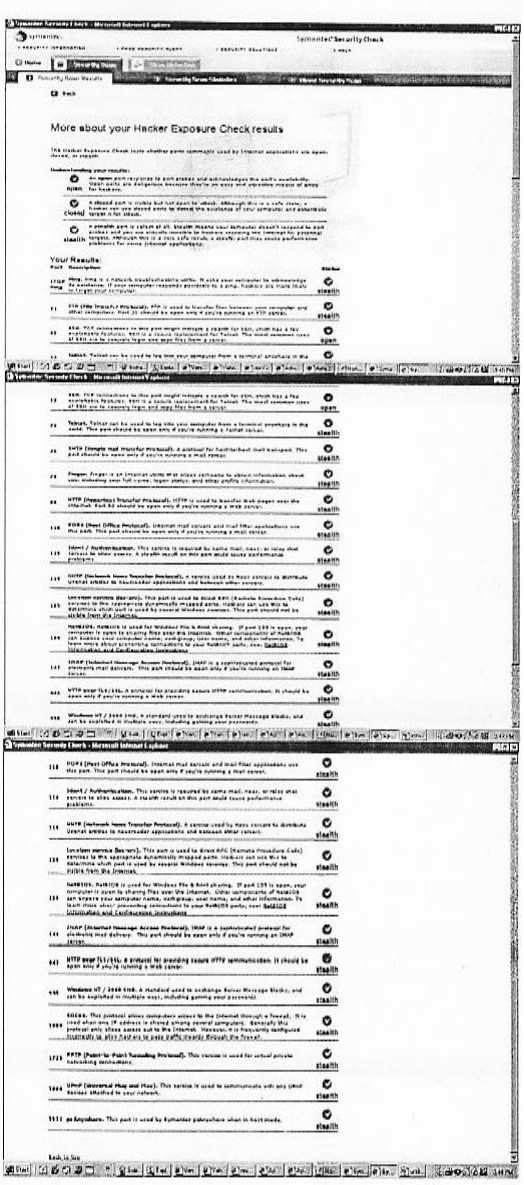
3.1 Analisis Sistem Keamanan Jaringan Menggunakan Webtools symantec.com

Analisis yang dilakukan dengan menggunakan *webtools* Symantec.com, memiliki perbedaan konfigurasi maupun hasil dengan tes sebelumnya. Hal ini dimaksudkan agar ada perbedaan pada hasil analisa. Perbedaan yang dilakukan adalah dengan membuka. *port* 22 (ssh), sehingga hasil yang terlihat

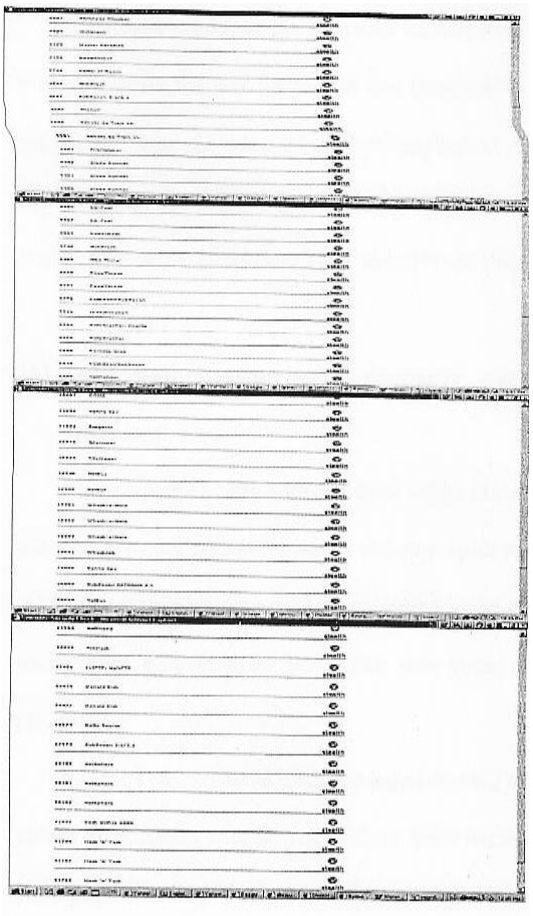
adalah bahwa sistem keamanan jaringan rentan akan bahaya penyerangan oleh para *cracker*. Dan perlu ada antisipasi dari pihak administrator sistem keamanan jaringan dengan menambahkan beberapa program keamanan lainnya. Berikut ini adalah urutan proses analisis:

1. Masuk ke dalam *home page* symantec.com
2. Lakukan *scanning security* jaringan
3. Ada dua hasil yang didapat, yaitu hasil *scanning port* dan hasil *check* Trojan horse, berikut ini adalah hasil-hasil yang diperoleh

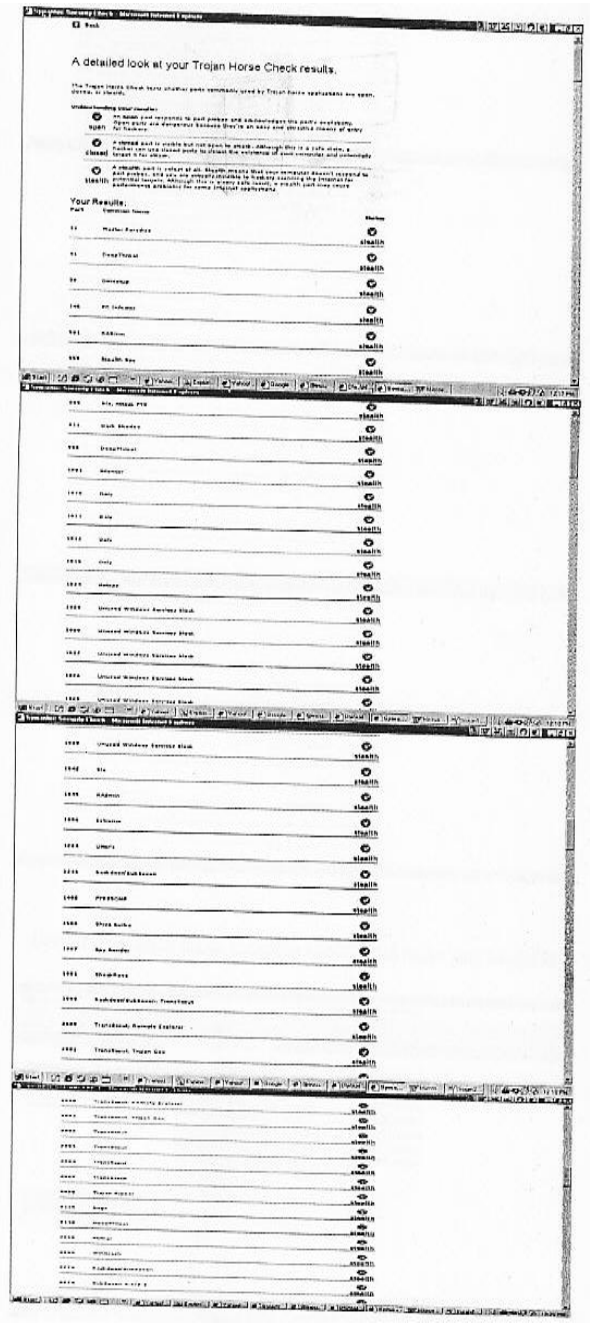
Gambar 7. Halaman Analisis Keseluruhan dari Sistem Keamanan Jaringan



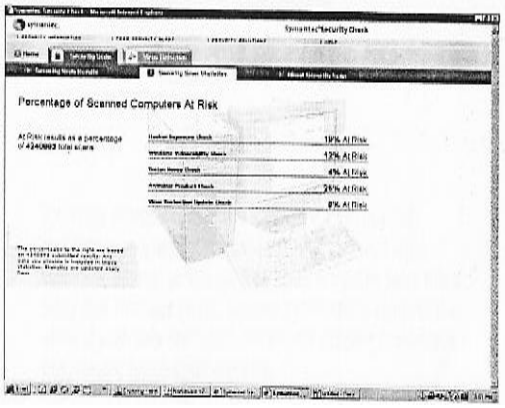
Gambar 8. Halaman *Probing Port* Symantec.com



Gambar 9. Halaman Analisis Trojan Horse (1)



Gambar 10. Halaman Analisis Trojan Horse (2)



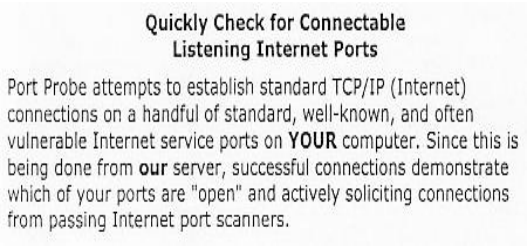
Gambar 11. Halaman Analisis Trojan Horse (3)

Dari hasil analisis yang dilakukan oleh Symantec.com baik untuk *probing port* maupun penelusuran akan bahaya serangan Trojan horse. Dengan perlakuan dibukanya *port* 22 (ssh), maka dapat dipastikan terdapat lubang keamanan yang dapat dipergunakan untuk menyerang sistem keamanan jaringan, baik melalui *spoofing*, *sniffing*, maupun melalui DoS *Attack*, serta jenis-jenis serangan lainnya.

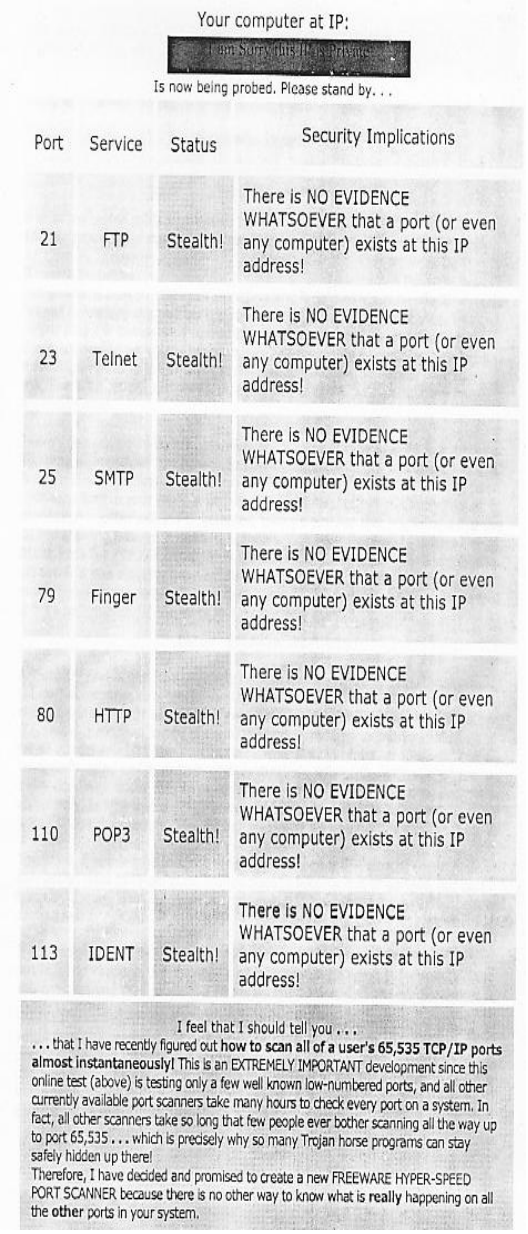
3.2 Analisis Sistem Keamanan Jaringan menggunakan *Webtools* venice florida.com

Proses analisis melalui *webtools* venice florida.com sangalah sederhana, tidak seperti proses yang dilakukan oleh *webtools* sebelumnya. Apabila ingin melakukan proses analisa yang harus dilakukan hanyalah masuk ke dalam situs venice florida.com, dan secara otomatis akan dilakukan proses *scanning* dan *probing port*.

Hasil analisis yang dihasilkan cukup baik, sama dengan hasil *probing* yang dilakukan oleh situs grc.com, dan dengan kondisi konfigurasi Iptables yang sama. Dengan pengertian bahwa konfigurasi untuk semua layanan komunikasi melalui *port-port* ditutup. Hasil analisis yang dilakukan melalui *webtools* venice florida.com disajikan pada Gambar 12.



Gambar 12. Halaman Hasil *Probing* (1)



Gambar 13. Halaman Hasil *Probing* (2)

So please be sure to add yourself to my eMail system so I can let you know when this new, completely free, port scanning application is ready!

Port Status Descriptions:

Stealth!

If all of the tested ports were shown to have stealth status, then **for all intents and purposes your computer doesn't exist to scanners on the Internet!**

It means that either your computer is turned off or disconnected from the Net (which seems unlikely since you must be using it right now!) or an effective stealth firewall is blocking all unauthorized external contact with your computer. This means that it is **completely opaque** to random scans and direct assault. Even if this machine had previously been scanned and logged by a would-be intruder, a methodical return to this IP address will lead any attacker to believe that your machine is turned off, disconnected, or no longer exists. You couldn't ask for anything better.

There's one additional benefit: scanners are actually hurt by probing this machine! You may have noticed how slowly the probing proceeded. This was caused by your firewall! It was required, since your firewall is discarding the connection-attempt messages sent to your ports. A non-firewalled PC responds immediately that a connection is either refused or accepted, telling a scanner that it's found a live one ... and allowing it to get on with its scanning. **But your firewall is acting like a black hole for TCP/IP packets!** This means that it's necessary for a scanner to **sit around and wait** for the maximum round-trip time possible – across the entire Net, into your machine, and back again – before it can safely conclude that there's no computer at the other end. That's very cool.

FALSE STEALTH REPORTS

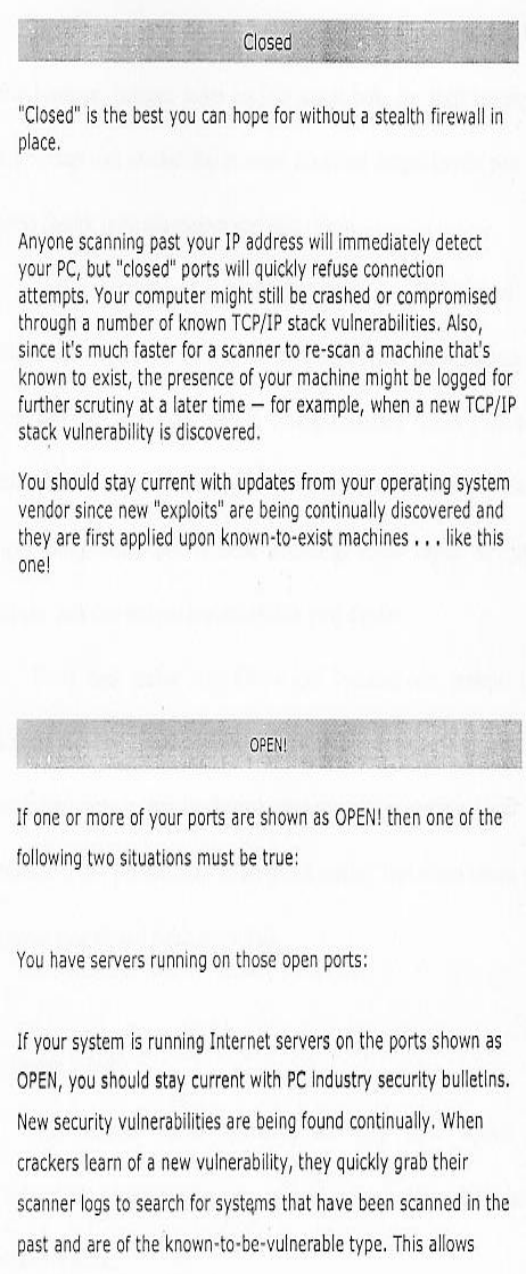
A "Stealth" port is one from which no reply is received (neither acceptance nor refusal) in response to a connection initiation request. This ShieldsUP web site sends a series of **four connection requests**, waiting for any reply after each one. If no reply is received to any of them, the port is declared to be "Stealth" . . . and for all intents and purposes that's exactly what it is. But Internet "packets" are continually being lost in route to their destination. When Internet "routers" are overloaded with traffic they have no recourse other than to simply drop packets completely, hoping that they will be resent when the destination fails to acknowledge their receipt. This, of course, is why we try four times to get through.

Therefore, if prime-time Internet congestion coupled with a slow or noisy connection were to cause those four packets to become lost or garbled, our port test would show "Stealth" when your port would have replied if it had ever received the request.

If you suspect that this may have happened during the assembly of the report above, simply refresh your browser's page to re-run the tests. If the results differ you can presume that congestion or a weak connection were the temporary cause.

NOTE: If your system did NOT show up as Stealth! but you wish that it could, you;ll need to use one of the inexpensive (or FREE in the case of ZoneAlarm 2!) personal firewalls I've discovered. I will also be creating my own firewall which you can monitor and be informed of, by adding yourself to **my eMailing System**. But in the meantime . . . I'd advise you not to wait! (Especially since ZoneAlarm 2 is completely FREE for individual use!)

Gambar 14. Halaman Hasil *Probing* (3)



Closed

"Closed" is the best you can hope for without a stealth firewall in place.

Anyone scanning past your IP address will immediately detect your PC, but "closed" ports will quickly refuse connection attempts. Your computer might still be crashed or compromised through a number of known TCP/IP stack vulnerabilities. Also, since it's much faster for a scanner to re-scan a machine that's known to exist, the presence of your machine might be logged for further scrutiny at a later time – for example, when a new TCP/IP stack vulnerability is discovered.

You should stay current with updates from your operating system vendor since new "exploits" are being continually discovered and they are first applied upon known-to-exist machines . . . like this one!

OPEN!

If one or more of your ports are shown as OPEN! then one of the following two situations must be true:

You have servers running on those open ports:

If your system is running Internet servers on the ports shown as OPEN, you should stay current with PC industry security bulletins. New security vulnerabilities are being found continually. When crackers learn of a new vulnerability, they quickly grab their scanner logs to search for systems that have been scanned in the past and are of the known-to-be-vulnerable type. This allows

Gambar 15. Halaman Hasil *Probing* (4)

Hasil analisis yang didapat dari Veniceflorida.com, menyatakan bahwa sistem keamanan jaringan dalam keadaan sangat baik dan kecil kemungkinan untuk disusupi oleh cracker. Hal ini dapat dibuktikan dengan kondisi port dalam keadaan *Stealth*, tanpa ada satupunpor/ yang terbuka.

Analisis yang diperoleh berdasarkan hasil dari *probing port* ketiga *webtools* sebelumnya, menunjukkan bahwa sistem jaringan berada dalam keadaan aman, karena *port-port* yang dapat menjadi lubang keamanan berada pada kondisi *Stealth*. Hal tersebut berindikasi bahwa sistem keamanan jaringan

komputer dengan menggunakan *Iptables* dapat melindungi semua bagian dari jaringan komputer, baik data maupun aplikasi-aplikasi yang dipakai.

Untuk hasil analisis yang didapat dari Symantec.com, terdapat lubang keamanan pada port 22 (ssh), tapi konfigurasi sistem keamanan jaringan memang dikondisikan berbeda dari konfigurasi sebelumnya, agar dapat menjadi bahan pembelajaran dan perbandingan dalam proses analisa. Tapi secara umum sistem keamanan yang dipakai sudah sangat baik.

4. PENUTUP

4.1 Kesimpulan

Dengan memakai *iptables* sebgai *firewall* sebenarnya cukup untuk melindungi jaringan yang tehubung dengan dunia luar. Dengan berbagai macam serangan dan ancaman yg datang dari pihak-pihak yang tidak bertanggung jawab. *Web tool* yang digunakan dalm *port probing* mampu mendeteksi lubang keamanan. Dalam pengamanan harus memiliki program aplikasi kemananan yang lain seperti antivirus dan lainnya supaya lebih terlindungi.

4.2 Usulan Solusi

Ada berbagai macam aplikasi-aplikasi yang dapat dipakai untuk melindungi dari *cracker-cracker* yang mencoba masuk ke dalam sistem jaringan. Di antaranya adalah:

1. Program aplikasi Antisniff
   Program aplikasi ini dibuat oleh LOpht heavy industries, Inc. program aplikasi ini dapat menscan segmen-segmen dari Network Interface Card. Program aplikasi ini didesain bekerja secara dua arah yang akan memeriksa dan mengidentifikasi mesin apa yang berada pada suatu segmen jaringan. Program ini dilengkapi juga dengan alarm sebagai pengingat apabila terjadi hal-hal yang dianggap mengancam sistem jaringan. Dan kelebihan lainnya adalah program aplikasi ini dapat mengirimkan pesan *email* kepada administrator jaringan apabila suatu waktu sedang berada di tempat lain. Sedangkan kelemahan dari program ini adalah tidak dapat mendeteksi adanya serangan DoS Attack, serta tidak dapat menutup *port* 25 apabila terjadi serangan.

2. Program aplikasi *Attacker*
   Program aplikasi ini dibuat oleh foundstone Inc, ini dapat mendengarkan *port-port* komunikasi TCP/IP maupun UDP, cara kerjanya adalah dengan mendeteksi koneksi komunikasi data pada port-port TCP/IP dan UDP dan mengirimkan hasilnya dengan menampilkan alamat dari koneksi itu berasal. berikut ini adalah gambar tampilan program aplikasi *attacker*. Program aplikasi ini memiliki kelemahan yaitu tidak dapat mendeteksi adanya penyusup yang menyerang melalui *port* 25. Demikianlah usulan solusi ini ditawarkan, untuk mengatasi atau sebagai bentuk antisipasi daripada serangan yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab.

REFERENSI

Andreasson, Oskar, Iptables Tutorial 1.1.19, blueflux@koffein.net, 2001-2003. Anonim, http://www.netfilter.org/, 2 Maret 2004, pk. 16.23 WIB.

Anonim,http://iptables-tutorial.frozentux.net/iptables-tutorial.html#RCFIREWALLTXT, 14 Desember 2003, pk. 12.03 WIB.

Anonim, http://iptables-tutorial.frozentux.net/iptables-tutorial.htmWRCFLUSH-IPTABLES TXT, 14 Desember 2003, pk. 11.38 WIB.

Anonim, http://www.netfilter.org/documentation/index.html # FAQ, 2 Maret 2004,pk. 16.18 WIB. Anonim, http://www.news.com / News / Item/ Textonly / 0 , 25 ,20278,00.html? pfv,13 Mei 2004, pk.21.40 WIB.

Anonim, http://www.news.com/News/Item/0,4,20226,00.html,13 Mei 2004, pk.21.27 WIB.

Anonim, http://www.ee.siue.edu/~rwalden/networking/icmp.htm, 1 Mei 2004, pk. 21.47 WIB

Anonim, http://ipsysctl-tutorial.frozentux.net/other/rfc792.txt, 14 Desember 2003,pk. 11.57 WIB.

Anonim, http://iptables-tutorial.frozentux.net/other/rfc793.txt, 14 Desember 2003,pk. 12.13 WIB

Anonim, http://iptables-tutorial.frozentux.net/other/ip_dynaddr.txt, 14 Desember2003, pk. 12.17 WIB.

Anonim, http://www.netfilter.org/unreliable-guides / packet - filtering - HO WTO/ index.html, 6 Maret 2004, pk. 20.21 WIB.

Anonim, http://www.netfilter.org/unreliable-guides/NAT-HOWTO/index.html,6 Maret 2004, pk. 20.25 WIB.

Anonim, http://www.netfilter.org/unreliable-

guides/netfilter - hacking - HOWTO/ index.html, 6 Maret 2004, pk. 20.40 WIB.
Anonim, http://www.grc.com, 8, 17 Juni 2004, pk. 10.12 WIB.
Anonim, http://symantec.com, 25 Juni 2004, pk. 14. 20 WIB.
Anonim, http://www.veniceflorida.com, 25 Juni 2004, pk. 14.26 WIB.
Linux , Mail Administrator, WebCenter Technologies Inc., 2001.
LINUX, System Administrator, WebCenter Technologies Inc., 2001.
Mei, Wang, MCSE Tutorial on Networking Essential, E-Book, 2002.
Purbo, Onno W., & Wiharjito, Tony, Keamanan Jaringan Internet, Elex MediaKomputindo, Penerbit Kelompok Gramedia, Jakarta, 2000.
Riza, Taufan, TCP/IP dan Managemen Jaringan, Elex Media Komputindo,Penerbit Kelompok Gramedia, Jakarta, 1999.
Sembiring, Jhony H, Jaringan Komputer Berbasis Linux, Elex MediaKomputindo, Penerbit Kelompok Gramedia, Jakarta, 2001.
Takenbaum, Andrew, Computer Network, 4th ed, 2003.
William, Stallings, Data and Computer Communication, 7th ed, 2004.