ANALISIS PERBANDINGAN PERFORMANSI DAN KEAMANAN FILE TRANSFER PROTOCOL OVER SSH TUNNELING (SECURE FTP) DENGAN FILE TRANSFER PROTOCOL OVER SSL (FTPS)

Eka Mahadi Fazar M[1], Tri Brotoharsono[2], Niken Dwi Wahyu Cahyani[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

---

Abstrak

File Transfer Protocol atau FTP adalah salah satu protokol yang digunakan untuk pertukaran file baik berupa upload file maupun download file. Sayangnya FTP masih meninggalkan lubang keamanan dimana data yang dikirimkan masih dapat dibaca dengan jelas. Selain itu, tidak adanya mekanisme autentikasi server, membuat client dapat beresiko untuk mengakses FTP server palsu.

Penelitian ini menguji Secure FTP dan FTPS, kedua metode keamanan yang diterapkan pada FTP untuk mengatasi celah-celah keamanan yang ditinggalkan oleh FTP. Aspek keamanan yang diuji mencakup confidentiality (kerahasiaan data) dan authentication (autentikasi). Selain itu, penelitian ini juga menguji kedua metode tersebut dari segi performansi. Aspek performansi yang diujikan mencakup delay,throughput, dan utilitas CPU serta memori pada single transfer dan multiple transfer, dan juga dari kompleksitas pemakaian metode tersebut.

Dari hasil pengujian didapatkan kesimpulan bahwa FTPS mempunyai tingkat keamanan yang lebih tinggi dibandingkan Secure FTP. Selain itu, pada aspek performansi, meskipun Secure FTP unggul pada performansi single transfer namun pada pengujian lain, FTPS mempunyai hasil yang lebih baik dibanding Secure FTP. Dari pengujian kedua aspek tersebut, dapat disimpulkan bahwa FTPS mempunyai kemampuan lebih baik daripada Secure FTP baik dari segi keamanan maupun performansi.

Kata Kunci : keamanan, performansi, FTP, Secure FTP, FTPS

Abstract

File Transfer Protocol or FTP is a protocol used to exchange files, either file upload or file download. Unfortunately, FTP still leaves a security hole where the transmitted data over that two channels can still be read clearly. In addition, the absence of a server authentication mechanism, make the client can access the FTP server at risk for false.

This study tested the Secure FTP and FTPS, both methods which are applied to the FTP security to address the security gaps left by FTP. Security aspects tested include confidentiality (data confidentiality) and authentication (authentication). In addition, this study also tested both methods in terms of performance. Performance aspects tested include delay, throughput, and utilities of CPU and memory on a single file transfers and multiple transfers, and also to the complexity of the use of both methods.

From the test results, obtained a conclusion that the FTPS has a higher security level than the Secure FTP. In addition,on the performance, though superior to the Secure FTP in single file transfers but on the other tests, FTPS have better results than the Secure FTP. From these two aspects of testing, we can conclude that the FTPS have better abilities than Secure FTP in terms of both security and performance.

Keywords : security, performance, FTP, Secure FTP, FTPS

---

1. Pendahuluan

1.1 Latar belakang

File Transfer Protocol atau FTP adalah protokol client-server yang digunakan untuk pertukaran file antara client dengan server [18]. FTP banyak diterapkan di perusahaan atau institusi untuk keperluan distribusi file-file penting mereka. FTP server ini umumnya dipakai untuk menyimpan laporan-laporan seperti laporan keuangan, data-data pegawai, dan laporan aset yang lain. FTP banyak digemari karena instalasi dan konfigurasinya yang mudah.

Tetapi dibalik itu, FTP juga meninggalkan lubang keamanan yang sangat terbuka lebar. FTP yang menggunakan dua *port* (jalur) untuk pertukaran informasi, yaitu *control port* (jalur kontrol) dan *data port* (jalur data), mengirimkan informasi antara client dan server pada kedua port secara *plain* dan tanpa *enkripsi* sama sekali [2]. Tidak ada mekanisme pengamanan data pada FTP sehingga rentan terhadap usaha pencurian data.Inilah yang menjadi incaran bagi para *cracker* karena FTP server ini jelas menjadi aset yang berharga bagi perusahaan dengan banyaknya informasi dan file-file penting didalamnya. FTP juga mempunyai autentikasi yang lemah sehingga rentan terhadap serangan *spoofing* [2][18].

Terkait dengan beberapa aspek keamanan seperti *confidentiality* (kerahasiaan data) dan *authentication* (autentikasi), beberapa metode keamanan telah diujicobakan di FTP server untuk pengamanan data, seperti *FTP over SSL* (FTPS) yang menggunakan SSL (*Secure Socket Layer*) atau Secure FTP yang menggunakan SSH (*Secure Shell*) *tunneling* (FTP over SSH *tunneling*). Secure FTP sendiri merupakan penamaan tidak resmi dari FTP over SSH *tunneling* ini. Masing-masing metode mempunyai keunggulan tersendiri seperti SSL yang memanfaatkan konsep *digital certificate* dan SSH yang dapat mentunnel melalui port SSH dan proses autentikasi yang lebih cepat. Tetapi masing-masing juga mempunyai titik lemah yang akan berpengaruh terhadap performansi FTP. FTPS akan melakukan autentikasi dengan sertifikat digital setiap kali dimulai suatu sesi SSL. Proses autentikasi ini jelas akan mempengaruhi dalam segi performansi. Sedangkan Secure FTP lebih kepada penggunaan *socket* yang berlebih karena setiap data yang mengalir harus melewati SSH terlebih dahulu. Proses enkripsi juga akan mempengaruhi performansi jika dibandingkan dengan FTP biasa.

Pada beberapa literatur disebutkan bahwa FTPS mempunyai keamanan yang lebih baik dibanding Secure FTP dikarenakan FTPS mengenkripsi informasi pada kedua port sedangkan Secure FTP hanya pada satu port [20]. Sayangnya belum ada pengujian resmi terhadap hal tersebut serta aspek performansi terhadap kedua FTP server ini, yang menyangkut waktu upload, waktu download, riil bandwidth atau throughput, kapabilitas server dalam menangani client serta kompleksitas pemakaian oleh client, sehingga belum dapat diketahui performansi dari kedua FTP server. Tugas akhir ini bertujuan membandingkan antara FTPS dengan Secure FTP baik dari segi keamanan maupun performansi. Diharapkan hasil dari tugas akhir ini dapat diajukan acuan dalam memilih metode keamanan yang

terbaik baik dari segi keamanannya maupun performansi yang dihasilkan sebagai FTP server.

1.2 Perumusan Masalah

Permasalahan yang menjadi objek dari penelitian tugas akhir ini, terdiri atas :

1. Bagaimana implementasi Secure FTP dan FTPS terhadap FTP server
2. Bagaimana tingkat keamanan yang diterapkan oleh Secure FTP dan FTPS jika dibandingkan dengan FTP biasa dilihat dari aspek *confidentiality* dan *authentication*
3. Bagaimana performansi yang dihasilkan oleh Secure FTP dan FTPS bila dibandingkan dengan FTP biasa dilihat dari beberapa faktor, seperti: waktu upload, waktu download, throughput dan pemakaian resource untuk single transfer, kapabilitas server serta kompleksitas pemakaian.

Dalam implementasi Tugas Akhir ini, batasan masalah yang diambil adalah:

a) Ketiga FTP server, yakni FTP, Secure FTP dan FTPS, serta SSH server akan diterapkan dalam satu komputer agar tidak ada perbedaan dalam spesifikasi secara *hardware*
b) Semua FTP server menggunakan username dan password sebagai autentikasi bagi client
c) Pengujian dilakukan pada layer aplikasi, sehingga pada penghitungan paket, paket TCP flag tidak ikut dihitung
d) Pengujian kapabilitas server dibatasi hanya lima koneksi secara simultan
e) Pengujian dilakukan di lingkungan jaringan internal, tidak melalui router dan Internet.
f) Pengujian penggunaan resource memori hanya terbatas pada *physical memory* (RAM) saja
g) Model FTPS yang akan digunakan adalah FTPS explicit SSL dengan autentikasi AUTH TLS
h) Proses sniffing dilakukan di node server dikarenakan keterbatasan alat
i) Aspek authentication yang diuji hanya autentikasi server, tidak ada pengujian autentikasi untuk client

1.3 Tujuan

Tujuan yang ingin dicapai dalam tugas akhir ini yakni :

1. Implementasi metode keamanan Secure FTP dan FTPS pada FTP server
2. Menguji dan membandingkan tingkat keamanan ketiga FTP server, yakni FTP, Secure FTP dan FTPS, ditinjau dari aspek *confidentiality* dan *authentication*
3. Menguji dan membandingkan performansi ketiga FTP server, yakni FTP, Secure FTP, FTPS dalam melayani client diukur dari beberapa parameter yaitu waktu upload, waktu download, throughput dan pemakaian resource untuk single transfer, kapabilitas server dan kompleksitas pemakaian

Hipotesis sementara yang dapat diambil berdasarkan studi literatur awal adalah:

1. FTPS mempunyai keamanan lebih baik dari segi confidentiality karena kedua jalur pada FTP,jalur data dan kontrol, terenkripsi. Secure FTP hanya dapat mentunnel jalur kontrol saja.

2. FTPS juga mempunyai keamanan lebih baik dari segi autentikasi karena ada mekanisme sertifikat digital yang akan mendeteksi adanya perubahan
3. Secure FTP mempunyai performansi single transfer lebih baik dibanding FTPS karena tidak ada proses autentikasi tambahan berupa sertifikat digital di awal dan proses enkripsi di dua port.
4. Kapabilitas FTPS lebih baik karena tidak ada pembukaan socket tambahan (SSH) seperti pada Secure FTP

1.4 Metodologi Penyelesaian Masalah

Metode yang digunakan untuk menyelesaikan Tugas Akhir ini yakni :

a) Studi Literatur, yaitu dengan mempelajari literatur-literatur yang ada sesuai dengan permasalahan meliputi: konsep dari keamanan jaringan (network security), konsep File Transfer Protocol (FTP) serta cara kerjanya, metode keamanan Secure Socket Layer (SSL) dan Secure Shell (SSH) Tunneling, teori implementasi Secure FTP dan FTPS pada FTP server, serta parameter-parameter yang akan diukur dalam pengujian nantinya.
b) Berkonsultasi kepada dosen dan para praktisi yang telah berpengalaman dalam bidang jaringan dan keamanan, meliputi: parameter-parameter tambahan yang dapat mendukung pengujian, model dan topologi yang digunakan serta aplikasi-aplikasi pembantu yang dapat digunakan.
c) Analisis requirement, dengan memperkirakan resource yang akan digunakan dalam implementasi, baik hardware maupun software.
d) Desain pengujian sistem, meliputi:
    a. Membuat desain alur kerja dasar ketiga sistem FTP server.
    b. Membuat desain topologi jaringan untuk tiap aspek pengujian. Desain topologi yang dibuat meliputi topologi pengujian keamanan dan topologi pengujian performansi
e) Uji Coba implementasi dan analisis terhadap sistem, meliputi :
    1. Implementasi sistem dengan menggunakan resource dan batasan masalah yang telah didefinisikan, antara lain:
        a. Pemasangan hardware-hardware sesuai dengan desain arsitektur yang telah dibuat sebelumnya
        b. Implementasi ketiga FTP server, FTP client, dan aplikasi-aplikasi yang terkait
        c. Pembuatan skenario pengujian untuk pengujian keamanan dan performansi
        d. Pengujian dengan menerapkan skenario pengujian dan topologi yang dibuat sebelumnya
    2. Analisis aspek keamanan ketiga FTP server
        a. Pengujian dengan menerapkan skenario pengujian keamanan, antara lain:
            - *Confidentiality*: menggunakan *packet analyzer* yang dijalankan di *node* server untuk melihat paket yang tertangkap.Kondisi yang dilihat adalah berapa prosentase paket FTP yang tidak terenkripsi.
            - *Authentication*: FTP client akan mengakses FTP server yang telah dispoof sebelumnya menggunakan IP spoofing [21].

Parameter yang dilihat adalah apakah client tetap dapat mengakses FTP server tersebut.

3. Analisis aspek performansi ketiga FTP server
   a. Pengujian dengan menerapkan skenario pengujian performansi, antara lain:
      - Upload file tunggal berukuran kecil dan besar. Untuk tiap pengujian akan diukur delay (waktu upload), throughput, serta penggunaan CPU dan memori
      - Download file tunggal berukuran kecil dan besar. Untuk tiap pengujian akan diukur delay (waktu download), throughput, serta penggunaan CPU dan memori
      - Kapabilitas server, menguji kemampuan menerima banyak request koneksi. diukur dengan membuka banyak koneksi dan transfer data (download) secara simultan, kemudian diukur delay (waktu download), throughput, serta penggunaan CPU dan memori [22].
      - Kompleksitas pemakaian oleh client, diukur dari banyak langkah yang dijalankan client, waktu koneksi, dan jumlah paket kontrol. Banyak langkah didefinisikan sebagai kuantisasi usaha (*effort*) yang dijalankan client untuk mengakses server

e) Penyusunan Laporan Tugas Akhir dan Kesimpulan Akhir.
Mengambil kesimpulan dari hasil analisis agar dapat terlihat kekuatan dari FTPS dan Secure FTP baik dari segi keamanan maupun performansi serta mendokumentasikannya dalam bentuk laporan tugas akhir.

5. Penutup

5.1 Kesimpulan

Berdasarkan hasil analisis yang dihasilkan dari pengujian pada penelitian ini, dapat diambil kesimpulan sebagai berikut:

1. Pada pengujian autentikasi, dengan serangan IP spoofing, kedua metode, baik Secure FTP maupun FTPS mampu melakukan autentikasi server dengan baik karena dapat mencegah client mengakses FTP server palsu. Namun pada pengujian *confidentiality* (kerahasiaan data), kelemahan terletak pada Secure FTP yang hanya bisa mentunnel jalur kontrol saja sehingga meninggalkan jalur data dalam keadaan tidak terenekripsi. Sebaliknya, FTPS mengenkrip tidak hanya jalur kontrol saja, melainkan jalur data juga. Efeknya, hanya sangat sedikit dari data-data tersebut yang bisa dibaca. Melihat dari kedua aspek keamanan yaitu *confidentiality* dan *authentication*, FTPS memiliki tingkat keamanan yang lebih baik dibanding Secure FTP
2. Aspek performansi yang diujikan mencakup performansi pada single transfer dan multiple transfer serta kompleksitas pemakaian. Pada pengujian single koneksi (single transfer) Secure FTP mempunyai performansi lebih baik di single transfer melalui delay dan utilitas CPU, namun ketika diterapkan pengujian kapabilitas (multiple transfer), FTPS masih lebih baik khususnya dalam hal pengalokasian memori. Pada pengujian kompleksitas pemakaian FTPS juga lebih unggul dalam hal waktu pembentukan koneksi dan jumlah paket kontrol yang digunakan. Sehingga dapat disimpulkan FTPS juga mempunyai performansi yang lebih baik dibanding Secure FTP

5.2 Saran

Saran-saran yang dapat diambil dari penelitian ini guna penyempurnaan penelitian ini kedepannya antara lain:

1. Salah satu kendala dalam penelitian ini adalah kurangnya perangkat keras dan lingkungan pengujian yang ideal. Penggunaan LAN Hub akan lebih mencerminkan peran attacker dalam pengujian confidentiality. Selain itu, penggunaan beban CPU yang sama, dengan membenchmark CPU hingga 100% utilitas, diharapkan juga dapat melihat perbedaan delay dan throughput yang dihasilkan
2. Diperlukan penelitian keamanan lebih lanjut untuk menangani bentuk-bentuk serangan yang lain yang mungkin terjadi pada FTP selain sniffing dan IP spoofing. Khususnya pada serangan autentikasi, dimana mempunyai banyak varian selain IP spoofing.
3. Disarankan dapat diujicoba metode keamanan lain pada FTP, seperti KEA dengan SKIPJACK yang tertera pada RFC 2228 dan RFC 2773 [15], sehingga dapat dibandingkan metode keamanan yang paling baik untuk FTP.

Daftar Pustaka

[1] *Active FTP vs Passive FTP, A Definitive Explanation.* http://slacksite.com/other/ftp.htmldiakses pada 16 April 2011

[2] Allman, M., Osterman, S. 1999. "FTP Security Considerations". *IETF RFC 2577*

[3] Bellovin, S., 1994. "Firewall-Friendly FTP". *IETF RFC 1579*

[4] Canavan, John E. 2001. *Fundamentals of Network Security.* London: Artech House

[5] Cisco Networking Academy. "Network Security". *CCNA Exploration 4.0: Accessing the WAN.* Bandung: IT Telkom Training Center

[6] *Configuring ProFTPD for FTP over SSH.* 2007. http://www.proftpd.org/docs/howto/SSH.html diakses pada 5 Juni 2011

[7] Cooper, D., Santesson, S., etc. 2008. "Internet X.509 Public Key Infrastrusture and Certificate Revocation List (CRL) Profile". *IETF RFC 5280*

[8] Dierks, T., Rescorla, E. 2008. "The Transport Layer Security Protocol (TLS) Version 1.2". *IETF RFC 5246*

[9] Feit, Sidnie. *TCP/IP: Architecture,Protocols,and Implementation with IPv6 and IP Security Second Edition*. McGraw-Hill

[10] Ford-Hutchinson, P. 2005. "Securing FTP with TLS". *IETF RFC 4217*

[11] *FTP Over SSH Tunnel*. 2009. http://www.ftpgetter.com/ftp-ssh-tunnel.php diakses pada 12 Oktober 2010

[12] Harini, Rahayu D. 2009. *Analisis dan Simulasi Keamanan Jaringan Pada Sistem Network Access Control (NAC).* Bandung: IT Telkom

[13] Harris, J.K., 2008. *Understanding SSL/TLS.* Virginia Tech

[14] Horowitz, M., Lunt, S. 1997. "FTP Security Extensions". *IETF RFC 2228*

[15] Housley, R., Yee, P. 2000. "Encryption using KEA and SKIPJACK". *IETF RFC 2773*

[16] *Kupas Tuntas SSH Tunneling.* http://www.ilmuhacking.com/how-to/kupas-tuntas-ssh-tunneling/ diakses pada 1 Agustus 2011

[17] *Network Eavesdropping.* https://www.owasp.org/index.php/Network_Eavesdropping diakses pada 5 Mei 2011

[18] Postel, J., Reynolds, J. 1985. "File Transfer Protocol (FTP)". *IETF RFC 959*

[19] Schafer, Gunter. *Security In Fixed and Wireless Network.* Wiley

[20] *Securing FTP with SSH.* http://hyperreal.org/info/ssh/ftp.htmldiakses pada 30 Juli 2011

[21] "Spoofing Attack". *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network.* http://newdata.box.sk/bx/hacker/ch28/ch28.htm diakses pada 20 Juni 2011

[22] Srivastava, Anand. 1996. *Performance Analysis of a Linux-based FTP Server.* Kanpur: Indian Institute of Technology

[23] Stevens, W.Richard. 2007. *TCP/IP Illustrated, Volume 1 The Protocols.* Addison-Wesley

[24] Ylonen, T., Lonvick, C. 2006. "The Secure Shell (SSH) Authentication Protocol". *IETF RFC 4252*

[25] Ylonen, T., Lonvick, C. 2006. “The Secure Shell (SSH) Connection Protocol”. *IETF RFC 4254*
[26] Ylonen, T., Lonvick, C. 2006. “The Secure Shell (SSH) Protocol Architecture”. *IETF RFC 4251*
[27] Ylonen, T., Lonvick, C. 2006. “The Secure Shell (SSH) Transport Layer Protocol”. *IETF RFC 4253*