PENCEGAHAN SERANGAN *BRUTEFORCE* DAN *SNIFFING* MENGGUNAKAN FAIL2BAN DAN OPENSSL PADA *VERY SECURE FTP DAEMON* (VSFTPD)

LAPORAN SKRIPSI

David Matius
4817050459

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
2021

PENCEGAHAN SERANGAN *BRUTEFORCE* DAN *SNIFFING* MENGGUNAKAN FAIL2BAN DAN OPENSSL PADA *VERY SECURE FTP DAEMON* (VSFTPD)

LAPORAN SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk Memperoleh Gelar Sarjana Terapan

David Matius
4817050459

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
2021

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : David Matius

NIM : 4817050459

Tanggal : 16 Juni 2021

Tanda Tangan :

HALAMAN PENGESAHAN

Skripsi diajukan oleh:

Nama	:	David Matius
NIM	:	4817050459
Program Studi	:	Teknik Multimedia dan Jaringan
Judul Skripsi	:	Pencegahan Serangan *Bruteforce* dan *Sniffing* Menggunakan Fail2ban dan OpenSSL pada *Very Secure FTP Daemon* (VSFTPD)

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Rabu, Tanggal …, Bulan … Tahun 2021 Dan dinyatakan **...**

Disahkan oleh

Pembimbing I : Ayu Rosyida Zain, S.ST, M.T. ( )

Penguji I : Drs. Abdul Aziz, M.M.SI. ( )

Penguji II : Syamsi Dwi Cahya, S.S.T., M.Kom. ( )

Penguji III : Indra Hermawan, S.Kom., M.Kom ( )

Mengetahui:

Jurusan Teknik Informatika dan Komputer

Ketua

Mauldy Laya, S.Kom., M.Kom.

NIP. 197802112009121003

KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa yang telah memberikan berkat dan rahmat sehingga penulis dapat menyelesaikan laporan skripsi yang berjudul Pencegahan Serangan *Bruteforce* dan *Sniffing* Menggunakan Fail2ban dan OpenSSL pada *Very Secure* FTP *Daemon* (VSFTPD). Penulisan laporan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Terapan Politeknik. Dengan rendah hati, penulis sadar bahwa tanpa bantuan dan bimbingan dari berbagai pihak sangatlah sulit bagi penulis untuk menyelesaikan laporan skripsi. Oleh karena itu, penulis mengucapkan terima kasih kepada:

a. Ayu Rosida Zain, S.ST, M.T., selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penyusunan laporan skripsi ini;
b. Dosen TIK PNJ, CCIT FTUI, CISCO yang telah memberikan ilmu dan bimbingannya sehingga penulis dapat mengerjakan skripsi ini;
c. Orang tua penulis yang telah memberikan bantuan dukungan moral dan material;
d. Yohana Rut Debora dan Novita Dogarmu sebagai kakak yang telah menyemangati penulis;
e. Tabitha Mellinia yang telah memberikan semangat dan dukungan.
f. Sahabat dari grup “Lighthouse Hahahihi”, “Bismillah”, dan “Moe-Moe” yang telah memberikan semangat;

Akhir kata, penulis berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga laporan skripsi ini membawa manfaat bagi pengembangan ilmu.

Depok, 16 Juni 2021

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya yang bertanda tangan dibawah ini :

Nama	: David Matius
NIM	: 4817050459
Program Studi	: Teknik Multimedia dan Jaringan
Jurusan	: Teknik Informatika dan Komputer
Jenis Karya	: Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul :

Pencegahan Serangan Bruteforce dan Sniffing Menggunakan Fail2ban dan OpenSSL pada Very Secure FTP Daemon (VSFTPD)

Dengan Hak Bebas Royalti Noneksklusif ini Politeknik Negeri Jakarta berhak menyimpan, mengalih media/format-kan, mengelola dalam bentuk pangkalan data (*database)*, merawat, dan mempublikasikan skripsi saya selama tetap mencamtumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok, Jawa Barat Pada tanggal : 16 Juni 2021

Yang Menyatakan

(David Matius)

Pencegahan Serangan Bruteforce dan Sniffing Menggunakan Fail2ban dan OpenSSL pada Very Secure FTP Daemon (VSFTPD)

ABSTRAK

Perkembangan *Information Technology* (IT) di dunia terus mengalami percepatan. Dengan adanya teknologi IT, banyak masalah yang dapat diselesaikan dengan waktu yang sangat singkat. Salah satunya adalah mengambil data dari *server* ke dalam komputer. Ada banyak cara bagi setiap orang untuk dapat mengambil beberapa data yang diinginkan dari suatu *server*, salah satunya adalah dengan menggunakan *File Transfer Protocol* (FTP). Dalam memberikan sebuah pengamanan terhadap FTP *Server* menggunakan VSFTPD ini digunakan beberapa *tools* seperti Fail2Ban yang akan dilakukan sebagai pengamanan FTP *Server* terhadap serangan *Bruteforce* serta menggunakan OpenSSL untuk memproteksi FTP *server* VSFTPD pada serangan *Sniffing* dengan tujuan untuk merekomendasikan penerapan keamanan dengan beberapa *tools* tersebut agar terciptanya sebuah keamanan pada FTP *Server*. Metode yang dilakukan pada penelitian kali ini adalah melakukan *penetration testing* pada VSFTPD yang berfungsi untuk mengetahui apakah langkah-langkah preventif yang dilakukan dengan mengkonfigurasi VSFTPD menggunakan Fail2Ban dan OpenSSL dapat memberikan keamanan ekstra terhadap pengguna VSFTPD dari serangan *bruteforce* dan *sniffing*. Dalam melakukan pengamanan terhadap VSFTPD dari serangan seperti *bruteforce* dan *sniffing* menggunakan *tools* Fail2Ban dan OpenSSL ini menunjukkan bahwa penggunaan kedua *tools* tersebut dapat mencegah serangan *bruteforce* dari tiga *tools bruteforce* dan mencegah serangan *sniffing* dari dua *tools sniffing* saat dilakukan pada VSFTPD.

Kata kunci : FTP, *Bruteforce, Sniffing*, OpenSSL, Fail2Ban, VSFTPD

Pencegahan Serangan Bruteforce dan Sniffing Menggunakan Fail2ban dan OpenSSL pada Very Secure FTP Daemon (VSFTPD)

ABSTRACT

The development of Information Technology (IT) in the world continues to accelerate. With IT technology, many problems can be solved in a very short time. One of them is to retrieve data from the server into the computer. There are many ways for anyone to be able to retrieve some desired data from a server, one of which is by using File Transfer Protocol (FTP). In providing a security for the FTP Server using VSFTPD, several tools are used, such as Fail2Ban which will be used as a security for the FTP Server against Bruteforce attacks and using OpenSSL to protect the VSFTPD FTP server against Sniffing attacks with the aim of recommending the application of security with these tools in order to create security on FTP Servers. The method used in this study is to perform penetration testing on VSFTPD which serves to determine whether the preventive steps taken by configuring VSFTPD using Fail2Ban and OpenSSL can provide extra security to VSFTPD users from bruteforce and sniffing attacks. In protecting VSFTPD from attacks such as bruteforce and sniffing using the Fail2Ban and OpenSSL tools, it shows that the use of these two tools can prevent bruteforce attacks from the three bruteforce tools and prevent sniffing attacks from the two sniffing tools when performed on VSFTPD.

***Keywords**:* FTP, *Bruteforce*, *Sniffing*, OpenSSL, Fail2Ban, VSFTPD

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan Information Technology (IT) di dunia terus mengalami percepatan. Dengan adanya teknologi IT, banyak masalah yang dapat diselesaikan dengan waktu yang sangat singkat. Salah satunya adalah mengambil data dari server ke dalam komputer. Ada banyak cara bagi setiap orang untuk dapat mengambil beberapa data yang diinginkan dari suatu server, salah satunya adalah dengan menggunakan File Transfer Protocol (FTP). File Transfer Protocol (FTP) merupakan jenis sistem yang menghubungkan hak pengakses (client) dan penyedia (server) dalam melakukan pertukaran data yang melewati port 21 yang banyak digunakan dalam melakukan pertukaran data di internet (BAKTI, 2021). Terdapat banyak penyedia aplikasi server FTP yang dapat digunakan, salah satunya yaitu Very Secure FTP Daemon (VSFTPD). VSFTPD atau "Very Secure FTP Daemon" sendiri merupakan server FTP untuk sistem UNIX, termasuk Linux.

Meski FTP dilindungi dengan beberapa keamanan seperti username dan password, bukan berarti FTP bisa aman dari berbagai percobaan peretasan. Ada beberapa cara untuk melakukan peretasan terhadap FTP seperti yang dikutip oleh (nusanet, 2017) yaitu serangan sniffing dan bruteforce merupakan jenis serangan yang sering dilakukan oleh penyerang dalam melakukan serangan pada FTP server. Kedua serangan tersebut dapat dilakukan pada FTP dikarenakan secara default, FTP tidak melakukan pengamanan terhadap data yang dikirimkan melalui lalu lintas jaringan, hal ini berhubungan dengan konsep sniffing yang dapat digunakan untuk menangkap semua aktifitas yang berada pada lalu lintas jaringan pada FTP. Selain itu juga FTP tidak memberikan batasan kesalahan akses pada FTP client yang mengakibatkan serangan bruteforce dapat digunakan untuk melakukan percobaan akses masuk dengan basis data yang telah diisikan kemungkinan kata sandi pada server.

Oleh karena kerentanan FTP *server* terhadap serangan tersebut, dalam mencegah serangan *bruteforce* terdapat sebuah *tools* yang dapat mendeteksi serangan

bruteforce yaitu Fail2ban (Unixmen, 2020) serta dibutuhkan juga sebuah *tools* yang dapat mengenkripsi setiap pertukaran data pada jaringan saat melakukan transfer sebuah data menggunakan FTP salah satunya yaitu menggunakan OpenSSL (Devi Ruwaida, 2018). Dengan menggunakan Fail2ban, setiap kesalahan akses yang dilakukan oleh FTP *client* pada FTP *server* akan dibatasi serta setiap pertukaran data pada lalu lintas jaringan akan terenkripsi oleh konfigurasi OpenSSL pada VSFTPD. Pada penelitian sebelumnya hanya membahas keamanan dari serangan *bruteforce* menggunakan Fail2ban yang digunakan pada ProFTPd tanpa menggunakan OpenSSL serta meneliti keamanan OpenSSL pada ProFTPd dan tidak menggunakan keamanan dari serangan *bruteforce* dengan Fail2ban. Perbedaan penelitian ini dengan yang dilakukan sebelumnya terletak pada penggunaan aplikasi *server* FTP serta menggabungkan kombinasi keamanan pada satu *server* FTP yaitu VSFTPD menggunakan Fail2ban dan OpenSSL secara bersamaan.

1.2 Perumusan Masalah

Perumusan masalah yang terdapat pada Pencegahan Serangan *Bruteforce* dan *Sniffing* Menggunakan Fail2Ban dan OpenSSL pada *Very Secure* FTP *Daemon* (VSFTPD) adalah:

a. Bagaimana Fail2ban dapat melakukan pengamanan terhadap bruteforce.
b. Bagaimana OpenSSL dapat melakukan pengamanan terhadap bruteforce.
c. Bagaimana kinerja Fail2ban dan OpenSSL dalam melakukan serangan *bruteforce* dan *sniffing*.

1.3 Batasan Masalah

Batasan masalah yang ditentukan dalam Pencegahan Serangan *Bruteforce* dan *Sniffing* Menggunakan Fail2Ban dan OpenSSL pada *Very Secure* FTP *Daemon* (VSFTPD) adalah sebagai berikut :

a. Menggunakan OS Ubuntu 18.04 dan Trisquel 8.0 dalam melakukan penelitian ini.
b. Menggunakan NMAP v7.01 dalam melakukan *scanning port* yang terbuka.
c. Menggunakan FTP *Server* sebagai tujuan dilakukan serangan. FTP *Server* yang digunakan yaitu *Very Secure FTP Daemon* (VSFTPD) v3.0.3.

d. Menggunakan IPTABLES v1.6.1 dalam memberikan izin *port* 21 untuk diaktifkan.

e. *Tools* yang digunakan dalam melakukan serangan yaitu Medusa v2.2_rc3, Metasploit v6.0.38-dev- serta Hydra v8.1 dalam melakukan serangan *Bruteforce* dan Wireshark v2.6 serta tcpdump v4.9.3 dalam melakukan serangan *Sniffing*.

f. *Tools* yang digunakan dalam melakukan pengamanan adalah Fail2ban v0.10.2 untuk melakukan pengamanan dari serangan *bruteforce* dan OpenSSL v1.1.1 untuk melakukan pengamanan dari serangan *sniffing*.

g. Menggunakan satu FTP *client* dalam melakukan pengujian terhadap FTP *server*

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Tujuan dari penelitian ini adalah melakukan implementasi pengamanan menggunakan Fail2ban dan OpenSSL terhadap serangan *bruteforce* dan *sniffing*.

1.4.2 Manfaat

Manfaat dari Pencegahan Serangan Bruteforce dan Sniffing Menggunakan Fail2Ban dan OpenSSL pada Very Secure FTP Daemon (VSFTPD) adalah dapat memberikan metode pengamanan tambahan terhadap FTP *Server* dari upaya penyadapan dengan teknik *Bruteforce* dan *Sniffing* bagi pengguna FTP *Server*.

1.5 Metode Pelaksanaan

Penelitian ini dilakukan dengan metode sebagai berikut:

1) Studi Literatur

Pada tahapan ini dilakukan pengumpulan informasi-informasi terkait dengan VSFTPD, Serangan Bruteforce dan Sniffing.

2) Perancangan Desain Sistem

Tahapan ini merupakan tahapan dimana penulis merancang desain sistem yang akan digunakan sebagai penelitian, yaitu Sistem Operasi Ubuntu 18.04 dan Trisquel 8.0 serta sistem VSFTPD yang akan dikonfigurasikan dengan keamanan menggunakan Fail2ban dan OpenSSL.

3) Implementasi Desain Sistem

Dalam tahapan ini dilakukan sebuah implementasi dari desain sistem yang dibuat dengan melakukan konfigurasi keamanan Fail2Ban beserta OpenSSL terhadap FTP *Server* yaitu VSFTPD.

4) Pengujian Sistem

Dalam tahapan ini dilakukan serangan *Bruteforce* dan *Sniffing* terhadap target yaitu FTP *Server* (VSFTPD) menggunakan tiga *tools bruteforce* dan dua *tools sniffing* yang berbeda. Saat dilakukan kedua serangan tersebut, FTP *Server* (VSFTPD) dalam keadaan sebelum dan sesudah terkonfigurasi keamanannya oleh Fail2Ban dan OpenSSL, sebelum dan sesudah terkonfigurasi hanya menggunakan Fail2ban, sebelum serta sebelum dan sesudah terkonfigurasi hanya OpenSSL.

5) Pengambilan Data

Tahapan ini merupakan tahap dimana penulis melakukan pengambilan data terhadap setiap kejadian saat dilakukannya serangan *bruteforce* dan *sniffing*.

6) Penyusunan Laporan Penelitian

Melakukan penyusunan laporan sesuai dengan pedoman yang telah ditetapkan oleh panitia skripsi Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta dan melakukan bimbingan kepada dosen pembimbing dan mendokumentasikan pengerjaan dalam bentuk foto, video, ataupun media lain yang dapat dijadikan dokumentasi.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang berjudul "Pencegahan Serangan Bruteforce dan Sniffing Menggunakan Fail2ban dan OpenSSL pada Very Secure FTP Daemon (VSFTPD)" dapat disimpulkan bahwa Implementasi pengamanan yang hanya menggunakan Fail2ban tanpa pengamanan OpenSSL pada VSFTPD berhasil mencegahan serangan bruteforce dari tools bruteforce yaitu Medusa, Metasploit, serta Hydra akan tetapi username dan kata sandi tetap terlihat saat serangan sniffing menggunakan tools Wireshark dan tcpdump dilakukan. Saat dilakukan implementasi pengamanan OpenSSL tanpa Fail2ban berhasil mengenkripsi semua data informasi yang terdapat pada lalu lintas jaringan saat dilakukannya pertukaran informasi dari FTP client dan server. Selain itu dengan konfigurasi OpenSSL serangan bruteforce yang dilakukan oleh dua tools bruteforce seperti Metasploit dan Hydra juga berhasil dicegah dikarenakan scanner FTP client pada Metasploit dan Hydra tidak mendukung TLS/SSL namun pada tools bruteforce menggunakan Medusa dapat berhasil dilakukan karena scanner FTP client yang dimiliki oleh Medusa mendukung koneksi aman TLS/SSL. Hal ini menunjukkan saat konfigurasi Fail2ban dan OpenSSL diaktifkan secara bersamaan dari setiap data percobaan serangan yang dilakukan menggunakan 3 tools bruteforce dan 2 tools sniffing terbukti bisa dapat mencegah serangan serangan tersebut.

5.2 Saran

Berdasarkan hasil penelitian ini, bisa dilakukan beberapa peningkatan yang dapat diimplementasikan, berikut di antaranya.

1. Melakukan pengujian terhadap enkripsi yang diberikan OpenSSL dalam melakukan pengamanan kepada FTP *server*.
2. Membuat *tools* serangan *bruteforce* yang mendukung koneksi aman TLS/SSL serta dapat melakukan pemindaian tipe enkripsi untuk pengujian terhadap *server* yang memiliki keamanan serupa yang lebih maju.

DAFTAR PUSTAKA

BAKTI. (2021). *MENGULAS SEPUTAR FTP SERVER: PENGERTIAN, FUNGSI, SERTA KELEBIHAN DAN KEKURANGANNYA*. Retrieved June 03, 2021, from https://www.baktikominfo.id/en/informasi/pengetahuan/mengulas_seputar_ftp_server_pengertian_fungsi_serta_kelebihan_dan_kekurangannya-678#:~:text=FTP%20Server%20atau%20File%20Transfer,banyak%20digunakan%20dalam%20jaringan%20internet.

Chanil-Park, H.-K. J.-O.-J.-Y.-H.-W. (2019). Analysis of the Noise Source Entropy Used in OpenSSL's Random Number Generation Mechanism. *IEEE*(OpenSSL), 59.

Devi Ruwaida, D. K. (2018). RANCANG BANGUN FILE TRANSFER PROTOCOL (FTP) DENGAN PENGAMANAN OPEN SSL PADA JARINGAN VPN MIKROTIK DI SMKS DWIWARNA. *CESS (Journal of Computer Engineering System and Science)*, 45.

Fail2ban. (2021). *Fail2ban:General disclaimer*. Retrieved May 19, 2021, from https://www.fail2ban.org/wiki/index.php/Fail2ban:General_disclaimer

foofus. (2016). *Medusa Parallel Network Login Auditor*. Retrieved June 03, 2021, from http://foofus.net/goons/jmk/medusa/medusa.html

Harjono, E. B. (2016). Analisa Dan Implementasi Dalam Membangun Sistem Operasi Linux Menggunakan Metode LSF Dan REMASTER. *SinkrOn, 1* (Membangun Sistem Operasi Linux), 31.

Hayati, D. D. (2020). Pengembangan Aplikasi Sistem Informasi Smart Register Online Berbasis Android Menggunakan Algoritma BruteForce. *EDUMATIC, 4*, 49.

Liren, M. (2018). *Kajian Software Penyadap: Sniffing*. Retrieved May 20, 2021, from https://cbn.ac.id/my/blog/view/265/kajian-software-penyadap-sniffing

NMAP. (2021). *https://nmap.org/*. Retrieved June 03, 2021, from https://nmap.org/

nusanet. (2017). *Apa itu FTP? Pengertian, Kelebihan, Kekurangan dan Cara Kerjanya*. Retrieved June 04, 2021, from https://bali.nusa.net.id/apa-itu-ftp-pengertian-kelebihan-kekurangan-dan-cara-kerjanya/

RAMADHAN, B. F. (2016). *Crack Web Based Login Page With Hydra in Kali Linux*. Retrieved June 03, 2021, from https://linuxhint.com/crack-web-based-login-page-with-hydra-in-kali-linux/

Security, O. (2021). *INTRODUCTION TO METASPLOIT*. Retrieved June 03, 2021, from https://www.offensive-security.com/metasploit-unleashed/introduction/

SOURCEFORGE. (2021). *FileZilla*. Retrieved May 20, 2021, from https://sourceforge.net/projects/filezilla/

tcpdump. (2021). *Man page of TCPDUMP*. Retrieved June 03, 2021, from https://www.tcpdump.org/manpages/tcpdump.1.html

Trisquel. (2021). *What is Trisquel?* Retrieved May 19, 2021, from https://trisquel.info/en/wiki/documentation

Ubuntu. (2021). *The story of Ubuntu*. Retrieved May 19, 2021, from https://ubuntu.com/about

Unixmen. (2020, June 18). *Prevent Brute Force Attacks Using These Tools*. Retrieved from Unixmen: https://www.unixmen.com/prevent-brute-force-attacks-using-these-tools/

VSFTPD. (2021). *About vsftpd*. Retrieved May 20, 2021, from https://security.appspot.com/vsftpd.html#about

Wireshark. (2021). *About Wireshark*. Retrieved May 20, 2021, from https://www.wireshark.org/

Zulkarnain. (2020). Analisis Keamanan FTP server Menggunakan Serangan Man-In-The-Middle Attack. *TELCOMATICS, 5*(Keamanan FTP Server), 12-13.

LAMPIRAN

DAFTAR RIWAYAT HIDUP

Lahir di Bekasi, 15 Maret 2000. Lulus dari SDN Wanasari 01 pada tahun 2011, SMPN 02 Cikarang Timur pada tahun 2014, SMAN 03 Cikarang Utara pada tahun 2017 dan Diploma II program studi *Network Administrator Professional* di CCIT-FTUI pada tahun 2019. Saat ini sedang menempuh pendidikan Diploma IV Program Studi Teknik Multimedia dan Komputetr Jurusan Teknik Informatika dan Komputer di Politeknik Negeri Jakarta.

Lampiran 2 *Screenshot* instalasi *tools* pada *server*

```
ubuntu@ubuntu-HP-Pavilion-g4-Notebook-PC:~$ sudo apt install fail2ban
[sudo] password for ubuntu:
Reading package lists... Done
Building dependency tree
Reading state information... Done
fail2ban is already the newest version (0.10.2-2).
0 upgraded, 0 newly installed, 0 to remove and 272 not upgraded.
```

```
ubuntu@ubuntu-HP-Pavilion-g4-Notebook-PC:~$ sudo apt install vsftpd
Reading package lists... Done
Building dependency tree
Reading state information... Done
vsftpd is already the newest version (3.0.3-9build1).
0 upgraded, 0 newly installed, 0 to remove and 272 not upgraded.
```

```
ubuntu@ubuntu-HP-Pavilion-g4-Notebook-PC:~$ sudo apt install fail2ban
Reading package lists... Done
Building dependency tree
Reading state information... Done
fail2ban is already the newest version (0.10.2-2).
0 upgraded, 0 newly installed, 0 to remove and 272 not upgraded.
```

```
ubuntu@ubuntu-HP-Pavilion-g4-Notebook-PC:~$ sudo apt install iptables
Reading package lists... Done
Building dependency tree
Reading state information... Done
iptables is already the newest version (1.6.1-2ubuntu2).
```

Lampiran 3 *Screenshot* instalasi *tools* pada *client*

```
vidius@vidius-Compaq-435-Notebook-PC:~$ sudo apt install vsftpd
[sudo] password for vidius:
Reading package lists... Done
Building dependency tree
Reading state information... Done
vsftpd is already the newest version (3.0.3-3ubuntu2).
The following packages were automatically installed and are no longer required:
  apt-clone archdetect-deb dpkg-repack gir1.2-appindicator3-0.1
  gir1.2-json-1.0 gir1.2-networkmanager-1.0 gir1.2-nma-1.0
  gir1.2-timezonemap-1.0 gir1.2-xkl-1.0 libatkmm-1.6-1v5 libcairomm-1.0-1v5
  libdebian-installer4 libglibmm-2.4-1v5 libgtkmm-2.4-1v5 libpangomm-1.4-1v5
  libparted-fs-resize0 libtimezonemap-data libtimezonemap1 python3-gi-cairo
  python3-icu python3-pam sbsigntool
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 122 not upgraded.
```

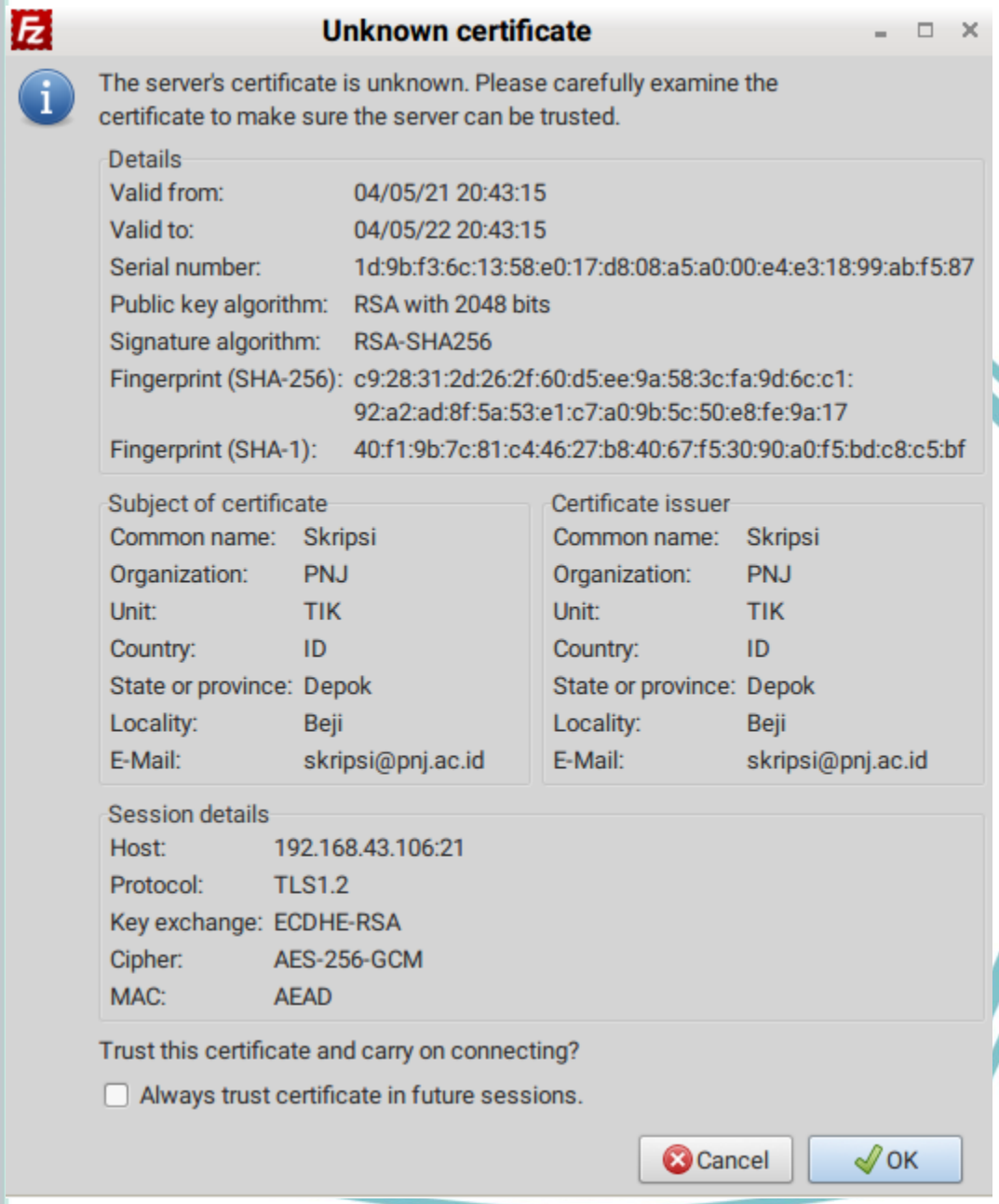
```
vidius@vidius-Compaq-435-Notebook-PC:~$ sudo apt install wireshark
Reading package lists... Done
Building dependency tree
Reading state information... Done
wireshark is already the newest version (2.6.10-1~ubuntu16.04.0).
The following packages were automatically installed and are no longer required:
  apt-clone archdetect-deb dpkg-repack gir1.2-appindicator3-0.1
  gir1.2-json-1.0 gir1.2-networkmanager-1.0 gir1.2-nma-1.0
  gir1.2-timezonemap-1.0 gir1.2-xkl-1.0 libatkmm-1.6-1v5 libcairomm-1.0-1v5
  libdebian-installer4 libglibmm-2.4-1v5 libgtkmm-2.4-1v5 libpangomm-1.4-1v5
  libparted-fs-resize0 libtimezonemap-data libtimezonemap1 python3-gi-cairo
  python3-icu python3-pam sbsigntool
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 122 not upgraded.
```

```
vidius@vidius-Compaq-435-Notebook-PC:~$ sudo apt install tcpdump
Reading package lists... Done
Building dependency tree
Reading state information... Done
tcpdump is already the newest version (4.9.3-0ubuntu0.16.04.1).
The following packages were automatically installed and are no longer required:
  apt-clone archdetect-deb dpkg-repack gir1.2-appindicator3-0.1
  gir1.2-json-1.0 gir1.2-networkmanager-1.0 gir1.2-nma-1.0
  gir1.2-timezonemap-1.0 gir1.2-xkl-1.0 libatkmm-1.6-1v5 libcairomm-1.0-1v5
  libdebian-installer4 libglibmm-2.4-1v5 libgtkmm-2.4-1v5 libpangomm-1.4-1v5
  libparted-fs-resize0 libtimezonemap-data libtimezonemap1 python3-gi-cairo
  python3-icu python3-pam sbsigntool
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 122 not upgraded.
```

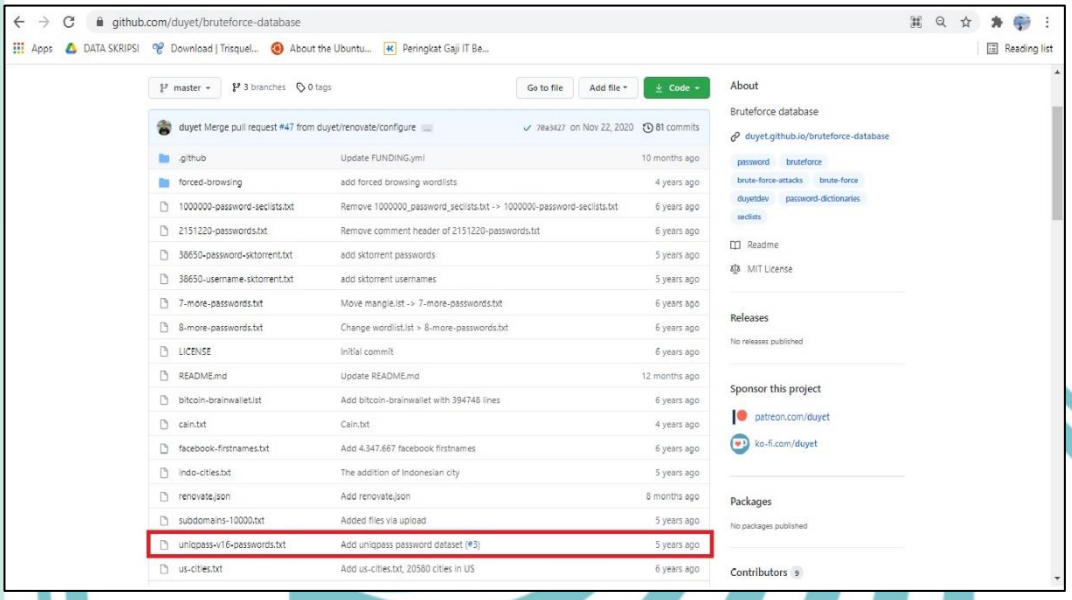
```
vidius@vidius-Compaq-435-Notebook-PC:~$ sudo apt install metasploit-framework
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  apt-clone archdetect-deb dpkg-repack gir1.2-appindicator3-0.1
  gir1.2-json-1.0 gir1.2-networkmanager-1.0 gir1.2-nma-1.0
  gir1.2-timezonemap-1.0 gir1.2-xkl-1.0 libatkmm-1.6-1v5 libcairomm-1.0-1v5
  libdebian-installer4 libglibmm-2.4-1v5 libgtkmm-2.4-1v5 libpangomm-1.4-1v5
  libparted-fs-resize0 libtimezonemap-data libtimezonemap1 python3-gi-cairo
```

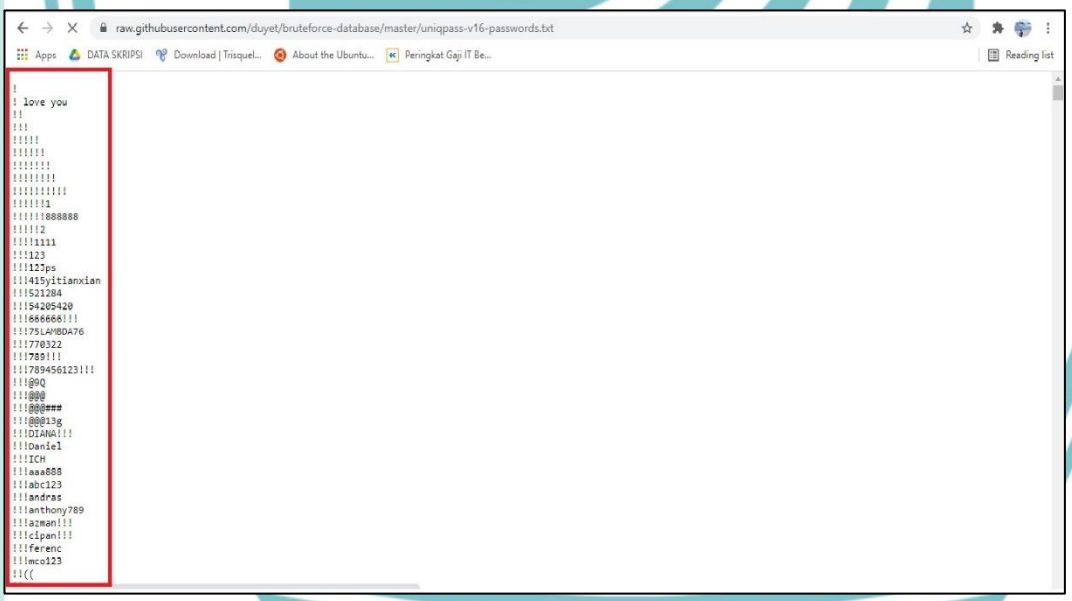
```
vidius@vidius-Compaq-435-Notebook-PC:~$ sudo apt install hydra
Reading package lists... Done
Building dependency tree
Reading state information... Done
hydra is already the newest version (8.1-1build2).
The following packages were automatically installed and are no longer required:
  apt-clone archdetect-deb dpkg-repack gir1.2-appindicator3-0.1
  gir1.2-json-1.0 gir1.2-networkmanager-1.0 gir1.2-nma-1.0
  gir1.2-timezonemap-1.0 gir1.2-xkl-1.0 libatkmm-1.6-1v5 libcairomm-1.0-1v5
  libdebian-installer4 libglibmm-2.4-1v5 libgtkmm-2.4-1v5 libpangomm-1.4-1v5
  libparted-fs-resize0 libtimezonemap-data libtimezonemap1 python3-gi-cairo
  python3-icu python3-pam sbsigntool
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 122 not upgraded.
```

Lampiran 4 Informasi SSL yang terhubung VSFTPD di FileZilla



Lampiran 5 Referensi pengambilan basis data kata sandi *bruteforce*





Sumber: https://github.com/duyet/bruteforce-database

Lampiran 6 Konfigurasi *default* VSFTPD