OPTIMASI KEAMANAN JARINGAN TERHADAP SERANGAN *BOTNET*

(Studi Kasus Serangan DNS *Poisoning* Pada DNS *Server*)

Skripsi

untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Teknik Informatika

disusun oleh :

Faizal Indrarukmana

10651032

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2014

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-07/R0

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : UIN.02/D.ST/PP.01.1/3264/2014

Skripsi/Tugas Akhir dengan judul : Optimasi Keamanan Jaringan Terhadap Serangan *Botnet* (Studi Kasus Serangan DNS *Poisoning* Pada DNS *Server*)

Yang dipersiapkan dan disusun oleh :
Nama : Faizal Indrarukmana
NIM : 10651032
Telah dimunaqasyahkan pada : Jum'at, 24 Oktober 2014
Nilai Munaqasyah : A -
Dan dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga

TIM MUNAQASYAH :

Ketua Sidang

Dr. Imam Riadi, M.Kom
NIY. 60020397

Penguji I

Sumarsono, M.Kom
NIP.19710209 200501 1 003

Penguji II

Nurochman, M.Kom
NIP. 19801223 200901 1 007

Yogyakarta, 30 Oktober 2014
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

Prof. Drs. H. Akh. Minhaji, M.A, Ph.D
NIP. 19580919 198603 1 002

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi
Lamp : 1 Bendel Laporan Skripsi

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Faizal Indrarukmana
NIM : 10651032
Judul Skripsi : Optimasi Keamanan Jaringan Terhadap Serangan *Botnet* (Studi Kasus Serangan DNS *Poisoning* Pada DNS *Server*)

Sudah dapat diajukan kembali kepada Program Studi Teknik Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Prodi Teknik Informatika

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqsyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 9 September 2014
Pembimbing

Imam Riadi, M.Kom
NIY. 60020397

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini:

Nama	: Faizal Indrarukmana
NIM	: 10651032
Program Studi	: Teknik Informatika
Fakultas	: Sains dan Teknologi

Menyatakan bahwa skripsi dengan judul **"Optimasi Keamanan Jaringan Terhadap Serangan *Botnet* (Studi Kasus Serangan DNS *Poisoning* Pada DNS *Server*)"** tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

.

Yogyakarta, 9 September 2014

Yang menyatakan

Faizal Indrarukmana
NIM. 10651032

KATA PENGANTAR

Puji syukur kehadirat Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi dengan judul "**Optimasi Keamanan Jaringan Terhadap Serangan *Botnet* (Studi Kasus Serangan DNS *Poisoning* Pada DNS *Server*)**" sebagai salah satu syarat untuk mencapai gelar kesarjanaan pada program studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta. Shalawat serta salam semoga tercurahkan kepada junjungan Nabi Muhammad SAW beserta seluruh keluarga dan sahabat beliau.

Penulis menyadari bahwa yang saya lakukan dalam penyusunan laporan proyek akhir ini masih terlalu jauh dari kata sempurna. Oleh karena itu, saya sangat mengharap kritik dan saran yang berguna dalam penyempurnaan sistem ini dimasa yang datang. Semoga yang telah saya lakukan ini dapat bermanfaat bagi pembaca.

Tak lupa penyusun juga mengucapkan terima kasih kepada pihak-pihak yang telah membantu dalam penyelesaian skripsi ini, baik secara langsung atau tidak langsung. Ucapan terima kasih penyusun sampaikan kepada:

1. Bapak Prof. Dr. H. Musa Asy'arie, M.A., selaku Rektor UIN Sunan Kalijaga Yogyakarta
2. Bapak Prof. Drs. H. Akh. Minhaji, M.A., Ph.D., selaku Dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.

3. Bapak Agus Mulyanto, S.Si., M.Kom., selaku Ketua Program Studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta.
4. Bapak Nurochman, M.Kom., selaku Sekertaris Program Studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta.
5. Bapak M. Mustakim, S.T, selaku Pembimbing Akademik selama masa kuliah.
6. Bapak Dr. Imam Riadi, M.Kom., selaku Dosen Pembimbing yang telah membimbing, memberikan koreksi dan saran kepada penyusun sehingga skripsi ini dapat terselesaikan.
7. Seluruh Dosen Program Studi Teknik Informatika UIN Sunan Kalijaga, terima kasih atas ilmu yang telah diberikan.
8. Ayahanda Agus Gunawan, Ibunda Supatmi tercinta, dan adekku tersayang Diah Ayu Fatmawati, penulis ucapkan terima kasih atas semua yang telah kalian berikan.
9. Teman-teman seperjuangan angkatan 2010 Program Studi Teknik Informatika.
10. Kakak-kakak dan adik-adik angkatan yang sudah memberikan dukungan dan membantu dalam penyelesaian skripsi ini.
11. Semua pihak yang tidak bisa disebutkan satu per satu, terima kasih atas segala bantuannya

Semoga Allah SWT memberikan pahala yang setimpal atas segala dorongan, bantuan, dukungan, semangat dan keyakinan yang sudah diberikan kepada penulis untuk menyelesaikan skripsi ini. Amin.

Yogyakarta, 9 September 2014

Penulis

HALAMAN PERSEMBAHAN

Skripsi / Tugas Akhir ini kupersembahkan kepada :

1. **Bapak Agus Gunawan, Ibu Supatmi yang tercinta, terimakasih atas doa, dukungan, semangat dan semua yang telah diberikan.**
2. **Adekku tersayang Diah Ayu Fatmawati terimakasih atas dukungan dan semangatnya.**
3. **Aniq Noviciatie Ulfah terimaksih selama ini sudah memberikan dukungan, doa dan semangatnya.**
4. **Seluruh dosen Teknik Informatika pak Agus, pak Nurrohman, pak Bambang, pak Sumarsono, pak Aulia, pak Didik, pak Mustakim, pak Agung, bu 'Uyun, bu Maria Ulfah, bu Ade, pak imam terimaksih atas ilmu yang telah diberikan, semoga bermanfaat dikemudian hari.**
5. **Para staff laboratorium, terimakasih dan maaf jika sering merepotkan ?.**
6. **Sahabat-sahabatku #bocahepakimam Fafa, Hanan, Arya, Feri, Fajar, opang yang telah berjuang bersama-sama, sampai setiap hari menginap di lab. Terpadu bersama-sama. Semoga kebersamaan ini senantiasa dieratkan.**
7. **Teman-teman seperjuangan Najib, Cincin, Toni, Fajar, lukman, Fina, Putri, Hafa, Sasti, Siska dan seluruh Keluarga Besar #hasioinside yang gak bisa disebut satu per satu. Terimaksih atas kebersamaan, semangat dan dukungannya.**

8. Teman-teman semua TIF semua angkatan mandiri dan reguler.
9. Teman-teman di PTIPD pak arif, bu ratna, pak hendra, mas gatra, mb amel, mb ayu, mas habibi, mb hajar, mb nova, mba fa,mas haidar, erfan dan yang lainnya yang ga bisa disebut satu persatu.
10. Teman-teman kontrakan suka-suka Bang keelek, Mbah Gendon, Ming Kincling, Ming Firis, Ming Pindi , Awu, Ari, Budi, dan Reza.

HALAMAN MOTTO

Setiap jiwa yang dilahirkan telah tertanam dengan benih untuk mencapai keunggulan hidup. Tetapi benih tidak akan tumbuh seandainya tidak dibajai dengan keberanian.

Tersenyumlah dalam situasi apapun, tanpa disadari senyum itu yang akan menguatkanmu.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR LISTING

DAFTAR SINGKATAN

BIND	:*Berkeley Internet Name Domain*
CD	: *CangeDirectori*
CT	: *Container*
C&C	: *Centralized*
DNS	: *Domain Name System*
DDOS	: *Distributed Denial of Service*
DOS	: *Denial of Service*
FQDN	: *Fany Qualified Domain Name*
FQPN	: *Freight QualitynPartnership Network*
FTP	: *File Transfer Protocol*
GNU	: *General Public License*
HTML	: *Hyper Text Markup Language*
HTTP	: *Hypertext Transfer Protocol*
HTTPS	: *Hypertext Transfer Protocol Secure*
IDS	: *Interuction Detection System*
IETF	: *Internet Engineering Task Force*
IPS	: *Intrusion Prevention System*
IP	: *Internet Protocol*
IPX/SPX	: *Internetwork Packet Exchange/Sequenced Packet Exchange*
IRC	: *Internet Relay Chat*
ISP	: *Internet Service Provider*
KVM	: *Kernel-Based Virtual Machine*
LAN	: *Local Area Network*
MAN	: *Metropolitan Area Network*
NIDS	: *Network Intrusion Detection System*
NOS	: *Network Operating System*
TCP/IP	: *Transmission Control Protocol/Internet Protocol*
P2P	: *Peer to Peer*
PSAD	: *Port Scanner Attack Detector*
RAM	: *Random Access Memory*
RISC	: *Reduced Instruction Set Computing*
SMB	: *Service Message Block*
SSH	: *Secure Shell*
TXT	: *Text*
URL	: *Uniform Resource Locator*
VE	: *Virtual Environtment*
VM	: *Virtual Machine*
VPS	: *Virtual Private Server*
WAN	: *Wide Area Network*

Optimasi Keamanan Jaringan Terhadap Serangan *Botnet* (Studi Kasus Serangan DNS *Poisoning* Pada DNS *Server*)

Faizal Indarukmana
NIM 10651032

INTISARI

Keamanan jaringan pada sistem operasi *Unix* di Internet sangat penting. Berbagai serangan keamanan jaringan muncul untuk hal-hal negatif. Salah satu serangan yang muncul adalah *botnet*. Serangan *botnet* ini dilakukan *attacker* dengan motif finansial ataupun pencurian informasi dengan menyebarkan *Denial of Servise* (DOS), penyebaran *malware*, *phising* dan *Domain Name System* (DNS) *poisoning*. Penggunaan IP publik beresiko diserang jika tidak ada keamanan yang memadai dan belum adanya pengamanan pada DNS *server* yang rentang terhadap serangan DNS *Poisoning*.

Mekanisme pencegahan serangan pada penelitian ini menggunakan *firewall Port Scanner Attack Detector* (PSAD) dan *fwsnort* yang dapat mencegah lalu lintas jaringan tidak aman dan mengijinkan lalu lintas jaringan yang aman. Perancangan jaringannya menggunakan komputer *server* fisik maupun *virtual* yang terhubung ke sebuah *ippublic.* Tahapan penelitian ini yaitu perancangan sistem dan jaringan, implementasi sistem dan pengujian sistem menggunakan *Strees Test*.

Berdasarkan hasil penelitian yang dilakukan terhadap pencegahan serangan DNS *Poisoning* dapat dicegah menggunakan *firewall* PSAD dan *fwsnort* dengan memblokir alamat IP, *port* dan paket yang mencurigakan. Sebagai tampilan GUI nya menggunakan IDS *Snort* dan *Snorby*. Hasil dari pengujian *Strees Test* dapat disimpulkan bahwa performa DNS *server* tetap berjalan normal. Hal ini dibuktikan dengan *presentase* 63.3 % sangat setuju dan 36.7 % setuju terhadap pengujian sistem yang dilakukan.

Kata Kunci : Optimasi, Keamanan, Jaringan, DNS *Poisoning, Botnet*

Optimization of Network Security Attack Againts Botnet (Study Case on DNS Poisoning Attack on the DNS Server)

Faizal Indarukmana
NIM 10651032

ABSTRACT

Unix operating system network security on the internet is very important. Various network security attacks appear to negative effect. One of the attacks that came up was the botnet. This botnet attacks performed by an attacker financial motive or theft of information by spreading Denial of Servise (DOS), the spread of malware, phishing and Domain Name System (DNS) poisoning. The use of public IP risk being attacked if there is no adequate security and the lack of security on the DNS server vulnerable to attack DNS Poisoning.

Attack prevention mechanism in this study using a firewall Port Scanner Attack Detector (PSAD) and fwsnort that can prevent insecure network traffic and allow a secure network traffic. The design of the network uses a physical or virtual server computer that is connected to ip public. Stages of this research is the design of systems and networking, system implementation and system testing using Strees Testing.

Based on the results of research conducted on the prevention of DNS poisoning attacks, DNS poisoning can be prevented using a firewall PSAD and fwsnort by blocking IP addresses, ports and suspicious packages. As its GUI using Snort IDS and Snorby. The results of the testing of Stress Test can be concluded that the performance of the DNS server is still running normally. This is evidenced by the percentage of 63.3% strongly agree and 36.7% agree with the system testing performed.

Keyword : Optimization, Security, Network, DNS *Poisoning*, Botnet

BAB I

PENDAHULUAN

1.1 Latar Belakang

Semakin banyak teknologi yang ada dan penggunaan jaringan komputer pada saat ini, sehingga memungkinkan banyaknya orang yang menyalah gunakannya untuk hal-hal yang negatif. Keamanan jaringan yang sekarang ini sering menjadi incaran para pengguna yang tidak bertanggung jawab untuk mendapatkan keuntungan bagi dirinya maupun orang lain. Banyaknya serangan pada keamanan jaringan membuat *user* merasa tidak nyaman. Serangan ini banyak macamnya salah satuya yaitu *botnet*.

Serangan *botnet* dilakukan *attacker* untuk berbagai macam tidak pidana bermotif finansial maupun pencurian informasi dengan cara penyebaran serangan *Denial of Service*(DoS), penyebaran *malware*, *phising*, dan DNS *Poisoning*. DNS *Cache Poisoning* merupakan sebuah cara untuk menembus pertahanan dengan cara menyampaikan informasi IP *Address* yang salah mengenai sebuah *host*, dengan tujuan untuk mengalihkan lalu lintas paket data dari tujuan yang sebenarnya (Hakim, 2011). Sehingga penggunaan IP publik ini beresiko diserang jika tidak adanya keamanan yang memadai dan belum adanya pengamana pada DNS *server* yang rentang terhadap serangan DNS *Poisoning*.

Attacker bisa membelokkan alamat website dengan menggunakan metode serangan DNS *Poisoning*, yang dapat memberikan *fake information* di *nameserver* yang mengakibatkan *nameserver* menerjemahkan *domain* asli ke dalam ip milik

attacker/penyerang. Penyerang itu sendiri telah menyediakan program *spoofing*. Akibatnya, setiap informasi yang di kirim ke *domain* tersebut akan masuk ke alamat *attacker* dan program *spoofing* yang terpasang telah membantu *attacker* untuk mendapatkan informasi penting seperti *login*, *password* bahkan mungkin data-data rahasia.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, didapat rumusan masalah dalam penelitian ini sebagai berikut :

1. Bagaimana melakukan tindakan pencegahan serangan DNS *Poisoning* pada DNS *Server*?
2. Bagaimana melakukan simulasi serangan DNS *Poisoning* pada DNS *Server*?

1.3 Batasan Masalah

Hal-hal yang dilakukan dalam dalam penelitian ini dibatasi pada masalah yang dibahas, yaitu:

1. Penelitian hanya untuk serangan DNS *Poisoning* pada DNS *Server*.
2. DNS *Server*yang digunakan adalah BIND versi 9.
3. Sistem operasi yang digunakan komputer *server* adalah Ubuntu *Server* versi 12.04
4. Mesin *Server* virtual dibangun diatas *Platform* KVM (*Kernel-Based Virtual Machine*).

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah, Tujuan penelitian ini adalah :

1. Mencegah serangan DNS *Poisoning* pada DNS *Server* menggunakan PSAD (*Port Scanner Attack Detector*) dan *fwsnort.*
2. Melakukan simulasi serangan DNS *Poisoning* pada DNS *Server*.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini, yaitu :

1. Memberikan manfaat bagi *client* untuk berhati-hati dalam menggunakan DNS *server* karena dapat diserang DNS *poisoning* dan diambil informasinya oleh *attacker.*
2. Memeberikan manfaat bagi admin dalam mengkonfigurasi DNS server agar tidak mudah terserang oleh Botnet. Dalam penelitian ini serangan *botnet* berupa serangan DNS.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian yang dilakukan, maka dapat diambil kesimpulan sebagai berikut:

1. Solusi untuk mencegah serangan DNS *Poisoning* dilakukan dengan menggunakan *firewall* PSAD (*Port Scanner Attack Detector*) dan *fwsnort* untuk memblokir IP *address* dan *port* yang mencurigakan dengan IDS *snort* dan Snorby sebagai *security monitoring*.
2. Simulasi dilakukan menggunakan komputer *server*, komputer *client* dan komputer *attacker* yang dihubungkan dengan *Local Area Network*(LAN). Pada simulasi ini telah berhasil melakukan serangan DNS *Poisoning* menggunakan *firewall* PSAD dan *FWSNORT* untuk memblokir alamat IP, *port* dan paket yang mencurigakan.

5.2 Saran

Berdasarkan penelitian yang telah dilakukan, masih membutuhkan saran-saran untuk mendukung kesempurnaan dalam penelitian ini, saran tersebut diantaranya sebagai berikut

1. Kedepannya DNS *Poisoning* dapat dicegah dengan *tools* yang lebih modern dan mudah dipahami oleh *user* yang belum paham.

2. Untuk kedepannya bisa menggunakan DNS *Server* yang lebih bagus untuk menghindari serangan DNS *Poisoning*.

DAFTAR PUSTAKA

Anta, A. P. (2013). *Rancang bangun jaringan lan menggunakan router mikrotik.* Bandung: unikom.

Ardiantoro, D. (2003). *Pengantar DNS (Domain Name System).* IlmuKomputer.Com.

Denny, A. (2012, 12 19). *dennyandryan.blogspot.com*. Retrieved 12 2013, 03, from http://dennyandryan.blogspot.com/2012/12/sejarah-sms.html

Dian, R. W. (2008). *Kerawanan Keamanan Jaringan pada DNS dan BIND.* Palembang: Universitas Sriwijaya.

Gusti, A. P. (2008). *Metode-Metode DNS Attack dan Penanganannya.* Palembang: Universitas Sriwijaya.

Hakim, A. R. (2011, Februari 25). *arief-referee.blogspot.coml*. Retrieved Desember 5, 2013, from http://arief-referee.blogspot.com/2011/02/jenis-jenis-serangan-terhadap-keamanan.html

Komputer, W. (2003). *Konsep jaringan komputer dan pengembangannya.* Jakarta: Salemba Infotek.

Nugraha, A. d. (2011). Botnet Detection Survey. *Seminar Nasional Teknologi Informasi & Komunikasi Terapan 2011 (Semantik 2011)*, 1-3.

Oetomo, B. S. (2003). *Konsep dan perancangan jaringan.* Yogyakarta: Penerbit Andi.

Prayogo, K. (2012). LIBI-Trie: Modifikasi HAT-Trie untuk DNS Suffix. *Gema Aktualita, Vol 1, No 1*, 1.

Pressman, R. S. (2013). *Rekayasa Perangkat Lunak Pendekatan Praktis Buku Satu.* Yogyakarta: 2002.

Rahardjo, B. (2005). *e-Procurement Security.* Bandung: Institut Teknologi Bandung.

Rohman, M. N. (2013). *Implementasi Dan Optimalisasi Switching DNS (Domain Name System) Untuk Filtering Konten Dengan Mikrotik Scheduler.* Yogyakarta: UIN Sunan Kalijaga.

Saha B, G. A. (2005). Botnet: An Overview. *CERT-In White Paper, CIWP-2005-05*.

Sutedjo, B. (2006). *Konsep dan Perancangan Jaringan Komputer* . Yogyakarta: Andi.

Syafrizal, M. (2005). *Pengantar Jaringan Komputer.* Yogyakarta: Penerbit Andi.

Wagito. (2007). *Jaringan Komputer Teori dan Implementasi Berbasis Linux.* Yogyakarta: Gava Media.

Wan, P. (2008, November 26). *wanbule.wordpress.com*. Retrieved Desember 5, 2013, from http://wanbule.wordpress.com/2008/11/26/penyerangan-dengan-menggunakan-dns-poisoning/

Yuan, L., Chen, C.-C., Mohapatra, P., & dkk. (2013). A Proxy View of Quality of Domain Name Service, Poisoning Attacks. *ACM Transactions on Internet Technology*, 12.

LAMPIRAN A

KODE SUMBER (*SOURCE CODE*) KONFIGURASI DNS *SERVER*

BIND9

Nama file : interfaces
Lokasi : DNS *Server* BIND9

```
This file describes the network interfaces available on your
system
#  and  how  to  activate  them.  For  more  information,  see
interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
address 192.168.100.5
netmask 255.255.255.0
network 192.168.100.0
broadcast 192.168.100.255
gateway 192.168.100.1
        # dns-* options are implemented by the resolvconf package,
if installed
dns-nameservers 192.168.100.1
dns-search lab.jarkom.uin
```

Nama file : resolv.conf
Lokasi : DNS *Server* BIND9

```
search lab.jarkom.uin
nameserver 8.8.8.8
```

Nama file : db.1
Lokasi : DNS *Server* BIND9

```
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     lab.jarkom.uin. admin.lab.jarkom.uin. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
604800 )       ; Negative Cache TTL
```

```
;
@       IN      NS      lab.jarkom.uin.
5       IN      PTR     lab.jarkom.uin.
```

Nama file : db.lab.jarkom.uin
Lokasi : DNS*Server* BIND9

```
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     lab.jarkom.uin. admin.lab.jarkom.uin. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800)       ; Negative Cache TTL
;
@       IN      NS      lab.jarkom.uin.
@       IN      A       192.168.100.5
www     IN      A       192.168.100.5
FTP     IN      CNAME   lab.jarkom.uin.
@       IN      AAAA    ::1
```

Nama file : named.conf.local
Lokasi : DNS *Server* BIND9

```
zone "lab.jarkom.uin" {
type master;
file "/etc/bind/db.lab.jarkom.uin";
};
zone "100.168.192.in-addr.arpa" {
type master;
file "/etc/bind/db.1";
};
```

LAMPIRAN B

KODE SUMBER (SOURCE CODE) KONFIGURASI ETTERCAP

Nama File : etter.dns
Lokasi : Ettercap

```
#####################################################################
##########
#
#
#  ettercap -- etter.dns -- host file for dns_spoof plugin
#
#
#
#  Copyright (C) ALoR & NaGA
#
#
#
#  This program is free software; you can redistribute it and/or
modify    #
#  it under the terms of the GNU General Public License as
published by    #
#  the Free Software Foundation; either version 2 of the License,
or       #
#  (at your option) any later version.
#
#
#
#####################################################################
##########
#
#
# Sample hosts file for dns_spoof plugin
#
#
#
# the format is (for A query):
#
#   www.myhostname.com A 168.11.22.33
#
#   *.foo.com          A 168.44.55.66
#
#
#
# or for PTR query:
#
#   www.bar.com A 10.0.0.10
#
#
#
# or for MX query:
#
```

```
#    domain.com MX xxx.xxx.xxx.xxx
#
#
#
# or for WINS query:
#
#    workgroup WINS 127.0.0.1
#
#    PC*       WINS 127.0.0.1
#
#
#
# NOTE: the wildcarded hosts can't be used to poison the PTR
requests      #
#       so if you want to reverse poison you have to specify a
plain       #
#       host. (look at the www.microsoft.com example)
#
#
#
#####################################################################
##########

#########################################################
# www.polito.it --> security.polito.it (130.192.1.8)
#
www.polito.it A 130.192.1.8

################################
# microsoft sucks ;)
# redirect it to www.linux.org
#

microsoft.com      A   198.182.196.56
*.microsoft.com    A   198.182.196.56
www.microsoft.com  PTR 198.182.196.56      # Wildcards in PTR are
not allowed

##########################################
# no one out there can have our domains...
#

www.alor.org  A 127.0.0.1
www.naga.org  A 127.0.0.1

###############################################
# one day we will have our ettercap.org domain
#

www.ettercap.org           A  127.0.0.1
ettercap.sourceforge.net   A  216.136.171.201

###############################################
# some MX examples
#
```

```
alor.org   MX  127.0.0.1
naga.org   MX  127.0.0.1

##############################################
# This messes up NetBIOS clients using DNS
# resolutions. I.e. Windows/Samba file sharing.
#

facebook.com        A      192.168.1.15
*.facebook.com              A      192.168.1.15
www.facebook.com            PTR    192.168.1.15

LAB-PC*  WINS  127.0.0.1

# vim:ts=8:noexpandtab
```

LAMPIRAN C

HASIL FILE TXT DARI SERANGAN DNS *POISONING*

```
Email: izal_suka@gmail.com
Password: aaaaaaaaa
IP Address: 192.168.10.91
Date Submitted: July 24, 2014, 4:25 pm
==========

==========
Email: novi@gmail.com
Password: novi
IP Address: 192.168.10.76
Date Submitted: August 9, 2014, 3:12 am
==========

==========
Email: novi@gmail.com
Password: 123456
IP Address: 192.168.10.76
Date Submitted: August 9, 2014, 6:32 am
==========

==========
Email: izal_suka@yahoo.com
Password: 1234567
IP Address: 127.0.0.1
Date Submitted: October 27, 2014, 5:56 am
==========

==========
Email: testing@yahoo.com
Password: 123456
IP Address: 192.168.1.10
Date Submitted: October 24, 2014, 9:13 am
==========

==========
Email: faizalindrarumana@yahoo.com
Password: testing
IP Address: 192.168.1.10
Date Submitted: November 10, 2014, 4:34 am
==========
```

LAMPIRAN D
ANGKET PENGUJIAN

LEMBARAN ANGKET PENGUJIAN IMPLEMENTASI FIREWALL PSAD DAN FWSNORT UNTUK MENCEGAH SERANGAN DNS *POISONING*

Nama : Arif Wibisono

Keterangan : Koordinator Relationship IT PTIPD

Daftar Pertanyaan Uji *Fungsional*

No	Pengujian	Pilihan	
		Ya	**Tidak**
1	Apakah skenario pengujian firewall PSAD dan *fwsnort* berhasil memblok serangan DNS *Poisoning*?	✓	
2	Apakah skenario pengujian firewall firewall PSAD dan *fwsnort* dapat mengatasi serangan DNS *Poisoning*?	✓	
3	Apakah skenario pengujian firewall PSAD dan *fwsnort* dapat mencegah serang DNS *poisoning*?	✓	
4	Apakah tombol yang berada pada modul *snorby* dapat berfungsi dengan baik?	✓	
Jumlah		4	

Daftar pertanyaan *Stress Test*

No	**Aspek**	**Pilihan**			
		SS	**S**	**KS**	**TS**
1	Apakah hasil pengujian *stress test* sudah sesuai dengan harapan?	✓			
2	Apakah solusi dengan *firewall* dapat mencegah serangan DNS *Poisoning*?	✓			
3	Apakah simulasi DNS *Poisoning* berjalan sesuai harapan?	✓			
Jumlah		3			

LEMBARAN ANGKET PENGUJIAN IMPLEMENTASI FIREWALL PSAD DAN FWSNORT UNTUK MENCEGAH SERANGAN DNS *POISONING*

Nama : Rahmadhan Gatra, S.T., MTCNA, MTCRE.

Keterangan : IT Networking PTIPD

Daftar Pertanyaan Uji *Fungsional*

No	Pengujian	Pilihan	
		Ya	Tidak
1	Apakah skenario pengujian firewall PSAD dan *fwsnort* berhasil memblok serangan DNS *Poisoning*?	✓	
2	Apakah skenario pengujian firewall firewall PSAD dan *fwsnort* dapat mengatasi serangan DNS *Poisoning*?	✓	
3	Apakah skenario pengujian firewall PSAD dan *fwsnort* dapat mencegah serang DNS *poisoning*?	✓	
4	Apakah tombol yang berada pada modul *snorby* dapat berfungsi dengan baik?	✓	
Jumlah		4	

Daftar pertanyaan *Stress Test*

No	Aspek	Pilihan			
		SS	S	KS	TS
1	Apakah hasil pengujian *stress test* sudah sesuai dengan harapan?	✓			
2	Apakah solusi dengan *firewall* dapat mencegah serangan DNS *Poisoning*?	✓			
3	Apakah simulasi DNS *Poisoning* berjalan sesuai harapan?	✓			
Jumlah		3			

LEMBARAN ANGKET PENGUJIAN IMPLEMENTASI FIREWALL PSAD DAN FWSNORT UNTUK MENCEGAH SERANGAN DNS *POISONING*

Nama : Ervan Yogi Arifianto

Keterangan : Relationship & Training

Daftar Pertanyaan Uji *Fungsional*

No	Pengujian	Pilihan	
		Ya	Tidak
1	Apakah skenario pengujian firewall PSAD dan *fwsnort* berhasil memblok serangan DNS *Poisoning*?	✓	
2	Apakah skenario pengujian firewall firewall PSAD dan *fwsnort* dapat mengatasi serangan DNS *Poisoning*?	✓	
3	Apakah skenario pengujian firewall PSAD dan *fwsnort* dapat mencegah serang DNS *poisoning*?	✓	
4	Apakah tombol yang berada pada modul *snorby* dapat berfungsi dengan baik?	✓	
Jumlah		4	

Daftar pertanyaan *Stress Test*

No	Aspek	Pilihan			
		SS	S	KS	TS
1	Apakah hasil pengujian *stress test* sudah sesuai dengan harapan?	✓			
2	Apakah solusi dengan *firewall* dapat mencegah serangan DNS *Poisoning*?	✓			
3	Apakah simulasi DNS *Poisoning* berjalan sesuai harapan?	✓			
Jumlah		3			

LEMBARAN ANGKET PENGUJIAN IMPLEMENTASI FIREWALL PSAD DAN FWSNORT UNTUK MENCEGAH SERANGAN DNS *POISONING*

Nama : Rahmat Nur faizin

Keterangan : Mahasiswa UIN

Daftar Pertanyaan Uji *Fungsional*

No	Pengujian	Pilihan	
		Ya	Tidak
1	Apakah skenario pengujian firewall PSAD dan *fwsnort* berhasil memblok serangan DNS *Poisoning*?	✓	
2	Apakah skenario pengujian firewall firewall PSAD dan *fwsnort* dapat mengatasi serangan DNS *Poisoning*?	✓	
3	Apakah skenario pengujian firewall PSAD dan *fwsnort* dapat mencegah serang DNS *poisoning*?	✓	
4	Apakah tombol yang berada pada modul *snorby* dapat berfungsi dengan baik?	✓	
Jumlah		4	

Daftar pertanyaan *Stress Test*

No	Aspek	Pilihan			
		SS	S	KS	TS
1	Apakah hasil pengujian *stress test* sudah sesuai dengan harapan?	✓			
2	Apakah solusi dengan *firewall* dapat mencegah serangan DNS *Poisoning*?		✓		
3	Apakah simulasi DNS *Poisoning* berjalan sesuai harapan?	✓			
Jumlah		2	1		

LEMBARAN ANGKET PENGUJIAN IMPLEMENTASI FIREWALL PSAD DAN FWSNORT UNTUK MENCEGAH SERANGAN DNS *POISONING*

Nama : Arya Ervan Leoresta

Keterangan : Mahasiswa UIN

Daftar Pertanyaan Uji *Fungsional*

No	Pengujian	Pilihan	
		Ya	**Tidak**
1	Apakah skenario pengujian firewall PSAD dan *fwsnort* berhasil memblok serangan DNS *Poisoning*?	✓	
2	Apakah skenario pengujian firewall firewall PSAD dan *fwsnort* dapat mengatasi serangan DNS *Poisoning*?	✓	
3	Apakah skenario pengujian firewall PSAD dan *fwsnort* dapat mencegah serang DNS *poisoning*?	✓	
4	Apakah tombol yang berada pada modul *snorby* dapat berfungsi dengan baik?	✓	
Jumlah		4	

Daftar pertanyaan *Stress Test*

No	Aspek	Pilihan			
		SS	**S**	**KS**	**TS**
1	Apakah hasil pengujian *stress test* sudah sesuai dengan harapan?	✓			
2	Apakah solusi dengan *firewall* dapat mencegah serangan DNS *Poisoning*?	✓			
3	Apakah simulasi DNS *Poisoning* berjalan sesuai harapan?	✓			
Jumlah		3			

LEMBARAN ANGKET PENGUJIAN IMPLEMENTASI FIREWALL PSAD DAN FWSNORT UNTUK MENCEGAH SERANGAN DNS *POISONING*

Nama : Hana Sofa

Keterangan : Mahasiswa UIN

Daftar Pertanyaan Uji *Fungsional*

No	Pengujian	Pilihan	
		Ya	**Tidak**
1	Apakah skenario pengujian firewall PSAD dan *fwsnort* berhasil memblok serangan DNS *Poisoning*?	✓	
2	Apakah skenario pengujian firewall firewall PSAD dan *fwsnort* dapat mengatasi serangan DNS *Poisoning*?	✓	
3	Apakah skenario pengujian firewall PSAD dan *fwsnort* dapat mencegah serang DNS *poisoning*?	✓	
4	Apakah tombol yang berada pada modul *snorby* dapat berfungsi dengan baik?	✓	
Jumlah		4	

Daftar pertanyaan *Stress Test*

No	**Aspek**	**Pilihan**			
		SS	**S**	**KS**	**TS**
1	Apakah hasil pengujian *stress test* sudah sesuai dengan harapan?		✓		
2	Apakah solusi dengan *firewall* dapat mencegah serangan DNS *Poisoning*?		✓		
3	Apakah simulasi DNS *Poisoning* berjalan sesuai harapan?		✓		
Jumlah			3		

LEMBARAN ANGKET PENGUJIAN IMPLEMENTASI FIREWALL PSAD DAN FWSNORT UNTUK MENCEGAH SERANGAN DNS *POISONING*

Nama : Sujud Arifin

Keterangan : Mahasiswa UIN

Daftar Pertanyaan Uji *Fungsional*

No	Pengujian	Pilihan	
		Ya	**Tidak**
1	Apakah skenario pengujian firewall PSAD dan *fwsnort* berhasil memblok serangan DNS *Poisoning*?	✓	
2	Apakah skenario pengujian firewall firewall PSAD dan *fwsnort* dapat mengatasi serangan DNS *Poisoning*?	✓	
3	Apakah skenario pengujian firewall PSAD dan *fwsnort* dapat mencegah serang DNS *poisoning*?	✓	
4	Apakah tombol yang berada pada modul *snorby* dapat berfungsi dengan baik?	✓	
Jumlah		4	

Daftar pertanyaan *Stress Test*

No	Aspek	Pilihan			
		SS	**S**	**KS**	**TS**
1	Apakah hasil pengujian *stress test* sudah sesuai dengan harapan?		✓		
2	Apakah solusi dengan *firewall* dapat mencegah serangan DNS *Poisoning*?		✓		
3	Apakah simulasi DNS *Poisoning* berjalan sesuai harapan?		✓		
Jumlah			3		

LEMBARAN ANGKET PENGUJIAN IMPLEMENTASI FIREWALL PSAD DAN FWSNORT UNTUK MENCEGAH SERANGAN DNS *POISONING*

Nama : Rasyid Yeni Saputra

Keterangan : Mahasiswa UIN

Daftar Pertanyaan Uji *Fungsional*

No	Pengujian	Pilihan	
		Ya	**Tidak**
1	Apakah skenario pengujian firewall PSAD dan *fwsnort* berhasil memblok serangan DNS *Poisoning*?	✓	
2	Apakah skenario pengujian firewall firewall PSAD dan *fwsnort* dapat mengatasi serangan DNS *Poisoning*?	✓	
3	Apakah skenario pengujian firewall PSAD dan *fwsnort* dapat mencegah serang DNS *poisoning*?	✓	
4	Apakah tombol yang berada pada modul *snorby* dapat berfungsi dengan baik?	✓	
Jumlah		4	

Daftar pertanyaan *Stress Test*

No	Aspek	Pilihan			
		SS	**S**	**KS**	**TS**
1	Apakah hasil pengujian *stress test* sudah sesuai dengan harapan?		✓		
2	Apakah solusi dengan *firewall* dapat mencegah serangan DNS *Poisoning*?		✓		
3	Apakah simulasi DNS *Poisoning* berjalan sesuai harapan?		✓		
Jumlah			3		

LEMBARAN ANGKET PENGUJIAN IMPLEMENTASI FIREWALL PSAD DAN FWSNORT UNTUK MENCEGAH SERANGAN DNS *POISONING*

Nama : Setiyo Budi

Keterangan : Mahasiswa UIN

Daftar Pertanyaan Uji *Fungsional*

No	Pengujian	Pilihan	
		Ya	**Tidak**
1	Apakah skenario pengujian firewall PSAD dan *fwsnort* berhasil memblok serangan DNS *Poisoning*?	✓	
2	Apakah skenario pengujian firewall firewall PSAD dan *fwsnort* dapat mengatasi serangan DNS *Poisoning*?	✓	
3	Apakah skenario pengujian firewall PSAD dan *fwsnort* dapat mencegah serang DNS *poisoning*?	✓	
4	Apakah tombol yang berada pada modul *snorby* dapat berfungsi dengan baik?	✓	
Jumlah		4	

Daftar pertanyaan *Stress Test*

No	**Aspek**	**Pilihan**			
		SS	**S**	**KS**	**TS**
1	Apakah hasil pengujian *stress test* sudah sesuai dengan harapan?		✓		
2	Apakah solusi dengan *firewall* dapat mencegah serangan DNS *Poisoning*?	✓			
3	Apakah simulasi DNS *Poisoning* berjalan sesuai harapan?	✓			
Jumlah		2	1		

LEMBARAN ANGKET PENGUJIAN IMPLEMENTASI FIREWALL PSAD DAN FWSNORT UNTUK MENCEGAH SERANGAN DNS *POISONING*

Nama : M. Ridwan Hanafi

Keterangan : Mahasiswa UIN

Daftar Pertanyaan Uji *Fungsional*

No	Pengujian	Pilihan	
		Ya	**Tidak**
1	Apakah skenario pengujian firewall PSAD dan *fwsnort* berhasil memblok serangan DNS *Poisoning*?	✓	
2	Apakah skenario pengujian firewall firewall PSAD dan *fwsnort* dapat mengatasi serangan DNS *Poisoning*?	✓	
3	Apakah skenario pengujian firewall PSAD dan *fwsnort* dapat mencegah serang DNS *poisoning*?	✓	
4	Apakah tombol yang berada pada modul *snorby* dapat berfungsi dengan baik?	✓	
Jumlah		4	

Daftar pertanyaan *Stress Test*

No	**Aspek**	**Pilihan**			
		SS	**S**	**KS**	**TS**
1	Apakah hasil pengujian *stress test* sudah sesuai dengan harapan?	✓			
2	Apakah solusi dengan *firewall* dapat mencegah serangan DNS *Poisoning*?	✓			
3	Apakah simulasi DNS *Poisoning* berjalan sesuai harapan?	X	✓		
Jumlah		2	1		