JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 3 Nomor. 1, April 2018
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

PERANCANGAN *SOFTWARE IDS SNORT* UNTUK PENDETEKSIAN SERANGAN *INTERRUPTION* (*Netcut*) PADA JARINGAN *WIRELESS*

Muhammad Akbar
akbar.stmikhdy@gmail.com
Sistem Komputer STMIK Handayani Makassar

Abstrak

Berkembangnya penggunaan internet di kalangan masyarakat, semakin membuat keamanan jaringan lebih rentan terhadap gangguan. Tujuan dari penelitian ini adalah merancang *software* IDS jenis *SNORT* yang berfungsi untuk melakukan pendeteksian serangan *interruption*, dimana hal ini adalah serangan terhadap jaringan *WiFi* atau *wireless*. Metode yang digunakan adalah perancangan *software* IDS yang bekerja dengan memantau berkas-berkas sistem operasi, yakni dengan cara melihat apakah ada percobaan untuk merubah berkas-berkas sistem operasi, utamanya berkasi file log. Hasil dari penelitian ini adalah *software* IDS yang dapat diinstal langsung ke komputer, baik dengan sistem operasi Linux maupun Windows, sehingga serangan dengan teknik *interruption* dapat dideteksi.

Kata kunci : *IDS, SNORT, interruption, software, WiFi*

I. PENDAHULUAN

Pada era global ini, keamanan sistem komputer berbasis jaringan harus sangat diperhatikan, karena jaringan komputer yang sifatnya publik dan global pada dasarnya tidak aman. Pada saat data terkirim dari suatu terminal asal menuju ke terminal tujuan dalam Internet, data itu akan melewati sejumlah terminal yang lain yang berarti akan memberi kesempatan pada user jaringan yang lain untuk menyadap atau mengubah data tersebut. Khususnya pada jaringan yang menggunakan media WiFI atau *Wireless* untuk terhubung dengan internet. Penggunaan jaringan *wireless* ini dapat dijumpai pada banyak tempat, seperti menjamurnya warkop dengan *hotspot*, universitas, perusahaan, sampai

JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 3 Nomor. 1, April 2018
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

penggunaan untuk rumahan pun telah banyak menggunakan sistem ini. Karena pada realitasnya, internet memang sudah menjadi kebutuhan utama bagi kalangan masyarakat. Untuk itu, pengamanan jaringan harus menjadi pekerjaan rumah yang harus dikerjakan oleh pakar keamanan jaringan atau pelaku-pelaku IT.

Serangan dengan metode *interruption* adalah serangan yang banyak dijumpai pada kasus-kasus keamanan jaringan. *Interruption* adalah ancaman terhadap *availibility* (ketersediaan) dimana data dan informasi yang berada dalam sistem komputer dirusak atau dibuang sehingga menjadi tidak ada dan tidak berguna. Contoh dari serangan ini adalah pengrusakan hardware (harddisk dan lain sebagainya), jalur komunikasi baik kabel maupun nirkabel dipotong.

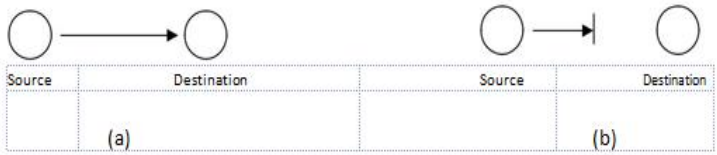
Salah satu aplikasi yang marak digunakan untuk serangan dengan metode *interruption* adalah *netcut. Netcut* adalah aplikasi yang mempunyai fungsi untuk menguasai suatu jaringan *wifi* dalam *hotspot*, dan fungsi lain yaitu sebagai pemotong akses *internet public* maupun *private* yang terdapat pada jaringan LAN, *wifi* dan *hotspot. Netcut* juga dapat memotong sambungan koneksi *internet* suatu *client* yang saling berhubungan dalam satu jaringan.

II. METODE PENELITIAN

2.1. *Interruption*

Interruption adalah salah satu serangan yang berhubungan kepada *availibility*, dimana serangan ini dapat merusak *hardware, software*, data dan juga *line* komunikasi yang terdapat di dalam suatu sistem komputer yang terhubung ke jaringan. Untuk *hardware*, peralatan dapat dirusak dengan cara langsung (dicuri atau dirampok), ataupun dirusak menggunakan serangan komputer dalam jaringan. Untuk *software* dan data, dapat dilakukan dengan cara dihapus, sedangkan untuk *line* komunikasi, kabel dapat dirusak atau diputus, atau dengan menggunaakn serangan pada jaringan komputer. Pada jaringan *wireless* untuk *line* komunikasi dapat dilakukan pemotongan jalur komunikasi dengan menggunakan aplikasi *netcut* yang akan dibahas lebih lanjut pada penelitian ini.

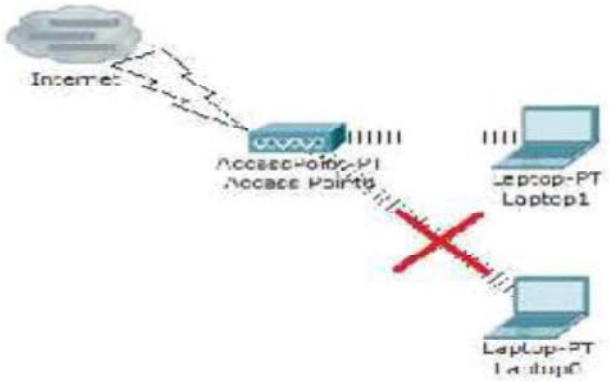
JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 3 Nomor. 1, April 2018
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id



Gambar 1. (a) Jaringan normal (b) jaringan dengan *interruption*

Netcut

Netcut atau *Network Cut* merupakan salah satu aplikasi jenis *interruption* yang belakangan ini banyak digunakan oleh para pelaku serangan pada jaringan komputer. *Netcut* adalah aplikasi *under windows* yang berfungsi untuk melakukan *cut* (pemotongan) terhadap akses jaringan *wireless.* Jika seseorang berada dalam jaringan *wireless* yang terhubung ke jaringan *internet*, penguna tersebut dapat memutuskan koneksi *wireless client* lain yang juga dalam satu jaringan, sehingga *client* yang lain tidak dapat terhubung ke jaringan. Alasan penggunaan *netcut* biasanya agar pelaku pengguna *netcut* dapat memanfaatkan seluruh fasilitas jaringan *internet* yang ada, seperti *bandwidth*, karena dalam satu jaringan, hanya terdapat satu *user*, sedangkan *user* yang lain aksesnya di *cut.*



Gambar 2. Skema jaringan penggunaan *netcut*

JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 3 Nomor. 1, April 2018
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

2.2 Bentuk Ekperimen

Seperti yang telah disampaikan sebelumnya, untuk *software* IDS disini dibuat pada sistem operasi *Linux Slackware 13.* Eksperimen dilakukan dengan menginstallkan software IDS pada sistem operasi Linux, dimana terhubung dengan jaringan internet melalui media *wireless.* Dalam jaringan tersebut juga terdapat 3 buah user, dimana user 1 akan melakukan akses internet secara normal, user 2 adalah user yang akses internetnya akan di cut, dan user 3 yang menjadi pelaku penyerangan *interruption* (*netcut*).

Spesifikasi untuk server IDS dan client sebagai berikut :

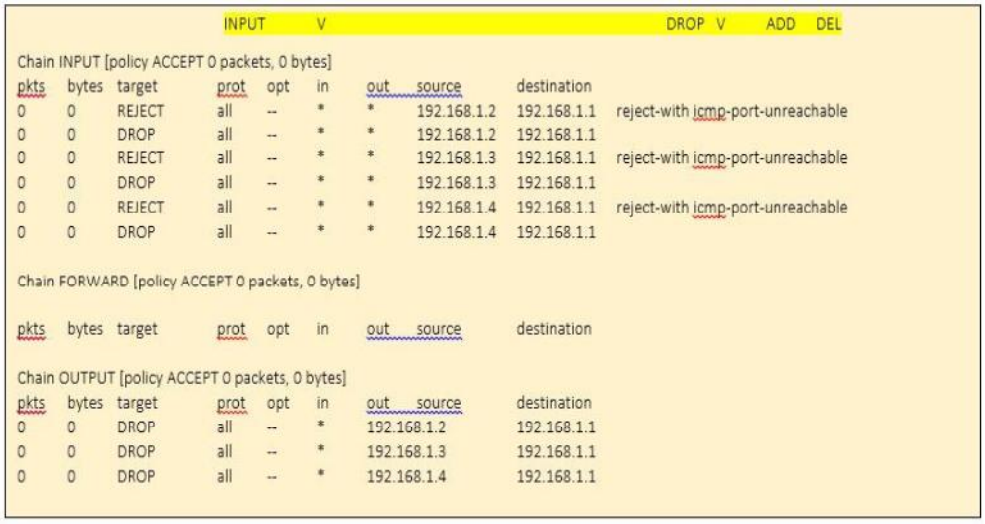
1. Server
   Sistem Operasi : Slackware 13
   Prosesor : Core 2 Duo
   Ram : 3 GB DDR 2
   Harddisk : 320 GB
   LAN Card : 1Gbps
2. Client
   Sistem Operasi : Windows 7
   Prosesor : AMD Athlon Dual Core
   Ram : 1GB DDR 2
   Harddisk : 250 GB
   LAN Card : 1Gbps

Dalam IDS (*Intrusion Detection System*) berbentuk *SNORT,* terdapat beberapa komponen yang biasa digunakan, seperti Snort (Engine dan Rules), BASE (*Basic Analysis and Security Engine*) dan *IPtables* (*Firewall*). Konfigurasi snort merupakan langkah awal dalam penelitian ini. Snort dapat diinstal secara free karena merupakan aplikasi open source yang secara default telah terinstal pada linux Slackware 13. Setelah terinstal, rules yang ingin digunakan diaktifkan,

JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 3 Nomor. 1, April 2018
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

semisal rules backdoor, dns, dos, dan rules-rules lainnya. Selebihnya paket pendukung lainnya dapat diinstal secara online melalui repository online.

Tahap selanjutnya yakni pembuatan database menggunakan MySql dengan komunikasi Apache dan PHP untuk web services. Iptables pada sistem ini berfungsi sebagai firewall. Konfigurasi firewall dapat dilihat pada gambar berikut :



INPUT V DROP V ADD DEL

Chain INPUT [policy ACCEPT 0 packets, 0 bytes]

pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	REJECT	all	--	*	*	192.168.1.2	192.168.1.1	reject-with icmp-port-unreachable
0	0	DROP	all	--	*	*	192.168.1.2	192.168.1.1	
0	0	REJECT	all	--	*	*	192.168.1.3	192.168.1.1	reject-with icmp-port-unreachable
0	0	DROP	all	--	*	*	192.168.1.3	192.168.1.1	
0	0	REJECT	all	--	*	*	192.168.1.4	192.168.1.1	reject-with icmp-port-unreachable
0	0	DROP	all	--	*	*	192.168.1.4	192.168.1.1	

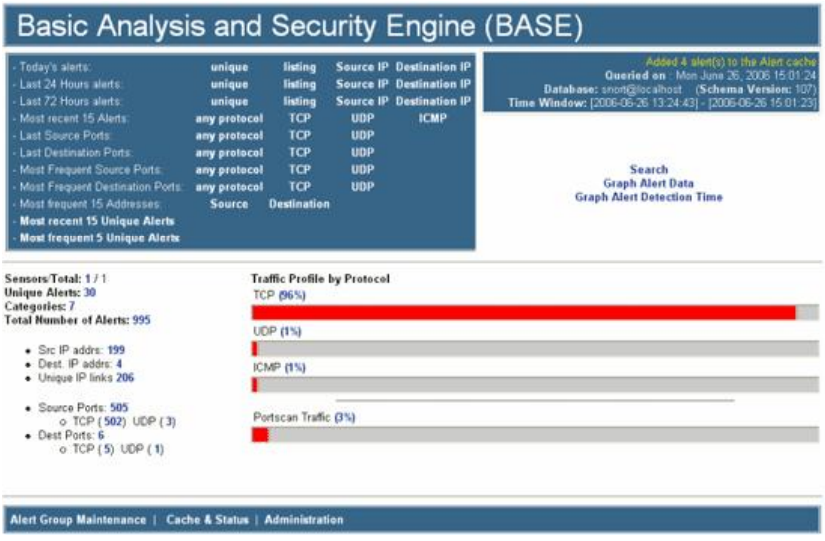
Chain FORWARD [policy ACCEPT 0 packets, 0 bytes]

pkts	bytes	target	prot	opt	in	out	source	destination

Chain OUTPUT [policy ACCEPT 0 packets, 0 bytes]

pkts	bytes	target	prot	opt	in	out	source	destination
0	0	DROP	all	--	*	192.168.1.2		192.168.1.1
0	0	DROP	all	--	*	192.168.1.3		192.168.1.1
0	0	DROP	all	--	*	192.168.1.4		192.168.1.1

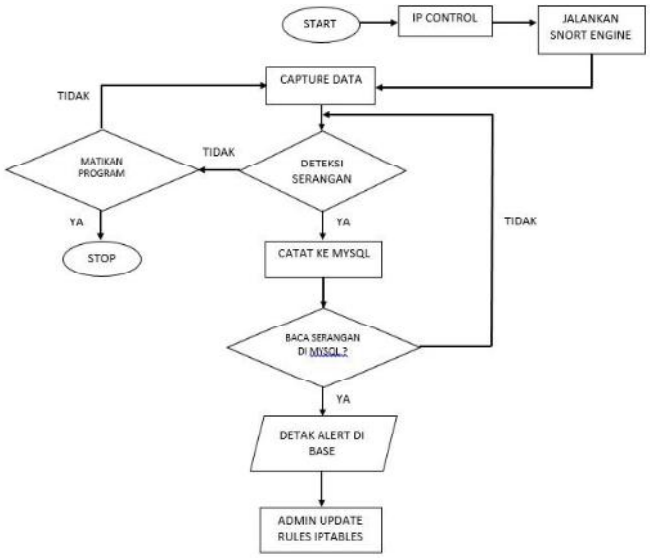
Gambar 3.Konfigurasi Firewall



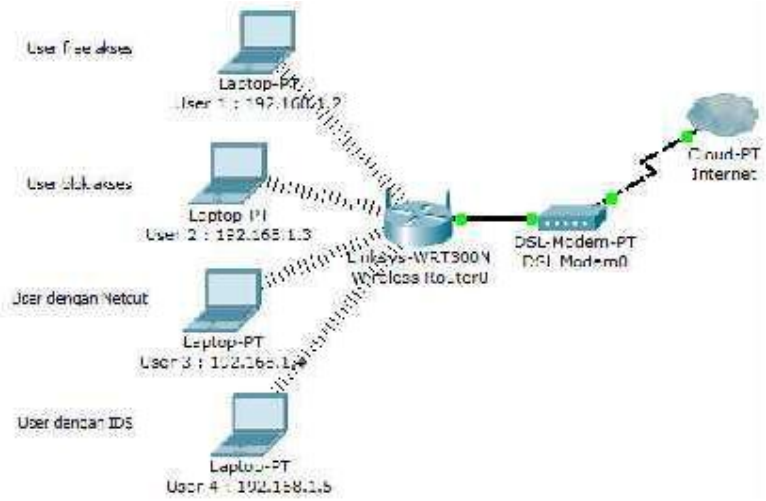
Gambar 4.Tampilan BASE (*Basic Analysis and Security Engine*)

JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 3 Nomor. 1, April 2018
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

Secara arsitektur komunikasi, dapat digambarkan dalam bentuk *flowchart* sistem sebagai berikut :



Gambar 5. *Flowchart* sistem *IDS* (*SNORT*)



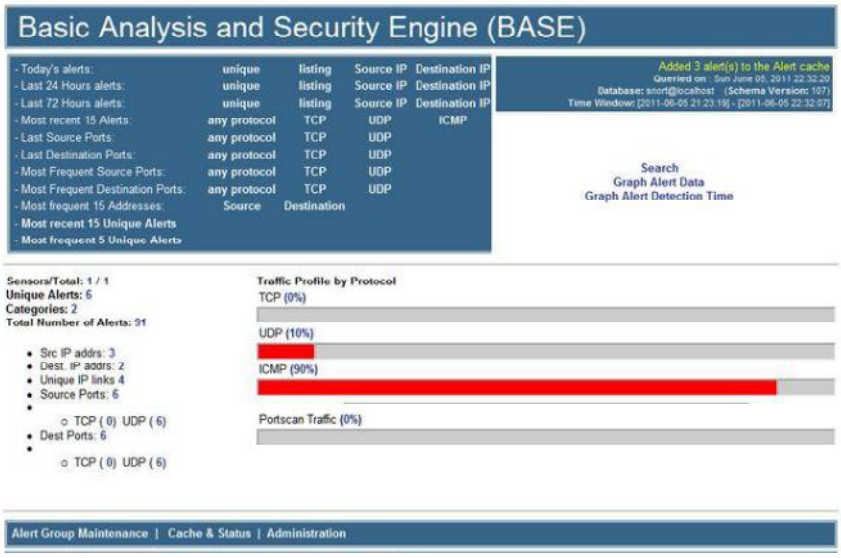
Gambar 6. Skema jaringan eksperimen

JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 3 Nomor. 1, April 2018
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

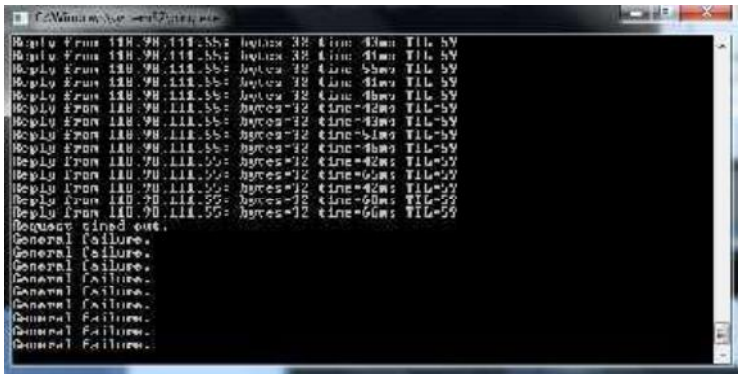
III HASIL DAN PEMBAHASAN

3.1 Percobaan Serangan *Interruption*

Berdasarkan dari eksperimen yang telah dilakukan, hasilnya menunjukkan bahwa, user 2 dengan IP address 192.168.1.3 telah berhasil diserang oleh user 3 dengan IP address 192.168.1.4 menggunakan aplikasi atau *tools netcut*. Hal ini mengakibatkan user 2 tidak dapat mengakses internet. Karena akses internetnya telah di *cut* oleh user 3. Hal tersebut dapat terdeteksi pada aplikasi web BASE, dimana terlihat paket ICMP yang mencapai angka 90%, karena pada dasarnya serangan Netcut menggunakan protocol ICMP dalam pengoperasiannya.



Gambar 7. Deteksi Serangan ICMP Netcut

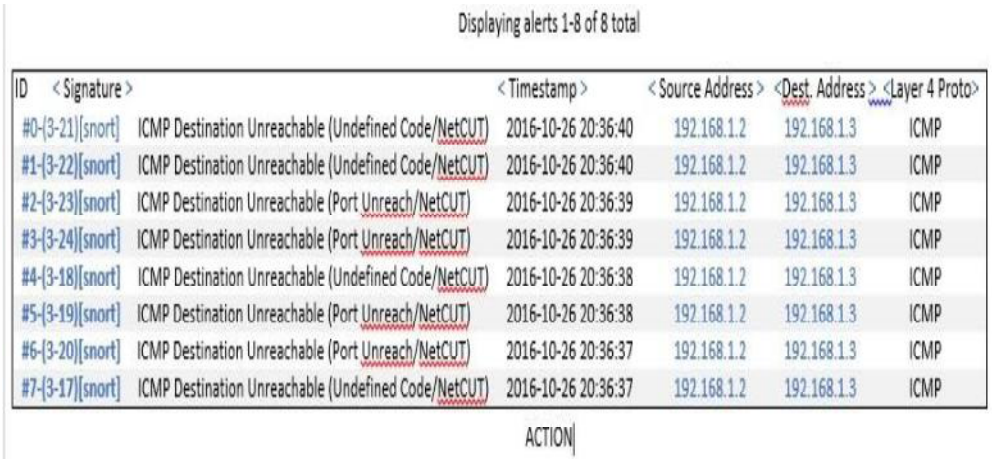


Gambar 8. Tampilan Ping Client Setelah Terserang Netcut

JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 3 Nomor. 1, April 2018
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

Pada eksperimen yang dilakukan menggunakan 4 buah user dengan range IP Address 192.168.1.2 – 192.168.1.5. Untuk komunikasi *wireless* menggunakan *access point Linksys* dengan kecepatan 54 Mbps dan untuk internet menggunakan koneksi *Telkom Speedy* dengan kecepatan 1MB. User 1 sampai dengan user 3 menggunakan sistem operasi Windows 7 Ultimate 32 bit.

Setelah user 3 melakukan serangan ke user 2, maka program IDS yang terdapat pada user 4 akan secara otomatis mendeteksi serangan tersebut. Sehingga dapat segera diketahui pelaku serangan *interruption* tersebut dari informasi tampilan program IDS. Informasi yang ditampilkan oleh program IDS adalah berupa *IP addres* dari pelaku serangan, seperti terlihat pada gambar di bawah :


Displaying alerts 1-8 of 8 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-[3-21][snort]	ICMP Destination Unreachable (Undefined Code/NetCUT)	2016-10-26 20:36:40	192.168.1.2	192.168.1.3	ICMP
#1-[3-22][snort]	ICMP Destination Unreachable (Undefined Code/NetCUT)	2016-10-26 20:36:40	192.168.1.2	192.168.1.3	ICMP
#2-[3-23][snort]	ICMP Destination Unreachable (Port Unreach/NetCUT)	2016-10-26 20:36:39	192.168.1.2	192.168.1.3	ICMP
#3-[3-24][snort]	ICMP Destination Unreachable (Port Unreach/NetCUT)	2016-10-26 20:36:39	192.168.1.2	192.168.1.3	ICMP
#4-[3-18][snort]	ICMP Destination Unreachable (Undefined Code/NetCUT)	2016-10-26 20:36:38	192.168.1.2	192.168.1.3	ICMP
#5-[3-19][snort]	ICMP Destination Unreachable (Port Unreach/NetCUT)	2016-10-26 20:36:38	192.168.1.2	192.168.1.3	ICMP
#6-[3-20][snort]	ICMP Destination Unreachable (Port Unreach/NetCUT)	2016-10-26 20:36:37	192.168.1.2	192.168.1.3	ICMP
#7-[3-17][snort]	ICMP Destination Unreachable (Undefined Code/NetCUT)	2016-10-26 20:36:37	192.168.1.2	192.168.1.3	ICMP

ACTION

Gambar 9. Tampilan Notifikasi *Alert* Pada BASE

IV.PENUTUP

4.1 KESIMPULAN

Dari penelitian yang telah dilakukan, dapat disimpulkan bahwa program IDS yang digunakan pada penelitian ini hanya dapat mendeteksi serangan *interruption* (*Netcut*) saja, serangan jenis lain belum dapat dideteksi. Program IDS dapat mendeteksi dengan baik serangan *netcut* yang terjadi pada jaringan. Program *netcut* yang dijalankan dapat melakukan pemotongan jalur koneksi *wifi* pada user yang lain. Hal tersebut dapat dilakukan secara simultan ke semua user yang ada pada jaringan..Program IDS hanya dapat mendeteksi serangan, namun tidak dapat melakukan pengamanan, oleh karena itu IDS dapat disandingkan

JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 3 Nomor. 1, April 2018
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

dengan program pengamanan *netcut* yang lain seperti *anti netcut, netcut defender*, dan lain-lain. Jaringan yang digunakan akan lebih aman jika menggunakan keamanan tambahan seperti *mikrotik*, karena berdasarkan penelitian serangan *netcut* tidak dapat berfungsi pada jaringan yang terdapat *mikrotik* di dalamnya.

DAFTAR PUSTAKA

http://ezine.omega.or.id/1/konsep-keamanan&kerahasiaan-data-1.txt diakses pada 28-11-2014 pukul 09.01

http://www.it-newbie.com/2014/09/cara-mudah-menggunakan-netcut-pada-wifi.html diakses pada 28-11-2014 pukul 09.06

https://www.facebook.com/permalink.php?story_fbid=225483790977295&id=186378531554488 diakses pada 04-12-2014 pukul 14.13

http://pacarita.com/pengertian-wireless-dan-cara-kerja-wireless.html diakses pada 04-12-2014 pukul 14.17

indra sufian. *Langkah-langkah sederhana untuk mengamankan handphone dan tablet anda*. magcover. 2012