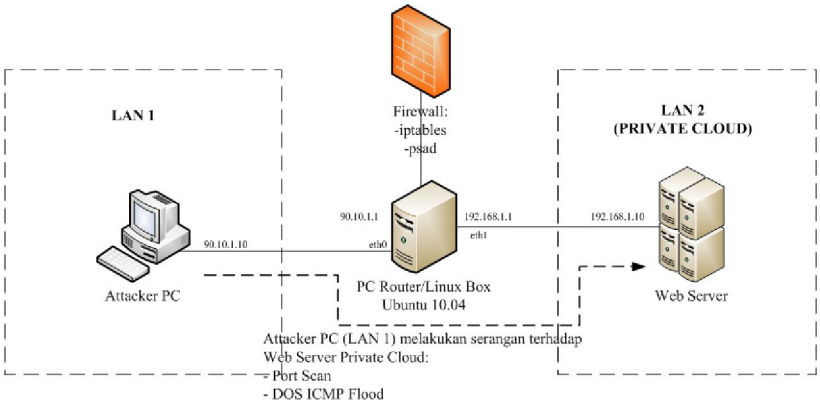
BAB IV
PENGUJIAN DAN ANALISA

Pada bab ini akan dijelaskan pengujian dari sistem keamanan yang telah dirancang.Dalam melakukan pengujian pada sistem keamanannya digunakan beberapa keadaan pengujian yang berbeda. Kemudian hasil pengujian dari masing-masing pengujian tersebut dianalisa serta dibandingkan bagaimana hasilnya dengan pengujian yang sebelumnya telah dilakukan.



Gambar 4.1 Pengujian Sistem Keamanan

Pada Gambar 4.1 diatas, pengujian yang dilakukan adalah sebuah PC yang ditugaskan sebagai penyerang (Attacker PC) berusaha melakukan penyerangan seperti mengumpulkan informasi-informasi dan melakukan serangan DOS (Flooding) terhadap server yang berada pada LAN 2 (Jaringan Private Cloud). Kedua jaringan dihubungkan sebuah perangkat PC, yaitu PC Router yang dimana pada PC Router tersebut digunakan tools keamanan yaitu Iptables sebagai Firewall dan Psad sebagai Log Analysis serta IDS (Intrusion Detection System). Sistem keamanan yang telah dirancang akan diuji dengan beberapa keadaan pengujian yang berbeda pada PC Router untuk membuktikan apakah sistem keamanan yang telah dirancang bekerja dengan optimal dan handal dalam melindungi server pada jaringan Private Cloud.

4.1 Pengujian Sistem Keamanan

Pada tahap pengujian sistem keamanan yang telah dibangun, dibuatkan beberapa keadaan/kondisi pada PC Router yang berbeda untuk menguji serta membandingkan bagaimana kinerja sistem keamanannya dengan membandingkan hasil dari masing-masing pengujian serta paket yang telah di-log. Berikut merupakan pengujian-pengujiannya:

1. PC Router sebagai Firewall (Iptables)
2. PC Router sebagai Firewall (Iptables) serta Log Analysis (Psad)
3. PC Router sebagai Firewall (Iptables) serta Log Analysis & IDS (Psad)
4. PC Router tanpa Firewall, Log Analysis dan IDS

Dari keadaan pengujian diatas, sistem keamanan tersebut akan diuji dengan menggunakan tools uji keamanan berikut:

1. Nmap (Network Mapper)

   Nmap digunakan untuk melakukan port scan/port sweep yang bertujuan untuk mengumpulkan informasi/reconnaissance terhadap komputer target yaitu layanan apa saja yang disediakan oleh komputer target atau web server Private Cloud. Pada pengujian sistem keamanannya dilakukan dua kali percobaan (percobaan 1 dan 2) yang masing-masing percobaan menggunakan fitur Nmap TCP Connect () Scan, yang dimana scan ini mengirim paket TCP utuh (SYN-SYN_ACK-ACK) pada komputer target kemudian periksa hasil data log sistem keamanan terhadap scan tersebut.

   Untuk dapat melakukan Nmap TCP Connect () Scan, ketikkan perintah berikut pada terminal:

   ```
   Nmap –sT 192.168.10
   ```

2. Hping3

   Hping3 digunakan untuk melakukan serangan DOS (Denial Of Service) yang berupa ICMP Flood yang dimana bertujuan untuk membanjiri komputer target dengan paket ICMP_ECHO_REQUEST yang berjumlah sangat banyak sehingga dapat menghabiskan resource (CPU Usage) yang dimiliki komputer target. Untuk pengujian sistem keamanannya dilakukan dua kali percobaan ICMP Flood yang masing-masing dilakukan selama 30 detik terhadap web

server cloud dan periksa hasil data log sistem keamanan serta dampak yang dihasilkan pada web server, dalam hal ini CPU Usage web server cloud.

Untuk dapat melakuan ICMP Flood menggunakan Hping3, ketikkan perintah berikut pada terminal:

```
hping3 –p 80 --flood –-icmp 192.168.1.10
```

Agar proses analisa data log dari setiap keadaan pengujian lebih efisien dan mudah dianalisa, maka untuk setiap pengujian file log akan dihapus kemudian dibuat kembali, serta log daemon serta sistem keamanan yang digunakan di-restart. Ini agar dalam setiap pengujian paket yang di-log oleh Iptables/Psad dapat berjumlah hingga ribuan paket sehingga dapat menyebabkan kesulitan dalam menganalisa data log dari setiap keadaan pengujian pada PC Router. Serta sampel log yang diambil adalah paket yang berada di urutan terakhir agar lebih memudahkan serta efisien dalam menganalisa paket tersebut.

Paket yang di log merupakan paket yang memiliki prefix sebagaimana berikut:

1. “INVALID PKT “

   Paket yang termasuk/memiliki prefix ini adalah paket yang tidak sesuai/invalid dengan state yang ada. Artinya tidak termasuk kedalam koneksi apapun yang berjalan/ada pada server.

2. “SPOOFED IP “

   Paket yang memiliki prefix ini adalah paket yang berasal dari LAN 1 yang memiliki alamat sumber sama dengan alamat IP dari LAN 2.

3. “DROP PKT “

   Paket yang memiliki prefix ini adalah paket yang tidak sesuai dengan rules yang ada pada firewall.

4. “ICMP FLOOD “

   Paket yang memiliki prefix ini adalah paket yang terdeteksi sebagai paket DOS ICMP Flood.

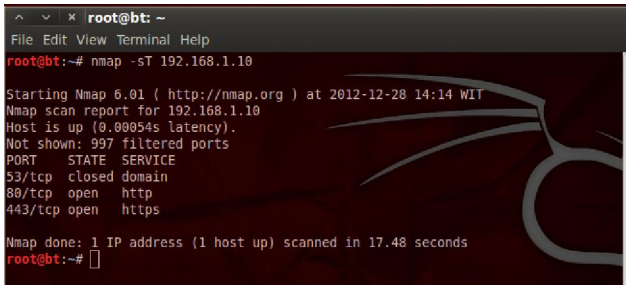
4.1.1 PC Router sebagai Firewall

Pada pengujian PC Router sebagai Firewall, fitur keamanan firewall yang digunakan yaitu Iptables. Dimana firewall Iptables sudah terkonfigurasi dan diatur paket-paket apa saja kah yang diijinkan masuk kedalam jaringan/web server dan

mana yang tidak (rules and policy). Paket yang tidak sesuai dengan rules/policy yang diterapkan akan di log dan data log tersebut akan dianalisis.

4.1.1.1 Pengujian Menggunakan Nmap

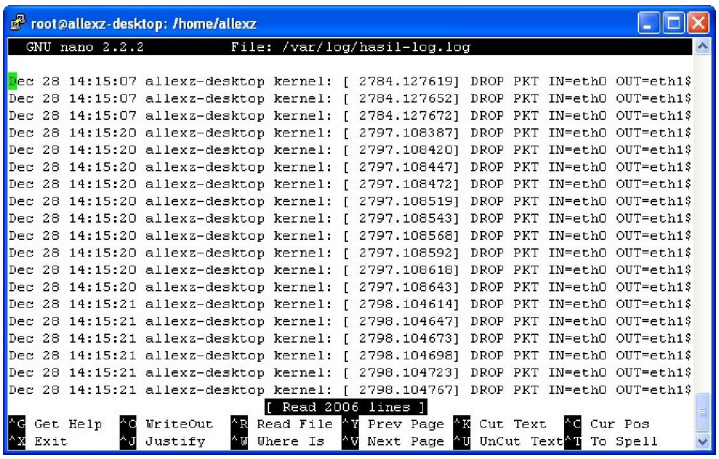
Digunakan Nmap TCP Connect Scan () untuk melakukan port scan/sweep terhadap web server cloud dan melihat hasilnya apakah firewall berfungsi dengan baik. Berikut merupakan hasil tampilan dari Nmap ketika firewall diterapkan.



Gambar 4.2 Tampilan Hasil Scan Nmap Firewall On

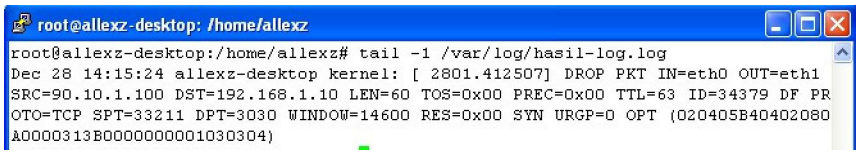
Pada tampilan hasil scan Nmap pada gambar diatas (Gambar 4.2), didapatkan hasil bahwa Nmap telah melakukan Port Scan pada web server selama 17,48 detik dan layanan (service) yang ada pada web server cloud adalah untuk http (port 80), https (port 443) dan DNS (port 53). Tetapi yang dalam keadaan terbuka (open/tersedia pada web server tersebut) adalah layanan untuk http dan https (port 80 dan 443), sedangkan untuk layanan DNS (port 53), walaupun pada web server ada layanan untuk DNS tetapi web server tidak menyediakannya untuk client karena dalam keadaan tertutup (closed).

Berikut merupakan hasil data log Iptables terhadap port scan yang dilakukan oleh Nmap.



Gambar 4.3 Tampilan Jumlah Paket Data Log Firewall On

Pada tampilan Gambar 4.3 diatas, didapatkan hasil bahwa Iptables telah melakukan log berjumlah 2006 paket yang dimana paket-paket tersebut berasal dari port scan yang dilakukan oleh Nmap yang sebelumnya (Gambar 4.2). Paket tersebut di log dan drop oleh Iptables karena tidak sesuai dengan rules dan policy yang diterapkan pada firewall. Hasil analisa ini didapat dari Prefix paket yang di-log tersebut yaitu “DROP PKT”, seperti yang digambarkan pada Gambar 4.3 diatas dan detil isi paket pada Gambar 4.4.



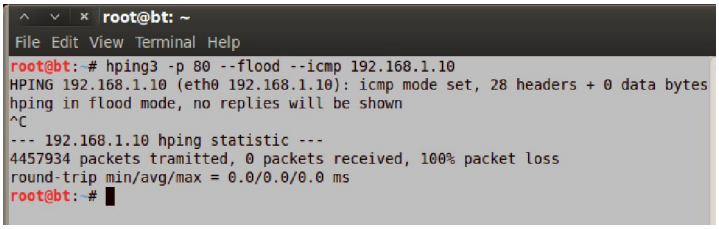
Gambar 4.4 Tampilan Sampel Paket Data Log

Pada Gambar 4.4 diatas merupakan sampel paket yang di-log oleh Iptables. Isi sampel paket tersebut berupa nilai-nilai yang ada pada TCP/IP header yang dimiliki oleh paket tersebut. Untuk penjelasan detil mengenai sampel paket log Iptables seperti yang digambarkan pada Gambar 4.4 akan dijelaskan di bagian lampiran.

Ketika dilakukan scan nmap kembali kepada web server private cloud, paket yang di-log oleh Iptables bertambah dari yang asalnya 2006 paket, menjadi 4012 paket. Dengan kata lain, setiap nmap TCP Connect Scan Iptables dapat melakukan log paket 1990-2020 paket.

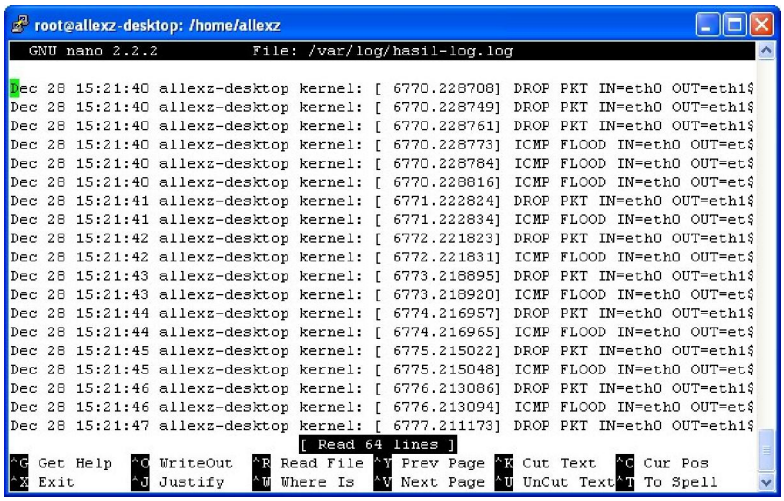
4.1.1.2 Pengujian menggunakan Hping3

Untuk melakukan serangan DOS, digunakan tools hping3 yang dimana tipe DOS yang dilakukan adalah ICMP Flood. Ketikkan perintah berikut pada terminal dan perhatikan hasil nya pada server dan data log sistem keamanan ketika firewall Iptables diterapkan.



Gambar 4.5 Tampilan Hping3 ICMP Flood

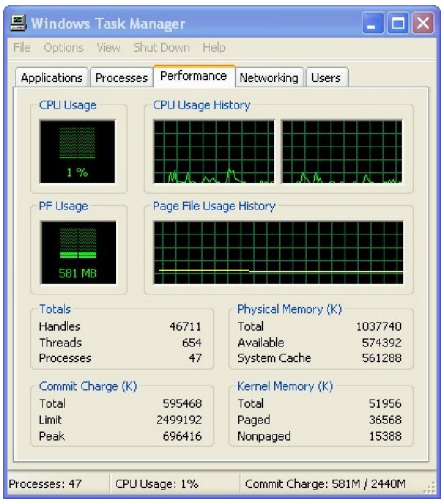
Dari Gambar 4.5 diatas didapatkan hasil bahwa selama 30 detik, hping3 mengirimkan paket ICMP_ECHO_REQUEST kepada web server sebanyak 4381686 paket dan paket tersebut 100% Loss. Ini karena hping3 dalam melakukan ICMP Flood, hanya mengirimkan paket yang berisi ICMP_ECHO_REQUEST saja kepada web server tanpa menghiraukan balasan dari web server cloud tersebut (ICMP_ECHO_REPLY) atas permintaan Attacker tersebut. Ini didapatkan dari Gambar 4.5 tersebut yang dimana ada keterangan 0 packets received. Berikut merupakan hasil log dari Iptables terhadap ICMP Flood yang dilakukan.



Gambar 4.6 Tampilan Jumlah Paket Log Hasil Hping3

Pada gambar 4.6 tersebut, dijelaskan bahwa Iptables telah melakukan paket log pada ICMP Flood tersebut sebanyak 64 paket. Yang dimana sebagian besar paket tersebut memiliki log prefix “ICMP Flood”. Ini artinya Iptables telah mendeteksi suatu serangan DOS berupa ICMP Flood dan kemudian paket ICMP tersebut di log dan drop oleh Iptables. Pada Gambar 4.6 dan 4.5 didapatkan hasil bahwa hping3 telah melakukan ICMP Flood dengan mengirimkan paket sebanyak 4381686 paket, tetapi paket yang di-log oleh Iptables hanya berjumlah 64 paket. Terjadinya perbedaan jumlah paket yang dikirim dan di-log oleh firewall ini karena keterbatasan kemampuan seberapa cepat Iptables menghasilkan sebuah pesan log. Dengan kata lain, karena Iptables menulis pesan log terlebih dahulu kepada sebuah Ring Buffer di dalam kernel, sehingga apabila traffic rate yang terjadi sangat cepat untuk menyebabkan penulisan ulang pesan yang ada pada Ring Buffer, sebelum pesan yang lama ditulis pada file log yang digunakan (/var/log/hasil-log.log), maka pesan tersebut akan hilang sebelum dikirim ke file log yang digunakan karena tertimpa pesan log yang baru.

Analisa ini didapat dengan cara melihat waktu log Iptables, bahwa rata-rata Iptables dalam 1 detik hanya dapat melakukan log paket sejumlah 2-4 paket, dan apabila dalam 30 detik maka Iptables hanya dapat melakukan log paket rata-rata sekitar sebanyak 60-80 paket. Sedangkan hping3 selama 30 detik menghasilkan sebanyak 4381686 paket, dan apabila dihitung hping3 dalam 1 detik menghasilkan/mengirimkan sebanyak 146056 paket. Sehingga terjadi perbedaan yang begitu besar antara pihak yang hanya mengirimkan paket yaitu Attacker PC dengan pihak yang menerima paket yaitu PC Router. Akibatnya adalah perbedaan jumlah paket yang di log oleh Iptables dengan paket yang dihasilkan oleh hping3. Berikut merupakan pengaruh/dampak yang terjadi pada CPU Usage web server private cloud terhadap serangan ICMP Flood tersebut.



Gambar 4.7 Tampilan CPU Usage Server (Firewall On)

Pada Gambar 4.7 diatas didapatkan bahwa ketika ICMP Flood dilakukan terhadap web server private cloud, web server tidak terpengaruh terhadap serangan tersebut. Ini dibuktikan dengan CPU Usage web server yang bernilai 0-1%.

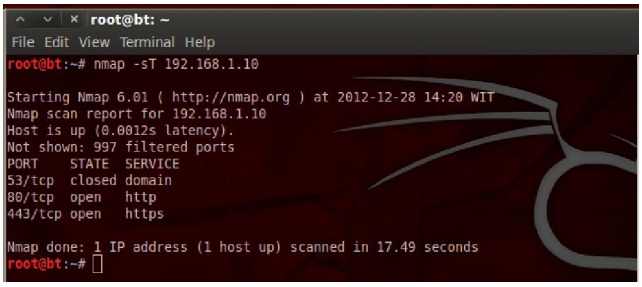
Ketika dilakukan serangan ICMP Flood kembali, jumlah paket yang di-log oleh Iptables bertambah dari yang sebelumnya berjumlah 64 paket menjadi 130 paket. Sehingga setiap pengujian menggunakan ICMP Flood pada web server, dalam 30 detik Iptables mampu melakukan log terhadap serangan tersebut sebanyak 60-80 paket.

4.1.2 PC Router sebagai Firewall dan Log Analysis

Pada pengujian PC Router sebagai Firewall dan Log Analysis, PC Router dari pengujian sebelumnya hanya menggunakan firewall dalam hal ini Iptables, maka pada pengujian berikut ditambahkan tools tambahan untuk melakukan log analysis terhadap paket yang di-log oleh Iptables, yaitu Psad. Hasil data log dari Iptables dan Psad akan dibandingkan untuk mengetahui apakah Psad sebagai log analysis bekerja dengan baik menerjemahkan log Iptables menjadi lebih mudah dimengerti.

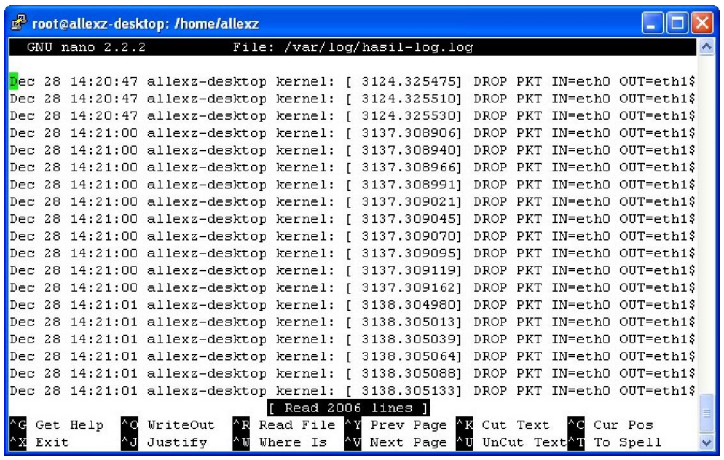
4.1.2.1 Pengujian Menggunakan Nmap

Sama seperti pengujian sebelumnya, dilakukan pengujian port scan/sweep menggunakan Nmap TCP Connect () untuk melakukan pengumpulan informasi/reconnaissance terhadap komputer target. Berikut merupakan hasil scan nmap di Attacker PC terhadap server.



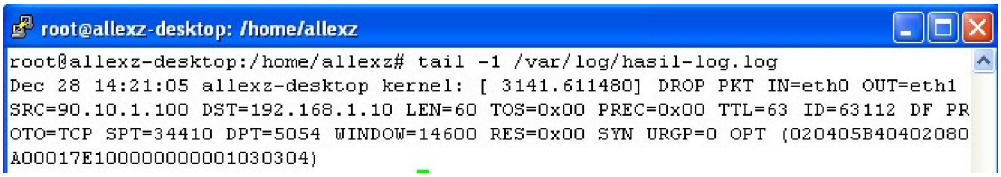
Gambar 4.8 Tampilan Hasil Scan Nmap Firewall & Log Analysis On

Pada Gambar 4.8 diatas, pada pengujian PC Router sebagai Firewall dan Log Analysis, nmap menyelesaikan port scan dengan waktu sekitar 17,98 detik. Apabila dibandingkan hasil port scan nmap pada Gambar 4.8 dengan pengujian yang sebelumnya dilakukan (Gambar 4.2), sama sekali tidak ada perbedaan. Yaitu tetap mendeteksi ada 3 port yang terlihat dari luar jaringan privete cloud yaitu http (port 80), https (port 443) dan DNS (port 53), tetapi server hanya menyediakan layanan http dan https untuk client, sedangkan DNS tidak menyediakan. Berikut merupakan hasil data log firewall pada PC Router dari nmap port scan yang dilakukan.



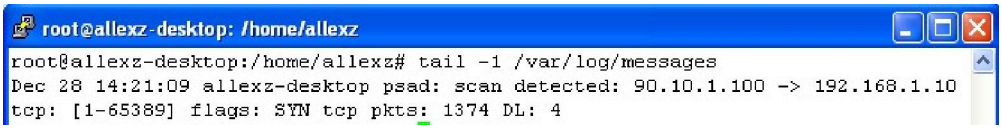
Gambar 4.9 Tampilan Jumlah Paket Log Firewall & Log Analysis On

Pada Gambar 4.9, dijelaskan bahwa Iptables melakukan log terhadap paket yang dihasilkan/dikirimkan nmap kepada web server sebanyak 2006 paket. Tidak berbeda dengan hasil dari pengujian sebelumnya (Gambar 4.3) bahwa paket-paket tersebut di drop oleh firewall karena tidak sesuai dengan rules dan policy yang diterapkan di sistem keamanan firewall PC Router. Analisa ini didapatkan dengan melihat log prefix yang ada pada paket-paket tersebut, dalam hal ini paket-paket tersebut memiliki log prefix "DROP PKT". Berikut merupakan hasil sampel data log paket dari scan nmap.



Gambar 4.10 Tampilan Sampel Log Iptables

Pada Gambar 4.10 diatas, tidak berbeda jauh dengan Gambar 4.4 dari pengujian sebelumnya yaitu sampel paket yang di-log oleh Iptables berupa nilai-nilai yang ada pada TCP/IP Header. Apabila terdapat ribuan paket yang di-log oleh Iptables dengan format yang sama dengan Gambar 4.4 dan 4.10, maka untuk dapat mengenali dan mengetahui secara spesifik mengapa paket tersebut di-log dan drop oleh firewall serta jenis serangan yang dilakukan terhadap server, diperlukan waktu dan tenaga yang lebih sehingga menjadi tidak efisien. Berikut merupakan sampel log yang dihasilkan oleh Psad.



Gambar 4.11 Tampilan Log Psad

Pada Gambar 4.11, dijelaskan bahwa Psad mendeteksi suatu serangan/scan yang dilakukan oleh komputer dengan alamat IP 90.10.1.100 (Attacker PC) terhadap web server dengan alamat IP (192.168.1.10) yang dimana usaha scan tersebut Psad mendeteksi sebagai DL=4. Artinya paket-paket yang dikirimkan Attacker PC lebih dari 1500 paket (dalam pengujian ini paket yang di-log oleh Iptables sebanyak 2007 paket/Gambar 4.9) atau usaha scan tersebut memiliki

suatu signature serangan yang Psad mengenalinya sebagai DL=4. Apabila dibandingkan antara Gambar 4.10 dengan 4.11, format log yang dihasilkan Psad (Gambar 4.11) lebih mudah dimengerti nilai-nilainya dibandingkan format log Iptables dan dengan demikian admin dapat lebih cepat mengenali dan tanggap terhadap serangan yang dilakukan terhadap web server. Untuk dapat lebih mengenali serta mengetahui secara detil serangan/scan paket apa saja yang dilakukan terhadap web server private cloud, berikut merupakan hasil laporan yang dikeluarkan Psad terhadap scan nmap tersebut.

```
[+] Top 25 attackers:
      90.10.1.100     DL: 4, Packets: 2005, Sig count: 80, (local IP)

[+] Top 20 scanned ports:
      tcp 8080  3 packets
      tcp 23    3 packets
      tcp 554   3 packets
      tcp 1723  3 packets
      tcp 143   3 packets
      tcp 445   3 packets
      tcp 110   3 packets
      tcp 3306  3 packets
      tcp 3389  3 packets
      tcp 8300  2 packets
      tcp 5666  2 packets
      tcp 8009  2 packets
      tcp 1169  2 packets
      tcp 5679  2 packets
      tcp 5030  2 packets
      tcp 32    2 packets
      tcp 1049  2 packets
      tcp 90    2 packets
      tcp 1801  2 packets
      tcp 6006  2 packets

[+] iptables log prefix counters:
      "DROP PKT": 2006

    iptables auto-blocked IPs:
        [NONE]

    Total packet counters: tcp: 2003 icmp: 2

[+] IP Status Detail:

SRC:  90.10.1.100, DL: 4, Dsts: 1, Pkts: 2005, Unique sigs: 19, Email alerts: 0, Local IP

    DST: 192.168.1.10, Local IP
        Scanned ports: TCP 1-65389, Pkts: 2003, Chain: FORWARD, Intf: eth0
```

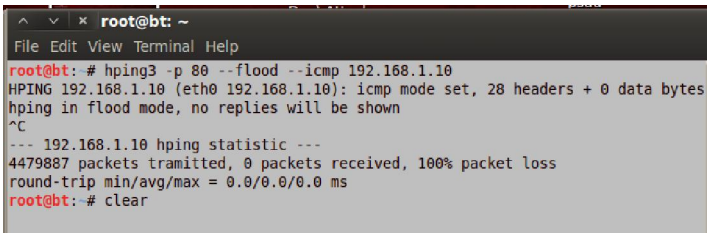
Gambar 4.12 Tampilan Laporan Psad

Pada Gambar 4.12, dijelaskan secara rinci mengenai paket-paket yang di-log karena scan nmap yang dilakukan. Dalam laporan tersebut ada bagian yang kosong atau bernilai [NONE] yaitu pada bagian iptables auto-blocked IPs: . Ini dikarenakan fitur IDS pada Psad tidak diaktifkan (OFF) sehingga apabila suatu Alamat IP melakukan serangan yang melebihi batas toleransi yang diijinkan oleh sistem keamanan (Danger Level/DL), tidak akan dilakukan pemblokiran alamat IP. Untuk penjelasan lebih detil mengenai hasil laporan Psad pada gambar diatas beserta signature-signature scan yang dilakukan tersebut akan dijelaskan pada lampiran.

Ketika dilakukan pengujian nmap scan kembali, hasil data log Iptables bertambah dari yang asalnya 2006 menjadi 4012 paket. Dari hasil yang didapat tersebut tidak berbeda jauh dengan pengujian sebelumnya (PC Router sebagai Firewall), dimana ketika dilakukan nmap scan kembali setelah percobaan pertama paket yang di-log oleh Iptables bertambah sekitar 1990-2010 paket.

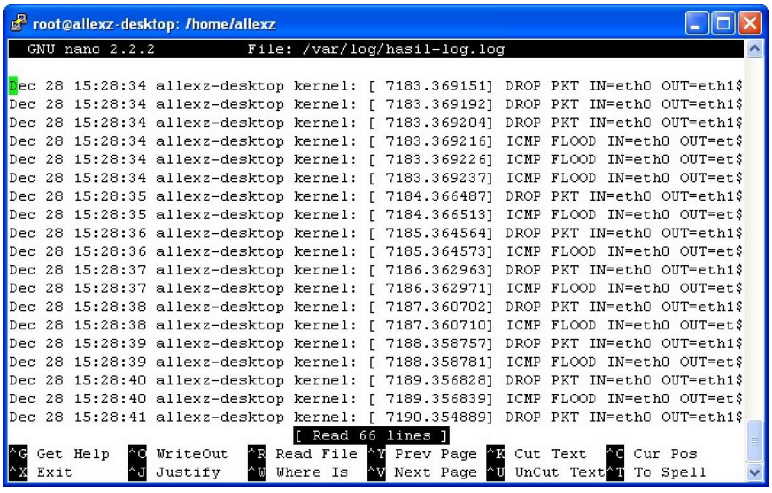
4.1.2.2 Pengujian menggunakan Hping3

Sama seperti pengujian sebelumnya (PC Router sebagai Firewall, bagian 4.1.2.2), untuk melakukan ICMP Flood dengan Hping3, ketikkan perintah berikut pada terminal dan perhatikan hasilnya pada server dan data log ketika firewall Iptables dan Log Analysis Psad diterapkan:



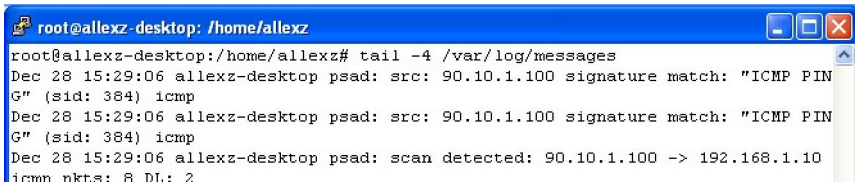
Gambar 4.13 Tampilan ICMP Flood Firewall & Log Analysis On

Pada Gambar 4.13 diatas paket yang dikirimkan/dihasilkan hping3 selama 30 detik adalah sebanyak 4479887 paket. Dan hasil yang didapatkan tidak berbeda jauh dengan pengujian sebelumnya (Gambar 4.5, Bagian 4.1.2.2). Berikut merupakan data log Iptables dari ICMP Flood yang dilakukan.



Gambar 4.14 Tampilan Jumlah Paket Log

Gambar 4.14 menunjukkan bahwa Iptables melakukan log paket dari ICMP Flood yang dilakukan oleh Attacker PC sebanyak 66 paket. Sama seperti dengan jumlah paket yang dihasilkan dari pengujian sebelumnya (Gambar 4.6, Bagian 4.1.2.2). yaitu berjumlah 66 paket. Selanjutnya merupakan sampel log oleh Psad dari usaha DOS ICMP Flood yang dilakukan.



Gambar 4.15 Tampilan Sampel Log Psad

Pada Gambar 4.15 hasil yang didapatkan tidak berbeda jauh dengan pengujian menggunakan nmap (Gambar 4.11). Hanya, pada pengujian menggunakan ICMP Flood, Psad mendeteksi bahwa serangan/scan yang dilakukan dari penyerang adalah berupa paket ICMP dengan kode 8 (ICMP_ECHO_REQUEST) serta memiliki Danger Level/DL bernilai 2 karena cocok dengan signature ICMP PING yang dimiliki Psad. Berikut merupakan hasil laporan yang dihasilkan Psad terhadap ICMP Flood yang dilakukan.

```
root@allexz-desktop:/home/allexz# psad -S
[+] psadwatchd (pid: 2530)  %CPU: 0.0  %MEM: 0.0
    Running since: Fri Dec 28 15:28:21 2012

[+] psad (pid: 2528)  %CPU: 0.0  %MEM: 0.6
    Running since: Fri Dec 28 15:28:21 2012
    Command line arguments: [none specified]
    Alert email address(es): root@localhost

[+] Version: psad v2.2

[+] Top 50 signature matches:
      "ICMP PING" (icmp),  Count: 66,  Unique sources: 1,  Sid: 384

[+] Top 25 attackers:
      90.10.1.100     DL: 2, Packets: 66, Sig count: 66, (local IP)

[+] Top 20 scanned ports:
        [NONE]

[+] iptables log prefix counters:
      "DROP PKT": 33
      "ICMP FLOOD": 33

    iptables auto-blocked IPs:
        [NONE]

    Total packet counters: icmp: 66

[+] IP Status Detail:

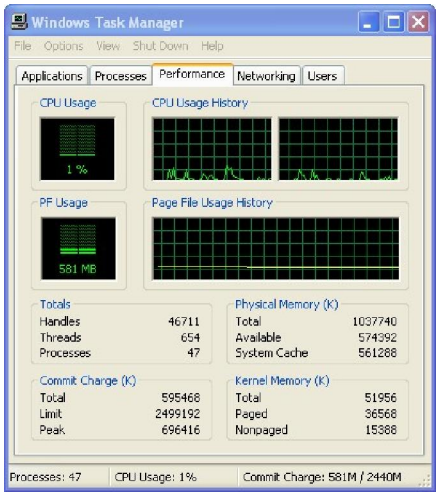
SRC:  90.10.1.100, DL: 2, Dsts: 1, Pkts: 66, Unique sigs: 1, Email alerts: 0, Local IP

    DST: 192.168.1.10, Local IP
        Signature match: "ICMP PING"
```

Gambar 4.16 Tampilan Laporan Psad

Pada Gambar 4.16, di dapatkan hasil laporan tidak berbeda jauh dengan pengujian yang sebelumnya dilakukan pada laporan Psad dijelaskan secara detil

mengenai serangan/scan yang terjadi tetapi pada Gambar 4.16 tersebut pada bagian Top 50 signatures mantches terdapat suatu keterangan terhadap serangan/scan yang terjadi yaitu “ICMP PING”. Berikut merupakan hasil yang terjadi pada server terhadap serangan ICMP Flood yang dilakukan.



Gambar 4.17 Tampilan CPU Usage Server

Pada Gambar 4.17, merupakan CPU Usage web server ketika web server diserang dengan ICMP Flood bernilai antara 0-1% dan hasilnya tidak berbeda jauh dengan pengujian sebelumnya. Dari hasil-hasil yang didapatkan pada pengujian PC Router sebagai Firewall dan Log Analysis, sistem keamanan Firewall pada PC Router bekerja dengan optimal serta Psad bekerja dengan baik dalam mendeteksi serta menerjemahkan (parse) pesan log dari iptables menjadi lebih mudah dimengerti sehingga dapat lebih cepat serta efisien dalam menanggapi suatu serangan yang terjadi.

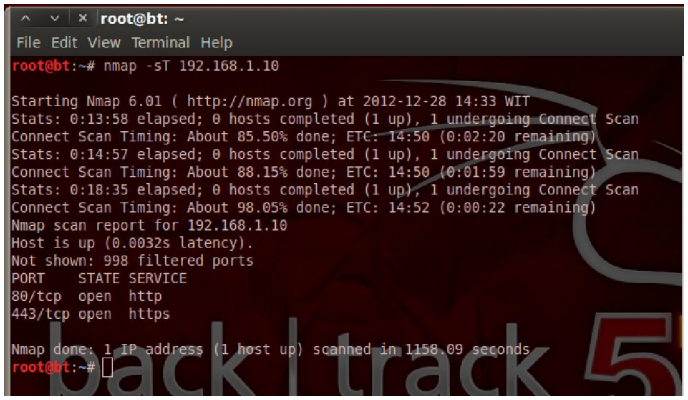
4.1.3 PC Router Sebagai Firewall, Log Analysis dan IDS

Pada pengujian ini sama dengan Pengujian PC Router sebagai Firewall dan Log Analysis, tetapi ditambahkan fitur IDS yang sudah ada pada Psad yang dimana IDS tersebut bertujuan untuk membuat Iptables dan Psad bertindak secara aktif (dalam hal ini mem-blok, tidak hanya mendeteksi) terhadap suatu alamat IP yang melakukan serangan/scan. Dimana parameter IDS melakukan blok suatu alamat IP adalah Danger Level/DL. Danger Level merupakan suatu parameter yang dimana digunakan oleh Psad untuk menentukan apakah suatu paket

berbahaya atau tidaknya dilihat dari karakteristik suatu scan/serangan (jumlah paket, port range, dan waktu interval), dan signature paket tersebut. Pada pengujian PC Router sebagai Firewall, Log Analysis dan IDS, Danger Level yang diatur untuk IDS melakukan blok alamat IP secara otomatis adalah DL=2. Ini artinya apabila suatu alamat IP mengirimkan paket dalam satu waktu lebih dari 15 paket atau cocok dengan suatu signature yang memiliki DL=>2 maka IDS akan memblok alamat sumber IP tersebut. Untuk lebih jelasnya mengenai Danger Level dapat dilihat pada lampiran.

4.1.3.1 Pengujian Menggunakan Nmap

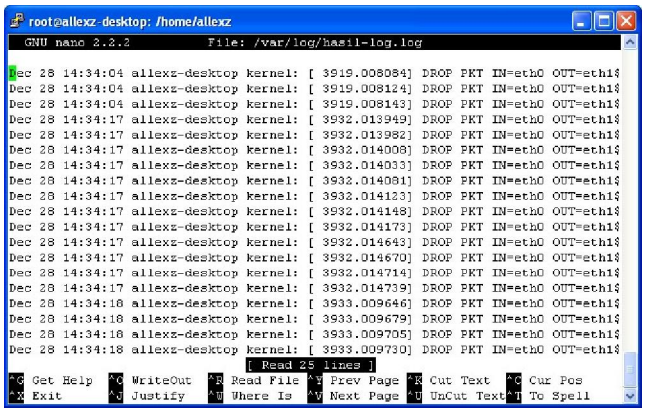
Sama seperti pengujian-pengujian sebelumnya dilakukan Port Scan/Sweep dengan menggunakan Nmap TCP Connect() Scan untuk mengetahui mengenai kinerja Sistem keamanan Firewall, Log Analysis dan IDS yang dirancang dan lihat hasil data log-nya.



Gambar 4.18 Tampilan Hasil Scan Nmap Firewall & IDS On

Pada Gambar 4.18 hasil yang didapatkan yaitu nmap menyelesaikan port scan-nya selama 1158,09 detik. Ternyata pada Pengujian PC Router sebagai Firewall, Log Analysis dan IDS, sistem keamanan yang dirancang dapat menghambat usaha nmap dalam melakukan pengumpulan informasi terhadap layanan-layanan yang disediakan web server cloud. Ini dikarenakan ketika nmap melakukan scan, sistem keamanan pada PC Router mendeteksi ada suatu serangan scan yang melebihi DL yang ditentukan sehingga ketika nmap masih berjalan IDS memblok alamat IP Attacker PC yang melakukan nmap scan. Sehingga waktu

yang dibutuhkan nmap untuk menyelesaikan usaha scan-nya sangat lama apabila dibandingkan dengan pengujian-pengujian sebelumnya. Selanjutnya merupakan hasil log dari Psad terhadap nmap port scan yang dilakukan.



Gambar 4.19 Tampilan Data Log Iptables

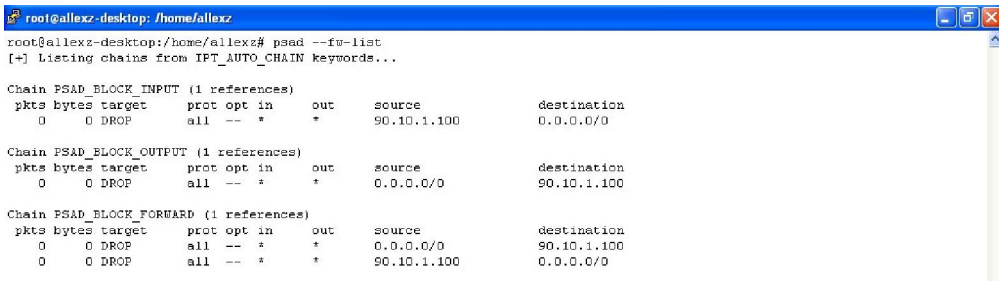
Pada Gambar 4.19 diatas, hasil yang didapatkan berbeda jauh dengan pengujian-pengujian sebelumnya. Karena pada pengujian-pengujian sebelumnya jumlah paket yang di-log oleh Iptables berjumlah ribuan, tetapi pada Pengujian PC Router sebagai Firewall, Log Analysis dan IDS, jumlah paket yang di-log sangat sedikit, hanya 25 paket. Ini disebabkan ketika nmap melakukan scan, paket yang dikirimkan ada yang mempunyai signature serangan DL=>2, sehingga IDS memblok alamat IP yang melakukan scan tersebut dan paket-paket selanjutnya tidak bias masuk/ditolak oleh sistem keamanan. Berikut merupakan data log Psad ketika IDS berfungsi:



Gambar 4.20 Tampilan Data Log Psad

Pada Gambar 4.20, di baris ketiga terdapat suatu keterangan bahwa Psad menambahkan suatu rules secara otomatis kedalam Rule Set Iptables yang dimana Rules tersebut untuk memblok alamat 90.10.1.100. Ini artinya adalah fitur IDS aktif untuk memblok Alamat IP 90.10.1.100 selama 3600 detik karena IP tersebut

telah mengirimkan paket yang melebihi batas toleransi atas paket tersebut berisi suatu signature melebihi yang diizinkan (Danger Level/DL) oleh Psad yang dimana Danger Level Psad bernilai 2 (150 paket). Sehingga apabila suatu alamat IP mengirimkan suatu paket dalam suatu rentang waktu melebihi atau bernilai sama dengan Danger Level (dalam hal ini DL=2=150 paket) serta memiliki signature yang bernilai DL=>2, maka alamat IP tersebut akan di-blok oleh Psad dengan menambahkan Rules kedalam Rule Set Iptables secara otomatis sesuai waktu yang ditentukan (dalam hal ini 3600 detik/1 jam). Untuk membuktikan apakah Psad secara otomatis menambahkan rules kepada Iptables, berikut merupakan hasil Rules yang ditambahkan psad pada Rule Set Iptables.



Gambar 4.21 Tampilan Hasil Ketika Psad Memasukkan Rule pada Firewall

Pada Gambar 4.21 didapatkan hasil bahwa Psad telah memasukkan Rules kedalam Rule Set Iptables untuk memblok alamat IP yang melakukan serangan. Untuk lebih jelas mengetahui secara detil serangan apa yang dilakukan pada server serta apakah ada keterangan alamat IP 90.10.1.100 telah di-blok oleh Iptables dan Psad berikut merupakan hasil laporan Psad yang dihasilkan.

```
[+] Top 25 attackers:
      90.10.1.100      DL: 2, Packets: 24, Sig count: 6, (local IP)

[+] Top 20 scanned ports:
      tcp 25    2 packets
      tcp 8888  2 packets
      tcp 3389  2 packets
      tcp 554   2 packets
      tcp 1720  2 packets
      tcp 143   2 packets
      tcp 256   2 packets
      tcp 23    2 packets
      tcp 113   2 packets
      tcp 587   2 packets
      tcp 995   1 packets
      tcp 3306  1 packets

[+] iptables log prefix counters:
      "DROP PKT": 25

    iptables auto-blocked IPs:
      90.10.1.100 (2276 seconds remaining)

    Total packet counters: tcp: 22 icmp: 2

[+] IP Status Detail:

SRC:  90.10.1.100, DL: 2, Dsts: 1, Pkts: 24, Unique sigs: 2, Email alerts: 0, Local IP

    DST: 192.168.1.10, Local IP
        Scanned ports: TCP 23-8888, Pkts: 22, Chain: FORWARD, Intf: eth0
```

Gambar 4.22 Tampilan Laporan Psad

Pada Gambar 4.22 diatas menjelaskan bahwa Psad telah memasukkan/membuat alamat IP 90.10.1.100 untuk di-blok secara otomatis karena telah melebihi Danger Level yang sebelumnya telah ditentukan (DL=2). Dapat dilihat pada bagian iptables auto-blocked IPs: terdapat keterangan bahwa alamat IP 90.10.1.100 telah di-blok dan waktu yang tersisa Rules blok IP tersebut berlaku tinggal 2276 detik (dari yang sebelumnya 3600 detik). Berikut merupakan tampilan hasil ketika Attacker PC melakukan nmap scan kembali setelah Psad memasukkan Rules secara otomatis kedalam Rule Set Iptables.

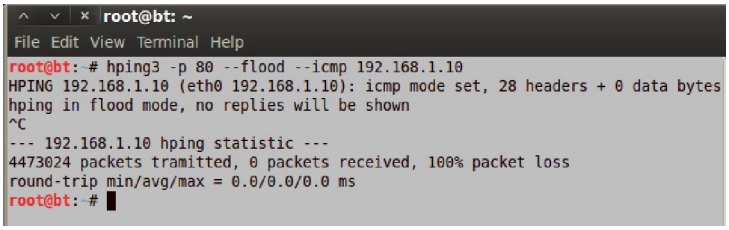


Gambar 4.23 Tampilan Hasil Scan Nmap Setelah Diblok

Terlihat pada gambar 4.23 diatas ketika Attacker PC melakukan Nmap TCP Connect () Scan kembali pada web server cloud, hasil yang didapatkan tidak menampilkan hasil port scan bila dibandingkan dengan Gambar 4.19 yang masih mengeluarkan laporan port/layanan mana yang terbuka dan tersedia. Dengan demikian sistem keamanan yang telah dirancang (Firewall dan IDS) bekerja dengan optimal dalam menanggapi suatu serangan port scan.

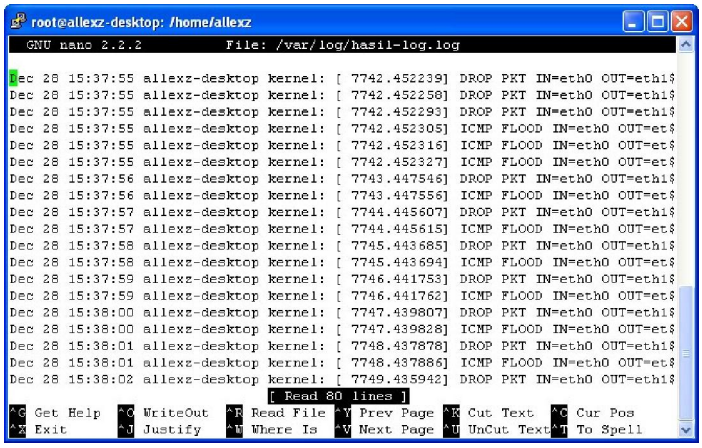
4.1.3.2 Pengujian menggunakan Hping3

Sama seperti keadaan pengujian sebelumnya, untuk melakukan ICMP Flood dengan Hping3, ketikkan perintah berikut pada terminal untuk melakukan serangan dan perhatikan hasil nya pada server dan data log, rules Iptables, fitur IDS ketika firewall Iptables , Log Analysis dan IDS Psad diterapkan.



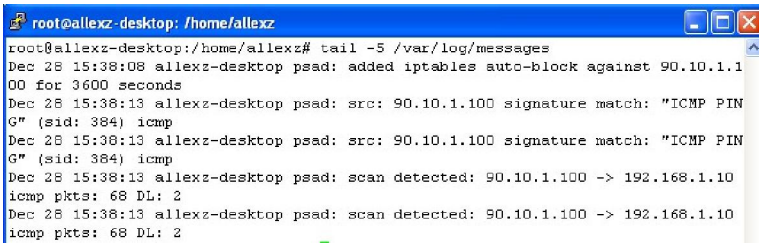
Gambar 4.24 Tampilan ICMP Flood Hping3

Dari Gambar 4.24, hping3 mengirimkan paket ICMP_ECHO_REQUEST sebanyak 4473024 paket selama 30 detik. Hasil yang didapatkan pada pengujian ini tidak berbeda jauh dengan pengujian-pengujian sebelumnya. Berikut merupakan hasil data log Iptables dari serangan yang dilakukan.



Gambar 4.25 Tampilan Jumlah Log Iptables

Gambar 4.25 menjelaskan paket yang di log oleh Iptables berjumlah 80 paket. Walaupun hasil data log yang didapatkan dari Iptables pada pengujian PC Router sebagai Firewall, Log Analysis dan IDS lebih banyak dari pengujian-pengujian sebelumnya (Gambar 4.6 dan 4.14), tetapi tidak berbeda jauh analisa terhadap perbedaan jumlah paket yang dikirimkan hping3 dengan yang di log oleh sistem keamanan. Berikut merupakan hasil log dari Psad.



Gambar 4.26 Tampilan Log Psad

Pada Gambar 4.26, hasil yang didapatkan tidak berbeda jauh dengan pengujian yang sebelumnya dilakukan (Gambar 4.15). Pada hasil pengujian ini oleh Psad terdapat beberapa baris yang menandakan bahwa Psad mendeteksi suatu serangan/scan yang cocok dengan signature serangan, dalam hal ini ICMP PING. Sehingga Psad menambahkan Rules kedalam Rule Set Iptables untuk memblok suatu alamat IP yang melakukan serangan selama 3600 detik. Berikut merupakan hasil laporan yang dihasilkan Psad terhadap serangan ICMP Flood yang dilakukan.

```
[+] Version: psad v2.2

[+] Top 50 signature matches:
      "ICMP PING" (icmp),  Count: 80,  Unique sources: 1,  Sid: 384

[+] Top 25 attackers:
      90.10.1.100     DL: 2, Packets: 80, Sig count: 80, (local IP)

[+] Top 20 scanned ports:
        [NONE]

[+] iptables log prefix counters:
      "DROP PKT": 40
      "ICMP FLOOD": 40

    iptables auto-blocked IPs:
      90.10.1.100 (3434 seconds remaining)

    Total packet counters: icmp: 80

[+] IP Status Detail:

SRC:  90.10.1.100, DL: 2, Dsts: 1, Pkts: 80, Unique sigs: 1, Email alerts: 0, Local IP

    DST: 192.168.1.10, Local IP
        Signature match: "ICMP PING"
```

Gambar 4.27 Tampilan Laporan Psad

Pada Gambar 4.27 diatas menjelaskan secara detil serangan apa saja yang terjadi terhadap web server. Hasil laporan yang dihasilkan tidak berbeda jauh dengan hasil pengujian yang sebelumnya dilakukan. Hanya, pada pengujian ini, keterangan iptables auto-blocked IPs:, terisi dengan alamat IP 90.10.1.100, ini menandakan bahw a IDS Psad bekerja dalam melakukan blok alamat IP. Berikut merupakan Rules yang ditambahkan Psad kedalam Rule Set Iptables.

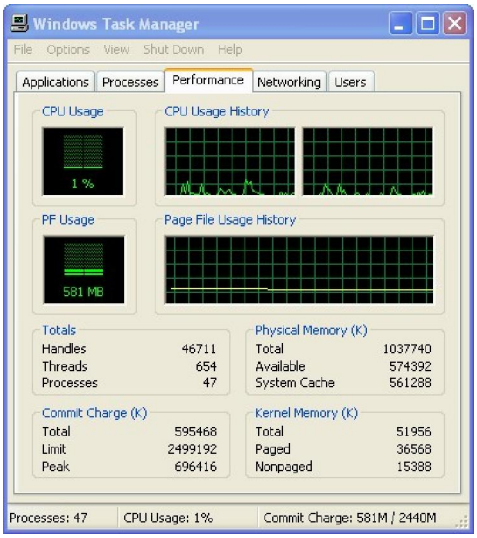
```
Chain PSAD_BLOCK_FORWARD (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  *      *       0.0.0.0/0            90.10.1.100
 2009  121K DROP       all  --  *      *       90.10.1.100          0.0.0.0/0

Chain PSAD_BLOCK_INPUT (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  *      *       90.10.1.100          0.0.0.0/0

Chain PSAD_BLOCK_OUTPUT (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  *      *       0.0.0.0/0            90.10.1.100
```

Gambar 4.28 Tampilan Auto-added Rules IDS

Pada Gambar 4.28, Psad telah memasukkan Rules kedalam Rule Set Iptables dalam melakukan blok alamat IP tertentu. Tidak berbeda jauh dari hasil yang didapatkan pada pengujian yang sebelumnya dilakukan. Berikut merupakan dampak yang terjadi pada server ketika ICMP Flood dilakukan ketika PC Router sebagai Firewall, Log Analysis, dan IDS.



Gambar 4.29 Tampilan CPU Usage Server

Pada Gambar 4.29, CPU Usage server yang terjadi ketika ICMP Flood dilakukan bernilai 0-1%, tidak berbeda jauh dengan pengujian-pengujian sebelumnya. Dengan kata lain, sistem keamanan yang dirancang, bekerja dengan optimal dalam menanggapi serangan ICMP Flood yang dilakukan. Dan hasilnya adalah ketika Attacker PC melakukan serangan ICMP Flood selama 30 detik kembali, hasil data log pada PC Router tetap berjumlah sama (yaitu 80 paket), ini artinya IDS bekerja dengan optimal dalam melakukan blok alamat IP sumber yang melakukan serangan ICMP Flood. Pada pengujian-pengujian sebelumnya ketika

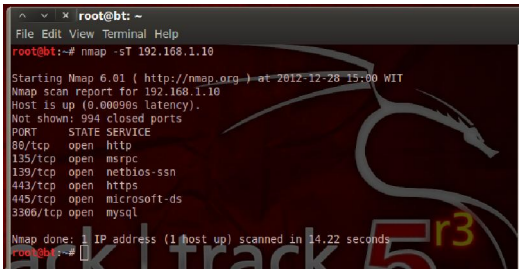
dilakukan usaha ICMP Flood kembali pada web server cloud, paket yang di-log oleh sistem keamanan mengalami kenaikan jumlahnya.

4.1.4 PC Router Tanpa Firewall, Log Analysis dan IDS

Pada pengujian PC Router tanpa Firewall, Log Analyis dan IDS, PC Router hanya berfungsi melakukan Routing, tanpa menerapkan sistem keamanan.

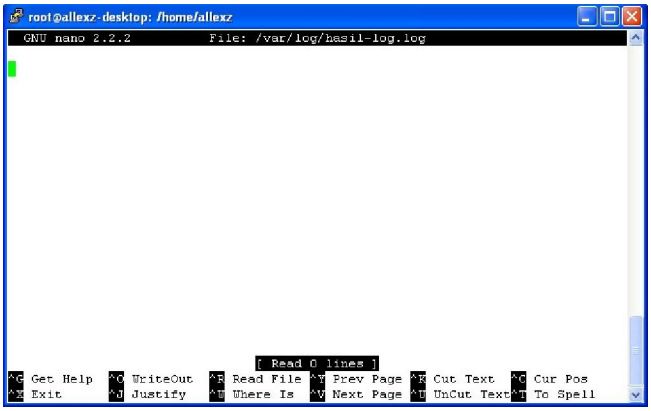
4.1.4.1 Pengujian Menggunakan Nmap

Berikut merupakan pengujian Nmap TCP Connect Scan () terhadap web server private cloud ketika PC Router tanpa Firewall, Log Analysis, dan IDS.



Gambar 4.30 Tampilan Nmap TCP Connect Scan

Pada Gambar 4.30, terlihat bahwa selain mendeteksi port 80 (http), dan 443 (https) dalam keadaan terbuka, port-port vital seperti port 135 (msrpc), 139 (netbios-ssn) , 445 (microsoft-ds), dan 3306 (mysql) pada web server private cloud terlihat dari luar dan dalam keadaan terbuka. Karena secara umum port yang dibuka pada web server hanya port 80, 443, tetapi pada hasil nmap pada Gambar 4.30 port yang bersifat khusus dalam keadaan terlihat dan terbuka. Dengan demikian menambah resiko serta rentan terhadap penyerang yang memanfaatkan port yang terbuka serta vital tersebut untuk masuk ke dalam sistem. Berikut merupakan data log Iptables dari scan nmap yang dilakukan.



Gambar 4.31 Tampilan Hasil Log Iptables

Pada Gambar 4.31 terlihat bahwa Iptables sama sekali tidak melakukan log terhadap paket yang menuju web server private cloud karena PC Router hanya melakukan Routing /mem-forward. Sehingga web server rentan karena paket apapun dapat memasuki PC Router. Berikut merupakan hasil laporan data log dari Psad.

```
root@allexz-desktop:/home/allexz# psad -S
[+] psadwatchd (pid: 2096)  %CPU: 0.0  %MEM: 0.0
    Running since: Thu Dec 27 19:47:17 2012

[+] psad (pid: 2094)  %CPU: 0.0  %MEM: 0.6
    Running since: Thu Dec 27 19:47:17 2012
    Command line arguments: [none specified]
    Alert email address(es): root@localhost

[+] Version: psad v2.2

[+] Top 50 signature matches:
        [NONE]

[+] Top 25 attackers:
        [NONE]

[+] Top 20 scanned ports:
        [NONE]

[+] iptables log prefix counters:
        [NONE]

    iptables auto-blocked IPs:
        [NONE]

    Total packet counters:

[+] IP Status Detail:
        [NONE]

    Total scan sources: 0
    Total scan destinations: 0

[+] These results are available in: /var/log/psad/status.out
```

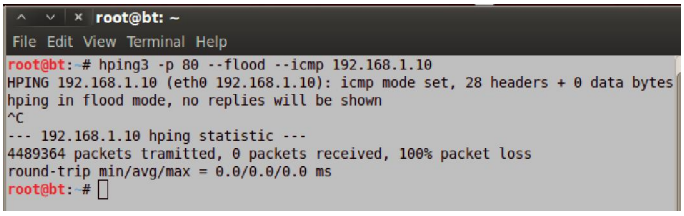
Gambar 4.32 Tampilan Laporan Psad

Pada Gambar 4.32 terlihat hasil laporan Psad tidak melaporkan sama sekali terhadap nmap scan yang dilakukan. Ini dikarenakan karena Iptables sama sekali tidak melakukan log paket atau PC Router tidak menggunakan fungsi Iptables sebagai firewall dan log paket serta men-drop-nya kemudian. Dan karena Iptables

firewall dalam keadaan tidak berfungsi sehingga otomatis fitur IDS pada Psad tidak berfungsi.

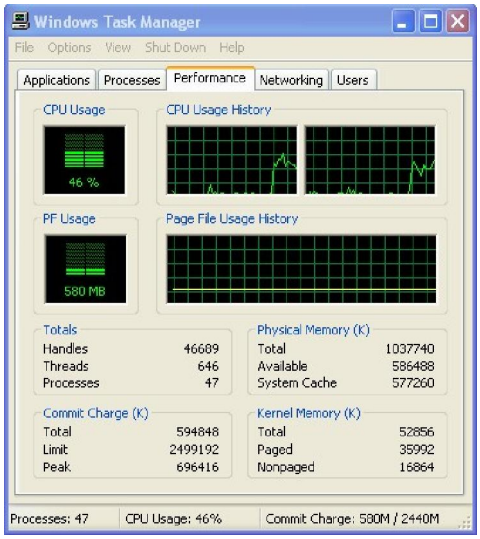
4.1.4.2 Pengujian Menggunakan Hping3

Berikut merupakan pengujian ketika Attacker PC melakukan serangan DOS ICMP Flood menggunakan hping3 terhadap web server private cloud ketika PC Router tanpa Firewall, Log Analysis dan IDS.



Gambar 4.33 Tampilan ICMP Flood Hping3

Pada Gambar 4.33 menunjukkan Attacker PC mengirimkan paket ICMP_ECHO_REQUEST pada web server private cloud selama 30 detik sebanyak 4489364 paket. Berikut merupakan dampak pada CPU Usage web server private cloud ketika ICMP Flood dilakukan.



Gambar 4.34 Tampilan CPU Usage Web Server

Pada Gambar 4.34 terlihat bahwa CPU Usage web server ketika ICMP Flood dilakukan membuat CPU Usage web server mengalami kenaikan hingga

mencapai 45-49% dari yang awalnya hanya berkisar 0-1%. Ini membuktikan bahwa web server terpengaruh dari serangan DOS ICMP Flood dan rentan crash apabila dilakukan serangan DOS terus-menerus. Karena web server sama sekali tidak terlindung oleh sistem keamanan.

4.2 Tabel Hasil Pengujian

Untuk lebih mudah menganalisa hasil-hasil dari setiap pengujian, berikut merupakan tabel hasil pengujiannya.

Tabel 4.1 Hasil Pengujian Menggunakan Nmap

No	Pengujian	Status IDS	Jumlah Paket yang di Log		Hasil Port Scan Nmap	
			Percobaan 1	Percobaan 2	Percobaan 1	Percobaan 2
1	PC Router Sebagai Firewall	OFF	2006	4012	53 (closed), 80 (open), 443 (open)	53 (closed), 80 (open), 443 (open)
2	PC Router Sebagai Firewall dan Log Analysis	OFF	2006	4012	80 (open), 443 (open)	53 (closed), 80 (open), 443 (open)
3	PC Router Sebagai Firewall, Log Analysis dan IDS	ON	25	25	53 (closed), 80 (open), 443 (open)	NONE (BLOCKED)
4	PC Router Tanpa Firewall, Log Analysis dan IDS	OFF	0	0	80 (open), 135 (open), 139 (open), 443 (open), 445 (open), 3306 (open)	80 (open), 135 (open), 139 (open), 443 (open), 445 (open), 3306 (open)

Pada Tabel 4.1 diatas, dapat terlihat bahwa sistem keamanan yang paling aman/baik adalah pada pengujian ketiga yaitu PC Router Sebagai Firewall, Log Analysis dan IDS. Dikarenakan adalah ketika Attacker PC melakukan serangan

Port Scan (percobaan 1) terhadap web server Private Cloud, serangan tersebut menyebabkan IDS bekerja secara otomatis mem-blok alamat IP yang melakukan serangan. Sehingga ketika Attacker PC melakukan Port Scan kembali (percobaan 2), pada hasil port scan-nya port-port pada web server tidak terlihat dan tertutup untuk Attacker PC. Serta jumlah paket yang di-log Iptables sama seperti sebelumnya, yaitu 25 paket. Ditambah waktu yang diperlukan nmap dalam menyelesaikan scan lebih lama apabila dibandingkan dengan pengujian yang sebelumnya. Ini artinya bahwa IDS sukses melakukan blok alamat IP Attacker PC.

Sedangkan yang paling tidak aman/baik adalah pada pengujian 4 (PC Router Tanpa Firewall, Log Analysis dan IDS). Karena pada pengujian 4, ketika port scan dilakukan. Didapatkan hasil bahwa port yang terbuka dan terlihat oleh Attacker PC selain Port-port yang secara umum terbuka (port 80, 443), port-port vital pun terlihat dari luar seperti port 135, 139, 445, dan 3306 sehingga menambah resiko keamanan Web Server itu sendiri. Karena pada pengujian 4 Sistem keamanan tidak diaktifkan, maka hasilnya sama sekali tidak ada paket yang di-log oleh firewall.

Tabel 4.2 Hasil Pengujian Mengguunakan Hping3

No	Pengujian	Status IDS	Jumlah Paket dikirim Hping3		Jumlah Paket yang Di-Log		CPU Usage Server
			(Percobaan 1)	(Percobaan 2)	(Percobaan 1)	(Percobaan 2)	
1	PC Router Sebagai Firewall	OFF	4381686	4467485	64	130	0-1%
2	PC Router Sebagai Firewall dan Log Analysis	OFF	4479887	4505001	66	132	0-1%
3	PC Router Sebagai Firewall, Log Analysis dan IDS	ON	4473024	4482804	80	80	0-1%
4	PC Router Tanpa Firewall, Log Analysis dan IDS	OFF	4489364	4491140	0	0	43-49%

Pada Tabel 4.2, dapat terlihat bahwa sistem keamanan yang paling baik, adalah sistem keamanan yang digunakan pada pengujian 3 (PC Router sebagai Firewall, Log Analysis dan IDS). Karena ketika dilakukan ICMP Flood pada percobaan 1, Attacker PC yang melakukan serangan, di-blok alamat IP-nya oleh IDS sehingga menyebabkan ketika Attacker PC melakukan serangan kembali sistem keamanan pada PC Router memblok paket-paket yang berasal dari Attacker PC. Ini dibuktikan dengan jumlah paket yang di-log sesudah percobaan 1 dan 2 berjumlah sama (80 paket). Sedangkan pada pengujian lain (Pengujian 1 dan 2) jumlah paket yang di-log setelah percobaan 1 dan 2 mengalami kenaikan.

Sebaliknya pada pengujian PC Router tanpa Firewall, Log Analysis dan IDS, Web Server Private Cloud rentan terhadap serangan DOS ICMP Flood yang dilakukan karena tidak menggunakan sistem keamanan. Sehingga pada pengujian PC Router tanpa Firewall, Log Analysis dan IDS, CPU Usage pada Web Server Private Cloud mengalami kenaikan menjadi 43-49%. Sedangkan pada pengujian-pengujian sebelumnya Web Server tidak terpengaruh terhadap serangan DOS, dibuktikan dengan nilai CPU Usage Web Server bernilai 0-1%.

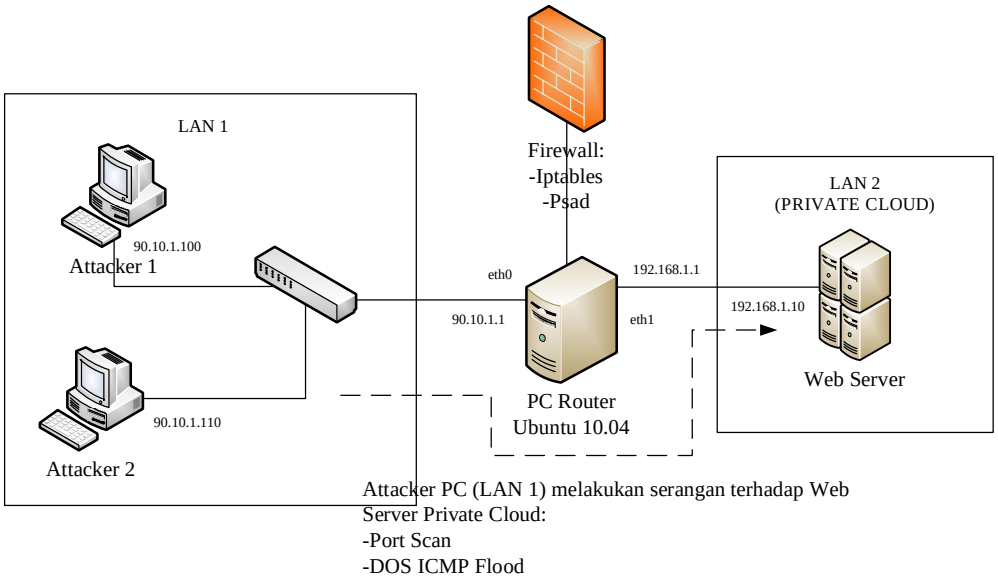
Sebagai tambahan berikut merupakan tabel penjelasan fungsi masing-masing port berdasarkan hasil-hasil yang didapatkan dari pengujian yang dilakukan:

Tabel 4.3 Penjelasan Port-port dari Hasil Pengujian

No	Port	Keterangan
1	53	Layanan DNS (Domain Name System) Untuk keperluan Transfer domain.
2	80	Layanan HTTP (Web), Untuk membuka halaman Web
3	135	Layanan Msrpc (Microsoft Remote Procedure Call) Untuk melalukan Remote kepada PC dengan OS Microsoft
4	139	Layanan Netbios-ssn, digunakan PC yang menggunakan OS sebelum Windows 2000 (untuk keperluan FTP, remote dan lain-lain.)
5	443	Layanan HTTPS (Web Secure) Sering digunakan dalam proses Login
6	445	Layanan Microsoft-DS, digunakan untuk resource sharing contohnya seperti File Sharing untuk OS Windows 2000, XP, 2003.
7	3306	Layanan MySQL, untuk Database Server

4.3 Pengujian Menggunakan Dua Attacker PC

Pada pengujian 4.3, komputer berperan sebagai penyerang (Attacker PC) akan ditambahkan satu buah lagi menjadi dua buah Attacker PC. Tujuannya untuk mengetahui pengaruhnya terhadap sistem keamanan dan server Private Cloud itu sendiri serta dibandingkan apa perbedaan ketika menggunakan satu buah Attacker PC. Berikut merupakan gambar pengujian sistem keamanan menggunakan dua buah Attacker PC.



Gambar 4.35 Pengujian Sistem Keamanan dengan Dua Attacker PC

Dari gambar 4.35 diatas bila dibandingkan dengan gambar 4.1 hampir sama hanya perbedaanya adalah pada LAN 1 ditambahkan satu buah komputer sebagai Attacker PC sehingga terdapat dua buah Attacker PC (Attacker 1 & Attacker 2 2)

Pada pengujian menggunakan dua buah Attacker PC, sama saja metode pengujian serta penggunaan tools pengujiannya tetapi pada bagian ini hanya akan menggunakan kondisi pengujian-pengujian berikut.

1. PC Router sebagai Firewall, Log Analysis dan IDS.
2. PC Router tanpa Firewall, Log Analysis dan IDS.

Hasil pengujiannya akan dipaparkan dalam bentuk tabel serta dianalisis hasil yang didapatkan tersebut dengan pengujian menggunakan satu Attacker PC.

4.3.1 Pengujian Menggunakan Nmap dengan Dua Attacker PC

Berikut merupakan hasil yang didapatkan ketika pengujian menggunakan Tools Nmap.

Tabel 4.4 Hasil Pengujian Nmap Dua Attacker PC

No	Pengujian	Jumlah Paket yang Di Log		Hasil Port Scan Nmap			
		P1	P2	P1		P2	
				ATT 1	ATT 2	ATT 1	ATT 2
1	PC Router Sebagai Firewall, Log Analysis dan IDS	1954	1954	53 (closed), 80 (open), 443 (open)	53 (closed), 80 (open), 443 (open)	NONE (BLOCKED)	NONE (BLOCKED)
2	PC Router Tanpa Firewall, Log Analysis dan IDS	0	0	80 (open), 135 (open), 139 (open), 443 (open), 445 (open), 3306 (open)	80 (open), 135 (open), 139 (open), 443 (open), 445 (open), 3306 (open)	80 (open), 135 (open), 139 (open), 443 (open), 445 (open), 3306 (open)	80 (open), 135 (open), 139 (open), 443 (open), 445 (open), 3306 (open)

Ket:
P1= Percobaan 1, ATT 1= Attacker 1
P2= Percobaan 2, ATT 2= Attacker 2

Pada Tabel 4.4 (Pengujian Nmap dengan dua Attacker PC) diatas dapat dibandingkan dengan Tabel 4.1 (Pengujian Nmap dengan satu Attacker PC). Hasilnya adalah sama ketika menggunakan satu maupun dua buah Attacker PC. Yang membedakan hanya jumlah paket yang di log sistem keamanan. Pada Tabel 4.1 paket yang di log berjumlah 25 paket tetapi pada Tabel 4.4 paket yang di log berjumlah 1954. Ini artinya setiap penambahan Attacker PC, maka paket yang di log oleh sistem keamanan bertambah banyak sesuai dengan jumlah Attacker PC. Walaupun jumlah paket yang di log lebih banyak, sistem keamanan bekerja dengan baik, sehingga ketika dilakukan Nmap Scan kembali, Attacker 1 dan

Attacker 2 tidak mendapatkan hasil layanan-layan apa saja yang tersedia pada server karena sudah di blok alamat IP masing-masing.

4.3.2 Pengujian Menggunakan Hping3 dengan Dua Attacker PC

Berikut merupakan hasil yang didapatkan ketika pengujian menggunakan tools Hping3:

Tabel 4.5 Hasil Pengujian Menggunakan Hping3 Dua Attacker PC

No	Pengujian	Jumlah Paket yang dikirim				Jumlah Paket yang di Log		CPU Usage Server
		P1		P2		P1	P2	
		ATT 1	ATT 2	ATT 1	ATT 2			
1	PC Router Sebagai Firewall, Log Analysis dan IDS	2434590	2458932	2256965	2309563	90	90	0-1%
2	PC Router Tanpa Firewall, Log Analysis dan IDS	2568332	2477932	2436788	2403783	0	0	43-49%

Ket:
P1= Percobaan 1, ATT 1= Attacker 1
P2= Percobaan 2, ATT 2= Attacker 2

Pada Tabel 4.5 diatas (Pengujian Hping3 dua Attacker PC) dapat dibandingkan dengan Tabel 4.2 (Pengujian Hping3 satu Attacker PC). Hasilnya tidak berbeda sama sekali pengaruh serangan DOS ICMP dengan dan tanpa sistem keamanan terhadap resource server. Perbedaannya hanya pada jumlah paket yang di log oleh sistem keamanan dengan jumlah paket yang dikirimkan. Semakin banyak Attacker PC maka semakin banyak pula paket yang di log oleh sistem keamanan. Untuk jumlah paket yang dikirimkan, untuk pengujian menggunakan satu Attacker PC, paket yang dikirimkan selama 30 detik untuk dua kali percobaan berkisar 4-5 juta paket. Tetapi ketika menggunakan dua Attacker PC paket yang dikirimkan berkisar antara 2-2,5 juta paket. Perbedaan ini disebabkan karena beberapa faktor, diantaranya adalah spesifikasi Switch dan NIC yang digunakan tipe Fast Ethernet (10/100 MB) juga cara kerja Ethernet itu sendiri

yaitu menggunakan CSMA/CD (Carrier Sense Multiple Access With Collision Detection).

Pada CSMA/CD, komputer yang terhubung pada jaringan untuk mengirimkan data harus memastikan bahwa di jaringan tidak ada komputer lain yang mengirimkan jaringan agar terhindar dari tabrakan paket (collision) atau dalam satu waktu cuma satu komputer yang dapat mengirimkan paket. Dengan demikian semakin banyak komputer Attacker PC maka semakin berkurang jumlah paket yang dikirimkan.