BAB V

Hasil Dan Pembahasan

5.1. Hasil

Pada penelitian ini penulis menggunakan Metode *Action Research* untuk menyelasaikan penelitian, berikut tahapannya dari metode yang penulis lakukan.

5.1.1 Diagnosis

Pada tahap ini penulis melakukan diagnosis dengan cara menganalisis permasalahan yang ada pada perusahaan ini,

5.1.1.1 Analisis Permasalahan

Hasil analisis yang penulis lakukan dengan menggunakan secara langsung koneksi jaringan pada PT.Satria Antaran Prima. Permasalahan yang ada pada perusahaan ini adalah sering terjadi koneksi jaringan terputus pada waktu-waktu tertentu , penyebab dari koneksi terputus ini belum diketahui, pada perusahaan ini juga kemanan jaringan hanya dibangun dari vendor sebuah provider. Rujukan gambar yang menunjukkan koneksi jaringan terputus yang penulis temukan dengan menguji koneksi *ping* terhadap *www.google.com* melalui *command prompt* pada jaringan PT. Satria Antaran Prima Terlihat pada gambar 5.1.

Reply from 216.58.281.281: bytes-32 time-14ms TL-52 Reply from 216.58.281.281: bytes-32 t	C\WINDOWS\system32\cmd.exe	-	0	×
Apply from 126.58.281.281: bytes-32 time-14ss TL-52 Apply from 126.58.281.281: bytes-32 t	Reply from 216.58.203.238: bytes=32 time=14ms TTL=52			^
<pre>hepsy from 216.58.281.281 bytes-32 time-1des TL-52 hepsy from 216.58.281.281 bytes-32 time-1des TL-52 h</pre>	Reply from 216.58.203.238: bytes=32 time=14ms TTL=52			
Request timed out. Reply from 216.58,283.238: bytes-32 time-14es TL-52 Reply from 2	Reply from 216.58.203.238: bytes=32 time=14ms TTL=52			
Reply from 126.58.281.281 bytes-32 time-16ms TL-52 Reply from 126.	Request timed out.			
<pre>Meply from 126.58.80.301 bytes-12 time-ides TL-52 Meply from 216.58.80.328: bytes-12 time-ides TL-52 Me</pre>	Reply from 216.58.203.238: bytes=32 time=16ms TTL=52			
Regist Lined out. Reply form 216.56.789.728 bytes-32 line-14es TL-52 Regust Lined out. Reply form 216.58.789.728 bytes-32 line-14es TL-52 Reply form 216.58.789.728 bytes-	Reply from 216.58.203.238: bytes=32 time=14ms TTL=52			
Hequer t timed out. hequely from 116.54.201.23: bytes-32 time-14ms TTL-52 hequer t timed out. Hequer t t timed out. Hequer t t timed out. Hequer t t timed out. Hequer t t t to t timed out. Hequer t t t to t timed out. Hequer t t t t to t timed t times t the to t timed t times t the to t time t times t the to t times t t to t time	Request timed out.			
Reply from 216.58.20.28: bytes-12 time-las TL-52 Reply from 216.58.20.28: bytes-12 time-lass TL-52 Reply from 216.58.20.28: bytes-21 time-lass TL-52 Reply from 216.58.20.28: bytes-22 time-lass TL-52 Reply from 216.58.20.28: bytes-22 time-lass TL-52 Reply f	Request timed out.			
Member 1 Time out. Merphy Con 216.58.200.238: bytes-32 time-1dms TL-52 Merphy Con 216.58.200.238: bytes-32 time-1dms TL-52 Merphy Form 216.58.200.238: by	Reply from 216.58.203.238: bytes=32 time=14ms TTL=52			
Reduct TimeC out. http://com.iii.doi.org/10.101/10	Request timed out.			
mepsy from 1/b.3s.set.23: pyters.21: immediates ITL-52 meply from 1/b.3s.set.23: pyters.21: immediates ITL-52 meply from 1/b.3s.set.33: pyters.31: immediates ITL-52	Request timed out.			
mepsy from 126:38.48.238: 09/18-324 mepsy from 126:38.48.238: 09/18-324 mepsy from 126:38.48.238: 09/18-324 Reply from 126:58.48.238: 09/18-324 mess TL-52 mepsy from 126:58.48.238: 09/18-324 mess TL-52 Reply from 126:58.48.238: 09/18-324 mess TL-52 mess TL-52 mess TL-52 Reply from 126:58.48.238: 09/18-324 mess TL-52 mess TL-52 mess TL-52 Reply from 126:58.48.238: 09/18-324 mess TL-52 mess TL-52 mess TL-52 Reply from 126:58.48.238: 09/18-324 mess TL-52 mess TL-52 mess TL-52 Reply from 126:58.48.238: 09/18-324 mess TL-52 mess TL-52 mess TL-52 Reply from 126:58.48.238: 09/18-324 mess TL-52 mess TL-52 mess TL-52 Reply from 126:58.48.238: 09/18-324 mess TL-52 mess TL-52 mess TL-52 Reply from 126:58.48.238: 09/18-324 mess TL-52 mess TL-52 mess TL-52 Reply from 126:58.48.238: 09/18-324 mess TL-52 mess TL-52 mess TL-52 Reply from 126:58.48.238: 09/18-324 mess TL-52 mess TL-52 mess TL-52 mess TL-52 Reply from 126:58.48.238: 09/18-324 mess TL-52 mess TL-52 mess TL-52 mess TL-52 mess TL-5	Reply from 216.58,203.238: bytes=32 time=14ms TTL=52			
mepsy rom 10: 53.s.ds. 238: 0748-53. immedias immedia mepsy rom 216: 53.e.ds. 238: 0748-53. immedias III.53 meply rom 216: 53.e.ds. 238: 0748-53. immedias III.52 meply rom 216: 58.e.ds. 238: 0748-53. Immedias III.52 meply <td< td=""><td>Reply from 216.58.203.238: Dytes-32 time-14ms 11L-52</td><td></td><td></td><td></td></td<>	Reply from 216.58.203.238: Dytes-32 time-14ms 11L-52			
meply from 16: 65:09:01 statestates TTL-52 meply from 26: 65:09:02 statestates TTL-52	KEPIV TFOM Z16.058.203.238: Dyte5=32 Time=14MS III=52			
mbpl; from 10: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0	Reply Trom 216.50.203.230: Uytes=32 lime+14H5 IIL=32			
Reply from 126 658.023.23 Cytes-32 time-1ass TL-52 Reply from 126 658.023.23 Cytes-32 time-1ass TL-52 Reply from 126.58.023.23	Reply from 216.69, 202.329, Upter-32 Lime-14ms.1(L=52 Banly from 216.69, 202.329, Upter-32 Lime-14ms.1TL=52			
Reply from 106.68.2012.019 Cytes-21 ime-1dem TL-52 Reply from 216.68.2012.019 Pytes-22 ime-1dem TL-52 Reply from 216.68.2012.019 Pytes-32 ime-1dem TL-52 Reply from 216.68.2012.019 Pites-32 ime-1dem TL-52 Reply from 216.	Repay from 246.50 202.200 bytes=22 time-temp frt=22			
Reply from 126 688.082.38 bytes-32 time-1408 TL-52 Reply from 216.68.08.07.38 bytes-32 time-1408 TL-52	Reply from 216.52, 282.328, bytes=32 time=14ms fT1=52			
Reply from 216.68.08.03.08 bytes-32 time-14ms TL-52	Reply from 216.58, 201,238; bytes-32 time-14ms TTI=52			
Reply from 216.58.203.20 bytes-32 time-14ms TL-52 Reply from 216.58.203.20	Reply from 216.58.203.238: bytes=32 time=14ms TTL=52			
Reply from 216.58.08.128: bytes-32 time-14ms TL-52 Reply from 216.58.08.201.28: bytes-32 time-14ms TL-52	Reply from 216.58.203.238: bytes=32 time=14ms TTL=52			
Reply from 216.68.043.238: bytes-32 time-14ms TL-52 Reply from 216.58.043.238: bytes-32 time-15ms TL-52 Reply from 216.58.0438: bytes-32 time-15ms TL-52 <td>Reply from 216.58.203.238: bytes=32 time=14ms TTL=52</td> <td></td> <td></td> <td></td>	Reply from 216.58.203.238: bytes=32 time=14ms TTL=52			
Heply from 216.58.00.238: bytes-32 time-16ms TL-52	Reply from 216.58.203.238: bytes=32 time=14ms TTL=52			
Heply from 216.58.00.238: bytes-32 time-times TL-52 Heply from 216.58.00.238: bytes-32 ti	Reply from 216.58.203.238: bytes=32 time=14ms TTL=52			
Heply from 216.58.08.128: bytes-32 time-14ms TL-52 Heply from 216.58.08.201.28: bytes-32 time-14ms TL-52 Heply from 216.58.08:	Reply from 216.58.203.238: bytes=32 time=15ms TTL=52			
Reply from 216.58.08.128: bytes-32 time-14ms TL-52 Reply from 216.58.08.201.28: bytes-32 time-14ms TL-52 Reply from 216.58.08.28: bytes-32 time-14ms TL-52 <t< td=""><td>Reply from 216.58.203.238: bytes=32 time=14ms TTL=52</td><td></td><td></td><td></td></t<>	Reply from 216.58.203.238: bytes=32 time=14ms TTL=52			
Reply from 216.58.00.128: bytes-32 time-1ams TL-52 Reply for 50.58.00.128: bytes-32 time-1ams TL-52 </td <td>Reply from 216.58.203.238: bytes=32 time=14ms TTL=52</td> <td></td> <td></td> <td></td>	Reply from 216.58.203.238: bytes=32 time=14ms TTL=52			
Reply from 216.58.843.238: bytes-32 time-14ms TL-52 Reply from 216.58.243.238: bytes-32 time-15ms TL-52 Reply from 216.58.247.238: bytes-32 time-15ms TL-52 Reply from 216.58.247.248.248.248.248.248 Reply from 216.58.248.248.248.248.248.248.248.248.248.24	Reply from 216.58.203.238: bytes=32 time=13ms TTL=52			
Reply from 216.58.08.128: bytes=32 time=14ms TIt=52 Reply from 216.58.08.128: bytes=32 time=14ms TIt=52 Reply from 216.68.08.08.28: bytes=32 time=14ms TIt=52 Reply from 216.68.08.08.28: bytes=32 time=14ms TIt=52 Reply from 216.58.08.08.28: bytes=32 time=14ms TIt=52 Reply transform 216.58.08.08: 208.08: bytes=32 time=14ms TIt=52 Reply transform 216.58.08: 208.02: 08: bytes=32 time=14ms TIt=52 Reply transform 216.58.08: 08: 08: 08: 08: 08: 08: 08: 08: 08:	Reply from 216.58.203.238: bytes=32 time=14ms TTL=52			
Amply from 216,58,293.25 https://timeliams/III.52 Amply from 216,58,293.55 https://timeliams/III.55 Amply from 216,58,293.55 https://timeliams/III.55 Amply from 216,58,293.55 https://timeliams/III.55 Amply from 216,58,293.55 https://timeliams/III.55 Amply from 216,58,293.55 https://timeliams/III	Reply from 216.58.203.238: bytes=32 time=14ms TTL=52			
Adpji yrrom 126.58.vd#.248: byfes-52 ima-1568 [11-52 Apply from 126.58.vd#.248: byfes-52 ima-1468 [11-52 Request timed out. Bing statistics for 116.58.203.238: Packetis: Bing statistics for 116.58.203.238: Packetis: Bing statistics for 116.58.203.238: Control.e Dispectation Packetis: Dispectation	Reply from 216.58.203.238: bytes=32 time=14ms TTL=52			
Appj Yrom 216.58.ex.32.58: bytes-52 time-14ms Tit-52 Nequest timed out. Ping statistics for 216.56.203.238: Packets: Sent = 429, Reclued = 361, Lost = 68 (15% loss), Approximater cound trip: times inmilli-seconds: Minima = 13ms, Maximum = 29ms, Average = 14ms Control-C rc c:Usuers\bagusprtmapping google.com	Reply from 216.58,203.238: Dytes-32 time-15ms (IL-52			
Apply Troff 210-38.cs2.58: 07tes-32 time-14ms 11-52 Ping statistics for 110.58.203.238: Packets: soft - 420, Received = 361, Lost = 68 (15% loss), Approximate round trip times in milli-seconds: Minima = Joss, Naxima = Joss, Average = 14ms Control_C C:Users/baguspertmaping google.com	Reply from 216.58.203.238: Dytes=32 Time-14MS [][L=52			
Medless Limer Dot. Packets: Sent = 420, Reclude = 361, Lost = 68 (15% loss), Approximate round trip: Ines: nmilli-seconds: Minimum = 13ms, MaxAmum = 29ms, Average = 14ms Control-C rc c:Users\bagusprtmapping google.com	Reply Trom Z10-58-203-238: Dytes=32 time=14ms IIL=52			
Ping statistics for 116.58.203.238: Packets: Sent 420, Received = 361, Lost = 68 (15% loss), Approximate round trip times in milli-seconds: minima = Juns, Maximan = Juns, Average = 14ms corrol.C c:Users/bagusptmaping google.com	Request timed out.			
Packets: Sent = 420, Bacelyod = 361, Lost = 68 (15% loss), Approximate round trip: Iness in milli-seconds: Minimum = 13ms, MaxAmum = 29ms, Average = 14ms Control-C rc C:Users\bagusprtma>ping google.com	Ding statistics for 216 58 203 238			
Approximate round trip times in milli-seconds: Minimum - Jims, Maximum - 29ms, Average - 14ms Control-C °C C:\Users\bagusprtma>ping google.com	Packats: Sent = 429 , Received = 361 , Lost = 68 (15% loss).			
Minimum = 13ms, Maximum - 29ms, Average = 14ms Control-C C C:Users\bagusprtma>ping google.com	Approximate round trip times in milli-seconds:			
Control-C °C C:\Users\bagusprtmayping google.com	Minimum = 13ms, Maximum = 29ms, Average = 14ms			
cc C:Users\bagusprtmasping google.com v	Control-C			
C:\Users\bagusprtma>ping google.com	^C			
	C:\Users\bagusprtma>ping google.com			~

Gambar 5.1: Hasil Uji Koneksi

Rujukan gambar 5.1 menunjukan koneksi jaringan dari hasil pengujian hari pertama selama beberapa menit didapatkan jarinan sering terputus dengan paket *lost* sebesar 15 persen .



Gambar 5.2: Hasil Uji Koneksi

Rujukan gambar 5.2 menunjukan koneksi jaringan dari hasil pengujian hari kedua jaringan sering terputus



Gambar 5.3: Hasil Uji Koneksi

Rujukan gambar 5.3 menunjukan koneksi jaringan dari hasil pengujian hari kedua jaringan sering terputus dengan paket *lost* sebesar 34 persen

5.1.1.2 Analisis Topologi Jaringan

Setelah melihat secara langsung pada PT.Satria Antaran Prima topologi jaringan yang di gunakan pada perusahaan ini adalah topologi *star* seperti terlihat pada rujukam gambar 5.4 :



Gambar 5.4 : Topologi Jaringan

Melihat topologi pada perusahaan ini memungkinkan setiap *device* yang terhubung ke jaringan dapat mengakses modem *router* baik dari dalam jaringan seperti LAN maupun luar jaringan menggunakan koneksi *wifi* sehingga sangat mengganggu keamanan apabila dimanfaat pihak yang tidak bertanggung jawab. Berikut percobaan penulis untuk masuk ke modem *router* bisa dilihat pada rujukan gambar



Gambar 5.5 : Modem TP-LINK

Rujukan gambar 5.5 menunjukkan Tampilan modem TP-LINK yang digunakan pada PT.Satria Antaran Prima.



Gambar 5.6 : Tampilan Akses Modem

Rujukan gambar 5.6 menunjukkan Tampilan akses *router* melalui ip 192.168.0.1 yang masih *default* vendor



Gambar 5.7 : tampilan input username dan password

Rujukan gambar 5.7 menunjukkan *Login account* dan *password* yang masih *default* dari vendor.

TP-LIN	K .		300M Wireless N Router Model No. TL-Witeless
Status Quick Setup WPS	Status		Status Help The Status page displays the Router's current status an
Network Wireless Guest Network DHCP	Firmware Version: Hardware Version:	3.16.9 Build 151229 Rel.72828n WR845N v1 00000000	configuration. All information is read-only. LAN - The following parameters apply to the LAN port of the Rous You can configure them in the Network > LAN page. • MAC Address - The physical address of the Router, as see them the LAN.
Forwarding Security Parental Control Access Control Advanced Routing	LAN MAC Address: IP Address: Subnet Mask:	D4-6E-0E-50-FF-E4 192,168.0.1 255.255.255.0	Br Address The LVM Paddress of the Roader South Makes The subset real associated with UVA address. Werkess The subset real associated with UVA address. Werkess These are the current settings or information for Werke You can configure them in the Werkess -> Werkess Settings page. Werkess These in UVA and the Settings of the Roader werkess are the information of ordisated workess are the Roader. Werkess These information of the Roader.
Bandwidth Control IP & MAC Binding Dynamic DNS IPv6 Support System Tools Loncot	Wireless Wreless Radio: Name (SSID): Mode:	Enable PT.Sabia Antara 11bgo mixed	 Mode: The current varies involve which the Roder excito 1 Character. The current varies is character for use. Mack Anderess: The physical address of the Roder, excito Mack Anderess: The physical address of the Roder, excito WOS Status: The status of VOS Convections, hit: Wit convection is down: Scatt. Thy Is find the AFP Autr. The moder Status: The status of VOS Convections, hit: Wit convection is down: Scatt. Thy Is in other AFP Autr. National MACK Anderess: The status and the AFP Autr. The moderest of the Autr. Autr. Autronia moderest of the AFP Autr. The moderest of the AFP Autr. The moderest of the Autr. Autronia moderest of the Autr. Autronia moderest of the Autronia the Autronia the moderest of the Autronia the Autronia the moderest of the Autronia the moderest of the Autronia the Autronia the moderest of the moderest of the mod
	Channel Width: Channel: MAC Address:	Automatic Auto (Current channel 10) DA-6E-0E-50-FF-E4	 WAN - The following parameters apply to the WAN points of the Rout You can configure them in the Newtork -> WAN page. MAC Address - The physical address of the WAN point, as see them the Internet.

Gambar 5.8 : Tampilan Setelah Berhasil Login

Rujukan gambar 5.8 menunjukkan penulis berhasil *login* menggunakan *username* dan *password* vendor. Kesimpulannya *username* dan *password* modem perusahaan ini masih *default* sehingga penulis dengan mudah bisa masuk ke modem dengan menggunakan koneksi *wifi* maupun LAN yang ada pada perusahaan ini .

5.1.2 Action Planning

Pada tahap ini penulis melakukan analisis kebutuhan dan melakukan perencanaan tindakan yang diambil dari pemasalahan yang ada dengan mengimplementasi OSSIM .

5.1.2.1 Analisis Kebutuhan

Permasalahan pada PT. Satria Antaran Prima berdasarkan hasil analisis permasalahan diatas adalah koneksi jaringan pada perusahaan ini sering terputus pada waktu-waktu tertentu serta keamanan modem yang masih *default* sehingga bisa dieksploitasi dengan mudah. Pada penelitian yang penulis lakukan diimplementasi OSSIM, untuk melihat apakah OSSIM bisa dimanfaatkan sebagai sebuah *server* monitoring yang bisa memantau keadaan yang sedang terjadi pada jaringan, OSSIM ini juga digunakan untuk bisa diketahui kenapa jaringan pada perusahaan ini sering terputus dan mengetahui apabila ada yang berusaha mengakses modem, berdasarkan hasil monitoring yang didapat diimplementasikan solusi untuk mengatasi masalah tersebut.

5.1.3 Action taking

Pada tahap ini penulis melakukan tindakan dengan melakukan implementasi OSSIM

5.1.3.1 Implementasi Ossim

OSSIM diimplementasikan pada PT.Satria Antaran Prima, untuk melihat apakah OSSIM ini mampu menemukan permasalahan sering terputusnya jaringan pada perusahaan ini selain itu OSSIM ini juga diharapkan dapat memonitor apa saja yang terjadi pada jaringan termasuk percobaan untuk masuk ke modem karena *security* yang masih *default* sehingga memungkinkan akses ke modem dari dalam maupun luar jaringan. Berikut topologi implementasi OSSIM pada jaringan PT. Satria Antaran Prima.



Gambar 5.9 : Topologi Implementasi OSSIM

Rujukan Gambar 5.9 merupakan topologi jaringan yang penulis terapkan pada jaringan perusahaan, dalam topologi terlihat ada penambahan *server* OSSIM yang terhubung melalaui kabel LAN.

5.1.3.2 Instalasi Alienvault

Penulis melakukan instalasi dengan konfigurasi *ip server* Alienvault yang disesuaikan dengan jaringan perusahaaan tempat penelitian pada penelitian ini penulis menggunakan ip 192.168.0.90/24 seperti terlihat Pada rujukan gambar 5.10



Gambar 5.10 : Konfigurasi Ip Address

Penulis mengkonfigurasi Gateway yang disesuaikan dengan jaringan

PT. Satria Antaran Prima terlihat pada rujukan gambar 5.12

ALIEN VAULT OSSIM		k
Configure the network The gateway is an IP address (four numbers separated by periods) that indicates		
The gateway is an IP address (four numbers separated by periods) that indicates		
also known as the default router. All traffic that goes outside your LAN (for insta sent through this router. In rare circumstances, you may have no router; in that o blank. If you don't know the proper answer to this question, consult your networ <i>Gateway</i> :	s the gateway nce, to the In case, you can rk administra	router, ternet) is I leave this tor.
192.168.0.1		
Screenshot	Go Back	Continue

Gambar 5.11 : Konfigurasi Gateway Alienvault

Konfigurasi server address yang penulis gunakan digunakan disamakan

seperti gateway jaringan terlihat pada rujukan gambar 5.13



Gambar 5.12 : Konfigurasi Server Address

Login pada server Alienvault, setelah penginstalan selesai masuk login

ke Alienvault terlihat pada rujukan gambar



Gambar 5.13 : login console Alienvault

Tampilan menu konfigurasi Alienvault telihat pada rujukan gambar



Gambar 5.14 : Menu Console Alienvault

Pada menu konfigurasi penulis mengaktifkan beberapa *plugin* terlihat pada

rujukan gambar 5.15



Gambar 5.15 : Tampilan Plugin Menu Alienvault

Penulis mengaktifkan beberapa *plugin* diantara Alienvault_*nids*, Alienvault *nids*, *nmap_host*, OSSIM_*agent*, *nessus* dan *nessus detector*. Terlihat pada gambar 5.16



Gambar 5.16 : Tampilan Pengaktifan Plugin Alienvault

Untuk mengakses Alienvault dengan tampilan *Web Interface* penulis mengakses melalui *Web Browser*, terlihat pada rujukan gambar 5.17



Gambar 5.17 : Login Alienvault Melalui Web Browser

Gambar 5.17 menunjukkan tampilan akses *Web Interface* Alienvault yang penulis lakukkan untuk masuk ke menu awal Alienvault,Tampilan awal Alienvault yang belum ada aktifitas seperti terlihat pada gambar 5.18



Gambar 5.18 : Tampilan Dasboard Alienvault

Gambar 5.18 menunjukkan tampilan awal OSSIM Alienvault yang berhasil diimplementasi pada PT.Satria Antaran Prima

5.1.4 Evaluation

Pada tahap ini penulis melakukan evaluasi dari hasil implementassi OSSIM.

5.1.4.1 Hasil implementasi ossim

Hasil implementasi ossim pada PT. Satria Antaran Prima, *assets* yang ada pada jaringan perusahaan ini ditunjukkan pada rujukan gambar

0	* ASSETS										
	HOSTNAME	IP	0	DEVICE TYPE	OPERATING SYSTEM \$	ASSET VALUE	¢	VULN SCAN SCHEDULED	0	HIDS	٥
	Host-192-168-0-125	192.168.0.125			Windows XP/2000	2		No		Not Deploy	ed 🖌
	Host-192-168-0-123	192.168.0.123			Windows 2000	2		No		Not Deploy	ed 🖌
	Host-192-168-0-118	192.168.0.118			Windows XP/2000	2		No		Not Deploy	ed 🔏
	Host-192-168-0-116	192.168.0.116			Windows XP/2000	2		No		Not Deploy	ed 🖌
	Host-192-168-0-114	192.168.0.114			Windows XP/2000	2		No		Not Deploy	ed 🗸
	Host-192-168-0-111	192.168.0.111			Windows 2000 SP4, XP SP1+	2		No		Not Deploy	ed 🗸
	Host-192-168-0-110	192.168.0.110			Windows XP/2000	2		No		Not Deploy	ed 🖌
	Host-192-168-0-109	192.168.0.109			Microsoft Windows 10 64-bit	2		No		Not Deploy	ed 🖌
	Host-192-168-0-106	192.168.0.106			Windows 2000 SP4, XP SP1+	2		No		Not Deploy	ed 🖌
	Host-192-168-0-104	192.168.0.104				2		No		Not Deploy	ed 🖌
	Host-192-168-0-101	192.168.0.101			Microsoft Windows 10 64-bit	2		No		Not Deploy	ed 🖍
	Host-192-168-0-100	192.168.0.100			Canonical Ubuntu Linux 16.04 LTS (Long-Term Support)	2		Yes		Not Deploy	ed 🗸
	Host-192-168-0-1	192.168.0.1		Network Device	Linux 2.6.X	2		Yes		Not Deploy	ed 🖍
	allenvault	192.168.0.90			AllenVault OS	2		Yes		Connected	4

Gambar 5.19 : Assets Alienvault

Gambar 5.19 menunjukkan *assets* yang ada pada perusahan ini, OSSIM yang diimplementasi mampu menangkap semua *host* yang terhubung pada jaringan baik yang terkoneksi melalui LAN maupun *wireless*. OSSIM juga menangkap *log, event* serta aktifitas yang terjadi pada jaringan, berikut rujukan gambar yang menunjukkan hasil yang didapat setelah OSSIM diimplementasi pada jaringan PT. Satria Antaran Prima



5.1.4.2 Hasil Pengujian Dashboard OSSIM

Gambar 5.20 : Log Alienvault Tanggal 22 Januari



Gambar 5.21 : Log Alienvault Pada Tanggal 23 Januari

Dari rujukan gambar diatas terlihat hasil dari aktivitas jaringan, grafik batang vertikal menunjukkan *event security* 5 top *alarm*, pada jaringan ,berikut rujukan gambar detail dari grafik batang

	I DAYS	.10	ol-17 10-01-10	3	0-01-19	0-01-20		10-01-21	10-0	1-22	10-01-23	
6												
R ag	ÖÖ atallatten				•							
Delry	ory G Attack											
-	Contraction of the Providence											
Erro A	0											
seow	20 • ENTRES									_		ac11994.4
	DATE .	status e	INTENT & STRATEGY	0	METHOD	o misk o	OTX	SOURCE	٥	DESTINATION		۰
	2018-01-19 21:38:39	open	🔆 Bruteforce Authentication		Leundonn		NIA	0000				Ø
	2018-01-19 21:37:14	oper	$\dot{igodoldelta }$ Bruteforce Authentication		STH	NOW 212	NA	alienvault.59810		6.0.0.035		Ø
	2018-01-19 21:51:27	-	🔆 Bruteforce Authentication		85H		NA	alienvault:54012				Ø
	2018-01-19 21:49:47	open	🔆 Welderver Attack - 525, injection		Attack Pattern Detection	NOW BE	NA	alienvault		0.0.0		Wi

Gambar 5.22 : Log Grafik Batang Vertikal

Gambar 5.22 menunjukkan adanya deteksi serangan *Bruteforce*, *Web* Server attack dan SQL injection yang terdeteksi oleh ossim pada top 5 alarm dasboard.

Selanjutnya Grafik lingkaran menunjukan 10 top *event* dari berbagai aktifitas seperti *authentifikasi, access, recon*, aplikasi, *suspicious, alarm* dan *alert* secara keseluruhan dalam jaringan yang ditampilkan dalam persentase dan ditunjukkan oleh warna yang berbeda-beda, dari kedua rujukan gambar diatas menunjukkan secara keseluruhan jumlah aktifitas yang dilakukan oleh *host* dalam jaringan yang ditunjukkan dalam persentase yang didominasi oleh nilai tertinggi 95% autentikasi, berikut rujukan gambar yang menunjukkan salah satu contoh autentikasi yang terdapat pada *database* Alienvault

DISPLAY	ING 1 TO 50 OF THOUSANDS OF EVENTS.						3,019 TOTAL EV	ENTS IN DATA	UBASE.
	EVENT NAME	▼ DATE GMT-8:00 ▲	SENSOR	отх	SOURCE	DESTINATION	ASSET S 🌩 D	RISK	
# 🗆	AlienVault HIDS: Login session opened.	2018-01-22 22:34:20	alienvault	N/A	0.0.00	0.0.0.0	2->2	LOW (0)	Ø
# 🗆	AlienVault HIDS: Login session closed.	2018-01-22 22:34:20	alienvault	N/A	0.0.0	0.0.0.0	2->2	LOW (0)	Ø
# 🗆	sudo: Session closed	2018-01-22 22:34:19	alienvault	N/A	0.0.0	0.0.0.0	2+>2	LOW (0)	Ø
# 🗆	sudo: Session closed	2018-01-22 22:34:19	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)	Ø
# 🗆	sudo: Session opened	2018-01-22 22:34:19	alienvault	N/A	0.0.0	0.0.0.0	2->2	LOW (0)	Ø
# 🗆	AlienVault HIDS: Login session opened.	2018-01-22 22:34:16	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)	Ø
# 🗆	AlienVault HIDS: Login session opened.	2018-01-22 22:34:16	alienvault	N/A	0.0.0	0.0.0.0	2->2	LOW (0)	Ø
# 🗆	AlienVault HIDS: Login session closed.	2018-01-22 22:34:16	alienvault	N/A	0.0.00	0.0.0.0	2->2	LOW (0)	Ø
# 🗆	AlienVault HIDS: Login session closed.	2018-01-22 22:34:16	alienvault	N/A	0.0.0	0.0.0.0	2->2	LOW (0)	Ø
# 🗆	sudo: Session closed	2018-01-22 22:34:16	alienvault	N/A	0.0.0.0	0.0.0.0	2+>2	LOW (0)	Ø
# 🗆	sudo: Session opened	2018-01-22 22:34:16	alienvault	N/A	0.0.0	0.0.0.0	2->2	LOW (0)	Ø
# 🗆	sudo: Session closed	2018-01-22 22:34:15	alienvault	N/A	0.0.0	0.0.0.0	2->2	LOW (0)	Ø

Gambar 5.23 : Log Grafik Lingkaran

Gambar 5.23 menunjukkan salah satu *log event autentikasi* yang terjadi pada jaringan, dengan tingkat resiko *low*. Grafik garis menunjukkan banyaknya *event* dalam jaringan, berikut salah satu isi dari *event* pada jaringan

DISPLA	YING 1 TO 50 OF THOUSANDS OF EVENTS.						2,038 TOTAL EV	ENTS IN DATA	ABASE
	EVENT NAME	▼ DATE GMT-8:00 ▲	SENSOR	отх	SOURCE	DESTINATION	ASSET S - D	RISK	
4	AlienVault NIDS: "ET POLICY Dropbox Client Broadcasting"	2018-01-22 21:53:44	alienvault	N/A	192.168.0.106:17500	255.255.255.255:17500	2->2	LOW (0)	ø
40	USer-Agent Outbound likely related to package management"	2018-01-22 21:49:26	alienvault	N/A	alienvault:45580	52.28.229.156:80	2->2	LOW (0)	Ø
4	User-Agent Outbound likely related to package management	2018-01-22 21:49:26	alienvault	N/A	alienvault:45580	52.28.229.156:80	2+>2	LOW (0)	Ø
40	User-Agent Outbound likely related to package management	2018-01-22 21:49:25	alienvault	N/A	alienvault:45580	52.28.229.156:80	2->2	LOW (0)	ø
4	User-Agent Outbound likely related to package management	2018-01-22 21:49:25	alienvault	N/A	alienvault:45580	52.28.229.156:80	2+>2	LOW (0)	Ø
40	User-Agent Outbound likely related to package management"	2018-01-22 21:49:25	alienvault	N/A	alienvault:45580	52.28.229.156:80	2->2	LOW (0)	Ø
4	User-Agent Outbound likely related to package management	2018-01-22 21:49:25	alienvault	N/A	alienvault:45580	52.28.229.156:80	2+>2	LOW (0)	Ø
4	User-Agent Outbound likely related to package management"	2018-01-22 21:49:25	alienvault	N/A	alienvault:45580	52.28.229.156:80	2->2	LOW (0)	ø
40	User-Agent Outbound likely related to package management"	2018-01-22 21:49:24	alienvault	N/A	alienvault:45580	52.28.229.156:80	2->2	LOW (0)	Ø
40	User-Agent Outbound likely related to package management	2018-01-22 21:49:24	alienvault	N/A	alienvault:45580	52.28.229.156:80	2->2	LOW (0)	Ø
4	User-Agent Outbound likely related to package management?	2018-01-22 21:49:24	alienvault	N/A	alienvault:45580	52.28.229.156:80	2+>2	LOW (0)	Ø
40	User-Agent Outbound likely related to package management	2018-01-22 21:49:24	alienvault	N/A	alienvault:45580	52.28.229.156:80	2->2	LOW (0)	ø

Gambar 5.24 : log event grafik garis

Gambar 5.24 menunjukan *log event* dari *server* Alienvault kejaringan luar terlihat pada *source* tujuan dengan alamat *IP public*. Grafik batang horizontal menunjukkan *event* setiap host dalam jaringan , setiap *host* dibedakan dalam warna yang berbeda berikut rujukan gambar yang menunjukkan asset yang ada pada jaringan serta *event* dan *vulnerability* pada host dalam jaringan yang terhubung pada OSSIM.



Gambar 5.25 : Log Grafik Batang Vertikal

Gambar 5.25 menunjukkan hasil log dari setiap host yang terhubung yang menunjukkan *event, vulnerability*.

Berikut rujukan gambar *scanning vulnerability* OSSIM pada beberapa *host* yang menunjukkan *detail vulnerability* yang ada pada *host* pada PT. Satria Antaran Prima

VULNERABILITIES	ALARMS EVENTS	SOFTWARE SERVICES PLU	IGINS PROPE	RTIES	NETFLOW	GROUPS	
10 VULNERABIL	ITIES						
SCAN TIME	ASSET	VULNERABILITIES	VULN ID	٥	SERVICE	SEVERITY	\$
2018-01-23 02:50:12	Host-192-168-0-109 (192.168.0.109)	Ping Host	100315		general (0/tcp)	Info	
2018-01-23 02:50:12	Host-192-168-0-109 (192.168.0.109)	ICMP Timestamp Detection	103190		general (0/icmp)	Info	
2018-01-23 02:50:12	Host-192-168-0-109 (192.168.0.109)	OS Detection Consolidation and Reporting	105937		general (0/tcp)	Info	
2018-01-23 02:50:12	Host-192-168-0-109 (192.168.0.109)	CPE Inventory	810002		general (0/CPE-T)	Info	
HOWING 1 TO 4 OF	4 VULNERABILITIES				<	PREVIOUS 1 N	EXT >

Gambar 5.26 : vulnerability host 192.168.0.100

Gambar 5.26 menunjukkan hasil *vulnerability scanning* OSSIM yang ada pada host 192.168.0.100

SCAN TIME	ASSET	VULNERABILITIES \$	VULN ID	٥	SERVICE	\$ SEVERITY	٥
2018-01-23 02:50:12	Host-192-168-0-100 (192.168.0.100)	phpinfo() output accessible	11229		http (80/tcp)	High	
2018-01-23 02:50:12	Host-192-168-0-100 (192.168.0.100)	TCP timestamps	80091		general (0/tcp)	Medium	
2018-01-23 02:50:12	Host-192-168-0-100 (192.168.0.100)	Ping Host	100315		general (0/tcp)	Info	
2018-01-23 02:50:12	Host-192-168-0-100 (192.168.0.100)	ICMP Timestamp Detection	103190		general (0/icmp)	Info	
2018-01-23 02:50:12	Host-192-168-0-100 (192.168.0.100)	OS Detection Consolidation and Reporting	105937		general (0/tcp)	Info	
2018-01-23 02:50:12	Host-192-168-0-100 (192.168.0.100)	Traceroute	51662		general (0/tcp)	Info	
2018-01- <mark>23</mark> 02:50:12	Host-192-168-0-100 (192.168.0.100)	CPE Inventory	810002		general (0/CPE-T)	Info	
2018-01-23 02:50:12	Host-192-168-0-100 (192.168.0.100)	HTTP Server type and version	10107		http (80/tcp)	Info	
2018-01-23 02:50:12	Host-192-168-0-100 (192.168.0.100)	Services	10330		http (80/tcp)	Info	
2018-01-23 02:50:12	Host-192-168-0-100 (192.168.0.100)	CGI Scanning Consolidation	111038		http (80/tcp)	Info	

Gambar 5.27 : vulnerability host 192.168.0.109

Gambar 5.27 menunjukkan hasil vulnerability scanning OSSIM yang ada pada host 192.168.0.100

4 Vulnerabilities	0 Alarms	135 Events Availabilit	ty Services	0 Groups)(0 Notes)
Description Unknown VULNERABILITIES	ALARMS EVENTS	SOFTWARE SERVICES	PLUGINS PROPERT	TES NETFLOW	GROUPS	5	
10 • EVENTS	SIGNATURE		SOURCE	DESTINATION	SENSOR	RISK \$	
2018-01-22 21:47:59	AlienVault NIDS: "ET SCAN Po	ssible Nmap User-Agent Observed"	Host-192-168-0-109	Host-192-168-0-100	alienvault	0	Ø
2018-01-22 21:47:59	AlienVault NIDS: "ET SCAN Po	ssible Nmap User-Agent Observed"	Host-192-168-0-109	Host-192-168-0-100	alienvault	0	Q I
2018-01-22 21:47:59	AlienVault NIDS: "ET SCAN Po	ssible Nmap User-Agent Observed"	Host-192-168-0-109	Host-192-168-0-100	alienvault	0	Q!
2018-01-22 21:47:59	AlienVault NIDS: "ET SCAN Po	ssible Nmap User-Agent Observed"	Host-192-168-0-109	Host-192-168-0-100	alienvault	0	Ø.
2018-01-22 21:47:59	AlienVault NIDS: "ET SCAN Po	ssible Nmap User-Agent Observed"	Host-192-168-0-109	Host-192-168-0-100	alienvault	0	Ø1
2018-01-22 21:47:59	AlienVault NIDS: "ET SCAN Po	ssible Nmap User-Agent Observed"	Host-192-168-0-109	Host-192-168-0-100	alienvault	0	Ø

Gambar 5.28 : detail event host 192.168.0.109

Gambar 5.28 menunjukkan *event* yang berhasil ditangkap oleh OSSIM adanya *event nmap* yang berasal dari *host* 192.168.0.100 menuju *host* 192.168.0.109.

5.1.5 Learning

Pada tahap ini penulis melakukan penerapan IDS Snort .

5.1.5.1 Penerapan IDS Snort



Gambar 5.29 : Snort Pada Console Alienvault

Gambar 5.29 Menunjukkan Snort Yang Aktif Pada Konsole Alienvault

[**] [1:10000001:1] PING ICMP [**]
[Priority: 0]
01/25-03:12:20.093109 192.168.0.100 -> 192.168.0.109
ICMP TTL: 64 TO3:0x0 ID:20865 IpLen: 20 DqmLen: 84 DF
Type:8 Code:0 ID:18650 Seg:5 ECH0
[44] [1-10000001-1] PING TOMP [44]
(Priority, 0)
01/25-01-12-20 002422 102 160 0 100 -> 102 160 0 100
TCMP TTL 128 TOB.040 TD146512 TPLAN 20 DPLAN 84
Turner of Cadeta Thileseo Parte Provensa
Type:0 Code:0 ID:18650 Seq:5 ECHO REPLY
[a] [1:10000001:1] PING ICMP [a]
[Priority: 0]
01/25-03:12:21.117013 192.168.0.100 -> 192.168.0.109
ICMP TTL:64 T03:0x0 ID:20941 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:18650 Seq:6 ECHO
[**] [1:10000001:1] PING ICMP [**]
[Priority: 0]
01/25-03:12:21.117408 192.168.0.109 -> 192.168.0.100
ICMP TTL:128 TOS:0x0 ID:16514 IpLen:20 DgmLen:84
Type:0 Code:0 ID:18650 Seq:6 ECHO REPLY
[**] [1:10000001:1] PING ICMP [**]
[Priority: 0]
01/25-03:12:22.141118 192.168.0.100 -> 192.168.0.109
ICMP TTL:64 TOS:0x0 ID:21062 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:18650 Seq:7 ECH0
[**] [1:10000001:1] FING ICMP [**]
[Priority: 0]
01/25-03:12:22.141552 192.168.0.109 -> 192.168.0.100
ICMP TTL:128 T05:0x0 ID:16515 IpLen:20 DgmLen:84
Type:0 Code:0 ID:18650 Seq:7 ECHO REPLY
[**] [1:10000001:1] PING ICMP [**]
[Priority: 0]
01/25-03:12:23.165034 192.168.0.100 -> 192.168.0.109
ICMP TTL:64 T03:0x0 ID:21304 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:18650 Seq:8 ECHO
[**] [1:10000001:1] PING ICMP [**]
The family of the second sec

Gambar 5.30 : Hasil Capture Snort



Gambar 5.31 : Hasil Capture Snort

Gambar 5.30 dan 5.31 menunjukkan hasil *capture snort* yang berhasil menangkap *ping flood* dari host 192.168.0.100 menuju *host* 192.168.0.109 yang menggunakan *protocol icmp*.

Pada jaringan perusahaan ini, OSSIM juga mendeteksi adanya akses terhadap *router* dengan *ip address* 192.168.0.1 dari *host* 192.168.0.100

	Tane	Source	Destination	Protocol	Length	Info.
	8.99999999	192.168.0.100	192.168.0.1	TCP	74	42544\xe2\x86\x9280 [5WN] Seq=0 Win=29280 Len=0 MSS=1460 SACK_PERM=1 TSVal=50593987 TSecr=0 WS=128
	0.000315000	192.168.0.100	192.168.0.1	TCP	66	42544\xe2\x86\x9280 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=50593987 TSecr=4472399
	0.000498000	192.168.0.100	192.168.0.1	HTTP	469	GET /WMWZVNCAZMXFJSJB/dynaform/custom.js HTTP/1.1
	0.012237000	192.168.0.100	192.168.0.1	TCP	66	42544\xe2\x86\x9288 [ACK] Seq=404 Ack=10 Win=29312 Len=0 TSval=50593990 TSecr=4472402
	0.012556000	192.168.0.100	192.168.0.1	TCP	66	42544\xe2\x86\x9280 [ACK] Seq=404 Ack=861 Win=32128 Len=0 TSvml=50593990 TSecr=4472402
	0.013173000	192.168.0.100	192.168.0.1	TCP	66	42544\xe2\x86\x9280 [FIN, ACK] Seq=404 Ack=862 Win=32128 Len=0 TSvml=50593990 TSecr=4472402
	0.013474000	192.168.0.100	192.168.0.1	TCP	74	42546\xe2\x86\x9280 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=50593990 TSecr=0 WS=128
	0.013730000	192.168.0.100	192.168.0.1	TCP	66	42546\xe2\x86\x9280 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=50593990 TSecr=4472403
	0.013916000	192.168.0.100	192.168.0.1	HTTP	468	GET /WMWZVNCAZMXFJSJB/images/top1_1.jpg HTTP/1.1
	0.022200000	192.168.0.100	192.168.0.1	TCP	74	42548\xe2\x86\x9280 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=50593992 TSecr=0 WS=128
	0.022519000	192.168.0.100	192.168.0.1	TCP	66	42548\xe2\x86\x9280 [ACK] Seg=1 Ack=1 Win=29312 Len=0 TSval=50593992 TSecr=4472405
ETH		atorisation fraterist	(100 100 0 100) BOT. 100 100 0	1 (102 168 0 1)		
ETH INT TRA	INET PROTOCOL V ISMISSION CONTRO	ERSION 4, SRC: 192.108.0.100	(102-100-0-100), UDI: 102-100-0- 42544), DST PORT: 80 (80), SEQ: /	(,LEN: 0		

Gambar 5.32 : Traffic Capture

Gambar 5.32 menunjukkan adanya akses ke *router* oleh *host* pada jaringan PT.Satria Antaran Prima.

Kesimpulan yang didapat dari implementasi OSSIM pada PT. Satria Antaran Prima

- OSSIM mampu mendeteksi serta menangkap *event* serta serangan yang terjadi pada setiap *host* dalam jaringan PT.Satria Antaran Prima dan disajikan dalam bentuk grafik
- OSSIM juga mendeteksi vulnerability dari masing-masing host yang terhubung
- 3. Adanya akses *router* yang dilakukan suatu *host* dalam jaringan seperti terlihat pada rujukan gambar 5.32
- 4. *Snort* yang diimplementasi menangkap adanya *ping flood* yang dilakukan oleh suatu *host* terhadap *host* yang lain dalam jaringan perusahaan ini seperti terlihat pada rujukan gambar 5.30 dan 5.31

5.2 Pembahasan

Kesimpulan yang didapat dari implementsi OSSIM PT. Satria Antaran Prima ini menunjukkan adanya aktifitas *ping flood* antar *host* pada jaringan, hal ini bisa menyebabkan terganggunya koneksi pada *host* sehingga fungsi dari komputer tersebut tidak bisa dimaksimalkan untuk urusan pekerjaan sehingga dapat merugikan perusahaan untuk masalah ini penulis menyarankan untuk pemasangan IPS pada *host* sebagai solusi untuk mencegah masalah tersebut. OSSIM juga mendeteksi adanya akses *router* dari *host* yang memungkin kan *host* tersebut merubah konfigurasi *router* karena keamanan dari *router* yang masih *default* sehingga sangat merugikan apabila dieksploitasi oleh orang atau karyawan yang tidak bertanggung jawab untuk hal ini penulis menyarankan untuk merubah *password* modem sebagai solusi.

5.2.1 Implementasi IPS

Pada penelitian ini penulis melakukan implementasi IPS menggunakan Snort dengan Mode Prevention.

alienvault@alienvault-W240HU-W250HUQ:-\$ sudo snort -A full -u snort -g snort -q -c /etc/snort/snort.conf -l /var/log/snort/ alienvault@alienvault-W240HU-W250HUQ:~\$ sudo snort -A full -q -u snort -g snort -c /etc/snort/snort.conf -l /var/log/snort/ -Q

Gambar 5.33: Rules Snort Mode Prevention

Rujukan gambar 5.33 menunjukkan konfigurasi rules snort sebagai

IPS yang penulis gunakan.

02/09-13:11:51.353860 [Drop] [**] [1:10000001:1] ICMP test detected [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP}
74.125.68.100 -> 192.168.20.4
02/09-13:11:52.358572 [Drop] [**] [1:10000001:1] ICMP test detected [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP}
74.125.68.100 -> 192.168.20.4
02/09-13:11:53.382543 [Drop] [**] [1:10000001:1] ICMP test detected [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP}
74.125.68.100 -> 192.168.20.4
02/09-13:11:54.406157 [Drop] [**] [1:10000001:1] ICMP test detected [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP}
74.125.68.100 -> 192.168.20.4
02/09-13:11:55.430217 [Drop] [**] [1:10000001:1] ICMP test detected [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP}
74.125.68.100 -> 192.168.20.4
02/09-13:11:56.453866 [Drop] [**] [1:10000001:1] ICMP test detected [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP}
74.125.68.100 -> 192.168.20.4
02/09-13:11:57.478220 [Drop] [**] [1:10000001:1] ICMP test detected [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP}
74.125.68.100 -> 192.168.20.4
02/09-13:11:58.502298 [Drop] [**] [1:10000001:1] ICMP test detected [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP}
74.125.68.100 -> 192.168.20.4
02/09-13:11:59.525591 [Drop] [**] [1:10000001:1] ICMP test detected [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP}
74.125.68.100 -> 192.168.20.4
02/09-13:12:00.550472 [Drop] [**] [1:10000001:1] ICMP test detected [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP}
74.125.68.100 -> 192.168.20.4

Gambar 5.34: Hasil Snort IPS

Rujukan gambar 5.34 menunjukkan hasil drop paket dari host

yang melakukan dos attack dengan protocol ICMP pada jaringan.