

## **BAB V**

### **Hasil Dan Pembahasan**

#### **5.1. Hasil**

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

##### **5.1.1 Diagnosis**

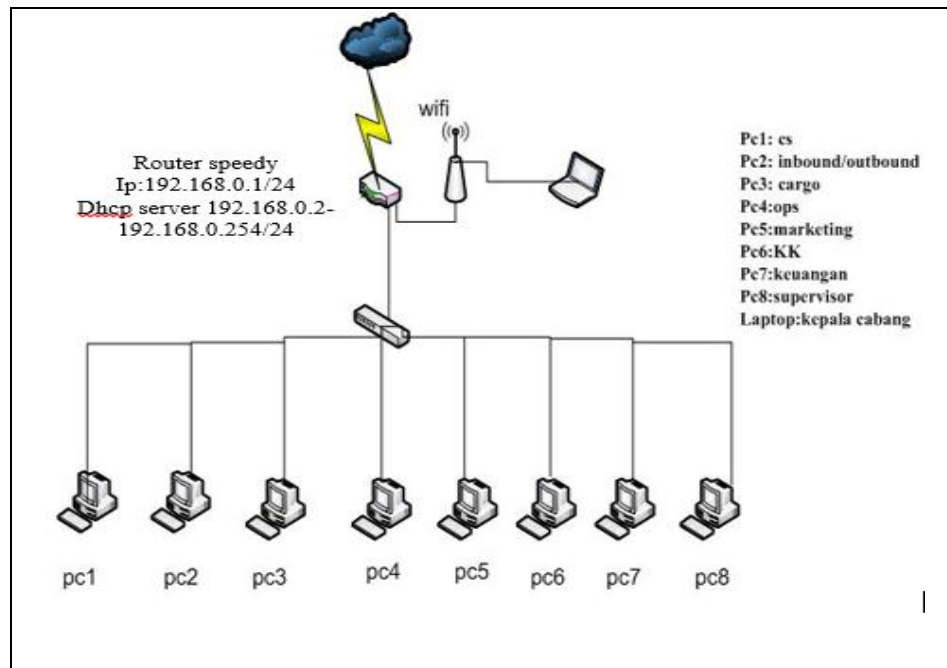
Pada tahap ini penulis melakukan diagnosis dengan cara menganalisis permasalahan yang ada pada perusahaan ini,

##### **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 kemandirian 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.







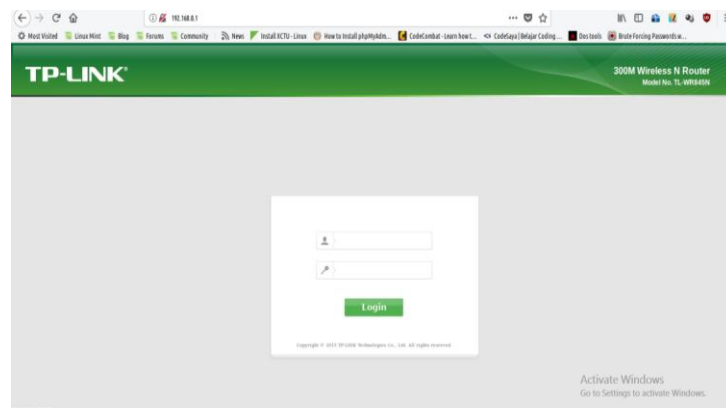
Gambar 5.4 : Topologi Jaringan

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 dimanfaatkan pihak yang tidak bertanggung jawab. Berikut percobaan penulis untuk masuk ke modem *router* bisa dilihat pada rujukan gambar



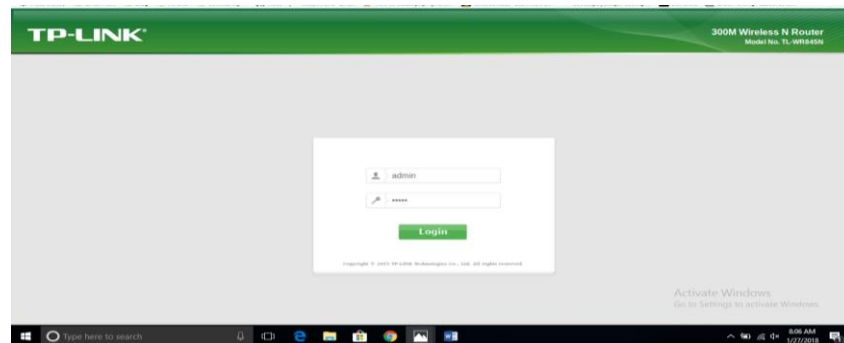
Gambar 5.5 : Modem TP-LINK

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



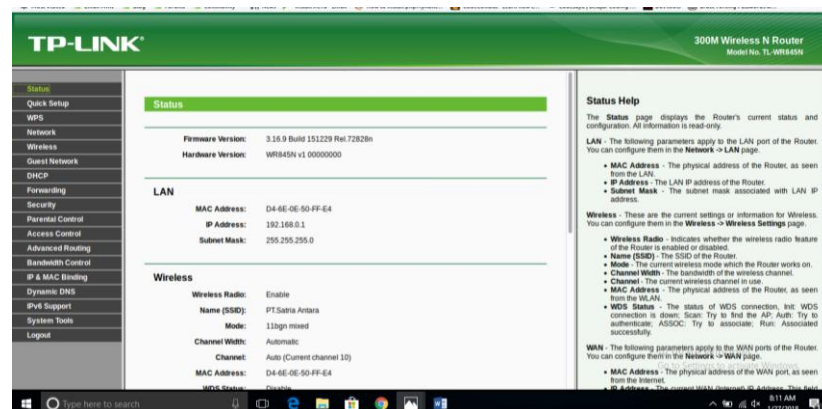
Gambar 5.6 : Tampilan Akses Modem

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.



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 permasalahan 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.

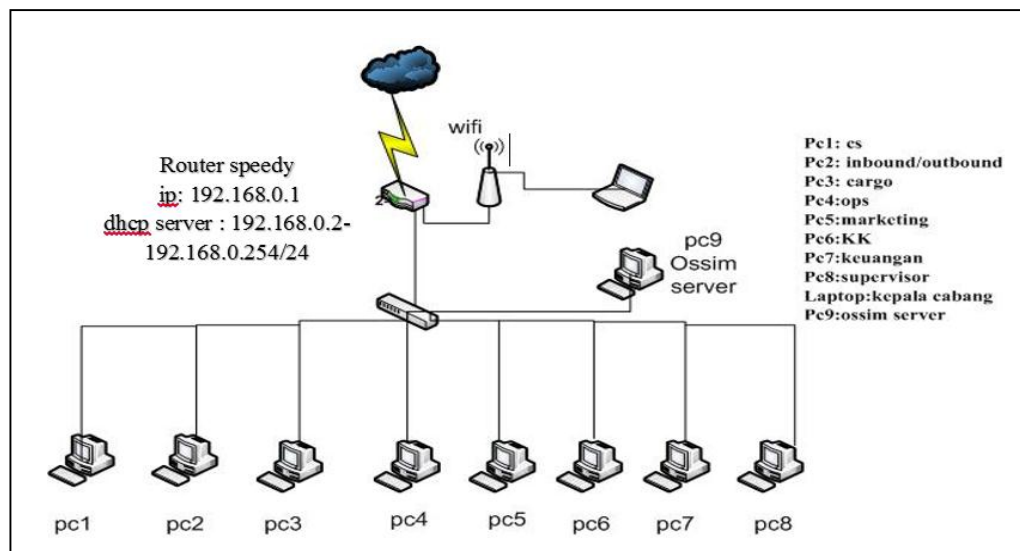
## **5.1.3 Action taking**

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 melalui kabel LAN.

### 5.1.3.2 Instalasi Alienvault

Penulis melakukan instalasi dengan konfigurasi *ip server* Alienvault yang disesuaikan dengan jaringan perusahaan 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



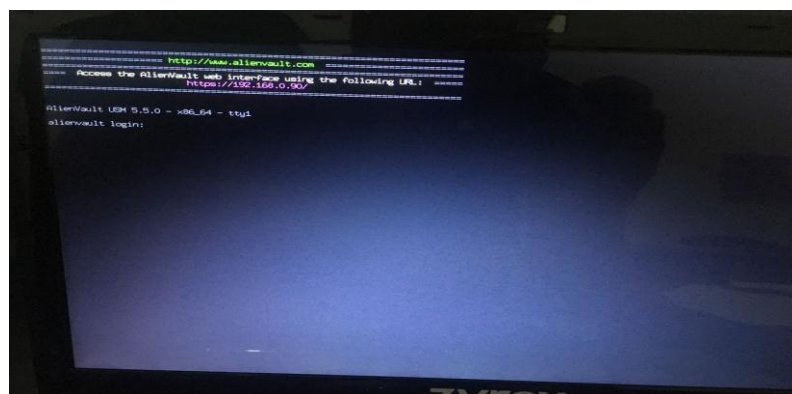
Gambar 5.11 : Konfigurasi *Gateway* Alienvault

Konfigurasi *server address* yang penulis gunakan digunakan disamakan seperti *gateway* jaringan terlihat pada rujukan gambar 5.13



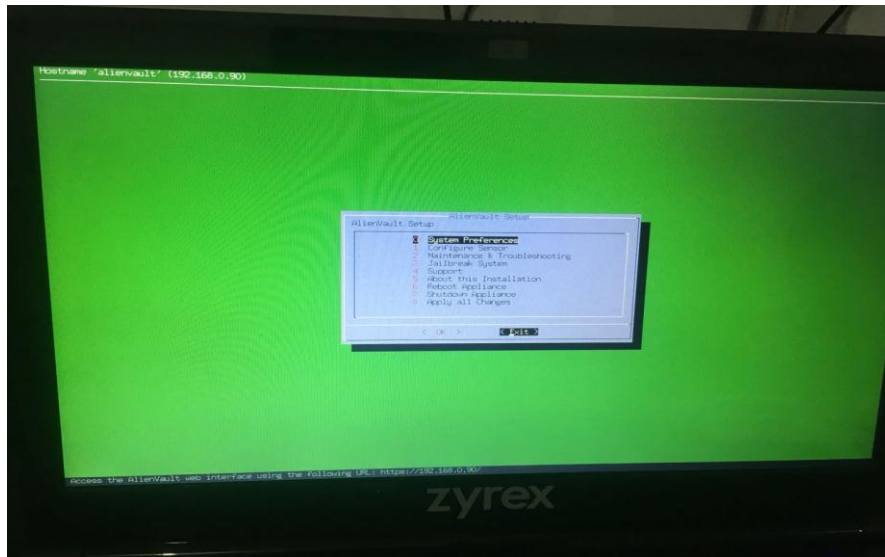
Gambar 5.12 : Konfigurasi *Server Address*

Login pada *server* Alienvault, setelah penginstalan selesai masuk login ke Alienvault terlihat pada rujukan gambar



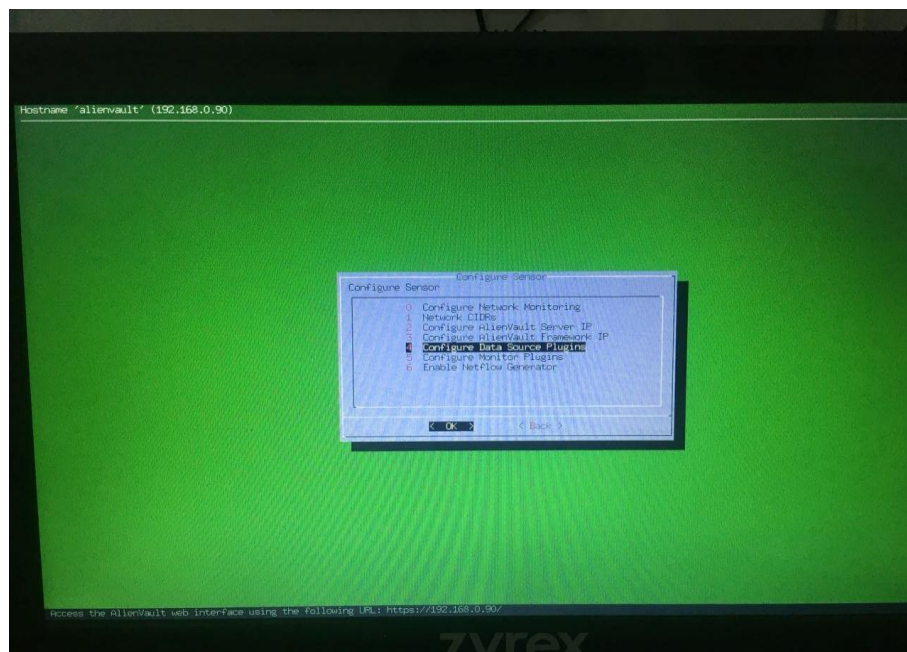
Gambar 5.13 : *login console* Alienvault

Tampilan menu konfigurasi Alienvault terlihat pada rujukan gambar



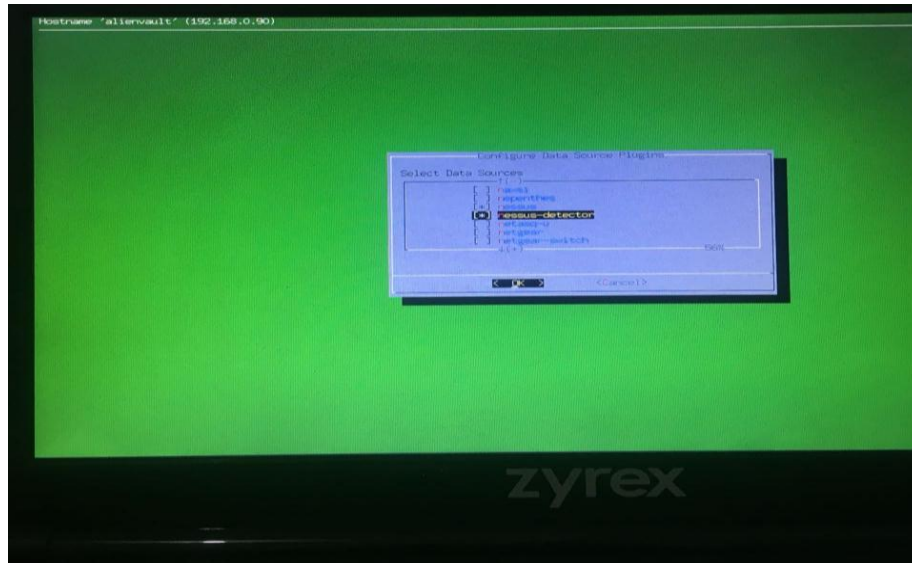
Gambar 5.14 : Menu *Console* Alienvault

Pada menu konfigurasi penulis mengaktifkan beberapa *plugin* terlihat pada rujukan gambar 5.15



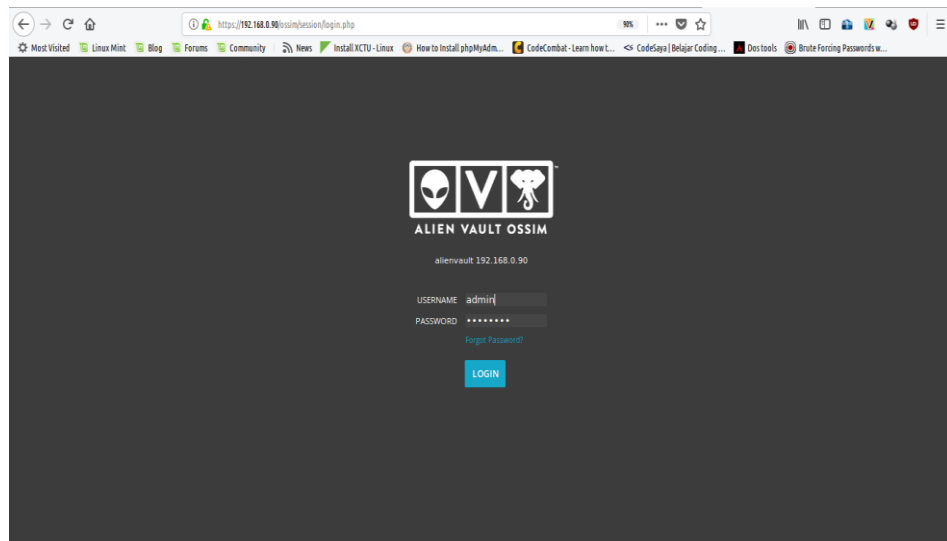
Gambar 5.15 : Tampilan *Plugin* Menu Alienvault

Penulis mengaktifkan beberapa *plugin* diantara *Alienvault\_nids*, *Alienvault nids*, *nmap\_host*, *OSSIM\_agent*, *nessus* dan *nessus detector*. Terlihat pada gambar 5.16



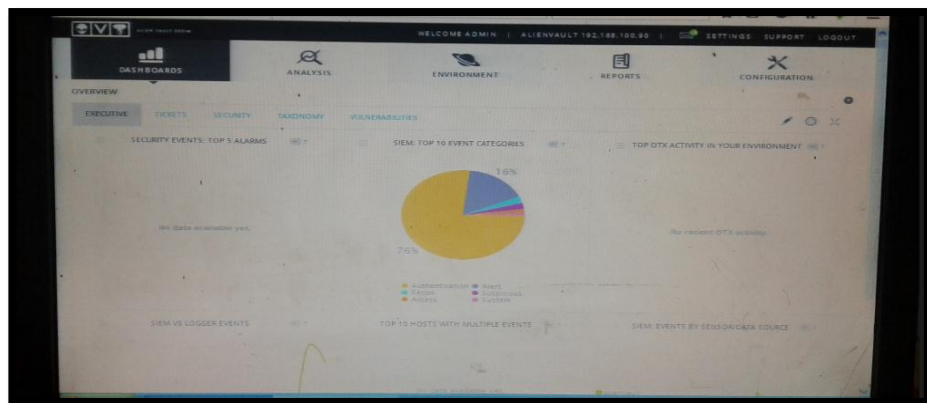
Gambar 5.16 : Tampilan Pengaktifan *Plugin* Alienvault

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 lakukan untuk masuk ke menu awal Alienvault, Tampilan awal Alienvault yang belum ada aktifitas seperti terlihat pada gambar 5.18



Gambar 5.18 : Tampilan *Dashboard* Alienvault

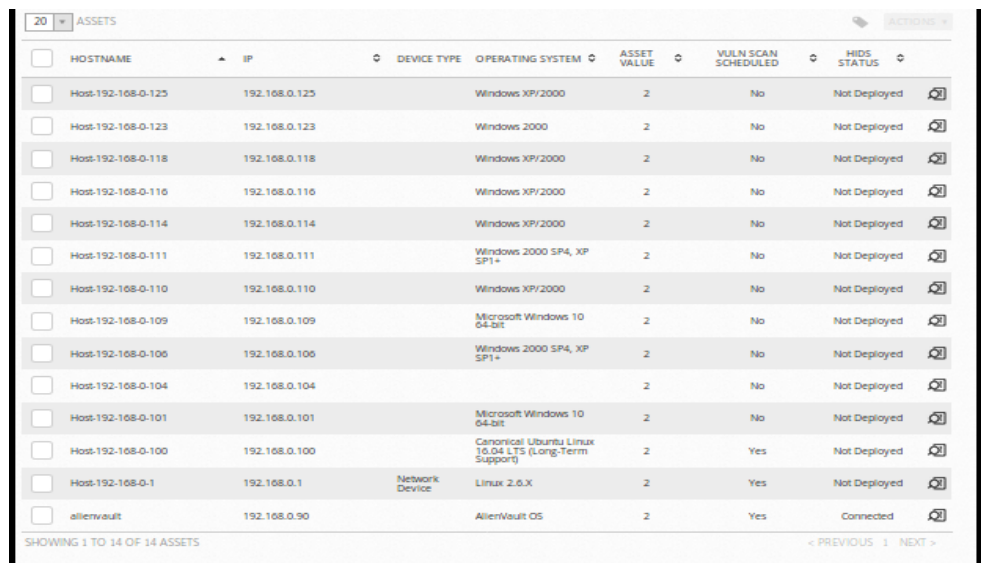
Gambar 5.18 menunjukkan tampilan awal OSSIM Alienvault yang berhasil diimplementasi pada PT.Satria Antaran Prima

## 5.1.4 Evaluation

Pada tahap ini penulis melakukan evaluasi dari hasil implementasi 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



HOSTNAME	IP	DEVICE TYPE	OPERATING SYSTEM	ASSET VALUE	VULN SCAN SCHEDULED	HIDS STATUS
Host-192-168-0-125	192.168.0.125		Windows XP/2000	2	No	Not Deployed
Host-192-168-0-123	192.168.0.123		Windows 2000	2	No	Not Deployed
Host-192-168-0-118	192.168.0.118		Windows XP/2000	2	No	Not Deployed
Host-192-168-0-116	192.168.0.116		Windows XP/2000	2	No	Not Deployed
Host-192-168-0-114	192.168.0.114		Windows XP/2000	2	No	Not Deployed
Host-192-168-0-111	192.168.0.111		Windows 2000 SP4, XP SP1+	2	No	Not Deployed
Host-192-168-0-110	192.168.0.110		Windows XP/2000	2	No	Not Deployed
Host-192-168-0-109	192.168.0.109		Microsoft Windows 10 64-bit	2	No	Not Deployed
Host-192-168-0-106	192.168.0.106		Windows 2000 SP4, XP SP1+	2	No	Not Deployed
Host-192-168-0-104	192.168.0.104			2	No	Not Deployed
Host-192-168-0-101	192.168.0.101		Microsoft Windows 10 64-bit	2	No	Not Deployed
Host-192-168-0-100	192.168.0.100		Canonical Ubuntu Linux 10.04 LTS (Long-Term Support)	2	Yes	Not Deployed
Host-192-168-0-1	192.168.0.1	Network Device	Linux 2.6.X	2	Yes	Not Deployed
allenvault	192.168.0.90		AlienVault OS	2	Yes	Connected

Gambar 5.19 : *Assets* AlienVault

Gambar 5.19 menunjukkan *assets* yang ada pada perusahaan 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

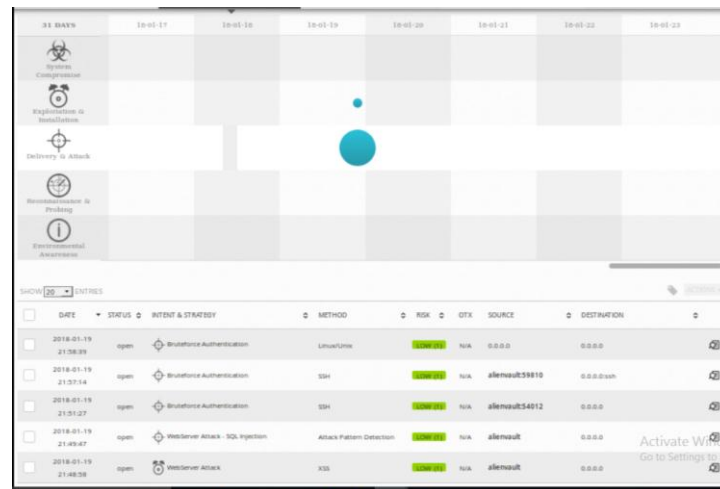


Gambar 5.20 : Log Alienvault Tanggal 22 Januari



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



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 dashboard.

Selanjutnya Grafik lingkaran menunjukkan 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



DISPLAYING 1 TO 50 OF THOUSANDS OF EVENTS. 3,019 TOTAL EVENTS IN DATABASE.

<input type="checkbox"/>	EVENT NAME	DATE GMT+8:00	SENSOR	OTX	SOURCE	DESTINATION	ASSET S=D	RISK
<input type="checkbox"/>	AlienVault:HIDS: Login session opened.	2018-01-22 22:34:20	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
<input type="checkbox"/>	AlienVault:HIDS: Login session closed.	2018-01-22 22:34:20	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
<input type="checkbox"/>	sudo: Session closed	2018-01-22 22:34:19	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
<input type="checkbox"/>	sudo: Session closed	2018-01-22 22:34:19	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
<input type="checkbox"/>	sudo: Session opened	2018-01-22 22:34:19	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
<input type="checkbox"/>	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)
<input type="checkbox"/>	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)
<input type="checkbox"/>	AlienVault:HIDS: Login session closed.	2018-01-22 22:34:16	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
<input type="checkbox"/>	AlienVault:HIDS: Login session closed.	2018-01-22 22:34:16	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
<input type="checkbox"/>	sudo: Session closed	2018-01-22 22:34:16	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
<input type="checkbox"/>	sudo: Session opened	2018-01-22 22:34:16	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)
<input type="checkbox"/>	sudo: Session closed	2018-01-22 22:34:15	alienvault	N/A	0.0.0.0	0.0.0.0	2->2	LOW (0)

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

DISPLAYING 1 TO 50 OF THOUSANDS OF EVENTS. 2,038 TOTAL EVENTS IN DATABASE.

<input type="checkbox"/>	EVENT NAME	DATE GMT+8:00	SENSOR	OTX	SOURCE	DESTINATION	ASSET S=D	RISK
<input type="checkbox"/>	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)
<input type="checkbox"/>	AlienVault NIDS: "ET POLICY GNU/Linux APT 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)
<input type="checkbox"/>	AlienVault NIDS: "ET POLICY GNU/Linux APT 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)
<input type="checkbox"/>	AlienVault NIDS: "ET POLICY GNU/Linux APT 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)
<input type="checkbox"/>	AlienVault NIDS: "ET POLICY GNU/Linux APT 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)
<input type="checkbox"/>	AlienVault NIDS: "ET POLICY GNU/Linux APT 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)
<input type="checkbox"/>	AlienVault NIDS: "ET POLICY GNU/Linux APT 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)
<input type="checkbox"/>	AlienVault NIDS: "ET POLICY GNU/Linux APT 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)
<input type="checkbox"/>	AlienVault NIDS: "ET POLICY GNU/Linux APT 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)
<input type="checkbox"/>	AlienVault NIDS: "ET POLICY GNU/Linux APT 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)
<input type="checkbox"/>	AlienVault NIDS: "ET POLICY GNU/Linux APT 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)

Gambar 5.24 : log event grafik garis

Gambar 5.24 menunjukkan *log event* dari *server* AlienVault ke jaringan 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	PLUGINS	PROPERTIES	NETFLOW	GROUPS
10 VULNERABILITIES							
SCAN TIME	ASSET	VULNERABILITIES	VULN ID	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		
SHOWING 1 TO 4 OF 4 VULNERABILITIES							
< PREVIOUS 1 NEXT >							

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	SERVICE	SEVERITY
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
2018-01-23 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

SHOWING 1 TO 10 OF 24 VULNERABILITIES < PREVIOUS 1 2 3 NEXT >

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	0	135	N/A	4	0	0
Vulnerabilities	Alarms	Events	Availability	Services	Groups	Notes
<b>Description</b> Unknown						
VULNERABILITIES	ALARMS	EVENTS	SOFTWARE	SERVICES	PLUGINS	PROPERTIES
10 EVENTS						
DATE	SIGNATURE	SOURCE	DESTINATION	SENSOR	RISK	
2018-01-22 21:47:59	AlienVault NIDS: "ET SCAN Possible Nmap User-Agent Observed"	Host-192-168-0-109	Host-192-168-0-100	alienvault	0	
2018-01-22 21:47:59	AlienVault NIDS: "ET SCAN Possible Nmap User-Agent Observed"	Host-192-168-0-109	Host-192-168-0-100	alienvault	0	
2018-01-22 21:47:59	AlienVault NIDS: "ET SCAN Possible Nmap User-Agent Observed"	Host-192-168-0-109	Host-192-168-0-100	alienvault	0	
2018-01-22 21:47:59	AlienVault NIDS: "ET SCAN Possible Nmap User-Agent Observed"	Host-192-168-0-109	Host-192-168-0-100	alienvault	0	
2018-01-22 21:47:59	AlienVault NIDS: "ET SCAN Possible Nmap User-Agent Observed"	Host-192-168-0-109	Host-192-168-0-100	alienvault	0	
2018-01-22 21:47:59	AlienVault NIDS: "ET SCAN Possible Nmap User-Agent Observed"	Host-192-168-0-109	Host-192-168-0-100	alienvault	0	

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

```

  2 byte states : 1.00
  3 byte states : 1.00
  4 byte states : 1.00
  [ Number of patterns truncated to 20 bytes: 608 ]
  Rule DB configured to passive "snort"
  Reloading rule sets from "snort"
  Reloading thread started, thread 0x7f497fa0c700 (10792)
  Decoding Ethernet
  --- Initialization Complete ---
  --> Snort! <--
  o'')'
  o'')'
  Version 2.9.11.1 GPL (Build 268)
  By Martin Roesch & the Snort Team: http://www.snort.org/contactteam
  Copyright (C) 2004-2012 Cisco and/or its affiliates. All rights reserved.
  Copyright (C) 2006-2013 Sourcefire, Inc., et al
  Using libpcap version 1.0.2
  Using PcapB version: 0.36 2014-04-04
  Using zlib version: 1.2.3
  Rules Engine: SF_SHORT_DETECTIONENGINE Version 3.0 (Build 1)
  Preprocessor Object: SF_DNS Version 1.1 (Build 1)
  Preprocessor Object: SF_IDPS2 Version 1.0 (Build 3)
  Preprocessor Object: SF_IPM* Version 1.0 (Build 1)
  Preprocessor Object: SF_ICMP Version 1.4 (Build 4)
  Preprocessor Object: SF_SIP Version 1.1 (Build 1)
  Preprocessor Object: SF_FTPM* Version 1.2 (Build 13)
  Preprocessor Object: SF_REPUTATION Version 1.1 (Build 1)
  Preprocessor Object: SF_IPRE Version 1.1 (Build 2)
  Preprocessor Object: SF_SDP Version 1.1 (Build 9)
  Preprocessor Object: SF_SDP Version 1.1 (Build 9)
  Preprocessor Object: SF_SDP Version 1.1 (Build 9)
  Preprocessor Object: SF_IPF3 Version 1.1 (Build 1)
  Preprocessor Object: SF_DTP Version 1.1 (Build 1)
  Preprocessor Object: SF_DTP Version 1.1 (Build 1)
  Commencing packet processing (pid=10792)

```

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 TOS:0x0 ID:20865 IpLen:20 DgLen:84 DF
Type:8 Code:0 ID:18650 Seq:5 ECHO

[**] [1:10000001:1] PING ICMP [**]
[PRIORITY: 0]
01/25-03:12:20.093422 192.168.0.109 -> 192.168.0.100
ICMP TTL:128 TOS:0x0 ID:16513 IpLen:20 DgLen:84
Type:0 Code:0 ID:18650 Seq:5 ECHO REPLY

[**] [1:10000001:1] PING ICMP [**]
[PRIORITY: 0]
01/25-03:12:21.117013 192.168.0.100 -> 192.168.0.109
ICMP TTL:64 TOS:0x0 ID:20941 IpLen:20 DgLen: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 DgLen: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 DgLen:84 DF
Type:8 Code:0 ID:18650 Seq:7 ECHO

[**] [1:10000001:1] PING ICMP [**]
[PRIORITY: 0]
01/25-03:12:22.141552 192.168.0.109 -> 192.168.0.100
ICMP TTL:128 TOS:0x0 ID:16515 IpLen:20 DgLen: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 TOS:0x0 ID:21304 IpLen:20 DgLen:84 DF
Type:8 Code:0 ID:18650 Seq:8 ECHO

[**] [1:10000001:1] PING ICMP [**]
[PRIORITY: 0]

```

Gambar 5.30 : Hasil *Capture Snort*

```

[+] [1:10000001:1] PING ICMP [+]
[Priority: 0]
01/25-09:12:20.093109 192.168.0.100 -> 192.168.0.109
ICMP TTL:64 TOS:0x0 ID:20865 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:18650 Seq:5 ECHO

[+] [1:10000001:1] PING ICMP [+]
[Priority: 0]
01/25-09:12:20.093482 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:5 ECHO REPLY

[+] [1:10000001:1] PING ICMP [+]
[Priority: 0]
01/25-09:12:21.117013 192.168.0.100 -> 192.168.0.109
ICMP TTL:64 TOS:0x0 ID:20941 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:18650 Seq:6 ECHO

[+] [1:10000001:1] PING ICMP [+]
[Priority: 0]
01/25-09:12:21.117408 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]
01/25-09:12:22.141118 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 ECHO

[+] [1:10000001:1] PING ICMP [+]
[Priority: 0]
01/25-09:12:22.141552 192.168.0.109 -> 192.168.0.100
ICMP TTL:128 TOS:0x0 ID:16515 IpLen:20 DgmLen:84
Type:0 Code:0 ID:18650 Seq:7 ECHO REPLY

[+] [1:10000001:1] PING ICMP [+]
[Priority: 0]
01/25-09:12:23.165034 192.168.0.100 -> 192.168.0.109
ICMP TTL:64 TOS:0x0 ID:21304 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:18650 Seq:8 ECHO

[+] [1:10000001:1] PING ICMP [+]
[Priority: 0]

```

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

Start time: Wed Jan 24 06:05:13 2018 End time: Wed Jan 24 06:05:19 2018  
 Capture duration: 6 seconds Number of packets: 357  
 Filter: src=192.168.0.100

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.100	192.168.0.1	TCP	74	42544Vaz2V86V8208 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=50593987 TSecr=0 WS=128
2	0.000350000	192.168.0.100	192.168.0.1	TCP	66	42544Vaz2V86V8208 [ACK] Seq=1 Ack=1 W=0 Len=0
3	0.000490000	192.168.0.100	192.168.0.1	HTTP	469	GET /AMN2WCAZMWF3538/dynaform/Custom.js HTTP/1.1
4	0.012370000	192.168.0.100	192.168.0.1	TCP	66	42544Vaz2V86V8208 [ACK] Seq=484 Ack=861 W=0 Len=0
5	0.012550000	192.168.0.100	192.168.0.1	TCP	66	42544Vaz2V86V8208 [ACK] Seq=484 Ack=861 W=0 Len=0
6	0.013170000	192.168.0.100	192.168.0.1	TCP	66	42544Vaz2V86V8208 [FIN, ACK] Seq=484 Ack=862 W=0 Len=0
7	0.013470000	192.168.0.100	192.168.0.1	TCP	74	42544Vaz2V86V8208 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=50593990 TSecr=0 WS=128
8	0.013730000	192.168.0.100	192.168.0.1	TCP	66	42544Vaz2V86V8208 [ACK] Seq=1 Ack=1 W=0 Len=0
9	0.013950000	192.168.0.100	192.168.0.1	HTTP	469	GET /AMN2WCAZMWF3538/images/top1_1.jpg HTTP/1.1
10	0.022090000	192.168.0.100	192.168.0.1	TCP	74	42544Vaz2V86V8208 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=50593992 TSecr=0 WS=128
11	0.022530000	192.168.0.100	192.168.0.1	TCP	66	42544Vaz2V86V8208 [ACK] Seq=1 Ack=1 W=0 Len=0

\* FRAME 11: 74 BYTES ON WIRE (592 BITS), 74 BYTES CAPTURED (592 BITS) ON INTERFACE 0  
 \* ETHERNET II, SRC: 28:02:44:09:05:61 (28:02:44:09:05:61), DST: 04:0E:0E:50:FF:EA (04:0E:0E:50:FF:EA)  
 \* INTERNET PROTOCOL VERSION 4, SRC: 192.168.0.100 (192.168.0.100), DST: 192.168.0.1 (192.168.0.1)  
 \* TRANSMISSION CONTROL PROTOCOL, SRC PORT: 42544 (42544), DST PORT: 80 (80), SEQ: 0, LEN: 0

```

0000 04 0e 0e 50 ff e4 28 02 44 09 05 61 00 00 45 00  .n.P...[.D..E.
0008 00 3c 00 3a 40 00 00 00 00 25 7c c9 00 00 04 c0 88  .<..B...[...E...
0010 00 01 80 00 00 50 54 e4 f4 54 00 00 00 00 80 82  .,..P...T.....
0018 72 10 00 0f 00 00 02 04 05 34 04 02 00 0e 06 04  .,.....
0020 00 c3 00 00 00 00 01 03 03 97  .,.....

```

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

1. OSSIM mampu mendeteksi serta menangkap *event* serta serangan yang terjadi pada setiap *host* dalam jaringan PT.Satria Antaran Prima dan disajikan dalam bentuk grafik
2. 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 implementasi 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 memungkinkan *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*.

```

allenvault@allenvault-W240HU-W250HUQ:~$ sudo snort -A full -u snort -g snort -q -c /etc/snort/snort.conf -l /var/log/snort/
allenvault@allenvault-W240HU-W250HUQ:~$ sudo snort -A full -q -u snort -g snort -c /etc/snort/snort.conf -l /var/log/snort/ -0

```

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 .