

Mengoptimalkan Pencegahan Serangan Brute Force pada Linux melalui Penerapan Metode Aplikasi IDS Snort

Dody Hidayat¹, Ramli²

^{1,2}Manajemen Informatika, Fakultas Teknik dan Komputer, Universitas Harapan Medan, Medan, Indonesia

¹hidayatdody91@gmail.com, ²ramli.brt@gmail.com

*) hidayatdody91@gmail.com

Abstrak—Keamanan jaringan pada server merupakan faktor penting untuk menjamin stabilitas, integritas dan validitas data. Implementasi Intrusion Detection System berbasis Snort dapat menghemat biaya pengadaan software karena gratis dan cukup handal dalam mendeteksi serangan keamanan. Snort Sistem berbasis IDS dapat diimplementasikan pada sistem operasi Linux. Suatu serangan dapat dideteksi atau tidak oleh IDS Snort, tergantung pada ada atau tidak adanya aturan yang sesuai. Proses pengujian yang digunakan yaitu teknik serangan port scanning, teknik serangan bruteforce attack dan melakukan blok ip address peretas. Pengujian dengan teknik port scanning dapat menghasilkan informasi penting pada suatu jaringan dan mendeteksi *port* yang terbuka, di antaranya port 22 yaitu ssh (secure shell) dengan hasil serangan ini membuktikan 1000 *paket* yang di kirim oleh penyerang. Teknik bruteforce attack dapat menghasilkan kombinasi username dan password yang ada pada sistem server secara illegal. IDS snort dapat mendeteksi serangan yang masuk pada sistem server, kemudian IDS snort dapat mendeteksi ip address yang mencoba meretas sistem server. Sehingga data yang ada pada sistem server dapat terjaga dengan aman, karena setiap aktifitas peretasan dapat dipantau oleh administrator untuk ditindak lebih lanjut.

Kata Kunci: IDS, Snort, Linux, Serangan, Brute Force

Abstract—*Network security system on the server is an important factor to ensure the stability, integrity and validity of data. Implementation of Snort-based Intrusion Detection System can save software procurement costs because it is free and reliable enough to detect security attacks. Snort-based IDS system can be implemented on Linux operating system. An attack may or may not be detected by Snort IDS depending on the presence or absence of appropriate rules. The testing process used is a port scanning attack technique, brute force attack technique, and hacker IP address blocking. The port scanning attack technique can generate important information about a network and can detect open ports, including port 22, which is the secure shell. The brute force attack technique can generate illegal username and password combinations on the server system. IDS snort can detect incoming attacks on the server system, then IDS snort can detect the IP address that is trying to hack the server system. Ensure data on the server system is secure by allowing the administrator to track any hacker activity.*

Keywords: IDS, Snort, Linux, Attack, Brute Force

1. PENDAHULUAN

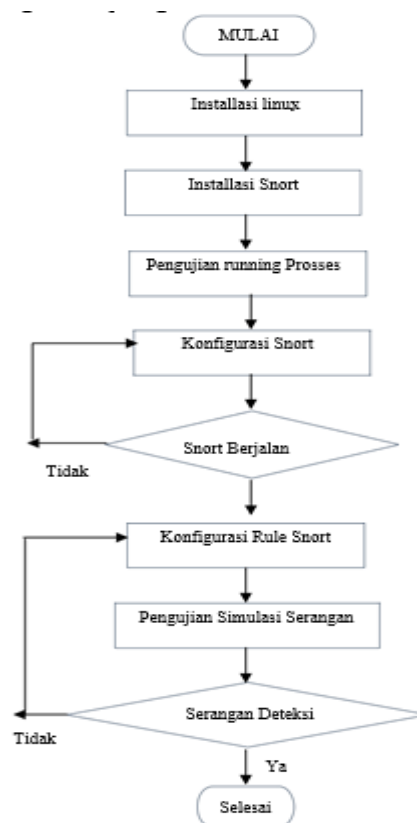
Perkembangan teknologi ini tidak hanya menimbulkan dampak positif bagi masyarakat, namun perkembangan teknologi juga menimbulkan dampak yang negatif dengan munculnya bentuk kejahatan baru yang belum pernah terjadi sebelumnya [1][2]. Tidak semua informasi dapat diakses untuk umum. Internet merupakan jaringan luas dan bersifat publik, oleh karena itu diperlukan suatu usaha untuk menjamin keamanan informasi terhadap data atau layanan yang menggunakan internet [3]. Sementara itu, masalah keamanan ini masih seringkali kurang mendapat perhatian, seringkali masalah keamanan ini berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap kurang penting. Apabila mengganggu informasi dari sistem, seringkali keamanan dikurangi atau dihilangkan [4]. Banyak sekali data-data penting yang tersimpan didalam database sebuah server, untuk itu diperlukan suatu sistem keamanan yang canggih untuk mengamankan data-data yang tersimpan di database server tersebut. Jika webserver tidak memiliki sistem keamanan yang canggih, maka para peretas atau hacker akan dengan mudah mencuri data-data penting yang tersimpan di database server tersebut [5]. Salah satu cara menjaga keamanan server yaitu dengan pendeteksian intrusi yang dianggap berbahaya menggunakan Intrusion Detection System (IDS) Snort [6]. IDS Snort merupakan salah satu perangkat lunak yang

berfungsi untuk mengetahui adanya intrusi. Implementasi Aplikasi pendeteksi intrusi / Intrusion Detection System berbasis Snort dapat menghemat biaya pengadaan software karena bersifat gratis dan cukup handal dalam mendeteksi serangan keamanan [7]. Sistem IDS berbasis Snort dapat diimplementasikan pada sistem Linux [8].

Faktor kewanjaran jaringan computer merupakan satu hal yang mutlak dalam membangun suatu jaringan. Pada dasarnya system keamanan yang dimiliki oleh system operasi tidaklah cukup untuk mengamankan jaringan komputer [9]. Oleh karena itu untuk mendapatkan sebuah keamanan jaringan computer maka diperlukan suatu tools yang dapat mendeteksi adanya suatu mekanisme serangan dari jaringan [10]. Penelitian terkait tentang sistem keamanan telah dilakukan oleh Marta, Hartawan dan Santika, sistem yang dibangun melakukan pendeteksian intrusi pada server secara realtime menggunakan snort [11]. Pada tujuan penelitian ini akan mengetahui kegiatan yang illegal ketika terjadi akses yang tidak wajar pada server, maka snort akan mendeteksi dan mengirimkan informasi terjadinya aktivitas yang tidak wajar ke administrator jaringan [12]. Selanjutnya penelitian dilakukan oleh Husain, Aksara dan Ransi, sistem pendeteksi dan pencegahan serangan dengan cara pemblokiran terhadap Internet Protocol (IP) penyerang [13], hasil yang diperoleh yaitu penggunaan snort dan IPTables sebagai sistem keamanan server pada jaringan wireless berhasil mengatasi jenis serangan pada port ICMP, FTP, SSH, TELNET, dan HTTP menggunakan berbagai macam penyerang seperti DDos Attack, Brute Force Attack, Bug CMS/Framework, Inject Malware, Email Scamming dan Spamming [14] [15].

2. METODE PENELITIAN

Penelitian yang dilakukan yaitu sebuah bentuk pengamanan dalam melakukan komunikasi data yang dilakukan menggunakan aplikasi *Oracle VirtualBox* yang dapat menjalankan sebuah virtual server yang memiliki peran sebagai server dan intruder dalam melakukan simulasi pengamanan data. Penggunaan metodologi yang dilakukan menggunakan metodologi pengembangan berbasis kualitatif. Langkah perancangan, konfigurasi server dan pengujian Snort IDS merupakan proses yang lebih kompleks dibandingkan langkah lainnya. Sehingga langkah – langkah tersebut dapat digambarkan dalam diagram alir pada gambar 1.



Gambar 1. Diagram Alur Perancangan dan Pengujian

1) Intrusion Detection System (IDS)

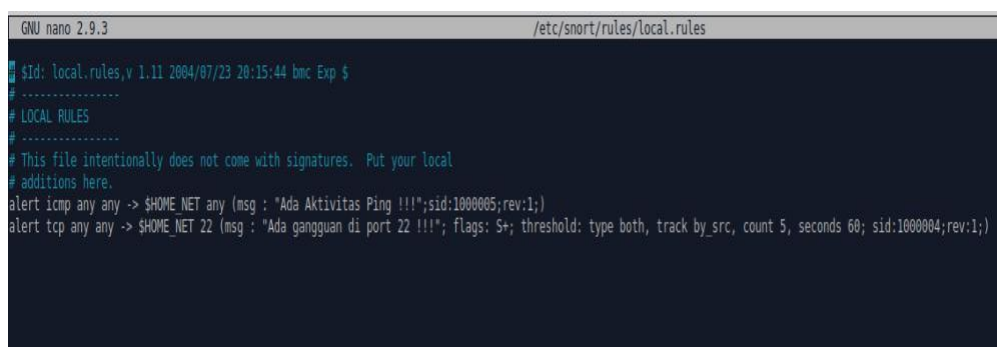
IDS merupakan suatu sistem yang memiliki kemampuan untuk menganalisis data secara realtime dalam mendeteksi, mencatat (log) dan menghentikan penyalahgunaan dan penyerangan. IDS merupakan security tools yang dapat digunakan untuk menghadapi aktivitas hacker. IDS ini mampu memberikan peringatan kepada administrator apabila terjadi suatu serangan atau penyalahgunaan di dalam jaringan, bahkan peringatan itu dapat pula menunjukkan alamat IP dari sebuah sistem penyerang.

2) Konfigurasi Snort

Untuk mengkonfigurasi Snort yaitu dengan membuka file snort.conf yang terdapat pada folder C:\snort/etc kemudian tambahkan rules pada file tersebut.

3) Konfigurasi Rules

Selanjutnya sebelum menjalankan snort tersebut, maka membutuhkan beberapa langkah lagi yaitu dengan mengkonfigurasi rules snort agar snort dapat bekerja dengan baik dengan perintah sebagai berikut: nano/etc/snort/rules/local.rules. Rules yang ditambahkan pada snort dapat dilihat pada gambar 2.



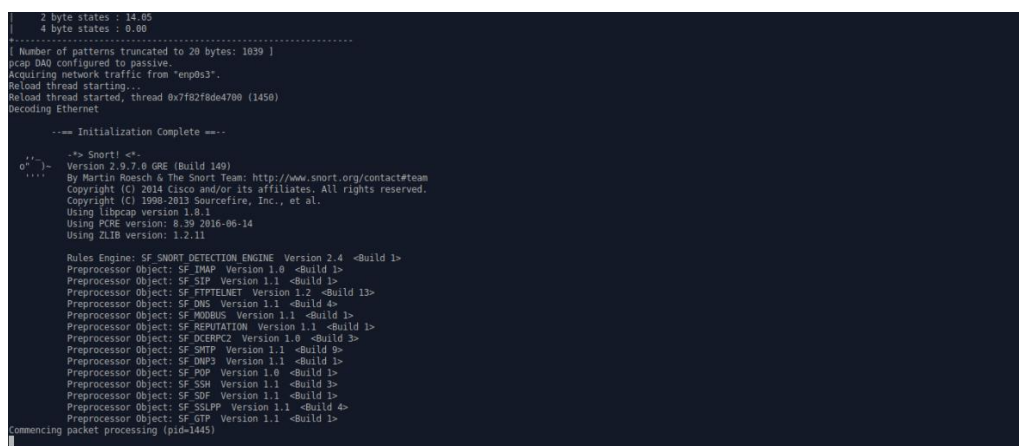
```
GNU nano 2.9.3 /etc/snort/rules/local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
#
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.
alert icmp any any -> $HOME_NET any (msg: "Ada Aktivitas Ping !!!";sid:1000005;rev:1;)
alert tcp any any -> $HOME_NET 22 (msg: "Ada gangguan di port 22 !!!"; flags: S+; threshold: type both, track by_src, count 5, seconds 60; sid:1000004; rev:1;)
```

Gambar 2. Konfigurasi Rules

Rules pertama untuk mendeteksi adanya Ping dari perangkat luar atau yang tidak dikenali. Rules kedua untuk mendeteksi serangan pada port SSH dengan perintah sebagai berikut: alert tcp any any -> \$HOME_NET 22 (msg:"isi pesan"; flags: S+; threshold: type both, track by_src, count 5, seconds 60; sid:1000004; rev:1;)

4) Menjalankan Snort

Menjalankan Snort yaitu dengan membuka terminal pada OS Linux dengan shortcut pada keyboard ALT+CTRL+T. Maka open terminal akan terbuka. Setelah itu masuk ke root dengan command line sudo su agar bisa mengakses semua fasilitas pada terminal. Setelah itu memasukkan command line Snort yaitu snort -c/etc/snort.snort.conf -i enp0s3 -A console. Seperti pada gambar 3.



```
2 byte states : 14.00
4 byte states : 0.00
-----
[ Number of patterns truncated to 20 bytes: 1039 ]
libcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Reload thread starting...
Reload thread started, thread 0x7f8278de4700 (1450)
Decoding Ethernet

--- Initialization Complete ---

--> Snort! <--
o'')- Version 2.9.7.0 GRE (Build 149)
..... By Martin Roesch & The Snort Team: http://www.snort.org/contactteam
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libcap version 1.8.1
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>
Preprocessor Object: SF_INMP Version 1.0 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_HOBBAS Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_DCEPRPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_DWEP3 Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SOF Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Commencing packet processing (pid=1445)
```

Gambar 3. Proses Menjalankan Snort

3. HASIL DAN PEMBAHASAN

3.1 Pengujian Deteksi Serangan Pada Port ICMP

Ketika terjadi komunikasi melalui port ICMP ke computer target dari peringkat yang tidak dikenali, snort akan memberikan pesan peringatan seperti gambar berikut:

```
Commencing packet processing (pid=1118)
06/17 12:42:55.432210 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.228.32:65425 -> 239.255.255.250:1980
06/17 12:42:55.446691 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.228.32:65425 -> 239.255.255.250:1980
06/17 12:42:56.443814 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.228.32:65425 -> 239.255.255.250:1980
06/17 12:42:56.447883 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.228.32:65425 -> 239.255.255.250:1980
06/17 12:42:57.433216 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.228.32:65425 -> 239.255.255.250:1980
06/17 12:42:57.448835 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.228.32:65425 -> 239.255.255.250:1980
06/17 12:42:58.434710 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.228.32:65425 -> 239.255.255.250:1980
06/17 12:42:58.448937 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.228.32:65425 -> 239.255.255.250:1980
06/17 12:43:06.532470 ** [1:366:7] ICMP PING 'NIX ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.228.175 -> 192.168.228.76
06/17 12:43:06.532470 ** [1:1080005:1] Ada Aktivitas Ping !!! ** [Priority: 0] [ICMP] 192.168.228.175 -> 192.168.228.76
06/17 12:43:06.532470 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.228.175 -> 192.168.228.76
06/17 12:43:06.532512 ** [1:1080005:1] Ada Aktivitas Ping !!! ** [Priority: 0] [ICMP] 192.168.228.175 -> 192.168.228.175
06/17 12:43:06.532512 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.228.76 -> 192.168.228.175
06/17 12:43:07.532769 ** [1:366:7] ICMP PING 'NIX ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.228.175 -> 192.168.228.76
06/17 12:43:07.532769 ** [1:1080005:1] Ada Aktivitas Ping !!! ** [Priority: 0] [ICMP] 192.168.228.175 -> 192.168.228.76
06/17 12:43:07.532769 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.228.175 -> 192.168.228.76
06/17 12:43:07.532811 ** [1:1080005:1] Ada Aktivitas Ping !!! ** [Priority: 0] [ICMP] 192.168.228.175 -> 192.168.228.175
06/17 12:43:07.532811 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.228.76 -> 192.168.228.175
06/17 12:43:08.545842 ** [1:366:7] ICMP PING 'NIX ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.228.175 -> 192.168.228.76
06/17 12:43:08.545842 ** [1:1080005:1] Ada Aktivitas Ping !!! ** [Priority: 0] [ICMP] 192.168.228.175 -> 192.168.228.76
06/17 12:43:08.545842 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.228.175 -> 192.168.228.76
06/17 12:43:08.545897 ** [1:1080005:1] Ada Aktivitas Ping !!! ** [Priority: 0] [ICMP] 192.168.228.175 -> 192.168.228.175
06/17 12:43:08.545907 ** [1:408:5] ICMP Echo Reply ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.228.76 -> 192.168.228.175
06/17 12:43:09.553217 ** [1:366:7] ICMP PING 'NIX ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.228.175 -> 192.168.228.76
06/17 12:43:09.553217 ** [1:1080005:1] Ada Aktivitas Ping !!! ** [Priority: 0] [ICMP] 192.168.228.175 -> 192.168.228.76
06/17 12:43:09.553217 ** [1:384:5] ICMP PING ** [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.228.175 -> 192.168.228.76
```

Gambar 4. Hasil Deteksi Serangan Port ICMP

Ketika terjadi serangan port ICMP, maka snort akan mengirimkan pesan “Ada Aktivitas Ping” serta terdeteksi alamat IP penyerang yaitu “192.168.228.175”.

3.2 Teknik Serangan Port Scanning

Teknik serangan *Port Scanning* Teknik serangan dengan *port scanning* ini bertujuan untuk mendapatkan kumpulan informasi penting yang ada pada suatu jaringan dan untuk mendeteksi *port* berapa saja yang terbuka pada server utama target. Proses serangan dengan teknik *port scanning* menggunakan *tools nmap* ditunjukkan pada Gambar 5.

```
test1@xubuntu:~$ nmap 192.168.228.0/24 -p 22 --open
Starting Nmap 7.60 ( https://nmap.org ) at 2023-06-17 12:12 +07
Nmap scan report for 192.168.228.76
Host is up (0.00092s latency).

PORT STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (3 hosts up) scanned in 20.18 seconds
test1@xubuntu:~$
```

Gambar 5. Hasil Port Scanning

Gambar 5 merupakan hasil serangan dengan teknik port scanning. Berdasarkan Gambar 5 serangan dengan menggunakan teknik port scanning dapat menghasilkan informasi penting yang ada pada suatu jaringan yaitu port 22/tcp dengan status terbuka pada perangkat dengan IP address 192.168.228.76. Port yang terbuka tersebut dapat membuka kesempatan bagi peretas untuk menyerang lebih lanjut terhadap server melalui port 22 ssh.

3.3 Hasil Deteksi Snort

Hasil dari pemberitahuan jika ada percobaan penyerangan pada port 22 dengan pesan “Ada gangguan di port 22” dengan IP address 192.168.100.166 dan pesan “Ada Aktivitas Ping” pada port ICMP seperti pada gambar 7.

```
Commencing packet processing (pid=1050)
06/18 11:21:26.754222 ** [1:1080005:1] Ada gangguan di port 22 !!! ** [Priority: 0] [TCP] 192.168.100.167:45054 -> 192.168.100.166:22
06/18 11:21:26.754222 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.100.32:61135 -> 239.255.255.250:1980
06/18 11:22:00.757831 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.100.32:61135 -> 239.255.255.250:1980
06/18 11:22:24.116230 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] Fe80::1:56942:::ff02::1:980
06/18 11:22:24.116230 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] Fe80::1:56942:::ff02::1:980
06/18 11:22:24.616888 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.100.148012 -> 239.255.255.250:1980
06/18 11:22:25.725380 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] Fe80::1:56942:::ff02::1:980
06/18 11:22:25.725380 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] Fe80::1:56942:::ff02::1:980
06/18 11:22:26.168759 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.100.32:59655 -> 239.255.255.250:1980
06/18 11:22:26.168759 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.100.32:59655 -> 239.255.255.250:1980
06/18 11:22:26.795249 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.100.32:59655 -> 239.255.255.250:1980
06/18 11:22:26.795249 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.100.32:59655 -> 239.255.255.250:1980
06/18 11:22:27.799712 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.100.32:59655 -> 239.255.255.250:1980
06/18 11:22:27.799712 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.100.32:59655 -> 239.255.255.250:1980
06/18 11:22:28.914264 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.100.194:61486 -> 239.255.255.250:1980
06/18 11:22:28.914264 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.100.194:61486 -> 239.255.255.250:1980
06/18 11:23:27.971481 ** [1:366:7] ICMP PING 'NIX ** [Classification: Misc activity] [Priority: 3] [ICMP] Fe80::1:56942:::ff02::1:980
06/18 11:23:27.971481 ** [1:1080005:1] Ada Aktivitas Ping !!! ** [Priority: 0] [ICMP] Fe80::1:56942:::ff02::1:980
06/18 11:23:27.971481 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.100.148012 -> 239.255.255.250:1980
06/18 11:23:27.971481 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.100.148012 -> 239.255.255.250:1980
06/18 11:23:28.573249 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] Fe80::1:56942:::ff02::1:980
06/18 11:23:28.573249 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] Fe80::1:56942:::ff02::1:980
06/18 11:23:29.176329 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.100.148012 -> 239.255.255.250:1980
06/18 11:23:29.176329 ** [1:1917:6] SCAN UHP service discover attempt ** [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.100.148012 -> 239.255.255.250:1980
06/18 11:23:32.446710 ** [1:1080005:1] Ada Aktivitas Ping !!! ** [Priority: 0] [IPV6-ICMP] Fe80::1:56942:::ff02::1:980:16c7:5c91:755f:f404:6145:56ad
06/18 11:23:32.446710 ** [1:1080005:1] Ada Aktivitas Ping !!! ** [Priority: 0] [IPV6-ICMP] Fe80::1:56942:::ff02::1:980:16c7:5c91:755f:f404:6145:56ad
06/18 11:23:32.446710 ** [1:1080005:1] Ada Aktivitas Ping !!! ** [Priority: 0] [IPV6-ICMP] Fe80::1:56942:::ff02::1:980:16c7:5c91:755f:f404:6145:56ad
```

Gambar 7. Alert Pada Snort



Gambar 7 merupakan pemberitahuan jika ada percobaan penyerangan pada port 22 dengan pesan “Ada gangguan di port 22” dengan IP address 192.168.100.166 dan pesan “Ada Aktivitas Ping” pada port ICMP seperti pada gambar 7.

4. KESIMPULAN

Berdasarkan hasil pengujian dari semua jenis serangan yang dilakukan oleh peretas atau attacker dengan menggunakan teknik serangan bruteforce attack maupun teknik serangan dengan port scanning terhadap server dapat dengan mudah terdeteksi oleh IDS snort. kemudian identitas dan aktifitas peretas tersebut bisa terlihat pada log snort ketika snort dijalankan. Saran untuk penelitian selanjutnya yaitu diharapkan bisa menggunakan metode pemblokiran atau IPS dan IDS selain snort untuk mengetahui hasil keamanan sistem yang berbeda dari penelitian ini.

REFERENSI

- [1] W. Zaenal Mutaqin Subekti, Hendra Setiawan, Satria, Widia Murni Wijaya, Aliy Hafiz, “Perancangan Infrastruktur Domain Name Server Lokal Menggunakan Ubuntu Server 16.04 Pada PT. Xyz,” no. 2, p. 6, 2021.
- [2] T. M. Diansyah and R. Liza, “Paper Simulasi Pengamanan Virtual Server Menggunakan Dionaea Honeypot Dan Tunneling Sebagai Proses Pengamanan Komunikasi Data”.
- [3] A. S. Rosana, “Kemajuan Teknologi Informasi dan Komunikasi dalam Industri Media di Indonesia,” *Gema Eksos*, vol. 5, no. 2, pp. 146–148, 2010, [Online]. Available: <https://www.neliti.com/id/publications/218225/kemajuan-teknologi-informasi-dan-komunikasi-dalam-industri-media-di-indonesia>
- [4] D. Purwanto, “Peranan Kriptografi Dalam Peningkatan Pengamanan Sistem Informasi,” *Semin. Soc. Sci. Eng. Hum.*, pp. 188–193, 2020.
- [5] R. Rupiati, S. Faisal, T. Al Mudzakir, and S. Arum Puspita Lestari, “Deteksi Serangan Peretas Menggunakan Honeypot Cowrie Dan Intrusion Detection System Snort,” *Conf. Innov. Appl. Sci. Technol.*, no. Ciastech, pp. 727–736, 2020.
- [6] J. Tektro, “IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) PADA SISTEM KEAMANAN JARINGAN MENGGUNAKAN TELEGRAM,” vol. 7, no. 1, pp. 44–50, 2023.
- [7] L. Putri, “Implementasi Intrusion Detection System (Ids) Menggunakan Snort Pada Jaringan Wireless (Studi Kasus : Smk Triguna Ciputat),” *Implementasi Intrusion Detect. Syst. (Ids) Menggunakan Snort Pada Jar. Wirel. (Stud. Kasus Smk Triguna Ciputat)*, no. 1, pp. 1–105, 2011.
- [8] F. A. Kurniawan, “Pendekatan Business Model Canvas Sebagai Perancangan Strategi Bisnis Baru (Studi Pada UMKM UD. Gading Mas Pasuruan),” *J. SKETSA BISNIS*, vol. 4, no. 2, pp. 123–131, 2017.
- [9] A. Aptika, “Keamanan Jaringan Internet dan Firewall,” 2017. <https://aptika.kominfo.go.id/2017/06/keamanan-jaringan-internet-dan-firewall/>
- [10] T. Pangestu and R. Liza, “Analisis Keamanan Jaringan pada Jaringan Wireless dari Serangan Man In The Middle Attack DNS Spoofing,” *Jitekh*, vol. 10, no. 2, pp. 60–67, 2022.
- [11] M. I. Triwahyudi and I. Veritawati, “Sistem Informasi Pelayanan Jaringan Komputer,” *Format J. Ilm. Tek. Inform.*, vol. 11, no. 1, 2022, doi: 10.22441/10.22441/format.2022.v11.i1.006.
- [12] I. K. K. A. Marta, I. N. B. Hartawan, and I. K. S. Satwika, “Analisis Sistem Monitoring Keamanan Server Dengan Sms Alert Berbasis Snort,” *Inser. Inf. Syst. Emerg. Technol. J.*, vol. 1, no. 1, p. 25, 2020, doi: 10.23887/insert.v1i1.25874.
- [13] A. Wicaksana and T. Rachman, “Implementasi Kinerja Intrusion Prevention System (IPS) sebagai sistem keamanan pada Jaringan Wireless,” *Angew. Chemie Int. Ed. 6(11)*, 951–952., vol. 3, no. 1, pp. 10–27, 2018, [Online]. Available: <https://medium.com/@arifwicaksanaa/pengertian-use-case-a7e576e1b6bf>
- [14] M. Ulfa, J. Jenderal, A. Yani, and N. Palembang, “Di Jaringan Internet Universitas Bina Darma,” *J. Imiah MATRIK*, vol. 15, no. 12, pp. 105–118, 2013.
- [15] M. Jufri and H. Heryanto, “Peningkatan Keamanan Jaringan Wireless Dengan Menerapkan Security Policy Pada Firewall,” *JOISIE (Journal Inf. Syst. Informatics Eng.)*, vol. 5, no. 2, pp. 98–108, 2021, doi: 10.35145/joisie.v5i2.1759.

