

## IMPLEMENTASI SISTEM KEAMANAN SERVER MENGGUNAKAN HONEYPOT DAN RASPBERRY PI TERHADAP ATTACKER

Aryo Nur Utomo, ST, M.Kom<sup>1</sup>, Muhammad Irfan Sulaiman<sup>2</sup>  
Program Studi Teknik Informatika, Fakultas Sains dan Teknologi Informasi  
Institut Sains dan Teknologi Nasional, Jakarta  
Email : [aryo.nurutomo@istn.ac.id](mailto:aryo.nurutomo@istn.ac.id)

Naskah diterima 20 September 2018

### ABSTRAK

Keamanan dalam jaringan komputer bisa rentan terhadap serangan-serangan dunia maya yang datang dari jaringan eksternal maupun dari jaringan internal, dikarenakan kelemahan dalam membuat kebijakan keamanan komputer, konfigurasi sistem komputer yang lemah atau *bug* dalam aplikasi perangkat lunak. Namun jika serangan tersebut datangnya berasal dari jaringan internal tentu lebih sangat bahaya karena dapat dengan mudah melewati *firewall* dan sulit terdeteksi. Agar mampu mendeteksi dan mempelajari motif, taktik, dan alat yang digunakan oleh para penyerang, sistem *honeypot* dapat dengan mudah dimanfaatkan untuk tujuan tersebut. *Honeypot* secara ringkas dideskripsikan sebagai *server* bayangan yang memberikan pelayanan serupa seperti *server* aslinya, berfungsi sebagai wadah untuk mempelajari motif dari penyerangan oleh *attacker*. Dengan memadukan IDPS pada *Honeypot* dapat meningkatkan keamanan pada *server* karena dapat mendeteksi dan mencegah serangan - serangan terhadap *server*. Berdasarkan pengujian yang telah dilakukan, Diketahui bahwa untuk menghemat biaya dan sumber daya yang dikeluarkan untuk membangun *honeypot* dan IDPS dapat diimplementasikan pada perangkat *Raspberry Pi*. Karena pada *Raspberry Pi honeypot* mampu untuk bekerja seperti *honeypot* pada umumnya dengan efektif dan efisien, Seperti melakukan deteksi dan pencegahan terhadap serangan yang datang hingga melakukan perekaman aktifitas *attacker*.

**Kata kunci:** *honeypot, raspberry pi, IDPS*

### ABSTRACT

*Security in computer networks can be vulnerable to cyber attacks coming from external networks as well as from internal networks, due to weaknesses in making computer security policies, weak computer system configurations or bugs in software applications. But if the attack comes from the internal network is certainly more dangerous because it can easily pass through the firewall and difficult to detect, In order to be able to detect and learn the motives, tactics, and tools used by the attackers, honeypot system can be easily used for the purpose. The Honeypot is briefly described as a shadow server that provides a similar service as the original server, serving as a container for learning the motive of an attack by an attacker. By integrating IDPS on Honeypot can increase security on the server because it can detect and prevent attacks against the server. Based on the tests that have been done, It is known that to save costs and resources spent to build the honeypot and IDPS can be implemented on Raspberry Pi devices. Because the Raspberry Pi honeypot is able to work like a honeypot in general with the cost and resources are cheap, Such as detection and prevention of attacks that come up to record the activities of attackers.*

**Key words:** *honeypot, raspberry pi, IDP*

**I. PENDAHULUAN**

Keamanan dalam jaringan komputer bisa rentan terhadap serangan-serangan dunia maya disebabkan karena memiliki kelemahan dalam membuat kebijakan keamanan komputer, konfigurasi sistem komputer yang lemah atau *bug* dalam aplikasi perangkat lunak. Serangan tersebut tidak hanya datang melalui jaringan eksternal namun juga dapat melalui jaringan internal.

Apabila penyerangan tersebut datang dari jaringan lokal (*intranet*) tentu lebih sangat bahaya karena dapat dengan mudah melewati *firewall* dan sulit terdeteksi, Agar mampu mendeteksi dan mempelajari motif, taktik, dan alat yang sekarang banyak digunakan oleh para penyerang, sistem *honeypot* dapat dengan mudah dimanfaatkan untuk tujuan tersebut. *Honeypot* sendiri adalah sistem terkontrol yang sengaja dipasang sehingga mampu berinteraksi dengan penyerang di dalam jaringan untuk mengumpulkan data serangan, teknik, dan perilaku serangan komunitas *blackhat* [1].

Tentu jika dipadukan dengan penggunaan IDS (*Intrusion Detection Systems*) dan IPS (*Intrusion Prevention Systems*) dapat meningkat keamanan pada *server* karena dapat mendeteksi dan mencegah serangan - serangan terhadap *server* baik berupa

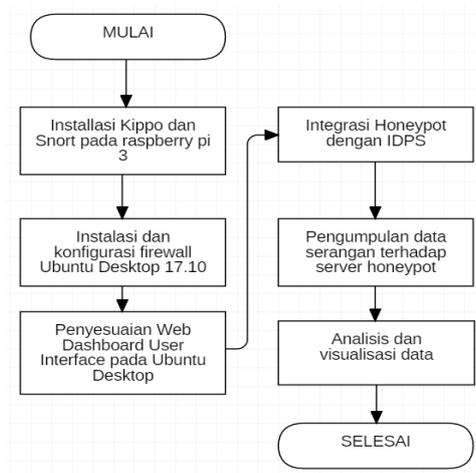
*software* maupun *hardware*. Penelitian mengenai *honeypot* dengan menggunakan teknologi *Modern Honey Network* (MHN) dan *dionaea* telah dilakukan oleh Setio Wahono dan Alif Subardono, Pada penelitiannya mengintegrasikan sensor-sensor *honeypot* *dionaea* ke dalam *Modern Honey Network* (MHN), *bebankerja* yang dilakukan oleh sensor menjadi lebih ringan dibandingkan dengan pemasangan *honeypot* *Dionaea* secara tradisional pada *server* komputer [1].

Penelitian ini membangun sebuah mini *server honeypot* pada perangkat *raspberry pi 3* dengan fitur IDPS pada *software kippo* dan *snort*, karena harga perangkat *raspberry pi 3* relatif murah [2] dibandingkan dengan perangkat *firewall* seperti Fortinet, Citrix, Sangfor, Paloalto, Sophos, Cisco, Juniper, Cyberoam, Netgear, atau Sonicwall [3]. Selain itu *software kippo* dan *snort* bersifat *open source* serta efisien setelah diimplementasikan ke dalam *raspberry pi* karena tidak mengkonsumsi ram yang banyak pada *server* *raspberry pi* dibandingkan dengan *Modern Honey Network* (MHN) dan *Dionaea*.

Oleh sebab itu, judul skripsi ini yaitu: “

**Implementasi Sistem Keamanan Server Menggunakan Honeypot Dan Rasperry Pi Terhadap Attacker”**

**II. METODE PENELITIAN**



Gambar 2. 1 Flowchart metode penelitian

**Perancangan Sistem**

Perancangan sistem menyangkut pembuatan sebuah skema dari alur kerja sistem *honeypot* pada *raspberry pi 3* yang akan dibangun.

**1.3.1. Implementasi Sistem**

Implementasi sistem merupakan tahap instalasi *Kippo* sebagai *honeypot* dan *snort* sebagai IDPS pada perangkat *raspberry pi 3*, kemudian instalasi dan konfigurasi *firewall* pada *Ubuntu Desktop 17.10* dan instalasi aplikasi monitoring pada *Ubuntu Desktop 17.10* sebagai *User Interface* untuk memantau aktifitas *honeypot* di *raspberry pi*

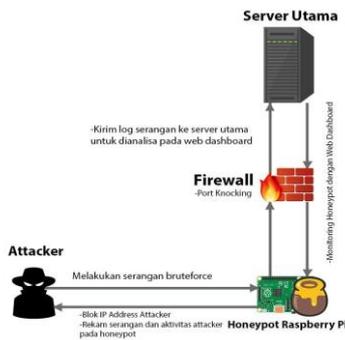
3. Serta tahap konfigurasi honeypot pada kippo dan snort dan Ubuntu Desktop 17.10.

**1.1. Pengujian Sistem**

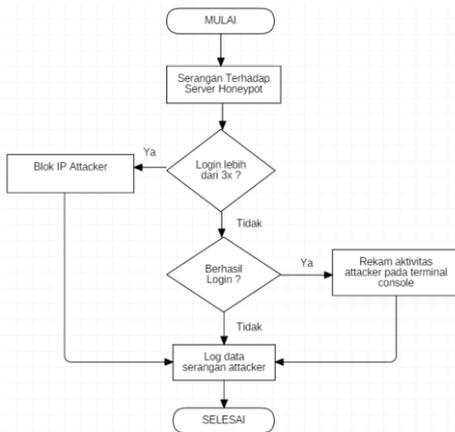
Pengujian yang dilakukan pada sistem honeypot dan Aplikasi User Interface untuk memantau aktifitas honeypot yang telah dibangun. Pengujian yang dilakukan bertujuan untuk menganalisa dan mendeteksi serangan pada honeypot di raspberry pi 3.

**1.2. Alur Skema Honeypot pada Raspberry Pi**

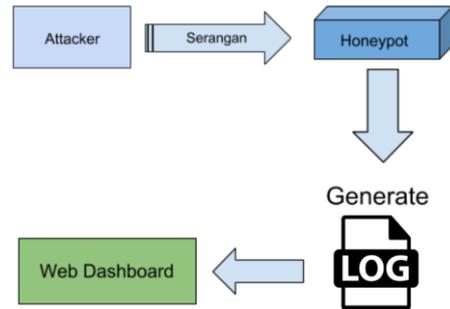
Gambar dibawah ini merupakan alur skema dan flowchart secara global dari honeypot pada raspberry pi.



Gambar 2. 2 Alur Skema Honeypot pada Raspberry Pi



Gambar 2. 3 Flowchart Skema Global Honeypot

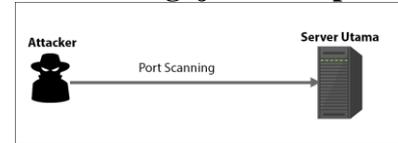


Gambar 2. 4 Alur Log Event Management

**1.3. Alur Skema Pengujian**

Dalam pengujian honeypot pada raspberry pi ini akan dilakukan 4 tahap pengujian yang berbeda.

**1.3.1. Pengujian Tahap Pertama**

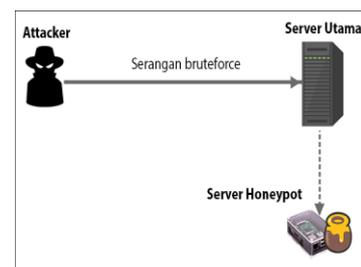


Gambar 2. 5 Pengujian Tahap Pertama

Pengujian tahap satu adalah melakukan port scanning, Port scanning merupakan tahap information gathering dalam penetration testing yang dilakukan oleh attacker untuk melakukan enumerasi terhadap setiap port yang terbuka pada server utama. Apakah port 22 (SSH) pada server utama terbuka (Open) atau tidak (Closed / Filtered).

Pada pengujian ini server utama akan meneruskan permintaan attacker terhadap port 22 di server utama ke port 22 pada server honeypot, Sehingga attacker akan menerima hasil port 22 yang terbuka pada server honeypot, walaupun IP Address yang diserang adalah IP Address server utama.

**1.3.2. Pengujian Tahap Kedua**

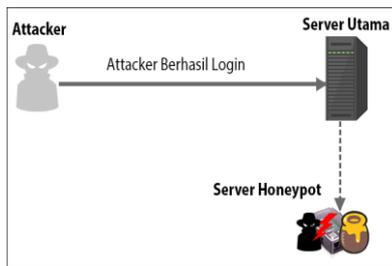


Gambar 2. 6 Pengujian Tahap Kedua

Pengujian tahap dua adalah serangan brute-force dari attacker ke server utama.

Serangan *brute-force* adalah metode serangan untuk meretas *password* dengan cara mencoba semua kemungkinan kombinasi *username* dan *password* yang ada dengan cara melakukan enumerasi dari huruf atau angka atau juga dengan menggunakan daftar list (*Dictionary / Wordlist*) *username-password* pada fitur atau fungsi *login*.

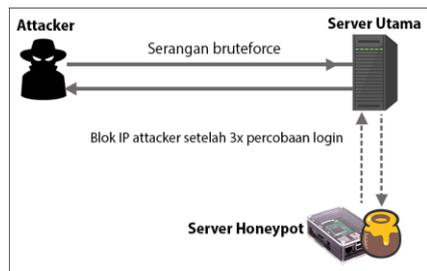
**1.3.3. Pengujian Tahap Ketiga**



Gambar 2. 7 Pengujian Tahap Ketiga

Pengujian tahap tiga adalah ketika attacker berhasil meretas *username* dan *password* dan sukses login pada server honeypot raspberry pi dan honeypot raspberry pi melakukan perekaman aktivitas attacker pada terminal console.

**1.3.4. Pengujian Tahap Keempat**



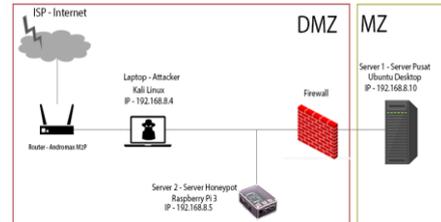
Gambar 2. 8 Pengujian Tahap Keempat

Pengujian tahap empat adalah server honeypot raspberry pi melakukan tindakan preventive terhadap serangan bruteforce yang dilakukan oleh attacker. Tindakan preventive tersebut adalah melakukan blok IP Address attacker setelah terjadi percobaan login yang terhubung (*Established*) sebanyak tiga kali.

**III. HASIL DAN PEMBAHASAN**

**a. Pembangunan Infrastruktur**

Pada tahap ini, dibuat rancangan topologi jaringan *Honeypot* dengan menggunakan *raspberry pi* menggunakan jaringan internal.



Gambar 3. 1 Topologi Jaringan

Perangkat	IP Address
Server 1 - Server Pusat	192.168.8.10
Server 2- Honeypot Raspberry	192.168.8.5
Laptop - Attacker	192.168.8.4

Tabel 1. 1 Tabel IP Address

**b. Tahap Implementasi**

Setelah dilakukan perancangan infrastruktur, maka tahap selanjutnya adalah melakukan implementasi *Honeypot* menggunakan *raspberry pi*. Langkah-langkah yang perlu dilakukan dalam implementasi tersebut adalah sebagai berikut:

- Instalasi Sistem Operasi Raspbian OS pada Raspberry Pi 3
- Instalasi Sistem Operasi Ubuntu Desktop pada Virtual Komputer.
- Instalasi Kippo dan Snort pada Raspberry Pi 3.
- Instalasi dan Konfigurasi Firewall pada Ubuntu Desktop.

**c. Konfigurasi**

Setelah dilakukan tahap implementasi, Maka tahap selanjutnya adalah melakukan konfigurasi Kippo dan Snort yaitu:

- Konfigurasi Kippo sebagai honeypot pada Raspberry Pi 3
- Konfigurasi Snort sebagai IDPS pada Raspberry Pi 3

**d. Tahap Pengujian**

Setelah dilakukan implementasi, maka tahap selanjutnya adalah melakukan pengujian.

**i. Hasil Pengujian Tahap Pertama.**

Pada pengujian tahap pertama ini akan dilakukan kegiatan information gathering yaitu melakukan tindakan port scanning terhadap port yang tersedia di server utama.

```
root@kali:~# nmap 192.168.8.10 -sT -Pn
Starting Nmap 7.60 ( https://nmap.org ) at 2018-08-14 11:34 WIB
Nmap scan report for 192.168.8.10
Host is up (0.042s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
2222/tcp  filtered EtherNet/IP-1
3306/tcp   open  mysql
Nmap done: 1 IP address (1 host up) scanned in 3.19 seconds
```

Gambar 3. 2 Port Scanning

Hasil dari port scanning menunjukkan bahwa server utama terdapat port 22 yang terbuka. Maka akan membuka kesempatan bagi attacker untuk melakukan serangan terhadap server utama terhadap port 22, tidak akan jadi masalah jika attacker melakukan serangan langsung terhadap server utama karena firewall server utama sudah aktif dan akan meneruskan permintaan pada port 22 di server utama ke port 22 di server honeypot. Kegiatan port scanning tersebut dapat dideteksi oleh snort, snort mendeteksi bahwa adanya kegiatan port scanning terhadap port SSH yaitu port 22 berasal dari IP Address server utama yang diakses oleh attacker yaitu 192.168.8.10. Untuk membuktikan bahwa kegiatan port scanning berhasil dilakukan adalah dengan melihat lalulintas data pada network dengan aplikasi network analyzer wireshark pada komputer attacker.

```
ip netns exec ns1 ip netns exec ns2 tcpdump -i eth0 host 192.168.8.10 && tcpdump -i eth0 host 192.168.8.10
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.8.4 192.168.8.10 TCP 60 50100 → 22 [RST] Seq=1
2 0.000000 192.168.8.4 192.168.8.10 TCP 60 50100 → 22 [RST] Seq=1
3 0.000000 192.168.8.4 192.168.8.10 TCP 60 50100 → 22 [RST] Seq=1
```

Gambar 3. 3 Wireshark

Hasil dari pengujian ini membuktikan bahwa server utama tidak bisa diakses secara langsung oleh attacker, Ketika attacker mencoba melakukan permintaan pada port tersebut maka secara otomatis server utama akan meneruskan setiap permintaan ke server honeypot. Bisa dilihat pada packet network traffic di server utama menggunakan wireshark.

```
192.168.8.10 → 192.168.8.10:22 [RST] Seq=1, Win=0, Len=0
```

Gambar 3. 4 Server utama redirect ke server honeypot

**ii. Hasil Pengujian Tahap Kedua.**

Pada pengujian tahap kedua ini akan dilakukan serangan brute-force oleh attacker terhadap honeypot untuk mencoba masuk ke dalam sistem dengan menebak username atau password pada server utama menggunakan Dictionary atau wordlist. Dengan adanya wordlist, attacker dapat mencoba login secara terus menerus hingga mendapatkan password yang benar. Untuk melakukan pengujian ini menggunakan alat brute-force yaitu medusa.

```
medusa -u root -P /usr/share/wordlists/rockyou.txt -h 192.168.8.10 -M ssh -t 1
```

honeypot merekam aktifitas percobaan login yang menggunakan serangan brute-force, Kemudian data rekaman tersebut akan divisualisasi pada web dashboard di server utama.



Gambar 3. 5 Web Monitoring



Gambar 3. 6 Log Aktifitas Serangan



Gambar 3. 7 Log Aktifitas Serangan 1

**iii. Hasil Pengujian Tahap Ketiga.**

Pada pengujian tahap ketiga ini akan dilakukan serangan brute-force oleh attacker terhadap honeypot namun attacker berhasil masuk ke dalam sistem honeypot dengan username dan password yang didapatkan melalui serangan brute-force. Sebelum melakukan serangan brute-force, atur password pada server honeypot dengan menggunakan password yang lemah [12]. Pada tahap pengujian

ketiga ini username dan password yang digunakan adalah root:123456. Lakukan kembali serangan *brute-force* dengan menggunakan aplikasi medusa pada komputer *attacker*.

```
ACCOUNT CHECK: [ssh] Host: 192.168.8.10 (1 of 1, 0 complete) User: root (1 of
complete) Password: 1234567 (7 of 14344391 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.8.10 User: root Password: 1234567 [SUCCESS]
root@kali:~#
```

Gambar 3. 8 Serangan berhasil

Ketika *attacker* berhasil login maka seluruh aktifitas *attacker* pada server honeypot akan direkam sampai sesi *attacker* berakhir. Untuk melihat aktifitas apa saja yang dilakukan oleh *attacker*, dapat dilihat pada web dashboard.

```
root@localhost:~# uname -a
Linux localhost 2.6.26-2-686 #1 SMP Wed Nov 4 20:45:37 UTC 2009 i686 GNU/Linux
root@localhost:~# id
uid=0(root) gid=0(root) groups=0(root)
root@localhost:~# ls
index.html
root@localhost:~# wget http://facebook.com/ -o facebook.html
--2018-08-14 15:58:18-- http://facebook.com/
Connecting to facebook.com:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html, charset=utf-8]
Saving to: ./root/index.html

100%[=====] 0 53K/s eta 5s

2018-08-14 15:58:25 (53 KB/s) - ./root/index.html' saved [402438/0]
root@localhost:~#
```

Gambar 3. 9 Interaksi *attacker* dengan server honeypot

Gambar 3. 10 Log Serangan Yang Berhasil

Gambar 3. 11 Rekaman Aktifitas *Attacker* Pada Terminal

Sampai sini *attacker* tidak dapat melakukan kegiatan lebih dalam lagi, karena server honeypot ini merupakan server imitasi dari server utama. Terlebih lagi petugas administrator dapat mengetahui motif dari *attacker* tersebut.

#### iv. Hasil Pengujian Tahap Keempat.

Pada pengujian tahap pertama ini akan dilakukan kegiatan preventif honeypot yaitu dengan melakukan blocking terhadap IP Address yang mencoba melakukan serangan *brute-force*. Untuk melakukan pengujian ini caranya sama seperti pada pengujian tahap kedua, Namun perlu diaktifkan IDPS pada *honeypot*. Dengan perintah berikut:

```
sudo snort -A console -Q -u snort -g snort -c
/etc/snort/snort.conf -i wlan0:wlx7cdd906959e0 -N
```

Selanjutnya adalah melakukan serangan *brute-force* kembali. IDPS akan melakukan blocking ketika terdeteksi ada 3 koneksi yang terhubung (established) dengan server honeypot.

```
2018-08-14 15:58:25 [**] [111000021] TCP scan detected on port 22 [**] (Classification: Attempted Informa
tion)
2018-08-14 15:58:27 [**] [111000021] TCP scan detected on port 22 [**] (Classification: Attempted Informa
tion)
2018-08-14 15:58:27 [**] [111000021] TCP scan detected on port 22 [**] (Classification: Attempted Informa
tion)
2018-08-14 15:58:27 [**] [111000021] SSH brute force attempt [**] (Classification: Misc activity) [**]
2018-08-14 15:58:27 [**] [111000021] SSH brute force attempt [**] (Classification: Misc activity) [**]
```

Gambar 3. 12 Blok serangan *brute-force*

Pemblokiran yang dilakukan oleh snort adalah menahan paket yang datang selanjutnya sampai proses *brute-force* dihentikan. Sedangkan salah satu fungsi kelebihan honeypot kippo sendiri adalah dapat mengumpulkan password-password yang diterimanya saat *attacker* mencoba login.

Dengan adanya pemblokiran ini dapat membuat *attacker* merasa yakin bahwa server yang diserang adalah server utama, karena server honeypot memiliki IDPS seperti pada server umumnya.

## IV. PENUTUP SIMPULAN

Berdasarkan Implementasi Sistem Keamanan Server Menggunakan Honeypot Dan Raspberry Pi Terhadap *Attacker* yang telah di buat dan dilakukan pengujian maka dapat diambil simpulan sebagai berikut:

1. Setelah di lakukan pengujian pada aplikasi yang di buat, hasil yang didapatkan sesuai dengan yang di harapkan, bahwa untuk membuat sistem Honeypot dan IDPS tidak diperlukan biaya yang mahal dan dapat diimplementasikan pada jaringan internal.
2. Kippo dapat berfungsi untuk mengumpulkan password yang diterima ketika ada percobaan login terhadap server utama.
3. Menggunakan aplikasi Snort sebagai IDPS merupakan cara yang efektif dalam menghemat resource.

**DAFTAR PUSTAKA**

- [1]Wahono, Setio. Alif Subardono. 2017. Analisis dan Implementasi Honeypot Terdistribusi sebagai Deteksi Aktivitas Blackhat pada Jaringan, ISSN: 2338 – 0276, Universitas Gajah Mada, Yogyakarta, 5 Agustus 2017.
- [2]Tokopedia.com, Harga Raspberry Pi, 2018  
<https://www.tokopedia.com/hot/raspberry-pi?keyword=raspberrypi>, 8 Agustus 2018.
- [3]Bhineka.com, Harga Firewall, 2018  
<https://www.bhinneka.com/jual-firewall/3454272>, 8 Agustus 2018.
- [4]Putra, Agfianto Eko, 2012. Mengenal Raspberry Pi.  
<http://agfi.staff.ugm.ac.id/blog/index.php/2012/08/mengenal-raspberry-pi/>, 19 Maret 2018.
- [5]A. Wahyuningsih, 2017. Mengenal Honeypot Sebagai Tools Untuk Menjebak Hacker, Netsec.ID.  
<https://netsec.id/honeypot/>, 25 Maret 2018.
- [6]Wu, Tzeyoung Max, 2009. “Intrusion Detection Systems”. Information Assurance Tools Report, Sixth Edition.
- [7]Kusumawati, Monika, 2010. Implementasi IDS (Intrusion Detection System) serta Monitoring Jaringan dengan Interface Web Berbasis Base Pada Keamanan Jaringan. Skripsi, Universitas Indonesia, Fakultas Teknik, Program Teknik Komputer.
- [8]E. K. Dewi. Model Rancangan Keamanan Jaringan Dengan Menggunakan Proses Forensik. Jurnal Maklumatika. [Online] vol. 2, p. 34.  
<http://maklumatika.uniat.ac.id/post-152-volume-3-no-2-januari-2017.html>, 7 Agustus 2018.
- [9]Kristiawan, Yogi. 2017. Perancangan Dan Implementasi Rule Based Dictionary Attack Pada Fuzzer WFUZZ Untuk Menguji Kerentanan Aplikasi Web. Tesis, Institut Teknologi Bandung, Program Studi Magister Teknik Elektro.
- [10]Y, Chrysanthou. 2013. Modern Password Cracking: A hands-on approach to creating an optimised and versatile attack. Tesis, University of London, Program Magister.
- [11]OWASP, 2011. Testing for Brute Force (OWASP-AT-004),  
[https://www.owasp.org/index.php/Testing\\_for\\_Brute\\_Force\\_\(OWASP-AT-004\)](https://www.owasp.org/index.php/Testing_for_Brute_Force_(OWASP-AT-004)), 29 Juni 2018.
- [12]Muller, Andrew, 2014. Testing for Weak Password Policy, OWASP.  
[https://www.owasp.org/index.php/Testing\\_for\\_Weak\\_password\\_policy\\_\(OTG-AUTHN-007\)](https://www.owasp.org/index.php/Testing_for_Weak_password_policy_(OTG-AUTHN-007)), 30 Juni 2018.