IMPLEMENTASI *HONEYPOT DIONAEA* UNTUK MENDETEKSI *MALWARE* MENGGUNAKAN *RASPBERRY PI*

SKRIPSI

Oleh:
Jacksen Merson Lim
150210225

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM
2019

IMPLEMENTASI *HONEYPOT DIONAEA* UNTUK MENDETEKSI *MALWARE* MENGGUNAKAN *RASPBERRY PI*

SKRIPSI

Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana

Oleh:
Jacksen Merson Lim
150210225

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM

2019

SURAT PERNYATAAN

Dengan ini saya menyatakan bahwa:

1. Skripsi ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (sarjana, dan/atau magister), baik di Universitas Putera Batam maupun di perguruan tinggi lain.
2. Skripsi ini adalah murni gagasan, rumusan, dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing.
3. Dalam skripsi ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di perguruan tinggi.

Batam, 25 Januari 2019

Yang membuat pernyataan,

Jacksen Merson Lim
150210225

IMPLEMENTASI *HONEYPOT DIONAEA* UNTUK MENDETEKSI *MALWARE* MENGGUNAKAN *RASPBERRY PI*

Oleh
Jacksen Merson Lim
150210225

SKRIPSI

Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana

Telah disetujui oleh Pembimbing pada tanggal
seperti tertera d bawah ini

Batam, 2 Februari 2019

Arif Rahman Hakim, S.Kom., M.Kom.
Pembimbing

ABSTRAK

Teknologi internet memungkinkan banyaknya pengguna komputer yang terhubung satu sama lain. Biaya yang lebih murah dan akses yang lebih mudah membuat penggunaan internet semakin banyak. Dalam sisi lain, hal ini juga membuat banyak pengguna internet untuk menerima serangan berbahaya berupa *malware*, terutama dalam jaringan nirkabel. Kurangnya pemantauan jaringan dapat meningkatkan resiko serangan. Salah satu solusi untuk dapat mendeteksi serangan *malware* pada jaringan adalah menggunakan *honeypot Dionaea* yang terpasang pada *Raspberry Pi*. Sistem *honeypot* merupakan sistem yang sengaja dirancang untuk menerima serangan, sehingga sistem ini membuka *port* pada *Raspberry Pi* ke jaringan. Namun, ini juga menyebabkan sistem *honeypot* berpotensi menjadi wadah untuk menyerang komputer lain pada jaringan yang sama. Untuk menghindari hal ini, penggunaan *router* yang dapat membuat dua SSID dengan fitur *Guest Network* bisa digunakan pada implementasi *honeypot* ke jaringan. Agar memudahkan akses laporan serangan, dilakukan instalasi sistem *Modern Honeypot Network* yang berperan sebagai *server* dan mempunyai antarmuka untuk menunjukan hasil serangan dari luar ke sistem *honeypot*. Setelah lima puluh simulasi serangan dilakukan pada jaringan yang terpisah, *Raspberry Pi* sebagai *honeypot Dionaea* mempunyai tingkat keberhasilan sebesar 85.33% dan mampu mencatat dan menyimpan serangan *malware* dan eksploitasi program berupa *file* yang bisa diakses dari *Raspberry Pi*. *Server* MHN juga membantu memudahkan pembacaan *log* serangan ke *honeypot* dengan menunjukan alamat IP penyerang, waktu, dan *port* yang diserang.

Kata kunci: Jaringan, *Honeypot, Dionaea, Raspberry Pi, Modern Honeypot Network*

ABSTRACT

The technology of the internet allows more users to connect one and another. Lower costs and easy access mean even more people access the internet. On the other hand, this also allows users to receive attacks from the internet such as malware, especially on wireless networks. The lack of network monitoring can increase the risk of such attacks. One of the solutions proposed to detect malware attacks in a network is to use Raspberry Pi with Dionaea honeypot installed in it. Honeypots are intentionally designed to receive attacks by exposing the ports to the network. However, this also causes the honeypot to be potentially dangerous as it can be used to distribute the attacks to other computers in the same network. To minimize the risk, a router with the capability of dual SSID through Guest Network feature can be used to isolate the honeypot system from the rest of the network. For easier access to the attack report, Modern Honeypot Network is installed that acts as a server for the honeypot and it does have graphical user interface that shows the attacks to the honeypot. After fifty simulated attacks are done on an isolated network, the Raspberry Pi, as a honeypot, has a success rate of 85.33%, and is proven to be capable on logging and saving the malware and exploit attacks, which can be accessed through the Raspberry Pi itself. The MHN server also shows the attacker's IP address, the time of the attack, and the attacked port, which makes the attack log easier to read and understand.

Keywords: ***Network, Honeypot, Dionaea, Raspberry Pi, Modern Honeypot Network***

KATA PENGANTAR

Penulis menghaturkan puji syukur kepada Tuhan Yang Maha Esa yang telah melimpahkan segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Program Studi Teknik Informatika Universitas Putera Batam. Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, penulis menyadari pula bahwa skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Rektor Universitas Putera Batam.
2. Ketua Program Studi Teknik Informatika Universitas Putera Batam.
3. Arif Rahman Hakim, S.Kom., M.Kom., selaku pembimbing Skripsi pada Program Studi Teknik Informatika Universitas Putera Batam.
4. Dosen dan Staff Universitas Putera Batam.
5. Keluarga penulis yang telah memberikan dukungan dan pengertian kepada penulis.
6. Teman-teman seperjuangan yang juga selalu memberikan motivasi baik berupa *sharing* pendapat hal-hal lainnya dalam rangka pembuatan penelitian ini.

7. Serta semua pihak yang tak dapat peneliti sebutkan satu persatu yang telah membantu dalam penyusunan proposal penelitian ini.

Semoga Tuhan Yang Maha Esa membalas kebaikan dan selalu mencurahkan hidayah serta taufik-Nya, Amin.

Batam, Januari 2019

Penulis

DAFTAR ISI

Halaman

DAFTAR TABEL

DAFTAR GAMBAR

Halaman

DAFTAR SINGKATAN

1. OSI (*Open System Interconnection*)
2. LLC (*Logical Link Control*)
3. MAC (*Medium Access Control*)
4. SIM (*Subscriber Identity Module*)
5. IP (*Internet Protocol*)
6. MHN (*Modern Honeypot Network*)
7. ISP (*Internet Service Provider*)
8. DHCP (*Dynamic Host Configuration Protocol*)
9. SSID (*Service Set Identifier*)
10. FTP (*File Transfer Protocol*)
11. SMB (*Service Message Block*)

DAFTAR LAMPIRAN