# 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:

- 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.
- 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.
- 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.
- Keluarga penulis yang telah memberikan dukungan dan pengertian kepada penulis.
- 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

HALAN	MAN SAMPUL DEPAN
HALAN	MAN JUDUL ii
HALAN	MAN PERNYATAANiii
ABSTR	<b>VAK</b> v
ABSTR	<i>ACT</i> vi
KATA	PENGANTARvii
DAFTA	AR ISI ix
DAFTA	<b>AR TABEL</b> xi
DAFTA	AR GAMBARxii
DAFTA	AR SINGKATAN xv
DAFTA	AR LAMPIRAN xvi
BAB I	PENDAHULUAN1
1.1	Latar Belakang 1
1.2	Identifikasi Masalah
1.3	Batasan Masalah
1.4	Rumusan Masalah 4
1.5	Tujuan Penelitian
1.6	Manfaat
BAB II	KAJIAN PUSTAKA
2.1	Teori Dasar
2.2	Teori Khusus 16
2.3	Tools
2.4	Penelitian Terdahulu
2.5	Kerangka Pemikiran
BAB II	I METODE PENELITIAN

3.1	Desain Penelitian	
3.2	Analisis Jaringan Lama/yang Sedang Berjalan	
3.3	Rancangan Jaringan yang Dibangun/Diusulkan	
3.4	Lokasi dan Jadwal Penelitian	
BAB IV	V HASIL DAN PEMBAHASAN	
4.1	Hasil Penelitian	
4.2	Pembahasan	
BAB V	KESIMPULAN DAN SARAN	
5.1	Simpulan	
5.2	Saran	
DAFT	AR PUSTAKA	

DAFTAR RIWAYAT HIDUP	78
LAMPIRAN	80

### DAFTAR TABEL

Tabel 3.1 Perangkat Jaringan Lama	
Tabel 3.2 Perangkat lunak yang digunakan di jaringan lama	
Tabel 3.3 Perangkat keras pada jaringan baru	
Tabel 3.4 Perangkat lunak yang akan digunakan di jaringan baru	
Tabel 3.5 Jadwal Penelitian	42
Tabel 4.1 Uji keberhasilan honeypot dalam merekam serangan	71

## DAFTAR GAMBAR

#### Halaman

Gambar 2.1 Jaringan PAN (Personal Area Network)	9
Gambar 2.2 Jaringan LAN (Local Area Network)	9
Gambar 2.3 Jaringan MAN (Metropolitan Area Network)	10
Gambar 2.4 Jaringan WAN (Wide Area Network)	10
Gambar 2.5 Desain jaringan Peer to Peer	12
Gambar 2.6 Model Lapisan OSI	13
Gambar 2.7 Diagram Low interaction honeypot	19
Gambar 2.8 Diagram high interaction honeypot	20
Gambar 2.9 Raspberry Pi 3 Model B+	23
Gambar 2.10 Arsitektur dari server Modern Honeypot Network	24
Gambar 2.11 Kerangka Pemikiran	28
Gambar 3.1 Desain Penelitian	31
Gambar 3.2 Topologi Jaringan Lama	33
Gambar 3.3 Topologi jaringan baru	35
Gambar 3.4 Flowchart implementasi honeypot dan simulasi serangan	41
Gambar 4.1 Pengaktifan router TL-MR6400	43
Gambar 4.2 Akses pengaturan router melalui laptop	44
Gambar 4.3 Aktivasi fitur Guest Network	44
Gambar 4.4 Merubah alamat IP untuk server DHCP	45
Gambar 4.5 Pengaturan Local Management	45
Gambar 4.6 Login Wi-Fi pada Raspberry Pi	46
Gambar 4.7 Uji ping ke router dan IP Google	46
Gambar 4.8 Uji akses router pada komputer didalam SSID Guest Network	47
Gambar 4.9 Uji ping pada perangkat diluar SSID Guest Network	47
Gambar 4.10 Instalasi Git	48
Gambar 4.11 Instalasi MHN	48
Gambar 4.12 Instalasi script MHN	48
Gambar 4.13 Konfigurasi Instalasi MHN	49
Gambar 4.14 Pendaftaran superuser pada instalasi MHN	50
Gambar 4.15 Konfigurasi mail pada MHN	50
Gambar 4.16 Request integrasi Splunk	51
Gambar 4.17 Request Instalasi ELK	51
Gambar 4.18 Instalasi MHN sukses	51

Gambar 4.19 Cek status MHN	52
Gambar 4.20 Direktori konfigurasi server MHN	52
Gambar 4.21 Perintah melakukan edit file	52
Gambar 4.22 Pencarian URL Server MHN	53
Gambar 4.23 Pengaturan alamat IP server MHN	53
Gambar 4.24 Restart ulang service mhn-uwsgi	54
Gambar 4.25 Cek status MHN	54
Gambar 4.26 Tampilan antarmuka server MHN	54
Gambar 4.27 Login ke server MHN	55
Gambar 4.28 Tampilan awal server MHN	55
Gambar 4.29 Instalasi OS Raspbian dengan NOOBS	56
Gambar 4.30 Tampilan desktop Raspbian	56
Gambar 4.31 Perintah konfigurasi Raspberry Pi	57
Gambar 4.32 Tampilan awal Raspberry Pi Software Configuration tool	57
Gambar 4.33 Pembukaan port SSH pada Raspberry Pi	58
Gambar 4.34 Tampilan Deploy pada server MHN	58
Gambar 4.35 Perintah script untuk Raspberry Pi	59
Gambar 4.36 Script instalasi honeypot Dionaea pada Raspberry Pi	59
Gambar 4.37 Perbaikan script instalasi honeypot Dionaea	60
Gambar 4.38 SSH ke Raspberry Pi	60
Gambar 4.39 Instalasi sistem honeypot Dionaea	61
Gambar 4.40 Cek status Dionaea	61
Gambar 4.41 Tampilan sensor honeypot pada server MHN	62
Gambar 4.42 Port Scanning ke sistem honeypot	62
Gambar 4.43 Hasil port scanning ke sistem honeypot	62
Gambar 4.44 Log dari uji port scanning	63
Gambar 4.45 Tampilan console dari Metasploit	64
Gambar 4.46 Command untuk pencarian server FTP	64
Gambar 4.47 Scanning pencarian server FTP	64
Gambar 4.48 Laporan serangan/scanning port 21	65
Gambar 4.49 Scanning port 445	66
Gambar 4.50 Eksploitasi MS17-010 dengan Metasploit	66
Gambar 4.51 Pengaturan serangan eksploitasi MS17-010	66
Gambar 4.52 Log serangan eksploitasi MS17-010	67
Gambar 4.53 Laporan serangan eksploitasi MS17-010	67
Gambar 4.54 Inisialisasi serangan eksploitasi MS10-061	68
Gambar 4.55 Pengaturan serangan eksploitasi MS10-061	68
Gambar 4.56 Log penyerangan dengan Metasploit	68
Gambar 4.57 Laporan serangan MS10-061 ke honeypot	69
Gambar 4.58 Payload serangan ke honeypot	69

Gambar 4.59 Lokasi file serangan pada Raspberry Pi	70
Gambar 4.60 Halaman utama VirusTotal	70
Gambar 4.61 Hasil scanning dari VirusTotal	71

### 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

- 1. Foto Penelitian
- 2. Script, Command, dan Log Konfigurasi