

**IMPLEMENTASI *HONEYPOT* PADA *CLOUD COMPUTING* UNTUK
IDENTIFIKASI SERANGAN *MALWARE***

SKRIPSI



disusun oleh

Muhammad Muallif Nashiruddin

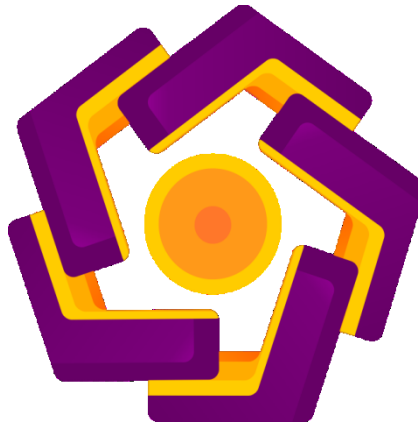
13.11.6878

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2017**

**IMPLEMENTASI *HONEYPOT* PADA *CLOUD COMPUTING* UNTUK
IDENTIFIKASI SERANGAN *MALWARE***

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Muhammad Muallif Nashiruddin

13.11.6878

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2017**

PERSETUJUAN

SKRIPSI

IMPLEMENTASI *HONEY*POT PADA *CLOUD* COMPUTING UNTUK IDENTIFIKASI SERANGAN *MALWARE*

yang dipersiapkan dan disusun oleh

Muhammad Muallif Nashiruddin

13.11.6878

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 8 Maret 2017

Dosen Pembimbing,

Armadvah Amborowati, S.Kom, M. Eng.

NIK. 190302063

PENGESAHAN

SKRIPSI

**IMPLEMENTASI *HONEY*POT PADA *CLOUD* COMPUTING UNTUK
IDENTIFIKASI SERANGAN *MALWARE***

yang dipersiapkan dan disusun oleh

Muhammad Muallif Nashiruddin

13.11.6878

telah dipertahankan di depan Dewan Penguji
pada tanggal 20 April 2017

Susunan Dewan Penguji

Nama Penguji

Arif Dwi Laksito, M.Kom.
NIK. 190302150

Barka Satva, M.Kom.
NIK. 190302126

Windha Mega Pradnya D, M.Kom.
NIK. 190302185

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
tanggal 22 April 2017



DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si, M.T.
NIK. 190302038

HALAMAN PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 20 April 2017



Muhammad Muallif Nashiruddin
NIM. 13.11.6878

MOTTO

"KEBIASAAN ITU MENUNJUKKAN KARAKTER DAN DAPAT MERUBAH SIFAT"

~Muhammad Muallif Nashiruddin~

*"JIKA KAMU **SEDANG** MANCARI IDE KREATIF, KELUARLAH DAN BERJALAN KAKI. MALAIKAT **BERBISIK** KEPADA MANUSIA, KETIKA DIA PERGI UNTUK BERJALAN KAKI"*

~Raymond Inmon~

"MENDAKILAH KETIKA KAMU LELAH MENJALANI HIDUP, PUNCAK DAN SEGENAP PEMANDANGANNYA AKAN MENGHAPUS BEBAN YANG SAAT ITU KAMU PIKUL"

~The A~

HALAMAN PERSEMBAHAN

Puji syukur kami panjatkan kepada Allah SWT yang telah memberikan kesempatan, kekuatan dan kesehatan untuk bisa menyelesaikan skripsi yang berjudul “Implementasi *Honeypot* Pada *Cloud Computing* Untuk Identifikasi Serangan *Malware*”.

Tidak lupa Sholawat serta Salam selalu tercurahkan kepada Nabi Muhammad SAW. Beliau adalah Sang Teladan Umat, panutan yang haq untuk senantiasa diteladani.

Kelancaran penulisan skripsi ini selain atas limpahan karunia Allah SWT, juga berkat dukungan pembimbing, orang tua dan kawan-kawan. Untuk itu penulis ingin mengucapkan rasa terima kasih kepada :

1. Prof. Dr. M. Suyanto, M.M. selaku rektor Universitas Amikom Yogyakarta.
2. Krisnawati, S.Si, M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
3. Sudarmawan, M.T. selaku Ketua Program Studi S1 Informatika, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta.
4. Armadyah Amborowati, S.Kom, M. Eng. selaku Dosen Pembimbing Skripsi.
5. Seluruh Dosen Universitas Amikom Yogyakarta.
6. Almarhum Bapak dan Ibunda tercinta serta saudara-saudara saya.
7. Seluruh teman-teman kelas 13 S1 Teknik Informatika 02 yang telah memberi semangat serta berjuang bersama.
8. Seluruh teman-teman kontrakan Pace (kobra), Heru, Heri, Udin, Alan, dan Wahyu. Terimakasih kalian telah menemani selama menuntut ilmu di Yogyakarta.
9. Seluruh teman-teman yang memberi tumpangan saya tidur selama menyelesaikan ujian skripsi. Khususnya untuk kontrakan Haji Sholeh dan Bagrek.
10. Seluruh teman-teman yang biasa ikut saya mendaki gunung serta *camping* di hutan belantara. Terimakasih sudah mau saya aniaya di alam bebas.

11. Seluruh teman-teman yang biasa menemani saya ngopi di *basement 2* kampus Universitas Amikom Yogyakarta. Jangan sampai jadwal kuliahmu mengganggu jadwal ngopimu.
12. Seluruh *shifu* saya di dunia *underground* yang tidak bisa saya sebutkan nama atau *nickname*-nya di sini.
13. Dan semua teman-teman atau pihak-pihak yang tidak bisa penulis sebutkan satu persatu. Terima kasih atas semuanya.

Demikianlah ucapan terima kasih saya selaku penulis. Semoga Allah SWT senantiasa memberikan balasan terbaik atas jasa-jasa yang telah diberikan kalian. Baik di dunia maupun di akhirat nanti. Aamiin.

Yogyakarta, 20 April 2017

KATA PENGANTAR

Puji syukur Alhamdulillah penulis panjatkan kehadiran Allah SWT yang telah memberikan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi dengan judul “Implementasi *Honeypot* Pada *Cloud Computing* Untuk Identifikasi Serangan *Malware*”.

Penulisan skripsi ini diajukan untuk memenuhi salah satu syarat kelulusan dalam jenjang perkuliahan Strata I Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Amikom Yogyakarta. Dalam penulisan skripsi ini tidak lepas dari hambatan dan kesulitan, namun berkat bimbingan, bantuan, nasihat dan saran serta kerjasama dari berbagai pihak, khususnya pembimbing, segala hambatan tersebut akhirnya dapat diatasi dengan baik.

Dalam penulisan skripsi ini tentunya tidak lepas dari kekurangan, baik aspek kualitas maupun aspek kuantitas dari materi penelitian yang disajikan. Semua ini didasarkan dari keterbatasan yang dimiliki penulis.

Penulis menyadari bahwa skripsi ini jauh dari sempurna sehingga penulis membutuhkan kritik dan saran yang bersifat membangun untuk kemajuan pendidikan di masa yang akan datang.

Terakhir semoga segala bantuan yang telah diberikan, sebagai amal soleh serta senantiasa mendapat Ridho Allah SWT. Sehingga pada akhirnya skripsi ini dapat bermanfaat bagi kemajuan dunia IT.

Yogyakarta, 20 April 2017

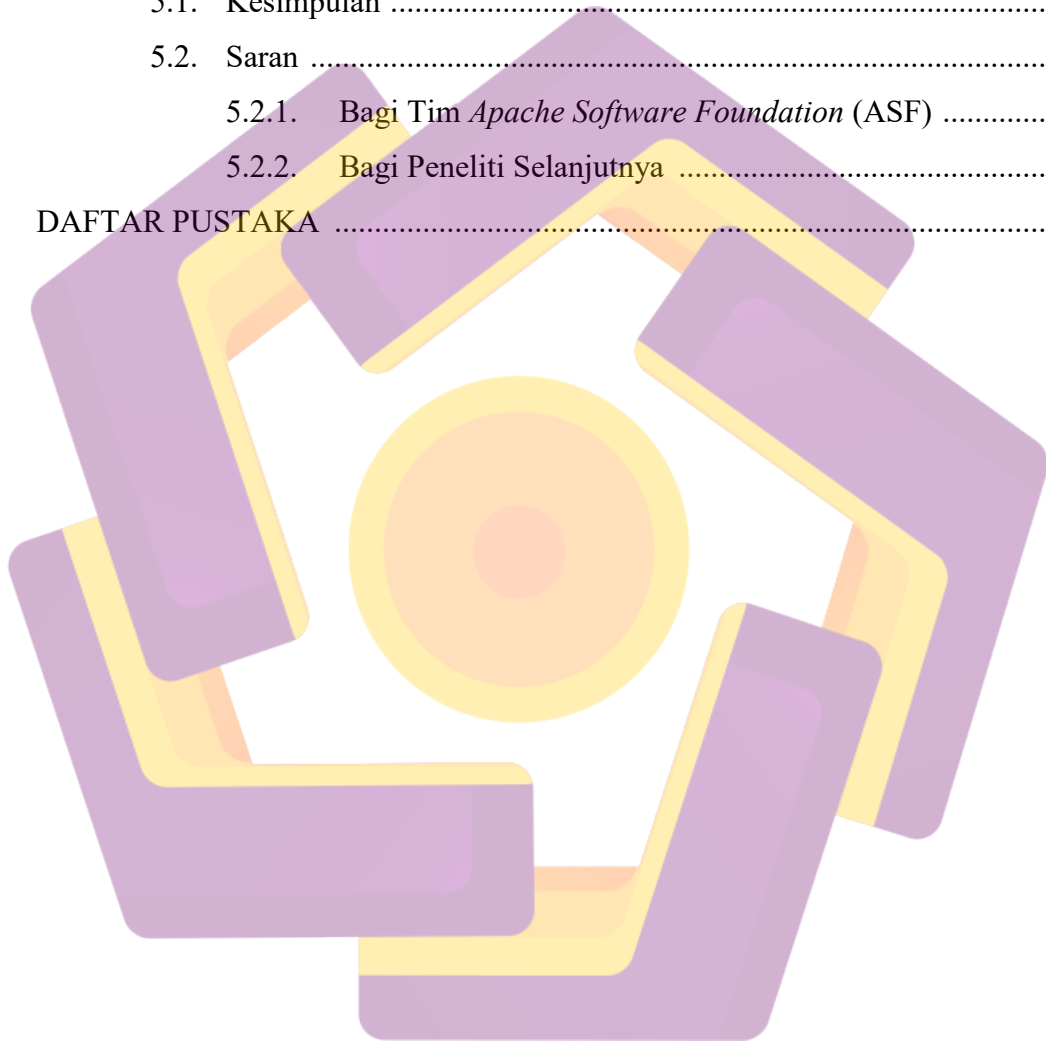
Penulis

DAFTAR ISI

<i>COVER</i>	i
HALAMAN JUDUL	ii
HALAMAN PERSETUJUAN	iii
HALAMAN PENGESAHAN	iv
HALAMAN PERNYATAAN	v
<i>MOTTO</i>	vi
HALAMAN PERSEMBAHAN	vii
KATA PENGANTAR	ix
DAFTAR ISI	x
DAFTAR TABLE	xiii
DAFTAR GAMBAR	xiv
INTISARI	xvi
<i>ABSTRACT</i>	xvii
BAB I PENDAHULUAN	1
1.1. Latar Belakan Masalah	1
1.2. Rumusan Masalah	2
1.3. Batasan Masalah	2
1.4. Maksud dan Tujuan Penelitian	3
1.5. Manfaat Penelitian	3
1.6. Sistematika Penulisan	4
BAB II LANDASAN TEORI	5
2.1. Tinjauan Pustaka	5
2.2. Dasar Teori	6
2.2.1. Jaringan Komputer	6
2.2.2. Topologi Jaringan Komputer	19
2.2.2.1. Topologi <i>Bus</i>	19
2.2.2.2. Topologi <i>Ring</i>	20
2.2.2.3. Topologi <i>Star</i>	21
2.2.2.4. Topologi <i>Daisy-Chain (Linear)</i>	22

2.2.2.5.	Topologi <i>Tree/Hierarchical</i>	23
2.2.2.6.	Topologi <i>Mesh dan Full Connected</i>	23
2.2.2.7.	Topologi <i>Hybrid</i>	24
2.2.3.	Keamanan Komputer	24
2.2.4.	Virtualisasi	27
2.2.5.	<i>Cloud Computing</i>	29
2.2.6.	<i>Apache CloudStack</i>	30
2.2.7.	<i>Malware</i>	31
2.2.8.	<i>Honeypot</i>	33
2.2.9.	<i>Dionaea</i>	37
2.2.10.	<i>ConfigServer Security & Firewall (CSF)</i>	38
2.2.11.	<i>Webmin</i>	39
BAB III METODE PENELITIAN		40
3.1.	Pendekatan Penelitian	40
3.2.	Teknik Pengumpulan Data	40
3.2.1.	Studi Literatur	40
3.2.2.	Observasi Eksperimental	41
3.3.	Alat dan Bahan Penelitian	41
3.3.1.	Kebutuhan perangkat keras (<i>hardware</i>)	41
3.3.2.	Kebutuhan Perangkat Lunak (<i>software</i>)	41
3.4.	Alur Penelitian	42
3.4.1.	Perancangan Sistem dan Jaringan	42
3.4.2.	Pengujian Sistem	43
BAB IV HASIL DAN PEMBAHASAN		45
4.1.	Implementasi Perancangan Sistem	45
4.1.1.	Instalasi <i>VMware vSphere Hypervisor 6.0</i>	45
4.1.2.	Instalasi VM Sistem Operasi <i>CentOS7</i>	48
4.1.3.	Instalasi <i>Apache CloudStack 4.9</i>	50
4.1.4.	Konfigurasi <i>Apache CloudStack</i>	59
4.1.5.	Konfigurasi <i>CloudStack Management</i>	66
4.1.6.	Instalasi dan Konfigurasi <i>Honeypot Dionaea</i>	68

4.1.7.	Instalasi dan Konfigurasi CSF	73
4.1.8.	Konfigurasi <i>Firewall</i>	77
4.2.	Pengujian <i>Penetration Testing</i>	78
4.3.	Pengujian <i>Performance Testing</i>	82
BAB V	PENUTUP	85
5.1.	Kesimpulan	85
5.2.	Saran	85
5.2.1.	Bagi Tim <i>Apache Software Foundation</i> (ASF)	86
5.2.2.	Bagi Peneliti Selanjutnya	86
DAFTAR PUSTAKA	87



DAFTAR TABEL

Tabel 2.1 Perbandingan Penelitian	5
---	---



DAFTAR GAMBAR

Gambar 2.1	Jaringan <i>Local Area Network</i>	9
Gambar 2.2	Jaringan <i>Metropolitan Area Network</i>	10
Gambar 2.3	Jaringan <i>Wide Area Network</i>	11
Gambar 2.4	Jaringan Terpusat	12
Gambar 2.5	Jaringan Terdistribusi	13
Gambar 2.6	Jaringan Kabel	15
Gambar 2.7	Jaringan Tanpa Kabel	16
Gambar 2.8	Jaringan <i>Client to Server</i>	17
Gambar 2.9	Jaringan <i>Peer to Peer</i>	18
Gambar 2.10	Topologi <i>Bus</i>	19
Gambar 2.11	Topologi <i>Ring</i>	21
Gambar 2.12	Topologi <i>Star</i>	22
Gambar 2.13	Topologi <i>Daisy Chain</i>	22
Gambar 2.14	Topologi <i>Tree/Hierarchical</i>	23
Gambar 2.15	Topologi <i>Mesh (full connected topology)</i>	23
Gambar 2.16	Beberapa jenis topologi	24
Gambar 2.17	Virtualisasi Komputer	29
Gambar 3.1	Topologi Jaringan Penelitian	43
Gambar 4.1	Instalasi <i>VMware vSphere</i>	45
Gambar 4.2	Instalasi <i>VMware vSphere</i> selesai	46
Gambar 4.3	Tampilan <i>VMware vSphere</i>	46
Gambar 4.4	Tampilan <i>host VMware vSphere</i>	47
Gambar 4.5	Tampilan <i>login VMware vSphere Client</i>	47
Gambar 4.6	Tampilan manajemen <i>VMware vSphere</i>	48
Gambar 4.7	<i>Datastore VMware vSphere</i>	48
Gambar 4.8	<i>File datastore VMware vSphere</i>	49
Gambar 4.9	Konfigurasi <i>virtual mesin</i>	49
Gambar 4.10	Instalasi sistem operasi <i>CentOS 7</i>	50
Gambar 4.11	Remote sistem operasi <i>CentOS 7</i>	51
Gambar 4.12	Instalasi <i>CloudStack Management</i> selesai	57

Gambar 4.13	Tampilan <i>User Interface CloudStack</i>	60
Gambar 4.14	<i>Splash screen</i> informasi <i>CloudStack</i>	60
Gambar 4.15	Mengganti <i>password login</i>	61
Gambar 4.16	Menambah <i>zone</i>	61
Gambar 4.17	Menambah <i>Pod</i>	62
Gambar 4.18	Menentukan <i>guest network</i>	62
Gambar 4.19	Menambah <i>Cluster</i>	63
Gambar 4.20	Menambah <i>Host</i>	63
Gambar 4.21	Menambah <i>Primary Storage</i>	64
Gambar 4.22	Menambah <i>Secondary Storage</i>	64
Gambar 4.23	Memulai <i>Setup Instalasi CloudStack</i>	65
Gambar 4.24	<i>Setup CloudStack</i>	65
Gambar 4.25	<i>Setup CloudStack</i> selesai	65
Gambar 4.26	<i>Dashboard CloudStack Management</i>	66
Gambar 4.27	Membuat virtual mesin di <i>CloudStack</i>	67
Gambar 4.28	Instalasi <i>Ubuntu Server 14.04</i>	68
Gambar 4.29	<i>Login Webmin</i>	75
Gambar 4.30	<i>Webmin Modules</i>	76
Gambar 4.31	Instal modul CSF <i>Webmin</i>	76
Gambar 4.32	<i>Data Analisis Malware</i>	81
Gambar 4.33	<i>Metadata Malware</i>	82
Gambar 4.34	<i>Resource Server</i>	83
Gambar 4.35	<i>Resource Server Stress Test</i>	84

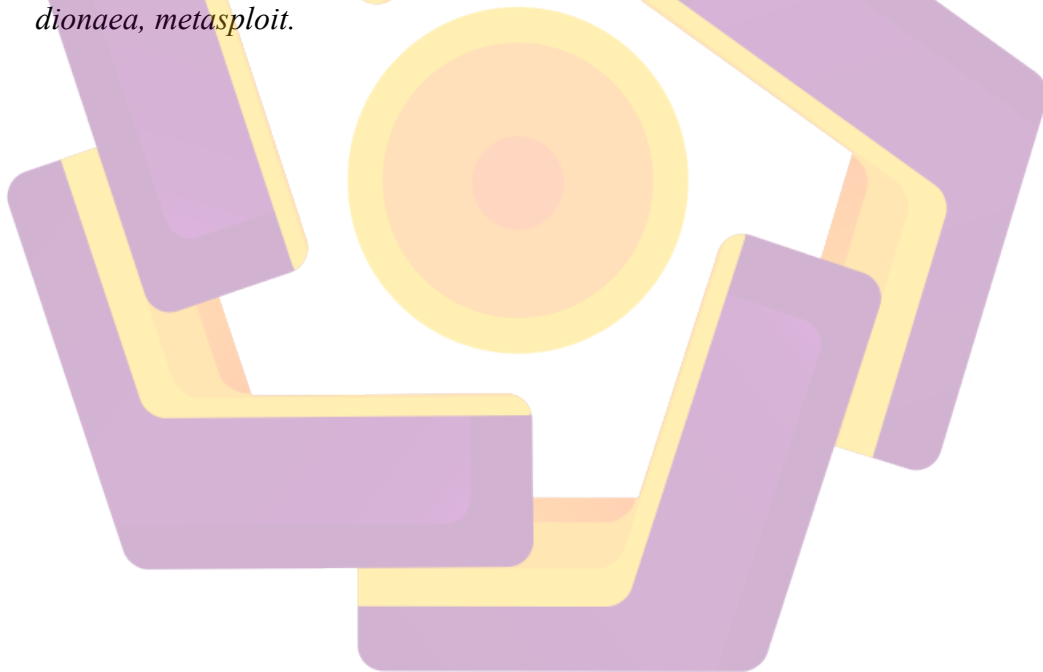
INTISARI

Cloud computing (komputasi awan) merupakan salah satu teknologi yang saat ini sedang banyak dikembangkan dan digunakan oleh perusahaan-perusahaan yang membutuhkan sumber daya komputasi yang besar dan efisien. Seiring perkembangan teknologi tersebut maka ancaman keamanan pada layanan *cloud computing* semakin meningkat.

Ancaman keamanan yang paling sering digunakan oleh penyerang adalah *malware*. Salah satu tindakan pengamanan yang dapat dilakukan yaitu dengan menggunakan *honeypot*. *Honeypot* merupakan salah satu teknologi atau sistem keamanan yang dapat memenuhi ketiga konsep keamanan teknologi informasi yaitu pencegahan (*prevention*), deteksi (*detection*) dan merespon (*respond*).

Honeypot dapat menangkap *malware* yang masuk ke jaringan, serta menangkap informasi mengenai identitas dan aktifitas yang dilakukan oleh penyerang yang kemudian akan digunakan oleh penyedia layanan *cloud computing* dalam meningkatkan sistem pengamanan.

Kata Kunci: *cloud computing, apache cloudstack, CSF, malware, honeypot dionaea, metasploit.*



ABSTRACT

Cloud computing is a technology that is currently developed and used by companies that require large and efficient computational resources. Along with the development of these technologies, the security threat of cloud computing has increased.

Security threats are most often used by attackers is malware. One of the security measures can be implemented is using honeypot. Honeypot is one of technology or security system that can fulfill the three concepts of information technology security: prevention, detection and respond.

Honeypot can capture malware that coming into the network, and capturing information about the identity and activities of the attacker that will be analyzed and used as reference for cloud computing providers to improving the security system.

Keyword: *cloud computing, apache cloudstack, CSF, malware, honeypot dionaea, metasploit.*

