PERANCANGAN DAN ANALISIS KEAMANAN JARINGAN MENGGUNAKAN HONEYPOT UNTUK MENDETEKSI SERANGAN BRUTE FORCE PADA CLOUD COMPUTING

SKRIPSI

disusun oleh

Tomy Prayoga Sukarno

13.11.6842

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

2017

PERANCANGAN DAN ANALISIS KEAMANAN JARINGAN MENGGUNAKAN HONEYPOT UNTUK MENDETEKSI SERANGAN BRUTE FORCE PADA CLOUD COMPUTING

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika

disusun oleh

Tomy Prayoga Sukarno

13.11.6842

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

2017

PERSETUJUAN

SKRIPSI

PERANCANGAN DAN ANALISIS KEAMANAN JARINGAN MENGGUNAKAN HONEYPOT UNTUK MENDETEKSI SERANGAN BRUTE FORCE PADA CLOUD COMPUTING

yang dipersiapkan dan disusun oleh

Tomy Prayoga Sukarno

13.11.6842

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 26 April 2016

Dosen Pembimbing,

Ali Mustopa, M.Kom.
NIK. 190302192

ii

PENGESAHAN

SKRIPSI

PERANCANGAN DAN ANALISIS KEAMANAN JARINGAN MENGGUNAKAN HONEYPOT UNTUK MENDETEKSI SERANGAN BRUTE FORCE PADA CLOUD COMPUTING

yang dipersiapkan dan disusun oleh

Tomy Prayoga Sukarno

13.11.6842

telah dipertahankan di depan Dewan Penguji
pada tanggal 12 Mei 2017

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Bayu Setiaji, M.Kom. **NIK. 190302216**	
Ali Mustopa, M.Kom. **NIK. 190302192**	
Rizqi Sukma Kharisma, M.Kom **NIK. 190302215**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 17 Mei 2017

DEKAN FAKULTAS ILMU KOMPUTER

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

iii

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, 15 Mei 2017

Tomy Prayoga Sukarno

NIM 13.11.6842

MOTTO

"Yesterday I was clever, so I wanted to changed the world. Today I am wise, so I am changing myself."

Jalaludin Rumi

"Man jadda wa jada."

" Barang siapa yang bersungguh-sungguh maka akan mendapatkan hasil."

"If you're good at something never do it for free."

The Joker (The Dark Knight)

"Life is simple, you make choices and you don't look back."

Han (The Fast and the Furious : Tokyo Drift)

PERSEMBAHAN

Alhamdulillah puji syukur kepada Allah SWT, atas rahmat dan hidayah-Nya saya dapat menyelesaikan skripsi ini dengan baik, karya sederhana ini kupersembahkan untuk :

1. Terimakasih kepada Ayahanda Sukarno dan Ibunda Tati Afriantini, dengan kerja keras, doa dan motivasi beliau saya dapat menyelesaikan studi S1 sesuai dengan target.
2. Untuk Adik ku tercinta Nino Cahyo Raino dan Nastiti Dianugraheni. Tetap semangat untuk cita-cita kalian dan selalu patuh dan sayang terhadap orang tua dan taat kepada Allah SWT.
3. Untuk Alm. Nenek dan Datuk yang telah beristirahat dengan tenang. Doa ku selalu untuk kalian.
4. Terimakasih kepada Dwi Cintia Putri, yang tidak pernah lelah dan sabar untuk memberi semangat serta mendukung saya selama ini.
5. Terimakasih untuk teman-teman Bambang Squad, Bang Roni, Mas Denim, Hamdi, Dimas, Mas Arif, Fazri, Mas Wawan, Panji dan Eza telah memberikan semangat dan saran dan wejangan selama ini.
6. Terimakasih untuk teman dan mentor saya Mas Alif dan Irul, tanpa kalian mungkin karya sederhana ini tidak dapat terselesaikan.
7. Terimakasih untuk teman-teman kelas 13-S1TI-02 yang tidak dapat disebutkan satu per satu. Karena kalian semua yang selalu membantu selama studi dan menjadikan motivasi untuk menyelesaikan skripsi ini.

KATA PENGANTAR

Assalamu'alaikum wr. Wb

Puji syukur penulis ucapkan kehadirat Allah SWT yang telah memberikan limpahan rahmat, kemudahan, kelancaran dan hidayah-Nya, terbukti penulis dapat menyelesaikan skripsi ini yang berjudul "Perancangan Dan Analisis Keamanan Jaringan Menggunakan Honeypot Untuk Mendeteksi Serangan Brute Force Pada Cloud Computing" dengan cukup baik walaupun disadari masih banyak sekali kekurangan yang itu semua tidak lepas karena keterbatasan penulis. Tidak lupa sholawat serta salam selalu dicurahkan kepada nabi besar dan rosul junjungan kita Rosulullah Muhammad SAW yang telah mengubah dari zaman kebodohan ke zaman yang penuh dengan keislaman.

Skripsi ini merupakan salah satu bentuk persyaratan kelulusan jenjang Program Strata satu (S1) Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta.

Dalam pembuatan skripsi ini, tentu saja penulis mendapat banyak bantuan dari berbagai pihak, oleh karena itu penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Bapak Prof. Dr. M. Suyanto, MM., selaku Rektor Univeraitas AMIKOM Yogyakarta.
2. Bapak Sudarmawan, MT., selaku Ketua Program Studi Strata 1 Informatika Universitas AMIKOM Yogyakarta.
3. Ibu Krisnawati S.Si, M.T., selaku Dekan Fakultas Ilmu Komputer Univeraitas AMIKOM Yogyakarta.

4. Bapak Ali Mustopa, M.Kom selaku Pembimbing dalam penyusun skripsi ini.
5. Bapak Rico Agung F, S.Kom dan Bapak Joko Dwi Santoso, M.Kom yang telah memberikan saran untuk skripsis ini.
6. Tim penguji, segenap dosen dan karyawan Universitas AMIKOM Yogyakarta yang telah memberikan ilmu dan pengalaman.
7. Kedua orang tua atas dukungan berupa doa dan materil selama perkuliahan dan hingga terselesaikan skripsi ini.
8. Teman – teman semua yang pennulis tidak bisa sebutkan satu per satu, karena kebaikan dan motivasi kalian skripsi ini bisa selesai.
9. Serta semua pihak yang telah membantu dalam penyelesaian penyusunan skripsi ini.

Penulis menyadari dalam penyusunan tugas akhir ini masih banyak kekurangan serta masih jauh dari kata sempurna. Maka dari itu kritik dan saran yang bersifat membangun sangat diperlukan. Semoga penyusunan skripsi ini dapat bermanfaat bagi pembaca dalam menambah wawasan dan pengetahuan, khususnya dalam bidang jaringan komputer.

Akhir kata penulis ucapkan terima kasih atas kesediaannya untuk membaca dan memahami skripsi ini.

Wassalamu'alaikum wr. Wb

Yogyakarta, 15 Mei 2017

Penulis

DAFTAR ISI

LEMBAR JUDUL i
PERSETUJUAN ii
PENGESAHAN iii
PERNYATAAN iv
MOTTO v
PERSEMBAHAN vi
KATA PENGANTAR vii
DAFTAR ISI ix
DAFTAR TABEL xii
DAFTAR GAMBAR xii
INTISARI xvi
ABSTRACT xvii
1. BAB I PENDAHULUAN 1
   1.1. Latar Belakang Masalah 1
   1.2. Rumusan Masalah 2
   1.3. Batasan Masalah 2
   1.4. Tujuan Penelitian 3
   1.5. Manfaat Penelitian 3
   1.6. Metodologi Penelitian 4
   1.7. Sistematika Penulisan 5
2. BAB II LANDASAN TEORI 7
   2.1 Tinjauan Pustaka 7
   2.2 *Cloud Computing* 8
      2.2.1. Definisi *Cloud Computing* 8
      2.2.2. Jenis Layanan *Cloud Computing* 9
      2.2.3. Tipe Penerapan *Cloud Computing* 10
   2.3 *Honeypot* 11
      2.3.1. Definisi *Honeypot* 11
      2.3.2. Tipe *Honeypot* 11

2.3.3. Klasifikasi *Honeypot* 12
2.4 *Proxmox VE* 15
2.5 *Brute-Force Attack* 15
2.6 *Linux Mint* 16
BAB III ANALISIS DAN SISTEM 17
3.1. Metodologi Penelitian 17
3.1.1 Alur Penelitian 17
3.1.2 Alat Penelitian 19
3.2. Desain Sistem 20
3.2.1 Topologi *Cloud Computing* 20
3.2.2 Topologi *Cloud Computing* dan *Honeypot* 22
3.3. Metode Penyerangan 23
3.3.1 Metode *Brute-Force* 23
3.3.2 *THC Hydra* 24
3.3.3 *CUPP (Common User Password Profiler)* 26
3.4. Metode Analisis 30
BAB IV ANALISIS DAN PEMBAHASAN 31
4.1. Spesifikasi *Hardware* 31
4.2. Instalasi dan Konfigurasi 31
4.2.1 Instalasi *Proxmox* 31
4.2.2 Konfigurasi *Proxmox* 34
4.2.3 Instalasi *Debian Server* 36
4.2.4 Konfigurasi *Interfaces* 36
4.2.5 Konfigurasi *SSH* 37
4.2.6 Instalasi *Linux Mint* 38
4.2.7 Konfgurasi *Interface Linux Mint* 38
4.2.8 Instalasi *THC Hydra* 39
4.2.9 Instalasi *CUPP* 41
4.2.10 Konfigurasi *CUPP* 42
4.2.11 Instalasi dan Konfigurasi *Kippo* 44
4.2.12 Instalasi dan Konfigurasi *Kippo Graph (Web Interface log Kippo)* 49

4.2.13 Konfigurasi *Firewall* 52
4.3. Tahap Penyerangan 53
4.3.1. Skenario Penyerangan *Server Non Honeypot* 53
4.3.2. Hasil Penyerangan *Non Honeypot* 54
4.3.3. Skenario Penyerangan *Server Kippo* 57
4.3.4. Hasil Penyerangan *Honeypot* 62
BAB V PENUTUP 80
5.1 Kesimpulan 80
5.2 Saran 81
DAFTAR PUSTAKA 82
LAMPIRAN 1

DAFTAR TABEL

Tabel 3.1 Kebutuhan *Software*.....20
Tabel 3.2 Keterangan *THC Hydra*.....26
Tabel 3.3 Keterangan *CUPP*.....29
Tabel 4.1 Spesifikasi *Hardware*.....31

DAFTAR GAMBAR

Gambar 3.1 Topologi *Cloud Computing*.....20
Gambar 3.2 Tampilan Utama *Proxmox*.....21
Gambar 3.3 Tampilan *Remote SSH Debian*.....22
Gambar 3.4 Topologi *Cloud Computing + Honeypot*.....22
Gambar 3.5 *THC Hydra*.....24
Gambar 3.6 *CUPP*.....27
Gambar 4.1 Membuat *VM Proxmox*.....31
Gambar 4.2 Konfigurasi *Network VBox*.....31
Gambar 4.3 Instalasi *Proxmox*.....32
Gambar 4.4 Memasukkan *Password* dan *Email*.....32
Gambar 4.5 Memasukkan *IP Address* dan *Hostname*.....33
Gambar 4.6 Konfigurasi *IP Address Host-Only Adapter*.....34
Gambar 4.7 Pengisian *IP Address*.....34
Gambar 4.8 Dasbor *Proxmox*.....35
Gambar 4.9 *Interfaces Debian1*.....36
Gambar 4.10 *Interfaces Debian2*.....36
Gambar 4.11 *Interfaces Linux Mint*.....38
Gambar 4.12 Halaman Utama *Hydra*.....39
Gambar 4.13 Halaman Utama *xHydra (GUI Hydra)*.....40
Gambar 4.14 Halaman Utama *CUPP*.....41
Gambar 4.15 Mengganti *Port* dan *Username*.....45
Gambar 4.16 *Setting Database MySql*.....45
Gambar 4.17 *Setting userdb.txt*.....47
Gambar 4.18 *Setting ssh.py*.....47
Gambar 4.19 *Setting 000-default.conf*.....50
Gambar 4.20 Hasil Serangan *Non Honeypot Debian1*.....53
Gambar 4.21 Hasil Serangan *Non Honeypot Debian2*.....54
Gambar 4.22 *Log auth.log Debian1*.....55
Gambar 4.23 *Log auth.log Debian2*.....55

Gambar 4.24 Hasil Serangan *Hydra* ke *Honeypot*.....58
Gambar 4.25 Hasil Serangan *Hydra* ke *Honeypot*.....59
Gambar 4.26 *Login Debian1 Kippo*.....59
Gambar 4.27 Isi Server Palsu *Kippo*.....60
Gambar 4.28 Login *Debian2 Kippo*.....60
Gambar 4.29 Isi Server Palsu *Kippo*.....61
Gambar 4.30 *Overview Top 10 Passwords*.....62
Gambar 4.31 *Overviews Top 10 Usernames*.....62
Gambar 4.32 *Overviews Top 10 User-Pass Combos*.....63
Gambar 4.33 *Overview Success Rasio*.....63
Gambar 4.34 *Overview Top 10 Successful User-Pass Combos*.....64
Gambar 4.35 *Overview Success per Day / Week*.....65
Gambar 4.36 *Overview Connections per IP*.....66
Gambar 4.37 *Overview Probes per Day / Week*.....67
Gambar 4.38 *Overview Top 10 SSH Clients*.....67
Gambar 4.39 *Input Overall Post-Compromise Activity*.....68
Gambar 4.40 *Input Human Activity Inside The Honeypot*.....69
Gambar 4.41 *Input Top 10 Input (Overall)*.....69
Gambar 4.42 *Input Top 10 Successful Input*.....70
Gambar 4.43 *Input Top 10 Failed Input*.....70
Gambar 4.44 *Input WGET Commands*.....71
Gambar 4.45 *Input Interesting Commands*.....71
Gambar 4.46 *Replay Input by Attackers Captured by The Honeypot System*.....72
Gambar 4.47 *TTY Playlog*.....72
Gambar 4.48 *TTY Playlog Information*.....73
Gambar 4.49 *Network IP Activity Gathered from The Honeypot System*.....73
Gambar 4.50 *Network IP 10.10.10.50*.....74
Gambar 4.51 *GeoIP Top 10 Address Probing The System*.....74
Gambar 4.52 *GeoIP Number of Connection per Unique IP*.....75
Gambar 4.53 *GeoIP Number of Connection per Unique IP*.....75
Gambar 4.54 *GeoIP Google Maps*.....76

Gambar 4.55 *GeoIP Number of Connection per Country*.....76
Gambar 4.56 *Graph Gallery*.....77
Gambar 4.57 *Change Log*.....77

INTISARI

Saat ini istilah *Cloud Computing* seringkali terdengar dan dapat dibaca di *internet*. Bahkan tanpa disadari masyarakat Indonesia seringkali menggunakan layanan berbasis *Cloud Computing*. Dibalik semua kemudahannya, ternyata teknologi ini memiliki beberapa kelemahan yaitu di bidang keamanan, misalnya saja pembobolan dengan metode serangan *brute-force*. Dari uraian diatas, maka dibuatlah sebuah sistem keamanan jaringan menggunakan *Honeypot* yang dapat menganalisis serta mengumpulkan informasi identitas serta aktifitas yang dilakukan oleh penyerang.

Honeypot untuk *SSH* atau *Kippo*, merupakan *security resource* yang sengaja dibuat untuk diselidiki, diserang atau dikompromikan yang berfungsi untuk mendeteksi, pencegahan dan merespon serangan yang datang. *Honeypot* berpura - pura menjadi *server* asli untuk melindungi *port SSH* dari serangan *brute force* serta dapat menangkap identitas dan aktifitas yang dilakukan oleh *attacker*. Untuk memvisualisasikan hasil *log* pada *honeypot* digunakan *tool* yaitu *Kippo-Graph*.

Hasil yang telah didapat, *Kippo* berhasil membuat *server* palsu serta dapat mengelabui penyerang yang mengira bahwa dia akan mendapatkan hak akses penuh terhadap *server*. *Kippo-Graph* berhasil memvisualisasikan *log* yang ada di dalam *Kippo* sebagai informasi kepada *admin* bahwa *serve*r telah diserang. *Kippo-Graph* juga berhasil memberian informasi tentang aktifitas *hacker*, salah satunya dengan menampilkan video kegiatan dari *hacker* tersebut, informasi *IP* dan *command* apa saja yang dimasukkan ke *Kippo.*

Kata Kunci : *Cloud Computing, Brute Force, Honeypot, Kippo, Kippo-Graph, Log.*

ABSTRACT

Currently the term Cloud Computing is often heard and can be read on the internet. Even without realizing the people of Indonesia often use Cloud Computing-based services. Behind all the ease, it turns out this technology has several weaknesses in the field of security, such as breaking with brute-force attack methods. From the description above, then made a network security system using Honeypot that can analyze and collect identity information and activities carried out by the attacker.

Honeypot for SSH or Kippo, is a security resource that deliberately created to be investigated, attacked or compromised that serves to detect, prevent and respond to attacks coming. Honeypot pretends to be the original server to protect SSH ports from brute force attacks and can capture the identity and activities of the attacker. To visualize the results log on the honeypot used tool that is Kippo-Graph.

The results that have been obtained, Kippo managed to create a fake server and can trick the attacker who thought that he will get full access rights to the server. Kippo-Graph successfully visualized the logs inside Kippo as information to the admin that the server has been attacked. Kippo-Graph also managed to provide information about hacker activities, one of them by showing video activities of the hacker, IP information and any command that is entered into Kippo.

Keyword : *Cloud Computing, Brute Force, Honeypot, Kippo, Kippo-Graph, Log.*