Investigasi Forensik *Cloud* IaaS Studi Kasus *Compromised* AWS EC2 menggunakan Metode *National Institute of Standards and Technology* (NIST)

SKRIPSI

Disusun oleh:

Andrian Raditya Rahma
17.83.0015

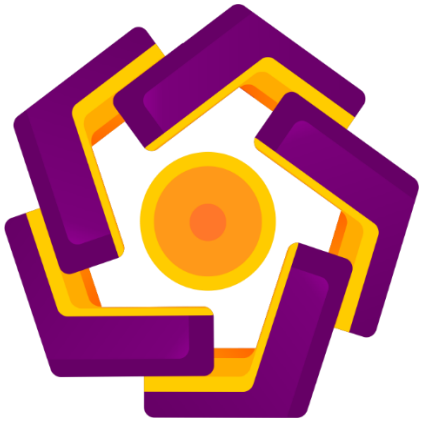
PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA

2021

Investigasi Forensik *Cloud* IaaS Studi Kasus *Compromised* AWS EC2 menggunakan Metode *National Institute of Standards and Technology* (NIST)

SKRIPSI

Diajukan kepada Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
untuk memenuhi salah satu syarat memperoleh gelar Sarjana Komputer
Pada Jenjang Program Sarjana – Program Studi Teknik Komputer



Disusun oleh:

Andrian Raditya Rahma
17.83.0015

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021

HALAMAN PERSETUJUAN

SKRIPSI

Investigasi Forensik Cloud IaaS Studi Kasus Compromised AWS EC2 menggunakan Metode National Institute of Standards and Technology (NIST)

yang dipersiapkan dan disusun oleh

Andrian Raditya Rahma

17.83.0015

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 26 April 2021

Dosen Pembimbing,

Melwin Syafrizal, S.Kom., M.Eng.
NIK. 190302105

HALAMAN PENGESAHAN

SKRIPSI

Investigasi Forensik Cloud IaaS Studi Kasus Compromised AWS EC2 menggunakan Metode National Institute of Standards and Technology (NIST)

yang dipersiapkan dan disusun oleh

Andrian Raditya Rahma

17.83.0015

Telah dipertahankan di depan Dewan Penguji
pada tanggal 26 April 2021

Susunan Dewan Penguji

Nama Penguji	**Tanda Tangan**
Joko Dwi Santoso, M.Kom. **NIK. 190302181**	_____
Mulia Sulistiyono, M.Kom. **NIK. 190302248**	_____
Melwin Syafrizal, S.Kom., M.Eng. **NIK. 190302105**	_____

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 26 April 2021

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Andrian Raditya Rahma
NIM : 17.83.0015

Menyatakan bahwa Skripsi dengan judul berikut:

Tuliskan Judul Skripsi

Dosen Pembimbing : M Syafrizal, S. Kom, M. Eng

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 29 April 2021

Yang Menyatakan,

Andrian Raditya Rahma

HALAMAN PERSEMBAHAN

Segala puji bagi Allah SWT atas limpahan rahmat dan hidayah serta karunia-Nya sehingga skripsi ini selesai dengan sebaik-baiknya. Skripsi ini saya persembahkan untuk :

1. Ibu saya, Ibu Sri Banon yang selalu mendoa'kan, memberi dukungan, fasilitas serta memberikan hasil kerja kerasnya kepada saya.
2. Bapak M Syafrizal, S. Kom, M. Eng Selaku dosen pembimbing yang telah membantu dalam penyusunan skripsi ini.
3. Kepada sahabat dan teman-teman yang ada disaat suka maupun duka selama masa perkuliahan saya.

KATA PENGANTAR

Puji dan syukur dipanjatkan kehadirat Tuhan Yang Maha Esa atas karunia yang telah dianugerahkan kepada penulis, sehingga penulis dapat menyelesaikan skripsi yang berjudul "Investigasi Forensik *Cloud* IaaS Studi Kasus *Compromised* AWS EC2 menggunakan Metode *National Institute of Standards and Technology* (NIST)". Skripsi ini disusun sebagai syarat memperoleh gelar Sarjana Komputer pada program Studi S1 Teknik Komputer Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

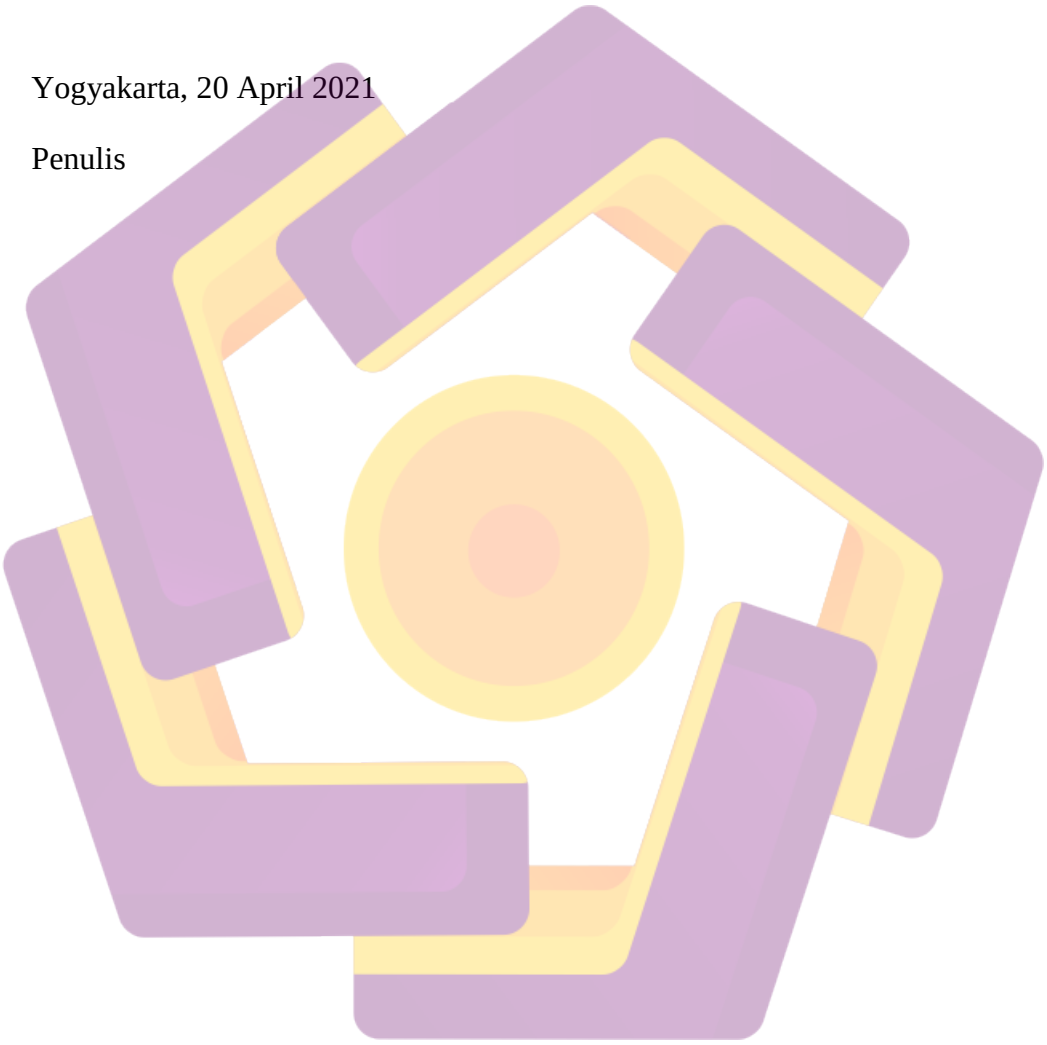
Penulis menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, skripsi ini tidak mungkin dapat terselesaikan. Oleh karena itu, penulis menyampaikan terima kasih kepada :

4. Allah SWT karena atas karunia-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan semoga dapat memberikan manfaat di kemudian hari.
5. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas AMIKOM Yogyakarta.
6. Bapak Dony Ariyus, M. Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta.
7. Bapak M Syafrizal, S Kom, M Eng selaku Dosen Pembimbing yang telah bersedia memberikan pengarahan dan bimbingan dalam penyususnan Skripsi ini.
8. Segenap Dosen, Staff, dan Karyawan Universitas AMIKOM Yogyakarta yang telah memberikan ilmu kepada penulis di bangku kuliah dan juga membantu penulis dalam kelancaran administrasi sampai terselesaikannya Skripsi ini.
9. Orang tua, saudara-saudara beserta keluarga yang selalu mendoakan dan memberikan dukungan penuh kepada penulis.
10. Serta kepada semua pihak yang telah membantu dalam penyusunan Skripsi ini yang tidak dapat penulis sebutkan satu per satu.

Penulis berharap semoga skripsi ini dapat bermamfaat bagi semua pihak yang terkait dalam penulisan ini. Dalam penulisan skripsi ini penulis menyadari masih banyak kekurangan karena terbatasnya pengetahuan dan pengalaman penulis. Karena itu, dengan lapang hati penulis mengharapkan kritik dan saran yang membangun guna menyempurnakan skripsi ini.

Yogyakarta, 20 April 2021

Penulis



DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Implementasi teknologi cloud computing pada berbagai sektor industri dan kebutuhan manusia saat ini sudah sangat populer. Banyak perusahaan besar melakukan migrasi teknologi ke infrastruktur cloud. Cepatnya perkembangan development dari sisi teknologi dan arsitektur cloud computing menjadi tantangan baru pada kasus digital forensik dalam mencari bukti potensial dalam penanganan kasus cybercrime.

Proses akuisisi atau data collection pada teknologi cloud banyak memiliki perbedaan dibandingkan arsitektur on-promise karena adanya teknologi baru di belakangnya. Untuk mendukung investigator dalam analisis forensik di sektor cloud, penelitian ini akan membahas proses investigasi barang bukti dengan studi kasus hacking pada AWS EC2 instance, yang merupakan layanan infrastructure as a service (IAAS) milik provider Amazon Web Service (AWS) menggunakan metodologi National Institute of Standards Technology (NIST).

Investigasi barang bukti berdasarkan kombinasi hasil akuisisi data EC2 image storage, memori ram dan kombinasi artefak inbound / outbound traffic yang bisa didapat pada layanan AWS Flow Logs. Hasil yang diperoleh dari ketiga teknik analisis diatas mampu membuktikan skenario serangan yang telah dibuat.

Kata kunci: Incident Response, Digital Forensic, Cloud Forensic, Cloud computing

ABSTRACT

The implementation of cloud computing for various industrial sectors and various areas of human life is very popular in recent years. Many companies are starting to shift business-critical workloads to cloud infrastructure, such as Amazon Web Services. The rapid development of cloud architecture technology creates new challenges in the field of digital forensics to find potential evidence against criminal activities in cloud environment cases.

The process of investigator access to evidence, identify, data collection, preservation, and analysis will be slightly different than the investigation on-premise architecture because of various unique cloud environments such as large storage capacity, geographic backend, multi-tenancy and data access control. To assist the investigator in the cloud forensic area, this paper is presented to provide specific information about performing potential analysis evidence of AWS EC2 instance hacking as a case study using the National Institute of Standards Technology (NIST) methodology.

Evidence analysis is based directly on EC2 image storage, memory ram and artifact combinations from inbound / outbound traffic AWS Flow Logs service. The results obtained from the three techniques above are able to create scenarios that have been created.

Keyword: Incident Response, Digital Forensic, Cloud Forensic, Cloud computing