INVESTIGASI FORENSIK CLOUD IAAS STUDI KASUS INFECTED GOOGLE CLOUD VM MENGGUNAKAN METODE NATIONALINSTITUTE OF STANDARDSAND TECHNOLOGY (NIST)

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

RAMDANI ILHAM PRATAMA

18.83.0273

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

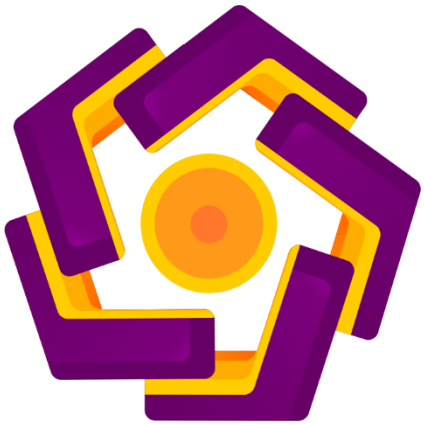
2023

INVESTIGASI FORENSIK CLOUD IAAS STUDI KASUS INFECTED GOOGLE CLOUD VM MENGGUNAKAN METODE NATIONALINSTITUTE OF STANDARDSAND TECHNOLOGY (NIST)

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer



disusun oleh

RAMDANI ILHAM PRATAMA

18.83.0273

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

HALAMAN PERSETUJUAN

SKRIPSI

INVESTIGASI FORENSIK CLOUD IAAS STUDI KASUS INFECTED GOOGLE CLOUD VM MENGGUNAKAN METODE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

yang disusun dan diajukan oleh

Ramdani Ilham Pratama

18.83.0273

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 15 Agustus 2023

Dosen Pembimbing,

Banu Santoso, S.T., M.Eng.

NIK. 190302327

HALAMAN PENGESAHAN

SKRIPSI

INVESTIGASI FORENSIK CLOUD IAAS STUDI KASUS INFECTED GOOGLE CLOUD VM MENGGUNAKAN METODE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

yang disusun dan diajukan oleh

Ramdani Ilham Pratama

18.83.0273

Telah dipertahankan di depan Dewan Penguji
pada tanggal 15 Agustus 2023

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Alva Hendi Muhammad, S.T, M.Eng., Dr. **NIK. 190302493**	
Senie Destya, M.Kom. **NIK. 190302312**	
Banu Santoso, S.T., M.Eng. **NIK. 190302327**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 15 Agustus 2023

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Ramdani Ilham Pratama
NIM : 18.83.0273

Menyatakan bahwa Skripsi dengan judul berikut:

Investigasi Forensik Cloud Iaas Studi Kasus Infected Google Cloud VM Menggunakan Metode NIST

Dosen Pembimbing : Banu Santoso, S.T., 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, 15 Agustus 2023

Yang Menyatakan,

Ramdani Ilham Pratama

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 dan Bapak saya, Ibu Renti Marini Dan Bapak Eko Erianto yang selalu mendoa'kan, memberi dukungan, fasilitas serta memberikan hasil kerja kerasnya kepada saya.
2. Bapak Banu Santoso, S.T., 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 Infected Google Cloud Vm Menggunakan Metode 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 Banu Santoso, S.T., 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 bermanfaat 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, 15 Agustus 2023

Ramdani Ilham Pratama

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMBANG DAN SINGKATAN

GCP	Google Cloud Platform
VM	Virtual Machine
NIST	National Institute Of Standards And Technology
VHD	Virtual Harddisk
SSH	Secure Shell
PCAP	Packet Capturing
IOC	Indicator Of Compromise

DAFTAR ISTILAH

Attacker/Threat Actor	Pelaku Penyerangan
Eksaminasi	Tahap Pra-duga

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 VM Google Cloud, yang merupakan layanan infrastructure as a service (IAAS) milik provider Google Cloud menggunakan metodologi National Institute of Standards Technology (NIST). Investigasi barang bukti berdasarkan kombinasi hasil akuisisi data VM image storage dan kombinasi artefak inbound / outbound traffic yang bisa didapat pada layanan VPC Flow Logs.

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

ABSTRACT

The implementation of cloud computing technology in various industrial sectors and human needs is currently very popular. Many large companies are migrating technology to cloud infrastructure. The rapid development in terms of technology and cloud computing architecture is a new challenge in digital forensic cases in finding potential evidence in handling cybercrime cases. The acquisition process or data collection in cloud technology has many differences compared to the on-promise architecture because of the new technology behind it. To support investigators in forensic analysis in the cloud sector, this study will discuss the process of investigating evidence with hacking case studies on Google Cloud VMs, which are infrastructure as a service (IAAS) services owned by Google Cloud providers using the National Institute of Standards Technology (NIST) methodology.). Investigation of evidence based on a combination of VM image storage data acquisition results and a combination of inbound / outbound traffic artifacts that can be obtained on the VPC Flow Logs service

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