

**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,

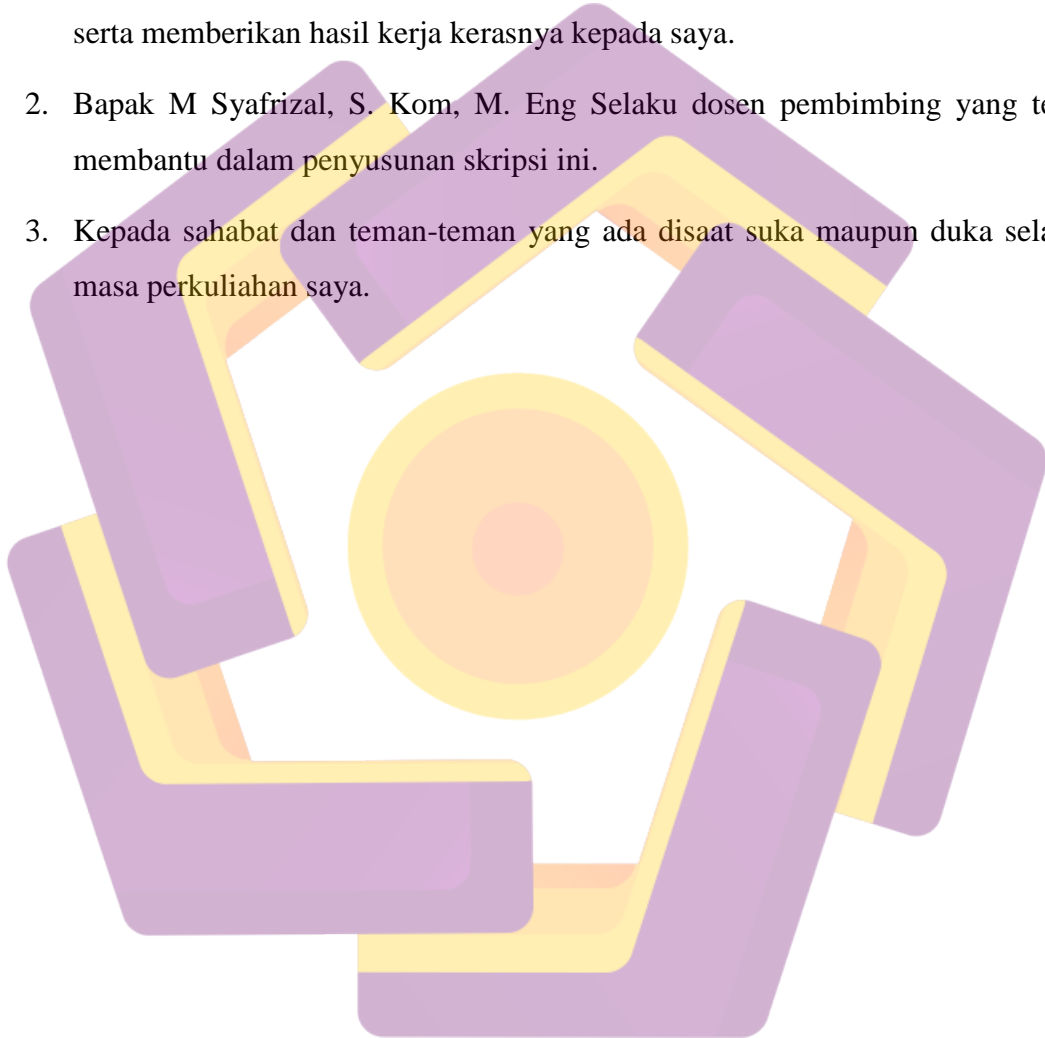


Andrian Raditya Rahma

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.

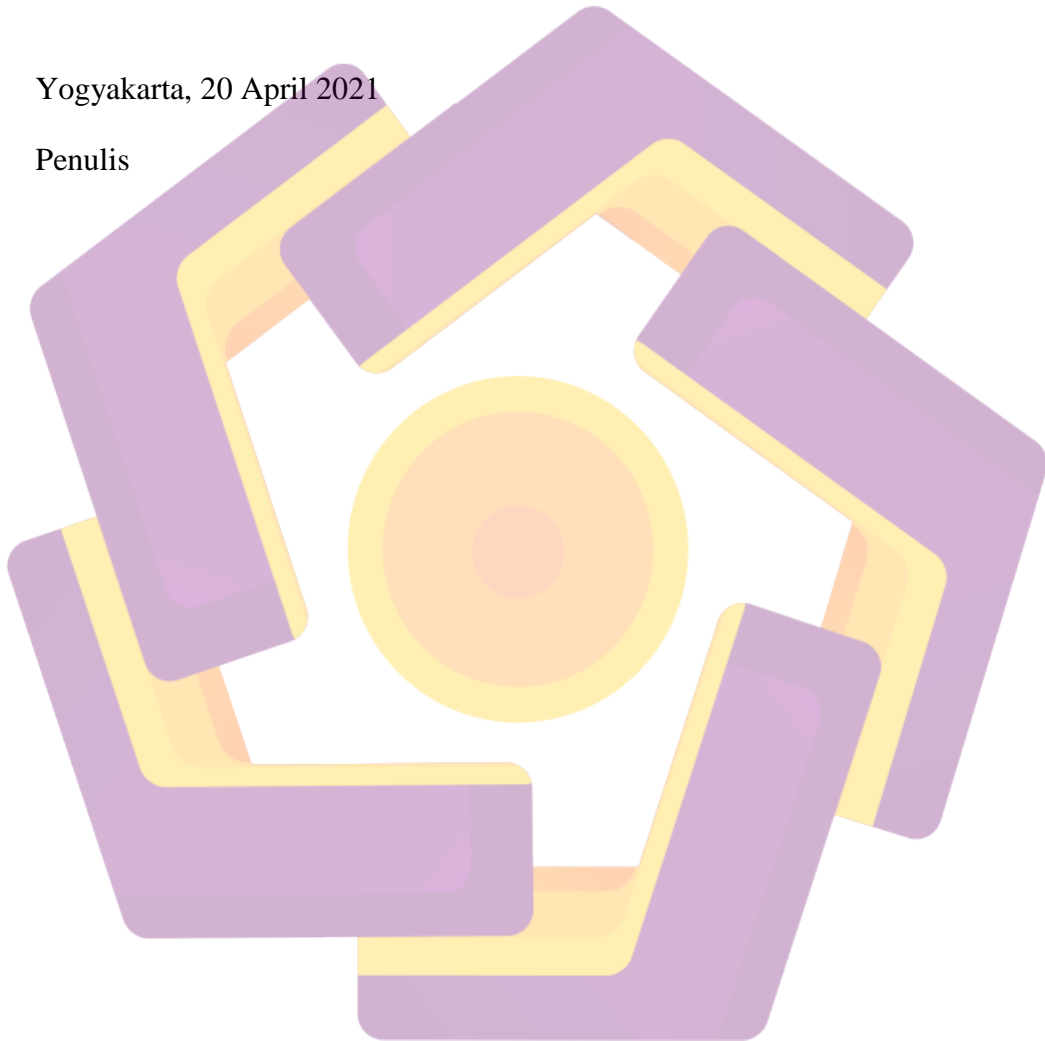
Penulis menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, skripsi ini tidak mungkin dapat terselesaikan. Oleh karena itu, penulis menyampaikan terima kasih kepada :

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 penyusunan 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 mengharapakan kritik dan saran yang membangun guna menyempurnakan skripsi ini.

Yogyakarta, 20 April 2021

Penulis



DAFTAR ISI

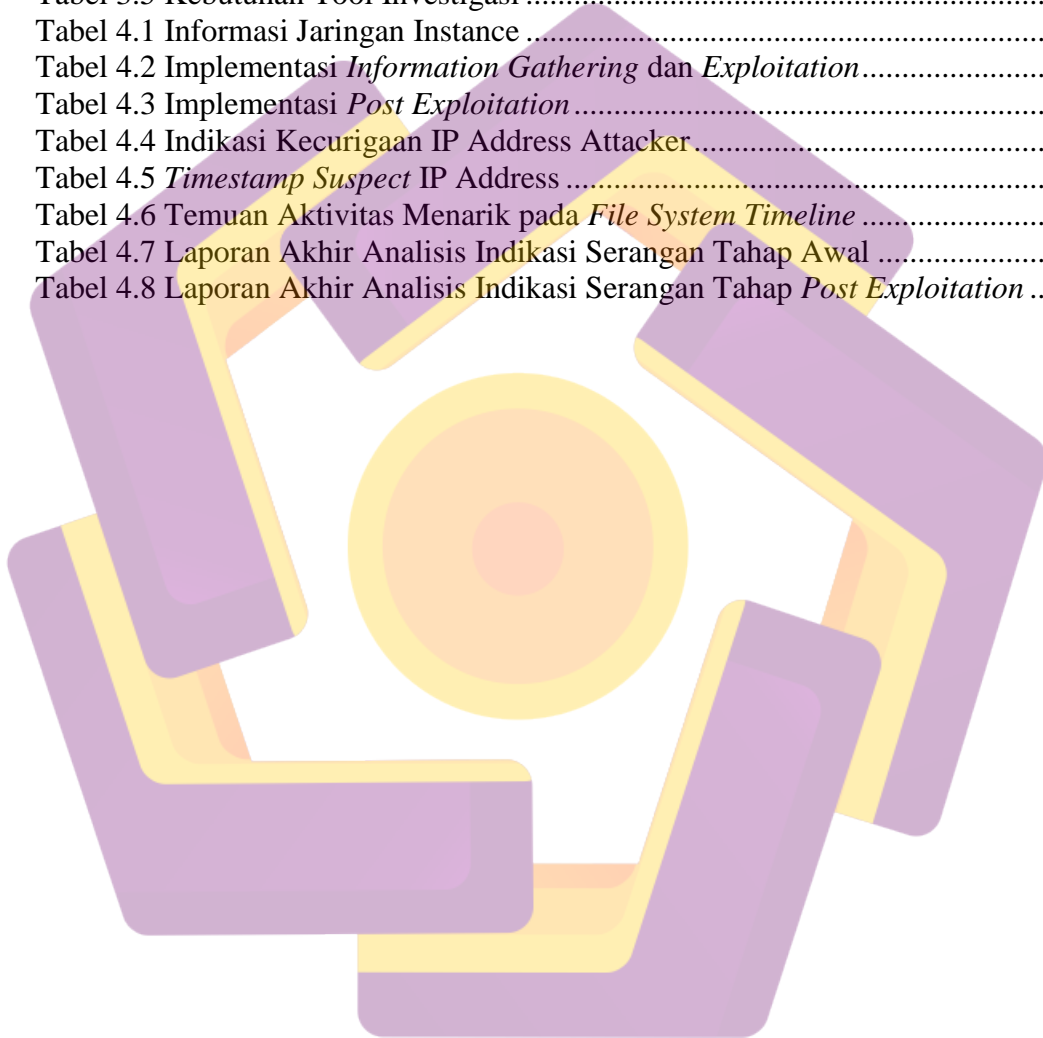
HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	iv
HALAMAN MOTTO	iv
HALAMAN PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xii
DAFTAR GAMBAR	xiii
INTISARI.....	xv
<i>ABSTRACT</i>	xvi
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	4
1.6 Sistematika Penulisan	4
BAB II LANDASAN TEORI	6
2.1 Tinjauan Pustaka.....	6
2.2 Forensika Digital.....	8
2.3 <i>Standard Operating Procedure (SOP)</i>	8
2.4 Bukti Digital.....	9
2.5 <i>Indicators of Compromise (IOC)</i>	9
2.6 <i>Network Forensic</i>	9
2.7 <i>Live Forensic</i>	10
2.8 <i>Disk Forensic</i>	11
2.9 <i>SIFT Workstation</i>	11

2.10 <i>Infrastructure as a Service (IaaS)</i>	12
2.11 Layanan AWS	12
2.11.1 <i>Elastic Compute Cloud (EC2)</i>	12
2.11.2 <i>Elastic Block Store (EBS)</i>	13
2.11.3 Amazon S3	13
2.11.4 Amazon Flow Logs	14
2.11.5 Amazon Athena	14
2.12 Kebutuhan Tool Investigasi	14
2.12.1 FLS dan <i>Mactime</i>	14
2.12.2 Dd	14
2.12.3 <i>Margarita Shogun</i>	15
2.12.4 <i>Volatility</i>	15
2.13 NIST <i>Framework</i>	14
2.13.1 <i>Collection</i>	14
2.13.2 <i>Examination</i>	14
2.13.3 <i>Analysis</i>	15
2.13.4 <i>Reporting</i>	15
BAB III METODOLOGI PENELITIAN	18
3.1 Skenario Kasus Serangan	19
3.2 Identifikasi Kebutuhan Layanan AWS	21
3.2.1 Kebutuhan <i>Service Cloud</i>	21
3.2.2 Kebutuhan Perangkat Lunak	23
3.3 Alur Investigasi dan Metode Analisis	23
BAB IV PEMBAHASAN	25
4.1 Persiapan	25
4.1.1 Persiapan Lingkungan <i>Cloud</i>	25
4.1.1.1 Pembuatan <i>EC2 Instance</i>	25
4.1.1.2 Persiapan Lab <i>EC2 Instance</i>	25
4.1.1.3 Konfigurasi <i>EC2 SIFT Workstation</i>	25
4.1.2 Implementasi Skenario Serangan	28
4.1.2.1 <i>Information Gathering & Exploitation</i>	28
4.1.2.2 <i>Post Exploitation</i>	31
4.2 Akuisisi Data	42

4.2.1	Akuisisi <i>Data Traffic</i>	43
4.2.2	Akuisisi <i>EC2 Disk Volume</i>	43
4.2.3	Akuisisi Memori <i>RAM</i>	43
4.3	Eksaminasi	42
4.3.1	Eksaminasi <i>Flow Logs</i>	43
4.3.1.1	<i>Querying Data Flow Logs</i>	44
4.3.2	Eksaminasi <i>Snapshot Disk Volume</i>	46
4.3.2.1	<i>Mount Snapshot Disk</i>	47
4.3.2.2	<i>Pembuatan Filesystem Timeline</i>	47
4.3.3	Eksaminasi Memori <i>Image</i>	48
4.3.3.1	<i>Pembuatan Volatility Profile</i>	48
4.3.3.2	<i>Mapping Memory Image</i>	49
4.4	Analisis Bukti Digital	50
4.4.1	Analisis <i>Flow Logs</i> dan Memahami Pola <i>Traffic</i>	51
4.4.2	Analisis <i>EBS (EC2 Snapshot Image)</i>	54
4.4.2.1	<i>Analisis Timeline FileSystem</i>	54
4.4.2.2	<i>Analisis Log Files</i>	55
4.4.3	Analisis Memori <i>Image</i>	57
4.4.3.1	<i>Analisis Artefak Jaringan</i>	58
4.4.3.2	<i>Analisis Artefak Linux Process</i>	59
4.5	Laporan Akhir Investigasi.....	61
BAB V PENUTUP.....		64
5.1	Kesimpulan	64
5.2	Saran	65
DAFTAR PUSTAKA		67

DAFTAR TABEL

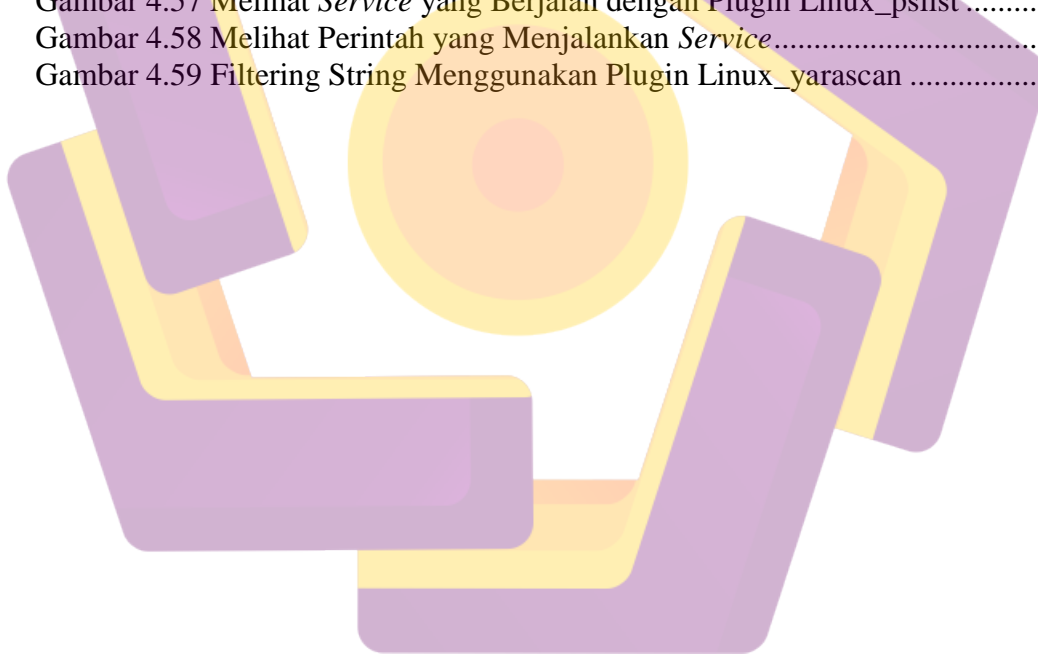
Tabel 2.1 Penelitian Terdahulu tentang Prosedur dan <i>Legal Issues</i>	6
Tabel 2.2 Penelitian Terdahulu tentang <i>Cloud Forensic</i> Secara Teknikal.....	7
Tabel 3.1 Perbedaan Perolehan data <i>On-Premises</i> dengan <i>AWS Cloud-Based</i> ...	18
Tabel 3.2 Dua Tahap Skenario Serangan.....	20
Tabel 3.4 Spesifikasi <i>EC2 Instance SIFT Workstation</i>	22
Tabel 3.5 Kebutuhan Tool Investigasi	23
Tabel 4.1 Informasi Jaringan Instance	26
Tabel 4.2 Implementasi <i>Information Gathering</i> dan <i>Exploitation</i>	28
Tabel 4.3 Implementasi <i>Post Exploitation</i>	31
Tabel 4.4 Indikasi Kecurigaan IP Address Attacker.....	53
Tabel 4.5 <i>Timestamp Suspect</i> IP Address	54
Tabel 4.6 Temuan Aktivitas Menarik pada <i>File System Timeline</i>	55
Tabel 4.7 Laporan Akhir Analisis Indikasi Serangan Tahap Awal	61
Tabel 4.8 Laporan Akhir Analisis Indikasi Serangan Tahap <i>Post Exploitation</i> ...	63



DAFTAR GAMBAR

Gambar 1.1 <i>Public Cloud Market Share</i>	2
Gambar 2.1 Tahapan Metodologi NIST	15
Gambar 3.1 Model Layanan pada Platform <i>Cloud</i>	19
Gambar 3.2 Tahap Skenario Serangan	20
Gambar 3.3 S3 <i>Bucket</i> untuk Menampung <i>Memory Image</i> dan Data Flow Log ..	23
Gambar 3.4 Alur Investigasi Forensik	24
Gambar 4.1 Pembuatan 2 EC2 <i>Instance</i>	26
Gambar 4.2 <i>Vulnerable Web App</i>	26
Gambar 4.3 Instalasi <i>Service vsftpd</i>	27
Gambar 4.4 <i>Service Vsftpd</i> Berjalan	27
Gambar 4.5 Instalasi SIFT	28
Gambar 4.6 Instalasi <i>Dependencies</i> Margaritha Shotgun	28
Gambar 4.7 <i>Port Scanning</i> Menggunakan NMAP	29
Gambar 4.8 Skenario Serangan SSH Brute Force	30
Gambar 4.9 Skenario Serangan <i>Brute Path</i> menggunakan Ffuf	30
Gambar 4.10 Eksploitasi <i>Service Vsftpd</i> Versi Lama	31
Gambar 4.11 Skenario <i>Enumerasi Sistem</i>	32
Gambar 4.12 Eksekusi <i>Malware</i> Trojan pada EC2 Victim	32
Gambar 4.13 Membuat User Baru dengan <i>Privilege Sudo</i>	32
Gambar 4.14 Skenario Menghapus Jejak <i>Log</i>	33
Gambar 4.15 Isolasi Jaringan VPC EC2 Victim	33
Gambar 4.16 Tahapan Analisis <i>Network Forensic</i>	35
Gambar 4.17 <i>Record File Flow Log</i>	35
Gambar 4.18 File Flow Log yang Tersimpan pada <i>Bucket</i>	36
Gambar 4.19 Tahapan Analisis <i>Disk Volume</i>	37
Gambar 4.20 Pembuatan <i>Snapshot Image</i>	37
Gambar 4.21 Membuat <i>Volume</i> Baru dari <i>Snapshot Image</i>	38
Gambar 4.22 <i>Attach Volume</i> ke EC2 SIFT	38
Gambar 4.23 <i>Volume Snapshot</i> Berhasil Ter-attach	39
Gambar 4.24 Akuisisi <i>Disk Volume</i>	39
Gambar 4.25 Perbandingan Checksum <i>Snapshot Disk</i> dan Hasil <i>Imaging</i>	39
Gambar 4.26 Tahapan Analisis <i>Live Forensic</i>	40
Gambar 4.27 Membuat LIME Module	41
Gambar 4.28 Kernel Module dari AMI EC2 <i>Victim</i>	41
Gambar 4.29 Md5 Sum dari <i>Memory Image</i> Hasil Akuisisi	41
Gambar 4.30 <i>Backup Memory Image</i> ke S3 <i>Bucket</i>	42
Gambar 4.31 <i>File Memory Image</i> Berhasil Terupload di S3 <i>Bucket</i>	42
Gambar 4.32 Format Flow Logs	44
Gambar 4.33 Membuat Tabel pada Amazon Athena	43
Gambar 4.34 <i>Query Filtering</i> Total Packet yang Terkirim	45
Gambar 4.35 <i>Query Filtering Traffic Port</i>	45
Gambar 4.36 Query Total Packet antar Beda IP Address	46
Gambar 4.37 <i>Mounting Snapshot Disk Volume</i>	47
Gambar 4.38 Membuat <i>File System Timeline</i>	47

Gambar 4.39 Membuat Modul Dwarf (Kernel Data Structure).....	48
Gambar 4.40 Module Dwarf Berhasil Dibuat	48
Gambar 4.41 Membuat <i>Volatility Profile</i>	49
Gambar 4.42 Custom <i>Volatility Profile</i> Berhasil Diloat	49
Gambar 4.43 Testing Plugin Banner Volatility Berhasil Berjalan.....	49
Gambar 4.44 <i>Memory Mapping</i>	50
Gambar 4.45 Kalkulasi <i>Space Address</i> pada <i>Memory RAM</i>	50
Gambar 4.46 Analisis <i>Data Packet Transferred</i>	52
Gambar 4.47 Analisis <i>Data Traffic</i> pada <i>Port</i> Tertentu.....	52
Gambar 4.48 Analisis <i>Data Traffic</i> dari Tiap Sumber IP yang Berbeda	52
Gambar 4.49 Analisis <i>Data Timestamp Traffic</i>	53
Gambar 4.50 Artefak <i>Filesystem Timeline</i> (MACB)	53
Gambar 4.51 Bukti Potensial Serangan pada <i>Filesystem Timeline</i>	55
Gambar 4.52 Aktifitas <i>Bruteforce</i> Tercatat di <i>Access.log</i>	56
Gambar 4.53 Bukti <i>Attacker</i> Membuat User Baru	57
Gambar 4.54 Akses Ftp dari <i>Suspect Ip Attacker</i>	57
Gambar 4.55 Melihat Informasi ARP dengan Plugin <i>Linux_arp</i>	58
Gambar 4.56 Melihat Informasi <i>Listening</i> Koneksi.....	59
Gambar 4.57 Melihat <i>Service</i> yang Berjalan dengan Plugin <i>Linux_pslist</i>	59
Gambar 4.58 Melihat Perintah yang Menjalankan <i>Service</i>	60
Gambar 4.59 Filtering String Menggunakan Plugin <i>Linux_yarascan</i>	60



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-premise 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

