INVESTIGASI CLOUD FORENSIC PADA DISK VOLUME AWS EC2 STUDI KASUS *PENETRATION TESTING* TERHADAP *INSTANCE*

Andriyan Dwi Putra [(1)], Joko Dwi Santoso [(2)], Adrian Raditya Rahma [(3)], Ipung Ardiansyah [(4)]
Sistem Informasi, Fakultas ilmu Komputer[1)]
Teknik Komputer, Fakultas Ilmu Komputer[2) 3) 4)]
Universitas AMIKOM, Yogyakarta, Indonesia[1)2)3)4)]
Andriyan.putra@amikom.ac.id[1)], jds@amikom.ac.id[2)]
andrian.rahma@students.amikom.ac.id[2)] ,ipung.19@students.amikom.ac.id[2)]

ABSTRACT

The implementation of cloud computing technology in the industrial sector is currently growing fast. The rapid development of technology and cloud computing architectures is a new task for digital forensic cases to find potential evidence to deal with cybercrime incidents. EC2 instances are one of the infrastructure as a service (IAAS) service (IAAS), which belongs to the Amazon Web Services (AWS), which is used by individuals and companies, when dealing with the needs of server service infrastructure. This is a basic researcher to force an analysis of the cloud sector by starting an example research on EC2 hacking activity scenarios such as National Technology Laboratories (NIST) methodology. Item Disk Collects scenarios of attack information, activity, exploitation, and non-enbitant signs of signs of attack information, activity activities, exploitation, and non-enbitant's signs based on the analysis of timeline file systems received from disk volume instance It was possible to prove that. During the information gathering and exploit phases, the attacker found two attacks. That is, the Web Path Bruteforce in the artifact source /var/log/access.log and the exploit (infringed instance) in the artifact source /var/log/vsftpd.log. , Two attacks were found during the exploit. That is, the "Maintaining Access" in the artifact source "/var/log/auth.log" and the "CoveringTrack" in the artifact source file system timeline.

Keywords: **Network Security, Digital Forensic, Cloud Forensic, Cloud Computing, NIST, Cybersecurity**

ABSTRAK

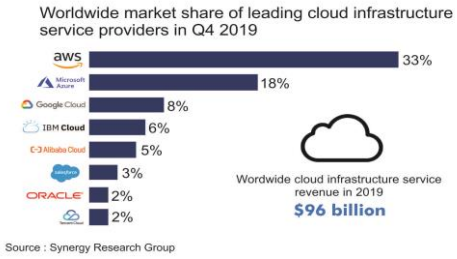
Implementasi teknologi cloud computing pada sektor industri saat ini sudah berkembang cukup cepat. Cepatnya perkembangan development dari sisi teknologi dan arsitektur cloud computing menjadi tantangan baru pada kasus digital forensik dalam mencari bukti potensial pada penanganan kasus cybercrime. EC2 instance merupakan salah satu layanan infrastructure as a service (IAAS) milik provider Amazon Web Service (AWS) yang banyak digunakan perseorangan maupun perusahaan dalam menangani kebutuhan infrastruktur layanan server. Hal ini menjadi dasar peneliti untuk melakukan analisis forensik pada sektor cloud dengan mengangkat studi kasus proses investigasi pada skenario aktivitas hacking EC2 instance menggunakan metodologi National Institute of Standards Technology (NIST). Berdasarkan hasil analisis artefak filesystem timeline dan log system yang diperoleh dari barang bukti volume disk instance, peneliti berhasil membuktikan skenario aktivitas serangan information gathering, eksploitasi dan post exploitation. Pada phase Information Gathering & Exploitation di temukan dua serangan yang dilakukan attacker yaitu Web Path Bruteforce di sumber artefak /var/log/access.log dan Exploitation (Compromised Instance) di sumber artefak /var/log/vsftpd.log, sedangkan pada phase Post Exploitation ditemukan 2 serangan yaitu Maintaining Access di sumber artefak /var/log/auth.log dan Covering Track di sumber artefak file system timeline.

Kata Kunci: Kemanan Jaringan, Digital Forensik, Cloud Forensic, Cloud Computing, NIST, Cybersecurity

PENDAHULUAN

Cloud computing menjadi model infrastruktur baru dengan banyak keunggulan dibandingkan arsitektur on-premise, seperti layanan on-demand, elastisitas, dan *configurable computing resources* (Morioka & Sharbaf, 2016)(Hung, 2019). Keunggulan cloud computing pada sisi bisnis dalam menekan biaya operasional yang begitu signifikan dan kenyamanan tanpa perlu mengelola infrastruktur membuat tren penggunaan cloud berkembang sangat pesat. Banyak organisasi, startup dan perusahaan besar bermigrasi ke layanan cloud **(**Agbedanu et al., 2019**)**. Berdasarkan data statistik Gartner, model Infrastructure as a Service (IaaS) akan menjadi segmen pasar yang tumbuh paling cepat dengan perkiraan pertumbuhan 24% **(**Gartner, 2019**).** Tim analis Forbes memprediksi penggunaan resource 41% dari beban kerja perusahaan akan dijalankan di platform public cloud pada tahun 2020, 83% dari adopsi teknologi perusahaan akan mengimplementasikan cloud pada tahun 2020, 20% lainnya akan menerapkan private cloud, dan 22% akan bergantung pada hybrid cloud (Columbus, 2018).

Amazon Web Services (AWS) merupakan salah satu cloud provider yang memimpin pasar public cloud dengan adopsi layanannya mencapai 47%. Pada 2020, metric pengguna service publik cloud AWS masih dominan dan terbanyak dan menjadi market leader dengan porsi market share mencapai 47.5%, diikuti Microsoft Azure 29.4% dan Google Cloud Platform 3.95% (Coles, 2017). AWS adalah salah satu provider besar dalam layanan public cloud yang menyediakan layanan seperti PaaS dan IaaS. Salah satu Infrastructure as a Service (IaaS) milik AWS dengan penggunaan terbanyak adalah Elastic Cloud Computing (EC2). Amazon EC2 service mengijinkan user untuk membuat virtual machine dengan spesifikasi dan berbagai konfigurasi yang bisa disesuaikan dengan keinginan. Pengguna dapat memonitor penggunaan resource, dan dipermudahnya management resource seperti clone, pause, shutdown, delete dan apapun yang ingin pengguna inginkan (Morioka & Sharbaf, 2016). Gambar 1 dibawah memperlihatkan market share dari tiap provider public cloud.



Gambar 1 Public cloud market share

Berdasarkan pertumbuhan data penggunaan layanan cloud di atas memberikan peluang tindak kejahatan yang melibatkan service cloud karena penerapan cloud yang sudah sangat masif, terutama pada penggunaan layanan cloud dari provider AWS (Yudhistira et al., 2018)(Simou et al., 2014)(George, 2013). Selain itu banyaknya tantangan dan kesenjangan penelitian di bidang cloud forensic menjadikan Peneliti tergerak mengangkat topik tersebut dengan membahas teknik investigasi yang bisa diterapkan pada lingkungan cloud IaaS dengan studi kasus layanan AWS EC2.

Terkait proses dan teknik investigasi pada layanan cloud IaaS, peneliti menggunakan teknik analisis disk/file system forensic. Hasil akhir dari penelitian ini adalah pengungkapan kasus skenario hacking yang sudah peneliti buat di environment AWS melalui berbagai artefak penting yang sudah diperoleh.

TINJAUAN PUSTAKA

Pada penelitian ini, peneliti akan menganalisis bukti potensial yang terdapat pada environment AWS dengan skenario yang sudah dibuat menggunakan metode National Institute of Standards Technology (NIST). Metode ini dipilih karena kerangka prosedur yang cocok untuk diterapkan pada penanganan insiden secara lebih efektif dalam banyak kasus cloud forensic dan juga menjadi standar prosedur dalam praktik investigasi, agar penanganan barang bukti tetap terjaga integritasnya (Yudhana et al., 2019).

Penerapan kerangka prosedur pada metode NIST mengarahkan penelitian ini pada penyelesaian masalah sesuai standar investigasi yang benar dan dapat dipertanggung jawabkan (Yudhana et al., 2018). Hal ini bisa terlihat pada gambar 2,

mulai dari tahap akuisisi barang bukti, duplikasi, pengecekan integritas, analisis file image lalu reporting. Terdapat 4 tahap penanganan forensik berdasarkan kerangka NIST diantaranya :

Gambar 2 Tahapan Metode NIST

Collection

Pengumpulan merupakan serangkaian kegiatan mengumpulkan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan digital (Mualfah & Ramadhan, 2020). Pada tahapan ini proses identifikasi akan dilakukan, proses akuisisi dan imaging bukti digital dilakukan dalam investigasi untuk menemukan keterkaitan terhadap bukti yang memiliki potensi terkait tindak kejahatan.

Examination

Merupakan tahap pemeriksaan data forensik yang dikumpulkan dengan kombinasi metode otomatis atau manual (Imam et al., 2020), bukti akuisisi akan dilakukan proses identifikasi dengan berbagai tool yang ada. Tahap ini melakukan pemrosesan data yang sudah dikumpulkan pada tahap sebelumnya menggunakan kombinasi dari berbagai tool baik manual maupun otomatis, dengan tetap mempertahankan integritas data. Data yang sudah terkumpul berupa artifak-artifak akan dianalisis pada tahap berikutnya.

Analysis

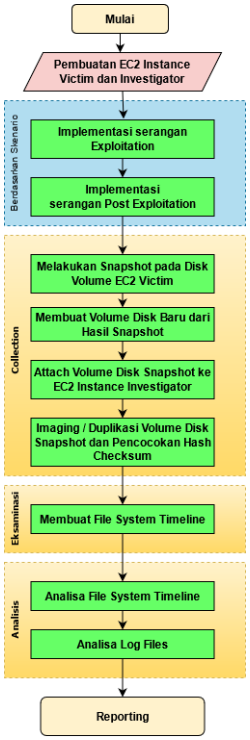
Data examination yang telah dilakukan ekstraksi selanjutnya dianalisis menggunakan metode dan teknik yang sesuai dengan prosedur yang berlaku. Analisis menggunakan metode yang dibenarkan secara hukum dan tidak merubah teknik untuk mendapatkan suatu informasi yang berguna dan dapat menjawab apa yang dibutuhkan sebagai pendorong untuk melakukan pengumpulan dan pemeriksaan data (Nasirudin et al., 2020).

Reporting

Hasil akhir analisis adalah dokumentasi atau report. Tahap reporting melaporkan hasil analisis yang meliputi hasil pembuktian skenario serangan. Pelaporan hasil analisis forensik dari awal hingga akhir disajikan dalam bentuk laporan tertulis sehingga dapat memberikan rekomendasi untuk perbaikan kebijakan, pedoman, prosedur, alat, dana spek lain dari proses forensik(Yasin et al., 2021)

METODOLOGI PENELITIAN

Gambar 3 menunjukkan langkah investigasi pada penelitian ini. Terdapat 2 artefak temuan yang peneliti gunakan dalam proses analisa, yaitu filesystem timeline dan file logs yang masih bisa diperoleh. Komponen dari kedua sumber artefak tersebut merupakan data yang dapat digabungkan untuk bisa menjawab kebutuhan informasi terkait aktivitas tindak kejahatan seperti apa yang sedang terjadi dan waktu kejadian saat kejahatan tersebut dilakukan.

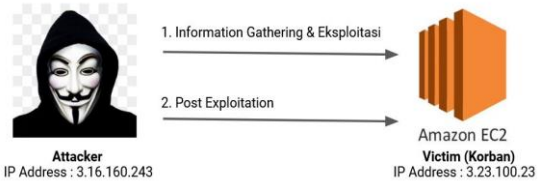


Gambar 3 Tahapan Implementasi dan Pengujian

Rancangan Simulasi

Pada penelitian ini dibuat beberapa skenario berupa aktifitas-aktifitas hacker ketika melakukan eksploitasi pada server dan aktivitas setelah mendapat akses penuh untuk dijadikan acuan artefak forensik dan menjadi parameter validasi keberhasilan analisa. Sebuah skenario dirancang untuk mendapatkan bukti digital untuk kemudian dianalisis. Skenario penelitian ini dibagi

menjadi dua phase. Phase yang pertama adalah *exploitation* (exploitasi pada sistem atau aplikasi yang memiliki kerentanan), yaitu segala tindakan dilakukan hacker untuk mendapat akses penuh (compromised instance) dan phase kedua adalah tahap post exploitation, kondisi dimana hacker sudah mendapat akses pada server yang kemudian attacker mencoba mencari informasi penting, mencuri data sensitive dan melakukan berbagai teknik yang digunakan untuk tetap mempertahankan akses pada Server EC2 Instance. Sistem operasi yang digunakan instance server EC2 adalah ubuntu 16.04. Skenario 2 phase serangan seperti pada gambar 4 menunjukkan bagaimana gambaran sederhana terjadinya proses hacking pada studi kasus penelitian ini. Terdapat dua tahap skenario serangan pada penelitian ini, yaitu tahap exploitation dan post exploitation.



Gambar 4 Skenario 2 Serangan

Pada tabel 1 memperlihatkan detail rentetan serangan dari kedua fase, berupa strategi, taktik dan teknik yang digunakan hacker (attacker). Hasil dari simulasi skenario ini akan meninggalkan rekam jejak berupa data-data bukti digital yang akan diangkat pada penelitian ini. Bukti digital dikumpulkan kemudian diperiksa dan dianalisis menggunakan teknik disk forensic. Berikut daftar serangan exploitation dan post exploitation yang diterapkan dalam skenario penelitian ini.

Tabel 1 Skenario Serangan

Phase	Serangan	Keterangan
Information Gathering & Exploitation	Web Path Bruteforce	Directory/path bruteforce menggunakan gobuster dengan wordlist sebanyak 30 baris path/endpoint
	Exploitation (Compromised Instance)	Eksploitasi service pada EC2 Victim yang memiliki kerentanan. Pada skenario kasus ini adalah service vsftpd 2.3.4
Post Exploitation	Menjalankan backdoor	Attacker menjalankan backdoor metasploit yang melakukan koneksi ke beda server
	Maintaining Access	Membuat user baru (adminserver2) dengan sudo privilege
	Covering Track	Attacker menghapus beberapa log yang tersimpan pada server victim

Berikut beberapa alat dan bahan yang diperlukan pada penelitian ditunjukkan pada tabel 2.

Tabel 2 Alat dan Bahan Penelitian

No	Alat dan Bahan	Keterangan
1	AWS EC2 Instance	Instance SIFT Workstation (Investigator), Ubuntu Server 16.04 LTS, vCPU 1 Core, vMemory 2 GB, SSD Storage 30 GB, Region us-east-2, Public IPv4 52.15.39.198
		Instance Victim (Korban), Ubuntu Server 16.04 LTS, vCPU 1 Core, vMemory 2 GB, SSD Storage 8 GB, Region us-east-2, Public IPv4 3.23.100.23
2	DD	Akuisisi disk
3	FLS & Mactime	Mengenerate file system timeline
4	md5sum	Pengecekan hash checksum

HASIL DAN PEMBAHASAN

Analisa disk image dan file system pada penelitian ini akan memanfaatkan fitur AWS yaitu snapshot atau duplikat disk. Disk volume milik EC2 Victim nantinya akan di snapshot menjadi image baru yang memiliki kesamaan data sama persis. Fitur snapshot pada teknologi cloud memudahkan investigator dalam hal efektifitas waktu dan efisiensi. Setelah snapshot disk volume dari EC2 Victim selesai dibuat maka setelah itu snapshot volume akan di attach ke EC2 SIFT Workstation. Snapshot volume nantinya akan di mount dan dianalisa secara langsung melalui tool tool yang sudah dipersiapkan pada EC2 SIFT Workstation.

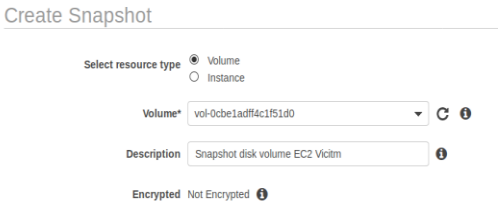
Proses analisa disk & file system pada penelitian ini akan berfokus pada beberapa artefak saja. Pada teknik analisa file system, dimana pada kasus penelitian ini adalah sistem operasi ubuntu 18.04 dengan file system ext4, peneliti akan menggunakan tool khusus untuk melakukan dump file system timeline. Pada artefak timeline inilah peneliti akan mengkorelasikan riwayat apa saja yang dilakukan attacker ketika mendapat akses penuh (compromise) pada server EC2 Victim. Gambar 5 dibawah menunjukkan gambaran tahapan persiapan analisa barang bukti disk image dari EC2 Victim.

Gambar 5 Tahapan Persiapan Analisa Disk Volume

Akuisisi EC2 Volume

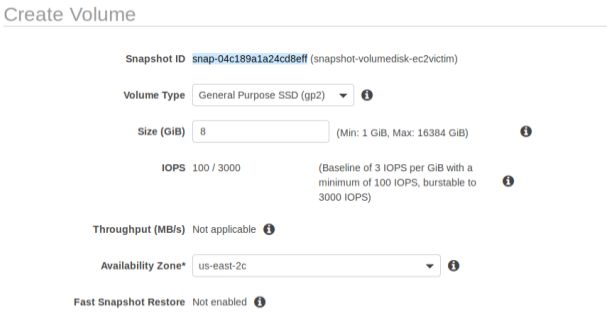
Terdapat 2 opsi pada akuisisi data volume disk. Pertama adalah membuat snapshot atau duplikasi volume disk dari EBS victim, lalu meng-attach snapshot image ke instance EC2 lain. Metode akuisisi kedua adalah melakukan detach pada EBS volume victim yang akan diselidiki lalu mendownload disk volume tersebut (Dykstra & Sherman, 2012). Pada kasus kali ini, peneliti memilih melakukan snapshot pada volume EBS dan meng-attach ke EC2 SIFT Workstation yang sudah dipersiapkan sebelumnya tanpa harus mendownload disk volume. Yang menjadi tantangan tersendiri pada proses akuisisi volume disk EBS adalah platform AWS tidak menyediakan fitur pengecekan hash checksum untuk memverifikasi integritas disk image dari instance. Hal ini tentu sangat berbeda dengan akuisisi disk pada kasus tradisional seperti barang bukti laptop.

Langkah pertama akuisisi volume disk EBS dengan cara membuat snapshot disk. Pembuatan snapshot dar volume instance EC2 Victim (vol-0cbe1adff4c1f51d0) ditunjukkan pada gambar 6.



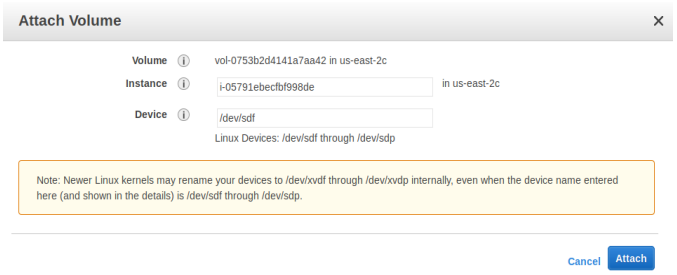
Gambar 6 Pembuatan Snapshot Disk

Setelah selesai dilakukan snapshot, langkah berikutnya membuat disk volume baru yang akan dipakai snapshot image (snap-04c189a1a24cd8eff). Konfigurasi availability zone harus disesuaikan dalam satu zona dengan instance EC2 SIFT Workstation yaitu us-east-2c. Disk volume baru yang akan dipakai snapshot image memiliki id vol-0753b2d4141a7aa42. Snapshot image nantinya akan tersimpan pada disk volume yang baru saja dibuat. Prosedur ini mirip dengan proses imaging (cloning) physical hard drive pada tradisional forensik. Proses pembuatan disk volume baru diperlihatkan pada gambar 7



Gambar 7 Membuat Volume Baru dari Snapshot Image

Selanjutnya dilakukan attach barang bukti snapshot image (vol-0753b2d4141a7aa42) ke instance SIFT Workstation (i-05791ebecfbf998de) yang ditunjukkan pada gambar 8.



Gambar 8 Attach Volume ke EC2 SIFT

Tabel 3 memperlihatkan disk volume id dari tiap tiap pemakaian

Tabel 3 Informasi Disk Volume

Disk Volume ID	Keterangan
vol-0cbe1adff4c1f51d0	Volume Disk Instance EC2 Victim
vol-0753b2d4141a7aa42	Volume baru untuk Snapshot Disk EC2 Victim

Disk volume snapshot image selanjutnya dismount ke instance investigator. Kemudian langkah terakhir adalah melakukan imaging partisi /dev/sdf milik snapshot image menggunakan tool dcfldd yang diperlihatkan pada gambar 10. Isi data dari disk image partisi tersebut akan benar benar mirip karena

dcfldd mengcopy secara bIt stream. Gambar 9 di bawah menunjukkan proses imaging yang sudah selesai dilakukan dengan output file ec2victim-volume.dd. Opsi perintah conv=noerror dan sync berguna agar tool dd tetap melakukan bit stream copy tanpa menskip sector manapun sehingga hasil imaging benar benar sama.

```
root@SIFT-Workstation:~# dd if=/dev/xvdf1 of=ec2victim-volume.dd conv=noerror,sync
16775135+0 records in
16775135+0 records out
8588869120 bytes (8.6 GB, 8.0 GiB) copied, 134.428 s, 63.9 MB/s
```

Gambar 9 Akuisisi Disk Volume

Gambar 10 merupakan perbandingan hash checksum antara partisi mounting dari snapshot disk volume dan hasil imaging yang menunjukkan hash yang sama.

```
root@SIFT-Workstation:~# md5sum /dev/xvdf1 ec2victim-volume.dd
0e18161c312f46d9361f5cf5a2048277  /dev/xvdf1
0e18161c312f46d9361f5cf5a2048277  ec2victim-volume.dd
```

Gambar 10 Perbandingan Checksum Snapshot Disk dan Hasil Imaging

Eksaminasi

Selanjutnya peneliti akan melakukan proses eksaminasi dalam rangka mengumpulkan data data dan menilai file artefak apa saja yang berelasi dengan kasus, data data yang peneliti gunakan dalam proses analisa disk volume ini bisa berupa file timestamp filesystem dan log files. Tahap ini akan menjabarkan proses dan teknik yang Peneliti gunakan dalam eksaminasi artefak dan data yang ada, dan bagaimana artefak timeline yang begitu berguna dalam mereduce besarnya data yang tersimpan pada disk image sehingga proses analisis nantinya lebih efisien.

Artefak filesystem timeline sangat penting pada tahap analisa disk volume nantinya karena file system timestamp menyimpan historical data apapun perubahan pada file system yang biasa dikenal dengan MAC time evidence (Modified, Accessed, Changed) sehingga sangat membantu dalam analisa kejadian kejadian perubahan yang tercatat pada filesystem. Gambar 11 memperlihatkan proses ekstraksi file system timeline menggunakan tool fls dan mactime. Output yang dihasilkan berupa file berekstensi csv dengan nama file ec2victim-file.csv.

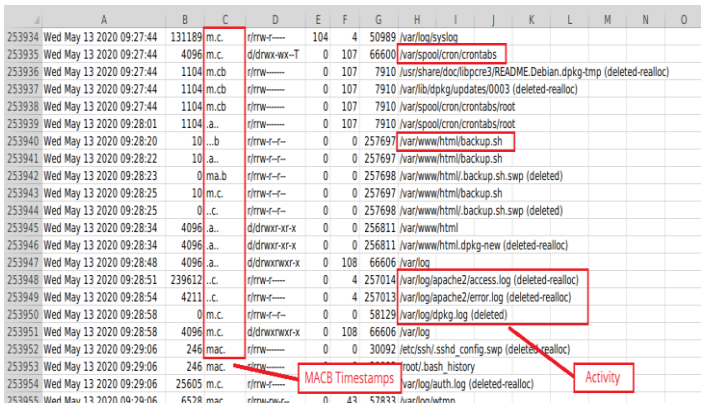
```
root@SIFT-Workstation:~# fls -r -m / ec2victim-volume.dd > ec2victim-volume-filesyste
root@SIFT-Workstation:~# mactime -b ec2victim-volume-filesystembody -d > ec2victim-fi
e.csv
```

Gambar 11 Membuat File System Timeline

Analisa EBS (EC2 Snapshot Image)

Analisa Timeline File System

Gambar 12 dibawah memperlihatkan struktur data filesystem timeline. Artefak ini sudah memberikan gambaran aktivitas suspect dalam mengakses file dan direktori (last access, modification dates). Dengan begitu peneliti dapat menelusuri rangkaian aktivitas yang dilakukan attacker.



	A	B	C	D	E	F	G	H
253934	Wed May 13 2020 09:27:44	131189	m.c.	r/rrw-r-----	104	4	50989	/var/log/syslog
253935	Wed May 13 2020 09:27:44	4096	m.c.	d/drwx-wx--T	0	107	66600	/var/spool/cron/crontabs
253936	Wed May 13 2020 09:27:44	1104	m.cb	r/rrw-------	0	107	7910	/usr/share/doc/libpcre3/README.Debian.dpkg-tmp (deleted-realloc)
253937	Wed May 13 2020 09:27:44	1104	m.cb	r/rrw-------	0	107	7910	/var/lib/dpkg/updates/0003 (deleted-realloc)
253938	Wed May 13 2020 09:27:44	1104	m.cb	r/rrw-------	0	107	7910	/var/spool/cron/crontabs/root
253939	Wed May 13 2020 09:28:01	1104	.a..	r/rrw-------	0	107	7910	/var/spool/cron/crontabs/root
253940	Wed May 13 2020 09:28:20	10	...b	r/rrw-r--r--	0	0	257697	/var/www/html/backup.sh
253941	Wed May 13 2020 09:28:22	10	.a..	r/rrw-r--r--	0	0	257697	/var/www/html/backup.sh
253942	Wed May 13 2020 09:28:23	0	ma.b	r/rrw-r--r--	0	0	257698	/var/www/html/.backup.sh.swp (deleted)
253943	Wed May 13 2020 09:28:25	10	m.c.	r/rrw-r--r--	0	0	257697	/var/www/html/backup.sh
253944	Wed May 13 2020 09:28:25	0	..c.	r/rrw-r--r--	0	0	257698	/var/www/html/.backup.sh.swp (deleted)
253945	Wed May 13 2020 09:28:34	4096	.a..	d/drwxr-xr-x	0	0	256811	/var/www/html
253946	Wed May 13 2020 09:28:34	4096	.a..	d/drwxr-xr-x	0	0	256811	/var/www/html.dpkg-new (deleted-realloc)
253947	Wed May 13 2020 09:28:48	4096	.a..	d/drwxrwxr-x	0	108	66606	/var/log
253948	Wed May 13 2020 09:28:51	239612	..c.	r/rrw-r-----	0	4	257014	/var/log/apache2/access.log (deleted-realloc)
253949	Wed May 13 2020 09:28:54	4211	..c.	r/rrw-r-----	0	4	257013	/var/log/apache2/error.log (deleted-realloc)
253950	Wed May 13 2020 09:28:58	0	m.c.	r/rrw-r--r--	0	0	58129	/var/log/dpkg.log (deleted)
253951	Wed May 13 2020 09:28:58	4096	m.c.	d/drwxrwxr-x	0	108	66606	/var/log
253952	Wed May 13 2020 09:29:06	246	mac.	r/rrw-------	0	0	30092	/etc/ssh/.sshd_config.swp (deleted-realloc)
253953	Wed May 13 2020 09:29:06	246	mac.	r/rrw-------				/root/.bash_history
253954	Wed May 13 2020 09:29:06	25605	m.c.	r/rrw-r-----				/var/log/auth.log (deleted-realloc)
253955	Wed May 13 2020 09:29:06	6528	mac.	r/rrw-rw-r--	0	43	57833	/var/log/wtmp

Gambar 1 Artefak Filesystem Timeline (MACB)

Log yang di generate tool fls secara default time zone nya adalah UTC, jika dikonversi ke Jakarta Time selisih +7 jam. Gambar 13 dibawah menunjukkan 2 log entries ketika attacker mendapatkan akses ke sistem yang mengindikasikan attacker menghapus file log untuk menghapus jejak (covering track). Dari petunjuk ini peneliti sudah mendapat petunjuk tentang kapan aktivitas post exploitation sedang terjadi.

Gambar 13 Bukti Potensial Serangan pada File System Timeline

Pada bukti timeline ini, peneliti memperoleh beberapa aktivitas mencurigakan lainnya yang ditampilkan pada tabel 3. Beberapa aktivitas di tabel tersebut sudah peneliti

konversi ke timezone Jakarta Time. Berdasarkan urutan data baris aktivitas mencurigakan tabel di bawah dapat peneliti simpulkan jika fase post exploitation attacker berlangsung selama satu hari tepatnya 9 Maret 2021.

Tabel 4 Temuan Aktivitas Mencurigakan pada File System Timeline

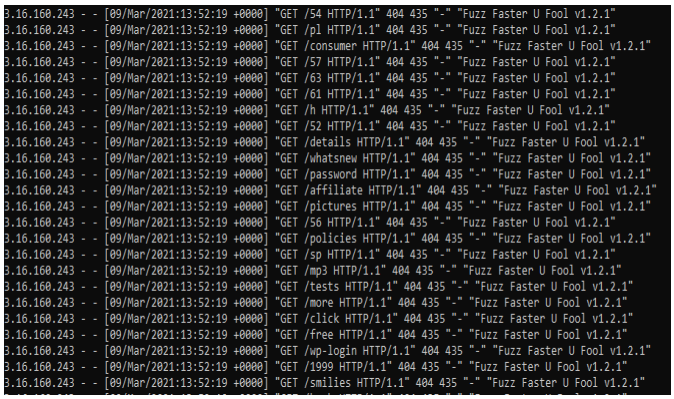
Date	UTC Time	Jakarta Time	UID/GID	Filename
Mar 09 2021	14:00:22	21:00:22	0 (root)	"/var/log/auth.log.1 (deleted)"
Mar 09 2021	14:00:22	21:00:25	0 (root)	"/var/log/dpkg.log (deleted)"

Analisa Log Files

Fokus utama setelah memperoleh informasi penting pada tahap filesystem timeline maka perlu dilakukan analisis file log yang bisa peneliti akses langsung ke direktori /var pada disk EC2 Victim yang sudah di mount. Berdasarkan informasi aktivitas yang dibuktikan pada artefak file system timeline, peneliti tidak menemukan indikasi attacker mendownload file seperti malware, sehingga fokus utama analisis tahap ini lebih ke file log linux yang berada di /var/log/. Beberapa log yang menjadi fokus analisis peneliti antara lain :

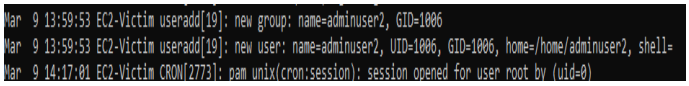
a. /var/log/auth.log : File log ini menyimpan semua event authentication dan cron job session.
b. /var/log/deamon.log : Log ini menyimpan user activites yang di generate background daemons.
c. /var/log/syslog : File log ini menyimpan linux system messages, seperti eksekusi cron job.
d. Access log (/var/log/apache2/access.log) dan error log (/var/log/apache2/error.log) : Log ini dihasilkan oleh service apache. Pada access.log tersimpan semua informasi http request yang berasal dari client. Sedangkan error.log dihasilkan ketika adanya error pemrosesan request (upaya mengakses file yang tidak mendapat permission).

File logs sudah tentu menjadi file artefak yang sangat penting dalam proses investigasi, banyak informasi berharga dapat dianalisa dengan mudah. Merujuk pada ditemukannya waktu aktivitas mencurigakan pada tahap analisis timeline, peneliti menggunakan acuan waktu tersebut dalam memfilter log. Peneliti menemukan beberapa suspicious activity yaitu pada 9 Maret 2021 UTC 13:52 yang berasal dari artefak file access.log. Gambar 14 menunjukkan log serangan dictionary attack. Access log menunjukkan ip address pelaku, payload bruteforce, path target serangan, http method, http response dari server, dan timestamp serangan.



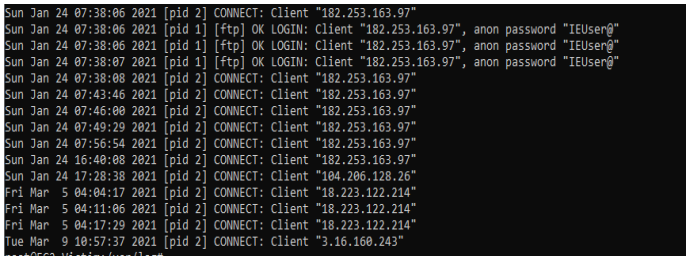
Gambar 14 Aktifitas Bruteforce Tercatat di Access.log

Gambar 15 di bawah menunjukkan bahwa attacker pada tahap ini sudah memiliki akses pada sistem. Dibuktikan dengan aktivitas attacker yang mencoba membuat user baru (adminserver2). Dengan adanya bukti attacker mampu melakukan tindakan ini, ada kemungkinan indikasi bahwa attacker sudah mendapatkan akses sudo bahkan root (privilege escalation).



Gambar 15 Bukti Attacker Membuat User Baru

Sampai tahap ini, sudah cukup memberikan bukti kuat mengenai alur serangan yang sudah terjadi. Peneliti mendapatkan informasi penting lainnya dari log vsftpd berupa percobaan akses ftp dari suspect ip 3.16.160.243 pukul 20:57:36 (Jakarta Time).



Gambar 16 Akses Ftp dari Suspect Ip Attacker

Reporting

Pada tahap ini merupakan hasil akhir analisa proses investigasi. Bagian ini menjelaskan detail hasil analisa yang memungkinkan dalam mengungkap kasus skenario serangan. Analisa barang bukti secara mendalam pada artefak yang ada, membuktikan fase attacker dalam melancarkan skenario serangan.

Pada skenario serangan post-exploitation, kondisi dimana hacker sudah mendapatkan akses penuh dan mencoba melakukan tindakan privilege escalation, maintaining access, bahkan covering track dapat peneliti buktikan. Berdasarkan analisa timeline filesystem sudah cukup memperkuat bukti adanya perubahan di sisi data dan direktori EC2 Victim, yang berarti attacker sudah benar benar mendapat akses penuh. Dari artefak file system timeline dan beberapa log peneliti memperoleh waktu attacker mendapat akses instance EC2 Victim.

Beberapa bukti data indikasi serangan dari temuan evidence ditunjukkan pada tabel 4. Timestamp pada tabel sudah Peneliti convert ke Jakarta time (UTC +7). Skenario web path brute force dan tahap eksploitasi dibuktikan berdasarkan artefak access.log dan vsftpd.log. Sedangkan skenario menjalankan malware backdoor tidak berhasil peneliti buktikan. Untuk fase post exploitation maintaining access bisa diungkap berdasarkan artefak auth.log. Skenario fase serangan tahap akhir yaitu covering track mampu peneliti buktikan dengan menganalisa artefak filesystem timeline.

Tabel 5 Laporan Akhir Analisa Indikasi Serangan Tahap Post Exploitation

Phase	Serangan	Hasil	Sumber Artefak	Timestamp Kejadian (Jakarta Time)
Information Gathering & Exploitation	Web Path Bruteforce	Ditemukan	/var/log/access.log	2021-03-09 (20:52:19)
	Exploitation (Compromised Instance)	Ditemukan	/var/log/vsftpd.log	2021-03-09 (20:57:37)
Post Exploitation	Menjalankan backdoor	Tidak Ditemukan	-	-
	Maintaining Access	Ditemukan	/var/log/auth.log	2021-03-09 (20:59)
	Covering Track	Ditemukan	File system Timeline	2021-03-09 (21:00:22)

SIMPULAN

Berdasarkan proses yang telah dilakukan sebelumnya, penggunaan metode NIST dalam investigasi forensik memperoleh alur penelitian yang sistematis dan dapat dijadikan acuan dalam penelitian. Pada skenario aktivitas hacking yang peneliti buat dalam rancangan simulasi, peneliti berhasil menganalisa sekaligus mengurai alur dari aktivitas hacking yang dilakukan dengan menerapkan teknik disk & *file system forensik* dengan dibantu beberapa tools. Analisa pada temuan *artefak log* dan *filesystem* dapat membuktikan aktivitas serangan yang dilakukan pelaku pada saat proses hacking berlangsung. Pada phase *Information Gathering & Exploitation* di temukan dua serangan yang dilakukan attacker yaitu *Web Path Bruteforce* di sumber artefak */var/log/access.log* dan *Exploitation (Compromised Instance)* di sumber artefak */var/log/vsftpd.log*, sedangkan pada phase *Post Exploitation* ditemukan 2 serangan yaitu *Maintaining Access* di sumber artefak */var/log/auth.log* dan *Covering Track* di sumber artefak file system timeline.

DAFTAR PUSTAKA

1]. E. Morioka and M. S. Sharbaf. (2016). Digital forensics research on cloud computing: An investigation of cloud forensics solutions. 2016 IEEE Symposium on Technologies for Homeland Security (HST), pp. 1-6. https://doi.org/10.1109/THS.2016.7568909

2]. Y. Hung. (2019). Investigating How the Cloud Computing Transforms the Development of Industries. in *IEEE Access*, vol. 7, pp. 181505-181517, https://doi.org/10.1109/ACCESS.2019.2958973

3]. P. R. Agbedanu, P. Wang, R. N. Nortey and L. K. Odartey. (2019). Forensics in the Cloud: A Literature Analysis and Classification. 2019 5th International Conference on Big Data Computing and Communications (BIGCOM), pp. 124-132. https://doi.org/10.1109/BIGCOM.2019.00027

4]. Gartner. (2018). Gartner Says 28 Percent of Spending in Key IT Segments Will Shift to the Cloud by 2022 (Online). https://www.gartner.com/

5]. Columbus, L. (2018). 83% Of Enterprise Workloads Will Be In The Cloud By 2020 (Online). https://www.forbes.com/

6]. Coles, C. (n.d.)(2017). AWS vs Azure vs Google cloud market share 2017. https://www.skyhighnetworks.com

7]. E. Morioka and M. S. Sharbaf. (2016).)Digital forensics research on cloud computing: An investigation of cloud forensics solutions. 2016 IEEE Symposium on Technologies for Homeland Security (HST), pp. 1-6, https://doi.org/10.1109/THS.2016.7568909

8]. Yudhistira, D & Riadi, I & Prayudi, Y. (2018). Live Forensics Analysis Method For Random Access Memory On Laptop Devices. International Journal of Computer Science and Information Security,. 16.

9]. Simou, S., Kalloniatis, C., Kavakli, E., Gritzalis, S. (2014). Cloud Forensics: Identifying the Major Issues and Challenges. In: , *et al*. Advanced Information Systems Engineering. CAiSE 2014. Lecture Notes in Computer Science, vol 8484. Springer, Cham. https://doi.org/10.1007/978-3-319-07881-6_19

10]. G. Grispos, T. Storer, and W.B. Glisson (2012). Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics. International Journal of Digital Crime and Forensics, Volume 4,Issue 2, Pages 28-48 https://doi.org/10.4018/jdcf.2012040103

11]. Yudhana, A., Riadi, I., & Anshori, I. (2018). Identification Of Digital Evidence Facebook Messenger On Mobile Phone With National Institute Of Standards Technology (Nist) Method. *Jurnal Ilmiah Kursor*, *9*(3). https://doi.org/10.28961/kursor.v9i3.152

12]. Yudhana, A., Riadi, I., & Anshori, I. (2018). Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist. *IT Journal Research and Development*, *3*(1), 13 - 21. https://doi.org/10.25299/itjrd.2018.vol3(1).1658

13]. Dykstra, J., & Sherman, A.T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digit. Investig.*, *9*, S90-S98. https://doi.org/10.1016/j.diin.2012.05.001

14]. Mualfah, D., & Ramadhan, R.A. (2020). Analisis Digital Forensik Rekaman Kamera CCTV Menggunakan Metode NIST (National Institute of Standards Technology).

15]. Nasirudin, Nasirudin & Sunardi, Sunardi & Riadi, Imam. (2020). Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express. Jurnal Informatika Universitas Pamulang. 5. 89. https://doi.org/10.32493/informatika.v5i1.4578

16]. Imam R, Abdul F, & Muhammad I A. (2020). Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST). *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(5), 820-828. https://doi.org/10.29207/resti.v4i5.2224

17]. Yasin, F., Abdul Fadlil, & Rusydi Umar. (2021). Identifikasi Bukti Forensik Jaringan Virtual Router Menggunakan Metode NIST. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *5*(1), 91 - 98. https://doi.org/10.29207/resti.v5i1.2784