Penanganan Insiden pada Subsistem Remote Backup dan Recovery pada Sistem Terdistribusi untuk Proteksi Web Server

Tugas Akhir Mata Kuliah Secure Operation
dan Incident Handling
EL6115

Oleh
AULIAK AMRI
NIM: 23215077
Program Studi Magister Teknik Elektro

SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA
INSTITUT TEKNOLOGI BANDUNG
2016

Daftar Isi

Pendahuluan

Backup dan recovery data merupakan proses penting dalam suatu sistem untuk menjaga integritas sistem dan data pengguna. Kehilangan dan kerusakan data pada sistem dapat disebabkan oleh beberapa hal diantaranya hardware atau software failure, kerusakan yang disengaja maupun tidak disengaja, seperti bencana alam, dan lain sebagainya. Backup dilakukan dengan membuat salinan data secara berkala sehingga dapat dilakukan recovery pada data yang rusak atau hilang [1]. Dengan demikian, backup dan recovery tidak hanya menjaga pertahanan sistem tetapi juga dalam disaster recovery [2].

Metode backup dan recovery ditentukan dalam tahap perencanaan sistem sesuai dengan kebutuhan dan kebijakan organisasi, apakah salinan data tersedia online atau offline, disimpan secara lokal atau ditransmisikan ke remote site. Pada setiap metode terdapat trade off yang perlu dipertimbangkan yaitu kemudahan implementasi dan biaya terhadap keamanan dan ketahanan sistem [1]. Remote backup menjadi pilihan karena apabila attacker berhasil menyerang sistem maka semua data di dalam server tidak dapat lagi dipercaya, yang kemudian perlu dilakukan recovery data yang berasal dari remote site [2]. Metode backup ini menggunakan multi version control, transfer data dilakukan dengan Rsync [3], dan File Transfer Protocol (FTP), standar protokol jaringan yang digunakan dalam proses transmisi data [2]. Selain itu, ada juga beberapa teknik dalam backup dan recovery pada lingkungan cloud, seperti RAID, HSDRT, PCS, ERGOT, Linux Box, Cold and Hot Backup Technique, SBBR, REN, dan sebagainya [4].

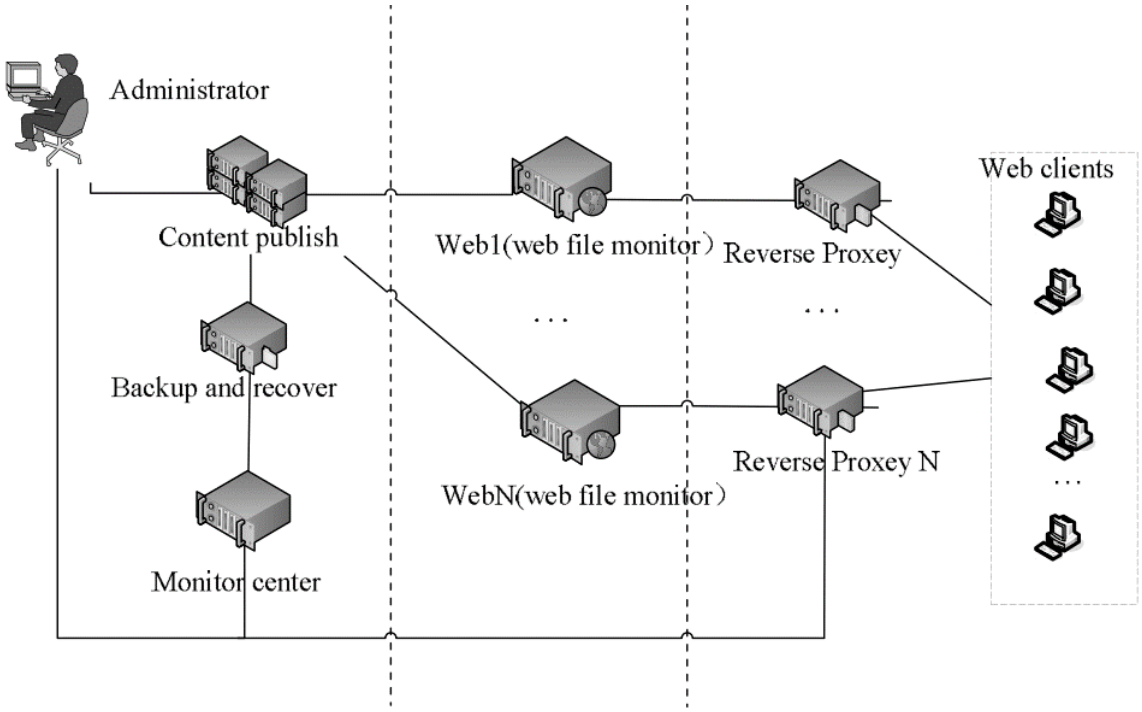
Proses transmisi file backup menggunakan rsync memerlukan akses ke remote backup server dengan Secure Shell (SSH). Namun demikian, salah satu target serangan yang paling sering digunakan oleh attacker adalah server yang memiliki service remote access, yaitu SSH [5]. SSH terutama digunakan untuk akses file dan sebagai tunnel antar protokol pada layer aplikasi. SSH menyediakan proses otentikasi, enkripsi, dan integritas data [6]. Attacker dapat melakukan percobaan login dan apabila berhasil, remote access ke server dapat dilakukan. Attacker dapat menggunakannya untuk melakukan kegiatan berbahaya, seperti pemasangan malware hingga penggunaan server tersebut untuk menyerang sistem yang lain [5]. Selain itu, transfer file menggunakan protokol FTP memiliki kelemahan keamanan yaitu FTP Brute Force Attack, Packet Capture (atau Sniffing), Spoof Attack, Port Stealing, dan FTP Bounce Attack [7].

Makalah ini membahas berbagai macam metode dan keamanan backup dan recovery serta bagaimana penanganan insiden pada remote backup dan recovery. Batasan makalah ini adalah pada pembahasan metode, analisis keamanan, dan penanganan insiden pada subsistem remote backup dan recovery. Backup dan recovery model yang digunakan adalah subsistem dari sistem terdistribusi yang merupakan sistem untuk memproteksi web server [8].

Arsitektur Sistem

Sistem terdistribusi

Backup dan recovery model adalah subsistem dari sistem terdistribusi yang merupakan sistem untuk memproteksi web server [8]. Sistem ini terdiri dari sub sistem monitor web file, content publish, reverse proxy, backup dan recovery, dan monitor center. Sistem dapat digambarkan sebagai berikut.



Gambar 1.Arsitektur Sistem Terdistribusi [2]

Subsistem backup dan recovery membuat salinan file program dari suatu website. Pada subsistem ini file backup dapat direcovery saat file website hilang ataupun telah dimodifikasi secara illegal. Remote dan backup yang dilakukan adalah berdasarkan pada subsistem ini.

Backup dan restore model

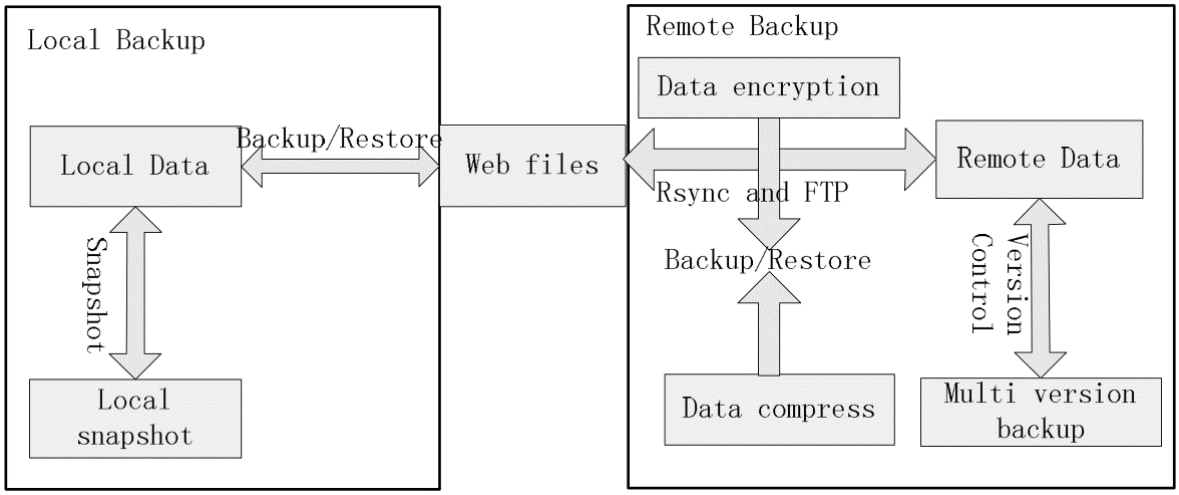
Model sistem backup dan recovery terdiri dari sistem local backup dan remote backup. Local backup menggunakan teknologi snapshot. Jika file snapshot rusak maka data tidak dapat direstore. Oleh karena itu, sistem tidak dapat hanya bergantung pada local backup. Untuk melindungi keamanan web server, file backup ditransmisikan ke remote backup server dan administrator dapat menentukan strategi backup.

Ada beberapa strategi pada remote backup yaitu full, differential, dan incremental. Full backup membuat salinan data keseluruhan oleh karenanya membutuhkan tempat yang lebih besar. Differential backup hanya membuat salinan untuk file mengalami perubahan saja sehingga menjadi lebih cepat. Terakhir, incremental backup yang memiliki kinerja yang lebih baik.

Administrator dapat memilih strategi backup sesuai dengan kebutuhan. Pada strategi incremental differential backup, terdapat mode yang bisa dipilih yaitu text dan file mode. Pada text mode setiap baris diperiksa, sedangkan pada file mode hanya mengecek apakah keseluruhan file mengalami perubahan atau tidak.

Version control management digunakan pada backup dengan text mode. Selama berjalannya waktu, file backup akan terus bertamah. Version control management digunakan agar administrator dapat memilih data backup pada periode waktu kapan yang akan direstore.

Pada proses backup dan restore, semua data diperoleh berdasarkan Rsync. Setelah itu, data backup dicompress dan ditransfer menggunakan protokol FTP pada jaringan sehingga dapat memperbaiki kecepatan backup dan restore serta mengurangi network load.



Gambar 2.Model Backup dan Recovery [2]

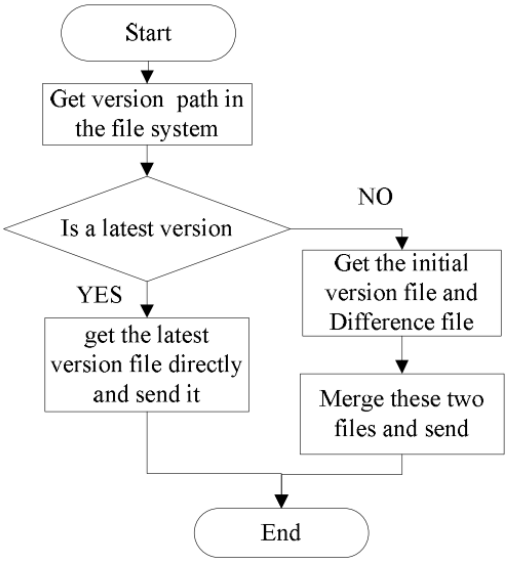
Text Version Control Management

Sistem version control memiliki karakteristik sebagai berikut:

(1) menggunakan versi dari directory tree untuk mengimplementasikan perubahan untuk melihat virtual version dari file system, file, dan directory
(2) merekam alasan perubahan dan modifikasi
(3) mendapatkan perbedaan antara suatu versi backup dengan local copy
(4) saat dua pengguna memodifikasi file, sistem secara otomatis akan menggabungkan perubahan
(5) mencegah modifikasi yang tanpa hak dan akses.

Tujuan dari perbandingan versi backup adalah untuk mendapatkan perbedaan antar dokumen yang sama dengan versi yang berbeda. Pembuatan differential file oleh sistem dilakukan berdasarkan dua rule yaitu operasi tambah dan operasi hapus.

Subsistem backup dan recovery menghasilkan versi yang baru saat subsistem content distribution memperbaharui website di web server. Saat web server secara ilegal dimodifikasi maka sub-module recovery akan menerima perintah restore dari pusat monitoring, kemudian menganalisis printah. Kemudian version control module mengekstrak versi backup dan mengirimkannya ke web server. Proses ini digambarkan pada bagan berikut.

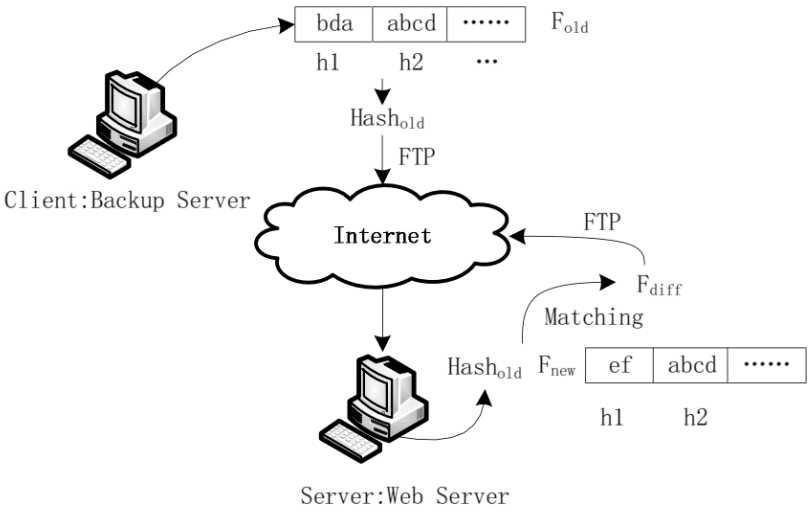


Gambar 3.Mekanisme Kontrol Versi Backup [2]

Remote transmission dan backup/recovery

Sinkronisasi dan Transmisi File

Dalam proses backup dan recovery, algoritma sinkronisasi dan transmisi file sangat mempengaruhi kecepatan. Rscyn dan protokol FTP standar dapat dipilih untuk proses tersebut. Dalam proses sinkronisasi, web server bekerja sebagai server dan backup server bekerja sebagai client. Client memeriksa data pada server secara rutin. Jika ada perubahan maka client akan mengirimkan permintaan sinkronisasi ke web server untuk memperbaharui data [2].



Gambar 4.Mekanisme Sinkronisasi dan Transmisi [2]

Misalnya, file pada client adalah F_{old} dan file pada server adalah F_{new}, maka F_{old} akan disinkronisasi menjadi F_{new}. Proses pengiriman F_{new} dapat dilakukan secara langsung dan sederhana, tetapi memiliki banyak kelemahan, khusunya ketika kecepatan jaringan lambat, pengiriman file akan menjadi sangat lama.

Algoritma rscync dapat menentukan perbedaan antara F_{old} dan F_{new} yaitu F diff. Perbedaan file tersebut ditransmisikan menggunakan protokol FTP, yang merupakan protokol jaringan standar yang digunakan untuk mentransmisikan file dari satu host ke host lain melalui TCP-based network.

Dalam proses sinkronisasi, F_{old} digunakan untuk menghasilkan F_{new}. Metode sinkronisasi dan transmisi terbagi dalam tiga tahap seperti terlihat pada gambar.

Tahap 1

Pada backup server, file yang akan disinkronisasi, F_{old}, dibagi menjadi beberapa blok. Tabel hash yang berisi 124 bit MD4 dan 32 bit checksum dihitung untuk tiap blok. Semua checksum dari semua file yang perlu disinkronisasi dihitung dan disimpan sebagai file checksum.

Tahap 2

Setelah menerima pesan permintaan, Server memeriksa checksums dan menghasilkan tabel hash untuk F_{new}, yaitu file kondisi terbaru. Jika tabel hash ini sama dengan hash yang dikirim oleh client berarti tidak ada perubahan. Jika berbeda, maka F diff, yaitu perbedaan file antara client dan server, perlu dibuat dan ditransmisikan ke backup server.

Tahap 3

Setelah menerima F diff, backup server akan membangun kembali F_{old} dan juga membuat temp file. Berdasarkan file F diff, blok yang tiak berubah disalin secara langsung ke temp file sedangkan file yang berubah disalin dari F diff sehingga temp file akan menjadi sama dengan F_{new} di server. Proses sinkronisasi selesai setelah F_{old} diganti oleh temp file.

Proses remote backup dan recovery

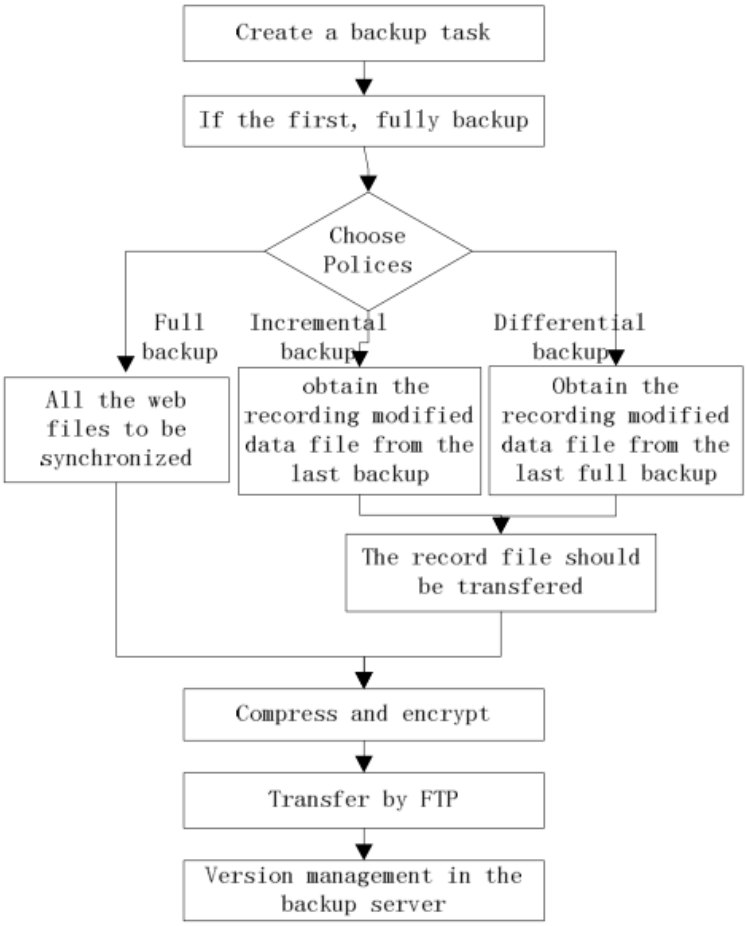
Pada remote backup administrator dapat memilih sumber backup, membuat backup task baru, dan memilih strategi backup. Proses backup dan recovery secara keseluruhan digambarkan pada flowchart berikut.

Tahap 1

Customer membuat backup task baru. Jika ini merupakan yang pertama kalinya maka full backup akan dijalankan secara otomatis. Jika tidak, strategi backup akan didefinisikan seperti yang diinginkan.

Tahap 2

File yang akan dibackup dioperasikan secara berbeda-beda berdasarkan strategi backup. Jika yang dijalankan adalah full backup maka semua file akan disinkronisasikan ke backup server. Berbeda dengan incremental backup, file yang baru ditambah atau dimodifikasi akan simpan pada temp file. Sedangkan pada differential backup, file yang akan dibackup ditentukan berdasarkan proses full backup yang dijalankan terakhir.



Gambar 5.Proses Remote Backup dan Recovery [2]

Tahap 3

Semua file yang meliputi file full backup dan temp file untuk incremental ataupun differential kemudian ditransmisikan ke backup server melalui protokol FTP. Jika strategi yang dipilih adalah incremental atau differential maka F diff hanya akan disimpan dan ditandai dengan versi backup tertentu dan tidak disinkronisasi. Backup server akan mengelola file tersebut untuk mengontrol versi backup dan proses recovering.

Proses recovery data merupakan proses kebalikan dari proses backup. Jika terjadi bencana atau kejadian yang memerlukan sistem untuk dikembalikan ke kondisi sebelumnya maka remote recovery perlu dilakukan. Administrator hanya perlu memilih folder atau file mana untuk merecover data pada server.

Eksperiman dan Analisis

Pengujian dilakukan dengan melakukan remote backup menggunakan protokol FTP dimana file backup dibuat menjadi beragam ukuran dari 1Mb hingga 51Mb, dan ada 10 persen perubahan data pada server. Hasilnya adalah jika kecepatan jaringan tidak terbatas maka metode rsync lebih lambat dibandingkan dengan FTP. Namun demikian, saat ukuran file lebih dari 11Mb, kecepatannya akan sama. Jika kecepatan jaringan 1 Mbps, maka rsync lebih baik dibandingkan FTP. Namun saat ukuran file 51 Mb, waktu untuk backup dapat dihemat hingga 86 percent dengan menggunakan rsync.

Metode Backup dan Restore

Pada subsistem backup dan restore di dalam sistem terdistribusi, terdapat metode yang dilakukan untuk melakukan backup dan restore yaitu pembentukan file backup dengan database dump, dan transmisi file backup ke remote backup server. Pembuatan database dump dilakukan pada database MySQL dengan perintah `mysqldump`, proses transmisi file backup dilakukan dengan menggunakan rsync-SSH dan FTP.

Database dump

Database dump merupakan file backup database yang berisi struktur tabel atau data dari database yang pada umumnya berupa script SQL [9]. Metode ini merupakan cara yang biasa digunakan untuk melakukan backup database sehingga dapat direstore ketika terjadi kehilangan atau kerusakan data pada database.

```sql
-- Database
CREATE DATABASE `example`;
USE `example`;

-- Table structure for table `users`
CREATE TABLE `users` (
  `id` int(8) unsigned NOT NULL AUTO_INCREMENT,
  `username` varchar(16) NOT NULL,
  `password` varchar(16) NOT NULL,
  PRIMARY KEY (`id`)
);

-- Data for table `users`
INSERT INTO `users` VALUES (1,'alice','secret'),(2,'bob','secret');
```

Gambar 6. Contoh isi file database dump

Database dump dilakukan dengan logical backup yaitu dengan memproduksi struktur tabel dan data tanpa menyalin file data sebenarnya. Output dari logical backup berupa pernyataan sql seperti `CREATE TABLE` dan `INSERT` yang dapat membangun kembali database. Kelebihan logical database adalah file backup dapat dimodifikasi definisi tabelnya sebelum dilakukan restore, tetapi waktu untuk melakukan restore lebih lama dibandingkan physical backup [10].

Pada database MySQL misalnya, logical backup dilakukan dengan perintah `mysqldump`. Perintah ini akan menghasilkan pernyataan SQL yang dapat dieksekusi untuk membangun kembali definisi dan data tabel dari database. hasil dari MySQL dump ini dapat digunakan untuk backup maupun transfer ke SQL server lain [11].

Backup Database MySQL pada sistem operasi Linux dilakukan menggunakan terminal dengan perintah dasar sebagai berikut [12].

```
mysqldump -u username -p database_to_backup > backup_name.sql
```

Untuk melakukan restore, terlebih dahulu login ke MySQL, setelah itu buat database baru dengan perintah sebagai berikut.

```
mysql -u username -p
CREATE DATABASE database_name;
Exit
```

File dump kemudian direstore ke database yang baru dibuat dengan perintah sebagai berikut.

```
mysql -u username -p database_name < backup_name.sql
```

Skalabilitas dan Kinerja `mysqldump`

Backup database dengan cara ini dapat memberikan fleksibilitas dan kemudahan karena sebelum direstore dapat dilihat dan bahkan dimodifikasi. Namun demikian, cara ini tidak dimaksudkan untuk backup data dengan skala besar. Pada data yang sangat besar, meskipun backup dilakukan tidak lama, proses restore data akan menjadi sangat lambat karena menjalankan pernyataan SQL melibatkan I/O disk, pembuatan index, dan sebagainya. Oleh karena itu, untuk backup dan restore data dengan skala besar dapat menggunakan physical backup untuk membuat salinan file data dalam format asli dan dapat direstore dengan cepat [11].

Physical backup merupakan backup dengan cara membuat salinan file data sebenarnya. Operasi physical melibatkan aspek terkait hardware seperti disk blocks, memory pages, files, bits, disk reads, dll. Physical backup pada MySQL dilakukan dengan menggunakan command `mysqlbackup`. Output backup ini berisi file data yang dapat digunakan secara langsung oleh mysqld server sehingga proses restore menjadi lebih cepat [10].

CHECKSUM TABLE

Sintak CHECKSUM TABLE menampilkan checksum dari isi sebuah tabel. Checksum digunakan untuk memverifikasi isi tabel adalah sama dengan keadaan sebelum dan setelah dilakukannya backup, rollback, atau operasi lainnya yang dilakukan untuk mengembalikan data ke keadaan tertentu. Nilai checksum tergantung dari format tabel. Jika format berubah, maka checksum akan berubah [13]. Pada MySQL perintah innochecksum mendiagnosa masalah corruption dengan menguji nilai checksum untuk tablespace tertentu. MySQL juga menggunakan checksum untuk tujuan replikasi [10].

Algoritma Rsync

Backup dilakukan dengan membuat salinan file dari backup client ke backup server. Jika file backup memiliki ukuran yang besar maka proses pengirimannya akan menjadi lama dan tidak efisien. Metode yang biasa digunakan adalah dengan hanya mengirimkan perbedaan file antara backup client dan backup server dan kemudian membangun kembali file backup pada backup server menggunakan file yang dikirim.

Algoritma rscync dapat menghitung secara efisien bagian mana dari file sumber yang match dengan file tujuan. Jadi, hanya bagian dari file sumber yang tidak match yang akan dikirim untuk kemudian membangun kembali file tujuan [3], yaitu file backup di backup server. Algoritma rsync dijabarkan sebagai berikut.

Diasumsikan terdapat dua buah computer α dan β. Computer α memiliki akses ke file A dan computer β memiliki akses ke file B, dimana A dan B adalah file yang sama. Algoritma rsync memiliki langkah-langkah sebagai berikut.

1. Computer β membagi file B menjadi rangkaian blok dengan ukuran S bytes dengan ukuran yang sama dan tidak ada overlapping. Blok terakhir bisa memiliki ukuran yang lebih kecil dari S bytes.
2. Untuk setiap blok ini, computer β menghitung dua checksum, yaitu 32 bit checksum dan 128 bit MD4 checksum.
3. Computer β mengirim checksum ini ke computer α.

4. Computer α melakukan pencarian pada file A untuk menemukan semua blok dengan panjang S bytes yang memiliki checksum yang sama dengan blok pada file B.
5. Computer α mengirim ke computer β sebuah rangkaian perintah untuk membangun salinan file A. Perintah ini berupa referensi ke blok file B ataupun berupa data. Data ini hanya dikirim untuk bagian dari file A yang tidak match dengan blok manapun pada file B.

Hasil akhirnya adalah computer β menapatkan salinan file A, tetapi hanya bagian file A yang tidak ditemukan pada file B.

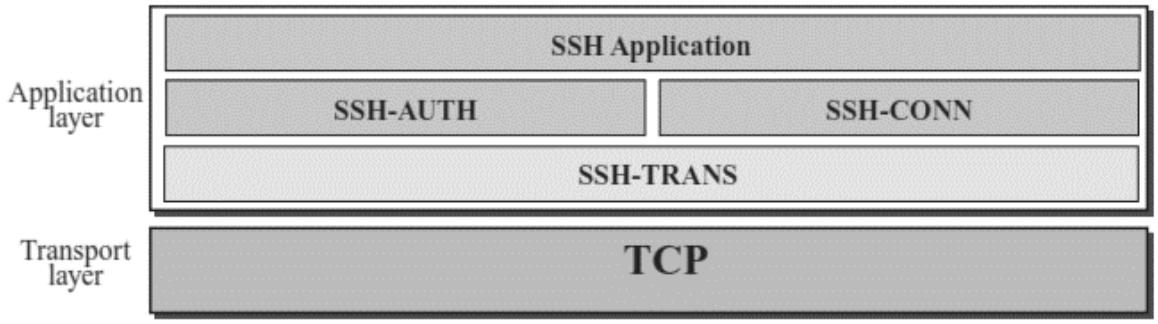
Secure Shell (SSH)

Dalam proses sinkronisasi file antara dua sistem, rsync menggunakan SSH untuk membuat koneksi ke remote host [14]. Berikut ini adalah contoh perintah menggunakan rsync.

```
rsync local-file user@remote-host:remote-file
```

Perintah diatas menunjukkan bahwa rsync akan melakukan sinkronisasi `local-file` dengan `remote-file` yang berada di `remote-host`. Rsync menggunakan SSH untuk membuat koneksi ke `remote-host` sebagai `user`.

SSH merupakan salah satu aplikasi yang digunakan untuk remote login. Ada dua versi SSH yaitu SSH-1 dan SSH-2 yang tidak kompatibel satu dengan yang lainnya. Versi pertama SSH saat ini sudah tidak digunakan karena memiliki kelemahan keamanan. SSH merupakan protokol pada layer aplikasi dengan empat komponen yaitu aplikasi SSH, SSH-AUTH, SSH-CONN, dan SSH-TRANS [15].



Gambar 7.Komponen SSH

SSH Transport-Layer Protocol (SSH-TRANS)

SSH adalah protokol yang membuat secure channel di atas protokol TCP. Layer ini merupakan protokol independen yang disebut dengan SSH-TRANS. Ketika suatu aplikasi menggunakan protokol ini, terlebih dahulu client dan server menggunakan protokol TCP untuk membentuk koneksi yang tidak aman (insecure proconnection). Setelah itu, beberapa parameter keamanan saling dipertukarkan untuk membentuk secure channel di atas protokol TCP. Service yang disediakan oleh protokol ini yaitu sebagai berikut.

1. Kerahasiaan pesan yang dipertukarkan.
2. Integritas data, yaitu pesan yang dipertukarkan dijamin untuk tidak diubah oleh attacker.
3. Autentikasi server, yaitu client yakin bahwa server benar merupakan server yang dimaksud.
4. Kompresi pesan yang memperbaiki efesiensi sistem.

SSH Authentication Protocol (SSH-AUTH)

Setelah secure channel dibentuk antara client dan server dan server terautentikasi, SSH memanggil aplikasi lain yang mengautentikasi client untuk server.

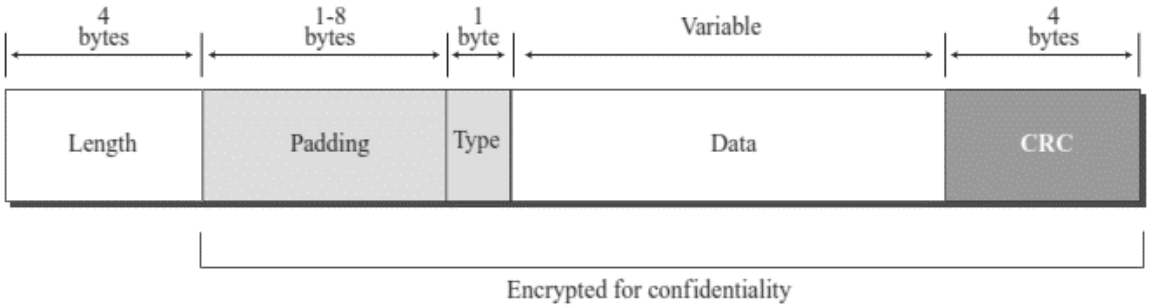
SSH Connection Protocol (SSH-CONN)

Setelah secure channel dan kedua client dan server sudah saling mengautentikasi, SSH memanggil aplikasi yang menjalankan protokol ketiga, yaitu SSH-CONN. Service yang disediakan protokol SSH-CONN adalah multiplexing. SSH-CONN menggunakan secure channel yang telah dibuat sehingga client dapat membuat beberapa channel logic di dalamnya.

SSH Applications

Setelah tahap pembentukan koneksi selesai, SSH mengizinkan beberapa program aplikasi untuk menggunakan koneksi. Tiap aplikasi dapat membuat logical channel dan mendapatkan koneksi yang aman. Remote login merupakan salah satu service yang menggunakan protokol SSH-CONN. Transfer file juga dapat menggunakan salah satu logical channel.

Format Paket SSH



Gambar 8. Format paket SSH

Gambar diatas merupakan format paket yang digunakan oleh protokol SSH. Berikut penjelasan ringkasnya.

a. Length
   Field berukuran 4 byte ini berisi definisi panjang paket.
b. Padding
   Padding berukuran satu hingga delapan byte ditambahkan ke dalam paket untuk membuat serangan keamanan menjadi lebih sulit.
c. Type
   Field berukuran 1 byte ini mendefinisikan tipe paket yang digunakan oleh protokol SSH.
d. Data
   Ukuran field ini bervariasi. Panjang dari data dapat diketahui dengan mengurangi lima bytes dari nilai yang ada pada field length.
e. CRC
   Cyclic Redundancy Check (CRC) digunakan untuk pendeteksian error.

SSH Attack

Serangan terhadap protokol SSH umum dilakukan oleh attacker karena serangan ini mudah dilakukan dengan melakukan brute-force untuk menebak informasi username dan password dari SSH. Saat ini telah banyak tools yang mudah digunakan untuk melakukan serangan secara otomatis, yaitu dengan metode serangan brute-force ataupun dictionary-based.

Analisis dan Visualisasi SSH Attack

Sebelum melakukan penyerangan, attacker mencari server di internet yang dapat digunakan untuk kegiatan berbahaya. Server yang menjadi target attacker adalah yang memiliki service remote access seperti Secure Shell (SSH). Attacker kemudian mencoba melakukan koneksi pada server tersebut dengan menggunakan berbagai macam kombinasi informasi autentikasi. Jika berhasil masuk dan mendapatkan remote access ke server, attacker dapat menggunakannya untuk kegiatan berbahaya seperti instalasi malware ataupun menggunakan server tersebut untuk melakukan serangan ke sistem yang lain [5].

Untuk mengidentifikasi pengguna berbahaya dan mendapatkan peringatan awal terhadap kelemahan dan eksploitasi, salah satu perangkat yang dapat digunakan adalah honeypot.

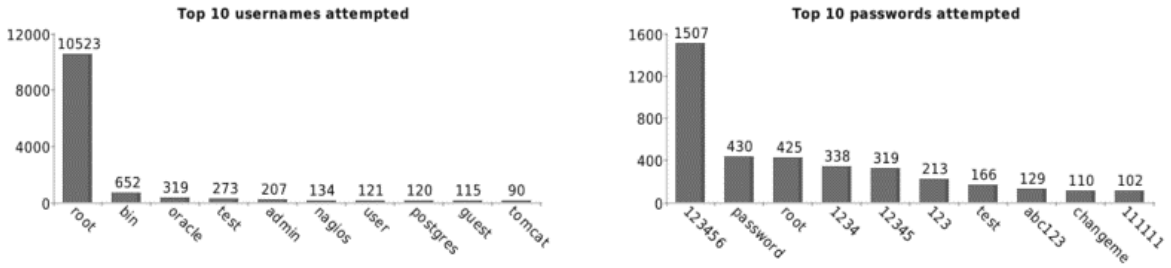
Honeypot dapat mengelabui pengguna berbahaya yang melakukan serangan terhadap server dan infrastruktur jaringan. Sistem ini digunakan sebagai mekanisme proteksi dengan mempelajari dan menganalisis serangan yang dilakukan attacker.

Attacker yang menargetkan service SSH untuk mendapatkan akses server secara ilegal dapat diketahui aktivitasnya melalui honeypot. Sistem tetap berjalan dan dapat menangkap serangan dan melakukan logging semua aktivitas attacker.

Honeypot bekerja dengan konsep bahwa pengguna sah tidak dapat menggunakan atau berinteraksi secara langsung dengannya, oleh sebab itu, segala percobaan komunikasi secara otomatis akan diidentifikasi sebagai serangan [16]. Dengan kata lain, honeypot yang mencoba melakukan koneksi dengan jaringan luar telah terkena serangan oleh attacker [17].

Honeypot merupakan perangkat untuk mengelabui dan menjebak. Perangkat ini dapat menipu pengguna berbahaya dengan bertindak seolah-olah sebagai sistem yang memiliki berbagai macam data dan service. Selama berinteraksi dengan attacker, honeypot melakukan log semua aktivitas. Dengan demikian, administrator dapat mempelajari teknik yang digunakan oleh attacker untuk menyerang.

Data yang dihasilkan honeypot dapat semakin bertambah dengan bertambahnya serangan selama berjalannya waktu. Oleh karena itu, sulit untuk menganalisis data secara manual. Visualisasi data dan analisis visual [18] dapat membantu administrator mendapatkan gambaran data dengan cepat dan rinci.



Gambar 9. Sepuluh username dan password terbanyak yang digunakan pada SSH brute force attack

Dalam percobaanya [5], data yang dihasilkan dari honeypot dilaukan visualisasi. Grafik diatas menggambarkan 10 teratas username dan password yang digunakan oleh sejumlah attacker yang melakukan serangan brute force SSH. Username "root" menjadi yang paling banyak digunakan, sedangkan password yang paling banyak digunakan adalah "123456". Kombinasi username dan password yang digunakan oleh attacker adalah "root" dan "123456". Pada percobaanya, visualisasi juga dilakukan untuk melihat distribusi 10 IP address terbanyak yang melakukan penyerangan beserta lokasi ip address. Honeypot juga mencatat command yang dilakukan oleh attacker. Sepuluh command terbanyak yang dilakukan oleh attacker dapat dilihat pada tabel di bawah.

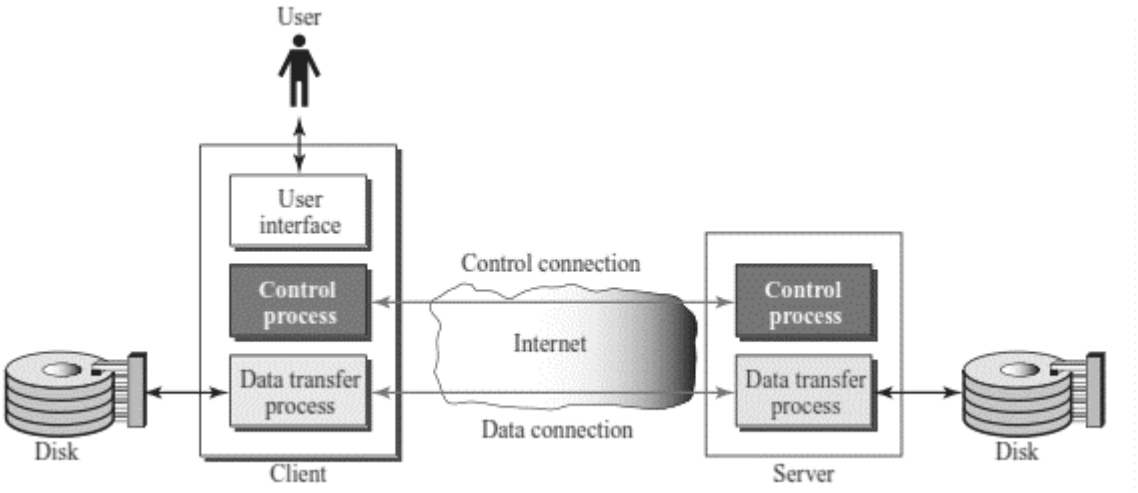
Command	Logged Attempts
w	38
ls –a	26
ls	17
chmod +x *	14
uname –a	12
cat /proc/cpuinfo	12
exit	9
wget	7
ps x	7
passwd	7

Tabel 1. Sepuluh command terbanyak pada SSH brute force attack

File Transfer Protocol (FTP)

File Transfer Protocol (FTP) adalah protokol standar jaringan yang digunakan untuk transfer file antara satu host dengan host lainnya pada suatu jaringan [19]. Beberapa permasalahan dalam transfer file yaitu kedua sistem memiliki sistem penamaan file yang berbeda, cara yang berbeda dalam merepresentasikan text dan data, dan struktur direktori yang berbeda. Semua ini bisa diselesaikan dengan FTP dengan cara yang sederhana.

FTP menggunakan model arsitektur client-server dan memiliki dua koneksi antara dua host, yaitu koneksi untuk transfer data dan informasi kontrol (perintah dan respon). Pemisahan ini membuat FTP menjadi lebih efisien. FTP menggunakan dua port TCP, yaitu Port 21 untuk koneksi kontrol dan port 20 untuk koneksi data.



Gambar 10.Model dasar FTP

Gambar diatas merupakan model dasar dari FTP. Client memiliki tiga komponen yaitu user interface, client control process, dan client data transfer process. Server memiliki dua komponen yaitu server control process dan server data transfer process. Koneksi kontrol dibuat antara dua control process, sedangkan koneksi data dibuat antara dua data transfer process.

Dalam proses transfer file, koneksi kontrol tetap terhubung selama sesi FTP berlangsung. Berbeda halnya dengan koneksi data yang koneksinya dibuka dan ditutup untuk tiap file yang ditransfer. Dengan kata lain, ketika pengguna memulai sesi FTP, koneksi kontrol akan dibuka. Selama koneksi kontrol dibuka, koneksi data akan dibuka dan ditutup beberapa kali jika dilakukan transfer pada beberapa file.

Keamanan FTP

FTP bukan merupakan protokol untuk transfer file yang aman dan protokol ini memiliki banyak kelemahan. FTP tidak menyediakan enkripsi untuk data yang ditransmisikan. Kebutuhan bisnis hanya pada transfer file antara dua tempat yang berbeda, tidak memperhatikan keamanan proses transfer file. Padahal penggunaan FTP untuk transfer file bisa menyebabkan data yang ditransmisikan mengalami banyak serangan keamanan [7], yaitu:

FTP Brute Force Attack

Serangan brute force untuk menebak password FTP server dapat dilakukan oleh attacker dengan melakukan percobaan kombinasi password yang berbeda berulang-ulang hingga dapat masuk ke FTP server. Password yang lemah dan penggunaan password yang sama untuk beberapa FTP server juga dapat mempermudah attacker mendapatkan akses dengan cepat.

Packet Capture (atau Sniffing)

Data yang ditransmisikan melalui FTP adalah teks tidak terenkripsi. Oleh karena itu, informasi sensitive seperti username dan password dapat dengan mudah diketahui dengan teknik sniffing paket. Sniffing dilakukan dengan program computer yang dapat menangkap paket data yang ditransmisikan dan membaca data di setiap field pada paket.

Spoof Attack

FTP server dapat membatasi akses berdasarkan ip address. Namun demikian, serangan masih mungkin dilakukan oleh attacker dengan menggunakan computer di luar perusahaan dan menjadikannya seolah-olah memiliki ip address dari computer jaringan perusahaan, kemudian dapat mendownload file selama transfer data.

Port Stealing

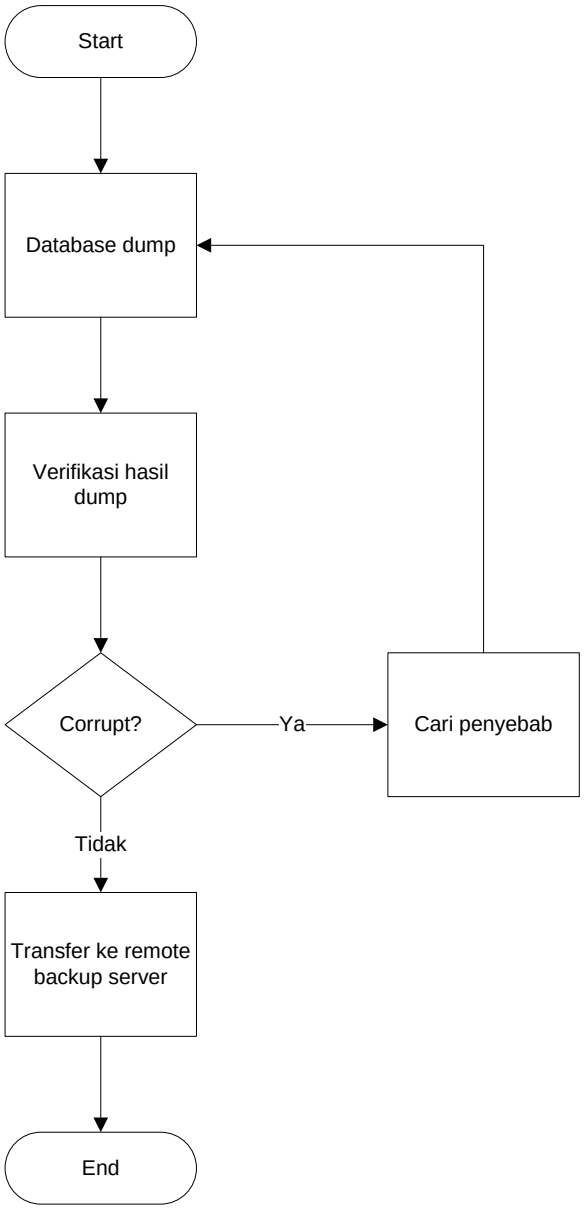
Sistem operasi dapat membuat port dinamis dengan urutan atau pola tertentu. Hal ini dapat digunakan oleh attacker membaca pola dan mengidentifikasi port berikutnya yang akan digunakan. Apabila attacker secara ilegal mendapatkan akses ke port tertentu, pengguna sah yang berusaha untuk mendapatkan akses ke file akan ditolak aksesnya dan attacker dapat mencuri file, atau bahkan memasukkan file palsu atau file berbahaya yang akan diakses oleh pengguna lain dalam organisasi.

FTP Bounce Attack

Saat terjadi koneksi jaringan lambat, pengguna sering menggunakan proxy FTP yang mengakibatkan FTP client meminta transmisi data secara langsung antara dua FTP server. Attacker dapat memanfaatkan hal ini dan menggunakan command PORT untuk meminta akses ke port dengan menyamar untuk meminta file transfer, kemudian menjalankan port scan secara diam-diam dan mendapatkan akses data yang ditransmisikan pada jaringan.

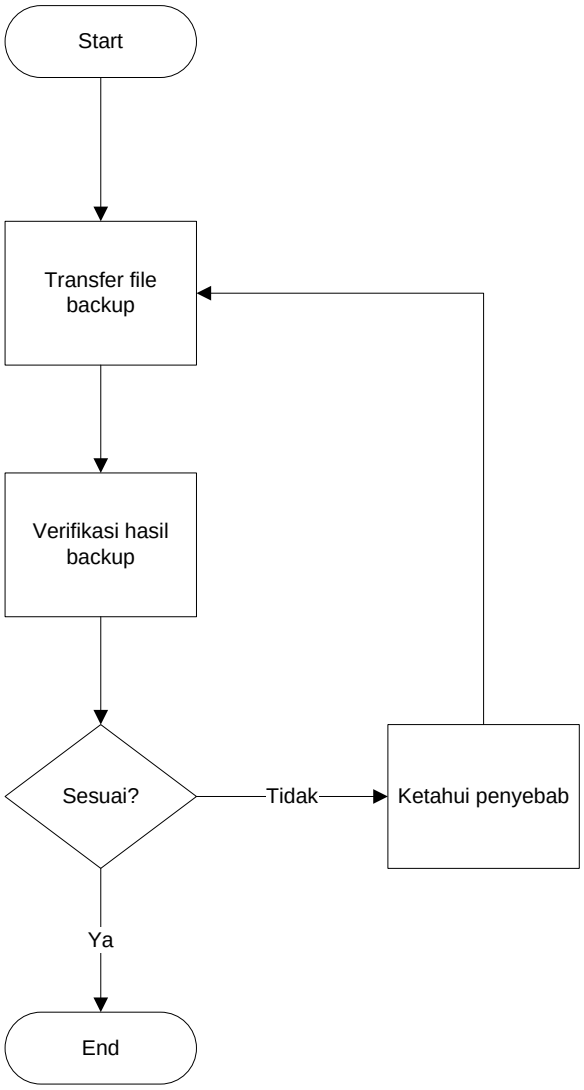
Penanganan Insiden pada subsistem backup dan recovery

Berdasarkan analisis keamanan diatas maka dapat dirumuskan insiden yang mungkin terjadi pada subsistem backup dan recovery adalah proses database dump yang tidak berhasil atau corrupted, gagal dalam proses transfer file backup ke remote backup server, adanya malicious user yang masuk ke dalam subsistem backup dan recovery dan kegagalan dalam proses restore file backup.



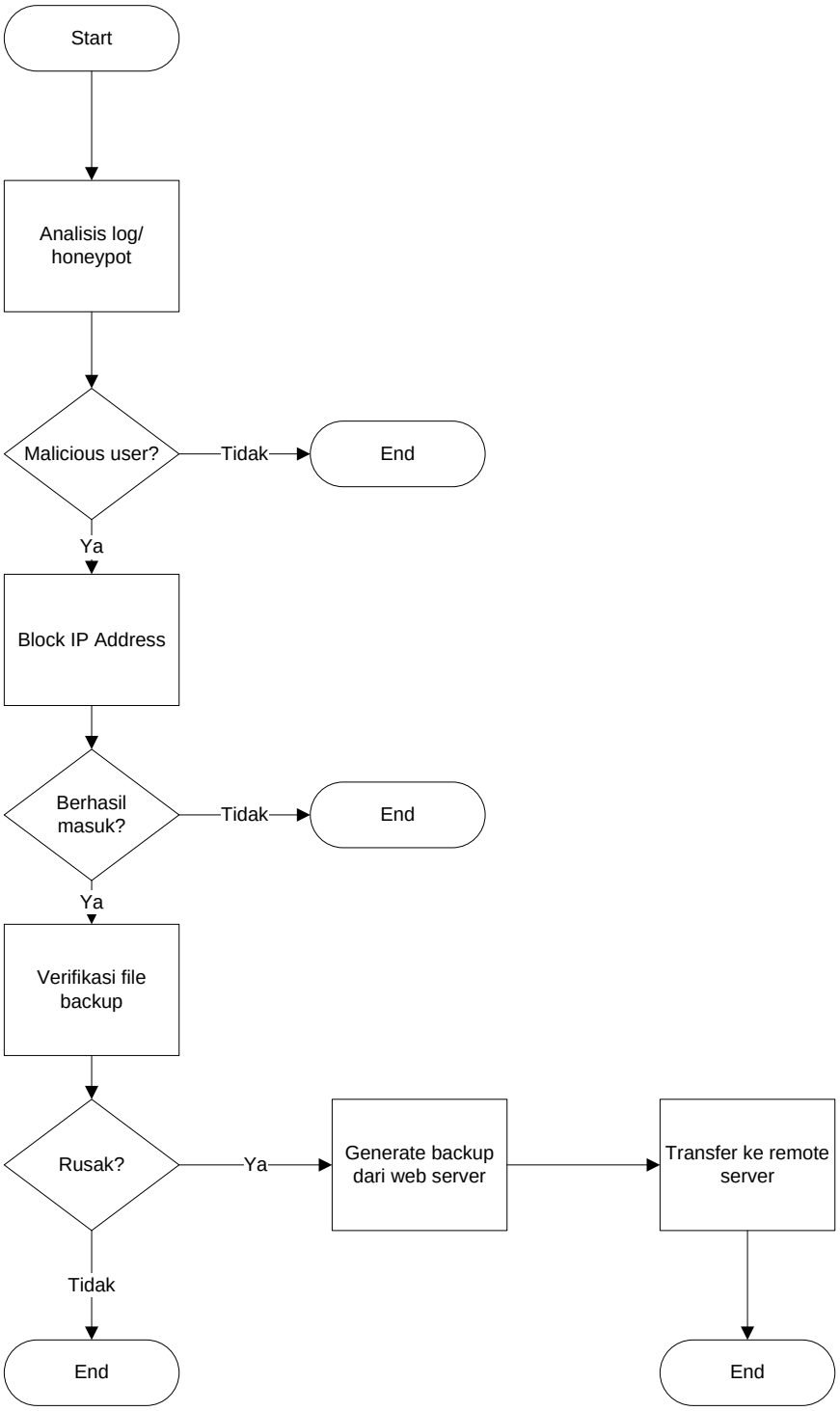
Gambar 11. Penanganan insiden akibat kegagalan dalam proses database dump

Gambar 11 adalah flowchart penanganan insiden dalam proses database dump. Setelah dilakukannya proses database dump maka akan dilakukan verifikasi apakah file backup yang dihasilkan rusak atau tidak. Verifikasi dapat dilakukan dengan menggunakan checksum, seperti telah dijelaskan pada bab sebelumnya, ataupun dengan menguji file backup dengan merestore pada sistem uji. Apabila database dump yang dihasilkan tidak sempurna maka ketahui penyebab kerusakan tersebut. Database dump memberikan fleksibilitas untuk dapat mengubah file backup sehingga dapat direstore. Oleh karena itu, perbaikan dapat dilakukan dengan mengubah file database dump tersebut atau dengan melakukan generate ulang database dump hingga menghasilkan file backup yang tidak corrupted. Setelah itu transfer file backup ke remote server.



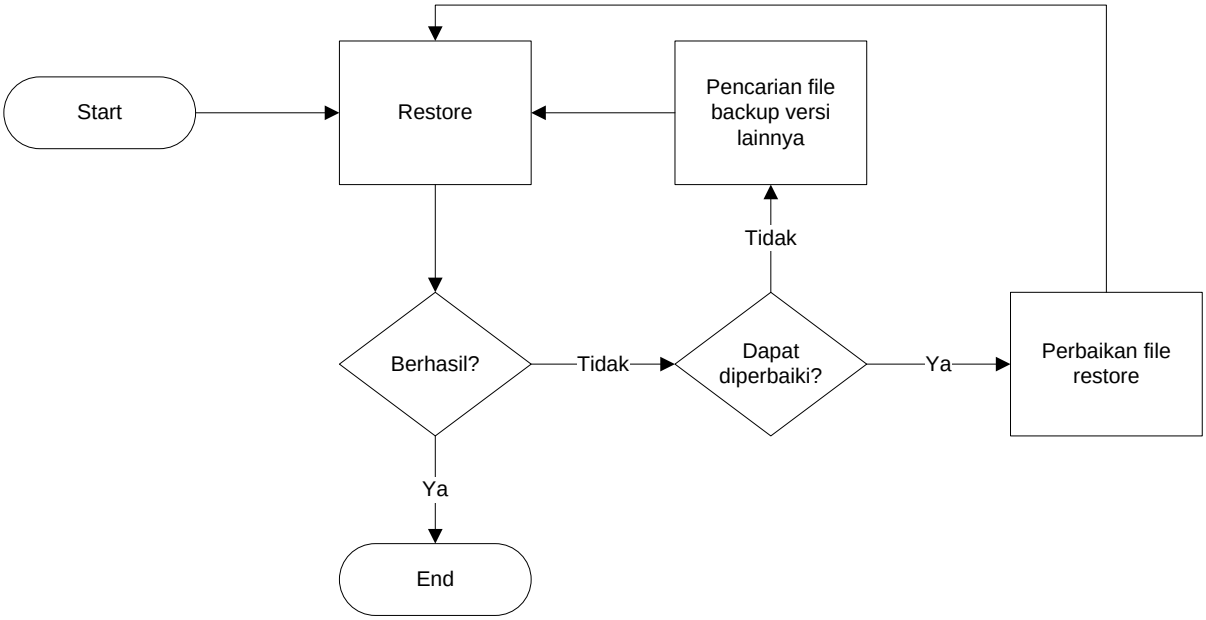
Gambar 12. Penanganan insiden dalam proses transfer file backup

Gambar diatas adalah flowchart penanganan insiden dalam proses transfer file backup. Setelah proses backup dilakukan, maka file backup akan ditransfer ke remote server backup. Proses transfer menggunakan rsync dan SSH atau menggunakan FTP. File backup yang telah ditransfer kemudian diverfikasi apakah sesuai dengan file backup yang digenerate dari web server. Apabila file backup mengalami kerusakan maka akan dilakukan analisis pada log server apakah penyebabnya adalah malicious user yang melakukan modifikasi, koneksi jaringan yang lambat atau terputus, atau penyebab lainnya. Setelah itu dilakukan transfer ulang pada file backup tersebut.



Gambar 13. Penanganan insiden terhadap malicious user

Gambar 13 adalah flowchart penanganan insiden terhadap malicious user. Seperti telah dijelaskan pada bab sebelumnya, aktivitas malicious user dapat diketahui dengan menggunakan log yang direkam oleh honeypot. Apabila terdeteksi terdapat malicious user pada subsistem backup dan recovery, maka dilakukan block ip address user tersebut. Setelah itu verifikasi pada file backup dilakukan untuk mengetahui apakah file backup rusak atau telah dimodifikasi oleh malicious user. Apabila file backup mengalami kerusakan maka lakukan backup dari web server dan transfer file backup tersebut ke remote backup server.



Gambar 14. Penanganan insiden dalam kegagalan restore file backup

Gambar diatas merupakan flow chart penanganan insiden dalam proses restore file backup. Proses restore dilakukan saat terjadi kegagalan sistem yang disebabkan oleh malicious user maupun bencana alam. Restore dilakukan menggunakan file backup yang diperoleh dari remote backup server. File backup dipilih dengan melihat versi backup yang terbaru. Apabila restore tidak berhasil dilakukan maka upaya perbaikan file backup akan dilakukan. Jika tidak dapat dilakukan, maka proses akan berlanjut ke pemilihan versi backup yang lebih lama. Proses akan kembali ke restore file backup.

Kesimpulan

Salah satu subsistem pada sistem terdistribusi untuk melakukan proteksi web server adalah subsistem backup dan recovery. Subsistem ini membuat file backup dan mentransmisikannya ke remote server backup. Pilihan strategi dalam melakukan backup yaitu full backup, differential backup, dan incremental backup. Version control management digunakan untuk membedakan file backup pada waktu yang berbeda.

Backup database menggunakan database dump yang berisi struktur tabel atau data dari database yang berupa script SQL. Backup database dengan cara ini dapat memberikan fleksibilitas dan kemudahan karena sebelum direstore dapat dilihat dan bahkan dimodifikasi. Namun demikian, cara ini tidak dimaksudkan untuk backup data dengan skala besar. Pada data yang sangat besar proses restore data akan menjadi sangat lambat. Oleh karena itu, untuk backup dan restore data dengan skala besar dapat menggunakan physical backup.

Sinkronisasi dan transmisi file backup ke remote backup server menggunakan rsync. Rsync menggunakan SSH untuk koneksi ke remote host. Target serangan yang paling sering digunakan oleh attacker adalah server yang memiliki remote access seperti SSH. Attacker dapat melakukan brute force untuk menebak username dan password untuk mengakses SSH.

Honeypot digunakan untuk mengelabui attacker dengan bertindak sebagai sistem yang memiliki data dan service. Selama berinteraksi dengan attacker, honeypot mengumpulkan informasi mengenai aktivitas attacker. Informasi tersebut dapat dianalisis dan divisualisasikan untuk melihat distribusi percobaan username dan password, IP address, dan command yang digunakan attacker.

Metode lain yang digunakan untuk transfer file backup adalah menggunakan FTP. Koneksi menggunakan FTP antara client dan server dilakukan dengan dua koneksi, yaitu koneksi kontrol dan koneksi data. FTP yang merupakan protokol untuk transfer file, masih memiliki kelemahan keamanan, seperti FTP Brute Force Attack, Packet Capture (atau Sniffing), Spoof Attack, Port Stealing, dan FTP Bounce Attack.

Penanganan insiden diberikan pada subsistem backup dan recovery. Berdasarkan analisis keamanan, maka insiden yang mungkin terjadi pada subsistem tersebut yaitu proses database dump yang tidak berhasil atau corrupted, gagal dalam proses transfer file backup ke remote backup server, adanya malicious user yang masuk ke dalam subsistem backup dan recovery, dan kegagalan dalam proses restore file backup. Flowchart penanganan insiden dibuat untuk setiap insiden yang terjadi.

Referensi

[1] W. Stallings and L. Brown, "Operating System Security," in *Computer Security Principles and Practice*, New Jersey, Pearson Education, Inc., 2014.

[2] H. Qian, G. Yafeng, W. Yong and Q. Baohua, "A Web Site Protection Oriented Remote Backup and Recovery Method," *CHINACOM,* 2013.

[3] A. Tridgell and P. Mackerras, "The rsync algorithm," [Online]. Available: https://rsync.samba.org/tech_report/. [Accessed May 2016].

[4] S. Suguna and D. A. Suhasini, "Overview of Data Backup and Disaster Recovery in Cloud," *ICICES2014,* 2014.

[5] I. Koniaris, G. Papadimitriou and P. Nicopolitidis, "Analysis and Visualizationn of SSH Attacks Using Honeypot," *EuroCon 2013,* 2013.

[6] O. Gasser, R. Holz and G. Carle, "A deeper understanding of SSH: Results from Internet-wide scans," *IEEE Network Operations and Management Symposium (NOMS),* 2014.

[7] S. Khandelwal, "Security Risks of FTP and Benefits of Managed File Transfer," December 2013. [Online]. Available: http://thehackernews.com/2013/12/security-risks-of-ftp-and-benefits-of.html. [Accessed May 2016].

[8] Z. Jun, H. Qian and Y. Linlin, "A distributed website anti-tamper system based on filter driver and proxy," in *Proc. of the 2011 MSEC International Conference on Multimedia, Software Engineering and Computing*, Wuhan, 2011.

[9] Wikipedia, "Database dump," [Online]. Available: https://en.wikipedia.org/wiki/Database_dump. [Accessed May 2016].

[10] MySQL, "MySQL Glossary," [Online]. Available: http://dev.mysql.com/doc/refman/5.7/en/glossary.html. [Accessed May 2016].

[11] MySQL, "5.5.4 mysqldump — A Database Backup Program," [Online]. Available: http://dev.mysql.com/doc/refman/5.7/en/mysqldump.html. [Accessed May 2016].

[12] J. Ellingwood, "How To Backup MySQL Databases on an Ubuntu VPS," DigitalOcean, 28 August 2013. [Online]. Available: https://www.digitalocean.com/community/tutorials/how-to-backup-mysql-databases-on-an-ubuntu-vps. [Accessed May 2016].

[13] MySQL, "CHECKSUM TABLE Syntax," [Online]. Available: http://dev.mysql.com/doc/refman/5.7/en/checksum-table.html. [Accessed May 2016].

[14] Troy.jdmz.net, "Using Rsync and SSH," [Online]. Available: http://troy.jdmz.net/rsync/. [Accessed May 2016].

[15] B. A. Forouzan, "Remote Login: TELNET and SSH," in *TCP/IP Protocol Suite*, New York, McGraw-Hill, 2010.

[16] L. Spitzner, in *Honeypots: Tracking Hackers*, Boston, MA, Addison Wesley, 2003.

[17] L. Spitzner, "Strategies and issues: Honeypots - sticking it to hackers," *Network Magazine,* 2003.

[18] D. Keim, F. Mansmann, J. Schneidewind, J. Thomas and H. Ziegler, "Visual analytics: Scope and challenges," *Visual Data Mining,* 2008.

[19] B. A. Forouzan, "File Transfer: FTP and TFTP," in *TCP/IP Protocol Suite*, New York, McGraw-Hill, 2010.