Penerapan *Privileged Access Management* Menggunakan *One Identity* Pada Sebuah Perusahaan

Hendra Nuryuliansyah[1]
Universitas Ibn Khaldun Bogor; Jl. KH Sholeh iskandar Km.2 Bogor, 0251-8380993
[3]Jurusan Teknik Informatika, Teknik UIKA, Bogor
e-mail: [1]**hendra@slackware-id.org**

Abstrak

One Identity Privileged Access Management (PAM) adalah solusi terhadap serangkaian upaya untuk mengurangi resiko keamanan dan membantu perusahaan dalam mengamankan, mengendalikan, memantau, menganalisis dan mengatur hak akses istimewa ke data dan aplikasi suatu organisasi yang sangat penting. Solusi PAM memungkinkan perusahaan untuk menyediakan kredensial penuh seperti Administrator pada Window, Root pada UNIX, Cisco Enable pada perangkat Cisco, serta password yang tertanam yang ditemukan dalam aplikasi dan skrip atau membatasi akses terhadap user (pengguna) biasa. Semua aktivitas hak akses istimewa (privilege account) dicatat dengan penganalisaan aktivitas dan data secara real-time. Dapat dihilangkan aktivitas saling berbagi password, sehingga keamanan dapat ditingkatkan dan kepatuhan atas aturan hak akses istimewa lebih efisien dan mudah teradministrasi. Masalah yang dapat digambarkan ketika pengguna password hak akses istimewa tidak mempunyai regulasi yang rutin dilakukan dalam mengubah password secara berkala yang sesuai dengan kebijakan pengamanan (password policy) bahkan untuk mendapatkan informasi siapa yang telah mengakses perangkat jaringan dengan menggunakan akun istimewa atau akun lain yang diperbolehkan. Tujuan dari penelitian ini adalah (i) mendapatkan hasil informasi atas perubahan password secara berkala berdasarkan konfigurasi yang sudah ditetapkan pada sistem PAM dan disesuaikan terhadap aturan password policy, (ii) mendapatkan informasi siapa yang mengakses perangkat jaringan beserta akun yang diaksesnya. Metode penelitian yang dilakukan adalah (i) melakukan mengumpulkan data dari sistem yang akan diimplementasikan, (ii) mengakses langsung sistem yang telah di data dan melihat informasi secara menyeluruh ke dalam sistem, (iii) mencocokan jenis sistem terhadap sistem yang didukung oleh sistem aplikasi PAM lalu diintegrasikannya. Pengujian dilakukan dengan cara melakukan akses ke target sistem menggunakan hak akses istimewa melalui sistem aplikasi PAM. Hasil yang diperoleh (i) dapat memudahkan pengguna password untuk tidak terlalu banyak mengingat password, (ii) dapat menghindari saling berbagi informasi password, (iii) password secara berkala berubah-ubah, (iv) mengetahui seluruh aktivitas pengguna password terhadap kumpulan target sistem jaringan yang diperbolehkan diakses, (v) merekam seluruh aktivitas akses dalam bentuk video.

Kata kunci*— Privileged Access Management (PAM), One Identity, Password Policy*

Abstract

One Identity Priveged Access Management (PAM) is a solution for a series of efforts to reduce security risks and help companies secure, control, monitor, analyze, and regulate privileged access rights to data and applications from very important organizations. The PAM solution allows companies to provide full credentials such as Administrators on Windows, Root on UNIX, Cisco Enable on Cisco devices, and embedded passwords found in applications and scripts or restricting access to ordinary users. All privileged account activities are recorded by analyzing real time activities and data. Password sharing activities can be eliminated, so security can be improved and compliance with privileges of privileged access rights is more efficient and manageable. Problems that can be explained when the user privileges password access rights do not have regular rules to change the password periodically in accordance with the security policy (password policy) even to obtain information that has accessed the network device using a special

account or other permitted account . The purpose of this study is (i) to obtain information about changes in passwords periodically based on the configuration that has been set in the PAM system and adjusted to the password policy rules, (ii) get information about who is accessing the network device and the account accessed. The research method that is carried out is (i) collecting data from the system that will be implemented, (ii) directly accessing the system that has data and viewing information thoroughly into the system, (iii) matching the type of system with the system supported by the PAM application system then integrate it. Testing is done by accessing the target system using privileged access rights through the PAM application system. The results obtained (i) can facilitate password users not to remember passwords too often, (ii) can avoid sharing password information, (iii) change passwords regularly, (iv) find out all user password activities against a set of targets network systems that are permitted to be accessed, (v) record all access activities in the form of videos.

Keywords— *Privileged Access Management (PAM), One Identity, Password Policy*

1. PENDAHULUAN

Perkembangan teknologi informasi dalam dunia komunikasi data global, senantiasa diikuti oleh berkembangan perangkat lunak secara cepat, sehingga keamanan merupakan suatu permasalahan yang perlu diperhatikan, seperti keamanan secara fisik, keamanan berupa data maupun keamanan akses aplikasi.

Perlu kita sadari bersama bahwa suatu keamanan berbanding terbalik dengan kenyamanan, dan untuk mencapai suatu keamanan itu adalah sesuatu hal yang sangat melelahkan, seperti contoh dalam dunia nyata sekarang ini. Rumah yang kita tempati tidak ingin di masuki oleh pencuri, maka kita buatkan pintu rumah kita menjadi tiga lapisan, lapisan pertama terbuat dari kayu, lapisan kedua terbuat dari besi dan lapisan ketiga terbuat dari baja. Masing-masing lapisan kita berikan gembok diantaranya pintu yang berlapiskan kayu di pasang gembok biasa, pintu yang berlapiskan besi di pasang gembok yang ada nomornya, pintu yang berlapiskan baja di pasang gembok sensor. Dari semua keamanan itu pasti kita akan merasa tidak nyaman jika ingin keluar rumah, maka kita harus membuka tiga pintu terlebih dahulu beserta gemboknya dan itu sungguh tidak nyaman. Begitu juga dengan keamanan sistem komputer. Namun yang bisa kita lakukan adalah untuk mengurangi gangguan keamanan seminimal mungkin dengan cara yang sangat efektif.

Salah satu kesadaran akan masalah keamanan atau *security awareness* pada sistem informasi yang sangat umum diketahui bersama yaitu kata sandi atau *password*. *Password* memiliki peranan penting dalam kaitannya dengan keamanan. *Password* bukan berarti suatu bentuk rangkaian kata-kata dan tentu saja *password* bukan berarti suatu kata yang mempunyai arti akan lebih sulit untuk ditebak. *Password* kadang-kadang digunakan juga dalam suatu bentuk yang hanya berisi angka salah satu contohnya adalah *Personal Identification Number* (PIN) dan umumnya cukup pendek sehingga mudah untuk diingat. Walaupun hanya terdiri dari angka, namun kegunaannya sama seperti *password*, yaitu untuk mengamankan informasi. Informasi yang disimpan tersebut biasanya sudah berbentuk digital.

Banyak dari para pengguna *password* yang membuat *password* secara sembarangan tanpa mengetahui kebijakan pengamanan (*password policy*) lalu menyimpannya dengan menuliskan kembali dibalik kalendar dimeja kerjanya dan meletakkannya begitu saja sehingga semua orang dapat membacanya atau memo berbentuk *post-it* dengan kata sandi yang ditulis di atasnya, sudah tentu merupakan perilaku yang beresiko tinggi. Berdasarkan *Mandylion Research Labs*, mengatur kembali sistem keamanan kata sandi suatu perusahaan yang memiliki 100 karyawan akan menimbulkan biaya $3.850 per tahun. Jika perusahaan

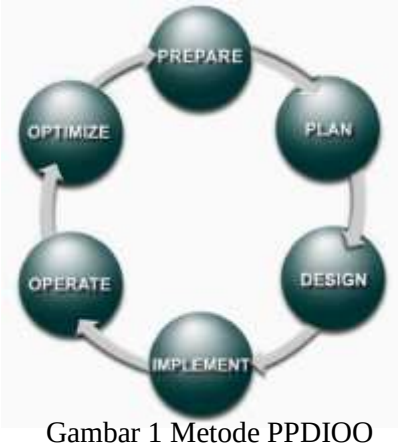
memiliki 1000 personil yang diberikan otorisasi, maka proses yang sama akan menimbulkan biaya hingga $38.500 per tahun! Mereka tidak peduli bagaimana membuat *password* yang kuat (*strong password*) dan bagaimana membuat *password* yang selalu berubah setiap saat bahkan penggatian *password* secara terjadwal oleh sistem. Sangatlah mahal untuk mengubah kata sandi. Mereka tidak sadar dengan bahayanya para 'penyerang' (*attacker*) yang dapat mencuri atau mengacak-acak informasi tersebut dengan alat *hacker* dapat digunakan untuk mencoba menebak setiap kata dalam kamus kumpulan *password* dalam waktu beberapa menit untuk mendapatkan akses secara tidak sah. Oleh karenanya, jika suatu kata sandi berupa sebuah kata atau nama dalam kamus, maka kata tersebut akan dengan mudah dibajak.

Untuk mengatasi permasalahan yang terjadi berkaitan dengan manajemen *password* untuk itu dibutuhkan sistem teknologi yang mengizinkan pengguna agar dapat mengakses sumber daya dalam jaringan melalui sesi *terminal* yang telah disediakan dengan menggunakan satu akun pengguna saja. Maka penulis mengimplementasikan dan menganalisa sistem *Privileged Access Management* (PAM) menggunakan aplikasi berlisensi dari *One Identity*. PAM sebagai solusi keamanan dalam siklus pengelolaan hak akun istimewa pada sistem operasi, perangkat jaringan dan aplikasi berbasis *website*. Menghindari berbagi dan saling tukar informasi mengenai *password* diantara pengguna sistem terhadap akun istimewa seperti Administrator pada Windows server, Root pada UNIX server, Cisco Enable pada perangkat jaringan Cisco, maupun menyematkan *password* pada aplikasi dan skrip. Informasi hak akses instimewa ini masuk dalam peraturan auditor dalam melakukan proses pengelolaan siapa yang memiliki akses terhadap informasi apa dari waktu ke waktu.

2. METODE PENELITIAN

2.1 Metode Penelitian PPDIOO *Network Lifecycle*

Cisco telah menghasilkan sebuah formula siklus hidup perencanaan jaringan, menjadi enam fase: *Prepare* (Persiapan), *Plan* (Perencanaan), *Design* (Desain), *Implement* (Implementasi), *Operate* (Operasi) dan *Optimize* (Optimasi). Fase-fase ini dikenal dengan istilah PPDIOO. Pada formula ini termasuk di dalamnya kemanan jaringan dan *server* [1].



Gambar 1 Metode PPDIOO

A. *Prepare* (Persiapan)

Pada fase pertama dalam metode pengembangan sistem menggunakan PPDIOO yaitu dimulai dari fase *prepare* atau tahap persiapan. Pada fase ini dilakukan proses mengumpulkan data dari target sistem yang akan diimplementasikan melalui proyek yang sedang berlangsung melalui: i) mengirimkan *form* data *gathering* dengan format dokumen MS. Excel (.xlsx) kepada seorang staf penanggung jawab proyek melalui *email* dan memintanya untuk mengirimkan kembali jika data sudah dilengkapi sepenuhnya, ii) verifikasi ulang data yang diberikan dan diolah kembali menggunakan aplikasi MS. Excel lalu mengklasifikasikan sistem mana memiliki *password*. *Password* merupakan sederet karakter string (huruf, angka, dan simbol lain) milik user yang digunakan untuk mendapat akses legal terhadap suatu sistem [2] yang dapat di kelola oleh PAM atau hanya dibuka *session terminal* atau *console* maupun hanya dibuka *session website*, iii) mengakses langsung target sistem menggunakan aplikasi *remote* akses dan melihat informasi secara menyeluruh ke dalam sistem mengenai jenis sistem operasi, versi, dll, iv) mencocokan jenis sistem terhadap sistem yang didukung oleh PAM, v) terhadap target sistem yang didukung oleh PAM harus dibuatkan *functional account* lalu *password* akun

tersebut di *reset* melalui PAM, vi) terhadap sistem yang tidak didukung oleh PAM harus diketahui akun dan *password* yang mempunyai tingkatan akses tertinggi dan *command line interface* (CLI) yang dapat diadaptasikan oleh PAM, vii) terhadap target sistem berupa aplikasi *web* maka URL harus dicoba terlebih dahulu melalui *server* pendukung PAM yaitu *jump box* maupun *archive server*.

B. *Plan* (Perencanaan)

Dalam tahap perencanan setelah data yang dipersiapkan sudah dilakukan sebelumnya, maka informasi yang didapat secara langsung dari masing-masing sistem seperti Windows, Unix/Linux dan beberapa perangkat jaringan seperti Cisco Router sehingga memungkinkan dapat dibuatkan user *functional account* setara dengan Administrator, Root atau Admin.

C. *Design* (Desain)

Dalam tahap desain yaitu membuat topologi untuk menentukan bagaimana semua perangkat pendukung PAM saling terhubung dan semua target sistem dapat diakses melalui PAM berdasarkan matriks pengguna, sehingga tidak ada lagi akses dari luar jaringan yang langsung dapat mengakses target sistem.

D. *Implement* (Penerapan)

Pada tahap implementasi ini menerapkan semua yang sudah disiapkan dan direncanakan dengan mengacu pada tahap desain yang telah dirancang. Ruang lingkup tahapan ini yaitu :

1. Menjadikan nama komputer (*hostname*) sebagai nama target sistem pada PAM.
2. Membedakan nama target sistem pada sistem operasi dan aplikasi *web* pada PAM.
3. Pengujian konektivitas terhadap target sistem berbasis aplikasi *web* melalui *PAM*.
4. Melakukan perubahan *password* secara manual pada target sistem yang hanya diberikan akses *session* melaui PAM.
5. Menerapkan otentikasi yang digunakan oleh *functional account* menggunakan SSH *key* bagi sistem operasi Unix/Linux.
6. Semua informasi target sistem yang sudah terintegrasi ke PAM masuk dalam jadwal berkas cadangan data yang akan disimpan dalam perangkat pendukung PAM yaitu *archive server*.
7. Kedua aplikasi PAM sudah diberikan *Ip Address* dan semua perangkatnya sudah saling terhubung sehingga sudah dapat diterapkan *load balancing* secara aktif pada *primary* dan secara aktif pada *replica*.

E. *Operate* (Operasional)

Proses pengujian pada fase ini yaitu melakukan akses ke target sistem sudah dapat melalui aplikasi PAM dan mencoba melakukan permintaan *password* yaitu *Privileged Password Management* (PPM) dan permintaan *session* yaitu *Privileged Session Management* (PSM).

F. *Optimize* (Optimalisasi)

Dikarenakan PAM menyimpan seluruh *password* target sistem, maka pada tahapan ini diperlukan perhatian khusus terhadap kebijakan yang perlu dibuat untuk mengatur dan membuat sistem aplikasi PAM agar selalu dapat berjalan dengan optimal. *Preventive maintenance* termasuk dalam fase ini.

3. HASIL DAN PEMBAHASAN

3.1 Tahap *Prepare* (Persiapan)

Hasil pengumpulan data sistem dilakukan untuk memperoleh informasi yang dibutuhkan dalam rangka mencapai tujuan mengintegrasikan perangkat ke PAM, informasi data secara menyeluruh disesuaikan oleh kebutuhan perangkat PAM diantaranya pengumpulan data melalui form MS. Excel dengan *field* "Data" pada Tabel 1 mendatar dari A-Z.

Tabel 1 *Form* data *gathering*

Data	Keterangan
Hostname	Penamaan pada server contoh "XDC"
Nama sistem pada PAM	Penamaan pertama pada PAM disesuaikan dengan *hostname* pada server

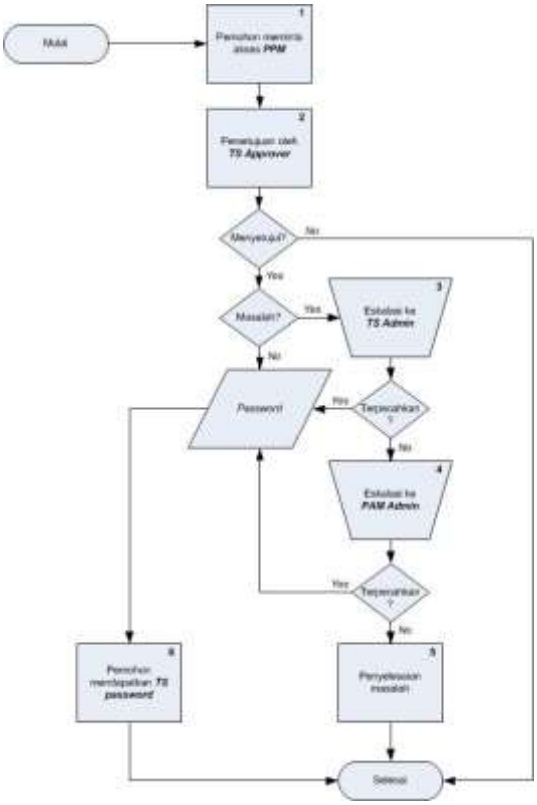
Nama sistem pada PAM	Penamaan kedua pada PAM jika perangkat server tersebut terdapat aplikasi berbasis *web* sehingga ditambahkan informasi "WEB-XDC"
IP Address	Pengalamatan *server*
PSM RDP	*Privileged Session Management* (PSM) untuk akses sistem Windows berupa akses *session*
PSM SSH	*Privileged Session Management* (PSM) untuk akses sistem Linux berupa akses *session*
PSM *Web*	*Privileged Session Management* (PSM) untuk akses *web* aplikasi
PPM	*Privileged Password Management* (PPM) untuk akses permintaan *password*
URL	*Uniform Resource Locator* untuk menunjukkan alamat suatu aplikasi berbasis *website*
Functional Account	Akun yang dirancang untuk mampu melakukan tugas fungsional yang dibutuhkan PAM untuk mengubah *password*.
User Managed	*User* sistem operasi yang *password* nya sudah berhasil diubah oleh PAM
Credential 1	Mempunyai satu *password* jika *user* yang dikelola oleh PAM baik PSM atau PPM
Credential 2	Mempunyai dua *password* jika *user* yang dikelola oleh PAM baik PSM atau PPM
Keterangan	Informasi tambahan pada proses pengumpulan data

Pada tahap kebutuhan ini data sistem masih terbuka dengan memberikan informasi *username* beserta *password*, sebagai informasi dasar yang akan diuji.

3.2 Tahap *Plan* (Perencanaan)

Hasil perencanaan data yang diperoleh yaitu:

a. Tahap pembiasaan menggunakan PAM, setiap pengguna dapat mengajukan *request* baik *Privileged Password Manager* (PPM) maupun *Privileged Session Manager* (PSM) ke semua target sistem dalam keadaan *password* belum diubah-ubah. Melalui tahapan *request* seperti berikut:

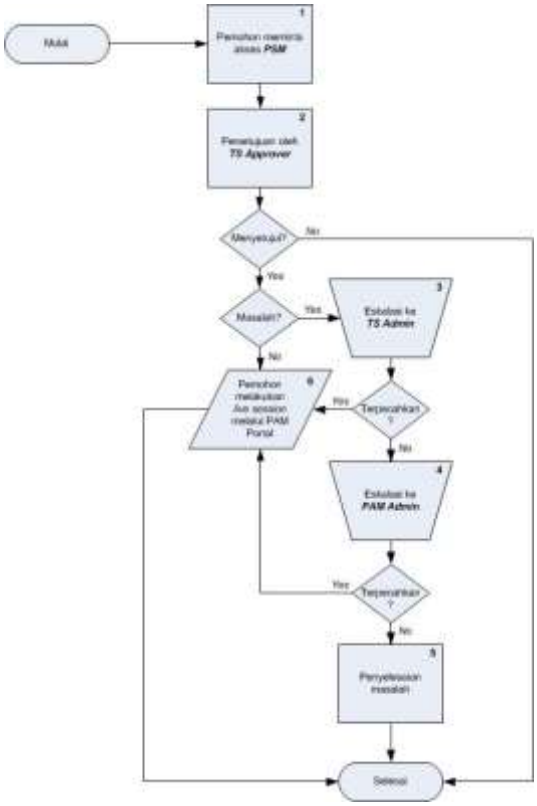


Gambar 2 *Flowchart* permintaan akses PPM

Tabel 2 Penjelasan *Flowchart* permintaan akses PPM

No	Penjelasan
1	Permohonan (*request*) akses PPM terhadap sistem yang sudah ditentukan.
2	Sistem yang akan diakses tersebut harus disetujui oleh TS *Approver*, jika disetujui dan sistem tersebut ada masalah seperti sistem tidak dapat di *request* atau terdapat sistem akan tetapi akun istimewa tidak terdapat sehingga tidak dapat di *request*, maka akan di eskalasi ke TS Admin.
3	TS Admin akan melakukan pengecekan terhadap permintaan PPM yang bermasalah seperti pengecekan tes sistem, *reset password* akun fungsional.
4	Eskalasi ke PAM Admin jika permasalahan tidak dapat diselesaikan oleh TS Admin.
5	Permasalahan yang dikerjakan oleh PAM Admin harus benar-benar

	selesai sehingga ketika permohon melakukan permintaan akses terhadap sistem yang sama tidak ada kendala apapun.
6	Jika selesai dan tidak ada kendala apapun, maka sistem PAM akan memberikan *password release* terhadap permohon. Semua proses tersimpan dalam *log* untuk kebutuhan audit.



Gambar 3 *Flowchart* permintaan akses PSM

Tabel 3 Penjelasan *Flowchart* permintaan akses PSM

No	Penjelasan
1	Permohonan (*request*) akses PSM terhadap sistem yang sudah ditentukan.
2	Sistem yang akan diakses tersebut harus disetujui oleh TS *Approver*, jika disetujui dan sistem tersebut ada masalah seperti sistem tidak dapat di request atau terdapat sistem akan tetapi akun istimewa tidak terdapat sehingga tidak dapat di *request*, maka akan di eskalasi ke TS Admin.
3	TS Admin akan melakukan pengecekan terhadap permintaan PSM yang bermasalah seperti pengecekan tes sistem, *reset password* akun fungsional.
4	Eskalasi ke PAM Admin jika permasalahan tidak dapat diselesaikan oleh TS Admin.
5	Permasalahan yang dikerjakan oleh PAM Admin harus benar-benar selesai sehingga ketika permohon melakukan permintaan akses terhadap sistem yang sama tidak ada kendala apapun.
6	Jika selesai dan tidak ada kendala apapun, maka sistem PAM akan memberikan *session release* terhadap permohon. Semua proses tersimpan dalam *log* dan rekaman video tersimpan dalam server *archive* untuk digunakan sewaktu-waktu oleh audit.

b. Melalui antarmuka persetujuan PAM, *Administrator* sistem yang memiliki hak sebagai approver di sistem PAM, dapat melihat semua permintaan akses *privilege* baik PPM maupun PSM, *Administrator* dapat menentukan apakah akan menyetujui atau menolak permohonan tersebut

3.2 Tahan *Design* (Desain)

a. Pengamanan jaringan

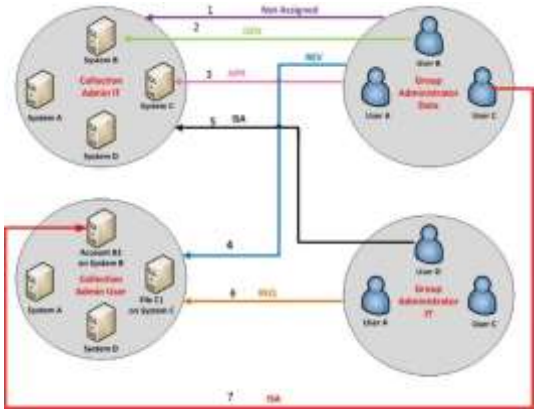
Pada tahap ini peneliti menggambarkan perancangan jaringan pada sistem aplikasi PAM dimana semua target sistem hanya dapat di akses melalui PAM untuk menutup semua akses yang tidak diperlukan, maka menggunakan teknik *whitelist* sangat efektif dengan cara menutup semua *port* dan hanya *port* 22 untuk protokol SSH, 3389 untuk protokol RDP, *port* 80 untuk protokol HTTP, *port* 443 untuk protokol HTTPS dan *port* 22/443 untuk akses DPA dari PAM ke target sistem.

b. Membatasi akses PAM

Pada tahap desain ini peneliti memaparkan, bahwa pada sistem aplikasi PAM terdapat tiga tampilan pengguna diantaranya, yaitu https://<IPAddress>/tpam adalah tampilan terhadap pengguna *requestor* dan *approver*. https://<IPAddress>/admin adalah tampilan terhadap pengguna TS Admin. https://<IPAddress>:8443/config adalah tampilan terhadap pengguna PAM Admin.

c. Matrik pengguna dalam pengendalian akses

Pada tahap desain pemetaan matrik pengguna adalam akses ke target sistem dibagi beberapa kumpulan yang terdiri dari pengguna akses ke PAM yang disebut *Group* dan kumpulan target sistem yang disebut *Collection.*



Gambar 4 pengendalian akses

Tabel 4 Matrik peran akses

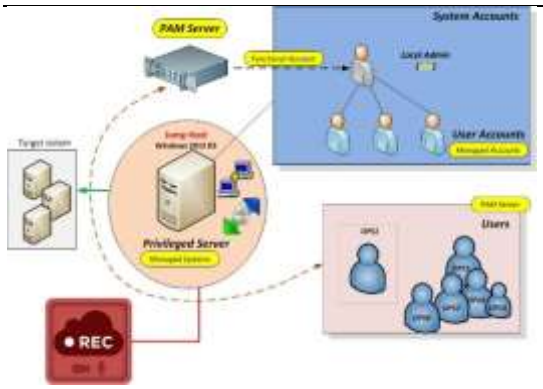
User / Peran	Admin *User*	Admin IT	*Role* ke-n	*Status*
Group Administrator Data (ALL User)	*Group Administrator Data*	*Collection Admin IT*	1	*Not Assigned*
User B	*Group Administrator Data*	*Collection Admin IT*	2	*Denied*
Group Administrator Data (ALL User)	*Group Administrator Data*	*Collection Admin IT*	3	*Approver*
Group Administrator Data (ALL User)	*Group Administrator Data*	*Collection Admin User*	4	*Reviewer*
User D	*Group Administrator Data*	*Collection Admin IT*	5	*ISA*
Group Administrator IT (ALL User)	*Group Administrator Data*	*Collection Admin User*	6	*Requestor*
User C	*Group Administrator Data*	*Collection Admin User*	7	*ISA*

Tabel 5 Matrik akses PAM

Role	Warna Garis	Keterangan
1		Administrator data tidak ada akses kemana pun terhadap *Collection* Admin IT yaitu *System* A, *System* B, *System* C dan *System* D
2		*User* B pada *Group* Administrator data tidak diperbolehkan mengakses *System* B pada *Collection* Admin IT
3		*Group* Administrator data diberikan hak akses untuk dapat melakukan *approve* terhadap *System* C dan ketika ada *user* yang mengakses *System* C, maka *approver* harus memenuhi dari ke tiga *User* A, *User* B dan *User* C. Atau dari ke tiga *User* tersebut *approver* boleh dari salah satunya.
4		*Group* Administrator data dapat melakukan *Reviewer* terhadap proses permintaan *password* pada *System* A, *Account* B1 pada *System* B, *File* C1 pada *System* C dan *System* D
5		*Group* Administrator IT dapat melakukan permintaan *password* dengan cara *retrieve password* tanpa melalui proses *request* dan *approval*. Dapat juga menambahkan *System* baru maupun menghapusnya.
6		Seluruh *user* pada *Group* Administrator IT dapat melakukan permintaan *password* terhadap *Collection* Admin *User*
7		*User* C dapat melakukan permintaan *password* dengan cara *retrieve password* tanpa melalui proses *request* dan *approval*. Dapat juga *edit* / *delete Account* B1 pada *System* B

d. Topologi *server jump host*

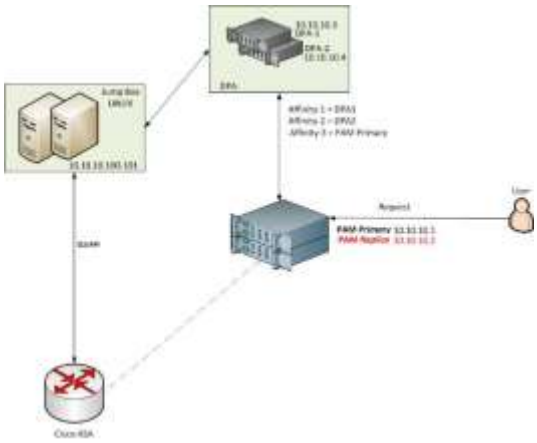
Jump host adalah *server* pendukung yang di desain pada *platform* ini menggunakan server perantara pada jaringan untuk melakukan semua komunikasi ke target sistem tanpa dibatasi. *jump host* telah disediakan dengan dua sistem operasi yang sama, yaitu sistem operasi Windows Server 2012 R2. Kebutuhan yang dapat disesuaikan untuk pekerjaan operasional dalam melakukan pekerjaan yang lebih cepat dan efisien diberikan oleh suatu tim bernama OPS yaitu tim operasional.



Gambar 5 Topologi *jump host*

e. Topologi server jump box

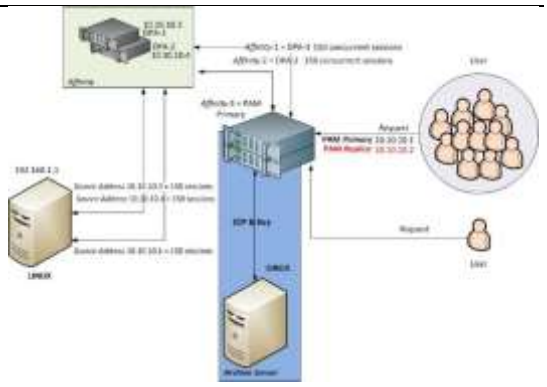
Jump box adalah *server* pendukung yang di desain pada *platform* ini menggunakan *server* perantara pada jaringan untuk melakukan semua komunikasi ke target sistem dan mengembalikan hasilnya ke PAM. *jump box* dapat digunakan saat platform memerlukan penggunaan API atau CLI [3] yang tidak dukung oleh PAM. *Jump box* terdiri dari dua jenis sistem operasi yang berbeda, yaitu sistem operasi Windows Server 2012 R2 dan sistem operasi Linux Red Hat versi 7.2.



Gambar 6 Topologi *jump box*

f. Topologi *archive server*

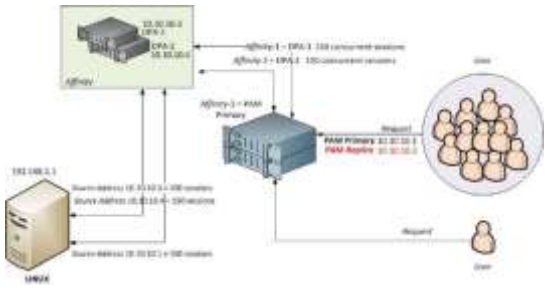
Archive adalah *server* yang diperlukan untuk menyimpan hasil perubahan konfigurasi, catatan aktivitas pengguna akses PAM dan video rekaman PSM. *Archive* menggunakan sistem operasi Linux Red Hat versi 7.2 untuk memudahkan dalam melempar berkas cadangan data menggunakan protokol *Secure Copy* (SCP) port 22.



Gambar 7 Topologi *archive server*

g. Topologi DPA *server*

DPA adalah *server* yang diperlukan untuk pembagian beban akses PSM dari PAM ke target sistem. Dalam satu *server* DPA terdapat 150 *concurrent session*, jadi jika terdapat 150 koneksi PSM secara bersamaan ke target sistem, maka kebutuhan ini sudah mencukupi. DPA menggunakan sistem operasi Linux Fedora.



Gambar 8 Topologi DPA *server*

3.2 Tahap *Implement* (Implementasi)

Dalam konteks sistem integrasi merupakan rangkaian proses untuk menghubungkan beberapa sistem-sistem komputerisasi dan perangkat lunak aplikasi baik secara fisik maupun fungsional. Dalam hal ini menghubungkan perangkat secara fungsional terhadap sistem-sistem Linux, Windows, Cisco, Fortinet dan *Web* Aplikasi dalam satu jaringan untuk dapat berkomunikasi dengan PAM.

A. Linux

Penambahan target sistem pada PAM berupa sistem operasi Linux yaitu dengan mengetahui informasi mengenai *IP Address* dan *Hostname* sebagai acuan penamaan yang akan diberikan pada nama target sistem PAM. Ada dua jenis target sistem Linux yang didukung oleh PAM yaitu Linux dan Linux tty. Jika menggunakan tipe Linux tty, maka

seting untuk membatasi *blacklist command line* tidak berhasil. Karena pada konfigurasi Linux dibatasi oleh audit tidak boleh ada *user* yang setara dengan root yang mempunyai UID (*User Identifier*) and GID (*Group Identifier*) bernilai nol, maka konfigurasi sudoers sebagai solusinya. Sehingga ada tambahan sudo pada kolom *Delegation Prefix* di PAM. Komunikasi PAM dengan target sistem Linux menggunakan SSH Key pada *Functional Account*.

B. Windows

Penambahan target sistem pada PAM berupa sistem operasi Windows yaitu dengan mengetahui informasi mengenai *IP Address* dan *Hostname* sebagai acuan penamaan yang akan diberikan pada nama target sistem PAM. Pengisian nama *Hostname* pada kolom *Computer Name* sangat penting sebagai validasi untuk berkomunikasi antara PAM dan target sistem Windows ditambah dengan pengisian *password* dari *Functional Account*.

C. Cisco Router (SSH)

Penambahan target sistem pada PAM berupa perangkat jaringan Cisco yaitu dengan mengetahui informasi mengenai IP Address dan Hostname sebagai acuan penamaan yang akan diberikan pada nama target sistem PAM.

D. Integrasi target sistem melalui perantara jump box

1. Aplikasi yang hanya bisa dibuka dengan *browser* Chrome.

Telah dilakukan uji coba terhadap sebuah aplikasi yang hanya bisa diakses melalui browser Chrome. Solusi untuk tetap dilakukannya monitoring terhadap aplikasi tersebut yaitu dengan memanfaatkan *jump box* Windows dengan *browser* Chrome.

2. Aplikasi lokal yang hanya dapat diakses dengan nama domain.

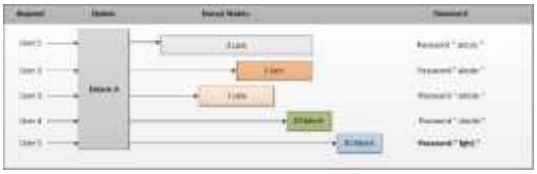
Maksudnya yaitu aplikasi yang hanya dapat diakses melalui domain bukan ip address dikarenakan menggunakan FQDN (*Fully Qualified Domain Name*). Definisinya adalah nama lengkap yang benar untuk suatu *host* yang menentukan lokasi pastinya dalam suatu hirarki DNS

3. Aplikasi yang menjalankan Java untuk membuka akses sistem operasi secara virtual.

Aplikasi ini menjalankan program Java yaitu javaws (*Java Web Start*). Dimana setiap aplikasi dibuka, maka akan melakukan proses pengunduhan file dengan ekstensi (.JNLP) yaitu *Java Network Launch Protocol*. Jika sistem operasinya terdapat program Java, maka *browser* secara otomatis akan menjalankan file JNLP dan jika tidak, maka secara bertahap akan membukanya dengan mengarahkan program Java untuk membuka file JNLP. Permasalahan yang terjadi di atas dapat diselesaikan menggunakan Jump Box Linux dengan Java yang sudah ada secara bawaan sistem operasi ketika terinstal yaitu pada direktori /usr/java/jdk1.8.0_25/jre/bin/javaws dan *browser* Firefox pada direktori /usr/bin.

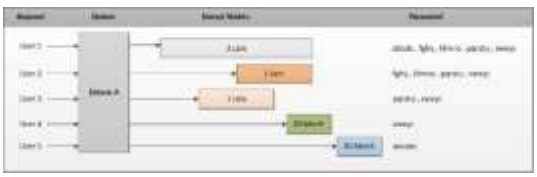
3.2 Tahap *Operate* (operasional)

Operasional dalam melakukan Request password berdasarkan lama durasi waktu yang diminta pada masing-masing user yang mempunyai irisan waktu satu sama lainnya akan mendapatkan password yang sama. Seperti gambar di bawah ini.



Gambar 9 Durasi waktu request password yang beririsan

Seting konfigurasi yang diberikan oleh PAM mengenai Request password berdasarkan lama durasi waktu yang diminta pada masing-masing user yang mempunyai irisan waktu satu sama lainnya akan mendapatkan password yang saling berubah-ubah. Berbanding terbalik seperti tidak mengindahkan aturan yang sudah ditetapkan pada gambar di atas, atau disebut juga *override*. Seperti gambar di bawah ini.



Gambar 10 Durasi waktu request password yang saling berubah-ubah

4. KESIMPULAN

Mengacu kepada hasil bahasan maka diperoleh kesimpulan sebagai berikut :

1. Hasil dari penerapan PAM sudah dapat dipergunakan dengan baik oleh perusahaan dalam mengatur regulasi penggunaan *password* dan akses terhadap sistem yang kursial.
2. Bahwa PAM memberikan solusi untuk pengaturan identitas di dalam sebuah organisasi yang mencakup *lifecycle* dari sebuah identitas di dalam sebuah perusahaan yang mencakup otentikasi, otorisasi, audit dan *user administration*. PAM sudah mendukung aturan audit ISO 27001 yang sangat dibutuhkan.

5. SARAN

Berdasarkan hasil dan pembahasan diharapkan kedepannya teknologi perangkat lunak Java sudah tidak digunakan lagi dalam proses konkesi PSM, dikarenakan sangat berat dan memakan *resource* yang banyak dan tidak fleksibel. Diharapkan pihak pengembang tidak menggunakan Java untuk menjalankan *remote session.*

UCAPAN TERIMA KASIH

Ucapan terima kasih sedalam-dalamnya yang dengan ketulusan hati telah membantu baik secara moril dan materil sehingga Jurnal ini dapat tersusun disampaikan kepada :

1. Kepada keluarga tercinta. Bapak, Ibu, Bapak Mertua, Ibu Mertua, Istri, Anak dan Adik atas doa, semangat, motivasi, kasih sayang tak terhingga, serta dukungannya selama ini.
2. Bapak Ade Hendri Hendrawan, S.Kom., M.Kom. selaku kepala program studi Teknik Informatika.
3. Bapak Ade Hendri Hendrawan, S.Kom., M.Kom. Selaku Dosen Pembimbing 1 Jurnal yang sangat membantu menjadi pembimbing Dalam Penyusunan Jurnal.
4. Bapak Ritzkal S.Kom,. M.Kom Selaku Dosen Pembimbing 2 Jurnal dan dan sebagai Kepala Lab. NCC yang sangat membantu menjadi pembimbing dalam penyusunan naskah jurnal.
5. Teman-teman NCC (Angkatan 2011 dan Angkatan 2013) yang telah memberikan semangat dan motivasi, serta masukan yang bermanfaat bagi penyusun.

Ucapan terima kasih juga kepada semua pihak terkait, semoga Allah SWT membalas semua kebaikannya tak lupa kritik dan saran yang sifatnya membangun tentunya sangat diharapkan demi kesempurnaan laporan ini, dan mudah-mudahan untuk kedepannya dapat terus di perbaiki. Akhirnya, semoga laporan ini dapat bermanfaat khususnya untuk penyusun dan umumnya bagi semua yang membacanya.

DAFTAR PUSTAKA

[1] Bruno, A., & Jordan, S. (2011, Juni 9). CCDA 640-864 Official Cert Guide. Retrieved from books.google.co.id: https://books.google.co.id/books?id=cuOoV5u3WCUC&printsec=frontcover&dq=640-864 ccda&hl=en&sa=X&redir_esc=y#v=onepage&q=640-864-ccda&f=false

[2] Burnett, Mark. (2006). Perfect Passwords: Selection, Protection, Authentication. Canada: Syngress Publishing, Inc.

[3] Software, Quest. 2011. “Achieving ISO 27001 Compliance with Quest One Solutions for Privileged Access”. Quest Solution Brief.