Jurnal Maklumatika
Vol. 11, No. 1, Januari 2024, Hal. 12 – 21

P-ISSN 2407-5043
E-ISSN 3025-2997

Implementasi Keamanan *Server Domain Controller* Active Directory Domain Services terhadap Berbagai Threat dan Attack

Nanang Sadikin[1*], Muhammad Sultan Mahardika[2]
[1,2] Program Studi Teknik Informatika, Sekolah Tinggi Teknologi Informasi NIIT
Jalan Asem Dua No. 22 Kelurahan Cipete Selatan Kecamatan Cilandak Jakarta Selatan
email: nanang.sadikin@i-tech.ac.id[1], sultanmahardika1907@gmail.com[2]

* Penulis korespondensi

Diajukan: 11 Desember 2023
Direvisi: 31 Januari 2024
Diterima: 31 Januari 2024
Dipublikasikan: 31 Januari 2024

Abstract

Domain controller is a server that provides Active Directory Domain Services. Domain controller is a server that is the center of a LAN or WAN computer network. There are many attacks that can hit Domain controllers, for example Denial of service attacks to Brute force attacks. Security measures are used to secure the domain controller against various existing attacks and threats. This research uses literature study methods and observation methods, as well as applying appropriate security procedure. The goal is to implement Security measures on the network to prEvent attack and threat. The conclusion of the research results is that attack and threat can be prEvented by implement series of Security measures.

Keywords: ***Domain controller, Security, Active Directory Domain Services, Attack, Threat***

Abstrak

Domain controller merupakan *server* yang memberikan layanan Active Directory Domain Services. *Domain controller* adalah *server* yang menjadi pusat jaringan komputer LAN atau WAN. Ada banyak serangan yang bisa menimpa *Domain controller* misalnya Denial of Service Attak hingga *Brute force attack*. Langkah-langkah keamanan digunakan untuk mengamankan *domain controller* terhadap berbagai attack dan threat yang ada. Penelitian ini menggunakan metode studi pustaka, dan metode observasi, serta menerapkan langkah keamanan terhadap *domain controller* yang tepat. Tujuan yang dicapai adalah mengamankan *Domain controller* di dalam jaringan untuk mencegah *attack*. Simpulan hasil penelitian adalah *attack dan threat* bisa dicegah dengan menerapkan langkah-langkah keamanan yang sesuai.

Kata kunci: Domain controller, Keamanan, Active Directory Domain Services, Attack, Threat

1. PENDAHULUAN

1.1. Latar Belakang

Domain controller merupakan *server* yang mengatur keseluruhan jaringan komputer. *Domain controller* memberikan layanan *Active Directory Domain Services* (ADDS) di jaringan *Local Area Network* (LAN) dan *Wide Area Network* (WAN). Di dalam jaringan LAN dan WAN bisa terdapat lebih dari satu *server Domain controller*. Penggunaan lebih dari satu *domain controller* bertujuan untuk load balancing dan high avalaibility. *Domain controller* bisa berbagi beban atau load balancing satu sama lain jika terdapat lebih dari satu *server domain controller* di jaringan. User akan diotentikasi oleh *domain controller* yang paling dekat dan siap di jaringan. Load balancing ini terjadi otomatis tanpa campur tangan administrator. User hanya perlu memasukan paling sedikit dua buah DNS *Server* untuk menentukan lokasi *Domain controller*. Dengan adanya dua *domain controller* atau lebih, maka layanan Active Directory Domain Services memiliki tingkat ketersediaan yang tinggi atau *high available*. Jika ada satu *domain controller* yang *down*, maka fungsinya akan diambil

alih secara otomatis oleh *domain controller* yang lain. *Domain controller* yang *down* tersebut bisa diperbaiki dengan melakukan troubleshooting. Pilihan yang lain jika *domain controller* tersebut rusak secara permanen, *domain controller* tersebut dihapus dari sistem dan fungsinya dipindahkan ke *domain controller* yang lain. (Krause, J:2023)

Karena fungsi *domain controller* yang sangat penting di jaringan, maka *server domain controller* sering menjadi target orang yang berniat tidak baik. Serangan dan ancaman yang paling sering menyerang *domain controller* adalah *brute force attack* dan *denial of service attack*. Serangan *brute force attack* merupakan serangan yang mencoba untuk membobol *Active Directory Domain Services*. Serangan *brute force* akan mencoba untuk menggunakan kombinasi user name dan *password* yang memungkinkan. Hal ini karena misalnya nama user tertinggi domain yang sudah diketahui adalah Administrator. Sehingga penyerang akan mencoba berbagai kombinasi *password*. Bisa juga penyerang menggunakan daftar kata-kata yang sudah ada di kamus, sehingga serangan itu disebut dengan *dictionary attack*. Jika attack ini berhasil maka penyerang akan menguasai sistem Active Directory Domain Services secara keseluruhan. Sedangkan serangan *denial of service attack* merupakan serangan yang membuat *domain controller* menjadi lumpuh atau *down*. Serangan ini bukan untuk mencuri user name dan *password*, namun untuk membuat kerusakan pada *server*.

Untuk mengelola *domain controller* ada berbagai macam perangkat manajemen yang digunakan. Ada yang berbasis *Graphical User Interface* (GUI) dan ada yang berbasis teks atau *command line*. Perangkat yang berbasis GUI antara lain *Server Manager*, *Active Directory Administrative Center* (ADAC), *Active Directory Users and Computers, Active Directory Domain and Trust, Active Directory Sites and Services, Windows Admin Center, Domain Name System* (DNS) *Server*, serta *Services*. Sedangkan perangkat yang berbasis *command line* antara lain *Comma Separated Value Directory Exchange* (CSVDE), LDIFDE, *Directory Services Tools, Command line*, *Windows Scripting Host* (WSH), serta *Windows PowerShell*. Perangkat yang berbasis *command line* digunakan untuk membuat objek dalam jumlah banyak sekaligus sehingga lebih efisien. Selain itu *Command line* juga digunakan untuk troubleshooting *domain controller*. (Berkouwer, S:2022).

Ada banyak faktor yang menyebabkan ancaman dan serangan terhadap *domain controller* yang ada di jaringan. Sebab-sebab ancaman dan serangan tersebut antara lain sistem operasi dan perangkat lunak aplikasi yang tidak diperbarui (*update*). Selain itu juga bisa disebabkan oleh tidak adanya perlindungan dari *malicious software* seperti *virus, worm, trojan*, dan *ransomware*. Selain itu bisa juga disebabkan oleh konfigurasi yang tidak benar seperti penggunaan protocol yang bersifat *cleartext*, dan belum diaktifkannya *Windows Firewall*. Selain itu bisa disebabkan juga karena *password* yang dipakai tidak sesuai dengan ketentuan keamanan. Bisa juga disebabkan oleh kurangnya monitoring dari system administrator terhadap berbagai *log* yang ada misalnya DHCP *log* dan DNS *log*. Selain itu juga bisa disebabkan karena *audit* belum diaktifkan sehingga sulit untuk melacak serangan seperti apa yang terjadi. (Dunkerley, M:2022)

Windows *Firewall* merupakan software yang terdapat pada sistem operasi Windows dan Windows *Server* yang digunakan untuk mengamankan komputer. Windows *Firewall* merupakan perangkat lunak yang mengatur *traffic* apa saja yang boleh masuk dan boleh keluar dari sistem operasi Windows dan Windows *Server*. *Traffic* yang berasal dari luar komputer tidak akan diijinkan untuk masuk jika *traffic* tersebut berbahaya. Contoh *traffic* yang berbahaya misalnya serangan *Ping of Death* dan *Brute force attack*. Serangan *Ping of Death* serangan yang termasuk *Denial of service attack*. Serangan ini mengirimkan packet ping yang berukuran besar dalam jumlah yang banyak secara terus menerus sehingga membuat target menjadi *down*. *Brute force attack* merupakan serangan yang berusaha untuk membobol *password* pada sistem operasi target.

Ada dua *policy* yang terdapat pada Domain yaitu Default *Domain controller Policy* dan Default

P-ISSN 2407-5043
E-ISSN 3025-2997

Domain *Policy*. Default *Domain controller Policy* merupakan *policy* yang berkaitan dengan hak-hak yang terdapat pada *server Domain controller*. Sedangkan Default Domain *Policy* merupakan *Policy* yang berlaku secara keseluruhan untuk domain. Contoh *policy* yang berkaitan secara keseluruhan untuk domain adalah *password policy*. *Password Policy* mengatur berapa panjang *password* minimal, berapa umur minimal *password*, berapa umur maksimal *password*, apakah menggunakan kompleksitas atau tidak dan apakah disimpan menggunakan enkripsi atau tidak. (Francis, D:2021).

User *account* merupakan akun yang digunakan untuk bekerja di jaringan. Setiap pemakai harus memiliki akun yang terdaftar pada *Active Directory* dan disimpan oleh *domain controller*. Akun tersebut digunakan untuk *log*in ke jaringan pada komputer *client* atau *server*. Untuk *log*in maka pemakai harus memasukan nama akun beserta kata sandi atau *password*. Jika kedua informasi yang dimasukan tadi benar maka pemakai bisa bekerja di jaringan. Jika salah satu informasi tadi salah, atau bahkan keduanya salah maka pemakai akan ditolak untuk masuk ke jaringan. Jika tiga kali salah, maka akun tersebut akan dikunci. Hal ini karena adanya *policy* untuk mengunci akun tersebut dimana ada kemungkinan akun dicuri dan adanya upaya penerobosan di jaringan. Setiap akun yang ada memiliki tingkatan akses yang berbeda. Jika akun tersebut menjadi anggota group Domain Admins maka akun tersebut memiliki kekuasaan di satu domain. Jika akun tersebut menjadi anggota Enterprise Admins, maka akun tersebut memiliki kekuasaan di seluruh forest yang terdiri dari banyak domain. (Francis, D:2021).

Remote Desktop Protocol merupakan *protocol* yang digunakan untuk melakukan manajemen *Windows Server* dari jarak jauh. Sehingga Administrator tidak perlu datang langsung ke *server* di data center kalau itu merupakan *server* fisik. Namun, protocol ini secara default bekerja dalam modus *cleartext*. Artinya *username* dan *password* yang dimasukan akan terlihat di jaringan. Sehingga protocol RDP dikenal merupakan *protocol* yang kurang aman. Supaya aman maka protocol RDP harus dikombinasikan menggunakan enkripsi sertifikat *Secure Socket Layer* (SSL). Kalau tanpa enkripsi SSL, *username* dan *password* yang dimasukan akan muncul saat ditangkap menggunakan aplikasi *packet capture* di jaringan.

Endpoint Security merupakan perangkat lunak anti *malicious software* yang digunakan untuk melindungi sistem operasi dari berbagai serangan *malicious software* seperti virus, trojan, worm dan *ransomware*. *Endpoint security* akan mendeteksi serangan yang masuk dan menghentikan serangan tersebut. *Endpoint security* yang terpasang pada *domain controller* merupakan sebuah agent. Terdapat *Endpoint security server* yang menjadi pusat dari semua perangkat yang ada baik itu *server* maupun *client*. *Endpoint security server* akan mengatur semua *policy* yang berkaitan dengan keamanan komputer *client*, misalnya mengatur jadwal scan rutin, mengatur apakah drive portable seperti flashdisk diperbolehkan, scan otomatis setiap drive portable dimasukan ke port USB dan sebagainya. Selain itu *Endpoint security server* juga akan men*download* pattern atau database malware secara otomatis dan mendistribusikan kepada seluruh *client*.

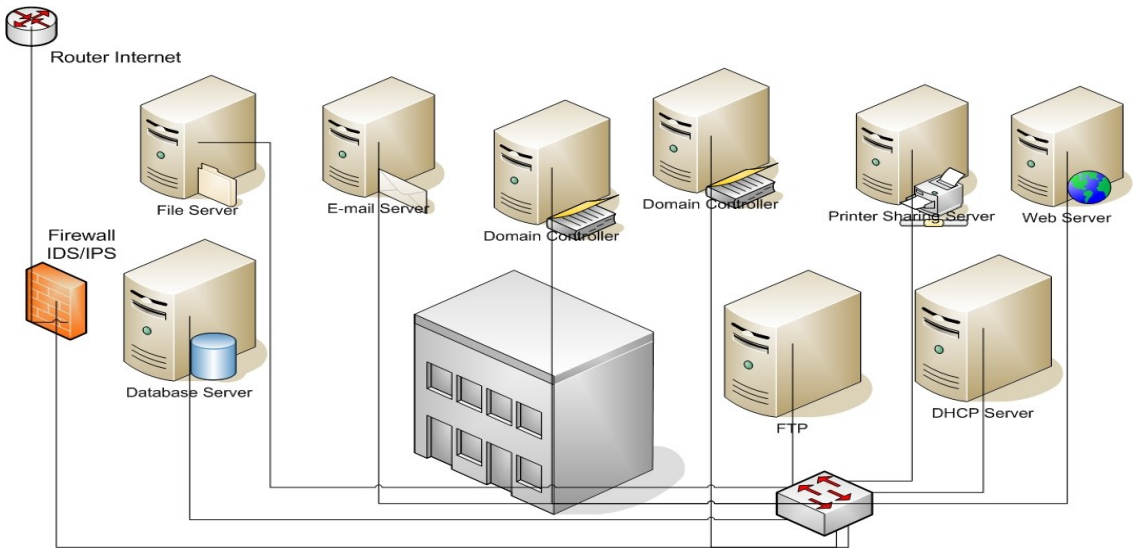
1.2. Rumusan Masalah

Berdasarkan uraian latar belakang yang telah dikemukakan tadi, masalah-masalah yang dirumuskan untuk penelitian ini adalah sebagai berikut:

1. Langkah-langkah keamanan apa yang digunakan untuk mengamankan Active Directory Domain Services *Domain controller*?
2. Bagaimana menerapkan Metode keamanan terhadap *server* Active Directory Domain Services *Domain controller*?

2. METODOLOGI PENELITIAN

Metode penelitian yang digunakan di dalam penelitian ini yaitu metode studi pustaka, dengan mempelajari berbagai literatur yang berkaitan dengan Keamanan *Active Directory*, keamanan informasi, dan *security* control lainnya. Selain itu metode yang digunakan adalah metode observasi dan studi kasus untuk mengamati objek dan lokasi tempat dimana penelitian dilakukan. Skema LAN dimana *Domain controller* yang akan diamankan ditunjukan pada gambar 2 di berikut ini.



Gambar 1. Diagram Jaringan *Active Directory Domain Services*

Pusat dari Jaringan komputer tersebut di atas adalah *server Domain controller* dari *Active Directory Domain Services* di Windows *Server*. Windows *Server* yang digunakan adalah Windows *Server* 2012 R2 Data Center. *Server Domain controller* tersebut berfungsi untuk melakukan otentikasi dari pemakai dan perangkat yang akan bekerja di jaringan. Selain berfungsi sebagai *server* otentikasi, *server* tersebut juga berfungsi sebagai *server Domain Name System* (DNS). *Server Domain controller* tersebut juga berfungsi sebagai *server Dynamic Host Configuration Protocol* (DHCP). *Server* DNS merupakan *server* yang bekerja untuk menterjemahkan nama domain atau nama komputer menjadi IP Address dan sebaliknya. *Server* DHCP merupakan *server* yang memberikan IP Address secara otomatis dan dinamis kepada komputer atau perangkat yang meminta IP Address. IP Address yang didapatkan oleh komputer *client* kemudian akan didaftarkan ke DNS *Server* secara otomatis.

File server yang ada di jaringan bukan merupakan *server domain controller*. *File server* merupakan *server* yang bergabung ke dalam domain atau join domain sehingga disebut sebagai member *server*. *File server* berfungsi untuk menangani layanan berbagi *file* dan *folder* antar pemakai di jaringan. *File server* memiliki kapasitas yang cukup besar yaitu lebih dari dua *terabyte*. Pemakai bisa mengakses *file* dan *folder* yang sudah dibagikan sesuai dengan hak akses yang sudah ditentukan. Hak akses tersebut ditentukan di dalam *Access Control Lists* (ACL) pada sistem *file* NTFS. Hanya NTFS yang memiliki ACL sedangkan sistem *file File* Allocation Table (FAT) atau FAT32 tidak memiliki ACL. *File server* ini menggunakan sistem operasi Windows *Server* 2012R2 Standard Edition.

Database *server* yang ada di jaringan bukan merupakan *server domain controller*. *Database server* merupakan *server* yang bergabung ke dalam domain atau join domain sehingga disebut sebagai member *server*. Database *server* berfungsi untuk menangani akses basis data dari aplikasi atau *client*. Database *server* memiliki kapasitas yang cukup besar yaitu lebih dari satu *terabyte*. Aplikasi yang berbasis web dan desktop mengakses database yang ada di database *server*. Setiap

P-ISSN 2407-5043
E-ISSN 3025-2997

aplikasi memiliki database tersendiri sehingga tidak saling mengganggu satu sama lain. Database *server* ini menggunakan sistem operasi Windows *Server* 2012R2 Standard Edition.

E-mail server yang ada di jaringan bukan merupakan *server domain controller*. *E-mail server* merupakan *server* yang bergabung ke dalam domain atau join domain sehingga disebut sebagai member *server*. *E-mail server* berfungsi untuk mengirim dan menerima *e-mail* dari *client* yang ada di jaringan lokal. Selain itu *e-mail server* juga mengirim dan menerima *e-mail* yang berasal dari Internet. *E-mail server* ini dilengkapi dengan aplikasi anti spam dan anti virus (ASAV) yang bisa menyaring *malicious software* seperti *virus, worm, trojan* dan *ransomware* yang akan masuk ke dalam jaringan melalui *e-mail*. *E-mail server* ini menggunakan sistem operasi Windows *Server* 2012R2 Standard Edition.

DHCP *server* yang ada di jaringan bukan merupakan *server domain controller*. DHCP *server* merupakan *server* yang bergabung ke dalam domain atau join domain sehingga disebut sebagai member *server*. DHCP *server* berfungsi untuk membagikan IP Address kepada komputer *client* atau perangkat lain membutuhkan IP Address. Selain itu DHCP *Server* juga akan mendaftarkan IP Address yang didapatkan oleh komputer *client* ke DNS *Server* sehingga record A dan PTR yang ada di DNS sesuai dengan informasi yang didapatkan oleh komputer *client*. Selain IP Address, DHCP *Server* juga akan membagikan parameter yang lain seperti Subnet Mask, *Default gateway*, DNS *Server*, DNS Domain Name dan lain sebagainya. DHCP *server* ini menggunakan sistem operasi Windows *Server* 2012R2 Standard Edition.

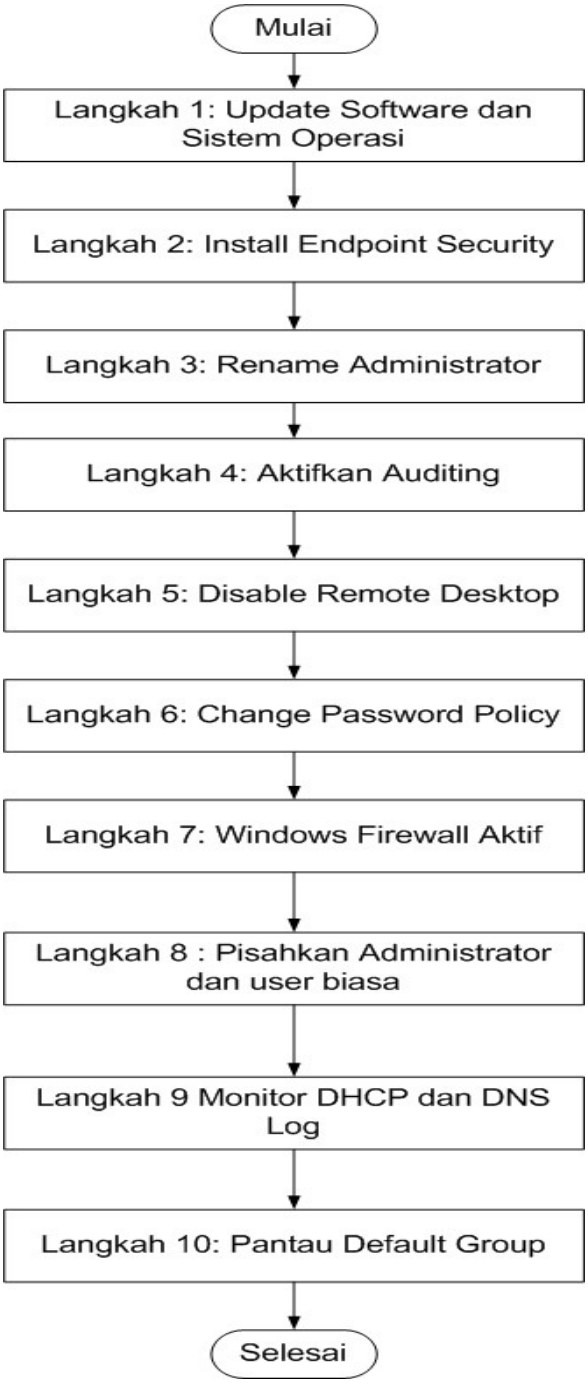
Web *server* yang ada di jaringan bukan merupakan *server domain controller*. Web *server* merupakan *server* yang bergabung ke dalam domain atau join domain sehingga disebut sebagai member *server*. Web *server* berfungsi untuk menampilkan web portal milik perusahaan. Web portal ini merupakan situs yang berisi informasi yang bersifat internal untuk pegawai perusahaan. Informasi web portal ini diperbarui setiap hari untuk menampilkan informasi-informasi penting untuk manajemen dan pegawai perusahaan. Informasi yang ditampilkan misalnya kebijakan cuti dan hari libur, kenaikan gaji, pertemuan tahunan dan sebagainya. Web *server* ini menggunakan sistem operasi Windows *Server* 2012R2 Standard Edition.

Printer *sharing server* yang ada di jaringan bukan merupakan *server domain controller*. Printer *sharing server* merupakan *server* yang bergabung ke dalam domain atau join domain sehingga disebut sebagai member *server*. Printer *sharing server* berfungsi untuk melayani pencetakan dokumen dari beberapa printer yang ada secara terpusat. Sehingga di jaringan tidak membutuhkan banyak printer yang harus disambungkan ke setiap komputer. Dengan printer *sharing server* cukup beberapa printer besar yang terkoneksi ke jaringan dan diatur oleh printer *sharing server*. Semua pemakai bisa mencetak dokumen sesuai dengan izin akses yang sudah diberikan. Printer *Sharing server* ini menggunakan sistem operasi Windows *Server* 2012R2 Standard Edition.

FTP *server* yang ada di jaringan bukan merupakan *server domain controller*. FTP *server* merupakan *server* yang bergabung ke dalam domain atau join domain sehingga disebut sebagai member *server*. FTP *server* berfungsi untuk tempat *download* dan *upload file* yang berukuran besar yang tidak bisa dikirim sebagai lampiran atau *attachment e-mail*. *File-file* yang berukuran besar umumnya adalah *file* ISO untuk instalasi sistem operasi atau aplikasi. *File-file* ISO ini umumnya berukuran di atas 4 GB. Misalnya ISO untuk instalasi Windows, Windows *Server* dan Microsoft office. Selain *file* ISO, *file* yang berukuran besar adalah *file-file* video atau data yang dipadatkan menggunakan aplikasi RAR atau ZIP. FTP *server* ini menggunakan sistem operasi Windows *Server* 2012R2 Standard Edition.

Selain itu di jaringan juga terdapat sebuah perangkat *firewall* yang digunakan untuk melindungi jaringan dari serangan yang berasal dari Internet. *Firewall* yang dipasang merupakan *firewall* yang berbentuk perangkat keras atau appliance. *Firewall* appliance yang dipasang pada jaringan memiliki dua buah interface. Satu *Interface* terhubung ke Internet melalui router yang terkoneksi ke Internet Service Provider (ISP). Internet yang terhubung ke Internet ini memiliki IP Address Public. Sedangkan satu buah *Interface firewall* yang lain terhubung ke jaringan LAN pada switch. *Interface* internal ini merupakan *default gateway* bagi komputer yang ada di jaringan LAN.

Gambar 3 di bawah ini menunjukan tahap-tahap yang dikerjakan untuk mengamankan domain controller Active Directory Domain Services dari berbagai threat dan attack.



Gambar 2. Alur Kerja Penerapan Metode Keamanan *Domain controller*

P-ISSN 2407-5043
E-ISSN 3025-2997

3. HASIL DAN PEMBAHASAN

Ada sepuluh langkah pengamanan Active Directory *Domain controller* yang akan diterapkan untuk mencegah attack yang dijelaskan lebih rinci sebagaimana berikut ini:

Langkah 1 Pengamanan

Langkah yang pertama kali dilakukan untuk mengamankan Active Directory *Domain controller* adalah dengan melakukan *upgrade* terhadap sistem operasi yang menjalankan *domain controller*. Sistem operasi yang digunakan saat ini adalah Windows *Server* 2012R2. Masa dukungan untuk Windows *Server* 2012R2 akan berakhir pada tanggal 14 Oktober 2023. Oleh karena itu perusahaan harus segera melakukan *upgrade* ke Windows *Server* versi yang lebih baru, yaitu Windows *Server* 2016, Windows *Server* 2019, atau Windows *Server* 2022. Ada dua metode *upgrade* terhadap *domain controller* yang bisa dilakukan. Pertama, *upgrade* menggunakan metode inplace *upgrade*. Pada metode inplace *upgrade*, *upgrade* sistem operasi langsung dilakukan pada mesin yang bersangkutan misalnya sistem operasi sebelumnya Windows *Server* 2012R2 dan sistem operasi penggantinya adalah Windows *Server* 2016. Caranya dengan menggunakan ISO atau DVD Windows *Server* 2016 yang dimasukan ke mesin 2012R2. Namun sebelum *upgrade* sistem operasi dilakukan terlebih dahulu harus menjalankan skema *update*. Setelah menjalankan skema *update* kemudian menjalankan *upgrade* sistem operasi. Cara kedua untuk melakukan *upgrade* sistem operasi *domain controller* adalah dengan metode *out of place upgrade*. Pada metode *out of place upgrade*, sistem operasi *domain controller* di*upgrade* menggunakan mesin yang berbeda. *Upgrade* dilakukan secara bertahap menggunakan virtual machine yang baru yang di*install* sistem operasi Windows *Server* 2016. Selanjutnya fungsi FSMO Roles yang ada kemudian dipindahkan dari Windows *Server* 2012R2 ke Windows *Server* 2016. Setelah sistem operasi di *upgrade* dari Windows *Server* 2012R2 ke Windows *Server* 2016, langkah selanjutnya adalah melakukan *update Security* terhadap Windows *Server* 2016. *Update security* ini dilakukan menggunakan Windows *Server Update* Service (WSUS) yang melakukan *download* dan *install security update* secara otomatis.

Langkah 2 Pengamanan

Langkah selanjutnya adalah melakukan instalasi *Endpoint Security* atau *Endpoint* Detection and Response (EDR) di *Domain controller* Windows *Server*. *Endpoint Security* atau EDR ini berfungsi untuk melakukan pencegahan terhadap berbagai threat dan attack yang mencoba untuk menyerang *domain controller* di Windows *Server* 2022. *Domain controller* ini akan di*install* sebagai salah satu *node* dari *Endpoint Security Server*. Instalasi EDR dilakukan dengan mengakses EDR *installation point* kemudian menjalankan *installation wizard* yang sudah disediakan. Setelah instalasi EDR selesai dilakukan langkah selanjutnya adalah melakukan *update* terhadap database dan pattern dari EDR agar bisa menangkal threat dan attack terbaru.

Langkah 3 Pengamanan

Langkah berikutnya untuk mengamankan *domain controller* active Directory domain Services adalah dengan mengganti nama administrator domain. Secara default, nama akun tertinggi yang memiliki hak akses yang tidak terbatas pada Active Directory Domain Services adalah Administrator. Nama akun ini merupakan akun yang umum sehingga menjadi target serangan *brute force attack* untuk mencoba menebak *password*. Nama akunnya sudah diketahui sehingga penyerang hanya tinggal mencoba untuk mendapatkan *password*. Penyerang akan berusaha untuk mendapatkan *password* dengan mencocokan kata-kata yang ada di kamus yang sering disebut dengan *dictionary attack*. Selain itu penyerang juga akan berusaha untuk mendapatkan *password* secara acak menggunakan *brute force attack*.

Langkah 4 Pengamanan

Langkah berikutnya yang dilakukan untuk mengamankan *Domain controller* adalah dengan mengaktifkan *Audit*ing. *Audit*ing merupakan fungsi untuk melakukan pencatatan secara rinci apa saja

yang terjadi di dalam sistem. Segala sesuatu yang terjadi akan dicatat di dalam *Event Log*. Ada tiga jenis *Event log* yang umum yang ada di Windows *Server*. System *Log* merupakan pencatatan yang berkaitan dengan Internal sistem operasi Windows *Server*. Misalnya ada services yang tidak jalan, driver yang bentrok dan sebagainya. Application *Log* merupakan pencatatan yang berkaitan dengan aplikasi yang ada di Windows *Server*. Misalnya ada aplikasi yang *crash* karena bentrok dengan aplikasi yang lain, atau ada *file* DLL dari aplikasi yang missing, dan sebagainya. *Security Log* merupakan pencatatan yang berkaitan dengan keamanan. Misalnya proses *logon* dan *log*off yang dilakukan oleh pemakai di jaringan. *Audit*ing yang diaktifkan nanti akan menyimpan semua catatan tersebut pada *Security Log* yang terdapat pada *Event Log*. *Event Log* ini bisa dilihat menggunakan *Event* Viewer *Log* yang terdapat pada *Server* Manager – Tools di Windows *Server*. *Audit*ing ini sendiri terbagi menjadi dua bagian yaitu *Success* dan *Failure*. *Success Audit* artinya hanya mencatat keberhasilan yang dilakukan oleh objek, misalnya *log*in user yang sukses saja yang dicatat. Sedangkan *Failure Audit* mencatat kegagalan *Event* yang terjadi, misalnya user gagal *log*in karena *password* salah. *Audit* ini bisa diaktifkan salah satu atau keduanya, *Success* saja atau *Failure* saja atau *Success* dan *Failure* sekaligus. Ada beberapa Setting yang bisa diaktifkan untuk *audit* ini. Setting tersebut yaitu *Audit account logon Event*s, *Audit account* management, *Audit* directory service access, *Audit logon Event*s, *Audit* object access, *Audit policy* changes, *Audit* privilege use, *Audit* process tracking, dan *Audit* system *Event*s.

*Audit account logon Event*s merupakan *audit* yang digunakan untuk mencatat keberhasilan atau kegagalan *log*in dari *account* domain Active Directory Domain Services. Sedangkan *Audit logon Event*s merupakan *audit* yang digunakan untuk mencatat keberhasilan atau kegagalan *logon* dari *account* local yang berada di komputer yang tergabung dengan domain atau join domain. *Audit account* management merupakan *audit* yang digunakan untuk mencatat pengelolaan akun, misalnya pembuatan user, group, contact dan sebagainya. *Audit* directory service access merupakan *audit* yang digunakan untuk mencatat apakah terjadi akses terhadap berbagai objek yang terdapat pada Active Directory. *Audit* object access merupakan *audit* yang digunakan untuk mencatat apakah terjadi akses terhadap objek-objek yang terdapat pada komputer lokal yang tergabung pada domain. *Audit policy changes* merupakan *audit* yang digunakan untuk mencatat apakah terjadi perubahan *policy* pada Active Directory Domain Services. *Audit* privilege use merupakan *audit* yang digunakan untuk mencatat apakah ada hak-hak administrator yang digunakan di dalam sistem. *Audit* process tracking merupakan *audit* yang digunakan untuk mencatat apakah ada proses-proses tertentu yang dijalankan dan sebagainya. *Audit* system *Event*s merupakan *audit* yang digunakan untuk mencatat kejadian-kejadian yang berhubungan dengan sistem. *Audit-audit* tersebut secara default berada pada Default *Domain controller Policy* dan belum diaktifkan. Setelah diaktifkan maka semua kejadian yang berhubungan dengan *audit* tersebut bisa dilihat pada *Event Log Security* yang bisa dilihat menggunakan *Event* Viewer *Log*. Kita bisa membuat Group *Policy* tersendiri untuk keperluan *audit* ini dan kita bisa mengaplikasikan Group *Policy* tersebut ke Domain, Site, maupun Organizational Unit sesuai dengan kebutuhan.

Langkah 5 Pengamanan

Langkah pengamanan *Domain controller* yang berikutnya adalah dengan menonaktifkan remote desktop protocol (RDP). Remote Desktop Protocol merupakan protocol yang digunakan untuk mengakses *server* secara remote melalui tampilan desktop langsung ke *server*. Remote Desktop Protocol (RDP) merupakan protocol yang memudahkan untuk mengelola *server*, namun protocol ini juga memiliki kelemahan. Protocol RDP ini secara default kurang aman karena tidak menggunakan enkripsi. User name dan *password* yang dimasukan melalui RDP akan terlihat di jaringan jika menggunakan perangkat lunak *packet capture*. Sehingga credential ini akan mudah untuk dicuri dan disalahgunakan oleh orang yang berniat tidak baik. Oleh karena itu protocol ini tidak diaktifkan. Untuk mengelola *server* Active Directory bisa menggunakan console virtualisasi secara langsung atau menggunakan keyboard mouse

P-ISSN 2407-5043
E-ISSN 3025-2997

dan monitor jika *server* fisik. Selain itu untuk pengelolaan jarak jauh bisa menggunakan Remote *Server* Administration Tools (RSAT) yang dipasang pada komputer lokal.

Langkah 6 Pengamanan

Langkah pengamanan berikutnya adalah dengan memperkuat *password* dengan mengubah *password policy*. Ada dua hal yang harus menjadi perhatian pada *password policy*. Pertama, adalah apa yang disebut *Complexity requirements*. *Complexity requirement* adalah setting yang mengatur *password* yang dibuat agar rumit sehingga tidak mudah untuk ditebak dan dibobol. Oleh karena itu setting *Complexity requirements* ini harus diubah menjadi *Enabled*. *Password* yang menggunakan setting *Complexity requirements* harus menggunakan kombinasi antara uppercase atau huruf besar, lower case atau huruf kecil, number atau angka dan juga karakter simbol. Huruf besar contohnya ABCDEF, sedangkan huruf kecil contohnya abcdef. Untuk angka contohnya 1234567890 sedangkan karakter simbol contohnya adalah karakter @#$%^&*(). Menggunakan kombinasi semua karakter tadi membuat *password* menjadi rumit dan sulit untuk dibobol. Contohnya *password* seperti "!nD0n3s!aMerD3k@" secara tertulis adalah Indonesia Merdeka, namun karena menggunakan berbagai karakter maka *password* tersebut menjadi sulit untuk dikenali. Kedua, yang harus diperhatikan disini adalah setting *Password Length* atau panjang *password*. *Password* yang singkat merupakan *password* yang mudah untuk dibobol contohnya misalnya **mobil**. *Password* ini hanya terdiri dari lima huruf dan huruf kecil semua. Selain itu kata **mobil** juga terdapat di dalam kamus. Oleh karena itu *password* yang singkat ini mudah untuk dibobol dan juga terkena serangan *dictionary attack* karena kata-kata ini terdapat di dalam kamus. Oleh karena itu *password* harus dibuat panjang setidaknya 15 karakter atau lebih sehingga tidak mudah untuk dipecahkan oleh orang-orang yang berniat tidak baik.

Langkah 7 Pengamanan

Langkah pengamanan *Domain controller* berikutnya adalah dengan mengaktifkan Windows *Firewall* yang terdapat di Windows *Server*. *Firewall* akan menyaring lalu lintas jaringan yang datang dan pergi. Inbound connection merupakan koneksi yang datang dari computer lain menuju *Domain controller*, misalnya dari computer *client* yang bergabung dengan domain ke *domain controller* untuk meminta otentikasi. Sedangkan outbound connection merupakan koneksi yang berasal dari *Domain controller* Active Directory Domain Services ke luar atau ke komputer lain di jaringan. Serangan yang mengancam *Domain controller* Active Directory Domain Services umumnya merupakan serangan yang berasal dari Inbound connection. Inbound connection ini bisa saja berasal dari komputer *client* yang sudah terkena *malicious software*. Sehingga *malicious software* yang tertanam di komputer *client* memanfaatkan komputer tersebut untuk melakukan attack terhadap *Domain controller* yang ada di jaringan. Jika di *Domain controller* tersebut dipasang *Endpoint Security*, maka tugas Windows *Firewall* akan diambil alih oleh *Endpoint Security* tersebut.

Langkah 8 Pengamanan

Langkah pengamanan berikutnya adalah pisahkan antara user biasa dengan Administrator. Jadi untuk penggunaan sehari-hari bekerja, misalnya mengirim dan menerima *e-mail*, membuat dokumen, mencetak, mengakses Internet, gunakan user biasa yang bukan merupakan Administrator. Sedangkan untuk untuk mengelola domain gunakan user yang sudah diberikan ijin akses misalnya untuk membuat user, mereset *password*, mengubah keanggotaan group dari user. Selain itu jangan gunakan user yang memiliki hak akses yang paling tinggi seperti Enterprise Administrator dan Schema Administrator karena jika user tersebut dicuri akan membahayakan jaringan Active Directory Domain Services secara keseluruhan.

Langkah 9 Pengamanan

Langkah yang kesembilan di dalam pengamanan Active Directory adalah memeriksa *log* DHCP dan DNS *Server*. DHCP *Server* merupakan *server* yang memberikan IP Address secara dinamis dan otomatis

kepada perangkat yang ada di jaringan, baik itu komputer, mobile device, atau perangkat lain yang ingin tersambung ke jaringan. Oleh karena itu administrator harus memeriksa *log* DHCP *Server* untuk memastikan apakah ada perangkat yang tidak dikenal yang mencoba masuk untuk mendapatkan IP Address. Seharusnya semua perangkat yang ada di jaringan harus menggunakan Media Access Control Address (MAC) atau alamat perangkat keras yang terdaftar di jaringan. MAC tersebut bisa didaftarkan pada DHCP *server* atau pada perangkat switch layer 2 atau switch layer 3 yang bisa dikelola. Selain itu Administrator juga harus memeriksa *log* DNS *Server* untuk memastikan tidak ada permintaan menuju ke alamat Internet yang tidak dikenal atau berbahaya.

Metode 10 Pengamanan

Langkah yang terakhir yang perlu dilakukan dalam mengamankan Active Directory *Domain controller* adalah dengan memantau Default Groups yang terdapat di dalam Active Directory. Jangan sampai di dalam Default Groups yang terdapat di dalam Active Directory Domain Services ada akun yang mencurigakan dan memiliki akes ke seluruh sistem. Default Groups yang terdapat di dalam Active Directory antara lain adalah Access Control Assistance Operators, *Account* Operators, Administrators, Allowed RODC *Password* Replication, Backup Operators, Certificate Service DCOM Access, Cert Publishers, Cloneable *Domain controller*s, Cryptographic Operators. Selain itu ada juga group Denied RODC *Password* Replication, Device Owners, DHCP Administrators, DHCP Users, Distributed COM Users, Dns*Update*Proxy, DnsAdmins, Domain Admins, Domain Computers, *Domain controller*s, Domain Guests, Domain Users. Group Default lain yang terdapat pada *Domain controller* adalah Enterprise Admins, Enterprise Key Admins, Enterprise Read-only *Domain controller*s, *Event Log* Readers, Group *Policy* Creator Owners, Guests, Hyper-V Administrators, IIS_IUSRS, Incoming Forest Trust Builders, Key Admins, Network Configuration Operators, Performance *Log* Users, Performance Monitor Users, Pre–Windows 2000 Compatible Access, Print Operators, Protected Users, RAS and IAS *Server*s. Selain itu ada juga group RDS *Endpoint Server*s, RDS Management *Server*s, RDS Remote Access *Server*s, Read-only *Domain controller*s, Remote Desktop Users, Remote Management Users, Replicator, Schema Admins, *Server* Operators, Storage Replica Administrators, System Managed *Account*s, Terminal *Server* License *Server*s, Users, Windows Authorization Access, serta group WinRMRemoteWMIUser.

4. SIMPULAN

Berdasarkan pembahasan di atas, kesimpulan hasil penelitian ini adalah sebagai berikut:

1. Langkah-langkah pengamanan yang digunakan untuk mengamankan Active Directory Domain Services *Domain controller* antara lain adalah *Update* software dan OS, *Install Endpoint Security*, Rename Administrator, Aktifkan *Audit*ing, disable Remote desktop, Perpanjang *password policy*, Aktifkan Windows *Firewall*, Memisahkan Administrator dan User biasa, Monitor *Log* DHCP dan DNS, Monitor Default Groups.
2. Metode pengamanan tersebut diterapkan dengan cara mengubah konfigurasi yang terdapat di *server Domain controller* yang terdapat di jaringan serta melakukan instalasi *Endpoint security*.

DAFTAR PUSTAKA

Berkouwer, S. (2022). Active Directory Administration Cookbook Second Edition. Packt Publishing. Mumbai.

Dunkerley, M. (2022). Mastering Windows *Security* and Hardening Second Edition. Packt Publishing. Mumbai.

Francis, D (2021). Mastering Active Directory Third Edition. Packt Publishing. Mumbai.

Krause, J. (2023). Mastering Windows *Server* 2022 Fourth Edition. Packt Publishing. Mumbai.