Jurnal Sistem Komputer dan Kecerdasan Buatan
Volume VII Nomor 2 Februari 2024

Update Software Sistem Operasi Server Infrastruktur dengan *Status End Of Support* Untuk Mengatasi Celah *Vulnerability* Guna Mencegah *Malicious Software*

Nanang Sadikin

Sekolah Tinggi Teknologi Informasi NIIT
Jl Asem Dua No. 22 Cipete Cilandak Jakarta Selatan
nanang_sadikin@yahoo.com

Diterima : 03 Januari 2024
Disetujui : 01 Februari 2024

***Abstrak*— Sistem operasi yang sudah tidak didukung lagi oleh pembuat perangkat lunak mengakibatkan tidak akan menerima lagi update yang berupa service patch, security update, maupun hotfix. Sehingga ini menimbulkan kelemahan atau celah keamanan yang disebut vulnerability. Jika vulnerability tidak ditambal maka akan menjadi pintu masuk bagi malicous software. Langkah-langkah update digunakan untuk memperbarui sistem operasi server infrastruktur untuk menutup celah keamanan atau vulnerability. Penelitian ini menggunakan metode studi pustaka, dan metode observasi, serta menerapkan langkah update yang tepat. Tujuan yang dicapai adalah mengupdate sistem operasi server infrastruktur yang ada. Simpulan hasil penelitian adalah update sistem operasi membuat sistem operasi memiliki vulnerability yang lebih kecil.**

Kata kunci: Update, Software, Sistem Operasi, Vulnerability, Malicious Software

I. PENDAHULUAN

Setiap perangkat lunak memiliki jangka waktu dukungan dari perusahaan yang membuatnya. Contoh perangkat lunak misalnya sistem operasi, aplikasi, anti virus dan lain sebagainya. Sistem operasi Windows Server merupakan sistem operasi yang dibuat oleh Microsoft. Windows Server 2012 dan Windows Server 2012R2 merupakan perangkat lunak yang berakhir dukungannya pada tanggal 10 Oktober 2023. Windows Server 2012R2 pertama kali diluncurkan pada tanggal 18 Oktober 2013 sedangkan Windows Server 2012 diluncurkan pertama kali pada tanggal 4 September 2012. Sejak dihentikan dukungan teknisnya pada tanggal 10 Oktober 2023, maka Windows Server 2012 dan Windows Server 2012R2 tidak akan mendapatkan update. Update yang dihentikan termasuk update yang berhubungan dengan bug perangkat lunak maupun update yang berhubungan dengan keamanan. Oleh karena itu Windows Server 2012 dan Windows Server 2012R2 tidak akan mendapatkan lagi update yang berupa Security Update, Windows Update, Hotfix, Security Patch dan sebagainya. Karena itu maka pengguna yang masih menggunakan Windows Server 2012 dan Windows Server 2012R2 disarankan atau diwajibkan untuk mengganti sistem operasi tersebut menjadi versi yang lebih baru seperti Windows Server 2016, Windows Server 2019, atau Windows Server 2022.

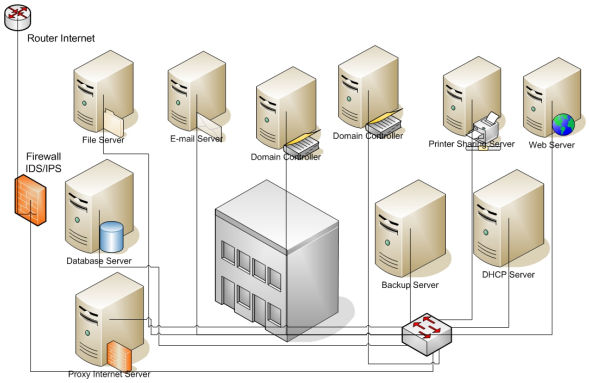
Tidak ada perangkat lunak yang sempurna termasuk Windows Server 2012 dan Windows Server 2012R2. Semua perangkat lunak yang ada pasti memiliki kelemahan yang disebut dengan vulnerability[1]. Setiap pembuat perangkat lunak memberikan dukungan perbaikan atau update dalam jangka waktu tertentu, misalnya selama sepuluh tahun. Dalam jangka waktu dukungan tersebut, jika ditemukan kelemahan maka

perusahaan pembuat perangkat lunak akan memberikan perbaikan secara gratis. Kelemahan atau vulnerability tersebut secara umum ada dua. Pertama, kelemahan perangkat lunak akibat adanya bug sehingga fungsi perangkat lunak tersebut terganggu. Kedua, kelemahan perangkat lunak yang berhubungan dengan fungsi keamanan. Kedua kelemahan tersebut bisa mengakibatkan kerugian jika tidak ditangani.

Kelemahan yang berhubungan dengan fungsi keamanan pada perangkat lunak termasuk hal yang beresiko tinggi. Hal ini karena kelemahan tersebut jika dimanfaatkan oleh orang yang berniat tidak baik akan menjadi pintu masuk bagi malicious software. Malicious software merupakan perangkat lunak yang berbahaya seperti virus, worm, trojan dan ransomware [3]. Virus merupakan perangkat lunak yang bisa masuk ke dalam sistem komputer melalui berbagai cara. Satu diantaranya adalah melalui lampiran yang di download pada e-mail. Virus juga bisa masuk melalui download otomatis saat mengunjungi suatu website yang berbahaya. Worm merupakan perangkat lunak yang berbahaya yang bisa menginfeksi komputer melalui jaringan tanpa adanya media perantara seperti file atau attachment seperti virus. Trojan merupakan perangkat lunak yang berbahaya yang tampak seperti perangkat lunak yang berguna, misalnya game catur. Tanpa disadari trojan merupakan pintu belakang yang bisa dimanfaatkan untuk mengendalikan komputer korban. Ransomware merupakan perangkat lunak yang berbahaya yang bekerja dengan cara mengenkripsi file yang dimiliki korban dan meminta tebusan.

II. METODE PENELITIAN

Metode penelitian yang digunakan di dalam penelitian ini yaitu metode studi pustaka, dengan mempelajari berbagai literatur yang berkaitan dengan Sistem Operasi dan Windows Server. Selain itu metode yang digunakan adalah metode observasi dan studi kasus untuk mengamati objek dan lokasi tempat dimana penelitian dilakukan. Diagram jaringan LAN dimana sistem operasi Windows Server yang akan diupgrade ditunjukan pada gambar 1 di berikut ini.



Gambar 1. Infrastruktur Server

Gambar 1 di atas menampilkan diagram jaringan dimana terdapat server-server yang berfungsi sebagai server infrastruktur di perusahaan. Di jaringan LAN tersebut terdapat dua server domain controller. Server domain controller merupakan server yang berfungsi untuk melakukan otentikasi terhadap pemakai yang login ke jaringan [7]. Server domain controller ini juga berfungsi sebagai Domain Name System (DNS) Server. Domain Name System (DNS) Server merupakan server yang bekerja untuk menerjemahkan nama domain atau nama host menjadi IP Address dan sebaliknya [2]. Dua server domain controller dan DNS Server membentuk sistem high availability atau HA. Jika satu server mengalami masalah, maka fungsi server tersebut akan diambil alih server yang berada di sebelahnya. Kedua server domain controller dan DNS Server tersebut menggunakan sistem operasi Windows Server 2012R2 Data Center Edition.

Pada gambar 1 di atas juga terdapat server Dynamic Host Configuration Protocol (DHCP). Server DHCP merupakan server yang bekerja untuk membagikan IP Address secara dinamis dan otomatis kepada komputer client atau perangkat lain yang meminta IP Address di jaringan [5]. Selain IP Address, Server DHCP juga membagikan parameter yang lain seperti subnet mask, default gateway, alamat DNS Server, dan DNS Domain Name. Server DHCP memiliki sebuah Scope yang berisi rentang IP Address yang akan dibagikan kepada komputer client dan perangkat lain. Pada Server DHCP, parameter yang akan dibagikan selain IP Address dimasukan sebagai Scope Options. Server DHCP ini bergabung ke dalam domain yang diatur oleh domain controller. Server DHCP menggunakan sistem operasi Windows Server 2012 Standard Edition.

Di jaringan ini terdapat sebuah File Server yang bergabung ke dalam domain yang diatur oleh domain controller. Pada File server terdapat folder-folder yang di sharing agar bisa diakses oleh komputer client dan server lain yang berada di jaringan. Pemakai bisa mengakses folder sharing sesuai dengan hak yang sudah ditentukan di dalam Access Control Lists (ACL). File Server tersebut menggunakan disk yang memakai partisi dengan sistem file NT File System (NTFS). Sistem File NTFS memungkinkan untuk mengunci file dan folder agar bisa diakses hanya oleh pemakai yang berhak. Tidak hanya folder yang dibuat ACL, bahkan sampai level file. File server menggunakan sistem operasi Windows Server 2012R2 Standard Edition.

Di jaringan terdapat sebuah email server yang bergabung ke dalam domain yang diatur oleh domain controller. Server e-mail ini bertugas untuk mengirimkan e-mail ke sesama pemakai yang ada di dalam jaringan. Selain itu e-mail server ini juga akan mengirim e-mail ke Internet dan menerima e-mail dari Internet. Pemakai yang mengakses e-mail dari komputer client menggunakan perangkat lunak e-mail client. Di dalam e-mail server terdapat database yang menyimpan mailbox untuk semua pemakai yang ada di jaringan. E-mail server ini menggunakan Windows Server 2012R2 Standard Edition.

Di jaringan ini juga terdapat printer sharing server yang tergabung dalam domain yang diatur oleh domain controller. Printer sharing server merupakan server yang memberikan layanan untuk pencetakan dokumen. Pada printer sharing server terdapat beberapa printer yang terkoneksi di jaringan. Driver untuk semua printer tersebut terpasang pada printer sharing server. Printer yang sudah terpasang tersebut kemudian di sharing agar bisa diakses oleh semua pemakai di jaringan. Sehingga di masing-masing komputer client tidak perlu ada printer yang terhubung langsung. Hal ini akan menghemat untuk jumlah printer yang ada. Cukup beberapa printer yang ada di printer sharing server dan bisa digunakan oleh semua pemakai di jaringan. Printer sharing server tersebut menggunakan sistem operasi Windows Server 2012R2 Standard Edition.

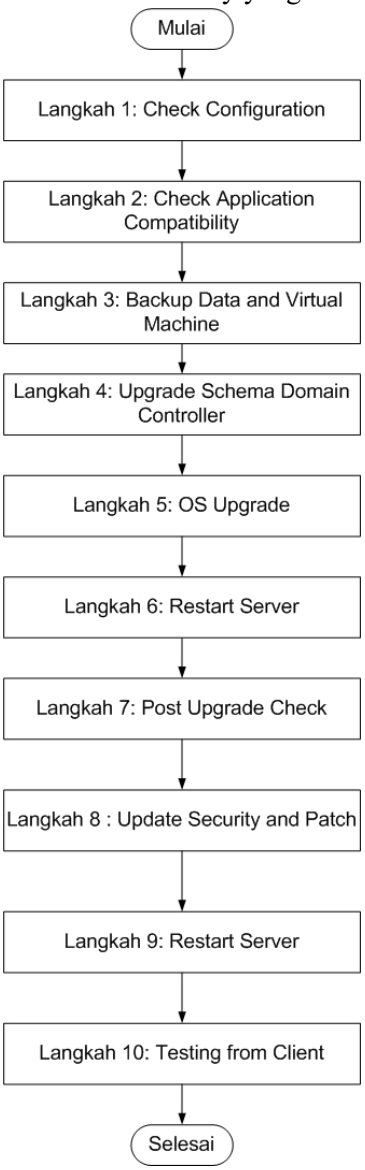
Di jaringan juga terdapat sebuah web server yang tergabung dalam domain yang diatur oleh domain controller. Web server ini berfungsi sebagai portal untuk menampilkan informasi perusahaan. Web server ini menghosting file-file yang digunakan untuk ditampilkan pada web browser, seperti file-file HTML, CSS, ASP, Java Script dan lain sebagainya. Untuk menampilkan web portal tersebut, pemakai menggunakan web browser dari komputer client dan mengetikan alamat URL. Alamat URL pada web server tersebut dikonfigurasikan pada DNS Server. Dengan adanya nama domain maka pemakai tidak perlu menggunakan IP Address untuk mengakses web portal. Cukup menggunakan nama domain yang sudah ditentukan. Web Server tersebut menggunakan sistem operasi Windows Server 2012R2 Standard Edition.

Di jaringan ini juga terdapat sebuah database server yang tergabung dalam domain yang diatur oleh domain controller. Database server ini menyimpan beberapa database yang digunakan oleh aplikasi yang ada di perusahaan. Database server ini menyimpan database yang digunakan oleh aplikasi yang berbasis web maupun aplikasi yang berbasis desktop. Aplikasi yang berbasis web terletak di server yang terpisah dengan database server. Aplikasi yang berbentuk web dibuat menggunakan ASP.NET, sedangkan aplikasi desktop terpasang pada beberapa komputer client. Database Server ini menggunakan sistem operasi Windows Server 2012R2 Standard Edition. Sedangkan aplikasi database server yang digunakan adalah SQL Server 2016 Standard Edition.

Di jaringan ini juga terdapat sebuah server backup yang tergabung dalam domain yang diatur oleh domain controller. Server backup ini terhubung dengan sebuah perangkat LTO atau tape drive. Backup server terhubung ke perangkat LTO menggunakan kabel SAS yang terdapat pada server backup dan konektor SAS yang terdapat pada perangkat LTO. Perangkat LTO tersebut bisa memuat delapan buah tape cartridge yang digunakan untuk membackup data. Software backup yang terpasang pada server backup adalah CA ArcServe. Di semua server yang dibackup dipasang backup Agent yang sesuai. Di server Active Directory Domain Controller dipasang agent Open Files. Pada Server File Sharing dipasang Agent for Open Files. Pada Server E-mail dipaang Agent for Exchange Server. Pada Server database dipasang agent for SQL Server.

Di Server Printer Sharing juga terpasang Agent for open files. Pada web Server juga terpasang agent for Open files. Pada Server DHCP juga terpasang agent for open files. Selain itu disemua server selain server backup juga terpasang Agent for virtual machine. Hal ini karena semua server kecuali backup server merupakan server yang berupa virtual machine. Server Backup ini menggunakan sistem operasi Windows Server 2012R2 Standard Edition.

Gambar 2 di bawah ini menunjukan tahap-tahap yang dikerjakan untuk mengupgrade sistem operasi Windows Server di jaringan untuk mengatasi celah vulnerability yang ada:



Gambar 2. Alur Kerja Update Sistem Operasi dan Security Patch

Gambar 2 di atas menjelaskan langkah-langkah yang dilakukan untuk mengupgrade sistem operasi yang terdapat pada masing-masing server infrastruktur secara berurutan.

III. HASIL DAN PEMBAHASAN

Ada sepuluh langkah untuk melakukan upgrade sistem operasi Windows Server yang dijelaskan lebih rinci sebagai berikut.

Langkah 1 Update

Langkah yang pertama kali dilakukan adalah memeriksa konfigurasi sistem operasi Windows Server. Konfigurasi yang harus dicek antara lain adalah nama komputer dan nama domain, IP Address komputer beserta dengan parameternya antara lain subnet mask, default gateway dan DNS Server. Selain itu yang harus dicek antara lain konfigurasi Remote Desktop, Windows Firewall serta Time zone. Selain itu yang perlu dicek juga versi sistem operasi yang digunakan. Hal ini penting karena lisensi sistem operasi yang berikutnya harus sesuai dengan lisensi sistem operasi yang akan diupgrade. Jika saat ini menggunakan edisi Standard maka sistem operasi penggantinya harus menggunakan edisi Standard. Jika saat ini menggunakan edisi Data Center, maka sistem operasi penggantinya juga harus menggunakan edisi Data Center.

Langkah 2 Update

Langkah yang kedua adalah melakukan check terhadap kompatibilitas aplikasi yang terpasang. Hal ini penting agar aplikasi yang sudah ada di server yang ada saat ini bisa berjalan dengan baik pada sistem operasi yang pengganti setelah upgrade dilakukan. Umumnya untuk aplikasi yang satu pabrik dengan sistem operasi tidak mengalami kesulitan dalam hal kompatibilitas. Yang perlu diperhatikan terutama adalah aplikasi yang berasal dari pihak ketiga seperti aplikasi backup, anti virus, atau aplikasi custom yang dibuat untuk fungsi tertentu. Contoh aplikasi custom misalnya aplikasi Enterprise Resource Planning (ERP). Kompatibilitas ini perlu diperiksa dengan menghubungi vendor yang membuat aplikasi tersebut. Atau bisa juga dengan melihat pada website vendor yang bersangkutan pada bagian hardware and software compatibility list. Misalnya aplikasi backup bisa berjalan dengan

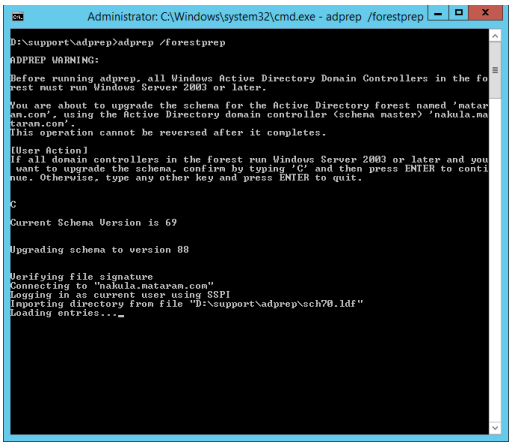
baik pada sistem operasi Windows Server 2012R2 dan Windows Server 2016. Kalau kompatibel tidak ada masalah. Namun jika tidak kompatibel, kita juga harus melakukan upgrade untuk aplikasi yang bersangkutan.

Langkah 3 Update

Langkah berikutnya sebelum melakukan update terhadap sistem operasi adalah dengan melakukan backup. Ada dua hal yang harus dibackup yaitu data dan sistem operasi itu sendiri [4]. Backup terhadap data bisa dilakukan menggunakan perangkat lunak khusus backup seperti Backup Exec atau ArcServe. Backup dilakukan menggunakan agent backup pada sistem yang menjadi target untuk dibackup. Jika misalnya akan membackup data yang ada di file server, maka agent for open files yang akan digunakan. Jika akan membackup data yang terdapat pada database server, maka akan menggunakan agent for SQL Server. Untuk membackup mailbox yang berada di Exchange maka bisa menggunakan agent for exchange. Untuk membackup sistem operasi beserta semua isinya bisa menggunakan agent for virtual machine. Backup tersebut semuanya disimpan pada sebuah tape yang dimuat ke dalam tape drive. Jenis backup yang dilakukan adalah Full Backup, artinya membackup semua yang ada secara keseluruhan.

Langkah 4 Update

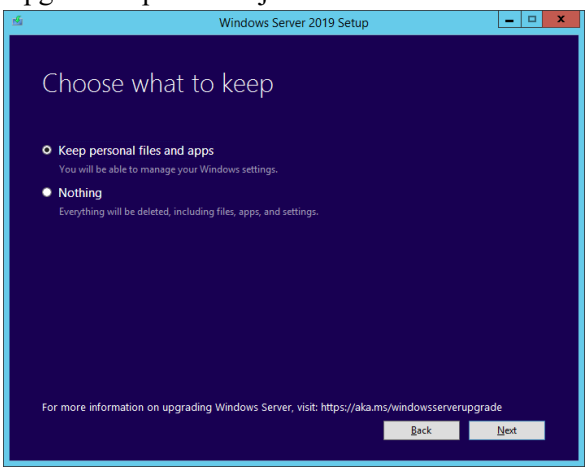
Langkah berikutnya yang harus dilakukan adalah melakukan update terhadap schema Active Directory Domain Services yang ada di server Domain Controller. Schema merupakan metadata atau data tentang data dari Active Directory Domain Services [8]. Windows Server 2012 memiliki versi schema XX sedangkan Windows Server 2016 memiliki versi Schema XX. Windows Server 2019 memiliki schema versi XX dan Windows Server 2022 memiliki schema versi XX. Ada beberapa proses update yang harus dilakukan terhadap server domain controller. Pertama adalah mengupdate Forest atau Forest Preparation. Proses update ini dilakukan di level forest, karena forest merupakan hirarki Active Directory yang paling tinggi. Langkah selanjutnya adalah melakukan update domain yang terdapat di dalam forest. Langkah selanjutnya adalah melakukan update Group Policy Object. Dan terakhir adalah melakukan update Read Only Domain Controller (RODC).



Gambar 3. Forest Preparation

Langkah 5 Update

Langkah yang kelima adalah melakukan update sistem operasi Windows Server. Pertama kali yang dilakukan adalah menyiapkan DVD Instalasi Windows Server 2016. Setelah itu layar instalasi Windows Server 2016 muncul dan diminta untuk memilih sistem operasi yang sesuai. Pilih sesuai dengan jenis lisensi yang dimiliki. Kemudian akan muncul layar untuk menerima pernyataan lisensi. Setelah itu kemudian berlanjut pada pilihan untuk instalasi baru atau mempertahankan konfigurasi yang ada. Pilih mempertahankan konfigurasi yang ada agar apa yang sudah ada di dalam sistem operasi yang lama tidak hilang. Setelah itu proses Upgrade siap untuk dijalankan.



Gambar 4. Konfigurasi

Langkah 6 Update

Langkah selanjutnya adalah melakukan Restart terhadap server. Proses restart ini sendiri akan terjadi beberapa kali selama instalasi berlangsung.

Jadi pastikan bahwa selama proses restart berlangsung tidak terjadi hal-hal yang tidak diinginkan. Hal yang terburuk yang kemungkinan terjadi adalah Blue Screen of Death (BSOD) dimana layar monitor berubah menjadi biru dan terjadi logging debug ke dalam file LOG. Hal ini biasanya terjadi karena ada driver yang konflik atau memory yang tidak cukup. Biasanya setelah terjadi BSOD, komputer akan melakukan restart dengan sendirinya. Setelah itu proses mencoba untuk melanjutkan proses upgrade. Jika gagal, maka kemungkinan besar sistem operasi sudah rusak dan terpaksa harus melakukan restore dari backup. Namun, ini jarang terjadi karena umumnya proses upgrade berjalan dengan mulus.

Langkah 7 Update

Proses update telah selesai dilakukan. Langkah selanjutnya adalah melakukan pemeriksaan pasca update atau post-upgrade check. Ada beberapa hal yang harus diperiksa kembali. Pertama, pastikan semua konfigurasi sama seperti sebelum upgrade, misalnya nama komputer, IP Address beserta dengan parameternya seperti Subnet Mask, Default gateway dan DNS Server, zona waktu, Remote Desktop, Windows Firewall, dan sebagainya. Kedua, pastikan data yang terdapat pada harddisk tidak hilang, misalnya data file sharing yang terdapat pada storage atau lokasi penyimpanan lainnya. Ketiga, pastikan semua services yang ada berjalan sebagaimana mestinya misalkan DHCP, DNS, Active Directory Domain Services, Exchange Server, SQL Server, File Server Resource Manager dan lain-lain. Keempat, pastikan aplikasi yang ada berjalan dengan baik misalnya Exchange Server, SQL Server, Backup Server, Anti Virus dan sebagainya. Kelima, pastikan di dalam Event Log tidak terdapat hal-hal yang mencurigakan dengan tanda Warning atau Error.

Langkah 8 Update

Berikutnya setelah memastikan semua berjalan dengan lancar, langkah selanjutnya adalah melakukan instalasi Security Update dan Windows Update. Security Update dan Windows Update bisa dilakukan dengan cara manual satu per satu. Cara lain yang bisa dilakukan secara otomatis adalah dengan menggunakan Windows Server Update Services (WSUS) [6]. WSUS merupakan layanan yang ada di Windows Server yang berupa sebuah roles di Windows Server. WSUS ini bisa diinstall di sebuah server, atau digabungkan dengan server yang lain misalnya server Active Directory Domain Services. Setelah itu langkah selanjutnya adalah mengkonfigurasikan Windows Update dan Security Update menggunakan Group Policy Object (GPO). Setelah GPO terbuat, selanjutnya adalah menghubungkan GPO tersebut ke Organizational Unit tempat server berada.

Langkah 9 Update

Setelah Windows Update dan Security Update dijalankan, langkah selanjutnya adalah melakukan restart terhadap server. Hal ini dilakukan untuk memastikan Windows Server bekerja dengan benar setelah semua update dipasang. Selain itu pastikan juga aplikasi yang terpasang pada server berjalan sebagaimana mestinya. Caranya dengan membuka console aplikasi yang bersangkutan misalnya SQL Server Studio, Exchange Management Console, File Server Resource Manager, dan sebagainya. Selain itu pastikan juga Services yang terdapat pada services console berjalan dengan status Running [9]. Hal ini terutama untuk services dengan Startup Type Automatic.

Langkah 10 Update

Langkah terakhir dari semua tahapan update adalah melakukan pengujian di sisi client. Hal ini untuk memastikan bahwa client bisa bekerja dan menggunakan semua layanan yang disediakan oleh server. Misalnya melakukan pengujian dari komputer client yang login terlebih dahulu ke domain. Setelah itu client bisa membuka sharing folder yang ada di file server. Jika share folder bisa terbuka maka file server sudah berjalan dengan baik. Setelah itu client bisa membuka e-mail client seperti Outlook kemudian mengakses e-mail server. Setelah itu client bisa membuka database client untuk mengakses database server. Jika database server bisa di query dengan baik berarti database server juga berjalan dengan sempurna.

IV. KESIMPULAN

Berdasarkan pembahasan di atas, kesimpulan hasil penelitian ini adalah sebagai berikut. Langkah-langkah untuk mengupdate Windows Server adalah memeriksa konfigurasi yang ada, memeriksa kompatibilitas aplikasi yang ada, melakukan backup data dan sistem, melakukan update schema Active Directory, melakukan upgrade sistem operasi, melakukan restart server, melakukan pemeriksaan pasca upgrade sistem operasi, melakukan update windows dan update security, restart server, dan terakhir melakukan pengujian pada client. Metode update tersebut diterapkan dengan cara yang berurutan sesuai dengan tahap-tahap yang telah dijelaskan.

DAFTAR PUSTAKA

[1] Primartha, R (2023). Belajar Security jaringan Komputer Berbasis Certified Ethical Hacker Edisi 2. Penerbit Informatika. Bandung.

[2] Purbo, O.W. (2018). Internet TCP/IP: Konsep dan Implementasi. Penerbit Andi. Yogyakarta.

[3] Sofana, I (2019). Network Security dan Cyber Security. Penerbit Informatika. Bandung.

[4] Sofana, I (2021). Panduan Menjadi Administrator Sistem. Penerbit Informatika. Bandung.

[5] Surya, G (2018). Bedah Total Server. Gramedia Pustaka Utama. Jakarta.

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

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

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

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