JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 12 No. 3, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v12i3.5105

PENCEGAHAN *RANSOMWARE* PADA *SERVER ON PREMISE* MENGGUNAKAN TEKNIK *SECURITY HARDENING*

Fariz Anasrullah[1*]

[1]Sistem Komputer, Universitas Narotama; Jl. Arief Rahman Hakim No. 51 Surabaya; telp/fax : (031) 5946404 / (031) 5931213

Received: 15 Juli 2024
Accepted: 31 Juli 2024
Published: 7 Agustus 2024

Keywords:
Ransomware;
Security Hardening;
Vulnerability Assessment;

Correspondent Email:
nasrulfariz31@gmail.com

Abstrak. Transformasi digital pada saat ini semakin banyak diterapkan di setiap aspek kehidupan sehari-hari, seperti halnya di bidang bisnis, budaya, pendidikan dan juga cara berinteraksi antara satu orang dengan orang lainnya. Terdapat banyak sekali kemungkinan-kemungkinan potensi ancaman yang dapat muncul, seperti serangan Denial of Service Attack (DDoS), Ransomware, Deface, pencurian data dan juga beberapa serangan-serangan yang diperuntukan untuk mengambil alih akses sebuah sistem. Pada tahapan implementasi ini merupakan bagian yang digunakan untuk melakukan remediasi dari windows server yang akan ditingkatkan standar keamanannya. Adapun pada tahapan prosesnya akan dibagi menjadi 3 bagian, yaitu Vulnerability Assessment, Pembaruan OS, dan Remediasi. Metode yang digunakan pada penelitian kali ini meliputi tahapan assessment, pembuatan SOP security hardening, pembuatan script security hardening, implementasi yang terdiri (vulnerability assessment, remediasi dan pembaruan operating system). Langkah terakhir adalah mengenai reporting hasil proses security hardening yang telah dilakukan. Berdasarkan hasil yang didapatkan, kerentanan yang ada di server tersebut sudah jauh lebih baik. Dimana saat ini menyisakan kerentanan dengan kategori medium sebanyak 2. Namun hal tersebut masih dalam kategori aman, karena kerentanan tersebut disebabkan oleh konfigurasi sertificate yang perlu dilakukan perbaikan oleh tim service owner dan tim infrastruktur.

Abstract. *Digital transformation is currently increasingly being applied in every aspect of daily life, such as in the fields of business, culture, and education, and also in how one person interacts with another. Many potential threats could arise, such as attacks. Denial of Service Attack (DDoS), ransomware, deface, data theft, and several other attacks were aimed at taking over access to a system. At the implementation stage, this is used to carry out remediation of the Windows server whose security standards will be increased. The process stages will be divided into 3 parts. Vulnerability Assessment, OS Update, Remediation The methods used in this research include the assessment stages, creating security hardening SOPs, creating security hardening scripts, implementation consisting of (vulnerability assessment, remediation, and operating system updates) and the final step is reporting the results of the security hardening process which has been done. Based on the results obtained, the vulnerabilities on the server are much better. Where currently there are 2 vulnerabilities in the medium category. However, this is still in the safe category, because the vulnerability is caused by the certificate configuration which needs to be repaired by the service owner team and the infrastructure team.*

1. PENDAHULUAN

Transformasi digital pada saat ini semakin banyak diterapkan di setiap aspek kehidupan sehari-hari, seperti halnya di bidang bisnis, budaya, pendidikan dan juga cara berinteraksi antara satu orang dengan orang lainnya. Hal tersebut juga dipengaruhi oleh perkembangan teknologi, terutama di bidang komputasi, konektivitas dan juga komunikasi yang semakin kompleks. Selain itu, transformasi digital juga didorong oleh perubahan perilaku konsumen semenjak pandemik *Covid-19* [1].

Semakin banyaknya peminat dalam bidang digitalisasi penulis ingin menerapkan bagaimana caranya untuk mengamankan sistem yang dimilikinya. Terdapat banyak sekali kemungkinan-kemungkinan potensi ancaman yang dapat muncul, seperti serangan *Denial of Service Attack (DDoS), Ransomware*, *Deface*, Pencurian data dan juga beberapa serangan-serangan yang diperuntukan untuk mengambil alih akses sebuah sistem.

Dalam hal ini, *Ransomware* merupakan sebuah *malware* yang digunakan untuk melakukan proses serangan kepada sebuah sistem dengan cara melakukan enkripsi data yang berada di sistem tersebut. Terdapat beberapa jenis *ransomware* yang serangannya cukup massive seperti *Wannacry*, *Locky*, *Cryptolocker*, *Badrabbit*, *Locbit* dan juga beberapa jenis *ransomware* yang lainnya [2].

Di Indonesia sendiri pada tahun 2023 menjadi target serangan *malware* dengan jenis *ransomware* yaitu *lockbit* yang berhasil masuk ke dalam sistem *server* dan berhasil untuk melakukan enkripsi data penggunanya baik data internal perusahaan dan juga melakukan pengambilan data eksternal perusahaan. Penyebab dari terjadinya serangan tersebut berasal dari beberapa kesalahan, baik dari sisi manusianya maupun sistem keamanan yang masih banyak memiliki celah. Maka dari itu, pada artikel ini akan melakukan riset dalam rangka meningkatkan standar keamanan, khususnya pada *server on-premise* dengan teknik *security hardening*.

Security hardening merupakan sebuah proses yang bertujuan untuk meningkatkan standar keamanan dari suatu sistem yang dalam hal ini adalah *server on-premise* dengan mengurangi kerentanan – kerentanan yang ada di dalam sebuah *server*. Pada prosesnya nanti, *security hardening* akan melakukan beberapa langkah pengamanan, seperti halnya *vulnerability assessment*, pembaruan perangkat lunak (*patching*) dan juga yang terakhir adalah melakukan proses *hardening* dengan menggunakan *auto script* agar proses peningkatan standar keamanan dapat lebih efisien [3]. Selain itu, untuk acuan standar keamanan dari *security hardening* sendiri, akan mengacu berdasarkan rekomendasi dari *Center of Internet Security Benchmark* (CIS). Dengan adanya penelitian ini diharapkan *server* dapat dilakukan peningkatan standar keamanannya untuk mencegah serangan *ransomware* yang saat ini masih terjadi khususnya di Indonesia dengan menggunakan teknik *security hardening*.

Dalam penelitian terdahulu yang berjudul **"*Increasing Windows security by hardening PC configurations,*"** menjelaskan terkait peningkatan standar keamanan *virtual server* yang menggunakan *operating system windows server* dengan teknik *security hardening*. Tujuan penelitian tersebut adalah untuk melakukan pencegahan serangan *Man in the Middle Attack* pada proses pertukaran data seperti halnya proses autentifikasi dan juga proses pertukaran data yang lainnya. Penerapan *security hardening* pada penelitian tersebut menggunakan bantuan *active directory*, yang dimana *server* tersebut sudah terintegrasi di dalamnya, sehingga metode remediasi yang dilakukan adalah menggunakan *push policy* dari *Group Policies Objects* (GPO) yang berisikan terkait dengan konfigurasi standar keamanan pada *windows server* [4].

Penelitian selanjutnya, dalam *Lecture Notes in Networks and Systems* yang berjudul ***"Identifying and Mitigating Vulnerabilities of Hardened Windows Operating System,"*** menjelaskan terkait dengan peningkatan standar keamanan *virtual server* yang menggunakan *operating system windows server* dengan teknik *security hardening* berdasarkan hasil *vulnerability assesment*. Dijelaskan pula mengenai pentingnya melakukan *periodic vulnerability assessment* untuk menutup kerentanan dari setiap server yang dimiliki pada organisasi tersebut. Perangkat lunak yang digunakan untuk melakukan pengujian *vulnerability assessment* adalah *Nessus* dengan jenis lisensi professional. Hal tersebut bertujuan untuk melakukan pengecekan "*compliance*

check" dari standar keamanan berdasarkan CIS *Security Benchmark*. Setelah hasil *vulnerability* keluar, maka akan langsung dilakukan remediasi dari setiap kerentanan-kerentanan yang menjadi temuan [5].

Penelitian selanjutnya adalah berjudul ***"Software Security Hardening Pada Virtual Private Server Berdasarkan NIST SP 800-123 di Universitas XYZ,"*** yang menjelaskan terkait dengan peningkatan standar keamanan *virtual private* server berdasarkan NIST 800-123 sebagai *benchmark*. Pada Univestas XYZ dilakukan peningkatan standar keamanan yang dibantu dengan menggunakan *tools Kaseya* untuk mempermudah proses remediasi dari sebuah *virtual private server*. Peningkatan standar keamanan sendiri ditujukan untuk mencegah *virtual private server* dari serangan-serangan yang kemungkinan akan muncul seperti *man in the middle attack, Denial of Service* dan beberapa serangan yang lain ketika aplikasi yang berjalan di atas *virtual private server* diakses oleh banyak pengguna [6].

Dalam penelitian ini, penulis menggunakan ketiga penelitian di atas sebagai referensi dan acuan, dimana penelitian-penelitian tersebut dinilai relevan untuk diimplementasikan dalam riset, yakni mengenai pokok permasalahan terkait pencegahan *ransomware* pada *server on-premise* dengan menggunakan teknik *security hardening.*

2. MATERI

2.1. *Vulnerability Assessment*

Vulnerability assessment merupakan sebuah proses yang dirancang untuk mengidentifikasi, menganalisis, dan menilai kerentanan dalam sistem komputer, jaringan, aplikasi, atau infrastruktur IT guna mengidentifikasi potensi ancaman keamanan yang dapat dimanfaatkan oleh penyerang. Tujuannya adalah untuk memberikan pemahaman tentang titik lemah dalam sistem dan membantu organisasi untuk mengambil tindakan pencegahan untuk mengurangi risiko keamanan [7].

2.2. *CIS Benchmark*

CIS Benchmark merupakan sebuah serangkaian panduan dan juga rekomendasi keamanan yang diterbitkan oleh *Center for Internet Security (CIS)*. *Center for Internet Security (CIS)* sendiri merupakan sebuah organisasi nirlaba yang berfokus pada bidang keamanan siber. Selain itu *Center for Internet Security (CIS)* dirancang untuk membantu organisasi meningkatkan standar keamanan yang mereka miliki, mulai dari level jaringan, *web server, server* fisik dan juga *database* [8].

2.3. *Nessus*

Nessus adalah salah satu perangkat lunak populer yang digunakan untuk melakukan pemindaian kerentanan *(vulnerability scanning)* pada jaringan dan sistem komputer. Ini adalah alat yang digunakan untuk mengidentifikasi dan mengevaluasi kerentanan keamanan dalam infrastruktur IT, termasuk *server*, perangkat jaringan, perangkat lunak, dan perangkat lainnya [9].

2.4. *Python*

Pyhton merupakan sebuah bahasa pemrograman tingkat tinggi yang serbaguna, mudah dipelajari, dan sangat populer. Diciptakan oleh Guido van Rossum dan pertama kali dirilis pada tahun 1991, *Python* telah menjadi salah satu bahasa pemrograman yang paling banyak digunakan di dunia. *Python* memiliki sintaks yang bersih dan mudah dibaca, yang membuatnya cocok untuk pengembangan perangkat lunak, pemrosesan data, ilmu data, kecerdasan buatan, pengembangan *web*, dan banyak penggunaan lainnya [10].

2.5. *Windows Server*

Windows Server merupakan sebuah sistem operasi *server* yang dikembangkan oleh *Microsoft. Windows Server* adalah versi dari sistem operasi *Windows* yang dirancang khusus untuk digunakan pada *server* dan lingkungan komputasi jaringan. *Windows Server* menyediakan berbagai fitur dan layanan yang memungkinkan organisasi untuk mengelola, menyimpan, dan mengakses data serta aplikasi di jaringan mereka [11].

2.6. *Ransomware*

Ransomware adalah jenis perangkat lunak jahat *(malware)* yang dirancang untuk mengenkripsi data pada komputer atau perangkat, kemudian meminta pembayaran tebusan *(ransom)* kepada korban agar data tersebut dapat diakses kembali. *Ransomware* sering kali mengunci akses ke data atau sistem yang terinfeksi dan hanya akan memberikan "kunci" atau dekripsi kepada korban setelah tebusan dibayarkan. *Ransomware* dapat merusak atau mengenkripsi berbagai jenis data,

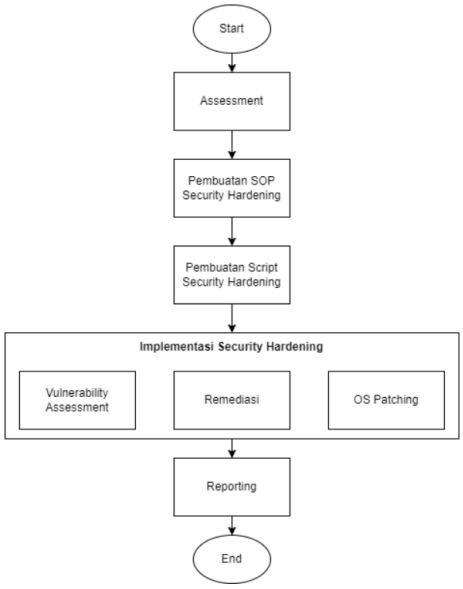
termasuk dokumen, foto, video, dan file penting lainnya [12].

2.7. *Brute Force Attack*

Brute Force Attack adalah teknik serangan terhadap sistem keamanan komputer yang menjebol akses *server* dengan mencoba menggunakan kemungkinan kombinasi dari kata sandi atau kunci enkripsi sampai kombinasi yang benar ditemukan [13]. Kata sandi yang mudah ditebak, misalnya menggunakan tiga karakter, nomor berurutan, atau tidak mengganti sampai berbulan-bulan.

3. METODE PENELITIAN

Metode yang akan digunakan selama proses penelitian tugas akhir ini adalah menggunakan metode pengembangan *agile*. Metode penelitian diperlukan guna mendapatkan hasil penelitian yang terarah, *valid* serta sistematis. Hal tersebut diperlukan agar penelitian yang dilakukan dapat dipertanggungjawabkan dan juga dapat menjadi sumber pustaka untuk pengembangan penelitian selanjutnya. Metode yang digunakan pada penelitian kali ini meliputi tahapan *assessment*, pembuatan SOP *security hardening*, pembuatan *script security hardening*, implementasi yang terdiri (*vulnerability assessment*, remediasi dan pembaruan *operating system*), dan Langkah terakhir adalah mengenai *reporting* hasil proses *security hardening* yang telah dilakukan. Berikut merupakan *flow* diagram metode penelitian yang akan digunakan selama penelitian berlangsung:



Gambar 3.1. Metode Penelitian

3.1. *Assessment*

Pada tahapan awal penelitian ini perlu dilakukan proses *assessment* mengenai beberapa hal yang nantinya akan menjadi acuan proses implementasi *security hardening*, dimana pada *assessment* awal akan dilakukan proses pendataan dari sisi infrastruktur *server*, seperti halnya berapa jumlah *server* yang akan dilakukan *hardening*, jenis *operating system* dari *server* yang akan dilakukan *hardening* dan juga melakukan pendataan pemilik dari masing-masing *server* yang ada. Setelah semua data tersebut telah didapatkan, maka akan disusun jadwal dari tahapan *security hardening*, mulai dari sosialisasi implementasi, *security awareness* dan juga tanggal implementasi *security hardening* pada setiap *server*-nya. Hal tersebut bertujuan untuk memastikan proses *security hardening* dapat berjalan dengan baik, diketahui semua pemilik *server* dan juga sesuai dengan jadwal yang ditetapkan.

3.2. Pembuatan SOP *Security Hardening*

Pada tahapan kedua ini diperlukan untuk melakukan proses penyusunan standar konfigurasi keamanan dari *server* yang akan dilakukan *hardening*. Pada prosesnya nanti *document* SOP terkait *security hardening* berisikan *policy-policy* yang diambil dari *CIS Benchmark*, yang kemudian disesuaikan kembali dengan kebutuhan. Hal tersebut dikarenakan tidak semua *policy* yang dari *CIS Benchmark* dapat diterapkan pada infrastruktur *server*. Maka dari itu, perlunya dilakukan diskusi dan juga penyesuaian kembali berdasarkan kondisi infrastruktur yang berkolaborasi dengan tim sistem *administrator*.

3.3. Pembuatan Script Security Hardening

Pada tahapan ketiga ini, merupakan proses yang digunakan untuk melakukan pengembangan dari SOP *security hardening*. Dimana pada umumnya proses remediasi dari SOP *security hardening* masih dilakukan secara manual dan membutuhkan waktu yang lama, ketika *server* tersebut tidak dalam kondisi bergabung dalam *domain (Active Directory)*. Maka dari itu, pada tahap ini akan dikembangkan sebuah teknologi *scripting* yang berisikan konfigurasi konfigurasi dari *security hardening*, yang nantinya akan dijalankan pada *windows server*. Bahasa pemrograman yang digunakan sendiri adalah menggunakan *pyhton* versi 3. Hal tersebut ditujukan agar proses remediasi nantinya dapat lebih efisien dan juga

efektif Ketika dilakukan implementasi dalam jumlah *server* yang banyak.

3.4. Implementasi *Hardening*

Pada tahapan implementasi ini merupakan bagian yang digunakan untuk melakukan remediasi dari *windows server* yang akan ditingkatkan standar keamanannya. Adapun pada tahapan prosesnya akan dibagi menjadi 3 bagian, yaitu:

1. *Vulnerability Assessment*
   Pada bagian ini merupakan tahapan yang wajib dilakukan secara periodic oleh tim. Hal tersebut digunakan untuk mengetahui kerentanan dari setiap server yang digunakan dan diakses oleh pengguna berdasarkan *Business As Usual* (BAU) yang sudah ada. Pada proses *vulnerability assessment* ini akan dibantu dengan *tools Nessus scanner* yang dipasang dalam satu *subnet* jaringan.
2. Pembaruan OS
   Pada tahapan pembaruan OS ini merupakan proses yang digunakan untuk menutup celah keamanan yang berasal dari CVE *operating system windows server* yang dikeluarkan oleh *Microsoft* berdasarkan hasil *vulnerability assessment*. Selain itu, proses pembaruan *operating system* ini akan memerlukan proses *restart server* untuk memastikan semua konfigurasi dari pembaruan dapat terimplementasi dengan baik dan sesuai berdasarkan langkah terbaik yang ada. Adapun manfaat dari proses pembaruan *operating system* ini selain menutup kerentanan yang disebabkan oleh perbedaan versi, yaitu untuk tetap menjaga performasi dari *windows server* yang digunakan. Hal itu akan berpengaruh dengan menghilangkan proses-proses *cache* dari sisi *windows server* itu sendiri.
3. Remediasi
   Pada tahapan remediasi ini merupakan proses yang digunakan untuk menjalankan *script* konfigurasi *security hardening* guna peningkatan standar keamanan dari *windows server*. Pada bagian ini juga akan melibatkan beberapa pihak mulai dari sistem administrator untuk melakukan proses *backup snapshoot* dari *windows server* dan juga pemilik *server* atau aplikasi guna melakukan pengecekan fungsionalitas aplikasi baik sebelum maupun sesudah dilakukannya proses remediasi *security hardening*. Hal tersebut digunakan untuk manajemen resiko dan memastikan bahwa tidak ada terjadi perbedaan baik dari sisi standar keamanan berdasarkan SOP dan juga dari sisi BAU aplikasi.

3.5. Pelaporan / *Reporting*

Pada tahapan terakhir dari metode penelitian ini adalah dengan melakukan pembuatan *document reporting* hasil implementasi dari *security hardening* yang sudah dilakukan. Dokumentasi yang ditulis dalam *reporting* nantinya akanberisikan *evidence* dari setiap konfigurasi atau *policy* yang sudah dilakukan perubahan. Hal tersebut bertujuan untuk memastikan bahwa proses implementasi *security hardening* telah dilakukan sesuai dengan SOP yang ada. Selain itu dokumentasi ini juga sebagai acuan untuk setiap *server* yang digunakan dan diakses baik menggunakan internet maupun dapat diakses menggunakan jaringan luar, telah dilakukan *security hardening* sebagai proses wajib yang harus dilakukan oleh pemilik *server* atau aplikasi

4. HASIL DAN PEMBAHASAN

4.1. Parameter Kebijakan Akun

Pada parameter ini akan memberikan kebijakan mengenai penggunaan *password* yang sesuai dengan *standard* yang mengacu pada *Center of Internet Security (CIS).*

4.2. Parameter Kebijakan Akun

Pada kebijakan penguncian akun ini digunakan untuk menangani percobaan serangan pembobolan *password (bruteforce attack)* yang dilakukan oleh seseorang penyerang.

Tabel 4.2. Kebijakan Akun

Item atau Aktivitas	Konfigurasi atau Tindakan yang Diperlukan	Landasan Implementasi
Account lockout duration (Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout duration)	15 Minutes	Durasi Penguncian Akun Menentukan jumlah menit akun yang terkunci tetap terkunci sebelum dibuka kuncinya secara otomatis. Kisarannya adalah 1 hingga 99999 menit.

		Anda dapat menentukan bahwa akun akan dikunci hingga administrator secara eksplisit membuka kuncinya dengan mengatur nilainya ke 0.
Account lockout threshold (Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold)	10 Invalid Logon Attempts	Ambang Penguncian Akun menentukan jumlah upaya masuk yang gagal yang akan menyebabkan akun pengguna terkunci. Akun yang terkunci tidak dapat digunakan sampai direset oleh administrator atau durasi penguncian akun telah habis. Anda dapat menetapkan nilai antara 1 dan 999 upaya masuk yang gagal, atau Anda dapat menentukan bahwa akun tidak akan pernah dikunci dengan menetapkan nilai ke 0
Reset account lockout counter after (Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Reset account lockout counter after)	15 Minutes	Atur Ulang Ambang Penguncian Akun menentukan jumlah menit yang harus berlalu setelah upaya masuk yang gagal sebelum penghitung upaya masuk yang buruk diatur ulang ke 0 proses masuk yang buruk. Kisarannya adalah 1 hingga 99999 menit.

4.3. Kebijakan *Kerberos Management Session*

Pada kebijakan mengenai *Kerberos*, digunakan untuk mengamankan jalur komunikasi dari *server* aplikasi menuju *server* lainnya atau *Active Directory (AD)* ketika menggunakan *protocol Kerberos*.

Tabel 4.3. Kebijakan *Management Session*

Item atau Aktivitas	Konfigurasi atau Tindakan yang Diperlukan	Landasan Implementasi
Enforce user logon restrictions (Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy\Enforce user logon restriction)	Enabled	Kontrol ini mendefinisikan atribut akun pengguna domain yang terkait dengan Kerberos, seperti masa pakai maksimum untuk tiket pengguna dan pengaturan Terapkan pembatasan logon pengguna. Menonaktifkan pengaturan kebijakan ini, pengguna dapat menerima tiket sesi untuk layanan yang hak penggunaannya tidak lagi mereka miliki karena haknya telah dihapus setelah mereka masuk.
Maximum tolerance for computer clock synchronization (Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy\Maximum tolerance for computer clock synchronization)	Domain Controller: 5 Others: Not Applicable	Kontrol ini menentukan toleransi maksimum untuk sinkronisasi jam komputer. Kerberos memanfaatkan stempel waktu sebagai mitigasi untuk bertahan dari serangan replay tiket. Agar mekanisme ini efektif, jam peserta Kerberos harus disinkronkan secara erat.
Maximum lifetime for service ticket (Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy\Maximum lifetime for service ticket)	Domain Controller: 600 Others: Not Applicable	Kontrol ini menentukan jumlah menit maksimum tiket sesi yang diberikan dapat digunakan untuk mengakses layanan. Menetapkan masa pakai tiket yang rendah akan memastikan bahwa akun pengguna yang telah dinonaktifkan atau dibatasi oleh jam masuk tidak dapat mengakses sumber daya Kerberisasi dengan tiket yang diberikan sebelum akun dinonaktifkan atau jam masuk berlaku.
Maximum lifetime for user ticket renewal (Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy\Maximum lifetime for user ticket renewal)	Domain Controller: 7 days Others: Not Applicable	Kontrol ini menentukan jumlah hari di mana tiket kisi-kisi pengguna (TGT) dapat diperpanjang. Menetapkan masa pakai tiket yang rendah akan memastikan bahwa akun pengguna yang telah dinonaktifkan atau dibatasi oleh jam masuk tidak dapat mengakses sumber daya Kerberisasi dengan tiket yang diberikan sebelum akun dinonaktifkan atau jam masuk berlaku.
Maximum lifetime for user ticket (Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy\Maximum lifetime for user ticket)	Domain Controller: 10 Others: Not Applicable	Kontrol ini menentukan jumlah jam maksimum tiket kisi tiket (TGT) pengguna dapat digunakan. Menetapkan masa pakai tiket yang rendah akan memastikan bahwa akun pengguna yang telah dinonaktifkan atau dibatasi oleh

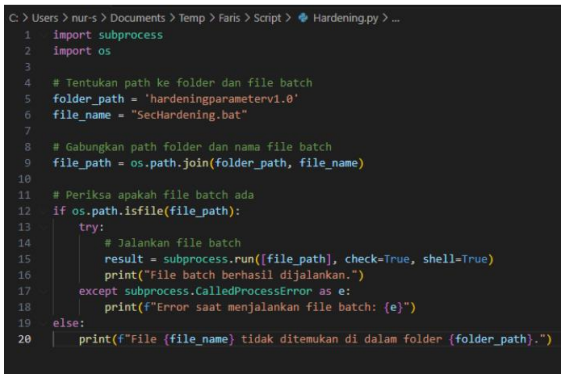
		jam masuk tidak dapat mengakses sumber daya Kerberisasi dengan tiket yang diberikan sebelum akun dinonaktifkan atau jam masuk berlaku.

4.4. Tahap Pembuatan *Script Security Hardening*

Pada tahapan kali ini digunakan untuk membuat *script* yang bertujuan mempermudah proses konfigurasi dari *security hardening* pada *windows server*. Terdapat dua bahasa pemrograman yang digunakan kali ini, yaitu *python* versi 3 dan *batch file* yang merupakan program asli yang ada di infrastruktur *windows server*.

4.4.1. Script Python

Berikut merupakan script pyhton yang digunakan pada penelitian kali ini:



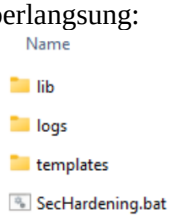
```
C: > Users > nur-s > Documents > Temp > Faris > Script > Hardening.py > ...
import subprocess
import os

# Tentukan path ke folder dan file batch
folder_path = 'hardeningparameterv1.0'
file_name = "SecHardening.bat"

# Gabungkan path folder dan nama file batch
file_path = os.path.join(folder_path, file_name)

# Periksa apakah file batch ada
if os.path.isfile(file_path):
    try:
        # Jalankan file batch
        result = subprocess.run([file_path], check=True, shell=True)
        print("File batch berhasil dijalankan.")
    except subprocess.CalledProcessError as e:
        print(f"Error saat menjalankan file batch: {e}")
else:
    print(f"File {file_name} tidak ditemukan di dalam folder {folder_path}.")
```

Gambar 4.4.1.1. Tampilan *Script Security Hardening*

Terdapat 2 *library* yang digunakan, yaitu *library subprocess* dan *library OS*. Secara struktur program ini akan mendeteksi, jika pada *directory* yang telah ditentukan terdapat file dengan nama *"SecHardening.bat"*. Maka proses perubahan konfigurasi akan dilakukan secara otomatis.

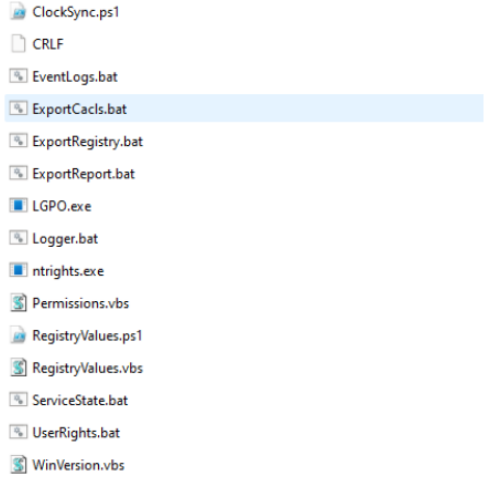
4.4.2. Struktur *Script Python*

Berikut struktur dari script batch file yang akan digunakan selama *proses hardening* berlangsung:



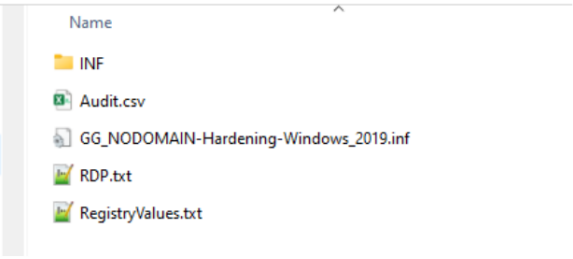
Gambar 4.4.2.1. Tampilan Hasil *Script.bat*

Dilihat dari susunan tersebut, terdapat *directory lib, logs, templates* dan juga file *SecHardening.bat.*



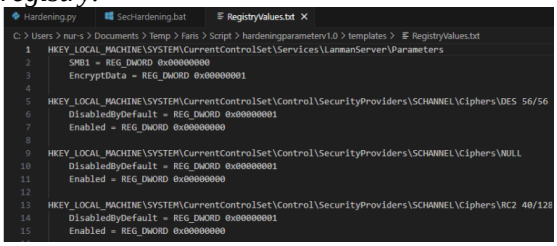
Gambar 4.4.2.2. Tampilan Hasil *Script.bat*

Directory lib berisikan beberapa program yang digunakan untuk *compatibility* dari *operating system windows* untuk bisa mendapatkan akses kedalam *local group policy* dan juga *file registry*. Kemudian untuk *directory log*, digunakan untuk menyimpan hasil log dari aktivitas ketika selesai dijalankan file *scripting*-nya.



Gambar 4.4.2.3. Tampilan *Directory lib*

Sedangkan untuk *directory templates* berisikan beberapa file yang digunakan untuk mendeklarasikan parameter-parameter apa saja yang digunakan di *local group policy dan file registry.*



```
Hardening.py  SecHardening.bat  RegistryValues.txt
C: > Users > nur-s > Documents > Temp > Faris > Script > hardeningparameterv1.0 > templates > RegistryValues.txt
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
    SMB1 = REG_DWORD 0x00000000
    EncryptData = REG_DWORD 0x00000001

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56
    DisabledByDefault = REG_DWORD 0x00000001
    Enabled = REG_DWORD 0x00000000

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL
    DisabledByDefault = REG_DWORD 0x00000001
    Enabled = REG_DWORD 0x00000000

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128
    DisabledByDefault = REG_DWORD 0x00000001
    Enabled = REG_DWORD 0x00000000
```

Gambar 4.4.2.4. Gambar *Script local group policy* dan *file registry*

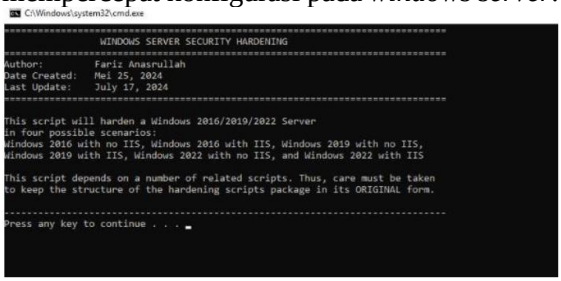
Pada gambar diatas merupakan contoh *script* yang digunakan untuk melakukan konfigurasi pada *file registry* dengan parameter mematikan nilai enkripsi yang rendah seperti DES, RC2 dan menggantinya dengan tipe enkripsi yang lebih tinggi seperti TLS versi 2 dan versi 3.

4.5. Tahap Implementasi

Pada tahapan ini merupakan bagian yang digunakan untuk melakukan implementasi *security hardening* pada *windows server*. Berikut merupakan beberapa tahapan yang dilakukan dalam proses *security hardening*.

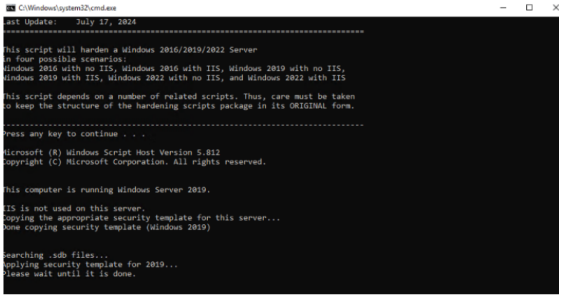
4.5.1. Proses *Security Hardening*

Pada tahapan ini merupakan bagian yang digunakan untuk melakukan *security hardening* dengan cara menjalankan *script* guna mempercepat konfigurasi pada *windows server*.



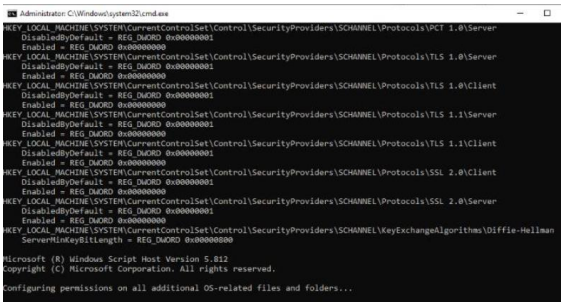
Gambar 4.5.1.1 Tampilan Proses Pertama *Security Hardening*

Pada gambar di atas merupakan tahap pertama *script* yang digunakan, dimana terdapat informasi bahwa akan dilakukan proses *security hardening* pada *windows server*. Hal tersebut bertujuan untuk menghindari kesalahan klik dari seseorang dan memastikan bahwa telah dengan sadar untuk melakukan perubahan di sisi konfigurasi *windows server.*



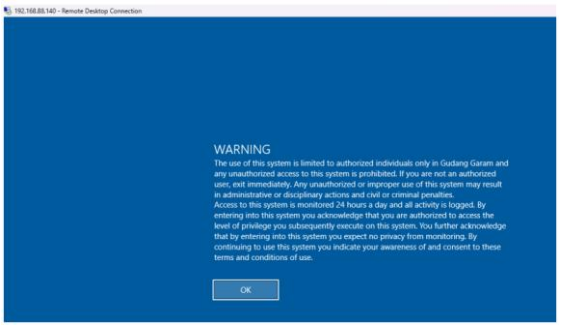
Gambar 4.5.1.2 Tampilan Proses Pertama *Security Hardening*

Pada gambar diatas merupakan contoh perubahan konfigurasi yang dilakukan pada *group policy* kususnya yang ada dibagian *security options.*



Gambar 4.5.1.3 Tampilan Proses Perubahan *Registry*

Pada gambar di atas merupakan proses perubahan yang dilakukan pada file *registry*, dimana beberapa protokol komunikasi yang memiliki enkripsi lama akan dinonaktifkan seperti SSL versi 1.0 dan 2.0. Kemudian pada protokol TLS 1.0, 1.1 juga akan dimatikan dan diganti menggunakan protokol enkripsi terbaru yaitu minimal menggunakan TLS versi 1.2 dan 1.3. Setelah semua konfigurasi selesai dilakukan, *windows server* perlu dilakukan proses *restart server*, hal tersebut bertujuan untuk memaksimalkan konfigurasi *security hardening* telah diimplementasi dengan baik.



Gambar 4.5.1.4 Tampilan Sistem Petama Kali Hidup

Pada gambar di atas merupakan indikator konfigurasi *security hardening* telah berhasil dilakukan, dimana setiap kali awal masuk ke dalam *server*, baik *server* setelah *restart* atau ketika ada pengguna yang akan masuk menggunakan RDP, akan selalu mendapatkan informasi keamanan seperti yang ditunjukkan pada gambar di atas.

5. KESIMPULAN

Berdasarkan hasil analisis dan pembahasan dalam beberapa tahap di atas, maka penulis dapat metarik beberapa kesimpulan dari penelitian ini:

1. ***Security Hardening*** **Implementasi** *Security Hardening* pada *server* menunjukkan peningkatan yang signifikan dalam keamanan sistem. Penurunan kerentanan dari kategori tinggi menjadi kategori medium menunjukkan bahwa konfigurasi keamanan yang diterapkan berhasil mengurangi risiko keamanan yang ada.
2. **Konfigurasi *Server***
   Setelah dilakukan *security hardening*, kebijakan mengenai *password* dan pengaturan *security options* telah sesuai dengan SOP yang telah dibuat. Hal ini memastikan bahwa sistem lebih sulit untuk diserang dan pengguna yang *valid* lebih sulit ditebak.
3. ***Vulnerability Assessment***
   Hasil dari *vulnerability assessment* menunjukkan bahwa setelah implementasi *security hardening*, kerentanan yang ada berkurang dan sistem berada dalam kategori aman. Meski masih terdapat beberapa kerentanan dengan kategori medium, hal ini disebabkan oleh konfigurasi *certificate* yang memerlukan perbaikan lebih lanjut.

Saran

1. **Peningkatan Pemahaman dan Kompetensi**
   Disarankan untuk meningkatkan pemahaman mengenai pentingnya keamanan sistem. Memberikan pelatihan dan sertifikasi profesional di bidang *cyber security* akan membantu meningkatkan kompetensi pegawai dalam menghadapi ancaman keamanan.
2. **Prosedur Keamanan yang Lebih Ketat**
   Diperlukan pembuatan kebijakan dan prosedur yang lebih ketat terkait *security hardening*, termasuk prosedur penanganan insiden dan audit keamanan sistem informasi. Hal ini akan memastikan bahwa langkah-langkah keamanan yang telah diterapkan tetap efektif dan diikuti dengan baik.
3. **Pemeriksaan Berkala**
   Melakukan pemeriksaan berkala terhadap konfigurasi keamanan dan melakukan *re-assessment* untuk memastikan bahwa sistem tetap berada dalam kondisi aman dan sesuai dengan standar yang telah ditetapkan.

Dengan mengikuti saran-saran tersebut, diharapkan dapat mempertahankan dan meningkatkan standar keamanan sistem sehingga dapat lebih baik dalam menghadapi ancaman keamanan di masa depan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pihak-pihak terkait yang telah memberi dukungan terhadap penelitian ini.

DAFTAR PUSTAKA

[1] M. Danuri, "Perkembangan dan Transformasi Teknologi Digital," *J. Ilm. Infokam*, vol. 15, no. 2, Sep. 2019, doi: 10.53845/INFOKAM.V15I2.178.

[2] H. Oz, A. Aris, A. Levi, and A. S. Uluagac, "A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions," *ACM Comput. Surv.*, vol. 54, no. 11s, Sep. 2022, doi: 10.1145/3514229/SUPPL_FILE/OZ.ZIP.

[3] R. R. Fakhry, "Penerapan Keamanan Server dengan Teknik Hardening pada Sistem Operasi Ubuntu Server," Universitas Muhammadiyah Surakarta, 2020. Accessed: Jul. 30, 2024. [Online]. Available: https://eprints.ums.ac.id/90707/1/NaskahPublikasi_L200170162_RezaRivaldoFakhry.pdf

[4] P. M. Zamora, M. Kwiatek, V. N. Bippus, and E. C. Elejalde, "Increasing Windows security by hardening PC configurations," *EPJ Web Conf.*, vol. 214, p. 08019, 2019, doi: 10.1051/EPJCONF/201921408019.

[5] M. Sreerag, M. Sethumadhavan, and P. P. Amritha, "Identifying and Mitigating Vulnerabilities of Hardened Windows Operating System," *Lect. Notes Networks Syst.*, vol. 191, pp. 623–632, 2022, doi: 10.1007/978-981-16-0739-4_59.

[6] F. R. Irfandi, Y. Kurnia, S. Hedianto, and A. Almaarif, "Software Security Hardening Pada Virtual Private Server Berdasarkan NIST SP 800-123 di Universitas XYZ," *J. Inf. Syst. Res.*, vol. 4, no. 1, pp. 94–102, Oct. 2022, doi: 10.47065/JOSH.V4I1.2299.

[7] A. Fatima *et al.*, "Impact and Research Challenges of Penetrating Testing and Vulnerability Assessment on Network Threat,"

2nd Int. Conf. Bus. Anal. Technol. Secur. ICBATS 2023, 2023, doi: 10.1109/ICBATS57792.2023.10111168.

[8] D. P. Prastika, J. Triyono, and U. Lestari, "Audit dan Implementasi CIS Benchmark pada Sistem Operasi Linux Debian Server (Studi Kasus: Server Laboratorium Jaringan dan Komputer 6, Institut Sains & Teknologi AKPRIND Yogyakarta)," *J. Jarkom*, vol. 6, no. 1, pp. 1–12, Jul. 2018, Accessed: Jul. 30, 2024. [Online]. Available: https://ejournal.akprind.ac.id/index.php/jarkom/article/view/2274

[9] S. Muhammad Abdul Muin, N. Kapti, and T. Tri Yusnanto, "Campus Website Security Vulnerability Analysis Using Nessus," *Int. J. Comput. Inf. Syst.*, vol. 3, no. 2, pp. 79–82, Jun. 2022, Accessed: Jul. 30, 2024. [Online]. Available: https://www.ijcis.net/index.php/ijcis/article/view/72

[10] G. LaMalva, S. Schmeelk, and D. Dinesh, "Python Cryptographic Secure Scripting Concerns: A Study of Three Vulnerabilities," *Lect. Notes Networks Syst.*, vol. 652 LNNS, pp. 602–613, 2023, doi: 10.1007/978-3-031-28073-3_42.

[11] F. Sierra-Arriaga, R. Branco, and B. Lee, "Security Issues and Challenges for Virtualization Technologies," *ACM Comput. Surv.*, vol. 53, no. 2, May 2020, doi: 10.1145/3382190.

[12] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions," *Comput. Secur.*, vol. 74, pp. 144–166, May 2018, doi: 10.1016/J.COSE.2018.01.001.

[13] A. Shafiyyah, G. F. Nama, and R. A. Pradipta, "Implementasi Wazuh Menggunakan Metode PPDIOO di Sistem Keamanan Jaringan PSDKU Universitas Lampung Waykanan sebagai Deteksi dan Respon Serangan Siber," *J. Inform. dan Tek. Elektro Terap.*, vol. 12, no. 2, pp. 2830–7062, Apr. 2024, doi: 10.23960/JITET.V12I2.4074.