**Hardening Competition!**

Kompetisi ini memiliki waktu start dan finish yang sudah ditentukan. Silahkan mengalokasikan waktu yang terbaik untuk menyelesaikannya.

Durasi maksimal adalah **120 menit**.

Harap selalu membaca dengan hati-hati setiap instruksi yang diberikan pada setiap bagian. Setiap bagian harus menampilkan verifikasi atau pembuktian bahwa policy yang diimplementasikan sudah berjalan sesuai dengan yang diharapkan (sesuai template yang diberikan).

Sistem yang digunakan sebagai target hardening adalah Windows Server 2012 R2 yang sudah disediakan.

Untuk user yang bisa digunakan ada 3 user berikut ini:

* Administrator
* Hardening1
* Hardening2

Password: P@ssw0rd

Setiap soal memiliki bobot penilaian yang berbeda sesuai dengan daftar berikut ini:

* Part 1: Update Security Patch (Poin: 10)
* Part 2: Password Policy (Poin: 10)
* Part 3: Account Policy (Poin: 20)
* Part 4: User Rights (Poin: 10)
* Part 5: Security Options (Poin: 10)
* Part 6: Audit (Poin: 10)
* Part 7: TroubleShoot (Poin: 10)
* Pembuatan Laporan (Poin: 10)
* Waktu tercepat dalam menyelesaikan kompetisi (Poin: 10)

**Identitas Peserta:** **SCORE:**

* Nama Peserta: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Nama Sekolah: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Berikut ini detail konfigurasi Hardening yang harus diimplementasikan:**

1. **Part 1: Update Security Patch.**

**Deskripsi**

Selalu install Patch keamanan terbaru merupakan salah satu cara untuk mengamankan sistem dari serangan cyber.

Pada bagian ini, anda diharapkan untuk bisa menunjukkan Patch yang sudah terinstall pada sistem yang tersedia. Informasikan cara akses ke halaman informasi ini, beserta dengan gambarnya. Berikan narasi atau penjelasan kapan sistem ini terakhir updatenya.

**Gambar dari jawaban part 1 (tampilkan beserta dengan alamat/lokasi aksesnya):**

**Keterangan gambar:**

1. **Part 2: Password Policy**

**Deskripsi**

Pengaturan keamanan ini menentukan jumlah kata sandi baru yang unik yang harus dikaitkan dengan akun pengguna sebelum kata sandi lama dapat digunakan kembali.

Kebijakan ini memungkinkan administrator untuk meningkatkan keamanan dengan memastikan bahwa sandi lama tidak digunakan kembali secara terus-menerus.

Konfigurasikan kebijakan bahwa password lama hanya bisa digunakan kembali setelah **5 kali** menggunakan password baru yang berbeda.

**Gambar dari jawaban part 2 (tampilkan beserta dengan alamat/lokasi aksesnya):**

**Gambar verifikasi bahwa tidak bisa ganti dengan password sama:**

Berikut ini informasi saat melakukan ubah password dengan password baru = password lama.

1. **Part 3: Account Policy**

**Deskripsi**

Pengaturan keamanan ini menentukan jumlah upaya masuk yang gagal yang menyebabkan akun pengguna terkunci. Akun yang dikunci tidak dapat digunakan hingga disetel ulang oleh administrator atau hingga durasi penguncian untuk akun telah kedaluwarsa.

Konfigurasikan kebijakan bahwa akun pengguna “**Hardening1**” akan terkunci setelah salah password sebanyak 3x, dan akan terbuka kembali secara otomatis setelah 45 menit.

**Gambar dari jawaban part 3 (tampilkan beserta dengan alamat/lokasi aksesnya):**

**Gambar verifikasi bahwa akun** “**Hardening1**” **akan terkunci setelah salah password 3x:**

1. **Part 4: User Rights**

**Deskripsi**

Pengaturan keamanan ini menentukan pengguna mana yang masuk secara lokal ke komputer yang dapat mematikan sistem operasi menggunakan perintah shutdown. Penyalahgunaan hak pengguna ini dapat mengakibatkan Denial of Service.

Konfigurasikan kebijakan bahwa perintah shutdown **hanya** bisa dilakukan oleh “administrators”.

**Gambar dari jawaban part 4 (tampilkan beserta dengan alamat/lokasi aksesnya):**

**Gambar verifikasi bahwa command shutdown hanya bisa dilakukan oleh grup Administrators (verifikasi bisa dengan menggunakan user Hardening2):**

1. **Part 5: Security Options**

**Deskripsi**

Pengaturan keamanan ini menentukan apakah nama akun yang berbeda dikaitkan dengan pengenal keamanan (SID) untuk Administrator. Mengganti nama akun Administrator yang membuat lebih sulit bagi orang yang tidak berwenang untuk menebak kombinasi nama pengguna dan kata sandi.

Konfigurasikan kebijakan bahwa nama akun “Administrator” diubah menjadi nama “HardenAdministrator”.

**Gambar dari jawaban part 5 (tampilkan beserta dengan alamat/lokasi aksesnya):**

**Gambar verifikasi bahwa akun HardenAdministrator sudah aktif dan bisa digunakan:**

1. **Part 6: Audit**

**Deskripsi**

Pengaturan kebijakan ini memungkinkan Anda untuk mengaudit peristiwa (event) yang dihasilkan oleh upaya masuk akun pengguna di komputer.

Event dalam subkategori ini terkait dengan pembuatan sesi logon dan terjadi pada komputer yang diakses.

Konfigurasikan kebijakan bahwa aktifitas logon ke sistem akan disimpan, baik itu untuk aktifitas GAGAL ataupun SUKSES.

**Gambar dari jawaban part 6 (tampilkan beserta dengan alamat/lokasi aksesnya):**

**Gambar verifikasi bahwa aktifitas logon tersimpan pada security log, baik itu untuk sukses ataupun gagal logon:**

1. **Part 7: TroubleShoot**

**Deskripsi**

Dalam proses Hardening diatas terdapat salah satu bagian yang melakukan pembatasan terhadap command shutdown, sehingga setelah proses ini, user Hardening2 tidak bisa menon-aktifkan sistem, dimana user ini digunakan sistem administrator untuk melakukan maintenance pada server yang dilakukan Hardening.

Analisa terkait hal ini, dan kemudian konfigurasikan kebijakan bahwa user Hardening2 merupakan bagian dari Administrators, sehingga user ini bisa digunakan untuk menjalankan command shutdown (tanpa mengubah Policy yang telah ditentukan sebelumnya).

**Gambar dari jawaban part 7 (tampilkan beserta dengan alamat/lokasi aksesnya):**

**Gambar verifikasi bahwa akun Hardening2 bisa digunakan untuk menonaktifkan sistem:**