

# TEMPLATE LAPORAN FINAL HARDENING (LINUX) LKS – KEAMANAN SIBER 2020

**nama tim :** VHS\_CyberTech - SMK Negeri 22 Jakarta

**nama anggota :** Andi Syahrudin, Muhamat Anwar Dwi Yanto

## HARDENING

NO	ITEM	PENJELASAN
1	Jenis Celah Keamanan/Kesalahan Konfigurasi	Php functions
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/home/messi/mtv.php
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Di dalam file /home/messi/mtv.php memiliki fungsi system() yang parameternya diambil di metode GET dan tidak memiliki filtering, sehingga attacker dapat memasukkan perintah lainnya yang akan dieksekusi pada sisi server
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Membatasi agar fungsi system() dalam file /home/messi/mtv.php (pada baris 4) hanya bisa menjalankan satu perintah tertentu (hard coded dalam baris baris pemrograman) seperti di bawah ini:  <?php echo system(\$cmd);  Cara lain yang bisa dilakukan adalah menonaktifkan fungsi system() melalui konfigurasi php.ini seperti di bawah ini:  Disable_functions = system
NO	ITEM	PENJELASAN
2	Jenis Celah Keamanan/Kesalahan Konfigurasi	Directory listing

	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/var/www/html/*
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Di dalam folder /var/www/html bisa directory listing yang parameternya diambil di metode GET dan tidak memiliki filtering, sehingga attacker dapat melihat perintah lainnya yang akan dieksekusi pada sisi server
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Mencofigure security.conf <pre>&lt;Directory /var/www/&gt;   Options -Indexes -FollowSymLinks   AllowOverride None   Require all granted &lt;/Directory&gt;</pre>
3	Jenis Celah Keamanan/Kesalahan Konfigurasi	Remote Code Execution
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	Pada File Backdoor Yang Mungkin Di upload melalui CSRF Upload
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Di dalam folder /var/www/html/temp dengan permission user apache boleh upload backdoor shell yang membuat si hacker bisa mendapatkan access ke server kita
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	maka dari itu saya menginstall pake tambahan yaitu modsecurity dan mencofigure php.ini <pre>allow_url_fopen = Off allow_url_include = Off max_input_time = 30 max_execution_time = 30 register_globals = off display_errors = Off open_basedir = "/var/www/html" session.cookie_httponly = 1 session.use_cookies = 1 session.use_only_cookies = 1 disable_functions = exec,system,highlight_file,source,show_source,</pre>

3	Jenis Celah Keamanan/Kesalahan Konfigurasi	Pengambil alihan ssh
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	-
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Ketika hacker bisa mendapatkan access root maka server dapat ambil alih seutuhnya
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Mencofigure sshd_config PermitRootLogin no Port 38150

# HARDENING WINDOWS 7

<b>NAMA TIM</b>	VHS_CyberTech - SMK Negeri 22 Jakarta
<b>KETUA</b>	Andi Syahrudin
<b>ANGGOTA</b>	Muhamat Anwar Dwi yanto



## 1. Security banner (Windows machines)

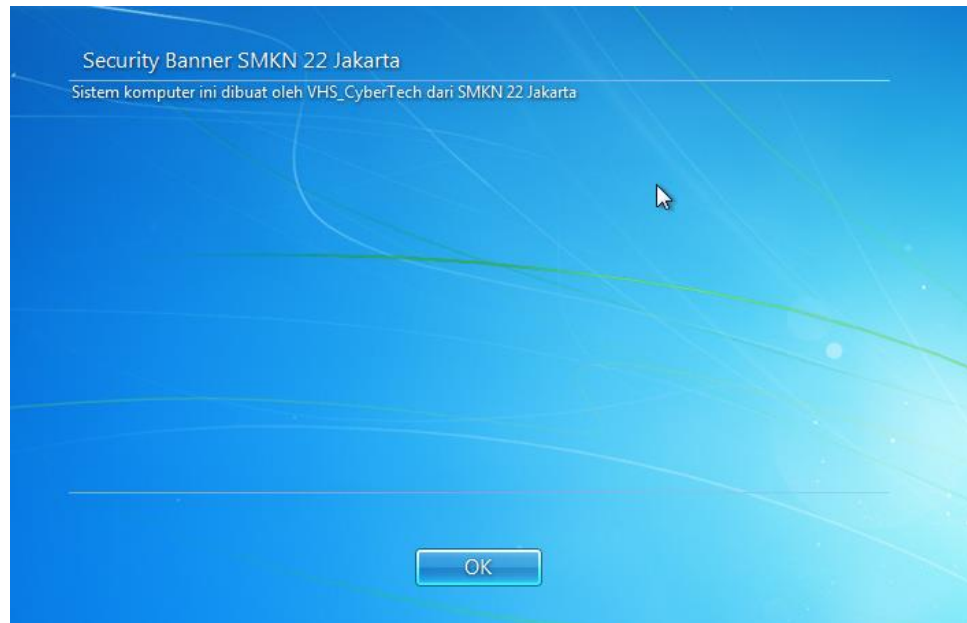
Challenge : On random windows machine go to login screen
<p>Windows 7 mempunyai fitur untuk menambahkan pesan yang ditampilkan di layar saat pengguna masuk.</p> <p>Untuk memberikan pesan bagi pengguna yang masuk ke komputer Windows 7 yang akan masuk/login. Pesan tersebut bersifat informatif dan tidak memberikan keamanan yang sebenarnya.</p> <p>Buatlah Security Banner Pesan sebelum login ke Komputer Windows 7</p>
Answer
<p>Windows + r --&gt; gpedit.msc --&gt; Computer Configuration --&gt; Windows Settings --&gt; Security Settings --&gt; Local Policies --&gt; Security Options ganti di Interactive logon: Message txt... dan Interactive logon: Message title....</p>

banner = Sistem komputer ini dibuat oleh VHS\_CyberTech dari SMKN 22 Jakarta  
title = Security Banner SMKN 22 Jakarta

### ScrenShoot

Masukan screenshot penyelesaian

1.



## 2. Password minimum length (Windows machines)

<b>Challenge : Pick random preconfigured account, change password to random one with length of 8 (which meets complexity requirements)</b>
<p>Windows 7 mempunyai Security Policy yang mengatur setiap user membuat password dengan minimal berapa karakter.</p> <p>Di Challenge nomor 2 para peserta membuat kebijakan setiap password untuk user di Windows 7 diharuskan memasukan password dengan 8 karakter.</p>
<b>Answer</b>
<p>Windows + r --&gt; gpedit.msc --&gt; Computer Configuration --&gt; Windows Settings --&gt; Security Settings --&gt; Account Policies --&gt; Password Policy dan yang di ganti di (Minimum password length) jadi 8 character. Harus ada 8 character tidak bisa kurang dari 8 character.</p>
<b>ScrenShoot</b>
<p>Masukan screenshot penyelesaian</p> <p>1.</p>



2.

Local Computer Policy

- Computer Configuration
  - Software Settings
  - Windows Settings
    - Name Resolution Policy
    - Scripts (Startup/Shutdown)
    - Deployed Printers
    - Security Settings
      - Account Policies
        - Password Policy**
        - Account Lockout Policy

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	8 characters
<b>Password must meet complexity requirements</b>	<b>Enabled</b>
Store passwords using reversible encryption	Disabled

f00ds  
Standard user  
Password protected

You are changing the password for f00ds. If you do this, f00ds will lose all EFS-encrypted files, personal certificates, and stored passwords for Web sites or network resources.

To avoid losing data in the future, ask f00ds to make a password reset floppy disk.

User Account Control Panel

The password you typed does not meet the password policy requirements. Check the minimum password length, password complexity and password history requirements.

OK

### 3. Password complexity (Windows machines)

**Challenge : Pick random preconfigured account, change password to random one with length of 8 (which meets complexity requirements)**

Challenge no 3 adalah mengaktifkan fitur complexity requirements di Windows 7.

Pengaturan keamanan ini menentukan apakah kata sandi harus memenuhi persyaratan kompleksitas.

Jika kebijakan ini diaktifkan, kata sandi harus memenuhi persyaratan minimum berikut:

- Tidak mengandung nama akun pengguna atau bagian dari nama lengkap pengguna yang melebihi dua karakter berturut-turut
- Panjangnya setidaknya delapan karakter
- Berisi karakter dari tiga dari empat kategori berikut:
- Huruf besar Bahasa Inggris (A sampai Z)
- Huruf kecil Bahasa Inggris (a hingga z)
- Basis 10 digit (0 hingga 9)
- Karakter non-alfabet (misalnya, !, \$, #, %)

#### Answer

Windows + r --> gpedit.msc --> Computer Configuration --> Windows Settings --> Security Settings --> Account Policies --> Password Policy dan diganti menjadi Enabled di (Password must meet complexity requirements). Dan Password yang bisa diganti salah satunya adalah ( P@ssw0rd1 ).

#### ScrenShoot

Masukan screenshot penyelesaian

1.

Local Computer Policy

Computer Configuration

Software Settings

Windows Settings

Name Resolution Policy

Scripts (Startup/Shutdown)

Deployed Printers

Security Settings


Account Policies

Password Policy

Account Lockout Policy

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

2.



f00ds

Standard user

Password protected

You are changing the password for f00ds. If you do this, f00ds will lose all EFS-encrypted files, personal certificates, and stored passwords for Web sites or network resources.

To avoid losing data in the future, ask f00ds to make a password reset floppy disk.

••••••••

••••••••

If the password contains capital letters, they must be typed the same way every time.

[How to create a strong password](#)

P@ssw0rd!

The password hint will be visible to everyone who uses this computer.

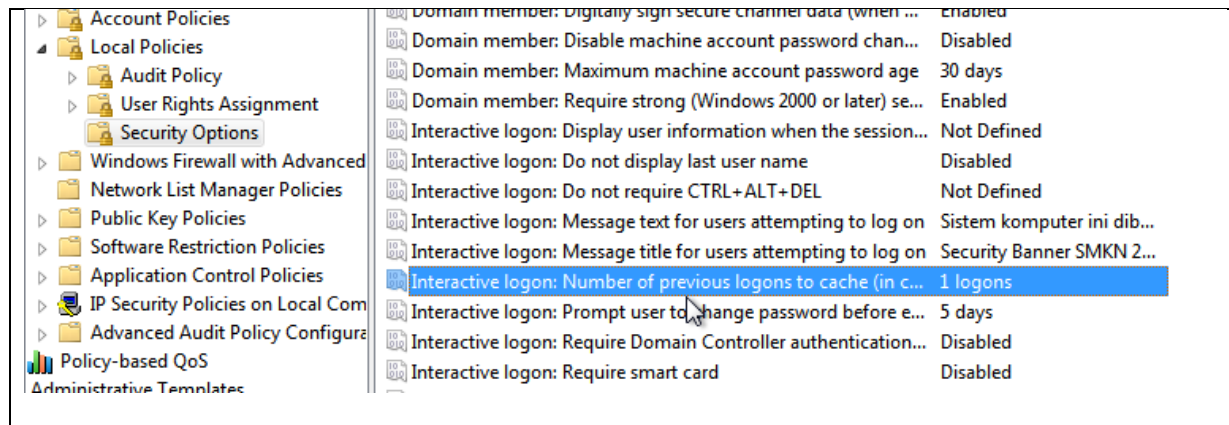
[What is a password hint?](#)

Change password

Cancel

#### 4. Cached logins (Windows machines)

<b>Challenge : On random windows client machine - login with random account, logoff, shutdown vNIC, try to login again with the same account</b>
<p>Chaced Login ke computer Windows 7 kredensial akun tersimpan di cached Login system dari Windows 7.</p> <p>Data cache disimpan dalam kunci registri HKLM\ SECURITY\Cache, yang hanya dapat diakses oleh akun SYSTEM. Penting juga untuk menyebutkan bahwa masa cache ini di komputer tidak terbatas.</p> <p>Setting Security di cached login Windows 7 yang hanya memperbolehkan user yang terakhir yang hanya dapat login ke dalam Windows 7.</p> <p>Secara teori, jika ada akses fisik ke komputer, penyerang memiliki kesempatan untuk menggunakan kredensial yang disimpan, disarankan untuk menonaktifkan cache lokal untuk keamanan yang lebih baik.</p> <p>Setting Logons cached yang disimpan diatur ke nilai value 1.</p> <p>Ini memungkinkan hanya pengguna terakhir untuk masuk ke sistem.</p>
<b>Answer</b>
<p>Windows + r --&gt; gpedit.msc --&gt; Computer Configuration --&gt; Windows Settings --&gt; Security Settings --&gt; Local Policies --&gt; Security Options yang diganti di ( Interactive logon: Number of previous logons to cache) jadi value 1.</p>
<b>ScrenShoot</b>
<p>Masukan screenshot penyelesaian</p> <p>1.</p>



## 5. Account lockdown (Windows machines)

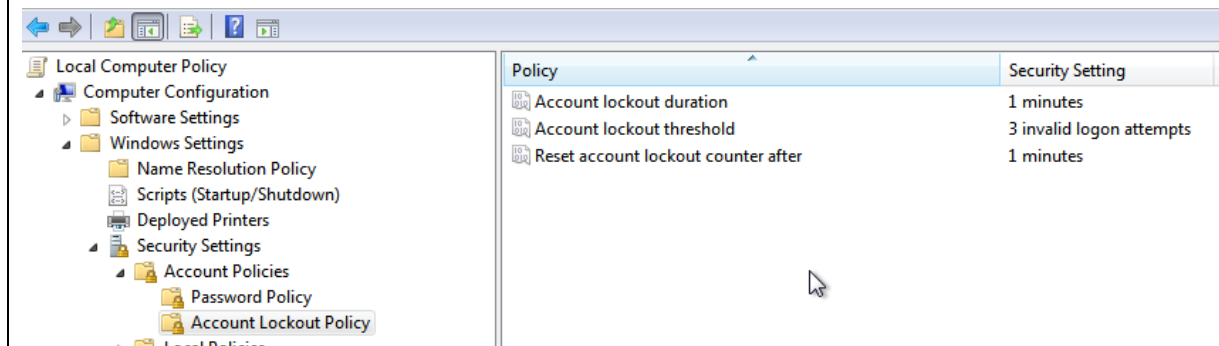
Challenge : On random windows machine - try to login 3 times with incorrect password
<p>Untuk menghindari serangan Brute Force pada akun windows 7 berilah security pada menu login user.</p> <p>Gunakan security jika salah memasukan password sebanyak 3 kali user akan diblok selama 1 menit.</p>
Answer

Windows + r --> gpedit.msc --> Computer Configuration --> Windows Settings --> Security Settings --> Account Policies --> Password Lockout Policy nah disini isi dulu yang ( Account lockout threshold ) yaitu 3 kali gagal login. Lalu ganti di ( Account lockout duration ) ini untuk 3 kali gagal login akan diblock selama 1 menit.

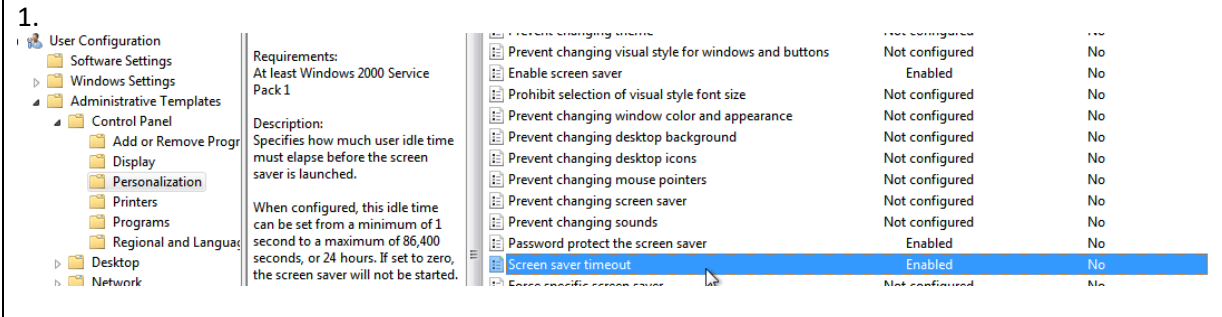
## ScrenShoot

Masukan screenshot penyelesaian

1.



## 6. Inactivity timeout (Windows machines)

Challenge : On random windows machine login and wait for 1 min																																									
Pada challenge No 6 disini peserta diharuskan membuat setting security pada Windows 7																																									
Jika selama 1 menit tidak ada aktifitas di Windows 7 akan otomatis terkunci/lock.																																									
Untuk masuk Kembali ke Windows 7 diharuskan untuk Login Kembali dengan user yang aktif.																																									
Answer																																									
Windows + r --> gpedit.msc --> User Configuration --> Administrative Templates --> Control Panle --> Personalization lalu ganti di( screen saver timeout ) enabled dan ganti jadi 60 seconds.																																									
ScrenShoot																																									
Masukan screenshot penyelesaian																																									
<p>1.</p>  <p>The screenshot shows the Windows 7 Group Policy Editor window. The left pane displays the tree structure: 'User Configuration' &gt; 'Administrative Templates' &gt; 'Control Panel' &gt; 'Personalization'. The right pane shows a list of policies. The 'Screen saver timeout' policy is highlighted in blue. Its status is 'Enabled' and the value is 'No'.</p> <table border="1"><thead><tr><th>Policy Name</th><th>Configuration</th><th>Value</th></tr></thead><tbody><tr><td>Prevent changing visual style for windows and buttons</td><td>Not configured</td><td>No</td></tr><tr><td>Enable screen saver</td><td>Enabled</td><td>No</td></tr><tr><td>Prohibit selection of visual style font size</td><td>Not configured</td><td>No</td></tr><tr><td>Prevent changing window color and appearance</td><td>Not configured</td><td>No</td></tr><tr><td>Prevent changing desktop background</td><td>Not configured</td><td>No</td></tr><tr><td>Prevent changing desktop icons</td><td>Not configured</td><td>No</td></tr><tr><td>Prevent changing mouse pointers</td><td>Not configured</td><td>No</td></tr><tr><td>Prevent changing screen saver</td><td>Not configured</td><td>No</td></tr><tr><td>Prevent changing sounds</td><td>Not configured</td><td>No</td></tr><tr><td>Password protect the screen saver</td><td>Enabled</td><td>No</td></tr><tr><td>Screen saver timeout</td><td>Enabled</td><td>No</td></tr><tr><td>Screen saver image</td><td>Not configured</td><td>No</td></tr></tbody></table>			Policy Name	Configuration	Value	Prevent changing visual style for windows and buttons	Not configured	No	Enable screen saver	Enabled	No	Prohibit selection of visual style font size	Not configured	No	Prevent changing window color and appearance	Not configured	No	Prevent changing desktop background	Not configured	No	Prevent changing desktop icons	Not configured	No	Prevent changing mouse pointers	Not configured	No	Prevent changing screen saver	Not configured	No	Prevent changing sounds	Not configured	No	Password protect the screen saver	Enabled	No	Screen saver timeout	Enabled	No	Screen saver image	Not configured	No
Policy Name	Configuration	Value																																							
Prevent changing visual style for windows and buttons	Not configured	No																																							
Enable screen saver	Enabled	No																																							
Prohibit selection of visual style font size	Not configured	No																																							
Prevent changing window color and appearance	Not configured	No																																							
Prevent changing desktop background	Not configured	No																																							
Prevent changing desktop icons	Not configured	No																																							
Prevent changing mouse pointers	Not configured	No																																							
Prevent changing screen saver	Not configured	No																																							
Prevent changing sounds	Not configured	No																																							
Password protect the screen saver	Enabled	No																																							
Screen saver timeout	Enabled	No																																							
Screen saver image	Not configured	No																																							

