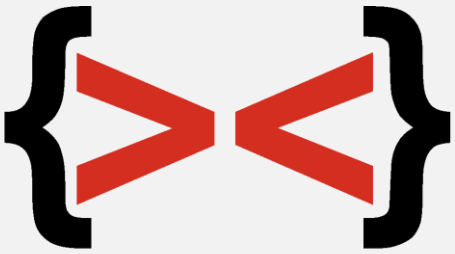
2017



Xcode Intensif Training

Advanced Linux Server

Hardening Security

XCODE

Advanced Linux Server Hardening Security

Pembelajaran linux server hardening security security secara advanced

Waktu Training: 4 hari antara 2-5 jam.

Objectives : Dengan Menyelesaikan training ini diharapkan peserta bisa melakukan keamanan dan pengawasan pada server linux secara advanced

XCODE

Advanced Linux Server Hardening Security

No	Session	Objective
Performing Basic System Management Tasks		
1	Session 1	Dasar jaringan dan linux - Dasar jaringan - TCP/IP - Subnet mask - Dasar linux - Setting IP address - Shell bash - Managemen user dan group - File Security, chown, chgrp, chmod (numeric coding, letter coding) - Penggunaan find untuk memeriksa hak akses pada file dan folder (Untuk keamanan) - Screen - SSH & pengawasan user - Pengawasan dengan Log pada server dan log pada history bash - IDS (Intrusion detection system) dengan Snort - NAT

		- Real Time Interactive IP LAN Monitoring - Transparent Proxy untuk memantau web yang dibuka client - Port forwarding - Firewall UFW
2	Session 2	- Contoh serangan fisik (reset password linux) - Pengujian dasar keamanan server dan jaringan - Contoh pemeriksaan aplikasi server hingga eksploitasi remote pada server linux yang berfirewall - Contoh serangan DoS pada web server target - Contoh Scanning celah pada web dan eksploitasi memanfaatkan celah XSS, LFI, RFI, SQL Injection - Contoh Eksploitasi SQL Injection pada halaman login - Penggunaan LAMPP lama yang dapat mengancam jika tidak teliti - Contoh scanning celah keamanan web dan eksploitasi dari web (remote dari celah web, analisis shell yang didapatkan, rooting hingga cracking password dengan john the ripper) - Contoh serangan pada SSH dengan brute force - Contoh serangan pada login wordpress dengan brute force - Contoh scanning dan eksploitasi plugin pada wordpress - Contoh serangan ARP Spoofing

3	Session 3	- Dasar system hardening - Menimbang aplikasi-aplikasi yang akan digunakan - Pengamanan server secara umum untuk meminimalisir serangan - Recovery mode dimatikan - Periksa kernel dan update Kernel - Periksa aplikasi server yang digunakan dan update - Update Kernel - Pengamanan dari serangan ARP Spoofing Hardening yang berhubungan dengan web - Pengamanan web server dari PHP Shell - Pengamanan web server dari DoS yang dilakukan pada contoh - Pengamanan web server dengan WAF (Web Application Firewall) - Pengecekan source code aplikasi web untuk menghindari serangan XSS, LFI, RFI, SQL Injection - Pengamanan dari sisi aplikasi web dari serangan XSS, LFI, RFI, SQL Injection - Pengamanan pada web login dari SQL Injection dari sisi pemrograman (pengecekan dengan input password) - Pengamanan pada web login dari SQL Injection dari sisi pemrograman (Filter pada input variablel)

		- Pengamanan dari sisi PHP.INI dari serangan seperti RFI
	Session 4	- Membangun web honeypot login dan memasangnya - Membangun komunikasi web dengan HTTPS (SSL Certificate) Keamanan dengan SAMBA & SFTP - Memberikan password pada akses share (SAMBA) - Mengenal SFTP (secure) - Installasi dan konfigurasi SFTP Hardening pada SSH - Pengamanan SSH Server dari serangan brute force - Mematikan user root untuk SSH - Memasang SSH Honeypot pada server - Port Knocking pada koneksi SSH - Banned ip luar yang melakukan nmap -A / nmap -sV - Banned ip luar yang melakukan serangan brute force pada SSH - Banned ip luar yang melakukan serangan XSS, file inclusion hingga SQL Injection pada web