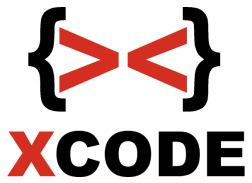


Xcode Private Training
Linux Server Hardening
Security



Linux Server Hardening Security

Pembelajaran linux ubuntu server hardening security security

Waktu Training: 3 hari antara 2-5 jam.

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

Linux Server Hardening Security

No	Session	Objective
Performing Basic System Management Tasks		
1	Session 1	<p>Dasar jaringan dan linux</p> <ul style="list-style-type: none"> - 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 paa history bash - Pengawasan dengan IDS Snort - Firewall UFW

2	Session 2	<p>Attack</p> <ul style="list-style-type: none"> - 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 - 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 <p>Hardening</p> <ul style="list-style-type: none"> - 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
4	Sesi 4	Hardening yang berhubungan dengan web

	<ul style="list-style-type: none">- Pengamanan web server dari PHP Shell- Pengamanan web server dari DoS yang dilakukan pada contoh- Pengamanan web server dengan WAF (Web Application Firewall)- Pengamanan pada aplikasi web berdasarkan dari contoh pada attack <p>Keamanan dengan SAMBA & SFTP</p> <ul style="list-style-type: none">- Memberikan password pada akses share (SAMBA)- Mengenal SFTP (secure)- Instalasi SFTP <p>Hardening pada SSH</p> <ul style="list-style-type: none">- Membatasi login SSH- 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
--	--