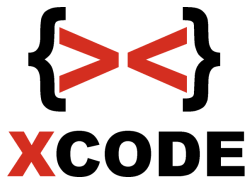


**Xcode Intensif Training**  
**Advanced Computer**  
**Networking**



## **Advanced Computer Networking**

Pembelajaran jaringan komputer dengan Mikrotik dan linux Ubuntu serta pembelajaran untuk keamanan server atau router.

**Waktu Training:** 6 hari antara 2-5 jam.

**Objectives :** Dengan Menyelesaikan training ini diharapkan peserta bisa melakukan instalasi jaringan yang disesuaikan dengan kebutuhan serta mampu melakukan dasar pengamanan dan pengawasan.

## Advanced Computer Networking

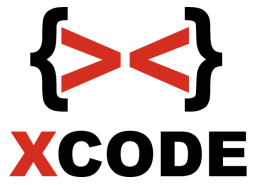
No	Session	Objective
<b>Performing Basic System Management Tasks</b>		
1	Session 1	<p>Dasar jaringan komputer</p> <ul style="list-style-type: none"> <li>- Dasar TCP/IP, ARP, Mac Address, pengenalan 7 layer OSI, firewall, etc</li> <li>- Mengenal service FTP, service Telnet, service SSH, SMTP, DNS, HTTP, POP3, SMB, VPN, service MySQL, RDP, VNC</li> <li>- Subnetting (CIDR, perhitungan biner ke desimal, perhitungan subnetting, etc)</li> <li>- Router Modem</li> <li>- Port forwarding</li> <li>- DMZ (Demilitarized Zone)</li> <li>- Praktek membangun jaringan sendiri dengan router modem wireless 4G Smartfren + AP TL-WN701ND sebagai client + router tp-link + laptop client</li> </ul>
2	Session 2	<p>Praktek membangun jaringan sendiri dengan Router dari koneksi indihome / modem router wireless 4G Smartfren + AP TL-WN701ND sebagai client + router mikrotik RB750 + laptop client</p> <p>DCHP Client pada Mikrotik</p> <p>DHCP Server pada Mikrotik</p>

		<p>Setting port lain pada RB750 lain agar dapat menjadi client</p> <p>Mengenal Extra package, backup dan mengganti password</p> <p>Membangun bridge dari router RB750</p> <p>Membatasi koneksi dari hotspot agar tidak masuk jaringan di atas router mikrotik</p> <p>Firewall layer 7 untuk blokir situs</p> <p>SNTP Client</p> <p>Blokir situs berdasarkan waktu</p> <p>Blok port (FTP, SSH dan sebagainya)</p> <p>Port Knocking (ICMP)</p> <p>Simple Queue (Sederhana)</p> <p>Simple Queue (Share)</p> <p>Simple Queue (Client ke jaringan lokal full bandwidth tapi ke jaringan internet dibatasi)</p> <p>Port Forwarding</p> <p>VPN Server PPTP</p> <p>Setting di VPN client di Windows</p> <p>Setting VPN Server agar client dari VPN dapat mengakses ip-ip di jaringan lokal</p>
<b>3</b>	Session 3	<p>Blokir situs dengan proxy</p> <p>Membatasi hanya beberapa situs yang bisa dibuka</p>

		<p>Blokir file ekstensi tertentu seperti misal jpg, png, agar irit bandwidth</p> <p>Memantau web yang dibuka client (dari mikrotik)</p> <p>Memantau web yang dibuka client dari Ubuntu menggunakan rsyslog dan rsyslog-mysql (log disimpan dalam file dan database dan hasilnya bisa ditampilkan di web melalui aplikasi web)</p> <p>Billing hotspot (membuat profile, bypass user)</p> <p>Membatasi bandwidth untuk client hotspot</p> <p>Membuat Trial pada login page hotspot</p> <p>Mengedit login hotspot yang bagus dan elegan untuk disesuaikan dengan kebutuhan hotspot yang dimiliki</p> <p>Membuat ip static saat user login sehingga bisa terpantau client tertentu membuat web apa saja</p> <p>Billing hotspot menggunakan User Manager</p>
4	Session 4	<p>Ubuntu administration, router &amp; server</p> <ul style="list-style-type: none"> <li>- Dasar linux</li> <li>- Mengenal partisi, mengenal /home, /var/log, /var/www, /etc</li> <li>- Perintah-perintah linux</li> <li>- Repositories (Ubuntu)</li> <li>- Setting IP Client di linux (Permanen &amp; non permanen)</li> <li>- koneksi wireless melalui terminal (tanpa proteksi dan dengan proteksi WPA-PSK)</li> </ul>

		<ul style="list-style-type: none"> <li>- Menambah ip baru pada interface</li> <li>- Mengenal file hosts, shadow, passwd, etc</li> <li>- Managemen user dan group (GUI dan terminal)</li> <li>- File Security, chown, chgrp, chmod (numeric coding, letter coding)</li> <li>- SSH Server (user desktop &amp; admin)</li> <li>- Screen pada terminal</li> <li>- Install dan setting samba (Hanya bisa baca, bisa baca dan write)</li> <li>- Setting samba dengan password</li> <li>- SMB Client untuk mengakses samba</li> </ul>
5	Session 5	<ul style="list-style-type: none"> <li>- DNS Server</li> <li>- Web Server (APACHE) &amp; MySQL Server</li> <li>- PHPMyadmin</li> <li>- Transfer file melalui protocol SFTP dengan menggunakan WinSCP</li> <li>- Installasi Wordpress di server</li> <li>- VPN Server di Ubuntu</li> <li>- Setting VPN Client di Windows</li> <li>- Firewall ufw (memahami allow, deny, reject dan mengujinya dengan nmap)</li> <li>- Blokir IP dengan firewall ufw</li> </ul>

		<ul style="list-style-type: none"> <li>- NAT (Network address translation)</li> <li>- Real Time Interactive IP LAN Monitoring</li> <li>- Bandwidth Managemen</li> <li>- DHCP Server</li> <li>- Squid Proxy dengan proxy transparent</li> <li>- Memantau web yang dibuka client</li> <li>- Port Forwarding</li> </ul>
6	Session 6	<p>Linux Server Hardening Security</p> <ul style="list-style-type: none"> <li>- Dasar keamanan server dan jaringan</li> <li>- Disable Recovery Mode</li> <li>- Pengujian dasar keamanan server dan jaringan</li> <li>- Update kernel pada ubuntu</li> <li>- Pengamanan web server dari PHP Shell (Pengujian sebelum diamankan dan setelah diamankan)</li> <li>- Mematikan direktori listing</li> <li>- Mengamankan Web Server dari serangan DoS (Pengujian sebelum diamankan dan setelah diamankan)</li> <li>- Log-log pada server</li> <li>- Instalasi dan dasar setting IDS dengan snort</li> <li>- Banned otomatis pada attacker yang melakukan scanning NMAP -A / nmap -sV</li> </ul>



- Banned otomatis pada attacker yang melakukan serangan brute force pada SSH Server
- Instalasi dan konfigurasi WAF serta pengujiannya