Cloudflare Intermediate Training

Curriculum 3 Days

Day - 1

- **Introduction to Cloudflare**
  - What Cloudflare is: Global edge network overview
  - Cloudflare as a Security + Performance platform
  - Use cases: Why organizations adopt Cloudflare
- **Understanding CDN (Content Delivery Network)**
  - CDN basics: caching, edge delivery, latency reduction
  - How Cloudflare's CDN differs from traditional hosting/CDNs
  - Role of DNS in CDN acceleration
- **Hands-On: Getting Started with Cloudflare CDN**
  - Registering a domain with Cloudflare
  - Configuring DNS records and enabling proxy
  - Setting caching rules and testing CDN delivery
  - Measuring performance improvements
- **Advanced CDN Features**
  - Tiered caching, cache keys, and cache rules
  - Automatic Platform Optimization (APO) for WordPress/other CMS
  - Image optimization (Polish, Mirage)
  - Argo Smart Routing for dynamic acceleration
- **Hands-On: Advanced CDN Tuning**
  - Implementing page rules for caching, redirects, and edge TTL
  - Testing with developer tools and performance monitoring
  - Hands-on demo: Serving static + dynamic content with optimal caching
- **Wrap-Up**
  - Key learnings from CDN modules
  - Discussion: Real-world CDN use cases and challenges

Day - 2

- **DDoS Fundamentals**
  - What is a DDoS attack?
  - Types of attacks:
  - L3/L4 (network & protocol attacks)
  - L7 (application attacks)
  - Business impacts of large-scale attacks
- **Cloudflare DDoS Architecture**
  - Always-on protection explained
  - How Cloudflare detects and mitigates volumetric and application-layer attacks
  - Role of Anycast in absorbing massive traffic
- **Hands-On: Configuring DDoS Protection**
  - Enabling "I'm Under Attack" mode
  - Using rate limiting rules for APIs and web apps
  - Setting up firewall rules for traffic filtering
  - Monitoring attack analytics in Cloudflare dashboard
- **Advanced DDoS Defense**
  - Protecting APIs and non-HTTP services with Cloudflare Spectrum
  - Magic Transit overview: Protecting entire IP ranges
  - Mitigating attacks on TCP/UDP traffic
- **Hands-On: Testing DDoS Resilience**
  - Simulating HTTP flood/slowloris-style attacks (in controlled lab)
  - Monitoring Cloudflare's mitigation in real time
  - Validating system resilience during attack simulations
- **Wrap-Up**
  - Summary of DDoS protections configured
  - Discussion: Lessons from real-world Cloudflare DDoS case studies

Day - 3

- **WAF Basics**
  - What is a Web Application Firewall?
  - OWASP Top 10 threats and how WAF mitigates them
  - Managed rulesets vs. custom rules
- **Cloudflare WAF in Action**
  - Enabling WAF for applications
  - Applying OWASP managed rules
  - Protecting against SQLi, XSS, CSRF, and RCE attacks
- **Hands-On: Configuring WAF**
  - Creating custom rules with Cloudflare Expression Language
  - Bot mitigation using WAF + Bot Management
  - API Shield for API schema validation and mTLS
  - Logging & monitoring blocked requests
- **Advanced Security Integration**
  - Combining WAF with CDN & DDoS defenses
  - Real-world example: End-to-end protection for a high-traffic website
  - Security analytics and log forwarding with Logpush
- **Capstone Lab (End-to-End Project)**
  - Participants design and implement a complete Cloudflare security + performance stack:
  - Step 1: Set up CDN with advanced caching rules
  - Step 2: Enable DDoS protection and simulate an attack
  - Step 3: Configure WAF managed + custom rules
  - Step 4: Document the architecture, configurations, and lessons learned
- **Wrap-Up & Next Steps**
  - Key takeaways from 3 days
  - Best practices for production deployments
  - Cloudflare roadmap: Zero Trust, Workers, and advanced services (for future learning)