

ALTA3 RESEARCH

Practical TLS & DNS for Developers

- 2 Days Course
- Hands-on Labs and Lecture

Course Overview

This 2-day, hands-on course teaches developers how to stand up secure services end-to-end: DNS with BIND 9 on Linux, TLS with Let's Encrypt/ACME, and a reverse proxy using Caddy or NGINX. You'll configure zones, obtain and auto-renew certificates, terminate TLS at a reverse proxy, and apply modern TLS 1.3 hardening—then troubleshoot like a pro.

Who Should Attend

- Developers deploying web apps/services
- DevOps / SRE, sysadmins, and security engineers responsible for TLS/DNS
- Teams standardizing on Caddy or NGINX for reverse proxy/ingress

What You'll Learn

- TLS/SSL fundamentals, x509, cipher suites, TLS 1.3 and extensions
- Let's Encrypt & ACME (HTTP-01, DNS-01, TLS-ALPN-01) and safe automation
- Reverse proxy termination with Caddy (auto HTTPS) and NGINX (certbot)
- Linux DNS with BIND 9: zones, records, email-related DNS, debugging
- Hardening: HSTS, OCSP stapling, PFS, secure ciphers, HTTP→HTTPS redirects
- Troubleshooting TLS and DNS with CLI tools and packet captures

Outline

1. Session 1 — TLS & ACME Foundations (Day 1)

- Lecture: TLS/SSL Overview; TLS 1.2 vs 1.3 essentials
- Lecture: Cryptography Basics (keys, PKI, trust)
- Lecture + Lab: x509 Certificates & Keys — Generate keypairs, CSRs; inspect with openssl
- Lecture + Lab: Security Through Certificates — Chains, intermediates, trust stores; verify paths
- Lecture + Lab: Let's Encrypt & ACME — ACME flow & challenge types (HTTP-01, DNS-01, TLS-ALPN-01); obtain and auto-renew with certbot and acme.sh; renewal hooks and zero-downtime reloads

2. Session 2 — DNS Foundations on Linux (Day 1)

- Lecture: DNS from First Principles; resolution path
- Lecture + Lab: Domain Names (root/TLDs/subdomains); dig basics
- Lecture + Lab: Operational DNS with BIND 9 — Install BIND 9; named.conf; forward & reverse zones; add A/AAAA/CNAME/MX/TXT; serials & zone reloads; validate with dig and packet capture

3. Session 3 — Reverse Proxy + TLS in Practice: Caddy & NGINX Options (Day 2)

- Lecture: Reverse Proxy Patterns & Security — TLS termination, upstream health, redirects, HTTP/2 & HTTP/3 (QUIC); HSTS, OCSP stapling, PFS, cipher policy, security headers
- Lecture + Lab (Option A: Caddy): Automatic HTTPS — Caddyfile basics; site block; reverse proxy to sample app; ACME built-in issuance (HTTP-01 / TLS-ALPN-01); auto-renew, graceful reload, checking cert state
- Lecture + Lab (Option B: NGINX): Certbot + NGINX — NGINX server blocks; reverse proxy to sample app; obtain certs via certbot (webroot & nginx plugins); OCSP stapling, HSTS, secure TLS 1.3 config & ciphers
- Lecture + Lab (Advanced/Optional): DNS-01 with BIND — ACME DNS-01 using acme.sh with RFC2136 updates to BIND; when to prefer DNS-01 (wildcards/private ingress)

4. Session 4 — TLS 1.3 Deep Dive & DNS in Practice (Day 2)

- Lecture: Cipher Suites (TLS 1.3 vs 1.2), Key Exchange, 0-RTT trade-offs
- Lecture + Lab: TLS/SSL Handshake Analysis — openssl s_client, openssl provider, Wireshark traces
- Lecture: TLS Defenses & Common Pitfalls — Header hardening, downgrade prevention, cert pinning caveats
- Lecture + Lab: TLS Attacks & Vulns (safe demos, mitigations)
- Lecture: TLS 1.3 Extensions (ALPN, SNI, OCSP stapling status, EMS, etc.)
- Lecture + Lab: DNS for Email + Debugging — MX/SPF/DKIM/DMARC; validate flows; trace failures with dig, logs
- Lecture + Lab (Capstone): End-to-End Mini-Project — Register/point domain → BIND 9 zones → Reverse proxy (Caddy or NGINX); obtain certs (ACME), enforce HTTPS, add security headers; verify TLS 1.3, HTTP/2/3, stapling, and renewal behavior; troubleshoot break/fix exercises (bad CNAME, stale serials, expired certs)

Prerequisites

Next Courses