G-echo
6 Avenue de la Gare - C24
31380 Garidech
+33.6.03.62.14.40
contact@g-echo.fr

Programme de formation

DNSSEC

But de la formation

- Acquérir la connaissance technique du protocole DNS et de l'extension DNSSEC
- Configurer une installation d'un résolveur (Unbound) validant les réponses avec DNSSEC
- Construire une infrastructure DNSSEC comprenant OpenDNSSEC pour gérer les clés et BIND pour servir les zones signées
- Éviter les pièges du DNS
- Déterminer l'intérêt réel d'un déploiement éventuel de DNSSEC dans leur environnement

Pré-requis

- Formation SECUCYBER
- ou connaissances préalables de l'administration système et des protocoles réseaux TCP/IP

Type de public

- Exploitants et administrateurs systèmes et réseaux,
- Responsables opérationnels,
- Architectes amenés à prendre des décisions de nature technique.

Moyens pédagogiques

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Sanction de la formation

- Formation non certifiante.
- Formation délivrée en partenariat avec HS2

Méthodes pédagogiques

- Cours magistral avec travaux pratiques et échanges interactifs

Durée

14 heures (2 jours).

Programme

DNS : Spécifications et principes

- Vocabulaire
- arbres, zones...
- resolver, cache, authoritative, fowarder...
- Organisation
- TLD, autres domaines, délégations...
- Protocole
- RRSet, entêtes, couche de transport et EDNS
- Problèmes liés aux pare-feux
- Les enregistrements (RR)
- A, AAAA, PTR, SOA, NS, MX ...
- Fonctionnement interne
- Récursion et itération, fonctionnement de la résolution, ...Logiciels
- Couches logicielles
- "stub resolver", résolveur, rôle de l'application...
- Alternatives à BIND
- Outils sur le DNS
- Zonemaster, dig, delv...

Sécurité du DNS

- Risques : modification non autorisée des données, piratage des serveurs, attaque via le routage ou autre "IP spoofing", empoisonnement de cache ... Ce qu'a apporté l'attaque Kaminsky.

Cryptographie

- Petit rappel cryptographie asymétrique, longueur des clés, sécurité de la clé privée ...

DNSSEC

- Clés : l'enregistrement DNSKEY. Méta-données des clés. Algorithmes et longueurs des clés.
- Signature des enregistrements : l'enregistrement RRSIG. Méta-données des signatures.
- Délégation sécurisée : l'enregistrement DS
- Preuve de non-existence : les enregistrements NSEC et NSEC3

DNSSEC en pratique

- Objectifs, ce que DNSSEC ne fait pas, les problèmes apportés par DNSSEC.
- Protocole
- bit DO et couche de transport (EDNS)
- Problèmes liés aux pare-feux
- Créer une zone signée à la main
- dnssec-keygen, -signzone, named-checkzone/conf
- Configurer le résolveur Unbound pour valider
- Vérifier avec dig et delv
- Déboguage
- Délégation d'une zone. Tests avec dnsviz
- Renouvellement de clés
- Créer une zone signée avec DNSSEC

Retour d'expérience

- Zone racine
- Domaines de premier niveau (.fr, .se, .org, ...)
- Zones ordinaires signées
- Stockage des clés. Les HSM.
- Problèmes opérationnels (re-signature, supervision)

Conclusion