** Cette fiche à été générée sur DNDA Formation le 18/05/2022 à 15:05 **

Ref : DNDADNSSEC | **Durée :** 2 Jours | **Tarif :** 1 380 € HT

Formation DNSSEC

Contenu

Objectifs de la Formation DNSSEC:

- 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

Programme de la Formation DNSSEC:

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 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

Public

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

Pré-requis

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

Méthodes pédagogiques

Cours magistral avec travaux pratiques et échanges interactifs.