Formation « DNSSEC »

Réf : DNSSEC

Le DNS est l'infrastructure sur laquelle tous les services d'Internet se reposent. DNSSEC peut protéger contre une large classe de problèmes, comme les attaques par empoisonnement, les serveurs menteurs, les révolveurs DNS configurés par certains fournisseurs pour rediriger les fautes de frappe vers de la publicité. En revanche, c'est une technologie délicate qui nécessite une bonne compréhension.

Objectifs

- 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

Durée & horaires

- 2 jours soit 14 heures
- De 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- 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

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs

Supports

- 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

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- **Cette formation n'est pas certifiante.**

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
- 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