Activité : Configurer une PKI pour gérer des certificats utilisateurs et serveurs

Présentation

Cette activité consiste :

- à comprendre les différences entre la création de certificats auto-signés de des certificats signés par une autorité de certification :
- mettre en oeuvre une infrastructure à clé publique (PKI) avec un pare-feu Stormshield ;
- · créer et utiliser :
 - des certificats utilisateurs signés pour s'authentifier sur un serveur distant et l'interface d'administration, du SNS Stormshield,
 - o des certificats serveurs pour configurer un site Web en HTTPS.

Activités

- Créer un certificat autosigné avec OpenSSH
- Créer un certificat signé par une CA avec openSSH
 - Fiche savoirs : infrastructures à clés publiques
 - Fiche savoirs : infrastructures à clés publiques
 - Fiche savoirs : PKI Stormshield
 - Fiche savoirs : création d'un autorité de certification (CA)
- Activité : créez une autorité de certification racine interne sur le pare-feu Stormshield et définissez-là comme CA par défaut.
- Créer une autorité de certification avec un SNS Stormshield
 - Fiche savoirs : création d'une identité serveur
- Activité : créez une identité pour l'un de vos serveur Debian avec le FQDN web.X.net et mettez-là en oeuvre en configurant par exemple un site Web en https.
 - Fiche savoirs : création d'une identité utilisateur
- Activité: créez-vous une identité utilisateur et utilisez-là pour vous connecter à distance à votre serveur Debian. Pour cela exportez le certificat et la clé privée au format PEM.
 - Fiche savoirs : gestion des identités et des certificats
 - Fiche savoirs : révocation de certificats et CRL

From

/ - Les cours du BTS SIO

Permanent link:

/doku.php/bloc3s1/activitepki?rev=1670165215

Last update: 2022/12/04 15:46

