ssh-keyscan

rassembler les clé publiques ssh

ssh-keyscan permet de rassembler les clé hôtes. Il a été conçu pour aider à construire et vérifier les fichiers ssh_known_hosts.

OPTIONS

-4 Force l'utilisation d'adresses IPv4 uniquement

-6 Force l'utilisation d'adresses IPv6 uniquement

-c Demande les certificats depuis les hôtes cible au-lieu des clés

-f file List les hôtes ou les paires "addrlist namelist" depuis le fichier spécifié, un par ligne

-H Hash tous les noms d'hôtes et les adresses dans la sortie.

-p port Port de connexion à l'hôte distant

-T timeout timeout pour les tentatives de connexion

-t dsa|ecdsa|ed25519|rsa Type de clé à récupérer dans les hôtes scannés

-v mode verbeux

Sécurité

Si un fichier ssh_known_hosts est construit avec ssh-keyscan sans vérifier les clés, les utilisateurs seront vulnérables aux attaques MITM. D'une autre manière, si le modèle de sécurité permet un tel risque, ssh-keyscan peut aider à detecter les fichiers de clé altérés ou les attaques MITM qui ont commencés après que le fichiers ssh_known_hosts ait été créé

Fichiers

Format d'entrée
1.2.3.4,1.2.4.4 name.my.domain,name,n.my.domain,n,1.2.3.4,1.2.4.4
Format de sortie pour RSA, DSA, ECSDA et Ed25519 :
host-or-namelist keytype base64-encoded-key
où keytype est "ecdsa-sha2-nistp256", "ecdsa-sha2-nistp384", "ecdsa-sha2-nistp521", "ssh-ed25519", "ssh-dss" ou "ssh-rsa"

Exemples

Affiche la clé hôte rsa pour la machine "hostname" :
ssh-keyscan hostname
Trouver tous les hôte depuis le fichier ssh_hosts qui ont une clé différente :
ssh-keyscan -t rsa,dsa,ecdsa,ed25519 -f ssh_hosts | sort -u - ssh_known_hosts | diff ssh_known_hosts -