51%

Challenges

L'attaquant contrôle plus de 50% de la puissance de calcul du réseau, ce qui lui permet de prendre le contrôle de la blockchain en invalidant des transactions ou en double-dépensant des fonds. Exemple d'attaque réelle : L'attaque contre la blockchain Ethereum Classic en janvier 2019, où un attaquant a réussi à contrôler plus de 50% de la puissance de calcul et à réaliser des double-dépenses.

#attaque

Double-dépense

Challenges

L'attaquant parvient à dépenser les mêmes fonds deux fois en validant deux transactions différentes sur la blockchain. Exemple d'attaque réelle : L'attaque contre la plateforme d'échange de cryptomonnaies Bitfinex en 2016, où des bitcoins ont été volés par une exploitation de failles dans le protocole pour effectuer des double-dépenses.

#attaque

L'homme du milieu

Challenges

L'attaquant intercepte et modifie les communications entre les participants de la blockchain pour voler des informations sensibles ou modifier les transactions. Exemple d'attaque réelle : L'attaque contre le projet MyEtherWallet en 2018, où des pirates ont utilisé une attaque MITM pour détourner les fonds des utilisateurs.

#attaque

Rejeu

Challenges

L'attaquant enregistre et rejoue des transactions déjà validées sur une blockchain alternative, ce qui peut entraîner des double-dépenses. Exemple d'attaque réelle : L'attaque contre la blockchain Ethereum Classic en janvier 2019, où des transactions précédemment validées ont été rejouées sur une blockchain alternative pour effectuer des double-dépenses.

#attaque

DDoS

Challenges

L'attaquant submerge le réseau de la blockchain avec un grand nombre de requêtes, ce qui peut entraîner des ralentissements, des interruptions de service ou une paralysie complète du réseau. Exemple d'attaque réelle : L'attaque contre le réseau Bitcoin en 2015, où des attaquants ont inondé le réseau avec une quantité massive de transactions, entraînant une congestion du réseau.

#attaque

Contracts malveillants

Challenges

L'attaquant exploite les vulnérabilités des smart contracts pour manipuler leur exécution, voler des fonds ou perturber le fonctionnement de la blockchain. Exemple d'attaque réelle : L'attaque contre le projet de contrat intelligent The DAO en 2016, où des attaquants ont exploité une vulnérabilité du smart contract pour dérober environ un tiers des fonds investis.

#attaque

Sybil

Challenges

L'attaquant crée de multiples identités ou nœuds falsifiés pour obtenir le contrôle ou l'influence sur la blockchain. Exemple d'attaque réelle : L'attaque contre la blockchain Peercoin en 2012, où un attaquant a réussi à contrôler une grande partie des nœuds du réseau en créant de multiples identités, remettant en question la sécurité du consensus.

#attaque