

TP IF03 – ROOT-ME

1. Créez un compte sur la plateforme : <https://www.root-me.org/>
2. Essayez de résoudre les Challenges suivants :

a. CRYPTANALYSE

[Encodage - ASCII](#)
[Encodage - UU](#)
[Hash - Message Digest 5](#)
[Hash - SHA-2](#)
[Substitution monoalphabétique - César](#)

b. CRYPTANALYSE

[Command & Control - niveau 2](#)
[Analyse de logs - attaque web](#)
[Command & Control - niveau 5](#)
[Trouvez le chat](#)
[Vilain petit canard](#)
[Active Directory - GPO](#)
[Command & Control - niveau 3](#)

c. RESEAU

[FTP - Authentification](#)
[TELNET - authentification](#)
[ETHERNET - trame](#)
[Authentification twitter](#)
[Bluetooth - Fichier inconnu](#)
[CISCO - mot de passe](#)
[DNS - transfert de zone](#)

d. STEGANOGRAPHIE

[Gunnm](#)
[Pas très carré](#)
[Point à la ligne](#)
[Steganomobile](#)
[Twitter Secret Messages](#)
[George et Alfred](#)

e. WEB - CLIENT

[HTML - boutons désactivés](#)
[Javascript - Authentification](#)
[Javascript - Source](#)
[Javascript - Authentification 2](#)
[Javascript - Obfuscation 1](#)
[Javascript - Obfuscation 2](#)
[Javascript - Native code](#)
[Javascript - Obfuscation 3](#)
[XSS - Stockée 1](#)

f. WEB - SERVEUR

[HTML](#)
[HTTP - Open redirect](#)
[Injection de commande](#)
[Mot de passe faible](#)
[User-agent](#)
[Fichier de sauvegarde](#)
[HTTP - POST](#)
[HTTP directory indexing](#)
[HTTP Headers](#)
[HTTP verb tampering](#)
[Install files](#)
[CRLF](#)
[File upload - double extensions](#)
[HTTP cookies](#)
[Directory traversal](#)
[PHP assert\(\)](#)
[SQL injection - authentification](#)