



Département Informatique

---

Promotion : 2001–2004

3<sup>ème</sup> année IT + ISIC

Nom :

Année scolaire : 2003–2004

Date : 23 février 2004

Prénom :

---

**Module IT-S301**  
**Session de février**

—  
**Sécurité des systèmes informatiques et**  
**réseaux**  
—

**Contrôle de connaissance<sup>1</sup> de 1 heure et 30 minutes**

---

Merci de répondre (au moins) dans les blancs.

Lire tout le sujet avant de commencer à répondre : cela peut vous donner de l'inspiration...

Chaque question sera notée entre 0 et 10 et la note globale sera calculée par une fonction des notes élémentaires. La fonction définitive sera choisie après correction des copies.

**Attention :** tout ce que vous écrirez sur cette copie pourra être retenu contre vous, voire avoir une influence sur la note d'IT-S301.

## **1 Authentification**

**Question 1 :** Vaut-il mieux un mot de passe du genre toto ou 1kd34@ERTG<sup>2</sup> ? Pourquoi ?

→  
→  
→  
→

---

<sup>1</sup>Sans document, sans calculatrice, sans triche, sans copie sur les voisins, sans micro-ordinateur portable ou non, sans macro-ordinateur, sans téléphone portable ou non, sans talkie-walkie, sans télépathie, sans métémsycose, sans pompe, sans anti-sèche, sans tatouage ni vêtement imprimé en rapport avec le sujet, sans mouchoir de poche pré-imprimé, sans piercing, sans scarification en rapport avec IT-S301,...

<sup>2</sup>Merci à Matthieu PLANTEY pour cette très culturelle question. ☺

**Question 2 : Qu'est-ce qu'une attaque par force brute ?**

**Question 3 :** Citer les 3 manières d'authentifier quelqu'un et donner des exemples.

**Question 4 :** Qu'est-ce que Kerberos ? Quels en sont les concepts principaux ?

**Question 5 :** Est-ce que le mécanisme d'authentification actuel des machines en libre service (distribution sur le réseau en clair via NIS des hachages de mots de passe Unix sur 56 bits) vous semble bien sécurisé. Pourquoi ?

→

## 2 Protocols

→

3

→  
→  
→  
→  
→  
→  
→  
→  
→  
→  
→  
→  
→  
→  
→  
→  
→

**Question 8 :** Imaginez les attaques possibles lors d'une connexion de type `ssh`.

→  
→  
→  
→  
→  
→  
→  
→  
→  
→  
→  
→  
→  
→  
→  
→  
→

**Question 9 :** Comment faire une attaque temporelle sur une connexion utilisant de l'OTP (*One-Time Password* ou mot de passe jetable) si on est capable d'analyser les paquets qui passent, sachant qu'à chaque caractère tapé (et donc y compris le mot de passe) un paquet réseau est envoyé ?

→  
→  
→  
→  
→  
→  
→  
→  
→  
→  
→  
→  
→  
→  
→  
→  
→

→

→

→

5

