M2-TIW4 sécurité des systèmes d'informations
Contrôle continu final – durée 1h30

Master Technologie de l'Information, promotion 2016 – 2017

Mercredi 1er février 2017

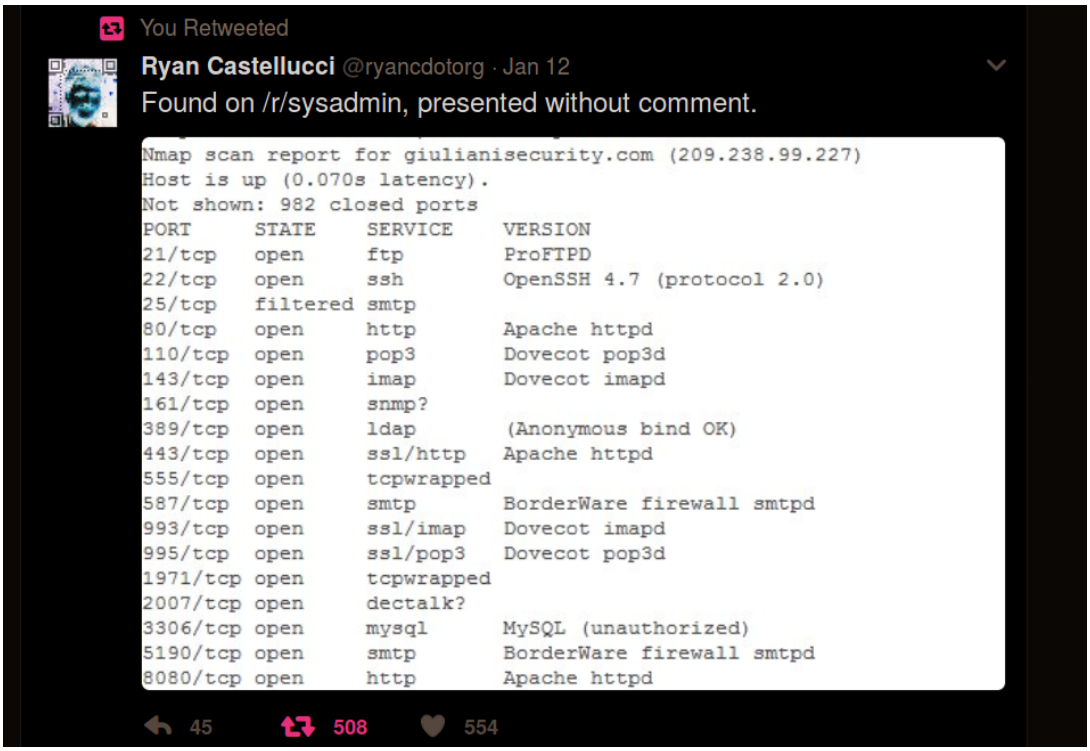
Aucun document autorisé. Le barème est indicatif. La concision, la précision et la clarté des réponses font partie intégrante de l'évaluation. Ne pas rendre le sujet avec la copie.

Exercice 1 : Actualité critique de la sécurité (/4)

Le 12 janvier 2017, le Washington Post publie un article avec le titre suivant "*Trump names Rudy Giuliani as cybersecurity adviser*" dont voici le début :

> President-elect Donald Trump named former New York mayor Rudolph W. Giuliani as an informal adviser on cybersecurity, according to the presidential transition office.
>
> Giuliani, who heads a cybersecurity consulting firm Giuliani Partners, will serve as an adviser on finding solutions to cyber-incursions in the private sector and to advise the government on possible responses.

Vous recevez le tweet ci-dessous sur votre fil :



1. Expliquez brièvement le contenu de la capture d'écran du tweet.
2. Commentez le tweet vis-à-vis de l'actualité.
3. Vous êtes consultant en sécurité. Quelles recommandations pourriez-vous faire à M. Giuliani ?

Exercice 2 : Bonnes et mauvaises pratique du PhP (/4)

Une page PhP vous est fournie en annexe A.

1. Expliquez quelle la fonctionnalité proposée par cette page.
2. Identifiez ses problèmes de sécurité et leurs impacts potentiels.
3. Vous souhaitez garder la fonctionnalité proposée. Que proposez-vous comme solution ?

Exercice 3 : Identity-based cryptosystems and signature schemes (/4)

Les deux premières pages de l'article *Identity-Based Cryptosystems and Signature Schemes* par Adi Shamir sont fournies en annexe B.

1. Expliquez quels sont les points communs et les différences avec les cryptosystèmes à clef publique de type RSA.
2. Ce système est-il intéressant pour protéger les communications sur internet, dans une université, dans un foyer ? Justifiez pour chacun des trois cas.
3. (Bonus) Que pouvez-vous dire sur l'auteur de cette communication ?

Exercice 4 : Andrew Secure RPC (/4)

Considère le protocole suivant appelé *Andrew Secure RPC* :

1. $A \rightarrow B : A, \{N_a\}_{K_{ab}}$
2. $B \rightarrow A : \{N_a + 1, N_b\}_{K_{ab}}$
3. $A \rightarrow B : \{N_b + 1\}_{K_{ab}}$
4. $B \rightarrow A : \{K'_{ab}, N'_b\}_{K_{ab}}$

1. Qu'est ce que désignent K_{ab}, N_a et N_b dans ce protocole ?
2. Expliquez à quoi sert ce protocole.
3. La quatrième étape de ce protocole est vulnérable à une attaque par rejeu où un attaquant peut écouter, bloquer, forger des messages et usurper l'identité d'un tiers. Expliquez le problème et donnez une séquence d'attaque en notant $I(X)$ l'attaquant I qui se fait passer pour X.

Exercice 5 : Modélisation des droits d'accès (/8)

On s'intéresse à une application centralisée de gestion des demandes de financement des travaux de recherche auprès de l'université Lyon 1. Vous participez à la réalisation de cette application, et en particulier du module de contrôle des accès.

L'organisation de l'université est réputée être une *structure* arborescente dont l'UBCL est la racine, les structures de niveau 2 sont les facultés et instituts qui lui sont immédiatement rattachées (exemples : Faculté des Sciences et Technologies – FST, Institut Universitaire Technologies – IUT, etc.) et les départements les structures de niveau 3 qui sont rattachées aux structures de niveau 2 (exemples pour la FST : Département Informatique, Département Physique, etc.).

Chaque structure (exemples : UCBL, IUT, FST, FST-Info, FST-Chimie, IUT-Biologie, etc.) est susceptible de financer des travaux de recherche. Le financement se fait sur examen d'un *dossier*. Chaque structure est dotée d'un unique *comité*, qui nomme en son sein des rapporteurs pour évaluer les dossiers. Après cette évaluation, les dossiers sont classés afin de déterminer lesquels seront financés.

Chaque *Enseignant-Chercheur* (E/C) est membre d'un département. Les E/C déposent des dossiers de demande de financement auprès des structures puis reçoivent la décision de financement quelques mois après. On ne peut déposer un dossier qu'à sa structure de rattachement ou aux structures parentes (exemple : un E/C FST-Info peut déposer auprès de FST-Info, de la FST ou de l'UCBL). Seuls peuvent être membres d'un comité les E/C des sous-structures de la structure du comité. Un E/C ne peut pas évaluer son propre projet.

Pour la modélisation, on considère les actions suivantes :

— `Deposer(idEC, numDossier, numComite)` quand un E/C dépose un dossier auprès d'un comité ;
— `AffecteC(idEC, numComite)` quand un E/C est nommé membre d'une commission ;
— `AffecteR(idEC, numDossier)` quand un E/C est nommé rapporteur d'un dossier déposé dans son comité ;
— `Rapporte(idEC, numDossier, note)` quand un E/C attribue une note à un dossier dont il est rapporteur.

1. Proposez un modèle relationnel de données pour stocker les *structures*, les *comités*, les *E/C*, les *dossiers* et les relations entres ces entités (exemples : les affectations des E/C aux départements, aux comités, etc.). Représentez graphiquement votre modèle en précisant le formalisme utilisé, les contraintes de clef primaire et étrangère. Un soin particulier sera attaché à la modélisation de la structure qui devra être justifié. On remarque notamment qu'il y a une bijection entre les *comités* et les *structures*.
2. Donner une requête SQL, ou à défaut un algorithme en pseudo-code, qui vérifie si un dépôt est autorisé, action `Deposer(idEC, numDossier, numComite)`.
3. Même question pour l'action `AffecteC(idEC, numComite)`.
4. Même question pour l'action `AffecteR(idEC, numDossier)`.
5. Même question pour l'action `Rapporte(idEC, numDossier, note)`.
6. Votre projet prend l'eau : le développement spécifique est arrêté et une solution d'un éditeur de logiciels est retenue. Cette solution s'appuie sur un modèle RBAC. Expliquez comment coder en RBAC les droits précédemment implémentés. Précisez les rôles et leur éventuelle hiérarchie.

A Annexe : code de `tools.php`

```
<?php require_once 'header.php' ?>

<h1>Free online tools</h1>

<div class="container background-white">
  <!-- Nmap Box -->
  <div class="col-md-6 col-md-offset-3 col-sm-offset-3">
      <form class="" method="POST" action="">
          <div align="center" class="error">
      <?php if(isset($error)) echo $error; ?>
          </div>
          <div class="login-header margin-bottom-30">
              <h2>Enter an IP Address</h2>
          </div>
          <div class="input-group">
              <span class="input-group-addon">
                  <i class="fa fa-eye"></i>
              </span>
              <input name="ip" placeholder="ip" class="form-control" type="text">
          </div>
          <div class="row">
              <div class="col-md-6">
                  <input type="submit" class="btn btn-primary pull-right" name="
                      submit" value="Try!" />
              </div>
          </div>
          <hr>
          <h4>Nmap, the best network scanner of the world...</h4>
          <p>
      </form>
  </div>
  <!-- End Nmap Box -->
</div>

<?php
  if(isset($_POST["submit"]))
  {
      if(empty($_POST['ip']))
          $error = "IP field is required.";
      else
      {
          $ip=$_POST['ip'];
          echo "<pre>";
          system("nmap -A ".$ip);
          echo "</pre>";
      }
  }
  require_once ('footer.php');
?>
```

B Annexe : extrait d'un article