Concours externe Inria 2013

Arrêté du 15 avril 2013

Poste LIL1 – Ingénieur systèmes et réseaux (H/F)

Accès au corps des Ingénieurs d'étude (IE)

Epreuve du 2 juillet 2013
Note sur 20 – Coefficient 3– Durée 3 heures

****

La notation prendra en compte la qualité des réponses, mais aussi la rédaction, la présentation, le style et l'orthographe.

Les questions peuvent être traitées dans l'ordre de votre choix. Aucun document autorisé.

Veuillez respecter l'anonymat dans les réponses.

Ne pas omettre de noter votre numéro d'ordre sur les feuilles intercalaires.

****

1. Questions système : (4 points)

1.1 Que fait la commande `chroot /dossierZen` dans un système linux. Expliquez à quoi cela sert-il en donnant un exemple. Donnez les avantages et les difficultés de mise en œuvre

1.2 Définir la différence entre RAID0, RAID1 et RAID5, le nombre de disques minimum nécessaires et leur tolérance de panne ?
1.3 Dans un solution de stockage, quelle est la définition d'un snapshot ? Donnez le principe de fonctionnement, et ses éventuelles variantes. Quels sont les avantages et inconvénients des snapshots ? Quels sont les usages des snapshots sur un système de stockage ? (Répondre en 10-15 lignes maximum)

1.4 Donnez la définition d'un SAN et d'un NAS. Pour chacun d'entre eux, précisez les avantages et inconvénients et les protocoles utilisés.

1.5 Qu'est que iSCSI ?

2. Programmation de scripts (3 points)

2.1 étude de script

```
# !/bin/sh
#Demarrage des news version INN2.2

HOMENEWS="/usr/lib/news"
case "$1" in
'start')
      if [ -f /var/run/news/innwatch.pid ] ; then
            rm /var/run/news/innwatch.pid
      fi
      if [ -f /var/run/news/innd.pid ] ; then
            rm /var/run/news/innd.pid
```

```
      fi
      if [ -f /var/run/news/innfeed.pid ] ; then
            rm /var/run/news/innfeed.pid
      fi
      if [ -f /var/run/news/LOCK.innwatch ] ; then
            rm /var/run/news/LOCK.innwatch
      fi
      pid=`ps -e | grep innd | awk '{print $1}'`
      if [! -z "$pid"] ; then
            echo "Arret innd News"
            kill -9 $pid
      fi
      pid=`ps -e | grep innfeed | awk '{print $1}'`
      if [! -z "$pid"] ; then
            echo "Arret innfeed News"
            kill -9 $pid
      fi
      pid=`ps -e | grep innwatch | awk '{print $1}'`
      if [! -z "$pid"] ; then
            echo "Arret innwatch News"
            kill -9 $pid
      fi
      su news -c ${HOMENEWS}/bin/rc.news
      ;;
'stop')
      rm /var/run/news/*.pid ; rm /var/run/news/LOCK.*
      pid=`ps -e | grep innd | awk '{print $1}'`
      if [! -z "$pid"] ; then
            echo "Arret innd News"
            kill -9 $pid
      fi
      pid=`ps -e | grep innfeed | awk '{print $1}'`
      if [! -z "$pid"] ; then
            echo "Arret innfeed News"
            kill -9 $pid
      fi
      pid=`ps -e | grep innwatch | awk '{print $1}'`
      if [! -z "$pid"] ; then
            echo "Arret innwatch News"
            kill -9 $pid
      fi
```

2.1.1 Que fait le script, et quelles sont les différentes étapes ? Comment sont utilisés ces scripts de forme bien particulière dans les systèmes linux ?

2.1.2 Expliquez la ligne suivante :

```
pid=`ps -e | grep innwatch | awk '{print $1}'`
```

2.2 Ecrivez un script shell qui prend en paramètre un répertoire, affiche la liste des fichiers avec l'extension `.csv` contenus dans ce répertoire, échange les colonnes 1 et 2 de chacun de ces fichiers et écrit le résultat dans le fichier correspondant avec une extension `.new` .

3. Question virtualisation (4 points)

Vous hébergez de nombreux sites web d'équipes de recherche hébergés sur des serveurs physiques. Vous devez faire évoluer votre parc de serveurs et vous envisager d'acquérir des serveurs de virtualisation.

3.1 Citez au moins 3 avantages à la virtualisation ?

3.2 Vous utilisiez les virtualhosts d'apache dans vos serveurs physiques actuels. Continuez-vous à utiliser cette pratique avec des serveurs virtuels et pourquoi ?

3.3 quelle architecture minimale ou configuration en terme de serveur/stockage préconiseriez-vous et pourquoi ?

3.4 quels sont les différentes approches pour virtualiser un serveur sur un hyperviseur existant :

→ pour serveur existant ;
→ pour un nouveau serveur
→ pour être capable de déployer un nouveau serveur web très rapidement

3.5 qu'est ce qu'un pool de serveurs de virtualisations et quel est son intérêt ?

4. Questions réseaux (4 points)

4.1 Citez les différents modes d'authentification utilisés sur les réseaux wifi et classez-les par ordre de sécurité croissant.

4.2 Quel est le type d'enregistrement DNS spécifiquement utilisé pour l'envoi de messages entre relais messagerie ?

4.3 Quelle est la norme qui permet de propager plusieurs VLANs sur un même lien physique ?

4.4 Expliquez le principe de fonctionnement d'un commutateur ethernet.
Comment est commutée une trame ethernet lorsque l'adresse de destination d'une machine n'est pas connue du commutateur ?
Expliquez l'intérêt de déployer des commutateurs supportant les VLANs.

4.5 Citez 2 protocoles de redondance de routeur et expliquez leur principe de fonctionnement (maximum 6 lignes)

4.6 Expliquez le principe de fonctionnement d'un routeur IP.
Décrivez la différence entre le routage statique et le routage dynamique.
Citez quelques exemples de protocoles de routage intérieurs et extérieurs ?
Dans quels cas convient-il d'utiliser un protocole de routage de type "extérieur" ?
Explicitez les principes de fonctionnement, notamment le niveau de granularité pour le routage "intérieur" et le routage "extérieur".

5. Question projet/méthodologie (2,5 points)

Vous êtes en charge d'un nouveau projet pour le centre de recherche. Il s'agit de la mise en place d'un nouveau service. Décrivez toutes les étapes à réaliser de l'idée originale à la mise en production pour vos utilisateurs. A chaque étape, indiquez les acteurs impliqués. Illustrez votre discours par le projet de mise en place d'un service de partage de fichier en ligne à la dropbox. (rédigez en 15-20 lignes)

6. Question sécurité (2,5 points)

6.1 Qu'est ce qu'un CERT. Qu'est ce que le CERTA en France

6.2 Certaines applications ou services web internes à l'établissement fonctionnent avec java. Vous venez de recevoir le bulletin de sécurité concernant java (cf Annexe).

- Décrivez en français, le problème et les risques encourus.
- Quelles mesures allez-vous prendre pour pallier à cette vulnérabilité ?
- Rédigez, en anglais et en français, l'annonce que vous allez envoyer aux utilisateurs.

6.3 (In English please) Explain in 10 lines what Single-Sign-On means. Provide examples.

Annexe : bulletin de sécurité

Alert (TA13-010A)

Oracle Java 7 Security Manager Bypass Vulnerability

Original release date: January 10, 2013 | Last revised: February 06, 2013

Systems Affected

Any system using Oracle Java 7 (1.7, 1.7.0) including

- Java Platform Standard Edition 7 (Java SE 7)
- Java SE Development Kit (JDK 7)
- Java SE Runtime Environment (JRE 7)
- OpenJDK 7 and 7u
- IcedTea 2.x (IcedTea7 2.x)

All versions of Java 7 through update 10 are affected. Web browsers using the Java 7 plug-in are at high risk.

Overview

A vulnerability in the way Java 7 restricts the permissions of Java applets could allow an attacker to execute arbitrary commands on a vulnerable system.

Description

A vulnerability in the Java Security Manager allows a Java applet to grant itself permission to execute arbitrary code. An attacker could use social engineering techniques to entice a user to visit a link to a website hosting a malicious Java applet. An attacker could also compromise a legitimate web site and upload a malicious Java applet (a "drive-by download" attack).

Any web browser using the Java 7 plug-in is affected. The Java Deployment Toolkit plug-in and Java Web Start can also be used as attack vectors.

Reports indicate this vulnerability is being actively exploited, and exploit code is publicly available.

Further technical details are available in Vulnerability Note VU#625617.

Impact

By convincing a user to load a malicious Java applet or Java Network Launching Protocol (JNLP) file, an attacker could execute arbitrary code on a vulnerable system with the privileges of the Java plug-in process.

Solution

Update Java

Oracle Security Alert CVE-2013-0422 states that Java 7 Update 11 (7u11) addresses this (CVE-2013-0422) and a different but equally severe vulnerability (CVE-2012-3174).

Java 7 Update 11 sets the default Java security settings to "High" so that users will be prompted before running unsigned or self-signed Java applets.

Disable Java in web browsers

This and previous Java vulnerabilities have been widely targeted by attackers, and new Java vulnerabilities are likely to be discovered. To defend against this and future Java vulnerabilities, consider disabling Java in web browsers until adequate updates are available. As with any software, unnecessary features should be disabled or removed as appropriate for your environment.

Starting with Java 7 Update 10, it is possible to disable Java content in web browsers through the Java control panel applet. From Setting the Security Level of the Java Client:

For installations where the highest level of security is required, it is possible to entirely prevent any Java apps (signed or unsigned) from running in a browser by de-selecting Enable Java content in the browser in the Java Control Panel under the Security tab.

If you are unable to update to Java 7 Update 10 please see the solution section of Vulnerability Note VU#636312 for instructions on

how to disable Java on a per-browser basis.Vulnerability Note VU#625617

References

- Vulnerability Note VU#625617
- Setting the Security Level of the Java Client
- The Security Manager
- How to disable the Java web plug-in in Safari
- How to turn off Java applets
- NoScript
- Securing Your Web Browser
- Vulnerability Note VU#636312
- Oracle Security Alert CVE-2013-0422
- Security Alert for CVE-2013-0422 Released
- JDK 7u11 Release Notes

Revisions

- January 10, 2013: Initial release
- January 14, 2013: Added fix information per Java 7u11 release
- January 15, 2013: Added OpenJDK and IcedTea to Systems Affected