UNIVERSITÉ CHEIKH ANTA DIOP DE DAKAR

ECOLE SUPERIEURE POLYTECHNIQUE

DEPARTEMENT GENIE INFORMATIQUE

MASTER2 EN GENIE LOGICIEL ET

SYSTÈME D'INFORMATION (GLSI) ET SRT

A08 :2021- DEFAILLANCES DU LOGICIEL ET DE L'INTEGRITE DES DONNEES

Victorine Sady NDIAYE

Anta Diop MBAYE

Mame Meissa DIENG

Zeinebou MOHAMED MAHMOUD

Plan

1. Matching des concepts par rapport à notre catégorie
2. Exploitation de la catégorie (CWE, CVE)
3. Illustration du scenario
4. Création d’un scénario
5. Outils
6. Mise en œuvre
7. Démonstration
8. Mesures préventives

1. Matching des concepts par rapport à notre catégorie

Le but premier de l'utilisation de la cryptographie est de garantir les quatre services fondamentaux de la sécurité des informations :

- La confidentialité,
- L'intégrité des données,
- L'authentification,
- La non-répudiation.

Dans notre cas, on étudie la défaillance du logiciel et de l'intégrité des données.

Intégrité des données :

C'est le service de sécurité qui s'occupe d'identifier toute altération des données.

Le destinataire d'un message doit pouvoir vérifier que celui-ci n'a pas été modifié en chemin.

Un intrus ne doit pas être capable de faire passer un faux message pour un légitime (chapitre 1).

❖ **Fonction de hachage**

Les fonctions de hachage sont utilisées pour l'intégrité des données en conjonction avec des schémas de signature numérique, où un message est typiquement haché en premier, puis la valeur de hachage, en tant que représentant du message, est signée à la place du message d'origine (chapitre 6).

On a deux types de fonctions de hachage qui sont liés à l'intégrité des données

- Une fonction de hachage à sens unique porte de nombreux noms : fonction de compression, fonction de contraction, digest, empreinte digitale, code correcteur cryptographique, code de vérification d'intégrité, code de détection de manipulation.
- Les MACs

  Les MAC peuvent être utilisés pour fournir l'intégrité des données et l'authentification d'origine des données, ainsi que l'identification dans les schémas symétriques.

2. Exploitation de la catégorie (CWE, CVE)

Les défaillances de l'intégrité des logiciels et des données sont liées au code et à l'infrastructure qui ne sont pas protégés contre les violations de l'intégrité. C'est le cas, par exemple, lorsqu'une application s'appuie sur des plugins, des bibliothèques ou des modules provenant de sources, de dépôts et de réseaux de diffusion de contenu (CDN) non fiables. Un pipeline CI/CD non sécurisé peut introduire un risque d'accès non autorisé, de code malveillant ou de compromission du système. Enfin, de nombreuses applications intègrent désormais une fonctionnalité de mise à jour automatique, où les mises à jour sont téléchargées sans vérification d'intégrité suffisante et appliquées à l'application précédemment fiable. Les attaquants pourraient potentiellement télécharger leurs propres mises à jour pour les distribuer et les exécuter sur toutes les installations. Un autre exemple est celui des objets ou des données qui sont codés ou sérialisés dans une structure qu'un attaquant peut voir et modifier et qui sont vulnérables à une désérialisation non sécurisée.

Il s'agit de l'un des impacts pondérés les plus élevés des données CVE/CVSS (Common Vulnerability and Exposures/Common Vulnerability Scoring System). Les Common Weakness Enumerations (CWE) notables comprennent :

- **CWE-494 : Téléchargement de code sans contrôle d'intégrité**
  - **CVE-2019-9534 :** Le téléphone satellite ne valide pas son image de micrologiciel.
  - **CVE-2021-22909 :** Chaîne : la procédure de mise à jour du micrologiciel du routeur utilise curl avec l'option "-k" (non sécurisée) qui désactive la validation du certificat (CWE-295), permettant la compromission de l'adversaire au milieu (AITM) avec une image de micrologiciel malveillante (CWE-494).
  - **CVE-2008-3438 :** Le système d'exploitation ne vérifie pas l'authenticité de ses propres mises à jour.
- **CWE-502 : Désérialisation des données non fiables**
  - **CVE-2019-12799 :** chaîne : contournement du problème de désérialisation non fiable (CWE-502) en utilisant une classe supposée fiable (CWE-183)
  - **CVE-2015-8103 :** Le problème de désérialisation dans la bibliothèque Java couramment utilisée permet une exécution à distance.
  - **CVE-2015-4852 :** Le problème de désérialisation dans la bibliothèque Java couramment utilisée permet une exécution à distance.

❖ **CWE-829 : Inclusion de fonctionnalités de la sphère de contrôle non fiable**

- **CVE-2010-2076 :** Le produit ne rejette pas correctement les DTD dans les messages SOAP, ce qui permet à des attaquants distants de lire des fichiers arbitraires, d'envoyer des requêtes HTTP à des serveurs intranet ou de provoquer un déni de service.
- **CVE-2004-0285 :** La modification de la variable de configuration supposée immuable dans le fichier d'inclusion permet l'inclusion de fichiers via une demande directe.
- **CVE-2004-0030 :** La modification de la variable de configuration supposée immuable dans le fichier d'inclusion permet l'inclusion de fichiers via une demande directe.

3. Illustration du scenario

SolarWinds a expliqué que les cybers délinquants avaient réussi à accéder au système de mise à jour de son logiciel Orion pour y insérer un code malveillant. C'est ce qu'on appelle une attaque sur la chaîne d'approvisionnement. Une méthode particulièrement prisée des pirates informatiques car elle leur permet de passer totalement inaperçus au sein d'un logiciel de confiance. Dans le cas de SolarWinds, la manœuvre s'est avérée d'une redoutable efficacité car des centaines de milliers d'entreprises et d'agences gouvernementales dans le monde utiliseraient le logiciel Orion. Microsoft a confirmé avoir trouvé des traces du malware dans ses systèmes qui a affecté une quarantaine de ses clients. L'entreprise de sécurité informatique FireEye a également été touchée par le logiciel malveillant qui s'est également propagé dans les systèmes de ses clients.

4. Création d'un scénario

Une entreprise pharmaceutique vante la sureté de son nouveau médicament miracle. Mais quand l'autorité sanitaire inspecte ce site, le travail est immédiatement arrêté. D'importantes données de contrôle qualité sont manquantes. En effet, un concurrent a payé un hacker pour qu'il modifie ces données de telle sorte que l'entreprise n'a pas pu remplir tous les critères imposés par l'autorité sanitaire.

5. Outils

- **SolarWinds**

SolarWinds est une société américaine qui développe des logiciels professionnels permettant la gestion centralisée des réseaux, des systèmes et de l'infrastructure informatique.

- **GNS3**

GNS3 (Graphical Network Simulator) est un logiciel libre permettant l'émulation ou la simulation de réseaux informatiques.

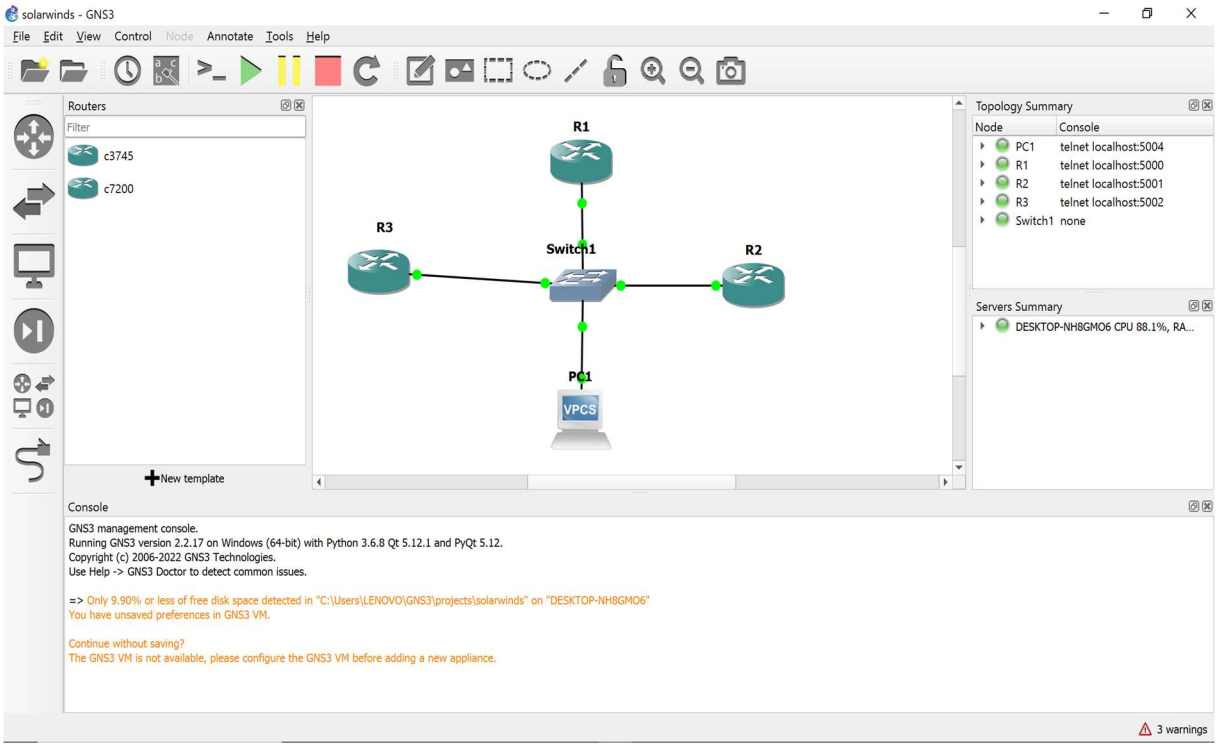
- **GNS3 VM**

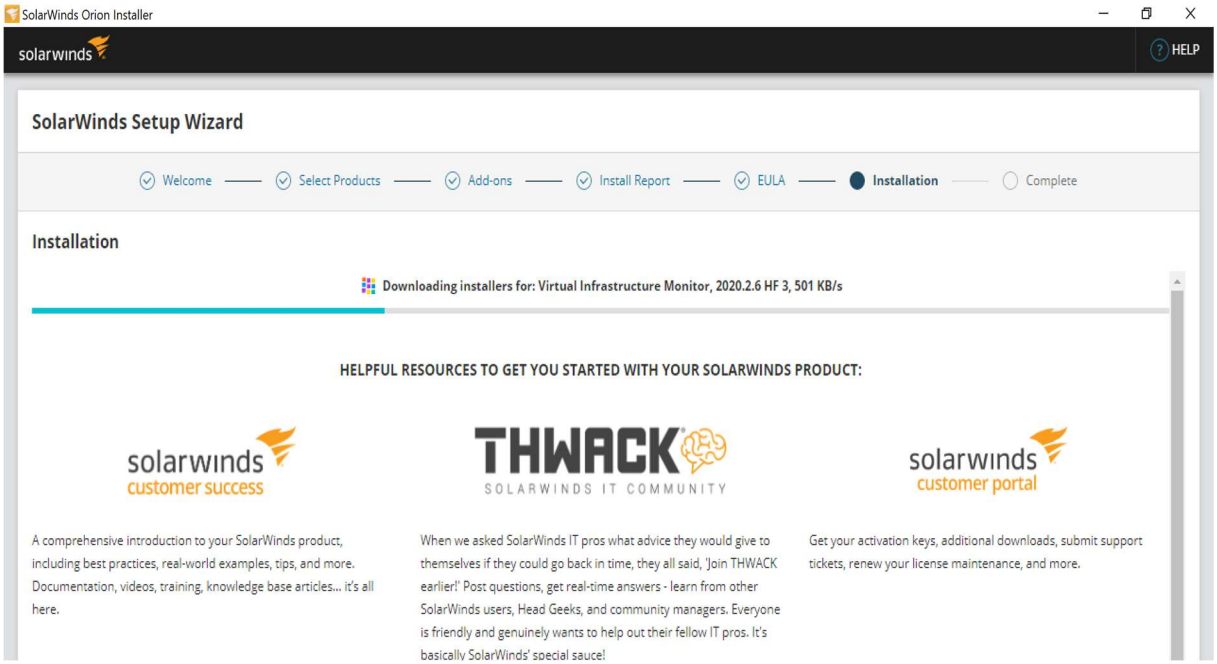
GNS3 VM est recommandée pour la plupart des situations lorsque vous utilisez Windows ou MAC OS. Elle permet de créer des topologies GNS3 qui évite de multiples problèmes courants rencontrés lors de l'utilisation d'une installation locale de GNS3.

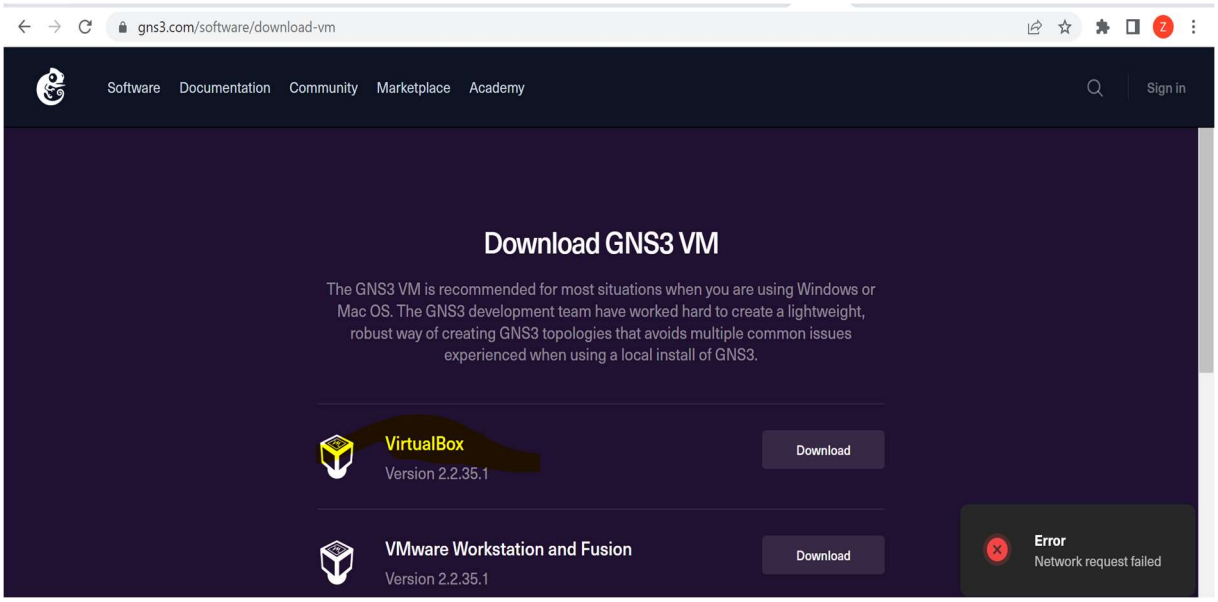
- **VirtualBox VM**

VirtualBox est un logiciel libre de virtualisation publié par Oracle.

6. Mise en œuvre







7. Démonstration

8. Mesures préventives

Contrairement à d'autres mesures de sécurité, les solutions de surveillance de l'intégrité des fichiers sont spécialement conçues pour surveiller les modifications apportées aux fichiers. Le logiciel capture généralement un instantané de votre système, puis le compare régulièrement à l'état actuel du système. Lorsqu'il détecte des modifications apportées aux fichiers qui suggèrent une intrusion non autorisée (comme des modifications de taille soudaines ou l'accès

de certains utilisateurs), il peut prévenir le personnel informatique ou agir pour réduire la menace.

- **SolarWinds Security Event Manager**

SolarWinds Security Event Manager est une option prête à l'emploi pour les entreprises qui centralise toutes les informations dont vous avez besoin pour mener une surveillance de l'intégrité des fichiers efficace, ainsi que d'autres tâches de surveillance essentielles. Les fonctions de surveillance en temps réel SIEM de l'outil peuvent rapidement vous prévenir d'une activité sur le registre, les fichiers et les dossiers.

- **OSSEC**

OSSEC est un système de détection des intrusions open-source pour Linux et Mac OS X. Il dispose d'une fonctionnalité de surveillance de fichiers spécifique appelée « Syscheck ». Par défaut, il s'exécute toutes les six heures pour vérifier les modifications apportées aux sommes de contrôle des fichiers principaux. Il est conçu pour réduire l'utilisation du processeur, ce qui signifie qu'il constitue un candidat potentiel pour les entreprises à la recherche d'une solution de surveillance de l'intégrité des fichiers avec un faible encombrement. Néanmoins, OSSEC est disponible uniquement pour Windows en mode serveur-agent, et n'offre donc pas de détection de rootkit pour Windows. En outre, vous devrez gérer tous les problèmes coûteux en temps liés aux programmes open-source. La plupart des entreprises optent rapidement pour une solution payante à la place.

- **SolarWinds Server & Application Monitor**

SolarWinds Server & Application Monitor est une autre bonne option pour surveiller votre système, car il peut surveiller Windows, Linux et diverses options de stockage sur site et dans le Cloud. Il dispose de modèles pour environ 1 200 applications, serveurs, bases de données et infrastructures fournisseur, vous permettant de garantir la sécurité des fichiers sur à peu près n'importe quelle partie de votre réseau global, le tout depuis une interface unique et simple