Master SSI - Projets

14 septembre 2020

Table des matières

1 Introduction

Ce document présente un certain nombre de projets associés aux UE GS11, GS13 et GS21 du master SSI.

2 Projet GS11 : Sécuriser l'infrastructure SI d'une entreprise

2.1 Scénario

L'entreprise « Mon beau réseau » a un réseau informatique composé de postes de travail windows (fixes et portables, dédiés ou partagés, Windows), d'un poste Windows d'administration, d'un serveur web Linux, d'un serveur Windows contrôleur de domaine Active Directory, d'un switch Cisco et d'un routeur connecté à Internet. L'entreprise souhaite sécuriser son réseau afin de protéger ses informations et de limiter la surface d'attaque. L'administrateur réseau de l'entreprise a placé un firewall Linux à 3 interfaces réseau. La première est connectée au routeur Internet, la seconde est connectée au serveur web Linux et la troisième à un switch disposant de VLAN différents pour le serveur Windows, les postes de travail et le poste d'administration. Pour la simulation le firewall aura **5 interfaces réseaux** :

- une connectée au routeur Internet
- une connectée au serveur web Linux
- un switch disposant de VLAN différents pour :
  - le serveur Windows
  - les postes de travail
  - le poste d'administration

2.2 Les étapes

2.2.1 Pour le firewall

Tout d'abord, vous devez configurer le pare-feu pour que :

- le serveur Linux en DMZ soit accessible de l'extérieur et du réseau interne et HTTP et HTTPS
- les postes Windows accèdent au domaine Active Directory,
- les postes de travail puissent accéder à des sites Web externes
- le poste d'administration puisse se connecter d'une part au pare-feu, routeur et serveur Linux en SSH et d'autre part au serveur Active Directory en Terminal Server et MMC

2.2.2 Pour le switch CISCO non simulé

Un seul équipement est connecté sur chaque port du switch. Puis, vous devez proposer une configuration pour chacun des 3 VLAN et limiter les attaques ARP en limitant le nombre d'équipements associés à un port physique

2.2.3 Pour le serveur web

Le serveur web Linux est configuré avec Apache. Il est lancé avec l'utilisateur www-data et le groupe www-data. La configuration d'Apache est dans le répertoire /etc/apache2 , le document root est le répertoire /var/www et le répertoire de log est /var/log . Vous devez ensuite configurer les droits des fichiers et répertoires /etc/apache2 , /var/www et /var/log . Puis, vous devez créer un **utilisateur « webadmin »** qui pourra modifier les fichiers du document root. et qui appartient au groupe www-data. En revanche l'utilisateur www-data ne pourra que lire et exécuter ces fichiers mais pas les modifier. L'utilisateur www-data pourra lire et modifier les fichiers dans le répertoire /var/log mais ne pourra pas les exécuter. Il pourra enfin lire et exécuter les fichiers dans le répertoire /etc/apache2, mais ne pourra pas les modifier

2.2.4 Pour Active directory

Vous devez configurer les GPO sur le serveur Windows Active Directory afin que :

- tous les mots de passe aient une taille minimum de 10 caractères et qu'ils contiennent au moins une majuscule, une minuscule et un chiffre. Vous devez également activer automatiquement l'écran de veille en cas d'inactivité d'un poste de travail au bout de 10 minutes et demander le mot de passe pour rouvrir la session
- une stratégie de restriction logicielle (SRP) soit appliquée sur les postes pour n'autoriser que les programmes des répertoires Windows hors répertoire temporaire et Program Files
- l'accès à l'administrateur local des postes ne soit pas accessible à distance

2.2.5 Pour le réseau

Pour simuler le réseau, vous utiliserez des machines virtuelles (sur Virtualbox). Le réseau nécessite de faire fonctionner plusieurs machines en même temps, il vous faut donc une configuration suffisamment puissante avec au minimum un processeur multicoeur (i5 conseillé) et 8Go de RAM. Pour la simulation, vous ne créerez qu'une seule machine Windows utilisateur (en plus du serveur Windows et du poste d'administration Windows).
Pour installer les machines Linux et Windows sous Virtualbox vous pouvez vous référer à la documentation officielle [1] et pour la partie réseau [2]. On utilisera aussi les liens de téléchargement suivants :

- Virtualbox [3]
- Linux Ubuntu [4]
- Windows Server 2016 [5]
- Windows 10 [6]

2.2.6 Résumé des instructions

Vous devrez donc :

- configurer le firewall Linux avec Iptables
- configurer le switch Cisco sans l'utiliser dans la simulation Virtualbox
- créer un utilisateur « webadmin » sur le serveur web Linux
- configurer les permissions des fichiers du serveur web Linux
- configurer les GPO Active Directory

Option : pour CISCO vous pouvez le simuler à part avec Packet Tracer, prendre le 3660 en s'inscrivant gratuitement sur le cours **netcad** [7].

2.3 Livrables

2.3.1 Fichiers

Dans un répertoire nommé "Securiser-infrastructure-NOM1-NOM2", vous mettrez à disposition du jury :

- un rapport (qui peut être un fichier de présentation ppt) qui résume ce que vous avez fait
- un fichier de scripts bash nommé "iptables.sh" contenant les commandes pour configurer le firewall avec Iptables avec les commentaires pour expliquer les commandes
- un fichier texte de configuration du switch
- un fichier de scripts bash nommé "webadmin.sh" contenant les commandes pour créer l'utilisateur « webadmin » et modifier les permissions des fichiers du serveur web avec les commentaires pour expliquer les commandes
- un fichier PDF nommé "GPO.pdf" contenant les captures d'écran de la configuration des GPO sur le contrôleur de domaine *Active Directory* avec une description de chaque capture pour expliquer la configuration qu'elle illustre

2.3.2 Soutenance

Pendant 15 minutes, vous présenterez au jury comment vous avez configuré les éléments de l'infrastructure SI en expliquant :

- quelles sont les commandes que vous avez utilisées
- comment afficher l'état de la configuration des éléments
- comment vérifier le bon fonctionnement des règles de sécurité mises en place

Cette présentation sera suivie de 10 minutes de questions-réponses.

2.4 Compétences à acquérir

Les compétences à valider sont ici :

- sécuriser les éléments du système informatique
- identifier et élaborer les solutions techniques

2.5 Cours associés

On pourra s'aider des cours en ligne suivants :

- Reprenez le contrôle à l'aide de Linux [8]
- Simulez les architectures réseau avec GNS3 [9]
- Centralisez et sécurisez votre annuaire Active Directory [10]

3 Projet GS11 : Sécurisation des applications

3.1 Scénario

Vous êtes développeur sécurité pour la société "A vos Marques" de 200 employés et 20 magasins spécialisée dans le commerce d'articles de sport. La société souhaite développer une application web pour que les vendeurs de ses magasins puissent commander de nouveaux stocks. Cette application est composée d'un serveur web et d'une base de données. De plus l'application comprend une interface de connexion et une interface de commande de produit. Le RSSI vous demande de vous assurer que l'application est développée de manière sécurisée. Pour cela, vous devez lister les exigences de sécurité de l'application pour l'interface de connexion et l'interface de commande de produits et les solutions pour sécuriser la mise en place de l'application. Les exigences de sécurité doivent répondre aux besoins suivants :

- les utilisateurs doivent s'authentifier avec leur mot de passe (qu'ils ont défini lors de la création de compte). Ce mot de passe ne doit pas être accessible à une personne tierce (sur le réseau et même en cas de vol de la base de données) (hash mot de passe, https)
- les interfaces clients de l'application ne doivent pas afficher d'autres informations que celles voulues par le cahier des charges, ni être modifiées par un attaquant (XSS)
- un attaquant ne doit pas pouvoir se connecter à un compte sans le bon mot de passe ni accéder ou modifier les informations des autres comptes.
- un utilisateur ne doit pas pouvoir faire de commande sans s'en rendre compte. Pour faire une commande, il doit cliquer sur le bouton "commander" de l'interface de commande de produit et le bouton doit être visible.
- un attaquant ne doit pas pouvoir lister les fichiers de l'application ni avoir accès aux information de configuration du serveur web.

3.2 Travail à réaliser

3.2.1 Analyse de code

L'équipe de développeur a développé la portion de code figure 1, téléchargeable [11]. Inspectez ce code et faites la liste des vulnérabilités présentes qui ne respectent pas les exigences de sécurité.
Rédigez une liste de tests de sécurité pour ce code en précisant quelle vulnérabilité est évaluée par le test et quels sont les résultats valides et invalides possibles.

3.2.2 Instructions

Vous devrez donc :

- faire la liste des exigences de sécurité en précisant les solutions techniques à mettre en oeuvre en 3 parties :
  - exigences de sécurité pour l'application globale

```
<%@page import="java.sql.*"%>
<%@ page language="java" contentType="text/html; charset=ISO-8859-
1" pageEncoding="ISO-8859-1"%>
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-
8859-1">
<title>Connexion ¢ A vos Marques</title>
</head>
<body>
<%
String identifiant = request.getParameter("identifiant");
String motDePasse = request.getParameter("motDePasse");
Class.forName("com.mysql.jdbc.Driver");
Connection con = (Connection)
DriverManager.getConnection("jdbc:mysql://localhost:3306/mydb",
"root" ,"");
Statement st= con.createStatement();
ResultSet rs=st.executeQuery("select * from utilisateurs where
ident='"+identifiant+"' and pass='"+motDePasse+"' limit 0,1");
if(rs.next())
{
out.println("Vous ↑tes bien connect← "+identifiant);
}
else
{
out.println("Erreur d'authentification pour
"+identifiant);
}
%>
</body>
</html>
```

FIGURE 1 – P4- Portion de code

  - exigences de sécurité pour la fonction "authentification"
  - exigences de sécurité pour la fonction "commande de produits"

- faire la listes des vulnérabilités présentes dans le code source
- proposer des tests de sécurité pour valider la conformité de l'application avec les exigences de sécurité, en détaillant le scénario testé et le résultat attendu.

3.3 Livrables

3.3.1 Fichiers

Dans un dossier nommé "Securite-Application-NOM1-NOM2", vous mettrez à disposition du jury :

- un fichier PDF nommé "exigences-securite.pdf" d'environ 5 pages détaillant les exigences de sécurité en précisant leur objectif, les vulnérabilités associées et les solutions de sécurité préconisées
- un fichier PDF nommé "vulnerabilites-code.pdf" d'environ 3 pages détaillant les vulnérabilités trouvées dans le code source
- un fichier PDF nommé "tests-securite.pdf" d'environ 3 pages détaillant les tests de sécurité à utiliser pour s'assurer de la conformité de l'application avec les exigences de sécurité

3.3.2 Soutenance

Pendant 15 minutes, vous présenterez au jury les exigences de sécurité que vous avez définies en justifiant quelles solutions techniques répondent aux besoins et quels tests permettent de valider le respect des exigences de sécurité. Cette présentation sera suivie de 10 minutes de questions-réponses.

3.4 Compétences à valider

Les compétences à valider dans ce module sont :

- lister les exigences de sécurité
- identifier les vulnérabilités présentes dans un code source
- proposer des tests de sécurité pour valider la conformité d'une application avec les exigences de sécurité

3.5 Cours associés

On pourra s'appuyer sur les cours en lignes suivants :

- Sécurisez vos applications [12]
- Sécurisez vos infrastructures [13]
- Sécuirsez vos données avec la cryptographie [14]

4 Projet GS11 : Audit de sécurité

4.1 Scénario

La mairie de la ville de "Chateaudo" souhaite auditer la sécurité de son SI afin de vérifier que objectifs de sécurité SI sont bien mis en oeuvre et d'évaluer les points forts et les faiblesses de son SI. En tant que Responsable Sécurité SI, vous êtes chargé de rédiger un plan d'audit qui définit les objectifs, le périmètre et le déroulement de l'audit. Le SI de l'entreprise est constitué de :

- 30 postes de travail Windows
- un serveur Windows contrôleur de domaine Active Directory
- un serveur d'application métier et de fichiers Windows
- un serveur web et email Linux
- un Firewall
- un switch réseau
- un routeur connecté à Internet

Les utilisateurs du SI sont :

- les utilisateurs simples, qui n'ont accès qu'à un nombre limité de données
- les utilisateurs managers, qui ont accès à l'ensemble des données de leur service
- les administrateurs systèmes qui ont un accès administrateur sur les postes de travail, les serveurs d'applications et les équipements réseau
- le responsable sécurité SI qui a un accès administrateur sur le contrôleur de domaine Active Directory et sur le Firewall

Les principaux objectifs de sécurité sont :

- la confidentialité des données de l'entreprise : seules les personnes autorisées doivent pouvoir accéder aux informations
- la disponibilité du SI : Les applications doivent être fonctionnelles et résistantes aux incidents de sécurité courants. En cas d'incident majeur, le SI doit être en mesure de revenir à un fonctionnement normal en minimisant la durée de la panne et la perte d'information

4.2 Travail à réaliser

4.2.1 Etape 1

Dans un premier temps, vous devez établir un plan d'audit de la sécurité du SI. Ce plan doit comprendre une partie organisationnelle qui évalue l'organisation et les procédures du SI et une partie technique qui doit évaluer la sécurité de l'architecture générale, des systèmes et des applications, y compris pour sensibiliser la direction sur les risques d'une compromission. Pour répondre à ces différents objectifs, vous devez proposer des types d'audit, leur démarche, des exemples de points de contrôle et de résultats qui pourraient être observés.

4.2.2 Etape 2

Dans un deuxième temps, vous devez réaliser un test d'intrusion sur une application web. L'application est contenue dans le fichier "Projet+5_DVWA.zip" et téléchargeable [15].
Elle peut être installée sur une machine virtuelle. Cette application contient **12 types de vulnérabilités** fréquentes, et **3 occurrences** du type de vulnérabilité selon le niveau de difficulté. Vous devez **rédiger un rapport d'audit** qui décrit la **méthodologie** et les **outils** utilisés pour réaliser le test d'intrusion, présenter chaque vulnérabilité et évaluer son impact et **proposer une solution** par type de vulnérabilité pour la corriger.

4.2.3 Instructions

Vous devrez donc :

- **établir un plan d'audit** de la sécurité du SI. Ce plan doit comprendre une partie organisationnelle qui évalue l'organisation et les procédures du SI et une partie technique qui doit évaluer la sécurité de l'architecture générale, des systèmes et des applications, y compris pour sensibiliser la direction sur les risques d'une compromission. Pour répondre à ces différents objectifs, vous devez proposer des types d'audit, leur démarche, des exemples de points de contrôle et de résultats qui pourraient être observés.
- **rédiger un rapport d'audit** qui décrit la méthodologie et les outils utilisés pour réaliser le test d'intrusion, présenter chaque vulnérabilité et évaluer son impact, et proposer une solution par type de vulnérabilité pour la corriger.

4.3 Livrables

4.3.1 Fichiers

Dans un dossier nommé “Audit-securite-NOM1-NOM2”, vous mettrez à disposition du jury :

- Un fichier PDF nommé "plan-audit.pdf" d'environ 5 pages détaillant le plan d'audit composé de :
  - Une introduction présentant le contexte et les objectifs du plan d'audit
  - Une liste d'audits que vous préconisez en détaillant le type d'audit, la démarche, les points de contrôle et les résultats possibles
- Un fichier PDF nommé "rapport-intrusion.pdf" d'environ 5 pages détaillant le rapport du test d'intrusion composé de :
  - Le périmètre du test d'intrusion, la méthodologie et les outils utilisés
  - La liste des vulnérabilités trouvées en précisant le type de vulnérabilité, son impact, le scénario d'attaque détaillé et la préconisation pour la corriger

4.3.2 Soutenance

Pendant 15 minutes, vous présenterez au jury la méthodologie pour rédiger le plan d'audit et le test d'intrusion et vous justifierez les choix que vous avez fait. Cette présentation sera suivie de 10 minutes de questions-réponses.

4.4 Compétences à valider

Les compétences à valider sont ici :

- conduire des tests d'intrusion
- maîtriser les types de menaces

4.5 Cours associés

On pourra utiliser les cours suivants :

- Planifier une politique d'audité [16]
- Conduire un test d'intrusion [17]

5 Projet GS13 : Gérer les risques SSI d'une organisation

5.1 Scénario

La société « InnovArt » est un cabinet de design de produits. Cette PME bordelaise est constituée d'une vingtaine de personnes. Elle réalise des plans de conception de produits et des maquettes virtuelles pour ses clients. La société est composée d'une direction générale, d'un service commercial qui communique avec les clients, d'un bureau d'étude qui rédige les documents techniques, d'un service de comptabilité qui s'occupe de la facturation et des finances et d'un service informatique qui administre le système informatique.
Le système informatique est composé d'un réseau wifi et d'un réseau Ethernet. Le bureau d'étude possède 10 ordinateurs fixes et utilise un logiciel professionnel de conception par informatique, le service commercial 3 ordinateurs portables et le service comptabilité 1 ordinateur fixe. Le service informatique possède un serveur connecté au réseau sur lequel sont stockés les fichiers partagés entre les employés avec un dossier par service. Chaque employé utilise un compte administrateur sur son ordinateur et un mot de passe wifi est partagé par tous les employés. Le service informatique effectue une sauvegarde du serveur une fois par semaine sur une clé USB stockée dans un coffre sécurisé à côté du serveur. Le site internet et le serveur email sont hébergés chez un prestataire externe.
Dans un contexte de développement de la société, vous êtes embauché en tant que RSSI afin d'**améliorer la sécurité** du système informatique et de **se mettre en conformité** avec la nouvelle réglementation RGPD. Le directeur de la société vous demande de procéder à l'**analyse des risques** informatiques de la société et d'**élaborer une politique de sécurité des systèmes**. Pour cela, vous devrez vous appuyer sur le scénario présenté, sur la réglementation RGPD et sur des hypothèses que vous justifierez rapidement dans les documents.

5.2 Instructions

Vous devrez donc :

- rédiger un document d'analyse des risques de sécurité SI composé :
  - d'une introduction décrivant le cadre de l'entreprise étudiée
  - d'une liste de 10 fiches de risques identifiés détaillant pour chaque risque le scénario d'attaque, les sources et acteurs impliqués, l'impact sur le SI et la vraisemblance du risque. Les risques devront être hiérarchisé dans l'ordre d'importance
- rédiger une politique de sécurité SI sous la forme d'un plan d'actions contenant une liste de mesures de sécurité en détaillant quels risques sont réduits par cette mesure, quelle est la difficulté à mettre en œuvre la mesure et quels biens sont concernés. Proposez également pour au moins un risque de ne pas mettre en place de mesure de sécurité en justifiant votre choix

5.3 Livrables

5.3.1 Fichiers

Dans un dossier nommé “Gestion-Risques-NOM1-NOM2”, vous mettrez à disposition du jury :

- un fichier PDF nommé "analyse-risques.pdf" d’environ 12 pages détaillant l’analyse des risques
- un fichier PDF nommé "plan-action.pdf" d’environ 5 pages détaillant le plan d’action proposé

5.3.2 Soutenance

Pendant 15 minutes, vous présenterez au jury la méthode que vous avez suivie pour réaliser l’analyse des risques et les choix de mesures de sécurité. Cette présentation sera suivie de 10 minutes de questions-réponses.

5.4 Compétences à valider

Les compétences à valider concernent la gouvernance SSI à savoir :

- gérer les risques
- définir et décliner la PSSI
- se conformer aux obligations légales lors de la mise en place d’une stratégie
- inclure la sécurité dans les projets

5.5 Cours associés

On pourra s’appuyer sur les cours en ligne suivants :

- Analysez et gérez les risques SI [18]
- Définissez la politique de sécurité de votre entreprise [19]
- Gérez un projet digital avec une méthodologie en cascade [20]
- Initiez vous à la gestion de projet agile [21]
- Maîtrisez les risques juridiques liés au numérique [22]
- Mettez en place un plan de continuation d’activités [23]

6 Projet GS21 : Mettre en place un système de surveillance

6.1 Scénario

La clinique privée "SantéPlus" souhaite surveiller la sécurité de son SI afin de détecter rapidement les attaques potentielles. Le SI est composé d'un serveur web et d'un serveur de base de données tous deux sous Linux, d'un firewall, d'un routeur internet, d'un switch Cisco, d'un serveur *Active Directory* et de postes de travail sous Windows. Le schéma d'architecture réseau est donné figure 2, il est téléchargeable [24] et [25] pour la version modifiable. En tant qu'ingénieur SOC (*Security Operation Center*), vous êtes chargé de proposer une architecture de surveillance du SI pour collecter et identifier les évènements de sécurité. Cette architecture sera composée des journaux sécurité, réseau, systèmes, applicatifs et d'un SIEM (*Security Information and Event Management*) qui collectera l'ensemble des évènements de sécurité. Pour chaque élément, justifiez l'objectif de la surveillance et les types d'attaques qu'elle pourra détecter.

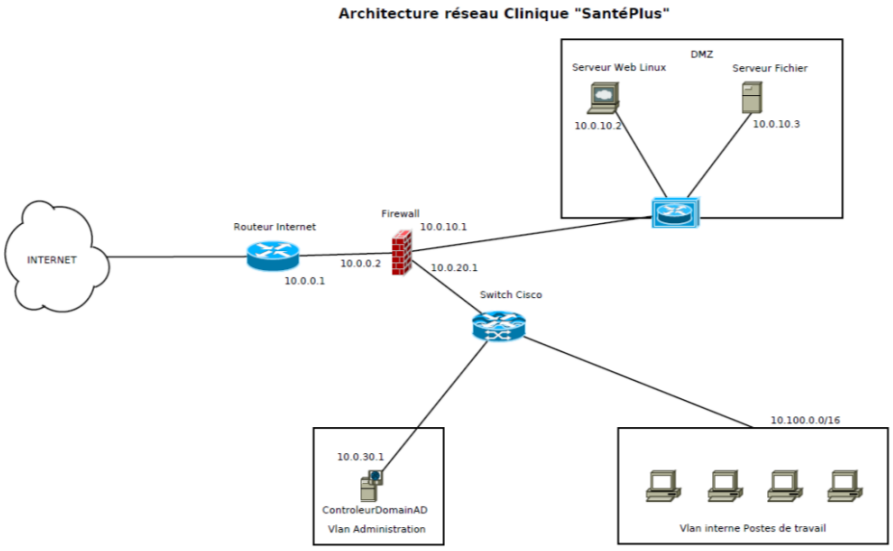

FIGURE 2 – Architecture réseau

6.2 Instructions

Vous devrez donc :

- modifier le schéma d'architecture SI et réseau pour y intégrer les services de surveillance de la sécurité et les flux d'informations entre eux
- proposer les éléments de configuration du switch Cisco pour transmettre à un serveur centralisé en Syslog les journaux relatifs aux authentifications, aux commandes passées et aux nouveaux systèmes identifiés sur le réseau

- proposer une configuration audit sous Linux pour journaliser les appels systèmes et Syslog pour transmettre les journaux de manière chiffrée vers un serveur centralisé
- proposer une configuration de la journalisation Windows, de l'envoi des journaux par WinRM et une configuration du service Sysmon
- proposer une adaptation de la configuration NfTables pour journaliser le trafic réseau et une configuration Syslog pour en transmettre les informations au serveur centralisé
- donner pour chaque catégorie de système (Linux, Windows, switch, pare-feu) un ou plusieurs exemples de scénarios de corrélation en décrivant l'attaque qui vise à être identifiée et en explicitant le détail des éléments de journalisation qui permettent de fournir les données source et la manière dont elles seraient corrélées.

6.3 Livrables

6.3.1 Fichiers

Dans un dossier nommé "Surveillance-securite-NOM1-NOM2", vous mettrez à disposition du jury :

- un fichier PDF nommé "architecture-surveillance.pdf" contenant le schéma d'architecture du SI
- un fichier texte nommé "configuration-journalisation-switch.txt" contenant les éléments de configuration du switch
- un fichier "configuration-journalisation-Linux.tgz" contenant les configurations Syslog et auditd
- un fichier "configuration-journalisation-Windows.pdf" contenant les extraits de GPO relatifs à la journalisation et les captures d'écran et les explications de la configuration WinRM
- un fichier "configuration-journalisation-Windows-Sysmon.xml" contenant la configuration du service Sysmon
- un fichier "configuration-journalisation-firewall.tgz" contenant la configuration NfTables et Syslog du pare-feu
- un fichier PDF nommé "scenarios-correlation.pdf" proposant 5 scénarios de corrélation détaillant l'attaque à identifier, les données sources à analyser et la manière dont elles seraient corrélées

6.3.2 Soutenance

Pendant 15 minutes, vous présenterez au jury l'architecture de surveillance proposée en justifiant les objectifs recherchés et les choix que vous avez faits. Cette présentation sera suivie de 10 minutes de questions-réponses.

6.4 Compétences à valider

Les compétences à valider sont ici relatives à la mise en place d'un système de détection, à savoir :

- surveiller le SI et détecter les intrusions
- sécuriser les architectures web
- sécuriser les nouvelles architectures

6.5 Cours associés

On pourra utiliser les cours en ligne suivants :

- Surveillez la sécurité des systèmes et des fichiers [26]
- Détectez les incidents de sécurité [27]

7 Projet GS21 : Investigation post-incident

7.1 Scénario

La société "Imarket" est une société de vente en ligne. L'équipe de Help-desk reçoit un appel d'un utilisateur interne expliquant qu'après avoir ouvert une pièce jointe d'un mail, son poste de travail est lent et instable. Le Help-desk a prévenu le RSSI en indiquant des doutes sur le caractère malveillant de la pièce jointe. Le RSSI de la société demande à un prestataire en traitement d'incident de réaliser un relevé de traces. En tant qu'analyste forensics, vous recevez des copies de la mémoire vive et du disque dur de la machine infectée réalisés avec FTK Imager immédiatement après l'incident [28].
Analysez ces éléments pour évaluer la nature de l'incident et son mode opératoire. Dans un rapport d'analyse, vous devez

- expliquer l'attaque et son potentiel impact,
- proposer des actions complémentaires d'investigation sur le reste du SI,
- donner des préconisations pour sa remédiation et éviter qu'une attaque similaire se reproduise.

7.2 Instructions

a) Décrivez l'analyse réalisée :

- sur l'image mémoire avec Volatility [29]. En particulier, déterminez le système d'exploitation de la machine, listez les processus en cours, leur hiérarchie, les fichiers ouverts, les utilisateurs, les commandes exécutées...
- sur la copie disque dur avec FTK Image [30]. En particulier, retrouvez le ou les fichiers malveillants, détectez les fichiers créés ou modifiés lors de l'incident, déterminez comment le virus est arrivé sur la machine, trouvez des informations sur l'origine et l'auteur de l'attaque...
- sur le PDF infecté avec les pdf tools, pdf parser [31].

b) Exécutez le logiciel malveillant dans une machine virtuelle isolée et l'analyser avec un antivirus pour chercher une correspondance de signature.
c) Rédigez votre rapport d'analyse de l'attaque et de recommandations. Donnez un exemple d'IOC permettant de rechercher si d'autres postes sont concernés.
d) Donnez un exemple d'IOC permettant de rechercher si d'autres postes sont concernés. Proposez des actions pour éviter qu'un incident similaire se reproduise.

7.3 Livrables

7.3.1 Fichiers

Dans un dossier nommé “Reponse-incident-NOM1-NOM2”, vous mettrez à disposition du jury :

- un fichier PDF nommé "methode-analyse.pdf" détaillant l'utilisation des outils d'analyse et les résultats obtenus

- un fichier PDF nommé "rapport-incident.pdf" contenant :
  - une synthèse de l'attaque observée et son impact sur le SI
  - une proposition d'actions complémentaires d'investigation
  - des recommandations pour supprimer les composants malveillants et se prémunir d'une future attaque similaire
- un ou plusieurs fichiers IOC nommé malware.IOC contenant une description des caractéristiques du malware permettant la recherche d'une compromission d'autres systèmes.

7.3.2 Soutenance

Pendant 15 minutes, vous présenterez au jury la méthodologie que vous avez appliquée pour analyser l'incident en expliquant les outils utilisés et les éléments saillants du rapport d'analyse. Cette présentation sera suivie de 10 minutes de questions-réponses.

7.4 Compétences à valider

Les compétences à valider sont ici relatives à la gestion des incidents à savoir :

- organiser un processus de traitement et de gestion des incidents
- mettre en oeuvre le processus forensic
- analyser la menace

7.5 Cours associés

On pourra s'aider des cours en ligne suivants :

- Menez une investigation d'incident (forensic) [32]

Références

[1] Virtualbox. Chapter1 : First steps. https://www.virtualbox.org/manual/ch01.html, 2019.

[2] Virtualbox. Chapter 6 : Virtual networking. https://www.virtualbox.org/manual/ch06.html, 2019.

[3] Virtualbox. Download virtualbox. https://www.virtualbox.org/Downloads, 2019.

[4] Ubuntu. Downloads. https://www.ubuntu.com/#download, 2019.

[5] Microsoft. Download windows server 2016. https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2016, 2019.

[6] Microsoft. Download virtual machines. https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/, 2019.

[7] Cisco Networking Academy. Packet tracer. https://www.netacad.com/, 2019.

[8] OpenClassrooms. Reprenez le contrôle à l'aide de linux. https://openclassrooms.com/fr/courses/43538-reprenez-le-controle-a-laide-de-linux, 2019.

[9] OpenClassrooms. Simulez des architectures réseau avec gns3. https://openclassrooms.com/fr/courses/2581701-simulez-des-architectures-reseaux-avec-gns3, 2019.

[10] OpenClassrooms. Centralisez et sécurisez votre annuaire active directory. https://openclassrooms.com/fr/courses/2222496-centralisez-et-securuisez-votre-annuaire-active-directory, 2019.

[11] OpenClassrooms. Projet 4 : analyse de code. https://s3-eu-west-1.amazonaws.com/static.oc-static.com/prod/courses/files/parcours_Responsable+en+securite+des+SI/Projets+_+Documents+a+integrer/Projet+4_application.pdf, 2019.

[12] OpenClassrooms. Sécurisez vos applications. https://openclassrooms.com/fr/courses/1761931-securisez-vos-applications, 2019.

[13] OpenClassrooms. Sécurisez vos infrastructures. https://openclassrooms.com/fr/courses/1761876-securisez-vos-infrastructures, 2019.

[14] OpenClassrooms. Sécurisez vos données avec la cryptographie. https://openclassrooms.com/fr/courses/1757741-securisez-vos-donnees-avec-la-cryptographie, 2019.

[15] OpenClassrooms. Projet 5 : Application web pour test d'intrusion. https://static.oc-static.com/prod/courses/files/parcours_Responsable+en+securite+des+SI/Projets+_+Documents+a+integrer/Projet+5_DVWA.zip, 2019.

[16] OpenClassrooms. Planifiez une politique d'audit. https://openclassrooms.com/fr/courses/1756306-planifiez-une-politique-daudit-au-sein-de-votre-entreprise, 2019.

[17] OpenClassrooms. Construisez un test d'intrusion. https://openclassrooms.com/fr/courses/1756296-construisez-un-test-dintrusion, 2019.

[18] OpenClassrooms. Analysez et gérer des risques si. https://openclassrooms.com/fr/courses/1734211-analysez-et-gerez-des-risques-si, 2019.

[19] OpenClassrooms. Définissez la politique de sécurité de votre entreprise, 2019.

[20] OpenClassrooms. Gérez un projet digital avec une méthodologie en cascade. https://openclassrooms.com/fr/courses/4296701-gerez-un-projet-digital-avec-une-methodologie-en-cascade, 2019.

[21] OpenClassrooms. Initiez vous à la gestion de projet agile. https://openclassrooms.com/fr/courses/4507926-initiez-vous-a-la-gestion-de-projet-agile, 2019.

[22] OpenClassrooms. Maîtrisez les risques juridiques liés au numérique. https://openclassrooms.com/fr/courses/5162341-maitrisez-les-risques-juridiques-lies-au-numerique, 2019.

[23] OpenClassrooms. Mettez en place un pca. https://openclassrooms.com/fr/courses/6227526-mettez-en-place-un-plan-de-continuite-dactivite-pca, 2019.

[24] OpenClassrooms. Projet 6 : Schéma d'architecture. https://static.oc-static.com/prod/courses/files/parcours_Responsable+en+securite+des+SI/Projets+_+Documents+a+integrer/Projet+6_Reseau.pdf, 2019.

[25] OpenClassrooms. Projet 6 : Schéma d'architecture à modifier. https://static.oc-static.com/prod/courses/files/parcours_Responsable+en+securite+des+SI/Projets+_+Documents+a+integrer/Projet+6_Reseau.dia, 2019.

[26] OpenClassrooms. Surveillez la sécurité des systèmes et des fichiers, 2019.

[27] OpenClassrooms. Détectez les incidents de sécurité, 2019.

[28] OpenClassrooms. Projet 7 : Relevés de traces. https://s3-eu-west-1.amazonaws.com/course.oc-static.com/projects/AIC_P7_SupervisezSIEntreprise/AIC_P7_documents.zip, 2019.

[29] Volatility Foundation. Releases. https://www.volatilityfoundation.org/releases, 2019.

[30] AccessData. Product downloads. https://accessdata.com/product-download/ftk-imager-version-4.2.0, 2019.

[31] Didier Stevens. Pdf tools. https://blog.didierstevens.com/programs/pdf-tools/, 2019.

[32] OpenClassrooms. Menez une investigation sur incident. https://openclassrooms.com/fr/courses/1750151-menez-une-investigation-dincident-forensic, 2019.