# **« Formation Simplon »**

# **Projet Chef-Œuvre**

Surveillance et analyse d’incidents de cybersécurité

**Mise en situation et contexte :**

Vous êtes analyste de cybersécurité dans une Entreprise. Vous êtes chargé de réaliser la surveillance et l’analyse d’incidents de cybersécurité.

Dans cette perspective, vous devez mener votre démarche d’une façon systématique en plusieurs étapes, organisées en 10 jours.

* Etape 1 / jour 1 : prise en main de votre environnement
* Etape 2 / jour 1 : élaboration du dessin d’architecture
* Etape 3 / jour 1 : réaliser une analyse des risques selon un modèle simple
* Etape 4 / jour 2 : vérification de la stratégie de collecte des logs
* Etape 5 / jours 3, 4 et 5 : réalisation d’un pentest
* Etape 6 / jour 6 : détection des tentatives de pentests et de compromission
* Etape 7 / jours 7 et 8 : investigation et analyse des logs
* Etape 8 / jour 9 : analyse des IOC et Hunting
* Etape 9 / jour 10 : rédaction du rapport chef d’oeuvre

**Démarche**

Il est important de respecter la démarche quotidienne pour avancer dans son chef d’œuvre, notamment :

1/ en prenant connaissance chaque jour de l’objectif de la journée, des travaux à mener et des résultats attendus

2/ Au fur et à mesure des travaux réalisés dans la journée, prendre des notes, des copies d’écran, des preuves, etc. pour pouvoir réaliser le rapport de fin de journée. La présente template vous donne des indications mais vous pouvez la compléter selon vos résultats.

Ces notes quotidiennes vont vous servir également à les consolider le dernier jour pour faire un rapport complet.

3/ réserver en fin de journée, le temps nécessaire pour le rapport de la journée. Ce rapport de fin de journée va vous permettre d’élaborer votre rapport de Chef d’œuvre en fin du parcours.

4/En plus du rapport détaillé de chef d’œuvre, vous avez une présentation à préparer avec les requis suivants :

a/ dans la présentation, il ne faut pas traiter de l’ensemble des sujets abordés dans le chef d’œuvre, mais plutôt faire le focus sur une thématique/sujet

b/ la présentation doit comprendre

* Une introduction (slide) présentant l’intérêt du thème choisi (le pourquoi)
* La démarche et les techniques adoptées
* Les résultats
* Tout autre élément complémentaire vous semble intéressant à présenter

|  |  |
| --- | --- |
|  | A completer |
| Nom & prénom |  |

|  |  |
| --- | --- |
|  | A compléter  Étape 1 – jour 1 : prise en main de votre environnement |
| Etape 1 – jour 1 : prise en main de votre environnement | **Objectifs :**  1/ Bien connaître l’environnement de travail pour pouvoir mener les travaux prévus dans le projet chef d’œuvre  2/ prise en main technique de chaque équipement  **Démarche :**  1/ Etape 1 : avoir la liste des équipements en place et leurs fonctions  2/ Etape 2 : se connecter sur chaque équipement (  3 Etape 3 : réaliser les vérifications nécessaires du bon fonctionnement  4/ Etape 4 : vérifier l’accessibilité/connectivité entre les équipements (VPN wireguard)  Informations nécessaires (user/mdp, adresse ip, outil recommandé pour la connexion, etc.).  Equipements :  Une VM Kali (mais de préférence travailler sur votre Kali en utilisant le VPN)  Une VM Selks  Une VM MISP  Une VM Metasploitable  Une VM Windows 10 1  Une VM Windows 10 2  Etc.  **Quelques ressources :**  Un document avec les informations sur les équipements est en pièce jointe avec l’ensemble des informations  Un document exhaustif vous sera présenté le premier jour listant l’intégralité des machines, credentials et ce que vous devez savoir pour être  **Résultats Attendus**  1/ connexion sur chaque équipement  2/ vérification de l’accessibilité et connectivité entre les équipements (ex : être sûr que l’équipement de pentesting accède aux différentes targets)  3/ bon fonctionnement de chaque équipement (les applications sont opérationnelles)  4/ prise des preuves à chaque étapes pour la documentation de l’environnement |

|  |  |
| --- | --- |
|  | A compléter / To be completed  Etape 2 – jour 1 : maîtrise de l’architecture de votre système d’information en dessinant l’architecture |
| Etape 2 – jour 1 : maîtrise de l’architecture de votre système d’information en dessinant l’architecture | **Objectifs :**  1/ savoir élaborer, sous forme de dessin, une architecture d’un système d’information  2/ et comprendre l’ensemble de l’architecture  3/ collecte des informations relatives à l’architecture  **Démarche :**  Etape 1 : Définir et dessiner avec un outil approprié (ex : draw.io) une architecture réseau sécurisé comprenant à minima :   * Une connexion à internet (avec votre poste comme client sur Internet) * les sous réseau contenant les équipements   Etape 2 : identifier sur le schéma le rôle ou la fonction de chaque équipement  Etape 3 : mettre les informations indispensables ou intéressantes sur le dessin de chaque équipement  Etape 4 : en annexe (sans les mettre sur le schéma), identifier les flux importants entre les équipements et quels sont les flux à autoriser en entrée.  Etape 5 : identifier les points (ou équipements) où il aura la collecte des logs et des détections d’événements de sécurité  Pour la collecte des informations, recommandation : utiliser des utilitaires du type namp (donner juste à titre indicatif)  Etape 1 : découverte des adresses IP des machines connectés  Indication  root@kali:~# nmap -sP xxx.xxx.xxx.0/24  Etape 2 : découvertes des services réseaux ouverts en découvrant les ports ouverts (TCP et UDP)  Indication  root@kali:~# nmap -sS xxx.xxx.xxx.xxx  root@kali:~# nmap -sU xxx.xxx.xxx.xxx  Etape 3 : compléter la collecte des informations avec les services et les versions  Indication  root@kali:~# nmap -sV -p 22 xxx.xxx.xxx.xxx  Etape 4 : idem par l’OS  root@kali:~# nmap -O xxx.xxx.xxx.xxx  Vous pouvez reprendre vos cours et notes en tout genre sur les déroulés de pentest que l’on a pu faire. Des TIPS vous seront fournis sur les tableaux  **Quelques ressources :**  [www.draw.io](http://www.draw.io) (ou équivalent pour le dessin de l’architecture)  mode d’emploi de nmap  https://nmap.org/man/fr/man-briefoptions.html  **Résultats Attendus**  1/ Schéma d’architecture (avec l’ensemble des informations des étapes 1 à 4)  2/la liste des flux  3/ les informations collectées |

|  |  |
| --- | --- |
|  | A compléter / To be completed  Etape 3 – jour 1 : réaliser une analyse des risques selon un modèle simple |
| Etape 3 – jour 1 : réaliser une analyse des risques selon un modèle simple | **Objectifs :**  1/ réaliser une analyse des risques  2/ proposer des mesures de protection pour réduire les risques à un niveau acceptable  **Démarche :**  En utilisant le formulaire Excel en annexe, compléter les étapes suivants :  Etape 1 : Identifier les équipements et les services proposés par la plate-forme, notamment le serveur web, un poste de travail windows et un serveur Windows. (Les autres équipements sont des outils techniques de protection qui doivent être utilisés dans la partie « mesures de protection »)  Etape 2 : Pour chaque équipement et service, identifier les événements redoutés (ou scénario)  Etape 3 : pour chaque événement redouté, préciser quel critère de cybersécurité DICP (Disponibilité, Intégrité, Confidentialité, Preuve) est impacté (il peut y avoir plusieurs critères impactés à la fois)  Etape 4 : Dans chacun des impacts identifiés, préciser si le type d’impact possible (financier, juridique, image de marque, etc.)  Etape 5 : proposer un niveau d’impact de 1 (faible) à 4 (vital)  Etape 6 : selon chaque scénario, évaluer une vraisemblance du scénario et calculer le niveau de risque  Etape 7 : proposer des mesures pour réduire le niveau de risque de chaque scénario, avec deux types de mesures :   * des équipements de sécurité (déjà en place dans l’infrastructure ou bien de nouvelles propositions) * des contrôles à mettre en place sous forme :   + de scans de vulnérabilités et pentests   + vérification de durcissement   Etape 8 : recalculer le niveau de risque une fois les mesures de sécurité mises en place (risque résiduel)  **Quelques ressources :**  Formulaire Excel « Analyse des risques simplifiés »  Plan de vérification de durcissement pour Windows  **Résultats Attendus**  Formulaire Excel « Analyse des risques simplifiés » complété  Identification des équipements et services à pentester et à analyser par la suite (Targets)  Identifications des équipements et services à durcir |

|  |  |
| --- | --- |
|  | A compléter  Etape 4 - jour 2 : vérification de la stratégie de collecte des logs |
| Etape 4 - jour 2 : vérification de la stratégie de collecte des logs | **Objectifs :**  1/ Vérifier les logs, journaux, alertes et les traces collectés sur chacun des équipements concernés.  2/ s’assurer que les collectes sont opérationnelles pour que lors des attaques des relevées soient effectués  3/ maîtriser les investigations des logs Windows et linux  Liste des équipements (à compléter d’une façon précise)   * IDS * Serveurs Web * Postes de travail et serveurs Windows   4/ Une machine est dédié (Serveur Web) à cet activité avec l’IDS  **Démarche :**  Etape 1 : sur chacun des équipements, identifier les logs, journaux, alertes et les traces collectés  Etape 2 : effectuer des revues et des recherches sur chacun des logs, journaux, alertes, etc.  Etape 3 : compléter / configurer d’autres logs ou outils si nécessaire  Pour windows 10, en utilisant Event viewer (observateurs des événements)  Visualisation des événements collectés.  Quelles sont les catégories des événements (ex : application, système, etc.)  Quelles sont les champs permettant de parcourir les événements  (ex : niveau, date, etc.)  Comment faire une recherche sur les événements (création d’une vue personnalisée)   * Entre deux dates * Niveau : critique (par exemple) * Mot clé (choix dans la liste)   Comment faire une recherche basique (fonction recherche)  Pour windows 10, en utilisant Powershell  Manipulation des logs avec PowerShell (commande : Get-WinEvent)  Importance : recherche d’un IOC (dans les événements sur un ensemble de machine)  Exemple en Powershell  PS P:\> Get-WinEvent -FilterHashtable @{LogName='System'} | Where-Object -Property Message -Match 'S-1-5-18'  Vérification de la configuration des logs  Commande : gpedit.msc  Le chemin : Windows Setting\Security Settings\Local Policies\ Security Options.  Vérification et Analyse des Log : Linux  Découvrir les logs dans le répertoire cd/var/log,  Quelles sont les logs disponibles (ex : >ls –lrt /var/log)  Pour voir en temps réel les derniers événements  tail -f /var/log/syslog  Décriver le format des logs  Vérifier la configuration des logs dans /etc/syslog.conf ou /etc/rsyslog.conf, |

|  |  |
| --- | --- |
|  | **Quelques ressources :**  1/ Documentation IDS  2/ Documentation serveurs Web  3/ Documentation postes de travail et serveurs Windows 10  **Résultats Attendus**  Rapport du jour avec les logs, journaux identifiés, les procédures pour y accéder, et les procédures pour les analyser (avec les copies d’écran)  Détailler les procédures et commandes de recherche sur les logs Windows 10 et Linux |

|  |  |
| --- | --- |
|  | A compléter  Etape 5 - jours 3, 4, et 5 : réalisation d’un campagne de pentest |
| Etape 5 - jour 3, 4 et 5 : réalisation d’une campagne de pentests | **Objectifs (savoir attaquer pour mieux se défendre) :**  1/ réaliser  un pentest sur les machines prévues à cet effet  2/ identifier et analyser les vulnérabilités des équipements et services cibles  3/ proposer des remédiations  **Démarche :**  **N.B : s’assurer pendant les pentests que les targets collectent bien les logs et les traces.**  Etape 1 : Points d’attention :  configuration des targets les systèmes windows et le site web Metaexploitable  configuration des formats des rapports (exemple : en PDF)  Etape 2 : lancer la campagne de pentest  Etape 3 : analyser les résultats dans les deux cas   * Par sévérité et complexité * Par CVE * Par Ports présentant des vulnérabilités * Quels sont, à priori, les 4 ou 5 vulnérabilités qu’il serait intéressant d’exploiter dans une phase de pentesting * Savoir utiliser des filtres du type : severity>8;Complexity=LOW pour faire des recherches sur les vulnérabilités   Etape 4 : Exporter les rapports aux bons formats.  Etape 5 : Utilisation les autres outils Kali ou d’autres outils complémentaires pour réaliser du pentesting  Etape 6: établisser le rapport de pentests avec les findings  Etape 7 : proposer des remédiations, en distinguant les mesures   * De configuration, durcissement et paramétrage * De nouvelles solutions techniques (ex : équipement WAF) |

|  |  |
| --- | --- |
|  | **Quelques ressources :**  Outillage  Quelques outils de pentests proposés (l’étudiant peut en adopter d’autres) : Kali, OpenVas, etc.  Documentation  Document général sur la démarche de pentests  Documentation des outils utilisés (Kali, OpenVas, …)  N’hésitez pas à utiliser les ressources sur Internet.  **Résultats Attendus :**  Rapport détaillé des scans de vulnérabilités et des pentests, incluant  :   * Chaque vulnérabilité fera l’objet d’un traitement de calcul de score CVSS 3.0 si cela vous semble réalisable. * Les recommandations pour remédier aux vulnérabilités * Attention : choisir les outils qui fournissent un maximum d’information * Pour la partie pentests : * Les vulnérabilités « pentestées » * Les procédures / tentatives d’exploitation suivies * Les preuves collectées (copies d'écran) * Les captures d’écrans et les éléments présents dans le rapport doivent être sans appel, ils doivent prouver la compromission soyez efficient.   Rapport de plan d’action de remédiation |

|  |  |
| --- | --- |
|  | A compléter / To be completed  Etape 6 : jour 6 : détection des tentatives de pentests et de compromission  Premier cas : au niveau des équipements et Linux |
| Etape 6 : jour 6 : Détection des tentatives de pentests et de compromission | **Objectifs :**  1/ analyser les logs, journaux, alertes et traces des scans de vulnérabilités et des pentests pour détecter des indicateurs de compromission  2/ A la suite du pentest des Findings et autres artefacts auront était découvert,ils doivent être agglomerés et traité en qualification OSINT dans un premier temps  **Démarche :**  Etape 1 : sur chacun des équipements concernés (windows et Linux) se connecter au logs, journaux et alertes et identifier et analyser les traces précises des tentatives de scans de vulnérabilités et des pentests, et des signes de compromission  Exemples Windows :  Pour Détection d’une DLL dont l’intégrité a été compromise  1/Utilisation de la commmande DOS, sfc en se mettant dans le bon dans le bon répertoire PS C:\WINDOWS\system32>sfc /VERIFYONLY  2/Utilisation de powershell avec la commande Get-AuthenticodeSignature  Get-AuthenticodeSignature -FilePath C:\Windows\System32\\*  3/ Pour Trouver un fichier particulier contenant des caractéristiques particulières (get-ChildItem et select-string)  Par exemple : fichier Chiffré, fichier Compressé, fichier contenant un pattern  Exemples Linux  Vérification d’intégrité sous Linux (en utilisant les packages linux)  Trouver un fichier particulier contenant des caractéristiques spécifiques  Soit en utilisant : Graphical file manager to find files in Linux, such as Nautilus in Gnome, Dolphin in KDE, etc.  Soit en utilisant les recherches avec les commandes find et grep  find . -type f -name "\*.java" -exec grep -il 'foo' {} \;  **Quelques ressources :**  Ressources concernant powershell  Ressources concernant les commandes linux find et grep  **Résultats Attendus :**  Rapport du jour avec les logs, journaux identifiés, les procédures pour y accéder, et les procédures pour les analyser (avec les copies d’écran) avec, à cette étape, les traces de compromission, d’attaques, et des scan |

|  |  |
| --- | --- |
|  | A compléter / To be completed  Etape 7 - jours 7 et 8 : investigation et analyse des logs  Deuxième cas : au niveau de l’équipement IDS/IPS (SELKS) |
| Etape 7 - jours 7 et 8 : Investigation et analyse des logs de | **Objectifs :**  1/ comprendre l’ensemble des fonctionnalités d’un IDS/IPS  2/ configurer les paramètres de fonctionnement et de détection des alertes  3/ analyser les logs et les alertes remontées  4/ Création d’une règle de filtre issue du pentest pour faire une nouvelle remontée d’alerte  **Démarche :**  Etape 1 : comprendre chaque composante  Lister les composants majeurs de Selks et donner une description rapide de chaque composante  S - Suricata IDPS  E - Elasticsearch  L - Logstash  K - Kibana  S - Scirius  EveBox  Configuration en FPC Retain avec Moloch  Etape 2 : configuration et analyse des résultats (logs et alertes)  Pratique de chaque composante  **Quelques ressources :**  http://suricata-ids.org/  https://www.elastic.co/products/elasticsearch  https://www.elastic.co/products/logstash  https://www.elastic.co/products/kibana  https://github.com/StamusNetworks/scirius  https://evebox.org/  **Résultats Attendus :**  **Réalisation une nouvelle règle de filtre, mise en place et test (présent à la MSP)**  Rapport sur les configurations et les paramétrages  Rapport sur les analyses et les logs et alertes remontés |

|  |  |
| --- | --- |
|  | A compléter / To be completed  Etape 8 - jour 9 : analyse des IOC et Hunting  Troisième cas : les IOC (MISP) |
| Etape 8 - jour 9 : analyse des IOC et Hunting | **Objectifs :**  1/ A la suite des artefacts collectés on effectura un comparaison sur diverses qualification en OSINT  2/ Si certains des ces artefacts sont connus comme IoC, on effectura une comparaison sous MISP  **Démarche :**  Etape 1 :  Lister vos artefacts  Selon les différents critères : le niveau de risques, la catégorie, etc.  **Quelques ressources :**  MISP : User guide a threat sharing plateform (livre en pdf MISP)  **Résultats Attendus :**  Rapport du jour avec les IOC identifiés, les procédures pour y accéder, et les procédures pour les analyser (avec les copies d’écran). |

|  |  |
| --- | --- |
|  | A compléter / To be completed  Etape 9 – jour 10 : rédaction du rapport chef d’oeuvre |
| Etape 9 – jour 10 : rédaction du rapport chef d’oeuvre | **Objectifs :**  1/ rédiger le rapport détaillé du projet chef d’œuvre  2/ rédiger la présentation du thème choisi  Dans la présentation du thème choisi, il ne faut pas traiter de l’ensemble des sujets abordés dans le chef d’œuvre, mais plutôt faire le focus sur une thématique/sujet  **Démarche :**  Etape 1 : consolider l’ensemble des rapports quotidiens en un seul rapport.  Il ne suffit d'ajouter pas les rapports les uns aux autres mais également de faire le lien entre les différentes parties.  Etape 2 : choisir un thème pour la présentation  Etape 3 : rédiger la présentation du thème choisi comprenant   * Une table des matières reprenant les Jours et déroulé de cette période de 10jours. Une introduction (slide) présentant l’intérêt du thème choisi (le pourquoi) * La démarche et les techniques adoptées * Les résultats * Tout autre élément complémentaire vous semblant intéressant à présenter   **Quelques ressources :**  Néant  **Résultats Attendus :**  Rapport détaillé du projet chef d’œuvre  Présentation du thème choisi |