CONTRAT D'AUDIT DE SÉCURITÉ

Nom Prénom :

Adresse mail:

Tél :

N° SIRET:

Ci-après dénommé l'auditeur,

Et

La société All-Safe au capital de 15 252 640,00 €, ayant son siège social au 1645 Rte des Lucioles, 06410 Biot ; ci-après dénommé le client

Il a été au préalable exposé:

Article 1 : Objet

Le présent contrat et un contrat de prestation et de conseil qui a pour objet l'audit de l'entreprise Allsafe qui a pour siège social basé à New-york qui a pour directeur Gideon Goddard et un site basé à Sophia antipolis , nous nous intéresserons au site basé à Sophia ,

Mentionner le périmètre du pentesting:

- Réseaux wifi
- BYOD
- Réseaux ethernet de l'entreprise
- base de donnée
- site Web (les différents nom de domaine utiliser, BDD, etc..)

Article 2: Prix

Les prestations définies à l'article 1 ci-dessus seront facturées au client mille cinq cent euros (1500 €) hors taxe par journée pour un maximum de cinq journées.

Par ailleurs, comme vu également, un surplus raisonnable de rémunération peut être calculé en fonction d'un pourcentage assis sur des éléments quantifiables pour faire participer le prestataire au succès de l'opération. S'ils ne sont pas compris dans le prix ci-dessus, il conviendra en outre que soient prévus les frais de déplacement, séjour et autres du prestataire.

Les frais engagés par le prestataire : de déplacement, d'hébergement, de repas et frais annexes de dactylographie, reprographie etc., nécessaires à l'exécution de la prestation seront facturés en sus au client sur relevé de dépenses et joints à la facture totale.

Les modalités de paiement du prix pourront soit figurer dans la présente clause de prix, soit dans une clause autonome, qui alors, pourra détailler davantage divers éléments.

Les sommes prévues ci-dessus seront payées par chèque, cinq jours calendaires à partir de l'émission de la facture, droits et taxes en sus.

Article 3: Durée de l'intervention

L'intervention durera théoriquement qu'une seul journée , je vous ramène les termes exact à l'article 2 qui possède plus d'information à ce sujet , mais la durée théorique estimer , dépendra des informations à traiter , si cela est faisable dans la mesure du possible et que les termes de l'article 2 soit respecté entre l'auditeur et l'entreprise.

Article 4 : Définition de la prestation

Le but de la mission auras pour objectif de faire un test de pénétration sur l'entreprise Allsafe, étant une entreprise très importante dans le monde de la cybersécurité elle se doit de pouvoir être au tope des exigence en matière de cybersécurité , et de pouvoir affirmer leurs dires en terme de sécurité et de pouvoir rassurer leurs clients , Alsafe nous donne toutes les permission nécessaires pour pouvoir mener à bien notre test de pénétrations sur leur système.

Dans le cas de ce contrat d'audit , nous allons utiliser le système d'exploitation linux nommé kali -linux , il va nous permettre d'utiliser différents outils pour mener à bien nos teste de pénétration et de pouvoir avoir des donnée précise en cas de faille majeur sur le système de Allsafe,les outils seront détaillés dans la partie trois , ce système d'exploitation tournera sur un containers pour plus de sécurité et de facilité ,ce qui en fait l'atout parfait pour des test de pénétration.

Les outils utilisés lors de cet prestation seront les seuls outils disposer à son pentesteur et ils seront les suivants:

Wireshark

Wireshark est un bon outil pour pouvoir détecter les différentes attaques et organiser des attaques MTM.

Nmap

Nmap est un scanner de ports libres créé par Fyodor et distribué par Insecure.org. Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant.

Metasploit

Metasploit, Metasploit Pen Testing Tool, est un projet en relation avec la sécurité des systèmes informatiques. Son but est de fournir des informations sur les vulnérabilités de systèmes informatiques, d'aider à la pénétration et au développement de signatures pour les systèmes de détection d'intrusion

Aircrack-ng

Aircrack-ng est une suite de logiciels de surveillance des réseaux sans fil dont l'utilisation principale est de « casser » les clés WEP et WPA des réseaux WIFI. C'est en fait une « reprise » du logiciel aircrack qui a été abandonné.

Wifite

Wifite est un outil pour auditer les réseaux sans fil cryptés WEP ou WPA. Il utilise les outils aircrack-ng, pyrit, reaver, tshark pour effectuer l'audit.

Cet outil est personnalisable pour être automatisé avec seulement quelques arguments et peut être exécuté sans supervision.

Mitmproxy

mitmproxy est votre couteau suisse pour le débogage, les tests, les mesures de confidentialité et les tests de pénétration. Il peut être utilisé pour intercepter, inspecter, modifier et rejouer le trafic Web tel que HTTP/1, HTTP/2, WebSockets ou tout autre protocole protégé par SSL/TLS. Vous pouvez embellir et décoder une variété de types de messages allant de HTML à Protobuf, intercepter des messages spécifiques à la volée, les modifier avant qu'ils n'atteignent leur destination et les rejouer ultérieurement sur un client ou un serveur.

BURP

urp Suite est une application Java, développée par PortSwigger Ltd, qui peut être utilisée pour la sécurisation ou effectuer des tests de pénétration sur les applications web.

sqlmap

sqlmap est un outil de test d'intrusion open source qui automatise le processus de détection et d'exploitation des failles d'injection SQL et de prise en charge des serveurs de base de données.

hascat

Hashcat est un outil de récupération de mot de passe. Il avait une base de code propriétaire jusqu'en 2015, mais a ensuite été publié en tant que logiciel open source. Des versions sont disponibles pour Linux, OS X et Windows.

SET (social engineering toolkit)

c'est un logiciel développé par TrustedSec et écrit par David Kennedy en python. Il est open-source et multiplateforme et propose un choix de fonctions permettant diverses attaques basées sur l'hameçonnage informatique

Article 5 : Confidentialité

L'entreprise se garde le droit sur la confidentialité des donnée qui vont être manipulé par le prestataire en d'autre mot , le prestataire doit garder la plus grande discrétion sur les donnée qu'il manipule et ne doit en aucun cas , divulguer des informations privées sur l'entreprise ,de prendre des notes personnel , de prendre des photos sur un smartphone personnel , d'enregistrer des informations concernant l'entreprise, pour éviter de potentiel fuite de données.

De plus, l'entreprise se réserve le droit d'embaucher une deuxième personne pour prendre note de tous les agissements du prestataire et de vérifier absolument toutes les informations traitées et notées pour l'entreprise .

Le prestataire considèrera comme strictement confidentiel, et s'interdit de divulguer, toute information, document, donnée ou concept, dont il pourra avoir connaissance à l'occasion du présent contrat. Pour l'application de la présente clause, le prestataire répond de ses salariés comme de lui-même. Le prestataire, toutefois, ne saurait être tenu pour responsable d'aucune divulgation si les éléments divulgués étaient dans le domaine public à la date de la divulgation, ou s'il en avait connaissance, ou les obtenait de tiers par des moyens légitimes.

Article 6 : Collaboration

La prestation d'audit penteste se fera en collaboration avec l'IUT de Sophia Antipolis qui sera assisté par Pierre Penalba (Ancien chef de première brigade de lutte contre la cybercriminalité au sein de la Police Nationale française) .Le client tiendra à la disposition du prestataire toutes les informations pouvant contribuer à la bonne réalisation de l'objet du présent contrat.

Article 7 Responsabilités

Le client convient que, quels que soient les fondements de sa réclamation, et la procédure suivie pour la mettre en œuvre, la responsabilité éventuelle du prestataire à raison de l'exécution des obligations prévues au présent contrat, sera limitée à un montant n'excédant pas la somme totale effectivement payée par le client, pour les services ou tâches fournis par le prestataire.

Par ailleurs, le client renonce à rechercher la responsabilité du prestataire en cas de dommages survenus aux fichiers, ou tout document qu'il lui aurait confié. Il donne l'autorisation expresse – en tant que maître du système – au prestataire pour procéder à toutes les investigations qui sembleront nécessaires à ce dernier.

Le prestataire dégage sa responsabilité à l'égard des dommages matériels pouvant atteindre les immeubles, installations, matériels, mobiliers du client.

Le client convient que le prestataire n'encourra aucune responsabilité à raison de toute perte de bénéfices, de trouble commercial, de demandes que le client subirait; de demandes ou de réclamations formulées contre le client et émanant d'un tiers quel qu'il soit.

Le client s'engage à prévenir les responsables techniques notamment l'hébergeur, qu'un pentest aura lieu, en précisant l'IP du prestataire, la durée d'exécution de la prestation ainsi que les éléments techniques nécessaires à l'hébergeur. Il s'engage également à informer le prestataire par courrier ou par email de la bonne délivrance de cette information.

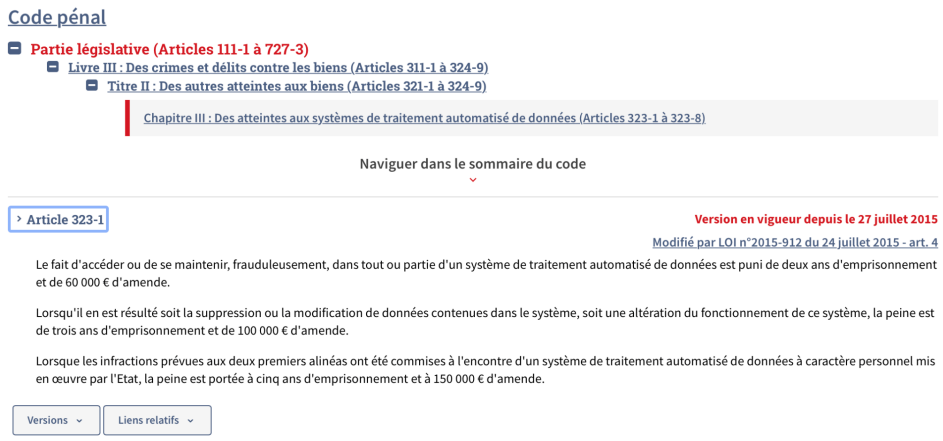
Article 8 : Référencement

Le client accepte que le prestataire puisse faire figurer parmi ses références les travaux accomplis dans le cadre du présent contrat, sans pour autant en dévoiler la nature exacte ni les résultats finaux.

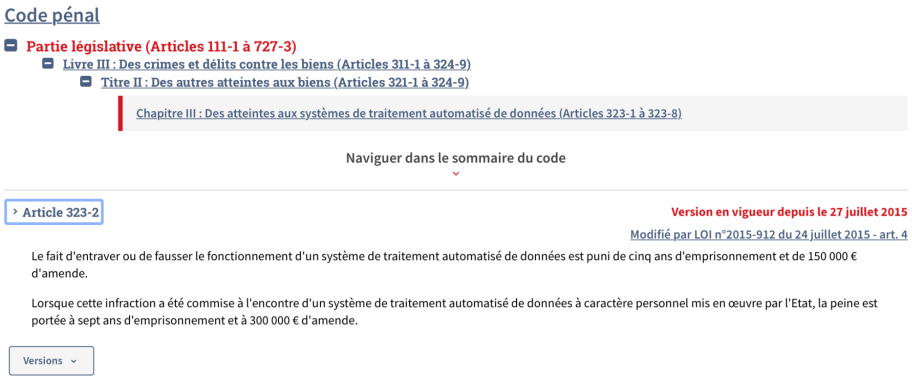
Article 9 : Pénale

Les différents articles du code pénal qui peut se retourner contre le prestataire si celui-ci décide de transgresser le contrat et ces articles s'appliquent .

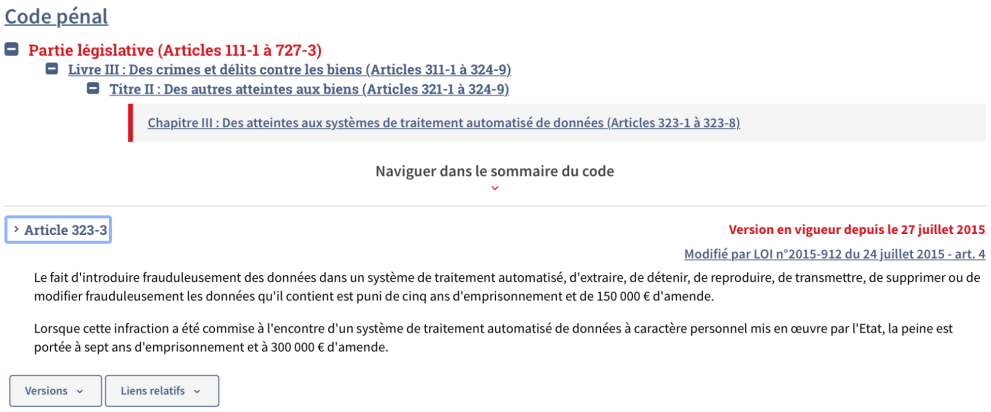
Article 323-1 du code pénale sur l'atteinte aux systèmes de traitement de données



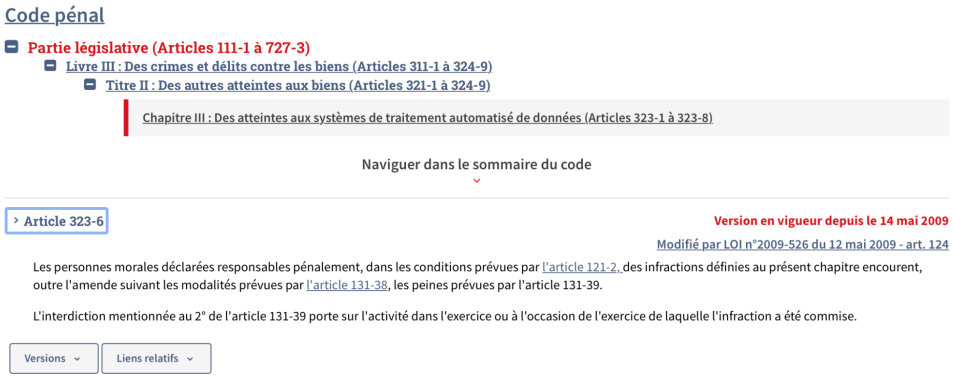
Article 323-2 du code pénal sur l'atteinte aux systèmes de traitement de données



Article 323-3 du code pénal sur l'atteinte aux systèmes de traitement de données



Article 323-6 du code pénal sur l’atteinte aux systèmes de traitement de données



Le client convient que, quels que soient les fondements de sa réclamation, et la procédure suivie pour la mettre en œuvre, la responsabilité éventuelle du prestataire à raison de l'exécution des obligations prévues au présent contrat, sera limitée à un montant n'excédant pas la somme totale effectivement payée par le client, pour les services ou tâches fournis par le prestataire.

Par ailleurs, le client renonce à rechercher la responsabilité du prestataire en cas de dommages survenus aux fichiers, ou tout document qu'il lui aurait confié. Il donne l’autorisation expresse – en tant que maître du système – au prestataire pour procéder à toutes les investigations qui sembleront nécessaires à ce dernier.

Le prestataire dégage sa responsabilité à l'égard des dommages matériels pouvant atteindre les immeubles, installations, matériels, mobiliers du client.

Le client convient que le prestataire n'encourra aucune responsabilité à raison de toute perte de bénéfices, de trouble commercial, de demandes que le client subirait; de demandes ou de réclamations formulées contre le client et émanant d'un tiers quel qu'il soit.

Le client s’engage à prévenir les responsables techniques notamment l’hébergeur, qu’un pentest aura lieu, en précisant l’IP du prestataire, la durée d’exécution de la prestation ainsi

que les éléments techniques nécessaires à l'hébergeur. Il s'engage également à informer le prestataire par courrier ou par email de la bonne délivrance de cette information.

Article 10 :Compromis

Tous compromis expliquer oralement ne seront pas pris en compte dans les termes du contrat qui a été initié à la base , tous les compromis seront donc écris et renvoyer à la société du prestataire qui en décideront par la suite avec le chargé du service informatique de l'entreprise faisant appelle au prestataire et à la personne qui a initié la demande d'audit.

Les litiges qui pourront naître entre les parties à l'occasion du présent contrat seront tranchés par un arbitre que les parties désigneront. L'arbitre nommé sera chargé de trancher le litige entre les parties. Les frais qui seront liés à son intervention seront payés par moitié par chacune des parties / par la partie qui l'a saisi / par le débiteur de l'obligation inexécutée à l'origine du litige tranché par l'arbitre.

Fait à Sophia Antipolis le 01/11/2022

signature Client **signature Auditeur**