

Hackmosphere

Votre sécurité nous tient hackeur.

-

Description des tests proposés

About Us

Notre activité

Hackmosphere fournit des services de hacking éthique pour les trois maillons de la chaîne cybersécurité : **cyber**, **physique** et **humain**.

Les services « cyber » (plus de détails dans les sections suivantes) :

- Une forme dite « sur périmètre », avec des tests d'intrusion sur des applications web & mobile, sur des infrastructures…
- Une forme dite « sur objectif », permettant d'effectuer une simulation d'attaque complète. Cette approche fournit une vision plus concrète quant à l'état de la sécurité globale de l'entreprise, puisque basée sur objectifs (ex. Devenir « domain admin »).

Les services « physiques » concernent l'accès à des données sensibles via les locaux de l'entreprise. Avec ces tests nous tentons, par exemple, de voler un fichier dans le bureau d'un membre exécutif de l'entreprise.

Les services « humains » sont effectués via des campagnes de phishing ou de formation de cybersécurité via un escape-game créé par notre équipe.

L'équipe

Florian Ecard s'est spécialisé dans la sécurité offensive après avoir obtenu son Master en 2015 dans une université prestigieuse. Il est expert pour tester les environnements Active Directory, ICS et applicatifs ainsi que pour réaliser des campagnes de phishing. Il a fondé Hackmosphere en 2018.

Piotr Wiecek est un consultant expérimenté en sécurité informatique, spécialisé dans les domaines du pentest Active Directory, Cloud & Kubernetes. Il fait régulièrement équipe avec Florian pour effectuer les tests d'intrusion. L'équipe compte également sur l'intervention ponctuelle d'autres consultants en cybersécurité.

Ils nous font confiance

Mini Green Power
L'énergie de demain

Lizee

BUT

S3pweb
L'agrégateur des data Transport

apria
R.S.A.

LANCEY
energy storage

gutenberg technology
Evolution is in the publishing process

Notre fonctionnement

Déroulé d'une mission de A à Z

- Contact initial et détermination du besoin réel (pentest, red teaming, formation cyber, phishing…) ;
- Envoi d'une proposition commerciale et des Conditions Générales de Services (CGS) ;
- Une fois la proposition et les CGS signées, une lettre d'engagement est rédigée. Cette lettre reprend les informations importantes du test (type de test, dates, contacts, tarifs…) et nous permettra ainsi d'effectuer nos tests en toute légalité ;
- Début des tests aux dates indiquées ;
- Rendu du livrable dans la semaine qui suit et présentation des résultats.

Le livrable

Le livrable est fourni sous forme de rapport, indépendamment du type de test réalisé. Chaque rapport est divisé en deux parties :

- Section exécutive : un rappel des informations globales sur le test réalisé est donné (type de test, dates, contacts…), ainsi qu'une vue d'ensemble des failles identifiées (résumé des failles dans un tableau, exemples de scénarios d'attaques…) ;
- Section technique : Chaque vulnérabilité est présentée afin d'en comprendre les détails, de pouvoir la reproduire et la résoudre. Chacune vulnérabilité est présentée en plusieurs parties :
    - Description
    - Impact & Risque CVSS
    - Preuves
    - Recommandation

Pentest & services associés (Cyber)

Test de sécurité de l'infrastructure Externe

Ce test simule une attaque sur une infrastructure informatique accessible depuis Internet. L'objectif d'un tel test est d'identifier les vulnérabilités des mesures de sécurité implémentées au niveau du réseau et du système d'exploitation des systèmes connectés à Internet.

- Temps moyen nécessaire : 2 jours / 15 IPs
- À partir de : 1000 € HT / 15 IPs

Test de sécurité de l'infrastructure Interne

Ce test simule une attaque sur les systèmes du réseau local de l'entreprise et les données sensibles qui y sont stockées. Il s'agit d'une attaque simulée par une personne qui a déjà accédé au réseau interne et qui en connaît les systèmes. Ce test se concentre sur l'identification structurée des vulnérabilités dans un ensemble étendu de systèmes internes. Nous pouvons également tester l'Active Directory pour des failles telles que Kerberoasting ou délégation sans contrainte.

- Temps moyen nécessaire :
    - 2 jours / 15 IPs
    - 2 jours / Active Directory (AD)
- À partir de : 1000 € HT / 15 IPs + 1000 € HT / AD

Test de sécurité des applications web

Lors de ce test, nous analysons les vulnérabilités des applications en nous basant sur l'OWASP Top 10, telles que l'injection SQL, le Cross-site Scripting (XSS), la validation des entrées utilisateurs et les interfaces de gestion vulnérables. Nous proposons plusieurs types de tests applicatifs :

- « Black box » - simule une attaque du point de vue d'un utilisateur *non-autorisé*. Les fonctions accessibles une fois connecté ne peuvent généralement pas être testées.
    - Temps moyen nécessaire : 3.5 jours / app
    - À partir de : 1750 € HT / app

- « Grey box » - simule une attaque du point de vue d'un utilisateur *autorisé* ***et*** *non-autorisé*. Ces tests impliquent l'utilisation de comptes spécifiquement fournis, dans l'objectif d'identifier des vulnérabilités concernant la logique d'application, telles que la vérification de l'accès non autorisé aux informations d'autres utilisateurs.
    - Temps moyen nécessaire : 6 jours / app
    - À partir de : 3000 € HT / app

Test de sécurité des applications mobiles

Ce test vise la sécurité des applications mobiles sur smartphones et tablettes, concernant la communication entre l'application (mobile) sur smartphone / tablette et l'environnement applicatif back-end. Dans cet objectif, nous ferons un test de sécurité d'application spécifique pour le back-end et un test de sécurité de code source pour l'application.

- Temps moyen nécessaire : 6 jours / app
- À partir de : 3000 € HT / app

Test de sécurité Wi-Fi

Un test de sécurité Wi-Fi simule une attaque sur un réseau sans fil. Nous entrerons sur un ou plusieurs sites avec un ordinateur portable spécialement préparé afin d'identifier les vulnérabilités de la technologie Wi-Fi en place, à plusieurs points stratégiques si nécessaire.

- Temps moyen nécessaire : 2 jours / AP
- À partir de : 1000 € HT / AP

Test de robustesse et complexité du mot de passe

Lors de ce test, nous évaluons la robustesse des mots de passe importants que les utilisateurs finaux ont pu choisir. Pour effectuer ce test, nous coopérons étroitement avec nos clients pour obtenir un extrait des hashs de mots de passe des utilisateurs sélectionnés. Nous essayons ensuite de « cracker » ces hashs, donnant ainsi un aperçu des mots de passe choisis et des statistiques associées (par exemple, définir combien de mots de passe peuvent être devinés en un temps défini).

- Temps moyen nécessaire : 3 jours / 500 hashs
- À partir de : 1500 € HT / 500 hashs

Test de sécurité SCADA / ICS

Les infrastructures critiques et les systèmes industriels dépendent de plus en plus de l'informatique, introduisant de nouvelles menaces dans les systèmes SCADA. Hackmosphere aide les organisations à évaluer et tester le réseau OT grâce à des tests de sécurité passifs et actifs, qui sont ensuite comparées au niveau de sécurité souhaité.

Au cours des tests passifs, nous revoyons par exemple la configuration de l'architecture en place, les contrôles d'accès physiques ou le process de management des mises-à-jour.

Les tests actifs comprennent des tests de pénétration de l'infrastructure informatique interne, des hôtes à double appartenance (IT & OT) et de l'infrastructure ICS. L'infrastructure ICS est testée avec des actions très limitées afin de s'assurer de ne pas perturber ces environnements hautement sensibles.

- Temps moyen nécessaire : 12 jours / site
- À partir de : 6000 € HT / site

Red teaming & services associés

Campagne de Phishing (maillon Humain)

Ce test vise à identifier les vulnérabilités de l'entreprise liées à l'aspect humain : les employés internes qui ont accès aux applications et informations critiques. Le test de phishing sensibilisera les employés à la cybersécurité. Il s'agira de leur envoyer un e-mail malveillant afin d'identifier le pourcentage du personnel ayant cliqué sur le lien ou ouvert la pièce jointe. Un rapport sans information personnelle sur les employés sera fourni et permettra aux employés d'être plus alertes quant aux risques cyber.
Plusieurs types de campagnes de phishing existent :

- Emailing de masse (> 50 emails) :
  - Link clicking (redirection to a website with a login page)
    - Temps moyen : 3 jours
    - À partir de : 1500 € HT
  - Pièce jointe malveillante (e.g. Word macro document)
    - Temps moyen : 5 jours
    - À partir de : 2500 € HT
- Spear-phishing (10 emails désignés):
  - Link clicking (redirection to a website with a login page)
    - Temps moyen : 5 jours / 10 emails
    - À partir de : 2500 € HT
  - Pièce jointe malveillante (e.g. Word document)
    - Temps moyen : 7 jours / 10 emails
    - À partir de : 3500 € HT

Test de sécurité physique (maillon Physique)

Ce test simule une pénétration physique par un étranger malveillant. Il est destiné à révéler les vulnérabilités et les risques liés à l'aspect physique. Les objectifs définis avec le client peuvent être d'accéder physiquement à des machines, des documents sensibles, des salles sécurisées ou encore d'accéder directement au réseau. Nous tenterons d'accéder à un ou plusieurs emplacements, depuis l'extérieur.

Pour ce faire, nous allons initier nos tests avec de l'OSINT (Open Source INTelligence) afin d'identifier un maximum d'informations sur Internet. Nous ferons ensuite une reconnaissance physique et essaierons de récupérer un maximum d'information, sans entrer à l'intérieur. Avec les informations recueillies, nous établirons des scénarios qui doivent être approuvés par notre client, et tenterons de pénétrer l'entreprise physiquement afin d'atteindre notre objectif.

- Temps moyen nécessaire : 12 jours / site
- À partir de : 6000 € HT / site

« Assumed breach » (maillon Cyber)

Ce test simule la réussite d'un attaquant à s'introduire dans le réseau de l'entreprise (par exemple via un email frauduleux ou une pénétration via une faille de sécurité physique ou informatique). L'objectif sera d'identifier le chemin le plus court permettant de prendre le contrôle de la ressource la plus importante du client (ex. accéder à des données confidentielles). Pour ce faire, nos testeurs identifieront une chaîne de vulnérabilités présentes dans l'infrastructure du client et ainsi les exploiteront pour atteindre l'objectif fixé.

- Temps moyen nécessaire : 5 jours / objectif
- Nombre d'objectifs recommandés : 2
- À partir de : 2500 € HT / objectif

Opération Full Red Teaming
(maillons Humain, Physique & Cyber)

Lorsqu'une entreprise pense avoir atteint un niveau de sécurité très élevé et est satisfaite de sa maturité en termes de cybersécurité, il devient alors très intéressant de pratiquer un test de red teaming.

Ce test permet d'effectuer une simulation d'attaque complète, contenant toutes les étapes d'une APT (Advanced Persistent Threat), par un groupe de hackeurs éthique d'élite. Cette approche fournit une vision plus concrète que des pentests habituels quant à l'état de la sécurité globale de l'entreprise. Ce type de test est abordé en trois dimensions et implique des tests d'ingénierie Physique, Cyber & Sociale, permettant ainsi de tester les 3 surfaces d'attaques de la sécurité de l'information.

En d'autres termes, ce test inclut les tests « Campagne de phishing », « Test de sécurité physique », « Test de sécurité de l'infrastructure Externe » & « Assumed breach ».

Dans un premier temps, l'équipe rassemblera une quantité importante d'informations sur la cible, puis tentera d'accéder au réseau de l'entreprise via une campagne de phishing et une pénétration physique. Une fois l'accès au réseau obtenu, l'équipe tentera d'identifier le chemin le plus court pour prendre le contrôle de la ressource la plus importante du client.

- Temps moyen nécessaire : 35 jours / 1 site & 2 objectifs cyber
- À partir de : 17500 € HT / 1 site & 2 objectifs cyber