Règles du Hackfest SE CTF

Avant de vous inscrire, lisez ATTENTIVEMENT TOUTES LES RÈGLES. Il est de la responsabilité de chaque concurrent de connaître et de respecter toutes les règles. Toute infraction à une règle peut entraîner la disqualification immédiate du concurrent et l'exposer à des poursuites pénales ou civiles.

Ces règles sont conçues pour vous protéger. Connaissez-les et respectez-les!

Phase un: phase de collecte d'informations OSINT

• Chaque candidat recevra un dossier par courrier électronique avec le nom et l'adresse URL de la société cible.

• Une liste contenant les drapeaux à rassembler et un score correspondant sera fournie à chaque concurrent au début de la compétition. Chaque concurrent disposera de deux (2) semaines pour rassembler les drapeaux correspondants, compléter et rédiger un rapport conformément aux règles énoncées dans les présentes.

• Chaque concurrent doit rassembler autant d'informations que possible en utilisant uniquement des sources publiques de renseignements à source ouverte (OSINT). Cela inclut, sans toutefois s'y limiter, les médias sociaux, les sites Web, les babillards électroniques, etc. La source de chaque drapeau doit être citée et accessible par les juges. Toute source citée inaccessible ou inaccessible par les juges ne sera ni prise en compte ni prise en compte.

• Il est interdit aux candidats d'appeler, d'envoyer un courrier électronique ou de contacter l'entreprise cible aux fins d'OSINT avant la partie en direct de la collecte d'informations, à la seule exception d'appeler un numéro pour s'assurer qu'il s'agit d'un numéro valide.

• Chaque concurrent doit créer un rapport sur la base des informations obtenues lors de la phase de collecte OSINT décrite ci-dessus. La lisibilité et le professionnalisme du rapport constitueront 25% de la note. Un exemple de rapport sera fourni à tous les candidats à titre indicatif.

• Le contenu des rapports de chaque concurrent sera mis à la disposition de la société cible à la demande de celui-ci.

• Tous les drapeaux trouvés et identifiés dans le rapport écrit se verront attribuer des demi-points. C’est dans votre intérêt de tenter de collecter autant de drapeaux que possible au cours de cette phase, car vous pourrez également les récupérer à nouveau lors de l’appel de points complets.

• Les candidats remettront leur rapport pour examen au jury au plus tard à la date mentionnée dans le dossier qui leur aura été transmis. Le fait de rendre un rapport tardif vous disqualifiera du concours, alors transmettez un rapport partiel si nécessaire.

Phase deux: phase d'appel en direct

• La deuxième phase aura lieu le vendredi 1er novembre au Hackfest.

• Les créneaux horaires des candidats seront aménagés de manière à optimiser les chances qu'ils obtiennent des représentants de la société cible par téléphone. Par exemple, les personnes ayant des cibles sur la côte est doivent concourir en premier, et les concurrents ayant des cibles sur la côte ouest doivent concourir plus tard dans la journée.

• Pendant chaque créneau horaire, les candidats seront placés dans une cabine insonorisée et disposeront exactement de 30 minutes pour appeler la société cible. Au cours de l'appel, les concurrents doivent tenter de capturer le plus de drapeaux possible. Les drapeaux capturés au cours de cette phase se voient attribuer tous les points.

• Avant le concours, les candidats doivent fournir une liste de tous les numéros de téléphone qu'ils ont l'intention d'appeler et des numéros dont ils ont besoin pour être usurpés.

• Si au cours de leur appel, ils apprennent qu'un autre numéro est utilisé, il peut être utilisé, mais nous ne pouvons / ne voulons usurper aucun numéro qui n'a pas encore été fourni.

• Tous les numéros de téléphone doivent être des numéros de téléphone du Canada ou des États-Unis.

• Chaque drapeau ne peut être marqué qu'une seule fois. Si un indicateur partiel est collecté, par exemple un type AV mais pas un numéro de version, un deuxième appel peut être passé pour obtenir le numéro de version.

• Les candidats ne peuvent à aucun moment pendant le CTF dire quelque chose qui ait pour effet de faire craindre pour le représentant de la société cible pour sa sécurité et la sécurité de leurs proches ou de leurs collègues. Il est illégal de le faire et les candidats ne sont pas autorisés à se faire passer pour des agents de la paix (police, ou similaire) ou des représentants du gouvernement.

• Seuls les employés de la société cible sont autorisés à être appelés. Cela peut inclure des employés contractuels.

• Aucun langage de harcèlement ou obscène ne sera autorisé ni toléré.

• Les informations personnelles qui ne sont pas directement liées au travail du représentant de la société cible ne seront ni demandées ni collectées. Cela comprend le NAS, l'adresse du domicile, les noms des enfants, etc.

• L'idée sous-jacente de ce concours est la suivante: personne ne sera victime pendant ce concours. Les compétences en ingénierie sociale peuvent être démontrées sans s'engager dans des activités contraires à l'éthique. Le concours met l'accent sur les compétences des candidats et non sur les dommages qu'ils peuvent causer. Notre objectif est de sensibiliser les organisations à la menace que représente l'ingénierie sociale. En fonction de la nature de la violation, si vous ne respectez pas l'une de ces règles, vous recevrez un avertissement ou vous serez disqualifié. En cas de seconde violation, vous serez disqualifié de la compétition.

• Faites preuve de bon sens, si quelque chose semble contraire à l'éthique, ne le faites pas. Si vous avez des questions, demandez à un juge.

Phase trois: Shmooze Off

• Les 5 meilleurs concurrents du vendredi devront participer au second tour de la compétition du samedi.

• Chaque concurrent devra être informé de sa nouvelle société cible et se verra attribuer un numéro. Aucune usurpation téléphonique ne sera autorisée.

• Une liste des drapeaux à rassembler sera fournie aux participants 60 minutes avant les appels du samedi.

• Chaque concurrent est autorisé à faire appel à l'audience de la FCE pour l'ingénierie sociale pour effectuer une reconnaissance OSINT et créer des prétextes.

• L'ordre des appels sera déterminé sur la base des notes du vendredi, allant du plus haut au plus bas. En cas d'égalité, le tirage au sort décidera.

Drapeaux: «sont une liste personnalisée d'informations spécifiques que vous devrez découvrir au cours de la phase de collecte des informations et lors de vos appels téléphoniques. Le panel de juges crée la liste et des points seront attribués pour chaque élément correctement trouvé (et documenté) dans la liste. Cette liste vous sera présentée avec votre paquet d'informations si vous êtes sélectionné pour concourir.

Pointage: une feuille de pointage détaillée sera fournie à tous les candidats. Toutefois, le flux de pointage général correspond à un demi-point pour chaque drapeau du rapport écrit, plus le score de qualité du rapport. Chaque drapeau marqué pendant la phase d'appel comptera pour un point complet. Pendant le Shmooze Off, chaque drapeau compte comme un point. Le gagnant du concours aura le plus grand nombre de points.

Frais d’entrée: pour éviter les défections, tous les candidats sélectionnés doivent payer un dépôt de 25 $ entièrement remboursable (via Paypal) pour pouvoir participer. L'acompte d'un concurrent leur sera remboursé lorsqu'il se présentera à son créneau horaire. Nous occuperons des postes en attente pour remplacer les défections (no-shows). Toutefois, les candidats en attente ne sont pas assurés d'avoir une place. Une fois qu'un concurrent a été informé qu'il est sélectionné pour la compétition, il disposera de 72 heures pour effectuer le dépôt. Si le dépôt n'est pas reçu dans les 72 heures, le concurrent sera remplacé par un autre concurrent.

NOTE: Notre SECTF est très étroitement basée sur la DEF CON SECTF gérée par Chris Hadnagy et son équipe, et nous avons copié sans vergogne leur format et leurs règles pour la plupart.