

Hackfest SECTF 2025

= = =

Registration

- 1) Email (shane@hackfest.ca) your name/handle, with 5 proposed target companies (must be Canadian companies, and you cannot have any affiliation with any of the targets), and the best email and phone number to reach you at
- 2) All entrants will receive a link where they must submit a \$25 CAD refundable registration fee. This fee is refundable if (and only if) a) you withdraw your application within 21 days of submitting it, or b) you show up and participate in the competition. If you do not show, or show but fail to participate, your entry fee will not be refunded, and will go towards beer/food/debauchery fund for all other participants. Failure to submit your registration fee will result in your removal from the contest.
- 3) Contest rules are available below.

Rules

Read ALL THE RULES CAREFULLY. It is each contestant's responsibility to know and abide by all the rules. Any violation of any rule may result in instant disqualification of the contestant, and may place them at risk of criminal or civil prosecution.

These rules are designed to protect you. Know them and abide by them!

Phase One: OSINT Information Challenge

- **September 10th → October 4th - Midnight Pacific**
- Each contestant shall be sent the target company via email with the name and URL.
- All contestants will be assigned the same target company to ensure fairness.
- A list containing the flags to be gathered and a corresponding score will be provided to each contestant at the start of the competition. Each contestant shall have until midnight, Sunday Oct 6 Pacific time, to gather the corresponding flags, complete and file a report in accordance with the rules set forth herein.
- Each contestant shall gather as much information as possible using public, open source intelligence (OSINT) sources only. This includes, but is not limited to, social media, websites, message boards, etc. The source of each flag must be cited and accessible by judges. Any cited

source which is inaccessible or unreachable by judges shall not be considered nor taken into account.

- Contestants are prohibited from calling, emailing, or contacting the target company for the purpose of OSINT, with the sole exception of calling a number to ensure it is a working number.
- Each contestant shall create a report based on the information obtained during the OSINT gathering phase described above. The report will list all the discovered flags, as well as proposed pretexts that could be used for social engineering calls.
- **Contestants must submit their report for review to shane@hackfest.ca on or before midnight, Pacific time, October 4th, 2025. Turning in a late report will disqualify you from the contest, so turn in a partial report if necessary.**

Phase Two: Specific Target OSINT

- **October 4th → October 15th**
- Each contestant shall be sent a unique target company via email with the company name and URL. This company will be the one you will be calling during Phase 3.
- The same flag list as that used in Phase One will be used. Each contestant shall create a dossier to use for the competition, however this dossier will NOT be scored. It is in your best interest to gather as many flags prior to your call to assist with your efforts. Each contestant shall have until **midnight October 15th** Pacific time, to gather the corresponding flags, complete and file a report in accordance with the rules set forth herein. **The dossier MUST contain a list of phone numbers to be dialed. No numbers shall be called during phase three that are not contained within the dossier, or discovered during the call(s) during the competition.**
- Contestants are prohibited from calling, emailing, or contacting the target company for the purpose of OSINT before the live information gathering portion of the competition, with the sole exception of calling a number to ensure it is a working number.
- Each contestant shall create a report based on the information obtained during the OSINT gathering phase described above. The report will list all the discovered flags found in the recon phase, as well as proposed pretexts to be used for their calls.

Phase Three: Live Call Phase

- **October 17th**
- Phase Three will occur on Friday, October 17 at 0830 at the HackFest SECTF village. **PLEASE ENSURE YOU HAVE A COPY ALL VETTED PHONE NUMBER/NAMES OF PEOPLE YOU WILL BE CALLING WITH YOU IN THE BOOTH.** Once your call starts you can only dial those phone numbers or others that you gather during your call(s).
- Contestant order will be drawn randomly, however time slots may also be arranged to optimize the chances of them getting target company's representatives on the phone. For example, people with targets on the East coast shall compete first, and contestants having West coast targets shall compete later in the day. Accommodations for speakers with conflicting schedules will be made.
- During each contestant's time slot, they will be placed in a sound-proof booth and given exactly 25 minutes to make call(s) to their target company. During the call(s), contestants

shall attempt to capture as many flags as possible. Flags captured during this phase are awarded full points.

- Please note, the clock will stop while you are on hold or waiting for someone to answer (to a maximum of 5 minutes). During this grace period the clock only advances while you are talking to someone. If someone is looking information up during a conversation the clock will continue to advance. Try to select numbers that you know will be staffed in order to maximize your chances of success.
- **Prior to the contest, contestants must provide a list of all numbers they intend to call, and any numbers they require to be spoofed. Calls will not be made to any numbers not listed on your dossier.** If during your call you learn of another number, it can be used, however we cannot/will not spoof any number not already provided.
- All phone numbers must be from Canada or USA.
- Each flag can only be scored once. If a partial flag is gathered, for example, an AV type but not version number, a second call can be made to get the version number.
- At no point in the CTF, can contestants say anything intended or effectively having the effect of having the target company's representative fear for their, their loved ones' or their colleague's safety. It is illegal to and contestants are not allowed to pose as law enforcement officers or government officials.
- Only employees of the target company are allowed to be called. This can include contract employees.
- No harassing or obscene language will be allowed nor tolerated.
- Personal information that is not directly connected to the job of the target company's representative shall not be requested nor collected. This includes SIN, home address, offspring's names, etc.
- The underlying idea of this contest is: **No one gets victimized** during this contest. Social engineering skills can be demonstrated without engaging in unethical activities. The contest focuses on the skills of the contestants, not on the damage they can cause. Our goal is to raise awareness of the threat that social engineering poses to organizations today. Depending on the nature of the breach, If you violate any of these rules, you will either receive a warning or be disqualified. In the event of a second violation you will be disqualified from the competition.
- Use common sense, if something seems unethical – don't do it. If you have questions, ask a judge.

Phase Four: Shmooze Off

- **October 18th**
- The top 4 ranking competitors from Friday shall move on to a Saturday competition runoff. The contest will commence at 0900hrs at the SECTF Village.
- Contestants will be calling a randomly selected company. The target and flags will be given to the contestant 30 minutes prior to their call. The contestant can utilize the audience to research the target, find numbers and contact names, and come up with a pretext.
- The order of calls will be selected via rock paper scissors, random draw, or another random method agreed to by the contestants.

General rules and definitions

- **Flags:** A custom list of specific bits of information”, which you will have to discover during the information gathering stage and during your phone calls. The judging panel creates the list and points will be awarded for each item correctly found (and documented) from the list. This list will be presented to you with your information packet if you are selected to compete.
- **Scoring:** A scoring sheet breakdown will be provided to all contestants, however the general scoring flow is half a point for each flag on the written report, plus the report quality score. Each flag scored during the call phase will count as a full point. During the Shmooze Off, each flag counts as a point. The overall contest winner shall have the highest accumulation of points.
- **Entrance Fee:** To prevent no-shows, all selected contestants must pay a fully refundable \$25 deposit (via Paypal) in order to compete. A contestant’s deposit shall be refunded to them when they show up at their time slot. We will hold standby positions to take the place of no-shows, however standby contestants are not guaranteed a slot. Once a contestant has been notified they are selected for the competition, they will have 72 hours to make the deposit. If the deposit is not received within 72 hours, the contestant will be replaced with another contestant.

Hackfest SECTF 2025

= = =

Inscription

- 1) Envoyez-nous par courriel (shane@hackfest.ca) votre nom/pseudonyme, ainsi que 5 entreprises cibles proposées (il doit s'agir d'entreprises canadiennes, et vous ne devez avoir aucun lien avec aucune des cibles), et votre adresse courriel et numéro de téléphone où nous pouvons vous joindre.
- 2) Tous les participants recevront un lien où ils devront s'acquitter de frais d'inscription remboursables de 25 \$ CAD. Ces frais sont remboursables si (et seulement si) a) vous retirez votre candidature dans les 21 jours suivant son dépôt, ou b) vous vous présentez et participez au concours. Si vous ne vous présentez pas ou si vous vous présentez mais ne participez pas, vos frais d'inscription ne seront pas remboursés et seront versés au fonds destiné à la bière, à la nourriture et aux festivités pour tous les autres participants. Si vous ne payez pas vos frais d'inscription, vous serez exclu du concours.
- 3) Le règlement du concours est disponible ci-dessous.

Règlements

Lisez ATTENTIVEMENT TOUTES LES RÈGLES. Il incombe à chaque participant de connaître et de respecter toutes les règles. Toute violation d'une règle peut entraîner la disqualification immédiate du participant et l'exposer à des poursuites pénales ou civiles.

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

Phase 1 : Défi lié aux informations OSINT

- **10 septembre → 4 octobre - minuit, heure du Pacifique.**
- Chaque participant recevra par e-mail le nom et l'URL de l'entreprise cible.
- Tous les participants se verront attribuer la même entreprise cible afin de garantir l'équité du concours.
- Une liste contenant les drapeaux à collecter et le score correspondant sera fournie à chaque participant au début du concours. Chaque participant aura jusqu'au dimanche 6 octobre à minuit, heure du Pacifique, pour collecter les drapeaux correspondants, remplir et déposer un rapport conformément aux règles énoncées dans le présent document.
- Chaque participant devra collecter autant d'informations que possible en utilisant uniquement des sources d'informations publiques et ouvertes (OSINT). Cela inclut, sans s'y limiter, les

réseaux sociaux, les sites web, les forums, etc. La source de chaque drapeau doit être citée et accessible aux juges. Toute source citée qui est inaccessible ou hors de portée des juges ne sera ni prise en compte ni considérée.

- Il est interdit aux participants d'appeler, d'envoyer des e-mails ou de contacter l'entreprise cible à des fins d'OSINT, à la seule exception d'appeler un numéro pour s'assurer qu'il est en service.
- Chaque participant doit créer un rapport basé sur les informations obtenues lors de la phase de collecte OSINT décrite ci-dessus. Le rapport répertorie tous les indicateurs découverts, ainsi que les prétextes proposés qui pourraient être utilisés pour les appels d'ingénierie sociale.
- **Les participants doivent soumettre leur rapport pour examen à shane@hackfest.ca au plus tard à minuit, heure du Pacifique, le 4 octobre 2025. La remise d'un rapport en retard entraînera votre disqualification du concours, alors remettez un rapport partiel si nécessaire.**

Phase deux : cibles spécifiques OSINT

- **4 octobre → 15 octobre**
- Chaque participant recevra par e-mail le nom et l'URL d'une entreprise cible unique. C'est cette entreprise que vous appellerez pendant la phase 3.
- La même liste de drapeaux que celle utilisée lors de la phase 1 sera utilisée. Chaque participant devra créer un dossier à utiliser pour le concours, mais ce dossier ne sera PAS noté. Il est dans votre intérêt de rassembler autant de drapeaux que possible avant votre appel afin de faciliter vos efforts. Chaque participant aura jusqu'au 15 octobre à minuit, heure du Pacifique, pour rassembler les drapeaux correspondants, remplir et déposer un rapport conformément aux règles énoncées dans le présent document. Le dossier DOIT contenir une liste des numéros de téléphone à composer. Aucun numéro ne sera appelé pendant la phase trois s'il ne figure pas dans le dossier ou s'il n'a pas été découvert pendant les appels passés pendant la compétition.
- Il est interdit aux participants d'appeler, d'envoyer des e-mails ou de contacter l'entreprise cible à des fins d'OSINT avant la partie de la compétition consacrée à la collecte d'informations en direct, à la seule exception d'un appel téléphonique visant à vérifier que le numéro est bien en service.
- Chaque participant devra rédiger un rapport basé sur les informations obtenues lors de la phase de collecte OSINT décrite ci-dessus. Le rapport devra contenir tous les indicateurs découverts lors de la phase de reconnaissance, ainsi que les prétextes proposés pour les appels téléphoniques.

Phase trois : phase d'appel en direct

- **17 octobre**
- La phase trois aura lieu le vendredi 17 octobre à 8 h 30 au village Hackfest SECTF.
ASSUREZ-VOUS D'AVOIR AVEC VOUS DANS LA CABINE UNE COPIE DE TOUS LES NUMÉROS DE TÉLÉPHONE ET NOMS DES PERSONNES QUE VOUS ALLEZ APPELER ET QUI ONT ÉTÉ VÉRIFIÉS. Une fois votre appel commencé, vous ne pourrez composer que ces numéros de téléphone ou d'autres que vous aurez obtenus pendant votre ou vos appels.
- L'ordre des participants sera tiré au sort, mais les créneaux horaires pourront également être organisés de manière à optimiser leurs chances d'avoir les représentants de l'entreprise cible au téléphone. Par exemple, les personnes ayant des cibles sur la côte Est concourent en

premier, et les participants ayant des cibles sur la côte Ouest concourent plus tard dans la journée. Des aménagements seront prévus pour les intervenants ayant des emplois du temps incompatibles.

- Pendant le temps imparti à chaque participant, celui-ci sera placé dans une cabine insonorisée et dispose exactement de 25 minutes pour passer des appels à l'entreprise cible. Pendant ces appels, les participants devront tenter de capturer autant de drapeaux que possible. Les drapeaux capturés pendant cette phase rapportent le maximum de points.
- Veuillez noter que le chronomètre s'arrêtera pendant que vous êtes en attente ou que vous attendez qu'une personne vous réponde (pendant 5 minutes maximum). Pendant ce délai de grâce, le chronomètre ne continue à tourner que lorsque vous êtes en conversation avec quelqu'un. Si une personne recherche des informations pendant une conversation, le chronomètre continuera à tourner. Essayez de sélectionner des numéros qui, vous le savez, seront pris en charge par du personnel afin de maximiser vos chances de réussite.
- **Avant le concours, les participants doivent fournir une liste de tous les numéros qu'ils ont l'intention d'appeler, ainsi que tous les numéros qu'ils souhaitent usurper. Aucun appel ne sera passé vers des numéros ne figurant pas dans votre dossier.** Si, au cours de votre appel, vous obtenez un autre numéro, vous pouvez l'utiliser, mais nous ne pouvons pas/ne voulons pas usurper un numéro qui n'a pas été fourni au préalable.
- Tous les numéros de téléphone doivent provenir du Canada ou des États-Unis.
- Chaque indicateur ne peut être comptabilisé qu'une seule fois. Si un indicateur partiel est collecté, par exemple un type AV mais pas le numéro de version, un deuxième appel peut être effectué pour obtenir le numéro de version.
- À aucun moment pendant le CTF, les participants ne peuvent tenir des propos visant ou ayant pour effet de faire craindre au représentant de l'entreprise cible pour sa sécurité, celle de ses proches ou celle de ses collègues. Il est illégal et interdit aux participants de se faire passer pour des agents des forces de l'ordre ou des représentants du gouvernement.
- Seuls les employés de la société cible peuvent être appelés. Cela peut inclure les employés contractuels.
- Aucun langage harcelant ou obscène ne sera autorisé ni toléré.
- Les informations personnelles qui ne sont pas directement liées à l'emploi du représentant de l'entreprise cible ne doivent pas être demandées ni collectées. Cela inclut le numéro d'assurance sociale, l'adresse personnelle, les noms des enfants, etc.
- L'idée sous-jacente de ce concours est la suivante : **personne ne doit être victime** pendant ce concours. Les compétences en ingénierie sociale peuvent être démontrées sans se livrer à des activités contraires à l'éthique. Le concours met l'accent sur les compétences des participants, et non sur les dommages qu'ils peuvent causer. Notre objectif est de sensibiliser les organisations à la menace que représente aujourd'hui l'ingénierie sociale. En fonction de la nature de l'infraction, si vous enfreignez l'une de ces règles, vous recevrez un avertissement ou serez disqualifié. En cas de deuxième infraction, vous serez disqualifié du concours.
- Faites preuve de bon sens : si quelque chose vous semble contraire à l'éthique, ne le faites pas. Si vous avez des questions, demandez conseil à un juge.

Phase quatre : Shmooze Off

- **18 octobre**
- Les quatre meilleurs concurrents du classement de vendredi passeront à la phase finale de la compétition samedi. Le concours débutera à 9 h au village SECTF.
- Les participants appelleront une entreprise choisie au hasard. La cible et les indicateurs leur seront communiqués 30 minutes avant leur appel. Les participants peuvent faire appel au public pour rechercher des informations sur la cible, trouver des numéros et des noms de contacts, et trouver un prétexte.
- L'ordre des appels sera déterminé par un jeu de pierre-papier-ciseaux, un tirage au sort ou toute autre méthode aléatoire convenue par les participants.

Règles générales et définitions

- **Drapeaux** : une liste personnalisée d'informations spécifiques, que vous devrez découvrir pendant la phase de collecte d'informations et lors de vos appels téléphoniques. Le jury établit la liste et des points seront attribués pour chaque élément correctement trouvé (et documenté) dans la liste. Cette liste vous sera remise avec votre dossier d'information si vous êtes sélectionné pour participer au concours.
- **Notation** : une feuille de notation détaillée sera fournie à tous les participants, mais le barème général prévoit un demi-point pour chaque drapeau sur le rapport écrit, plus la note attribuée à la qualité du rapport. Chaque drapeau noté pendant la phase d'appel comptera pour un point entier. Pendant le "Shmooze Off", chaque drapeau compte pour un point. Le gagnant du concours sera celui qui aura accumulé le plus grand nombre de points.
- **Frais d'inscription** : Afin d'éviter les absences, tous les candidats sélectionnés doivent verser un acompte entièrement remboursable de 25 \$ (via Paypal) pour pouvoir participer au concours. Le dépôt d'un participant lui sera remboursé lorsqu'il se présentera à l'heure prévue. Nous garderons des places en attente pour remplacer les absents, mais les participants en attente ne sont pas assurés d'avoir une place. Une fois qu'un participant a été informé qu'il a été sélectionné pour la compétition, il dispose de 72 heures pour verser le dépôt. Si le dépôt n'est pas reçu dans les 72 heures, le participant sera remplacé par un autre participant.