Hackfest SE CTF Rules

Before you sign up, 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 Gathering Phase

· Each contestant shall be sent a dossier via email with the name and URL of their target company.

· 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 two (2) weeks 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 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's readability and professionalism will make up 25% of the score. A sample report will be provided to all contestants as a guideline.

· Contents of each contestant's reports will be made available to the target company should they request it.

· Any flags found and identified in the written report will be awarded half-points. It's in your best interest to try and collect as many flags as possible during this phase as you will also be able to collect these flags again during the call for full points.

· Contestants will submit their report for review to the judging panel on or before the date mentioned on the dossier transmitted to them. Turning in a late report will disqualify you from the contest, so turn in a partial report if necessary.

Phase Two: Live Call Phase

· Phase Two will occur on Friday, November 1st at Hackfest.

· Contestant's time slots will be arranged to optimize the chances of them getting target company' 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.

· During each contestant's time slot, they will be placed in a sound-proof booth and given exactly 30 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.

· Prior to the contest, contestants must provide a list of all numbers they intend to call, and any numbers they require to be spoofed.

· If during their call they learn of another number, it can be used, however we cannot/will not spoof any number not already provided.

· All phone numbers Canada or USA phone numbers.

· 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 colleagues 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 Three: Shmooze Off

· The top 5 ranking competitors from Friday shall move on to a Saturday competition runoff.

· Every contestant shall be informed of their new target company, and will be provided with numbers. No phone spoofing will be allowed.

· A list of flags to gather will be provided to the contestants 60 minutes prior to the calls on Saturday.

· Each contestant is allowed to enlist the help of the Social Engineering CTF audience to perform OSINT recon and come up with pretexts

· The order of calls will be determined on the basis of Friday's scores, going from highest score to lowest. In the event of a tie, a coin toss shall decide.

Flags: "are 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.

NOTE: *Our SECTF is based very closely on the DEF CON SECTF run by Chris Hadnagy and crew, and we have shamelessly copied their format and rules for the most part.*