TOURNAMENT PARTICIPANTS' PRE-GAMEDAY BRIEFING : 8 JUNE 2018

The CDDC 2018 competition is an integrated cybersecurity tournament (CST) for Institutes of Higher Learning or IHLs (i.e. Universities, Polytechnics, etc) and Junior-College/Integrated-Programme-level participants.
For the tournament (the "Event"), all participating teams will be scored based on their ability to successfully achieve both defensive-oriented objectives as well as cybersecurity-auditing, incident-response and other multi-faceted objectives.

To score big, you will be expected to think both directly and laterally. This is not built as a one-area/one-subject "hacking" or "capture-the-flag" format. This is a multi-topic, multi-challenge real-working-world-style tournament that will involve you having to (a) maintain legal compliance with the management-directed scope of work, (b) obtain clues and information from various different sources, (c) make logical and educated deductions and decisions based on the available information and environment encountered as well as cross-reference information acquired across the entire duration of the tournament, (d) prioritize objectives based on your team's strategy, (e) harden / defend your own server against attacks while ensuring that essential services needed for your server's end-users are kept operationally available at all times, (f) shift resources dynamically between goals and perform resource and time management depending on circumstances, (g) perform security-testing and audits of multiple targets across different subnets, etc. In short, you will want to complete as many mission objectives as accurately, as quickly and as to the letter as possible. Some targets are too easy, others not so much, and the big points require a lot of thinking and some effort. So some teams will have problems getting in first gear while others will be able to cruise along initially - but the further you get in, the harder it generally gets. And if you do compromise some servers, congrats but don't stop there - there is a lot more that you are have yet to encounter :)

Within the gameplay, whatever actions which are (i) not barred by the Event rules outlined in this document, (ii) not barred by any other related document issued pre-gameplay and/or during gameplay and/or (iii) not prohibited under any rule communication from the event organizers at any time before and/or during the gameplay, are allowed to be performed, as long as the actions themselves are not in violation of any Singapore law.

1. GAMEPLAY OVERVIEW

Your cybersecurity team is part of a larger infocomm security and audit assurance group under the Garponesi Interior Ministry (GIM) of the fictitious contry of Garponesi. Your team is one of many which has been seconded by GIM to a Garponesian government agency. Every Garponesian government agency has a similar team assigned to it.

The Garponesi government is a very interconnected entity which relies heavily on IT networks and systems for proper functioning of its various component bodies, such as the agency your team has been assigned to. As such, ensuring the operational readiness and uptime of the systems you have been tasked with guarding and finding out weaknesses before any potential attacker does is of the utmost national importance and is a high priority for the Garponesi government.

Increasingly, there have been more and more attacks, either threatened by hacker groups or from covert state-level operations undertaken against the Garponesian state by rival countries. The Garponesi government is therefore anxious to ensure that all of its various agencies as well as the core backbone and server infrastructure of the Garponesi Defense Ministry (GDM) are secure.

To this end, the Garponesi Government is organizing a series of wargame-style cybersecurity exercises to ensure the readiness of its systems and find out any weaknesses before potential rivals do and that is where your team comes in. Your role within the government agency your team has been assigned to is to secure the agency's services and defend its infrastructure against attacks as well as to perform technical security audits against both the GIM's and the GDM's key networks and systems.

One of the primary objectives as communicated by the GIM's Directorate Head (DH) Mr Lim Lao Peh is to secure the infrastructure of the agency you have been seconded to. Specifically, you are required to protect a set of agency services from potential attack while ensuring that they are kept operational and accessible by the users of the service at all times.

Another primary objective is the auditing of the GIM's and GDM's networks and systems, which are different from the agency you are seconded to. The security audits are a 100% blackbox free-fire engagement where you are given nothing at the start other than the information you already have in this document and the information that you will receive through your individual team dashboards on gameday, and any information that you can find/correlate yourself as you proceed through the exercise.

A major restriction, however, are the GIM's rules of engagement which spell out the scope of work. Certain systems and networks in GIM and GDM are considered out-of-bounds and GIM DH has specified that those areas are not to be touched for the purposes of this exercise for classified reasons beyond your pay grade. Accordingly, you may ONLY engage targets that fall under the scope of work as communicated to you in all *official* communications from GIM DH only. The exact scope of work and targets will be made known to you at the start of the engagement on gameday via your team's in-game dashboard.

At this stage, the only information regarding the engagement scope of work / targets which have been communicated to the GIM Audit Assurance teams is that all the same department-related functions all reside together inside the same network range, i.e. all Garponesi government department X server IPs will all be inside the same IP segment, all division Y IPs will be inside the same IP segment, and so on.

Note that engaging a target that is outside the target list for this exercise will violate the scope of your work/engagement and potentially cause outage on the out-of-scope system attacked. This may also cause the Garponesi government to incur a major backlash from the citizens of Garponesi if they cannot access the out-of-scope systems. Staying within a communicated scope of work is a very real issue that all real-life IT cybersecurity practitioners face in the real world and you get to experience this too. Apart from the documentation you will receive on gameday through your team's dashboard interface, you will also need to use all your skills to deduce and correlate which are the authorized targets within the scope of work and to only engage those which are within the scope of work.

Further information about the rules of engagement and other information will be provided on gameday.

2. EVENT INFRASTRUCTURE

A purpose-built infrastructure comprised of wired, wireless, web, application, biometric and various other technologies has been designed and setup to simulate the targets which your team will attempt to engage within the context of the Garponesi government audit and assurance wargame exercise. By logical deduction and analysis of the information on hand, the information given out at the start of the tournament and the information embedded within the network you are connected to, the targets are easy to identify once found and the naming convention is very obvious upon discovery / correlation. Success in this tournament is more dependent on your being able to hunt, gather, correlate, analyze and take advantage of all information, data and/or observations encountered in-game, than any familiarity with using any particular tool.

Participants can engage only the infrastructure provided for the Event according to the details of the stipulated rules which will be given out at the start of the Gameday and no other.

Please refer to the other parts of this document, all relevant Gameday-issued in-game documentation and any other authorized instructions issued during the Tournament for further details.

You should prepare all your tools in advance (e.g. LiveUSBs, wireless hardware, software, 3G/4G-connection, etc) as there is no guarantee that any in-venue internet connection provided for you during the tournament by the Event venue (if available) will be sufficiently stable or fast or secure enough for you to download your tools on-site.

However, if you have your own on-site 3G/4G internet connection and/or are a legitimate user or subscriber of any public wireless internet access provider around the Event location, you can use your own internet / subscriber account to do any on-site independent research or tool download should you so wish.

3. PRE-TOURNAMENT PREPARATION

There are 2 things your team needs to do to be able to participate in this tournament.

(i) During your registration process, you team would have been asked to nominate a GMAIL account to the Event Organizer. Please ensure that this team account continues to remain valid and operational.

Please note that once you have provided the GMAIL account name, it is permanent and cannot be changed. The account name you provide is a very important part of the tournament and you should treat said account name, login and password with at least the same level of secrecy and confidentiality as you would treat your online-banking, online-email or online-gaming account.

If you accidentally or deliberately reveal your account user and password to any other team or person and they lock you out, terminate or do anything to your account, we will not be able to help you in any way and you will suffer the consequences of your own carelessness.

(ii) It is strongly recommended that your team have its own 3G/4G connection to access your team's nominated GMAIL account for participation in the Tournament and to interact with the in-game scoring system. We strongly advise **AGAINST** trying to use the in-game network to do so because it is a hostile environment filled with all sorts of attackers so doing so would be considered very dangerous and risky for your team - **you have been warned!!** If you are accessing your GMAIL account via a mobile device, you should also go to the App Store or Play Store or whatever store your device uses and download/install any free office app on your mobile device that will allow you to open up standard office document formats such as PDF, XLS, DOC, etc.

Therefore, at least one of your team members should have a 3G/4G-capable device with a data plan that has at least 1-to-2GB of data usage left on the device's data plan for the Tournament day and that device's data usage should not be used for any purpose other than interacting with your team's nominated GMAIL account and the team dashboard.

Please note that these 2 things are an absolute **MUST**. If you are unable to perform any action or activity due to any contravention of the abovementioned, we will not be able to assist you in any way.

4. EVENT RULES & LIABILITY WAIVER

Please remember that you participate in the Event at your own risk. The Event organizers are not responsible for your actions during the Event and are not responsible for any loss and/or damage to you and/or your and/or any personal, third-party and/or other equipment, hardware and/or software that you choose to bring for participation in any part of the Event. When you go for lunch or breaks, we advise you don't leave your equipment unattended, even if this is Singapore. And do not assume people are going to respect your ownership of any equipment. :)

This document incorporates by reference the Event rules and any organizer's indemnity form or liability waiver which the organizer(s) may require all participants to sign in order to participate in the Event as well as all relevant Event-related documentation issued.

Depending on the type of breach of the rules, there are significant point penalties, disqualification from the Event and/or criminal penalties involved (e.g. if you go and attack a private non-Event-related network). Please read and adhere to the rules carefully.

5. GAMEDAY

The tournament hall will be open **at 0745 hrs on 11 June 2018 (subject to Organizer's discretion) and the tournament is currently scheduled to start at 0800 hours**.

We advise you to arrive earlier than the tournament start time to ensure that you do not rush and injure yourself and also to get the maximum time to get ready before the release of the game-related starting documentation at the **start of the tournament at 0800 hrs on 11 June**.

Remember that haste makes waste - do not rush or run or push your way into the venue and always look where you are going to avoid bumping or tripping into tables, chairs, people or other things. Follow this simple rule and everyone will have a safe game whether they are first or last.

The next set of game-related information will be issued to you at the start of gameday via your team's nominated GMAIL account. Those teams who arrive after the hall is opened will ***NOT*** get any extra time to digest the information, may lose valuable points and/or other stuff happen to them, etc, so don't be late !

Again, since the targets involve wired, wireless, web-app, client-server-app, mobile-app and various other technologies, you should make sure you bring all the hardware and software which you think may be necessary or relevant, for example and including but not limited to : LiveCD/LiveUSB distros such as the OSWA-Assistant™, personal laptops, Linux-natively-supported wireless 802.11-based adapters, Bluetooth dongles, directional hi-gain antennae, etc.
If in doubt, bring it...but be sure you are prepared to defend it as well! Physical security is just as important as cyber-security.
During the tournament, this document will continue to be available at the download link where you accessed it from so that you can read it together with the rest of the documentation you will be receiving on gameday (you can also save it to your phone and view it at any time offline before gameday). Correlation of different pieces of information is going to be VERY important in this Tournament (hint hint).

...MORE TOURNAMENT DETAILS AVAILABLE WHEN YOU ARRIVE ON GAMEDAY....!