Cyber Security Challenge Australia 2015: The game

What is CySCA?

- CYSCA is a ‘capture the flag’ (CTF) style competition.
- CTFs are competitions where players are given puzzles and once they solve a puzzle they get a ‘flag’. Players then submit the flag to game organisers to gain points for their team. At the end of the allocated time, the team with the most points wins (CySCA 2015 will run for 24 hours).

The 2015 Scenario – the Enterprise Cloud Wellness Initiative

- For CySCA 2015, you will be working will the Enterprise Cloud wellness Initiative (ECWI).
- Recently, some influential CEOs happened to watch some Hollywood hacking movies such as Hackers and WarGames.
- The problem? These CEOs mistook the films for documentaries and decided they needed to address these shocking cyber attacks – and fast!
- So they established an initiative that would provide “Cloud Wellness”, or the provision of advice and assistance to enterprises suffering from “Cyber Problems”.
- Great right? Not so much.
- The ECWI has a problem. A recent third party review discovered that confusing job titles such as “Innovation Sherpa” and total misunderstanding of job roles by the current “Chief Visionary Officer” has meant that none of the ECWI staff have any technical cyber security skills.

This is where your team comes in…

- Your team has been contracted into ECWI to provide technical skills and assistance.
- The Chief Visionary Officer would also like you to perform a thorough assessment of ECWI’s systems to ensure that they are secure (because providing security advice when you’re not secure yourself is not a good business model!).
- As part of the assessment you have been asked to conduct:
    1. a penetration test of the ECWI web based intranet site
    2. a penetration test of the ECWI corporate network with a written report outlining findings to non-technical initiative staff
    3. a forensic analysis of some potentially malicious activity on ECWI networks and systems
    4. an analysis of network traffic to detect any real-time threats with written information sharing reports to be distributed to ECWI partner enterprises

So what will CySCA 2015 actually look like?

- CySCA 2015 will consist of a number of Linked Challenges (your mission as set by the Chief Visionary Officer of ECWI) and some “Extra” Challenges.

Linked Challenges

- In the Linked Challenges, you will start at the first task and will be required to capture the flag to gain access to the next task (so each flag you capture means you are on the right track).
- However, you don’t have to submit associated ‘non-technical reporting’ requirements before you move to the next task. The forms will be unlocked when you capture the flag, but you can fill them in later if you wish. But don’t forget to do them!!

- CySCA Control is giving you more time on the written parts of the Challenge because we want you to think about your responses.
- The written answers are worth a lot of points this year and if you do them well you could easily bump yourself up the leader board – check out the details on in the "How do you win?" section below.
- You'll be allocated three submissions for each written task so you can review your work and edit it. Once you've submitted the third version you'll be locked out of that task.

Extra Challenges

- As well as the Linked Challenges, CySCA Control also want to expand the range of skills you are tested on and exposed to during the competition.
- Keep an eye on the website for the final details, but at the moment we're thinking the Extra Challenges might to include crypto, programming and password cracking.
- Extra challenges won't be unlocked progressively, so all the tasks will be in a separate category and available at the very start of the game.

Flag explanations

- CySCA Control can (and do) review flag submissions.
- Generally flags are discrete, either you get all of the points, or none of them. But this year, we're also asking you to briefly describe how you captured each flag along the way.
- Once you've submitted a flag, a text box will pop up for you to fill in.
- These answers don't have to be long (or in non-technical language!) – just enough info for us to see what you've done. For example, "I scanned machine X with X, saw that X was there, and used X tool with X arguments to obtain the flag". Simple!
- We're asking you to do this so we know information isn't being shared amongst teams, but also so we can see the different ways our Challenges can be solved – sometimes solutions come up that we had never thought of and that's really cool for us to see!
- If you don't fill in the box, we may have to remove the points for that flag, or in extreme cases, disqualify you.

Tools

- You will need a number of tools to complete the challenges in CySCA 2015. Here are some of them, I would suggest you get comfortable with using them:
  - Kali Linux 1.1.0a (we know Kali Linux 2 has just been launched – but we are testing the challenges with Kali Linux 1.1.0a, so that would be a good base to use).
  - Metasploit
  - Burp suite
  - SQLmap
  - Wireshark
  - Native disassembler (IDA or objdump)
  - Dubugger (GDB)
  - Text editor (vim, emacs)
  - Managed Disassembler (ILSpy)
  - Volatility
- This list of tools is not exhaustive, and there may be other tools you will use during CySCA2015.

- Find some instructions, find some tutorials and play with these tools BEFORE GAME DAY. You don't want to do this for the first time in the heat of competition
- You don't have to become Australia's foremost expert on the tools, you just want to play with them, understand what they can and can't do.

Hints and tips

Other CTFs

- The best way to prepare for CySCA 2015 is to play other CTFs.
- Both CySCA 2014 and 2013 are available on cyberchallenge.com.au (including CySCA 2014 In a Box), but you should also have a look at the write-ups as well as working on the challenges so you understand more than just entering the commands that are listed.
- There are also some great websites to visit too:
  - Ctftime.org – great for finding new CTFs to play and looking at write ups.
  - PicoCTF – this one is fantastic for CTF first-timers and newbies. It has good introductory challenges get you started and some more difficult ones to progress to.

Plan!

- It's the best way to have fun and look after yourself and your teammates.
- This is a big one – get some sleep.
- A couple of hours might seem like a big investment in a 24 hour competition, but it really isn't.
- The benefit from having a short sleep and therefore being able to keep thinking clearly far outweighs the couple of hours you might gain.
- Trust us, sleep deprivation leads to players using their time really ineffectively. When you are fatigued you'll get stuck because you'll make mistakes. Save yourself the angst and get some shut eye.
- Some teams prefer to schedule sleep, so that they always have someone awake, just in case anything happens. It really is up to your team to decide how you will approach CySCA – there is no 'right' way to do it.
- Make sure you eat and stay hydrated. This will also help with your focus and your thinking. No one makes good decisions on an empty stomach or with a pounding headache.

Written submissions – they matter!

- The written components of the game are important. Not only can they get you extra points, but they can also lose you points if you do a bad job.
- We reckon you should tackle the written questions when you are awake and alert (so just after you've had a sleep or some food). Explaining technical concepts to a non-technical person is hard enough when fully awake!
- We also suggest you give a written answer to a team mate to read before you submit it. If your team mates don't understand what you're going on about, then our non-techie assessor at CySCA Control probably won't either. Remember, these could get you a lot of points!

How do you win?

- Basically, players submit flags and answers to score points for their team, and the team with the highest amount of points is the winner.

- In the case of a tie (where two or more teams end up with identical scores), the team that captured their final flag first will be declared the winner.

Written submissions

- CySCA Control will mark the written answers at the end of the game to make sure
- So even if your team captures all of the flags, and even if you get there first, you won't necessarily be the winner.

Score updates during the game

- The scoreboard and progress information will be publicly available during the competition. You will be able to see what the current positions of the teams are and also what tasks a given team has completed.

When are the scores finalised?

- At the close of the game (12 noon AEST, 1 October 2015), the team scores as you'll see them on the score board are NOT final.
- CySCA control will then moderate the scores for the written tasks together to ensure the marks are consistent and fair.
- This means the score board from the end of the game may change (it has happened before!).

Getting set up

- So now you know how to win you need to know how to access the game!
- Teams will receive an information pack with support contacts, terms and conditions, login credentials and other relevant information.
- Plan, plan, plan. This is the best way to enjoy your experience! Okay, now onto the details…
- Each team will be given access to their own sandbox network. This means other teams can't mess with your environment and you can't mess with theirs.
- However, it does mean can mess with others in your team. Coordinate with your team to ensure you don't step on each other's toes!
- Players will use OpenVPN to connect their system to their team's sandboxed network.
- When you connect, you will get an IP in the network, allowing your machine to access the challenges.
- Teams will have an opportunity to test the VPN connectivity before the game, details for this will be provided in your player information packs.
- Test your VPN connection from the location you will be playing from BEFORE game day! If you lose time at the start of the game because you can't connect, you won't be given any extra time at the end of the day.
- Just so you know, by default, the OpenVPN configuration routes ALL traffic to the sandboxed network.
- This means you CAN'T access the internet from your machine at the same time as the VPN is connected.
- Plan for this! Have another way to search the internet and/or a plan for how to connect to the internet and download tools.

- We recommend installing your Kali VM in a virtual machine, and installing guest additions/VMware tools so that you can easily transfer files and tools while remaining connected to the VPN.
- Teams will be provided with a single logon account for the scoreboard that all team players can use to submit flags and answers.

Legal things

- The CySCA 2015 Terms and Conditions are on the website and will be in your information packs.
- READ THEM.
- You will be asked to accept the Terms and Conditions when you first login to the scoring site.
- Teams will again be able to choose their own name. However, any name deemed by CySCA Control to be derogatory, offensive, impersonating another university and/or containing swear words will be reset to your university name and team number.
- You will not get another chance to set it.
- The scoreboard is not part of the game. It's not in scope. Targeting it will result in your team being disqualified. If you are unsure, make sure you contact CySCA Control.

CySCA Control (or Challenge Control, formerly Exercise Control)

- CySCA Control will be available for the entire competition to troubleshoot any challenge related problems.
- Telstra's network support team will also be available for the entire competition to troubleshoot any issues connecting to the game environment.
- Both CySCA Control and Telstra will be co-located so if you're not sure who you need to speak to, we'll be able to get you an answer.