Cyber Security Challenge Australia

2014

cyberchallenge.com.au
CyberChallenge@pmc.gov.au
@CySCAExCon

Australian Government

Introductions

CySCA Supporters

- Australian Government
  - Australian Signals Directorate
  - The Department of the Prime Minister and Cabinet
  - Attorney-General's Department (CERT Australia)
- Telstra
- PwC Australia
- NBNCo
- Microsoft

What is CySCA?

- A cyber security competition for Australian university undergraduate and TAFE students
- Promote cyber security as an interesting and challenging career option
- Highlight the key skills required in a cyber security career
  - Ensure students are developing the skills we are seeking

Scenario

- Fortress Certifications Pty Ltd
  - Small start up specialising in Cyber assurance solutions
  - High risk of business failure if reputation is damaged by a compromise

Your Mission

- Perform a penetration test of the FortCerts web site
- Perform a penetration test of the FortCerts corporate network
- Conduct an analysis of a cyber incident involving a mobile phone running Android
- Analyse a number of products certified by FortCerts and confirm the validity of certification process

Challenge Components

- Four sub-challenges
  - Corporate Penetration Testing
  - Web Penetration Testing
  - Forensics
  - Certification Validation
    - Random
    - Reverse Engineering
    - Shellcoding
    - Software Code Review
    - Network Forensics
    - Crypto
    - Programming

Scoring

- Submit flags to score points and unlock mitigation questions for extra points
- Real time display of teams scores and progress
- Exercise control will review responses, in case of misuse or difficult questions
- Tie-breaker – first to score final flag wins

Team and Player Access

- Each team will be given access to their own sandbox network hosted by Telstra
- VPN access (OpenVPN) from your university to your sandbox network
  - Default routes will be pushed to disallow access to the internet. Plan for this.
- Flags and Answers are submitted through scoreboard website
  - Each team will get a login account to submit flags
  - Read the terms and conditions you have been provided. You will be required to accept them when you first login to the scoring site

Event details

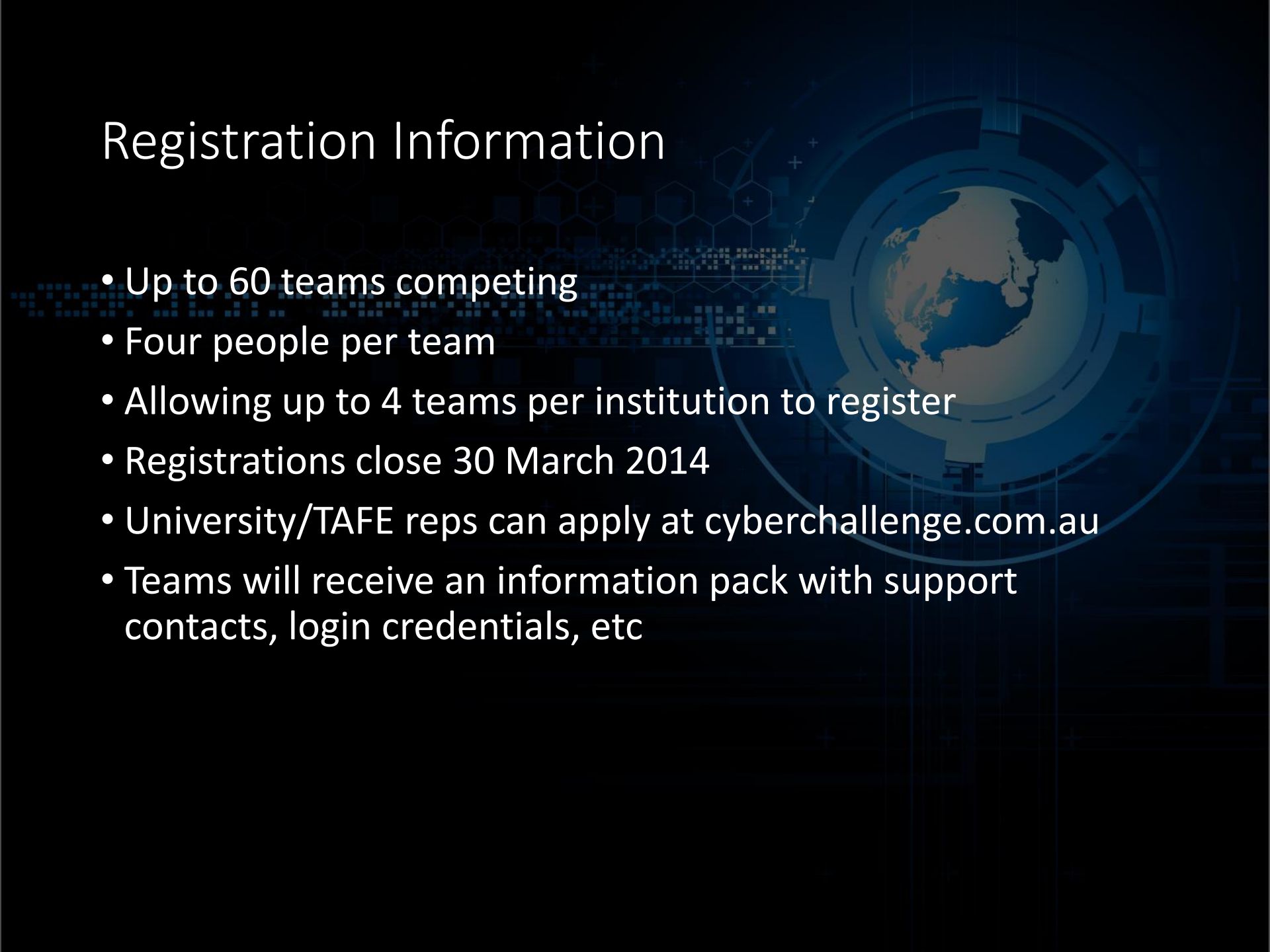
- CySCA 2014 will be held from (AEST) 12:00pm 7 May to 12:00pm 8 May 2014
- Exercise Control will be available for the 24 hours on IRC
- Telstra's technical support team will be available via phone or IRC

Prizes

Provided by Telstra

- 1st place
  - Trip to 2014 Black Hat Security Conference in Las Vegas USA
    - includes travel, accommodation and conference fees
    - Passports and US Visas are your responsibility
  - Sponsorship to attend award ceremony during 2014 Cyber Security Awareness Week
- 2nd and 3rd place
  - Players choice of a new tablet or phone

Registration Information



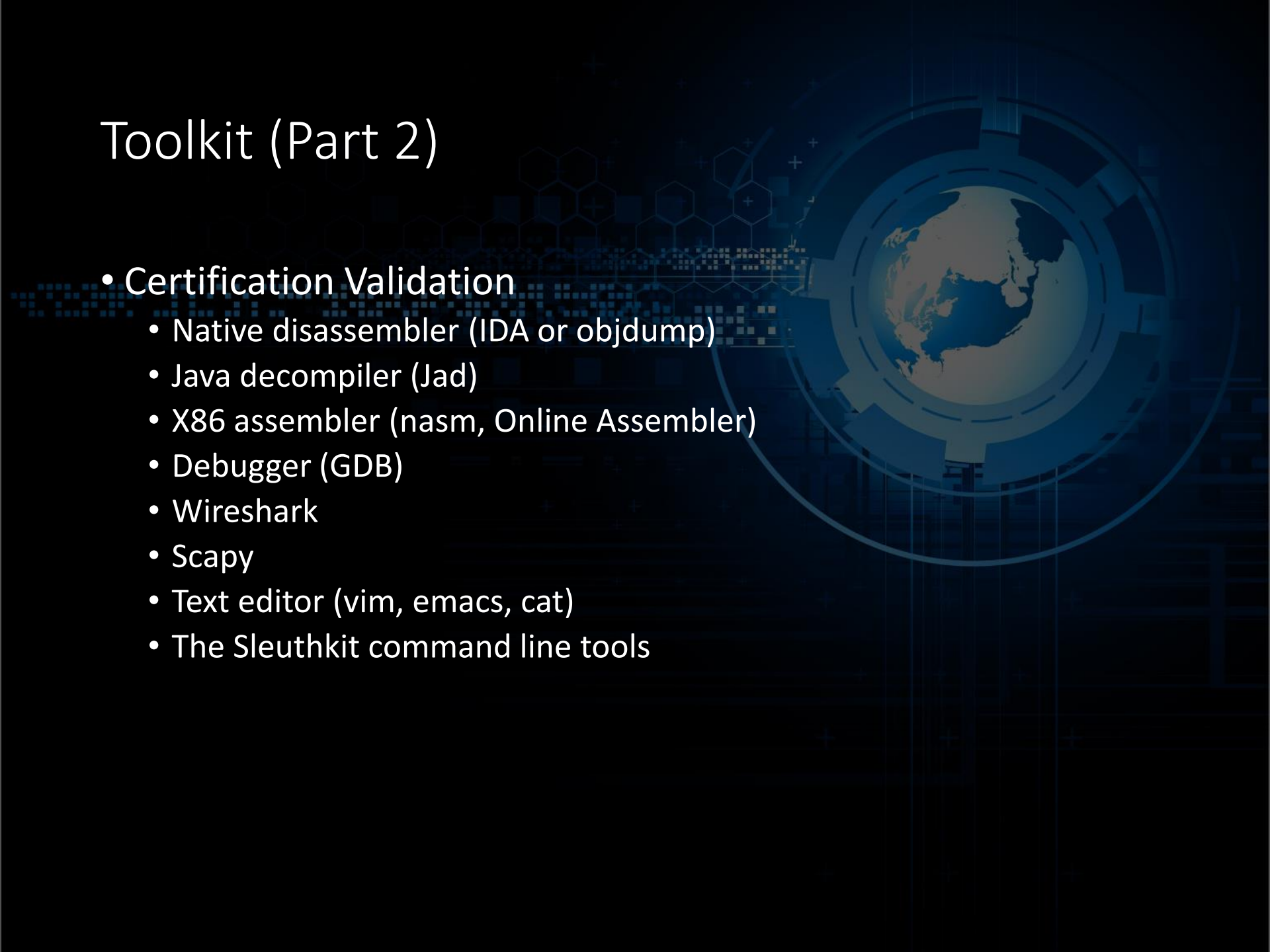
- Up to 60 teams competing
- Four people per team
- Allowing up to 4 teams per institution to register
- Registrations close 30 March 2014
- University/TAFE reps can apply at cyberchallenge.com.au
- Teams will receive an information pack with support contacts, login credentials, etc

Preparation

Toolkit (Part 1)

- Get comfortable using these tools!
- Kali 1.0.6 (32bit)
- Corporate Pen Test
  - Metasploit
  - Sysinternals tools
- Web Pen Test
  - Burp suite
  - SQLmap
- Forensics
  - Volatility

Toolkit (Part 2)



- Certification Validation
  - Native disassembler (IDA or objdump)
  - Java decompiler (Jad)
  - X86 assembler (nasm, Online Assembler)
  - Debugger (GDB)
  - Wireshark
  - Scapy
  - Text editor (vim, emacs, cat)
  - The Sleuthkit command line tools

Practice makes perfect

- Best way to prepare is to participate in other CTF events
- Last years official CySCA writeups
  - https://cyberchallenge.com.au/CySCA2013_Solutions_Writeup.pdf
- ctftime.org
  - Upcoming CTF schedule
  - Previous CTF event write-ups – CSAW, PlaidCTF, CodeGate
- picoctf.com
  - Almost perpetual CTF
  - Challenges still available
  - Includes introductory resources

Day in the life…

- Internships available this summer 2014
- 2015 Defence Intelligence and Security Development Program – closes 7 April 2014

Apply at the website

asd.gov.au/careers

Link Spam

- Corporate Penetration Testing Links
  - http://www.offensive-security.com/metasploit-unleashed/Main_Page
  - http://www.irongeek.com/
  - Encyclopaedia Of Windows Privilege Escalation - http://www.youtube.com/watch?v=kMG8IsCohHA
  - https://cyberchallenge.com.au/CySCA2013_Solutions_Writeup.pdf
  - https://github.com/pwnies/pwntools
- Web Penetration Testing Links
  - http://www.amanhardikar.com/mindmaps/Practice.html
  - http://sourceforge.net/projects/mutillidae/
  - https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
  - https://cyberchallenge.com.au/CySCA2013_Solutions_Writeup.pdf
- Forensics Challenge Links
  - http://code.google.com/p/volatility/wiki/AndroidMemoryForensics
  - https://tzworks.net/prototypes.php
  - https://digital-forensics.sans.org/summit-archives/2012/android-mind-reading-memory-acquisition-and-analysis-with-lime-and-volatility.pdf
  - http://stackoverflow.com/questions/2451384/creating-an-image-of-an-android-phone
  - http://www.utdallas.edu/~anf061000/Digital%20Forensics%20and%20File%20Carving%20on%20the%20Android%20Platform.pdf

Link Spam (The Rest)

- http://myne-us.blogspot.com/2010/08/from-0x90-to-0x4c454554-journey-into.html
- http://code.google.com/p/it-sec-catalog/wiki/Exploitation
- http://www.overthewire.org
- https://cyberchallenge.com.au/CySCA2013_Solutions_Writeup.pdf
- https://code.google.com/p/bletchley/wiki/Overview
- http://ppp.cylab.cmu.edu/wordpress/
- https://isisblogs.poly.edu/
- http://eindbazen.net/
- http://security.stackexchange.com/questions/3592/what-hacking-competitions-challenges-exist
- http://fumalwareanalysis.blogspot.com.au/p/malware-analysis-tutorials-reverse.html
- http://www.webantix.net/2009/08/war-games-current-and-past-hacking.html