

Symantec Cyber Readiness Challenge

Black Hat Webcast – June 20, 2013

Michael Garvin, Senior Principal Security Analyst
Information Security Services



What is the Cyber Readiness Challenge?



Symantec.

Cyber Readiness Challenge

PROTECT AND PREVAIL



An offensive (red team) capture the flag style event, inspired by real-life security issues to help understand the vulnerabilities in today's global threat landscape and to gain critical security intelligence to improve security posture.

Why Are We Doing It?

"Know both yourself and your enemy and you can win a hundred battles without jeopardy."

- Walk in our adversary's footsteps to understand motivations
- Understand the five stages of a cyber attack –
Reconnaissance, Incursion, Discovery, Capture and Exfiltration
- Develop and practice offensive skills to aid in defense
- Apply knowledge and experience to real-world problems

23 Events in 21 Locations to Date



Cyber Readiness Challenge Experience



Cyber Readiness Challenge Online



Self-contained, online cyber range accessed via provided VPN

Cyber Readiness Challenge Online

The screenshot shows a web browser window with the URL 'Symantec CRC'. The navigation bar includes 'Home', 'Progress', 'Settings', and 'Sign Out'. The main content area is divided into several sections:

- LEVEL 1 0 / 10**: A progress indicator for the current level.
- The Game Name**: A section header for the current challenge.
- YOUR POINTS**: A section showing the current score, which is **0**.
- TIME LEFT**: A section showing the remaining time, which is **2 hrs 6 mins**.
- Level 1 - The Game Name**: A large text area containing introductory text about the challenge's objectives and realism.
- Flag1**: A section for a specific challenge, worth **300 pts**. It includes a description of the flag, a 'Submit Flag' button, and three hint buttons labeled **Hint 1**, **Hint 2**, and **Hint 3**.

Objective driven, progressive capture the flag style event

Cyber Readiness Challenge Online

The screenshot shows a web browser window titled "Symantec CRC". The navigation bar includes "Home", "Progress", "Settings", and "Sign Out". On the left, a "TIME LEFT" box shows "2 hrs 6 mins". The main content area displays three flag questions:

- Flag1** (300 pts): "This is a flag! It will ask specific questions about the system(s) you are playing against. Answers to the flags can be found by using a wide range of ethical hacking skills and techniques. The games are designed to allow all levels of players to participate. Level 1 starts with flags that a general IT professional can answer, all the way up to harder flags in later levels to test more advanced information security and ethical hacking professionals." Includes a "Submit Flag" button and "Hint 1", "Hint 2", "Hint 3" buttons.
- Flag2** (500 pts): "Flags can have one of three difficulties, easy, medium and hard. Each one has a different point value ranging from 300 up to 1000." Includes a "Submit Flag" button and "Hint 1", "Hint 2", "Hint 3" buttons.
- Flag3** (1,000 pts): "A flag can fall into one of Symantec's five stages of a cyber attack, reconnaissance, incursion, discovery, capture and exfiltration. Different techniques and tools will be required for each stage." Includes a "Submit Flag" button and "Hint 1", "Hint 2", "Hint 3" buttons.

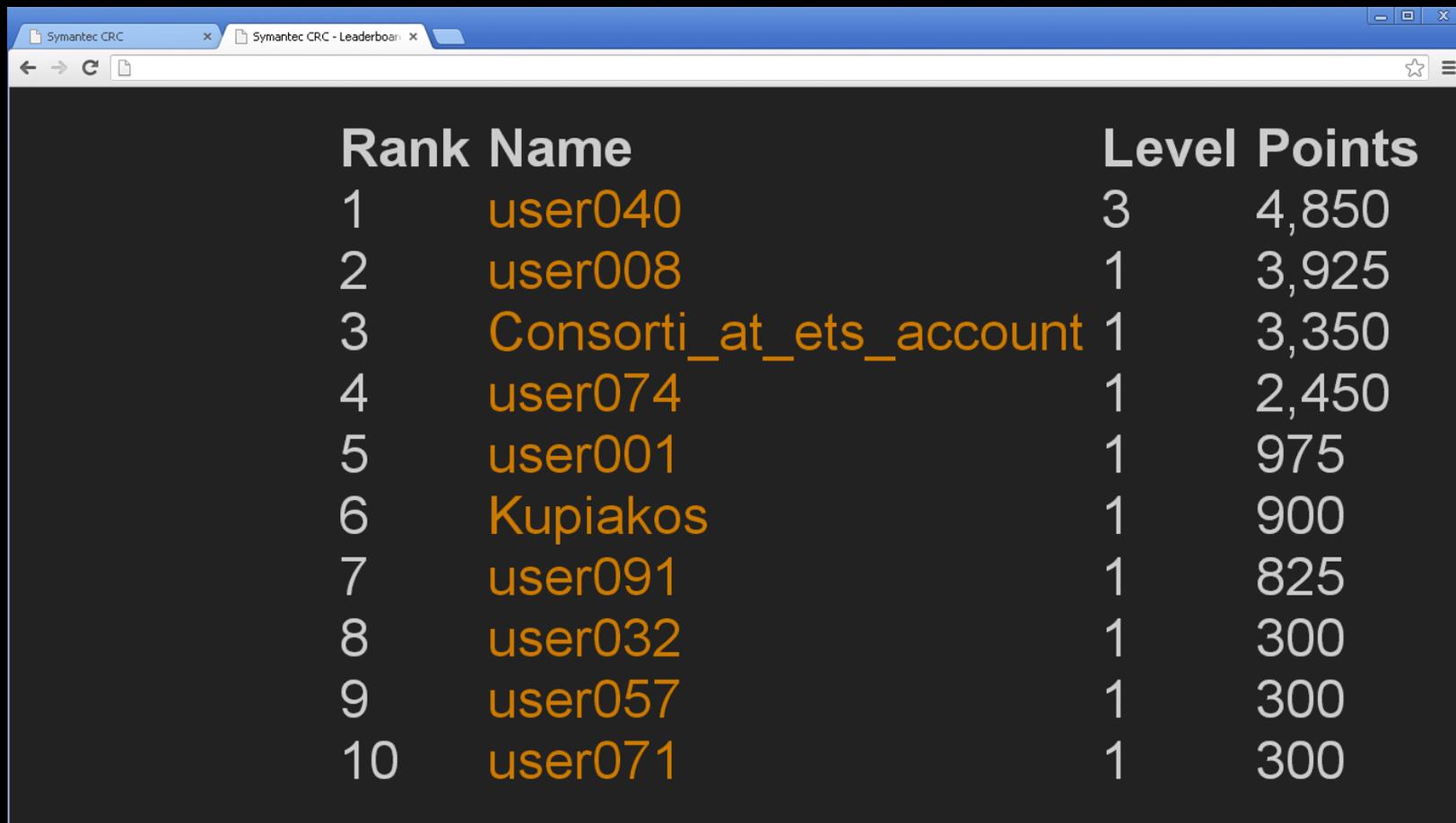
Flags across difficulty levels and skill domains

Cyber Readiness Challenge Online

The screenshot shows a web browser window titled "Symantec CRC". The navigation bar includes "Home", "Progress", "Settings", and "Sign Out". On the left, there is a "YOUR TEAM" section with a "player1" button and a "TIME LEFT" section showing "1 hr 59 mins". The main content area features a "Flag1" challenge worth 225 points, indicated by a green progress bar. Below the flag description, there are "Submit Flag" and "Hint 1", "Hint 2", "Hint 3" buttons. A tooltip for "Hint 1 Revealed" is displayed, stating: "You can take hints along the way if you get stuck, they will however reduce your total points available". Below this, a "Flag2" challenge worth 500 points is partially visible, with an orange progress bar and similar "Submit Flag" and "Hint" buttons.

Hints support varying skill levels and learning

Cyber Readiness Challenge Online



Rank	Name	Level	Points
1	user040	3	4,850
2	user008	1	3,925
3	Consorti_at_ets_account	1	3,350
4	user074	1	2,450
5	user001	1	975
6	Kupiakos	1	900
7	user091	1	825
8	user032	1	300
9	user057	1	300
10	user071	1	300

Leader board with top rankings

Register and Participate



Registration

June 20, 2013 – July 26, 2013, and onsite

Event

24x7 Noon PT Monday,
July 29 – Noon PT
Thursday, August 1, 2013

go.symantec.com/cyber-readiness