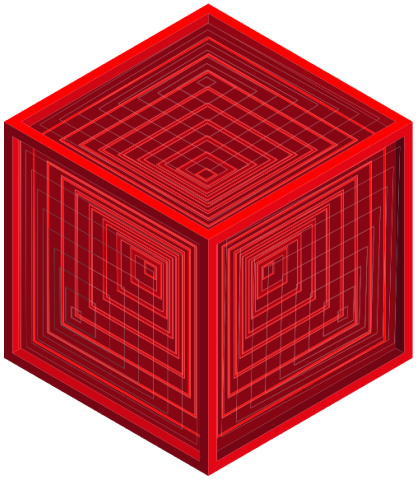

#HITB2013KUL

CAPTURE THE FLAG

WMD: WAR OF THE WORLD

TEAM HANDBOOK

Table of Contents

Terms & Acronyms

Term/Acronym	Definition
Government Center	Daemons that generate HP for players' countries
Finance/Business Center	Daemons that generate and add more cash to players' countries
Firepower	Attack damage that will be dealt to opponent's country's HP

Previously at #HITB2012KUL CTF

In our previous CTF (Fallout Apocalypse), each team had a set of daemons (called the Reactor Cores, or RC) running on their machines. Every solved RC granted the solving team with a Weaponized SCADA Exploit (WSE) that can be used to damage rival teams' RC. Teams could also bid for exploits of certain RC on the Black Market using the currency LeetCash (LC). Each team started with an equal amount of LC and they generated LC by keeping their RCs up and running.

Overview

In WMD: War of the World (referred to as WMD:WotW), each team will be given a country and they are required to protect their daemons that represent the Government Centers (GC), Finance Centers (FC), and Business Centers (BC). They are also required to launch attacks against rival teams' countries. Teams will also be given side challenges (from categories such as forensic, reversing, network analysis (pcap), steganography and cryptography) that can be accessed by solving daemons. Nukes that are capable of completely destroying a rival team's daemon can be unlocked by solving bonus challenges.

Each team will start the game with an equal amount of HP. The HP can be regenerated back to 100% by keeping their GC daemons up and running. Teams will also have FC and BC daemons that generate cash. Cash generated can be used to buy shields and to repair any damaged daemons. Cash can also be earned by solving daemons and challenges. Firepower is required in dealing damage to a rival team's HP.

By solving a daemon, a team will be granted cash and access to challenges. Teams will have to use firepower obtained from solving challenges to attack rival teams. Each challenge has its own level relative to the level of the daemon (E.g.: daemon 1 unlocks challenge 1 and so on). Damage dealt by firepower will be determined by the levels of challenges solved, such that:

- Challenge for daemon 1 = firepower level 1
- Challenge for daemon 2 = firepower level 2 and so on

Also, each team will be given a bonus challenge that can only be solved once. Solving a bonus challenge grants nuke that can be used to cause "total loss" to a particular daemon. A daemon that is in the state of "total loss" must be rebuilt instead of the regular repair. Once a GC daemon has been attacked, it will stop generating HP and must be fixed for it to function again. If a team's HP reaches zero (0), the team will be automatically eliminated from the game (how can one country fight if its government has fallen?). For defensive measures, teams can use shields to reduce the impact of firepower, except for nuke, which always causes "total loss" to a particular daemon.

At the end of the competition, the team with highest HP will be the winner of the war. In case of two different teams having the same HP amount, whoever sustained the HP value the longest till the end of the game will be the winner. Hence, teams must keep their GC daemons up and running at all times. The CTF network will be isolated from the rest of the conference network, and we will NOT provide Internet on the CTF network. However, you are free to use the HITB conference wireless network.

Game Format

- WMD: WotW is and Attack & Defend CTF.
- The objective of this CTF is to be the country with the most HP.

Scoring System

- **Each team starts with 100% HP**
- **Attacking:**
    - Firepower = attack damage
    - Attacks will damage daemons based on firepower levels.
        - Higher-level attacks deal higher damage to a daemon.

- **Nukes**
    - Can only be used once.
    - Deals "total loss" to daemons.
    - Daemons attacked by nukes will have to be rebuilt.

- **Shield**
    - Reduces the impact of attack (except for nuke)
    - Defends the daemons based on level of the shields:
        - If attack level > shield level: damage dealt will be reduced by level difference.
        - If attack level == shield level: Zeroes out both.
        - If attack level < shield level: Shield level will be reduced by level difference.

- **Defensive points**
  - Up and running GC daemons generates HP
  - Point reduction will be determined by the damage done on GC:
    - Higher damage on GC == reduces more HP
    - Last damage level = daemon down = minus daemon total points. (Need more details)
  - In case of nuke:
    - Rebuild!!! (Requires longer time than the usual repair)

- **Cash daemons and Cash**
  - Do not affect the HP of a team.
  - Finance Center daemons
    - Generates base cash.
    - Suffers level based damage, just like GC daemons.
  - Business Center daemons
    - Add cash by fixed increment rate
    - Always suffer full damage regardless of the firepower level.
    - Will not function if FC daemons are not running.

Government Centers

- Daemons that generate HP for a team
- Solving these unlocks additional challenges that give firepower.

Finance Centers

- Daemons that generate cash for repairing and buying shields.
- Finance center daemons generate base cash, and suffer damage based on the firepower level of the attacker.

Business Centers

- Daemons that generate cash according to a fixed rate.
- Suffer full damage regardless of the attacker's firepower level.
- Will only function when finance centers are up and running.

Rules & Regulations

- Show up in time or you'll miss the briefing
- No off-the-shelf automated scanning tools such as Nessus, OpenVAS etc. It's useless and we'll kick you out for that lame ass shit.
- No flooding and / or DoS attacks.
- No ARP spoofing.
- No physical attacks against other players.

- All participants must obey to PIT STOP calls. PIT STOP calls are rest intervals where all the players must leave the CTF area to facilitate for the CTF Crew to perform maintenance work.
- Teams who don't adhere to the rules will be penalized or disqualified from the competition.

Prizes

TBA – SEE CONFERENCE WEBSITE:
http://conference.hitb.org/hitbsecconf2013kul/event/capture-the-flag/

Contact

Email: ctfinfo@hackinthebox.org