

Week 4 discussion

[Technology, Information Technology](#)



Running Head: Designing Cyber Competitions. Department Question Cyber exercises provide a useful learning experience to students studying computer sciences especially at college and university levels. Competitions can be organized periodically within or between universities under monitored conditions on issues such as security. The main objective is for students to acquire hands on and experiential skills on information security. The design of these competitions is a complex task requiring the input of different minds as well as consideration of a number of pertinent issues. It is therefore very important that we understand the issue to consider when designing the exercises.

One important issue of consideration is the structure and approach of the competition. There is need for adoption of a uniform structure throughout the exercise as this presents participants with a level playing ground. Any exercise must have certain objectives to be met and as such defining objectives is important in designing cyber competitions. The kinds of equipment to be used in terms of hardware and software as well as approach to be taken are important issues in cyber exercises. These are heavily dependent on the objectives set for the competition. It is very important to decide the overall topology over which the competition is run keeping in mind the available/chosen equipment for the exercise.

The next consideration after deciding on the topology is to formulate the exercise scenario, come up with rules to govern the competition and also define the metrics for evaluating the competition's efficiency basing on the set objectives. There should also be a methodology with which to gather lessons learned from the simulation by both the participants and organizers.

a very important consideration is defining the entities to make up the competition; generally, competitions on cyber security have two sides i. e. the attacking site & the defense side. Every side has systems which are managed by participating teams and each side should have at least a system to facilitate participation in the competition.

Question 2

In order to protect any web application from vulnerabilities and threats of attack, a comprehensive understanding of every communication by the application is required. This is because the security solution/device must be able to see data in the same way as the application to be protected in so as to map out areas of threat. In other words, security devices must be in the position of performing complete deconstruction of HTML data play sessions and monitor all applications sessions in order to secure the application. It is my opinion that deploying firewalls is the best way to protect web applications of critical importance.

Firewalls for protecting web applications operate at the level of application layer as opposed to many other security solutions which operate at the level of network. They are therefore able to terminate all the sessions of the application and carry out a complete bi-directional audit on all the applications data. Through inspection of actual HTML communication, reading all user requests in the application as well as responses by the application as well as the contexts in which they reach the Web servers, application firewalls are able to enforce appropriate behavior of the application and deter any malicious action. One very common for carrying out scripting attacks is by injecting malicious scripts through HTML form

fields. Implementation of application firewalls is the only security solution able to detect, prevent and even defeat such malicious actions on crucial web applications.

References.

1. Victor-Valeriu Patriciu and Adrian Constantin Furtuna. (2008). Guide for Designing Cyber Security Exercises.