Impact of InCTF in Security Education

Anu V
Department of Computer Science
Amrita School of Engineering, Amritapuri
Email: anuv.1994@gmail.com

***Abstract*—Security education is not a part of the undergraduate curriculum in India. Its because of this reason people are unaware of the applications of security vulnerabilities which result in the creation of insecure applications. Due to this reason, many Indian websites are compromised frequently. This paper describes InCTF, Indias first CTF style ethical hacking contest which helps in augmenting security education, both theoretical and practical.**

Keywords*—Compromised websites, Security education, Capture the flag, ethical hacking, beginners

I. Introduction

Many Indian websites have been compromised frequently in the past few years. A steady increase was found in the occurrence of such security breaches from 2004 to 2009. The mission of tracking the defacements of Indian websites were done by Computer Emergency Response Team India (CERT-In). And 6023 defacements were tracked in 2009 [3]. The websites with .in domain were found to be defaced more . A sum total 3042 .in domain websites were defaced. And several more web sites probably exist which were compromised but not documented [3].

Lack of security awareness is one of the key reasons behind this staggering number of security breaches. Application designers seldom follow secure coding practices while designing applications. They fix bugs when a problem arises rather than preventing the occurrence by writing secure codes.

This problem arises because security education is not emphasized in their undergraduate education. Despite the fact that need for computer security has increased greatly and the availability of several tools to teach security concepts, security education is not prevalent in India. Students tend to restrict themselves to theoretical knowledge [4, 5, and 6] and computer security can never be fully understood with theoretical knowledge alone.

Computer security competitions and challenges are an excellent method to foster innovation and educate students about computer security in a highly-motivating environment [7]. They are practical and if crafted properly, provide the right amount of realistic scenario to facilitate learning of security principles and vulnerabilities. Amrita University has been a pioneer by participating in various international CTF contests over for the past years and incidentally the only one from India to do so. In 2010, Amrita University conducted India's first national level CTF style ethical hacking contest InCTF. Conducted by the team of students who represented Amrita University in the international CTF contests, the event was a phenomenal success. Another edition of the event was organized in the following year, which was as successful as the previous edition. This paper describes these two competitions and what sets InCTF apart from other contests of the same kind.

II. Related Work

In the past, security exercises have been held in India in conjunction with security conferences. The events usually come with a fee to attend, which was not affordable for students. There was no platform where the students could improve their security skills for free. Also, such contests are usually focussed on a particular area such as web security where participants had to exploit vulnerabilities in a web application and the realism involved in such events is quite less. These contests required physical presence and students are often unwilling to travel due to academic or other commitments.

Several CTF style ethical contests especially for students are organized annually such as iCTF by University of California, Santa Barbara [1, 2], Collegiate Cyber Defense Competition [4] and CIPHER CTF by RWTH, Aachen, RuCTF and RuCTFe by Ural State University. However, not all of these contests are international contests. And the international contests are not beginner friendly and participation in these requires previous knowledge of advanced security principles and vulnerabilities, of which there is a lack in India. This was probably the reason for a lack of participation of teams from India in such competitions.

Eventhough several security exercises existed, they didnt suit the present scenario in India. Hence, a different well tailored format was created which suited the present Indian scenario. In the following sections, we present two CTF style ethical hacking contests organized in 2010 and 2011, the outcomes, learning and challenges involved in organizing them.

III. The Contest

The contest was conducted in two editions in 2010 and 2011, both by Amrita University and TIFAC CORE in association with VeriSign. The format of both the events weren largely the same, no much changes were made. In the second edition only a slight variations were made. Both of the events are briefly described separately.

A. InCTF 2010

The contest featured 290 teams from 150 premier institutions, including IITs and NITs, from 19 states. This was truly a rare achievement for any contest of this kind in India. It was held from February 2010 to March 2010.

1) First Round: Learning Round: Almost all CTF contests require participants to have prior knowledge of security vulnerabilities and principles. This however is not the scenario in India where majority of the students have little or no exposure to the same.

The first round was specially designed to address this issue. The round highlighted what would eventually be useful in later stages of the contest. The set of tasks exposed the student to basics of Linux, networking, Apache, PHP, SQL, cryptography, phishing, secure coding and cyber laws. On completion of this learning round, students were equipped with knowledge that enabled them to perform better in subsequent rounds as well as become confident that they can indeed make a mark in this contest. This was a radical departure from traditional CTF's, which serve as a finishing test for information security courses.

2) Second Round: Web Application Exploit: The second round was a web application exploit round. It was modelled on the format of the popular online hacking and security web site Hack This Site's basic missions. Popular exploits such as SQL injection, Javascript injections etc. were among the flaws of the web application.

Participants had to penetrate into a vulnerable web application and points (100, 250 or 500) were awarded for each vulnerability they discovered. Timestamps were used to resolve ties, if any. 30 teams qualified to the final round.

3) Final Round: Network based CTF style contest: The final round was held in February, 2010. 30 teams from across India participated in the 5 hour long round. The round was played over a Virtual Private Network and each team was assigned an IP address range.

Each team had a copy of the vulnerable machine in a virtual environment such as Virtual Box and their goal was to discover and fix vulnerabilities as well as exploit the machines of other teams using the same. The ethical element was ensured by not scoring any flag submissions during the initial period and instead encouraged teams advisories highlighting vulnerabilities and how to fix them. These advisories were publicly visible, which was visible to all teams. Thus, all teams could look at submissions and apply the suggested patches to their vulnerable machine. Points were awarded tothe advisories submitted depending on the quality of the advisory, the vulnerability reported and the proposed fix for the same.

The following table lists the teams who finished in the top three places of InCTF 2010.

IV. Conclusion

Security education is not prevalent in India and that is the important reason why several Indian websites are compromised on a regular basis. The key reason is lack of emphasis on security education, both theoretical and practical, in the courses all over India. By hosting InCTF for couple of consecutive years, several students have been exposed to security principles, vulnerabilities and the need for security in today's world. Thus live security exercises are a useful tool to augment and spread security education.

A CTF contest can only augment what has already been learnt but can never replace the formal training. Security education requires to be included in the curriculum in order to be effective. Nevertheless, a third edition of the event has been scheduled to take place later this year. We are hoping that the contest reaches far and wide thus exposing several students security vulnerabilities and security practices and eventually security education will be made part of the undergraduate curriculum

Acknowledgment

Thanks to official hacking team of Amrita University (Team bi0s) for reviewing this paper.

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.