Search: GO

- Front Page
- Blog Posts
- Resources
  - Downloads
  - Whitepapers
- Media
  - Videos
  - Whitepapers
  - Visit SecurityWeek.Com

- Login
- Register for Free

Can CTF Players Replace Professional Penetration Testers?

Wednesday, September 23, 2015
Contributed By:
Ilia Kolochenko

I have been asked by several friends who are CISOs within different organizations if Capture the Flag (CTF) experience makes any difference in how I evaluate incoming CVs for internal IT security auditor or similar positions. This complicated question is also one that I ask myself each time I consider incoming CVs for new penetration tester vacancies that we have.

According to ISACA’s State of Cybersecurity: Implications for 2015 report, 72.33% of respondents said that the biggest skill gap in today’s security professionals is *ability to understand the business*. Another interesting fact from the survey is that the majority of respondents found that less than 25% of applicants were qualified for a cybersecurity position. These numbers highlight a very serious gap between people looking for an infosec job and modern businesses. A similar gap also exists between

CTF contests and professional penetration testing.

Unlike when I was a student, today one can easily find a great variety of CTF events of all sorts and types, from the easiest tasks to complicated reverse and crypto challenges. However, many CTFs are organized by security enthusiasts and their main audience are students or newbies who want to try their offensive security skills in the wild without breaking the law. Even at famous CTF events, usually organized in parallel with various conferences, many CTF players are students or have just started their first infosec job. Sadly, quite often prominent teams of young but talented players fail to participate in a CTF due to the high price of travel and the events being held in venues they simply cannot afford. This is why online CTFs have become more and more popular. Many security companies of different sizes organize or sponsor CTFs in order to attract media attention and recruit the most prominent players. Let's try to understand what impact CTF experience may have on one's habitudes, technical skills and cybersecurity career.

During weekends, I like reading CTF write-ups from time to time, especially those that cover web security challenges. However, I remember very few of them covered real business case scenarios that professional penetration testers face every day. I obviously omit sophisticated crypto challenges, car hacking, phreaking, ATM hacking and non-security challenges that CTF organizers set up to bring some fun to the event. But even the remaining part is still pretty far from daily reality. So, what is the practical difference between CTF and penetration testing, and what impact can it have on a business?

The first issue with the majority of CTFs is that they focus on single result (flag), rather than a process of comprehensive consecutive security testing. I saw many cases when a penetration test, conducted by CTF players, consisted of exploiting one single vulnerability to facilitate exploitation of all others. The upcoming report contained quite irrelevant information, such as demonstration of web application source code and databases obtained via brute-forced FTP password or arbitrary file upload vulnerability. At the same time simple SQL injection vulnerabilities in web services were not even mentioned in the report, as penetration testers considered that 'capturing the flag' via getting all confidential information from the server is enough to impress the customer. In reality, very few customers are ready to pay for such service, as it has very low (if any) value from the business' point of view.

The second concern is that very few CTFs offer technical infrastructure similar to a real business environment. CTF is about hacking a deliberately insecure system intentionally left vulnerable, while a penetration test is about testing a complicated system that a team of cybersecurity professionals tries to keep secure. The way of thinking during a CTF and a penetration test is totally different. Being in a 'pentest mode' you will hardly solve even the easiest CTF challenge and vice-versa: during a CTF you usually look for direct or indirect hints as to the logic of the task's creator, while during a penetration test you need to entirely understand the business' logic and global cybersecurity vision, and the strategy of your customer.

The next problem one may face is the security tester's responsibility when selecting attack methodologies and techniques. What would happen during a CTF if you suddenly or deliberately crashed the system, making others unable to test it? In the worst case, your team would lose some scoring points. During a penetration test, such imprudence may cost your customer millions of dollars. A similar problem also exists in some car racing games that provoke imprudent driving in reality.

Scope of testing is also very important: at High-Tech Bridge for almost every penetration test, we have some special business requirements in terms of scope and perimeter of testing. A penetration test is process oriented, while CTF is mainly result oriented. Customers are usually aware that, for various business and operational reasons, some components of their IT infrastructure are vulnerable, and they are not ready to pay to have that fact reported on paper. Instead,- they hire us to test the resistance of the secure part of their infrastructure, while patching or migrating the vulnerable ones. For a penetration test, it is very important to clearly define what to test and how to test, otherwise you will likely just irritate your customer. I saw several cases when professional CTF players were not able to control their behavior during a penetration test, as they used to have 'no limits' taking the entire process as a game. Despite the "got root" results they had, their customers were about to sue them for attacking wrong systems.

Yan Borboën, Partner at PwC Switzerland, MSc, CISA, CRISC, shared his opinion about the subject: "With the increasing number of attacks in the world, companies need to recruit well trained people.

CTF is an extraordinary game field for people to train and to demonstrate their motivation.

At PwC, we sponsor security competition as Swiss Cyber Storm Security challenge because it is clearly an opportunity to identify and recruit talent. However, technical capabilities is only one aspect of a penetration test and will provide assurance against common everyday attacks, they do not provide assurance against more sophisticated and persistent attacks.

To provide real value to our client, we would rather recommend intelligence led security testing (e.g. CREST STAR), which incorporates threat intelligence and penetration testing to replicate accurately a full scenario of a targeted attack against an entire organisation including people, processes and technologies."

Therefore, when hiring a new team player, I would definitely prefer an experienced penetration tester to a CTF champion. However, with all other equals, a CTF experience may definitely be a good added-value. CTF helps to develop and to perfect stand-alone technical skills and exploitation techniques. A CTF player can also bring some useful insights to your team and a vision from a different angle that others will probably not have.

Nevertheless, we should always keep in mind that CTF is a game, while penetration testing is a business. Don't confuse the two.

About the Author: *Ilia Kolochenko is CEO & President at High-Tech Bridge and* and Chief Architect of ImmuniWeb. *Hehas a university degree with honors in Mathematics and Computer Science from Geneva, his city of origin. Ilia Kolochenko started his career as a penetration tester, he also was a security expert and team leader working for various financial institutions and large companies in Switzerland and abroad. His military service in artillery troops took place in Frauenfeld, Switzerland. At the end of 2007 he founded High-Tech Bridge, aiming to deliver efficient and effective penetration testing to companies of all sizes. In 2010 Ilia Kolochenko created a concept of hybrid security assessment of web applications, called ImmuniWeb, that was globally launched in 2014. Being web application security expert and chief architect of ImmuniWeb, he is personally involved into ImmuniWeb's daily operations, implementing new features and functions.*

Share This! |

Possibly Related Articles:

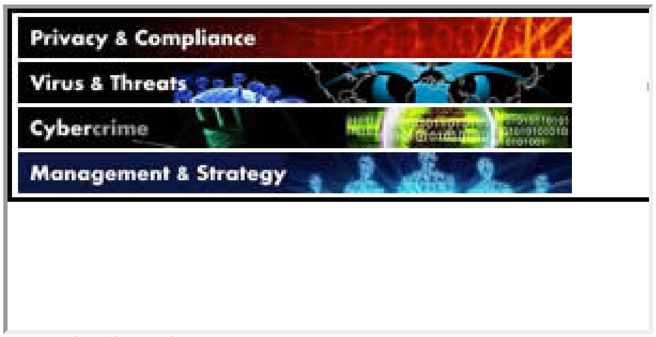
- ICS-CERT: Siemens Simatic WINCC Multiple Vulnerabilities
- The Chilling State of Cyber Affairs (US DoD Report)
- BlackHat 2012: Alexander Polyakov on New SAP Vulnerabilities
- Guess Who's Not going to Black Hat Europe 2012
- What We Know About Shellshock and Why the Bash Bug Matters

Views:	1429
Categories:	Enterprise Security Security Awareness Security Training Vulnerabilities
Tags:	Exploits Security Pentesting cyber CTF Capture the Flag contest

Post Rating I Like this!

Comments:

The views expressed in this post are the opinions of the Infosec Island member that posted this content. Infosec Island is not responsible for the content or messaging of this post.



Most Liked

Latest Member Comments

> *"Fast And Furious 7 Full Movie Online Watch http://www.mastimovie.net/fast-and-furious-7-full-movie-online-watch/ Fast And Furious 7 ..."*

PoS Malware Kits Rose in Underground in 2014... *on 03-17-2015*

> *"Fast And Furious 7 Full Movie Online Watch http://www.mastimovie.net/fast-and-furious-7-full-movie-online-watch/ Fast And Furious 7 ..."*

New PCI Compliance Study... *on 03-17-2015*

> *"Fast And Furious 7 Full Movie Online Watch http://www.mastimovie.net/fast-and-furious-7-full-movie-online-watch/ Fast And Furious 7 ..."*

PCI Security Standards Council Statement on ... *on 03-17-2015*

> *"Fast And Furious 7 Full Movie Online Watch http://www.mastimovie.net/fast-and-furious-7-full-movie-online-watch/ Fast And Furious 7 ..."*

16 Million Mobile Devices Infected With Malw... *on 03-17-2015*

Latest Posts

- Can CTF Players Replace Professional Penetration Testers?
- 3 out of 4 Consumers Will Leave your Websites Because of Security Concerns
- Red Hat Warns of Ceph Website Breach

- The 2015 ICS Cyber Security Conference
- FS-ISAC to Share Threat Intelligence With Federal Reserve Banks
- BYOx: Developing and Deploying Effective Strategies to Safeguard Data
- Beware of the Imitations
- Similar Threats, Different Reponses: Report
- Wireless Security 101
- Webcast: Segmentation Beyond VLANs, Subnets, and Zones

Home | Articles | Downloads | Blog Posts | Contact Us | Register for Free | About Us | Privacy