# Organising Monkeys or How to Run a *Hacking* Club

Andreea-Ina Radu, Sam L. Thomas
School of Computer Science
University of Birmingham
Email: {A.I.Radu, S.L.Thomas}@cs.bham.ac.uk

***Abstract*—We describe the organisation of the University of Birmingham hacking club, and associated Capture The Flag team, AFiniteNumberOfMonkeys (AFNOM). We detail the difficulties involved in running such a club and how we attempt to overcome them.**

***Keywords*—*offensive security, cyber-security education, collaborative learning, student engagement***

## I. Introduction

The hacking club at the University of Birmingham, AFiniteNumberOfMonkeys (AFNOM) was founded in 2012 by Dr. Tom Chothia [1] and Dr. Marco Cova [2] and currently has approximately 20 members. In 2014, we have been ranked first UK academic team and 33rd world-wide. The members of the club get together every week to look at offensive hacking and cyber-security. We believe that understanding threats and how attackers think is the best way to keep computers secure.

In our experience, enthusiasm and perseverance have proven to be the key factors for running our hacking club and CTF team. Through low or high attendance, we keep preparing and organising meetings and taking part in competitions. And we believe our past year's results show our strategy is successful.

In this paper we will describe how our club is organised, what major challenges we face and how we tackle them, and what does competitive hacking mean.

## II. Organisation

The hacking club is overseen by a senior lecturer of the Computer Science department. The group has an organiser who is responsible for overall management and reports it to the senior lecturer. The organiser also takes care of resource management, venue and competition registrations. There is a network administrator who arranges the network equipment (routers, switches, Wi-Fi, laptops) and deals with other technical issues during meetings and competitions. The website designer keeps our website [3] up to date, adds resources and the write-ups fellow members provide at the end of competitions. There are also two people responsible for finding new hacking challenges. They need to search the internet for suitable exercises for the upcoming meeting. While these responsibilities are assigned to certain members of the club, sometimes they cannot fulfil them (due to workload) and others step in, in order to insure the sessions run as expected.

It is important for a club to build an identity and allow members to express their affiliation with it. In this respect, we have designed and acquired hoodies which have the AFNOM logo and members nicknames. This action has been very popular and met with enthusiasm by our members who proudly wear the hoodies during the meetings.

## III. Competitive "Hacking"

Alongside the general *hacking* club, we also run a successful Capture The Flag (CTF) team, which in 2014 was ranked as the best United Kingdom based academic team and 33rd worldwide. Capture The Flag is a blanket term adopted for describing offensive security competitions where the primary objective is to earn points by obtaining so-called *flags*. These events are primarily targetted at a worldwide audience, and are, in the majority of cases based online – thus, anyone is free to participate.

### *A. Capture The Flag Competition Format*

Events usually last between 24 and 48 hours and are clustered into two distinct formats: Attack-Defence and Jeopardy. Each format exposes the participants to a different environment in which they must adapt to gain points.

Attack-Defence is by far the most dynamic of the two formats. It sees participants defending a server littered with vulnerable services while concurrently developing exploits to attack other teams servers. This format generally favours larger, more experienced teams, since points are scored for both patching vulnerable services and exploiting other teams vulnerable services, thus, the faster both sub-objectives can be accomplished, the greater amount of points scored.

Jeopardy on the other hand, involves solving a fixed set of challenges determined by the event organisers. This format allows for more esoteric challenges and greater diversity in skills required to participate. For example, challenges range from cryptography-based to reverse-engineering, web hacking and remote exploitation. Such competitions occur much more frequently than their Attack-Defence counterparts and are generally more *friendly* towards beginners. Although solving challenges first generally affords the solving team a small amount of bonus points, speed is less of a concern.

What must be emphasised is that such competitions provide a safe training environment for largely offensive cyber-security techniques.

### *B. Group Organisation within Competitions*

In general, due to the times that competitions are held – weekends – most participants take part remotely and coordinate online. To this end, for both competition formats we organise the group via use of Internet Relay Chat (IRC) and the real-time collaborative Wiki software, Rizzoma [4] . We find that collaboration on tasks allows those in the club whom are new or lacking in knowledge to feel a sense of accomplishment when a task they participated in is solved – again providing a source of motivation for further learning. In addition, it also allows for a sort of mentoring whereby more experienced members of the group are able to demonstrate the process involved in solving challenges in a somewhat interactive format where others can contribute the the solution.

Following participation in competitions, group members that solved challenges are encouraged to produce formalised write-ups [5] detailing the precise solution and thought process that allowed them to solve the challenge in question. These then serve as material for presentations in the following group meeting, and aid in solving challenges in subsequent competitions.

## IV. Challenges

There is no set successful formula for running a hacking club. It is about handling a small community that is in a yearly flux – by the very nature of being in an academic setting – requiring constant adaptation and dedication to keep motivated. Members need to feel they fit in, they are welcome and acknowledged. The challenges we encounter arise from the need to keep our members informed, engaged and entertained during the club sessions. In the following sections we discuss the main challenges we deal with and how we overcome them.

*a)Hacking club attendance:* For the club, attendance is the major challenge we face on a weekly basis. During term-time the number of active participants is approximately 10 – 15. In order to attract the students we make sure to prepare beforehand, deciding on a topic for the next meeting and searching for hacking exercises, which are called *challenges*, to solve. We always send out an email reminding the time and location and include a brief explanation of what we plan to do.

Meetings that contain presentations of write-ups of previously solved hacking challenges have proved to be very successful and we have decided to adopt the format permanently. If we cannot present write-ups, we have short crash-courses on a specific topic (e.g. buffer overflows, IDA Pro, ARM assembly) and solve hacking challenges related to it. Members take turns and choose the topic they want to present. They do not need to be savvy about the field, the idea is to learn and share the knowledge.

Another way of attracting new students is by presenting the club in computer security related lectures and organising an introductory special hacking club meeting. We explain who we are, what we do and why they should join us. Many students think the hacking club is a place for experts. In the meeting we show them we cater for all levels of skills. As means of introduction to hacking, we are particularly fond of the Natas by OverTheWire [6] wargame.

*b)Alumni engagement:* Alumni are an important part of our group and we keep them up to date and involved in the club activities. As most of them are unable to attend the meetings (due to relocation), we pass on information through our *mailing list*. Alumni take part in the online competitions we participate in (see Section III) and we hold special guest sessions when they visit us. Another means of communication with our alumni is through Internet Relay Chat (IRC). An interesting aspect we have noticed is that our alumni community is largely dominated by students of post-graduate level courses (approximately 75%).

*c)Difficulty level:* As we welcome members with any skill level, it is sometimes delicate to find the correct difficulty level for the hacking challeges undertaken during meetings. We keep a balance, such that knowledgeable members do not feel bored and new members are not overwhelmed. We hold introductory courses into basics such as Linux commands or web vulnerabilities, and we always make sure to communicate, track individual progress and ask for feedback during a session. We also believe that learning by practice is the best way to go and we encourage members to train on the demo challenges. We encourage members of different skill levels into working together and avoid pairing new members, as they might not yet feel comfortable or confident enough to speak up and ask questions.

*d)Competition participation:* As with the hacking club in general, motivating participation in competitions is a challenge. Especially so since the vast majority take place over weekends. This is compounded by the belief amongst many that attend the hacking club, that either their participation will not be worth the time investment or that the competition challenges will be too difficult to complete given their current knowledge. We attempt to overcome these difficulties by ensuring enough notice is given as to when competitions take place, and encourage meeting in person to take part, thus, adding a social aspect. As a consequence of being an almost exclusively academic group, many of our most experienced members leave as they graduate. Thus, retaining sufficient knowledge within the group is a difficulty, especially in mentoring new members to become experienced enough to participate in competitions. Though we see this as somewhat remedied by the participation of both alumni and graduate students, which comprise a significant portion of our CTF team.

## V. Conclusion

We present the difficulties and organisational practices of running both a successful hacking club and CTF team. As much as teaching defensive security is important, the converse, offensive security is just as important, yet there is little opportunity to learn these related techniques. Hacking clubs such as that held at the University of Birmingham allow for such skill development and knowledge transfer outside of a classroom environment, so to speak. Enabling the practice of offensive security – all too often mistaken for illegality – in a safe, legal environment.

While we have stated a number of challenges involved in running such a club and how we have attempted to overcome them, it is hoped our experiences can be translated into a blueprint, motivating further United Kingdom based hacking clubs and corresponding CTF teams.

## References

[1] T. Chothia, “Tom Chothia.” [Online]. Available: http://www.cs.bham.ac.uk/~tpc/

[2] M. Cova, “Marco Cova.” [Online]. Available: http://marcocova.net/

[3] AFNOM, “AFiniteNumberOfMonkeys - University of Birmingham Hacking Club.” [Online]. Available: http://afnom.net

[4] Tekliner, “Rizzoma.com.” [Online]. Available: https://rizzoma.com

[5] AFNOM, “AFiniteNumberOfMonkeys - WriteUps.” [Online]. Available: http://afnom.net/writeups/

[6] OverTheWire, “OverTheWire: Natas.” [Online]. Available: http://overthewire.org/wargames/natas/