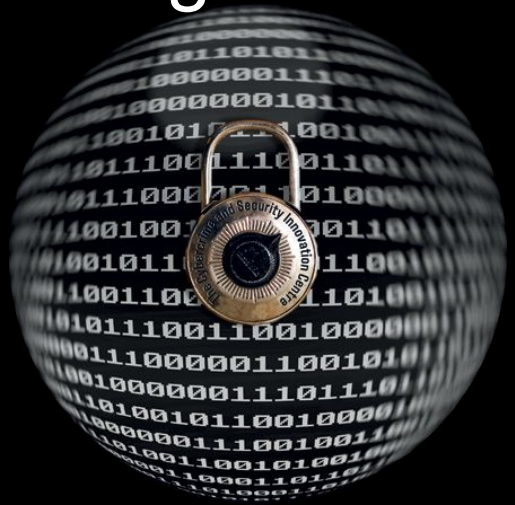
LEEDS BECKETT UNIVERSITY

Open Source CyBOK Practical Challenges and Learning Resources



Dr Z. Cliffe Schreuders
&
Tom Shaw

The importance of hands-on technical challenges

Hands-on experience with defensive tools, and hacking tools with access to vulnerable systems

Building CTF challenges into cyber security labs is an effective way of engaging students, but it's hard work

Offensive security helps to develop the security mindset

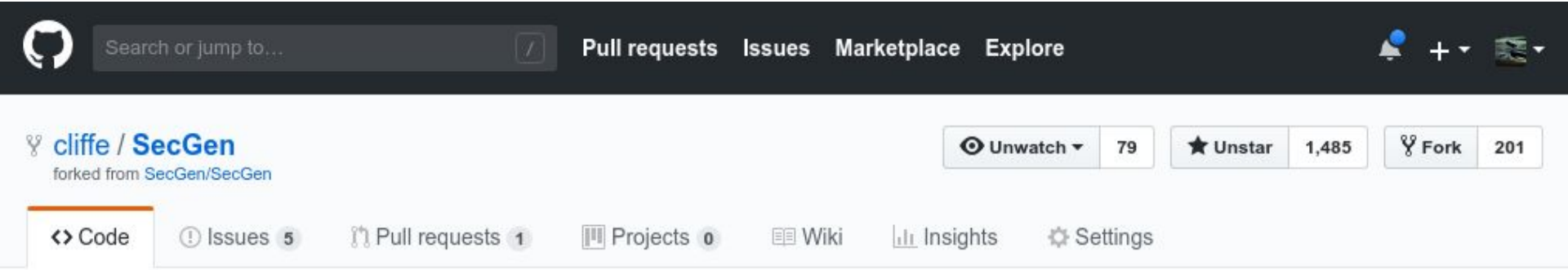
Randomised cyber security challenges

Most cyber security is taught using static challenges

We have developed a unique solution:

- a platform for generating randomized vulnerable systems

SecGen generates randomised VMs, meaningful security challenges, and CTF scenarios



Hackerbot

Defensive and investigative challenges: Hackerbot chatbot

- Students can IM the chatbot
- Hackerbot presents challenges to students
- Hackerbot attacks their VMs, students need to defend or investigate

Students have found Hackerbot

- Fun and enjoyable, interesting and unique
- Enjoyed the instant feedback
- Usable (SUS) & motivating (IMMS)

Hackerbot


Buddy List
Buddies Accounts Tools Help
Buddies
Hackerbot
Available
Hackerbot
Conversation Options Send To
Hackerbot
(06:28:47 AM) scylla: hello
(06:28:47 AM) Hackerbot: Hello, scylla (172.16.0.2).
(06:28:47 AM) Hackerbot: You are about to be attacked!
(06:28:47 AM) Hackerbot: ** #7 **
(06:28:47 AM) Hackerbot: Create a Snort rule that detects any TCP connection attempt to HTTP (just the connection attempt, does not require content inspection) on 172.16.0.4. The alert must include the message "ff9d4c".
(06:28:48 AM) Hackerbot: 'Ready'?
Font Insert Smile! Attention!
Desktop

Randomised challenges

We have developed a whole curriculum of labs, spanning technical CyBOK topics, most of which include randomised CTF challenges:

- ethical hacking and penetration testing
- web and network security
- systems security
- incident response and investigation
- malware and reverse engineering
- software security and exploit development

Project aims

Open source resources mapped to CyBOK covering a wide range of KA's with a focus on hands-on application of theory and technical applied skills development.

Mapping approximately 40 full length VM scenarios/challenges/labs.

Labtainer scenarios (an open source framework by the Postgraduate Naval School, included in SecGen) which has 60+ shorter cyber security labs.

25 recent lecture videos published to YouTube with CyBOK KAs and Topics.

Project outputs

103 practical cyber security labs mapped to CyBOK

https://github.com/cliffe/SecGen/blob/master/README-CyBOK-Scenarios-Indexed.md

70 recent lecture videos with CyBOK KAs and Topics

https://github.com/cliffe/SecGen/blob/master/README-CyBOK-Lecture-Videos.md

Project benefits

Helpful for HE educators to plan curriculum based on CyBOK, finding and making use of these resources.

Our technical framework provides a common method for sharing lab challenges and VMs based on clear CyBOK mapping.

Clear demonstration of the mapping to CyBOK, which will help in HE planning towards NCSC course accreditation.

Our open source frameworks and resources include innovations, such as randomised CTF challenges and interactive attacker chatbots that can be deployed into a cloud-based infrastructure.

Next steps

Phase 2 Open Source CyBOK Practical Challenges and Learning Resources:

- Integrate CyBOK deeper within SecGen, at a modular level
- Enable scenario randomisation based on configuration related to CyBOK topics
- Build and publish an extensive catalog of CTF scenarios mapped to CyBOK; new and existing capture the flag (CTF) scenarios, designed for CTF games and competitions

Hacktivity Cyber Security Labs:

- Going online with our lab infrastructure, currently used by our students

LEEDS BECKETT UNIVERSITY

The Cybercrime & Security Innovation Centre (CSI)

Hacktivity Hacktivities Hackers Teams Login Register

Hacktivity

Cyber Security Labs

About

Security Scenario Generator (SecGen): A Framework for Generating Randomly Vulnerable Rich-scenario VMs for Learning Computer Security and Hosting CTF Events

Z. Cliffe Schreuders, Thomas Shaw, Mohammad Shan-A-Khuda, Gajendra Ravichandran, and Jason Keighley, *Leeds Beckett University*
Mihai Ordean, *University of Birmingham*

Abstract

Computer security students benefit from hands-on experience applying security tools and techniques to attack and defend vulnerable systems. Virtual machines (VMs) provide an effective way of sharing targets for hacking. However, developing these hacking challenges is time consuming, and once created, essentially static. That is, once the challenge has been "solved" there is no remaining challenge for the student, and if the challenge is created for a competition or assessment, the challenge cannot be reused without risking plagiarism, and collusion.

Security Scenario Generator (SecGen) can build complex VMs based on randomised scenarios, with a number of diverse use-cases, including: building networks of VMs with randomised services and in-the-wild vulnerabilities and with themed content, which can form the basis of penetration testing activities; VMs for educational lab use; and VMs with randomised CTF challenges. SecGen has a modular architecture which can dynamically generate challenges by nesting modules, and a hints generation system, which is designed to provide scaffolding for novice security students to make progress on complex challenges. SecGen has been used for teaching at universities, and hosting a recent UK-wide CTF event.

1. Introduction

Computer security students benefit from hands-on experience applying security tools and techniques to attack and defend vulnerable systems. Practical lab work and pre-configured hacking challenges are common practice both in security education and also as a pastime for security-minded individuals. Competitive hacking challenges, such as Capture the Flag (CTF) competitions have become a mainstay at industry conferences and are the focus of large online communities. CTF activities have been used in education as an effective way of providing and assessing engaging hands-on security challenges, and is often the focus of student hacking society activity (see e.g. [1]–[3]). Virtual machines (VMs) provide an

Gamification for teaching and learning computer security in higher education

Z. Cliffe Schreuders, *Leeds Beckett University* Emlyn Butterfield, *Leeds Beckett University*

Abstract

In many cases students in higher education are driven by assessments and achievements rather than the "learning journey" that can be achieved through full engagement with provided material. Novel approaches are needed to improve engagement in and out of class time, and to achieve a greater depth of learning. Gamification,

tasks [2, p. 154]. However, this approach has its own considerations, such as ensuring that marking criteria remain clear and transparent, marked consistently, feedback is constructive and timely, and all managed within the constraints of staff availability.

In this study gamification was investigated as a method of motivating students to engage in a range of learning tasks with clear and timely assessment and feedback.

Gamification is defined as the application of game mechanisms to non-game contexts, and is becoming widely used across a range of domains, including within higher education, to increase motivation and engagement [3]. A gamified assessment structure and assessment tasks (referred to as 'quests') were developed for a final year undergraduate computer security module, in an attempt to motivate students to engage in a range of learning activities.

Despite the availability of a number of online gamification web apps, scripts, and content management systems (CMS), none of these systems fit the requirements for our intended approach to gamification of education, which is discussed in the Results section. Therefore, a new VLE was developed, which integrated with the University's existing VLE (Blackboard), and provided a unique gamified experience, with quest descriptions, criteria, and real-time feedback capabilities, based on a semi-automated assisted marking back-end.

In this paper, we describe our approach to gamified assessment tasks and structure for the module 'Incident Response and Investigation', a module covering incident response topics such as information security management, log management, integrity and network monitoring, intrusion detection, and live and dead disk analysis. We also present My XP, a novel free and open source software (FOSS) gamification VLE, along with the open educational resources (OER) teaching materials we developed. Although these were developed in tandem and to complement each other, these could be used independently: for example, the labs can be used to teach computer security topics without the gamification assessment aspect.

2. Aims

The primary aims of our approach was to:

Improve student engagement and motivation: As discussed in the next section, it is generally accepted in the literature that gamification has the potential to improve motivation. In particular, we aimed to improve engagement with out-of-class activities, such as completing lab

Hackerbot: Attacker Chatbots for Randomised and Interactive Security Labs, Using SecGen and oVirt

Z. Cliffe Schreuders, Thomas Shaw, Aimée Mac Muireadhaigh, Paul Staniforth, *Leeds Beckett University*

Abstract

Capture the flag (CTF) has been applied with success in cybersecurity education, and works particularly well when learning offensive techniques. However, defensive security and incident response do not always naturally fit the existing approaches to CTF. We present Hackerbot, a unique approach for teaching computer security: students interact with a malicious attacker chatbot, who challenges them to complete a variety of security tasks, including defensive and investigatory challenges. Challenges are randomised using SecGen, and deployed onto an oVirt infrastructure.

Evaluation data included system performance, mixed methods questionnaires (including the Instructional Materials Motivation Survey (IMMS) and the System Usability Scale (SUS)), and group interviews/focus groups. Results were encouraging, finding the approach convenient, engaging, fun, and interactive; while significantly decreasing the manual marking workload for staff. The cloud infrastructure deployment using SecGen/oVirt was a success, generating VMs with randomised challenges, and enabling students to work from home.

1. Introduction

Computer security education benefits from hands-on interactive learning activities. Capture the flag (CTF) has been applied with success in education [1]–[4], and works particularly well when learning offensive techniques. However, defensive security and incident response do not always naturally fit the existing approaches to CTF. Defensive and investigative tasks challenges, rewarding correct solutions with flags. We deployed an oVirt infrastructure to host the VMs, and leveraged the SecGen framework [6] to generate lab sheets, provision VMs, and provide randomisation between students.

2. Related Literature

Capture the flag (CTF) is a type of cyber security game which involves collecting flags by solving security challenges. CTF events give professionals, students, and enthusiasts an opportunity to test their security skills in competition. CTFs emerged out of the DEFCON hacker conference [7] and remain common activities at cybersecurity conferences and online [8]. Some events target students with the goal of encouraging interest in the field: for example, PicoCTF is an annual high school competition [9], and CSAW CTF is an annual competition for students in Higher Education (HE) [10].

Applications of CTF scenarios have demonstrated pedagogical utility when used within HE. Challenges have been adapted and used successfully in CTF-style lab exercises [1], [2], [11], in class competitions [12] and extra-curricular activities [4], [13].

Prior work on the Security Scenario Generator (SecGen) framework aimed to solve issues present when using static CTF challenges in assessment situations [6], [14]. Hacking challenge scenarios are expensive and time consuming to create [15]. CTF challenges should not typically be reused in assessment situations, such as university assignments, competitions or job recruitment, as solutions and discussion of the