The importance of hacking challenges

Offensive security helps to develop the security mindset

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

Hacking challenges are fun
The Cybercrime & Security Innovation Centre (CSI)

Current projects

Capture the Flag (CTF)
The challenge

Admin access to systems
Install OS and software of their choice
Freedom to explore with networking of systems
Hands on hacking and malware analysis and exploit development
Access to vulnerable systems to attack
Reset systems when things go wrong
Protect university infrastructure
Remote access to safe lab environments
Prevent plagiarism and unfair practice

...
Most ethical hacking is taught using static challenges.

We have developed a unique solution:

- A platform for generating randomized vulnerable systems

**SecGen** generates randomized VMs, meaningful security challenges, and CTF scenarios.
Randomised hacking challenges

SecGen use-cases include

- Simulations of organizations with a mix of secure and insecure services; with desktop and servers; for simulated security audits;
- Challenges for CTF events or CTF-style lab work;
- Security lab exercises
System overview
Integration with oVirt

Uses VM templates as base-boxes, and provisions them with Vagrant and Puppet

Affinity groups and networks

Snapshots
Hackerbot

Hackerbot chatbot

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

Students found Hackerbot

- Fun and enjoyable
- Interesting and unique
- Enjoyed the instant feedback
- Usable (SUS)
- Motivating (IMMS)
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?'
Unique features

Used to manage the provisioning of pools of VM Sets onto oVirt via SecGen

Acts as a portal for students to control and access their VMs running on oVirt

Capture the flag marking (percentage-based, time-based)

Late penalties and timed tests

Leaderboards

Remote access to our lab infrastructure

Automated marking of tests and tasks!
Security Scenario Generator (SecGen): A Framework for Generating Randomly Vulnerable Rich-scenario VMs for Learning Computer Security and Hosting CTF Events

Z. Cliff Schreuders, Thomas Shaw, Mohammad Shaw-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 making plagiarism and collusion impossible.

SecGen 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 base generation system, which is designed to be pluggable for scaffolding for novice security students to make progress on complex challenges. SecGen has been used for teaching at universities and is now a recent UK-wide CTF infrastructure.

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. CTFs 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 security activity (e.g. [3]-[5]). Virtual machines (VMs) provide an

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

Z. Cliff Schreuders, Thomas Shaw, Ainée Mac Mulreadhaigh, Paul Stanforth, Leeds Beckett University

Abstract
Capture the flag (CTF) has been applied in success in cybersecurity education, and works particularly well when leveraging offensive techniques. However, defensive security and incident response do not always naturally fit the existing approaches to CTF. We present Hackxerbot, 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 investigative challenges. Challenges are randomly selected 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 with groups. Results were encouraging, finding the approach 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]-[3], and works particularly well when leveraging offensive techniques. However, defensive security and incident response do not always naturally fit the existing approaches to CTF. We present Hackxerbot, 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 investigative challenges. Challenges are randomly selected 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 with groups. Results were encouraging, finding the approach 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.

Ganification for Teaching and Learning Computer Security in Higher Education

Z. Cliff Schreuders, 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 and interest within class time, and to achieve a greater depth of learning. Ganification.

Ganification is defined as the application of game mechanics 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 interactive learning modules (referred to as “quests”) were developed for a first year undergraduate computer security module, aiming to motivate students to engage in a range of learning activities.

Despite availability of a number of online ganification websites, scripts, and content management systems (CMS), some of these systems fit the requirements for our intended approach to gamification of education, as discussed in the Related section. Therefore, a new VLE was developed, which integrated with the University’s existing VLE (Blackboard), and provided unique gamified experience with quest descriptions, criteria, and real-time feedback capabilities.

In this paper, we describe our approach to gamification and assessment tasks across the module. The Incident Response and Investigation, a module with many real-life use cases, was an ideal gamification target, and presented unique gamified experience with quest descriptions, criteria, and real-time feedback capabilities.

In this paper, we describe our approach to gamification and assessment tasks across the module. The Incident Response and Investigation, a module with many real-life use cases, was an ideal gamification target, and presented unique gamified experience with quest descriptions, criteria, and real-time feedback capabilities.

Despite availability of a number of online ganification websites, scripts, and content management systems (CMS), some of these systems fit the requirements for our intended approach to gamification of education, as discussed in the Related section. Therefore, a new VLE was developed, which integrated with the University’s existing VLE (Blackboard), and provided unique gamified experience with quest descriptions, criteria, and real-time feedback capabilities.

In this paper, we describe our approach to gamification and assessment tasks across the module. The Incident Response and Investigation, a module with many real-life use cases, was an ideal gamification target, and presented unique gamified experience with quest descriptions, criteria, and real-time feedback capabilities.

In this paper, we describe our approach to gamification and assessment tasks across the module. The Incident Response and Investigation, a module with many real-life use cases, was an ideal gamification target, and presented unique gamified experience with quest descriptions, criteria, and real-time feedback capabilities.

In this paper, we describe our approach to gamification and assessment tasks across the module. The Incident Response and Investigation, a module with many real-life use cases, was an ideal gamification target, and presented unique gamified experience with quest descriptions, criteria, and real-time feedback capabilities.