UNIVERSITY OF CAMBRIDGE

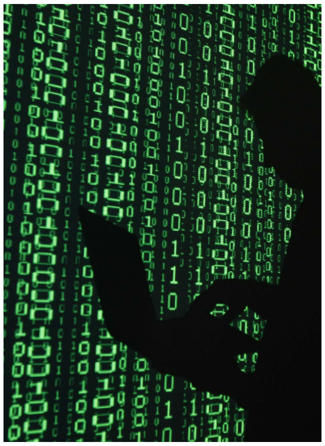
TALLINNA TEHNIKAÜLIKOOL

[CONFIDENTIAL]

>>Exercise Mercury

An Ethical Hacking Exercise

Kieren Lovell, David Modic and Olaf Manuel Maennel



First released on
June 26, 2018

COOPERATIVE CYBER DEFENCE
CENTRE OF EXCELLENCE

TALLINNA
TEHNIKAÜLIKOOL

UNIVERSITY OF
CAMBRIDGE

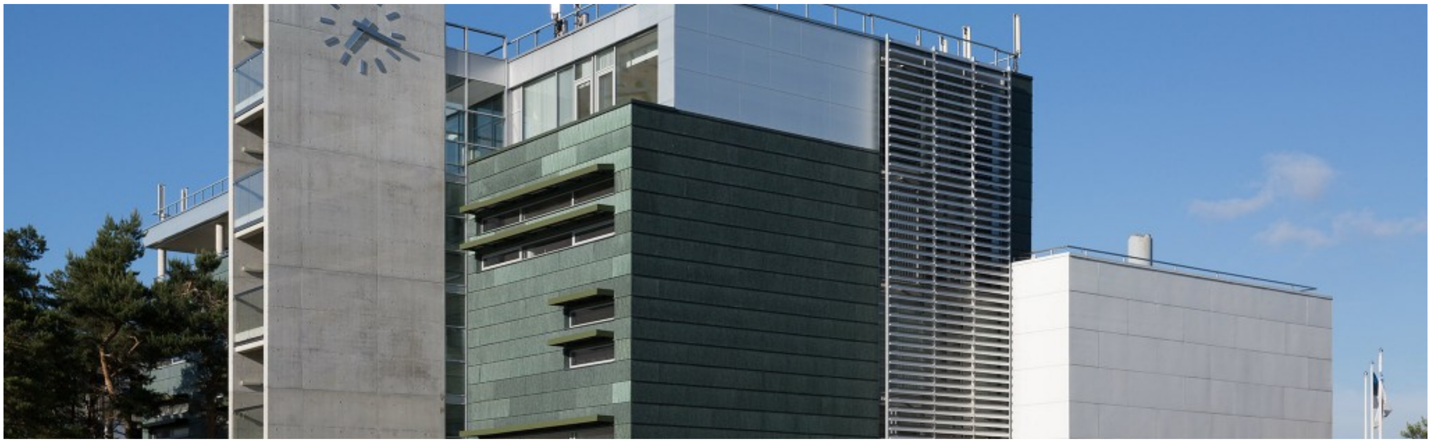
Table of Contents

Overview

Exercise Mercury was an exercise between the University of Cambridge, Tallinn Technical University, and supported by the NATO Cooperation Cyber Security Centre of Excellence. The purpose of the Exercise was to test each others' infrastructures, and for operators to gain real life experience in under standing their respective systems from a hacking prospective. The exercise ran for a week, starting with traditional skills in Open Source Intelligence Profiles (OSINT), then practising and developing existing skills to test, probe, report and mitigate threats on operational systems, within a safe and secure manner.

As a result, the exercise feedback has been very positive (4.7/5) with only two negative points:

1. Can the exercise be longer?
2. Can the exercise count as work?



Aim & Priorities

TRAIN AS YOU FIGHT, FIGHT AS YOU TRAIN

As you can see from the overview of the exercise, the premise is to better understand the technical and management challenges that we face here at the University of Cambridge.

However, whilst we may think we know where our vulnerabilities are, these have never been tested from the perspective of the University as a whole, only within each individual College, Department, Section or system. As a result, it is inevitable that we would fail to notice major weaknesses within our systems. Threat Actors do not care about the internal politics of the University, all they want is to gain elevated access or to cause reputational damage to us as a whole.

Additionally, with this in mind, we wanted to make sure that the exercise helps us to develop a plan that will aid us to achieve the following priorities:

- Identify key areas that require immediate mitigation
- To gain an insight of our vulnerabilities and how we can best serve the University to improve our security posture.
- To practice Command, Control, and Communications (C3) methods within UIS.

AIM

To provide a realistic, but safe, exercise to find, locate, and mitigate various threats in the University, whilst adhering to the Rules of Engagement of the exercise.

Rules of Engagement

Improving Security via OSINT is the most forgotten and least used resource available to organisations

PRIMARY RULE

We will have a Zero Digital Footprint policy. Other than the submitted report, all material collected will be deleted in accordance with HMG IA guidelines (Erased with at least three rewrites over the sectors). If at any point it was thought an action would impact on an operational system, the activity was immediately ceased and the Gamemaster was advised (Kieren Lovell).

GAMEMASTER

The Gamemaster is the key point of contact that controls the exercise. Co-coordinating and controlling the exercise ensuring that the exercise is safe, and does not cause any operational impact to our Universities, or to any other third parties. Any impact, the exercise would immediately stop.

SAFEGUARD RULE

It is important before the exercise starts to make sure that it does not impede, damage, or cause confusion with the normal running of the University. The point of the exercise is to test and improve responses to real threats; not to damage the organisational incident response structure.

With this in mind, all exercises will be governed by the SAFEGUARD rule. This rule, which is a standard term used in practising incidents, is here to protect the organisation from real threats. During the exercise, we act and communicate as if it were real life events. However, this can cause confusion if a real incident happens during the exercise. To this end, any communications that are real, and not related to the exercise, are prefixed with 'SAFEGUARD SAFEGUARD SAFEGUARD'. This is included in all communications (telephone, voice, email, fax).

In order to make this work, all members of staff involved must be briefed on the SAFEGUARD rule before the start of the exercise. This is normally completed verbally for the Command Team, and via telephone/email during the COMMS CHECK before STARTEX. COMMS CHECK & SAFEGUARD BRIEF must be completed before any exercise is commenced. To this end, it must be stressed that the COMMS CHECK is not to test comms as part of the Team marking process (That will be part of the exercise), but between the key contacts in the University (Cambridge and TTU), University Security, & CamCERT before the activation of the exercise. This ensures that we have functioning communications between key information feeds and confirms, before launching the exercise, that there is not an ongoing incident. If an incident develops during the exercise, everyone involved needs to understand the procedure to switch to real life reactions.

Exercise Results

TTU

4645

Winners

Cambridge

2100

Runners Up

RESULTS

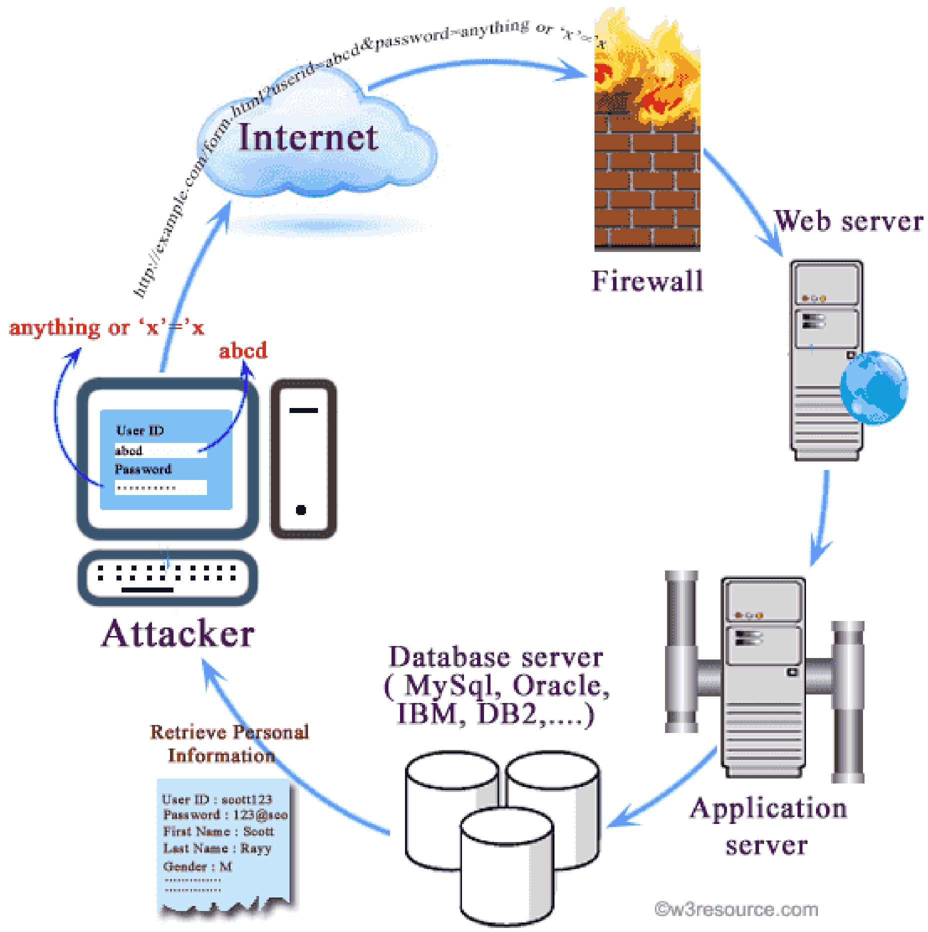
From the outset, it might be noted that Cambridge were expecting to lose. We have a much larger digital footprint than Tallinn, and UIS is not used to these exercises (in fact, this type of exercise is the first of its kind in the United Kingdom). However, I will add that Cambridge really did very well. They harnessed their own abilities, and gained a level of interdepartmental leadership and communications skills that have not been actively practised previously.

As someone who joined UIS only two years ago, I can say that this is the first time I truly saw the department working as one, without the legacy divisions casting a shadow and, as a result, it has vastly improved communications across the organisation within UIS.

VULNERABILITY ASSESSMENT

TTU's open source intelligence profile against us provided some interesting reading, along with their technical scans. The key points of the information are as follows:

- Ownership and patching of systems is not being maintained. However, the results point to both central / departmental systems as well as individual research projects.
- The overall reason for a number of these vulnerabilities is because they are running a service that we do not centrally support. (for example, 65 wordpress sites) that have been set up and are not being actively managed. This would be rectified if we ran Wordpress as a service, or provided an avenue for them to host this as a managed service with a third party.
- Overall, of our webserver estate, 51% of our Apache servers were found to be out of date. This, of course, does not necessarily mean that they are security risks, however it does increase the likelihood of a breach by a large factor.
- A number of firewalls were incorrectly configured and in some cases, actively assisted hackers in redirecting their requests to a device. These have all been rectified, but it does stress that the Managed Firewall Service is an approach that we should take.
- Four key webservers are not running their websites without certificates. In running a service using HTTP (not HTTPS) they are exposing themselves, and in a non security aspect, reducing their ranking within Bing and Google. These sites have been identified and assistance will be given as requested.
- A number of these vulnerabilities could not be seen by UIS, but could be seen on the wider stage. This data has proven invaluable.



Impact on Cambridge

SQL INJECTIONS

A number of simple SQL injections were located (86) from College, Departmental, and Research Group servers. They have been contacted and they are being assisted in fixing their systems when possible.

SOCIAL ENGINEERING

During the Exercise there was a day of attempting to spear phish people in UIS (the biggest source of compromise within the University is spear phishing emails). I'm pleased to say, only one person clicked the email, on a device that would not have caused a compromise. A great result.

CREDENTIALS

Over 12,000 usernames and passwords were located on various hacking forums, using their CRSID. It must be noted, that these details are not related to a breach of our database, but that users have had their details compromised from third party services. Passwords can and might be reused across services (as people may use passwords across systems). One of the great improvements we have now implemented is that the password reset application for Raven is now connected to the haveibeenpwned.com database. If users try to use a password that has been compromised, it will refuse.

IMPACT

Only positive. No operational system was impacted during the exercise, and their was no effect on any University System. However, we have definitely reduced our risk profile by using this exercise as a test bed. I look forward to running similar exercises in the future.

Future Exercises

JUNE

In June of this year, I will be running an exercise in Estonia in learning how to compromise a warship. Whilst this is not really helpful to the University of Cambridge, it has allowed us to use the expertise of TTU and NATO in using them as a resource for these exercises as payment (Prior to arriving at Cambridge, I was Battlewatch Captain & Chief Information Security Officer for Commodore NATO Standing Maritime Group 1). As such, I think we will have a great opportunity to develop this exercise, and to open it up to the University as a whole, safe in the knowledge that the ROE's work.

EMBASSY SUPPORT

Due to the exercise, the British Embassies in Latvia, Estonia and Lithuania are using CamCERT to teach OSINT and best practice cyber warfare training in their security training package Garage48. As a result, I have now received a training package provided by UK Government to train my team in many different aspects of cyber security. As well as having a close working relationship with the Estonian authorities, we will also be gaining support from the Ministry of Defence in Latvia. Developing these links will be incredibly helpful, as we will be gaining intelligence briefings of the new trends and IT events that will help us to stay ahead of the game, It will also assist us in filling in any gaps we may have when the United Kingdom leaves the European Union.

Overall, the exercise has proven to be a very positive experience for a very low cost outlay. There seems to be a new interest in cyber security within UIS. Bringing colleagues together from across UIS has brought a great level of enthusiasm, and highlighted extra skills we have within UIS. All high level possible compromises have been notified.

KIEREN NICOLAS LOVELL - HEAD OF CERT