An open cloud-based virtual lab environment for computer security education

A pilot study evaluation of oVirt

Z. Cliffe Schreuders, Emlyn Butterfield, and Paul Staniforth
School of Computing, Creative Technologies and Engineering
Leeds Beckett University
Leeds, UK

***Abstract*— Providing an environment that enables students to gain hands-on experience with security tools in rich and complex learning scenarios, while granting them the freedom to experiment with potentially harmful tools, is an issue for many universities and organisations. As is the challenge of enabling students the flexibility to work from home. This paper presents the results of a pilot study of our proposed solution based on oVirt. Opportunities for improvements are identified, and it is concluded that oVirt is a feasible platform on which to build a lab environment for teaching computer security.**

Keywords—security education; laboratory work; learning environments; virtualisation.

I. INTRODUCTION

Digital security education benefits from hands-on practical application of theory, such as students conducting ethical hacking exercises, network authentication and access control configuration, and network monitoring and incident investigation of attacks. Providing a laboratory environment that can adapt to various learning objectives, while granting learners the flexibility to experiment with potentially dangerous tools, is an issue for many organisations, and was a common theme of discussions between academics at the recent HEA Computing Workshop – Cyber Security Pedagogy: Teaching, Learning & Assessment in HE [1]. Many universities are limited in their capacity to deliver these experiences for students, and maintain their own bespoke solutions, which are typically based on running local virtual machines (VM) on lab computers. These teaching environments often do not enable off-site access to the practical learning environment, do not enable learners to interact with each other's systems, and cannot provide realistically complex networks of systems for security learning scenarios, or exposure to modern cloud-computing environments.

Cloud-based provisioning, and desktop and server virtualisation technologies, present newfound possibilities for providing secure and flexible learning environments; however, interfaces to these technologies are not typically designed for educational use, and despite some training companies licensing proprietary solutions, adoption by universities has been limited.

We plan to develop, deploy, and evaluate a laboratory environment based on free and open source software (FOSS) that satisfies the needs for delivering digital security education.

Our proposed solution is based on the oVirt platform [2,3]. Developed by RedHat, oVirt provides a technical means to deliver desktop and server virtualisation to an organisation (which we contend will provide the advantages outlined earlier); however, the adoption to an educational setting requires evaluation and development, including the development of interfaces and configuration to enable effective security education. The hardware and configuration requirements for the platform and how this can be achieved within the host-university's existing infrastructure (and how this can be generalised to other contexts) will be determined and implemented.

In order to measure the feasibility of this approach a pilot study was conducted to gather student feedback regarding the interface and capabilities of oVirt for this purpose.

II. AIMS

Our aims are to provide: ***A FOSS solution*** based on open source technologies that can be used to deliver security education; ***On-site and remote access to labs*** for distance learning, using state of the art remote desktop technologies – this alleviates dependence on specialist lab rooms, which can be in high demand and technically difficult to implement and manage; ***A secure and scalable system*** with cloud-provisioning benefits, including live migration and thin provisioning; ***Integration with existing university systems*** for automatic access and authentication to materials, with a user interface that is educationally focused, and has demonstrable usability; A student lab platform that has ***independence from the physical infrastructure***: for example, supports a variety of hardware for servers and desktop lab systems, independent from the server and desktop operating systems used in the learning scenarios; ***Scenario-based provisioning of networks, servers, and desktops***, as required to complete a variety of security lab exercises, including ethical hacking, incident investigation and response, exploit research and development, malware analysis, and defensive configurations including network authentication and access control; And importantly, ensuring that ***student opinions and experience*** of the system are positive: including responsiveness, feature set, and usability.

III. METHODS

There are many available virtualisation deployment platforms including oVirt, OpenStack, OpenNode, Eucalyptus, VMware vSphere, and VMware Horizon; each have their own strengths [4,5]. Based on a comparison of our aims and

requirements, oVirt was identified as one of the most promising options: it provides flexible cloud-provisioning features, and it provides an appropriate platform for servers, and desktop VMs via SPICE, which can provide high performance platform independent desktop access.

An initial oVirt datacenter configuration was designed and deployed internally at Leeds Beckett University.

To measure the student experience component, and to identify areas for development, a pilot study was conducted. Undergraduate and postgraduate students studying security modules were invited to participate in the study. Six students participated in the trial.

Participants were given an introduction to the session. They had an hour to work through a laboratory worksheet involving LDAP authentication[1]. The oVirt user portal configured with a basic view was used to present each student with three VMs, which they started and used for the tasks: a SLES server, an openSUSE desktop, and a Windows XP VM with pGina. The task involved creating a CA for the server, configuring a centralised LDAP server, and configuring the the two desktop systems to authenticate users against the server. Security aspects, such as the security of the LDAP connection and certificates were explored.

During the study, the researchers were present to observe and take note of user experiences, and answer questions. After the session a focus group was run to collect feedback regarding the oVirt lab environment from the participants.

IV. Results

Features that students liked: it was stated that the experience was "pretty much painless." Students appreciated the persistence of their VMs state across sessions, for example when moving between rooms the state of their VMs would remain. It was also noted that they liked that this means that their own computers would not need to be high-spec in order to work at home, since running many local VMs can be demanding. Also, the new laboratory system compares favourably to the current system in place, the Image Management System (IMS), which can take some time to save state back to the server.

Speed performance: once running VMs were responsive and performance was satisfactory (agreed by 5/6 students). However, it was noted that VMs were slow to boot and restart, which was exacerbated by a user interface issue, where no progress information was provided regarding VM start up, and clicking on the boot icons again provided an obtuse error message. However, the startup time compares well to the IMS. The desktop experience was satisfactory (5/6 students), although one participant suggested that they would like an option to allocated a quota of RAM to VMs at will.

Features they would like to see (that are provided by alternative oVirt portal interfaces): Students should have an interface to configure: multiple NICs, RAM allocation, ability to either directly upload and create VMs or an avenue to suggest ISOs, OSs, and VMs for inclusion. They should be able to maintain multiple states/snapshots of each individual VM, and have the ability to restore states. There should be an indication of the resources quota available to students.

Features they would like to see added: Progress for VM startup and restart. A convenient way to upload and download files between and from any of their VMs.

User interface: The user portal and SPICE interface was seen to be intuitive. However, it was observed that some students found it confusing to start the VM desktop interaction. This involved ignoring an error message on the Web interface, downloading a SPICE client configuration file, then opening this with the SPICE client. A clarified message from the Web interface would be an improvement. There were some minor responsive design issues when resized. The keyboard shortcuts used by the SPICE client were somewhat confusing, partly due to familiarity with alternative systems.

Technical issues: For one student the openSUSE VM did not start correctly and entered emergency mode; it is suspect that this was due to an error during VM setup. For one student their Linux terminal was suspended until Ctrl-Q was entered (although this may have been due to an accidental Ctrl-S suspension).

V. Conclusion

Based on this pilot study we conclude that oVirt is a feasible platform on which to build a lab environment for teaching computer security. oVirt provides a large degree of flexibility, including remote access, scalability, integration, independence from hardware, network and software availability, persistence of state, and features that could be further utilised to improve student experience. Many of the features that were requested by participants are available via alternative user portal views and via oVirt's extensive set of permissions, quotas, and QoS to control creation and use of resources.

The learning activity was conducted without any major issues, and the study has identified guidance for our next stage in development of the system: user interface improvements, conversion of existing VMs in use, automation of VM provisioning and allocation to students, and platform and VM configuration to provide a positive student experience. Leeds Beckett University have started to invest in this development and also the server infrastructure required to deploy this solution.

1 Based on an OER LDAP laboratory worksheet available at: http://z.cliffe.schreuders.org/

References

[1] *HEA Computing Workshop – Cyber Security Pedagogy: Teaching, Learning & Assessment in HE*, 2013, Warwick, UK.

[2] oVirt, http://www.ovirt.org/

[3] A. Lesovsky, Getting Started with OVirt 3.3. Packt Publishing Ltd, 2013.

[4] D. Cerbelaud, S. Garg, and J. Huylebroeck, Opening the clouds: qualitative overview of the state-of-the-art open source VM-based cloud management platforms, *Proceedings of the 10th ACM/IFIP/USENIX International Conference on Middleware*. Springer-Verlag New York, Inc., 2009.

[5] R. Lixandroiu, and C. Maican, A Model for Comparing Free Cloud Platforms, *Informatica Economica* vol 18.4, 2014, pp. 40-49.