**USE OF REMOTE ACCESS TECHNOLOGIES FOR CYBERSECURITY EDUCATION IN POST-COVID ERA**

H. Leung

Department of Information Technology

Hong Kong Institution of Education (Chai Wan)

Vocational Training Council

hleung@vtc.edu.hk

**Abstract**

**After three years of isolation, Hong Kong is now going into the post-COVID era. The crisis has exposed a great challenge in the delivery of Cybersecurity training and education. During the last three years, there were no normal face-to-face classes, and hands-on labs/practical sections. Most of the teaching activities must be delivered with online mode. Students were required to complete the hands-on practical exercises of cybersecurity-related modules at home. With the application of virtualization technology, most of the students can complete the training exercises at home. However, it was extremely difficult to monitor the progress of students. In case there was any problem encountered by the student. It was almost impossible to troubleshoot in such a remote environment. Due to the limitation of Wi-Fi/broadband router at home, it was also not possible to pass through the Wi-Fi/broadband router to access the student’s home internal network to perform any kind of troubleshooting.**

**Because of such a challenge, we find that we should apply remote access technology to support and monitor student progress in practical labs, especially for different kinds of server/system administration modules. In the world of cybersecurity, remote access technology for penetration testing can be applied to solve the problem. Open-source penetration testing tools may become a feasible solution for monitoring and supporting tools for practical labs at home. Reverse-shell agency script generation tool can be used to create a system monitoring agency for tracking the activities of students doing their practical labs at home. Also, the command-and-control server (C&C) can be used as the central console. In case troubleshooting is required, the lecturer/trainer can perform different kinds of operations through the C&C server to the student virtual machine. This model can further develop to become a full-fledged online training system for the delivery of cybersecurity practical labs.**

**Keywords:** *Cybersecurity, System Administration, Command and Control Server, C&C, Adversary Tools, Reverse Shell, Shellcode, Red Teaming, Remote Access*

**Introduction**

COVID-19 has disrupted students' lives in various ways, including the operation of the Vocational and Professional Education and Training (VPET) sector in Hong Kong. Traditionally, each module of an IT-related Higher Diploma programme at the Hong Kong Institute of Vocational Education (HKIVE) comprises two components: lectures and practical labs. However, due to the pandemic, most campuses have been locked down, making it impossible to deliver face-to-face lectures and practical labs.

Lectures can be easily changed from face-to-face to online mode through video conferencing platforms such as Microsoft Teams and Zoom, with slightly less interactive Q&A sessions. An advantage of this approach is that students can revisit lectures to clarify any parts they didn't understand during the e-lecture. However, practical labs pose significant challenges, especially for modules related to system and network administration and penetration testing. Troubleshooting is difficult, and the lecturer can only rely on screen captures provided by students to identify issues, which can be time-consuming and not scalable. In case there is more than one student with problems, the lecturer is not possible to help all of them simultaneously.

Additionally, due to home network configurations, remote access to student virtual machines is not possible. Therefore, a tailor-made lab monitoring and administration system is needed to support students in doing their practical labs at home. The system should provide monitoring functions such that the lecturer can easily identify the problem in each virtual machine through the central dashboard or console. However, the development cost for such a tailor-made system is expensive and it also requires a long time to develop.

As a lecturer teaching Cybersecurity, I find that there already is such a platform used by most penetration testers and it is open-source and free. In this paper, we demonstrate how to use a communication and control (C&C) server, a penetration testing tool, to effectively and efficiently support students in their Linux server administration labs at home. This platform provides a central dashboard/console for the lecturer to easily monitor each virtual machine and identify any issues. This open-source solution offers a practical and effective solution for supporting IT practical home labs for VPET institutions facing similar challenges.

**Lab Environment at Student Home**

Before going into details of our implementation, it is important to understand the student home lab setup. The diagram below shows the network environment for the student home lab. Students run the VMware workstation on their PC and all the lab servers are running under the VMware workstation virtual environment. The server virtual machines (VMs) are connected to the host PC network through VMware NAT virtual network. The student PC (host of VMware workstation) is connected to the Internet (the Internet Service Provider) through the home wifi/broadband router with NAT. It means that the server VMs are running in a private network and cannot be assessed from the Internet.

A diagram of a computer network

Description automatically generated with low confidence

Figure 1 Network environment for student home lab

**Terminologies used in Penetration Testing**

To have the common ground of understanding the proposed solution to remote lab monitoring, it is crucial to understand the terminologies used in Cybersecurity especially the terms related to penetration testing.

Command and Control Server (C&C): Command and control are defined as a technique used by threat actors to communicate with compromised devices/servers over a network. C&C usually involves one or more covert channels, but depending on the attack, specific mechanisms can vary greatly. Attackers use these communication channels to deliver instructions to the compromised devices to download additional malware, create botnets, or exfiltrate data.

A command-and-control server (C&C) is a computer that threat actors use to send instructions to compromised systems. Their goal is to direct infected devices into performing further malicious activities on the host or network. There are a lot of open-source command-and-control servers available e.g., Caldera, Silver, and Empire.

Reverse Shell: A reverse shell is a shell session established on a connection that is initiated from a remote machine, not from the attacker’s host. Attackers who successfully exploit a remote command execution vulnerability can use a reverse shell to obtain an interactive shell session on the target machine and continue their attack. Reverse shells can also work across a NAT or firewall.

**CALDERA Terminologies**

A screenshot of a computer

Description automatically generated

Figure 2 CALDERA Web Console

To fully realize the potential of the C&C framework, CALDERA, you will need to familiarize yourself with the following terminologies.

CALDERA: It is a cyber security framework designed to easily run autonomous breach-and-simulation exercises. It can also be used to run manual red-team engagements or automated incident responses. CALDERA is built on the MITRE ATT&CK™ framework and is an active research project at MITRE.

Ability: An ability is a specific ATT&CK tactic/technique implementation that can be executed on running agents. Abilities will include the command(s) to run, the platforms/executors the commands can run on (ex: Windows / PowerShell), payloads to include, and a reference to a module to parse the output on the CALDERA server.

Adversary: Adversary in cyber security is a term used to describe a malicious actor or group of actors that are attempting to gain unauthorized access to a computer system or network. Adversaries can range from individual hackers to organized crime syndicates, and they can use a variety of techniques to gain access to a system. In CALDERA, adversary profiles are groups of abilities, representing the tactics, techniques, and procedures (TTPs) available to a threat actor. Adversary profiles are used when running an operation to determine which abilities will be executed.

Agents: They are software programs installed on target hosts/clients that connect back to CALDERA at certain intervals to get instructions. Agents communicate with the CALDERA server via a contact method, initially defined at agent installation.

**Scenario**

To demonstrate how to apply the remote access technology used by the penetration tester, the following lab scenario is used as a showcase. Five students are required to complete a simple Linux server administration lab exercise. It is to install and set up the Nginx web server in a CentOS 9 Stream server. The CentOS stream server runs under VMware workstation running in the student PC. The tasks for each student include Nginx installation, creation of a simple web page and finally testing for Nginx server operation. The lecturer is required to monitor the progress of all students and check which task is completed successfully. In case there is any problem, the lecturer should perform troubleshooting within the student’s CentOS Stream server VM.

**Demonstration/Show Case**

**A diagram of a computer network

Description automatically generated with low confidence**

Figure 3 Network setup for home lab monitoring system using CALDERA

The above diagram shows the setup of the proposed solution for remote monitoring of the server administration lab using CALDERA. Using the terminologies of Cybersecurity, the lecturer acts in the role of an adversary in CALDERA; all students act as the role of victims; and the server VMs administered by the students are the victim servers.

The lecturer uses the agent script generation function in CALDERA to generate the reverse shell agent script for the Linux platform as shown in the diagrams below.

A screenshot of a computer

Description automatically generated

Figure 4 CALDERA – agent script generation

A screenshot of a computer

Description automatically generated

Figure 5 CALDERA- platform selection for agent script generation

A screenshot of a computer

Description automatically generated

Figure 6 CALDERA – generated agent script

The agent script can be sent through email or posted in Moodle (VTC e-learning platform). Students download and execute the agent script in their server VM. Then, the lecturer can identify each student's virtual machine in the CALDERA Agents console (as shown in Figure 7).

A screenshot of a computer

Description automatically generated with medium confidence

Figure 7 CALDERA Agents Console

To check tasks assigned to students, the lecturer is required to set up a series of adversary abilities. Each ability corresponds to one or a series of Linux commands for checking whether a task is completed. Then, these abilities are stored under an adversary profile. The diagrams (Figure 8 and 9) below show the abilities created and the corresponding adversary profile in CALDERA.

A screenshot of a computer

Description automatically generated

Figure 8 CALDERA – abilities

A screenshot of a computer

Description automatically generated with medium confidence

Figure 9 CALDERA – adversary profiles

After the above setup, the lecturer can check the progress of each student at any time by creating an operation and executing the adversaries profile created in the previous step. The diagrams (Figures 10 and 11) show the progress of assigned tasks. If it is in green color, it means the student completes the assigned tasks successfully. The red color means the task is not complete.

A screenshot of a computer

Description automatically generated

Figure 10 CALDERA console for an operation – checking the progress of a selected student

A screenshot of a computer

Description automatically generated with medium confidence

Figure 11 CALDERA console for an operation - check whether a task is completed

A screenshot of a computer

Description automatically generated with medium confidence

Figure 12 Display output of checking script for a special task

A screenshot of a computer

Description automatically generated

Figure 13 CALDERA console for checking all assigned tasks of a student

The lecturer can also check all the student’s progress in an operation. The diagrams (Figures 14 and 15) below show the operation console for checking all students’ progress. The result can be output to JSON format for further processing such as marking and recording the performance of each student in this lab.

A screenshot of a computer

Description automatically generated

Figure 14 CALDERA Console for checking the progress of all students

A screenshot of a computer

Description automatically generated

Figure 15 CALDERA Console to view status of all students

During the lab section, if troubleshooting is needed from any student, the lecturer can issue Linux commands directly to the student server VM through the operation tab of the CALDERA operation console. The output of the commands can be viewed directly in the console. It can help to identify the problem of the student effectively. The following diagrams (Figures 16 and 17) are an example that the lecturer trying to check the status of SELinux by using the Linux command, **sestatus**, and the output of the command can be viewed from the CALDERA console operation tab.

A screenshot of a computer

Description automatically generated

Figure 16 Execution of troubleshooting commands

A screenshot of a computer

Description automatically generated

Figure 17 Output of the troubleshooting commands

**Further Development**

CALDERA provides a range of built-in adversary profiles, each with its own set of abilities that correspond to Mitre Att@ck Tactics, Techniques, and Procedures (TTPs). By making only minor modifications, some of these adversary profiles can be directly applied to labs in different Cybersecurity modules, including Penetration Testing, Windows Administration and Security, and Digital Forensics and Incident Response.

All data collected by CALDERA can be output in various formats, such as JSON, which can be used to generate lab progress reports. Automation scripts can be developed to automatically grade assessments.

CALDERA supports the development of plugins; it is possible to create a highly automated monitoring system that provides interactive support to students performing their labs any time at home. This system can also provide support or guidance to students at certain automatic levels, making the learning process more efficient and effective.

**Conclusions**

Laboratory work or hands-on practical labs are considered to be at the heart of learning in the discipline of Cybersecurity and can have a strong impact on students’ learning outcomes. Due to the lockdown of COVID-19, for the last three years, it was not possible to have face-to-face classes or on-premises hands-on practical labs. Students do their practical lab exercises at home with virtualization technology. In case there is a problem encountered, the teacher/lecturer is extremely difficult to perform troubleshooting. A cost-effective and scalable remote lab monitoring and supporting system is needed. Open-source Communication and Control server (C&C) is a perfect match for the requirement. This paper demonstrates how to apply the remote monitoring technology of Cybersecurity to effectively and efficiently support home labs.

In conclusion, the post-COVID era has brought about unique challenges in delivering cybersecurity education remotely. However, the use of remote access technologies such as the open-source communication and control server CALDERA can effectively support and monitor student progress in practical labs. By using this technology, instructors can troubleshoot problems in real-time, track student progress, and apply automatic scripts to assess the lab work performance of the student. This technology has the potential to become a full-fledged online training system for the delivery of cybersecurity practical labs. As such, it represents a valuable tool for cybersecurity education in the post-COVID era and beyond.

**References**

Brezo, F., & Santos, I. (2012). C&C techniques in botnet development. In *Proceedings of the 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)* (pp. 1-6).

Aguilera-Hermida, A. P. (2020). College students’ use and acceptance of emergency online learning due to COVID-19. *International Journal of Educational Research Open*, 1, 100011.

Ogunyemi, A., & Amresh, A. (2016). The use of virtual machines to support hands-on learning experiences in undergraduate systems-oriented courses. *Journal of Computing Sciences in Colleges*, 31(6), 96-104.

Caldera. (n.d.). CALDERA documentation. Retrieved May 19, 2023, from <https://caldera.readthedocs.io/en/4.1.0/>