A Zero-Entry Cyber Range Environment for Future Learning Ecosystems

Elaine M. Raybourn, Michael Kunz, David Fritz, and Vince Urias

Abstract Sandia National Laboratories performed a 6-month effort to stand up a "zero-entry" cyber range environment for the purpose of providing self-directed practice to augment transmedia learning across diverse media and/or devices that may be part of a loosely coupled, distributed ecosystem. This 6-month effort leveraged Minimega, an open-source Emulytics™ (emulation + analytics) tool for launching and managing virtual machines in a cyber range. The proof of concept addressed a set of learning objectives for cybersecurity operations by providing three, short "zero-entry" exercises for beginner, intermediate, and advanced levels in network forensics, social engineering, penetration testing, and reverse engineering. Learners provided answers to problems they explored in networked virtual machines. The hands-on environment, Cyber Scorpion, participated in a preliminary demonstration in April 2017 at Ft. Bragg, NC. The present chapter describes the learning experience research and software development effort for a cybersecurity use case and subsequent lessons learned. It offers general recommendations for challenges which may be present in future learning ecosystems.

1 Introduction

Most technology-mediated learning interventions, instructions, and assessments are intended for use in blended (instructor-led) or formal (schoolhouse-based) learning contexts. Most cybersecurity education geared for adult learners is delivered online via e-learning slide presentations, webinars, video lectures (see Federal Virtual Training Environment https://niccs.us-cert.gov/training/federal-virtual-training-environment-fedvte), or face-to-face consisting primarily of lecture,

E. M. Raybourn (✉) · M. Kunz · V. Urias
Sandia National Laboratories, Albuquerque, NM, USA
e-mail: emraybo@sandia.gov; mkunz@sandia.gov; veuria@sandia.gov

D. Fritz
Sandia National Laboratories, Livermore, CA, USA
e-mail: djfritz@sandia.gov

Ç. K. Koç (ed.), *Cyber-Physical Systems Security*,
https://doi.org/10.1007/978-3-319-98935-8_5

hands-on individual practice, team practice, and/or Capture the Flag (CTF) exercises. While cybersecurity education may require self-motivation for student success, few curricula are actually designed to facilitate *informed self-directed learning* such as that found in an apprenticeship, internship, or mentorship program (see Sandia National Laboratories Technical Internships to Advance National Security [TITANS] http://www.sandia.gov/titans/), and even fewer still offer *connected* learning experiences such as those supported by storytelling that comes to life in and across different media—offering off-ramps to auxiliary resources and activities intended to incentivize rich on-demand, self-directed, informal learning. Connected learning experiences are facilitated by transmedia learning. *Transmedia learning* is defined as the scalable system of messages representing a narrative or core experience that unfolds from the use of multiple media, emotionally engaging learners by involving them personally in the story [1].

A science and technology (S&T) goal for many is to enable personalized, data-driven, and lifelong technology-enabled learning. The long-term goal is that ecosystems of connected, transmedia systems will provide adaptive, personalized learning that is facilitated by data shared among technologies in the ecosystems. While transmedia learning is a goal of future learning ecosystems, near-term emphasis is usually placed on supporting instructor-led, blended, linearly sequenced, or stand-alone learning via different web-based technologies. In that respect, future transmedia learning ecosystems—those that offer self-directed, connected, story-driven learning experiences—must not only engage the learner personally but also provide authentic experiences for learners of all levels. The S&T challenge is to create rapidly configurable environments and learning pathways flexible enough to support a learner's unique and authentic journey across multiple media and modalities, and designed to promote self-directed exploration over time.

Our team developed *Cyber Scorpion*, a Capture the Flag cyber range lab environment to address this gap. Cyber Scorpion can share exercise completion data through a web interface using the xAPI specification [2] saving to a Learning Record Store (LRS). Subsequent sections describe the research and development effort of Cyber Scorpion for the specific use case of offering off-ramps to auxiliary cybersecurity resources, activities, and lessons learned. Cyber Scorpion logged when learning started, when milestones were being attempted, and when milestones were completed. While Minimega, the technology underlying the virtual lab in Cyber Scorpion, is capable of stealth assessment (see [3]), learner actions and behaviors in the emulated environment were not logged or recorded in the present effort.

2 Limitations of Current Practice

As described in the previous section, the current practice of cybersecurity training for adult learners is largely delivered online via e-learning slide presentations, webinars, video lectures, slide presentations, or face-to-face consisting primarily of lecture, hands-on individual practice, team practice, and/or Capture the Flag

(CTF) exercises. However, the current practice of pass/fail assessment results in insufficient fidelity to reveal useful detail about whether/how/when “learning” is occurring. Although adult active duty military or reserve learners may engage in highly orchestrated exercises distributed across installations in the United States or around the globe, these exercises, such as Cyber Flag and Cyber Guard, may only occur once a year. Additionally, many ranges used for these exercises are “heavy”—being bound to a physical infrastructure, particular vendor software stack, databases, and large maintenance staff.

Military-grade cybersecurity game-based training is gaining popularity, but these games are usually not lightweight and rapidly configurable, nor rapidly scalable. Other options for training are more “academic” and often do not reflect real-world network or adversary behavior. Modernization will require much more realistic scenarios utilizing robust models, simulations, and emulations, with adaptive, persistent, and blended live, virtual, constructive, and gaming environments [4]. According to retired CYBERCOM Chief of Staff, Air Force Major General Jim Keffer, “We don’t have—but we need—an exercise environment where you do rehearsals, go against adversary networks, and figure out ways to better protect your own . . . the team training, the force-on-force training, that is primarily limited by a lack of a persistent training environment” [5].

Another limitation to the current practice is the lack of congruency with respect to language and meaning leading to misunderstandings. For example, the definitions for emulation and simulation are often confused, especially when referring to cyber training environments. *Emulation* has been defined as a reproduction or replica of the function or action of a particular system, whether it is software or hardware. An emulation replicates a system as specifically and exactly as possible. *Simulation*, on the other hand, models the internal state of a system and is an abstraction rather than an exact replica. Emulation may or may not model the internal state of a system. In cybersecurity operations training, it is important to “train as you fight, fight as you train.” To do this, training should be executed in *emulated* systems and networks.

Finally, cyber operations training is not nearly as on-demand as required, so learners do not have the opportunity to continually train as much as they should. Therefore, much of the current practice is either limited to training that is not rapidly configurable, unengaging, and stale or highly engaging training that is executed by face-to-face teams or via logistically complicated, over-orchestrated distributed exercises.

To summarize, there are at least three limitations to the current practice that Sandia Cyber Scorpion sought to address:

- Not rapidly configurable or scalable
- Not persistent or on-demand
- Not sufficiently realistic

2.1 Specific Problem Being Solved

Currently, cyber defender training is performed on (1) operational systems, (2) a limited testbed, or (3) simulated models of the system of interest. Each of these has inherent limitations that can be addressed by using an emulated system.

According to Urias et al. [6], "Analysis and training on operational systems is usually limited to the most benign levels since any disruption to the operational system has potentially severe consequences. Testbeds for analysis and training are typically expensive and time-consuming to construct and deploy, single-purpose, and difficult to maintain. Another option for cyber defender training would be a simulated environment. In many cases however, the simulation program code needs to be developed to simulate the system and devices in question or extensions need to be made to answer specific questions. These (sometimes buggy) simulation codes typically do not depict an accurate picture of the system. To increase simulation result accuracy, models have to be extended and validated."

These processes can be time-consuming and inefficient. Thus there is a need for the ability to rapidly create, tear down, recombine, and reuse high-fidelity replications, or emulations, of information systems for cybersecurity training. Our team has participated on multi-year research projects in the development of new strategies and methodologies that enable researchers to quickly and accurately model information systems hosts and networks of interest for cyber analysis and training. Therefore an early determination was made that Cyber Scorpion should serve as a "zero-entry" practice environment.

The specific problem being solved by Cyber Scorpion is the demonstration of the ability to offer a cyber range capability with a government-owned, open-source virtual machine (VM) management tool called Minimega via a web interface with the ability to share learner data. Cyber Scorpion, by virtue of being an emulated environment, is rapidly configurable and able to support persistent training that allows learners to "train as they fight, fight as they train."

3 Research

3.1 Research Question

The authors of the present chapter addressed the following research question, "What are the learning experience challenges associated with bringing a zero-entry, cyber range environment to future learning ecosystems that allow learners and instructors to transition among learning activities, devices, and modalities?"

Subsequent sections detail the approach taken by our team for design and software development, followed by the lessons learned.

3.2 Learning Science Approach

Learning experience design (LX) is a subset of user experience design (UX) that addresses the synthesis of learning sciences, human-computer interaction, and design thinking. Learning experience design puts the learner at the center of the product or service design process. As more immersive simulations and persistent transmedia learning [1] experiences are developed with distributed exercise environments, games, and virtual/mixed/augmented realities, it can be useful to ground approaches in theory such as Distributed Cognition (see Sect. 3.2.2) and design methods such as the Simulation Experience Design Method [4]. The Simulation Experience Design Method specifically aims to bring to the fore initial assumptions, biases, or notions of expectations that inform the decisions shaping the design of learning experiences. Sections 3.2.1 and 3.2.2 further discuss the method used to design the learning experience and its theoretical underpinning.

3.2.1 Simulation Experience Design Method

The Simulation Experience Design Method and Framework [4] is a process that addresses the design of learning as a system of experiences that exists within an emergent, adaptive cultural context that the designer strives to engender throughout engagement, as well as before, between, and after formal learning has concluded.

The word simulation in the name of the method refers to an experience in which the role of a human, environment, or both can be simulated. The Simulation Experience Design Method, briefly described in this section, has been applied by the author and others to serious game design [4, 7] and transmedia learning [1]. Whether UX or LX, experience design solutions require that designers understand what makes a good experience first and then translate these principles, as efficiently as possible, into the desired medium without the technology dictating the form of the experience. In simulated environments in which learners are creatively problem solving together, one's experience may be unpredictable, may not have a right or wrong approach, or may not be what the designer intended. The Simulation Experience Design Method can be helpful in framing the co-creation of problem-solving opportunities as an open-ended, rich *system of experiences* that fosters learning (Fig. 1).

The Simulation Experience Design Method suggests that supporting equitable intercultural communication and learning is comprised of several salient elements, among them (1) the *interactions* or type of communication (interpersonal, group, etc.); (2) the *narratives* that are co-created by interlocutors; (3) the *place*, or context, in which narratives occur; and (4) the *culture that emerges* from the social construction of experience [8]. Following the circular framework from upper left to upper right, design tasks may then be considered as facilitating a journey or connected learning experience from interactions to emergent culture that iteratively lead to new interactions spawned by the emergent culture. Use of the framework

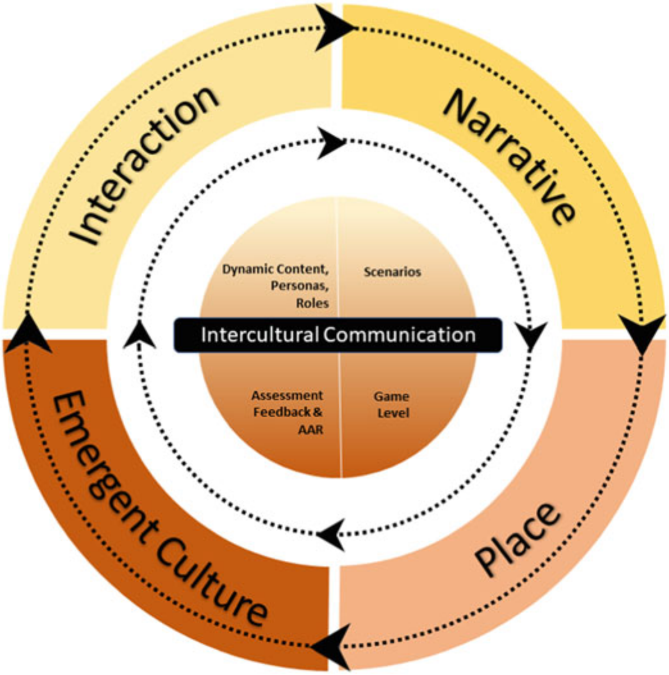
Interaction
Narrative
Place
Emergent Culture
Dynamic Content, Personas, Roles
Scenarios
Intercultural Communication
Assessment Feedback & AAR
Game Level

Fig. 1 Simulation Experience Design Method and Framework [4]

is intended to improve the quality of equitable learning in collaborative, immersive environments such as serious games, simulations, and transmedia storytelling and learning ecosystems [1, 4, 7].

Finally, by treating intercultural communication as a *core value*, the individual cultural backgrounds the players bring to their experiences are considered strengths, not design liabilities. As we strive to create engaging immersive experiences, differing cultural values of designers, developers, stakeholders, and players can create a myriad of complications and competing desires or expectations. The Simulation Experience Design Method can serve to socially construct narratives and establish a shared understanding for thoughtful analysis from which to better ground assessment and evaluation of human performance, creativity, and expertise [9].

3.2.2 Distributed Cognition Theory

The theory of Distributed Cognition, advanced by Edwin Hutchins [10], provides a framework from which cognition can be viewed as an ecosystem involving people, artifacts, tools, and environments. The Simulation Experience Design Method and Framework applies Distributed Cognition and the notion of “cognition in the wild” to LX design. Cognition in the wild refers to human cognition as it naturally occurs and adapts in the everyday world—situated in culturally constituted human activity [10]. Distributed Cognition is a distributed, social process in which human knowledge and cognition are not confined to the individual and often reside in other people, tools, or artifacts. As we move along the Simulation Experience Design Method and Framework to supporting learning with technology, we can see the application of Distributed Cognition. For example, learners may work in face-to-face teams, but they also use media—papers, pencils, tablets, collaborative tools, computers, etc. They may engage in dialogue as they walk through Cyber Scorpion exercises, but they may also take notes or save data to extend their working memory. Their cognition may be characterized as distributed among artifacts and people. After the 10-hour test and demonstration, they may have engaged in online discussions and/or crowdsourced information via social media. Their cognition is also distributed among persistent artifacts such as digital messages that facilitate asynchronous collaboration and help them remember, understand, and connect with others. In this sense, their working knowledge exists among diverse systems and cannot truly be understood without taking this socially distributed sense-making into account [11]. Distributed Cognition underpins distributed learning science and particularly transmedia learning, by providing a grounding theory for the learning experience facilitated by transmedia ecosystems utilizing diverse media, devices, and modalities.

3.3 Learner Analysis

The John F. Kennedy Special Warfare Center and School (JFKSWCS) is the United States Army's school for professional training of Army special operations forces personnel. The United States Army JFKSWCS (USAJFKSWCS) is also responsible for training US Army Reserve and National Guard Civil Affairs and Psychological Operations conventional forces. As a component subordinate command of the United States Army Special Operations Command, JFKSWCS enables the Army Special Operations Force (ARSOF) force modernization and conducts institutional training through a headquarter, center, and school. There are two formal distance learning (DL) instances in JFKSWCS training—(1) the Reserve Component Civil Affairs (CA) Phases 1 and 3 of Captains Career Course and (2) the Psychological Operations (PSYOP) Reserve Officer Qualification Course Phase 1.

Little was known about the individual learner's job/role at the time of Cyber Scorpion learning experience development. However, we assumed that since learners could potentially be from CA, Military Information Support Operations Command (MISOC) formerly PSYOP, and SF (Special Forces), we could apply this general information to the design of a zero-entry environment that would engage beginners, intermediate, and advanced learners.

We also observed that the learners could be highly motivated individuals who are risk-takers, adaptive, and competitive. They could speak a second or third language or be in the process of learning one. Trained in understanding the human

Table 1 Terminal learning objectives

1.	Describe network architecture, browser configuration, and hardware/software for secure Internet browsing
2.	Understand social engineering concepts in cyberattacks (e.g., phishing, waterhole attacks, lures)
3.	Run penetration tests to locate potential security threats (network enumeration using NMAP, Wireshark)
4.	Know how to analyze a network packet capture file
5.	Recognize, document, and analyze a successful attack from point of entry, pivoting, and systems controlled
6.	Successfully execute the steps in creating a software exploit

domain, these individuals could have prior knowledge that is relevant to the topic of social engineering, but not likely network forensics, penetration testing, or reverse engineering. As they may already be skilled social engineers, their expectations could be high regarding this topic, and it is likely that this topic will be easiest for them and of interest. In either case, they would not like to waste their free time, since they do not normally get a lot of it. Given the background information above, we concluded that the learning experience be designed to address the variance in prior knowledge, interest, and familiarity with the technical topics.

3.4 Cybersecurity Terminal Learning Objectives

Informed by the learner analysis, we identified six terminal learning objectives (TLOs) for cybersecurity that were based on the National Cybersecurity Workforce Framework [12]. The terminal learning objectives are documented in Table 1.

Given the tactical emphasis of the JFKSWCS, we decided to address terminal and enabling learning objectives by focusing on providing "hands-on practice" in the emulated Cyber Scorpion environment.

4 Cyber Scorpion Design

Based on the observations from the learner analysis, our technical approach for the preliminary user experience demonstration was to design an experience that facilitated a "zero-entry" mindset intended to incentivize learners' curiosity to dig deeper and explore transmedia content. Using The Simulation Experience Design Method [4], a hypothetical narrative was generated to identify potential challenges and opportunities that might arise during the learning experience demonstration [13]. This narrative, or learner sketch, also informed the design of Cyber Scorpion exercises and its interaction experience approach.

4.1 Cyber Scorpion Learner Sketch

An excerpt of the full learner sketch is provided in the present section to orient the reader toward the intended use of Cyber Scorpion in the context of the transmedia learning demonstration.

> US Army Captain Angela Diablo has volunteered for a 4-day cybersecurity transmedia learning experience. She has volunteered because in her support role as a PSYOP specialist she needs to leverage cyber technologies to conduct research for the development of PSYOP campaigns. She's interested in learning about offensive and defensive techniques. She arrives at the computer lab and sits in front of an open work area.
>
> The facilitator directs her attention to the devices in front of her: a laptop, a smart phone, ear buds, and a tablet. She picks up the tablet and notices content on the basics of social engineering. There is a flashcard game that is fun for a while. She watches a video on the smart phone. She looks at the clock and 20 minutes have gone by. This background information is okay, but she wants to test her skills. She logs into the laptop and sees several applications: a lecture-based cyber security course, some penetration testing tools with associated exercises, videos and PowerPoint slides, read me files on how to access a cyber range called Cyber Scorpion, and a game. She starts playing the education game. It starts out easy, but she soon realizes she doesn't understand how to solve the challenges.
>
> She decides to brush up her skills with Cyber Scorpion, where she can learn pentesting and gain hands-on experience. While getting hands-on training in the Cyber Scorpion environment, she proceeds at her own pace through the scenarios and puzzles by watching Cyber Scorpion step-by-step video tutorials and accessing other resources available on the laptop or from the Internet. Cyber Scorpion allows her to use virtual machines from the web interface without downloading a plug-in. The zero-entry approach gradually increases the difficulty without overwhelming her confidence. After a few hours of hands-on training, she's ready to try the game or go straight to the Cyber Scorpion "capstone" final assessment exercise.

We anticipated an interaction experience during the demonstration for motivated, self-directed learning. Cyber Scorpion was designed to increase learner familiarity and boost confidence. We believed this approach to LX could also engender curiosity and encourage learners to engage other content longer.

Subsequent sections describe the software development approach and underlying technology for Cyber Scorpion.

5 Software Environment

5.1 Cyber Scorpion Underlying Technology: Minimega

Cyber Scorpion leverages a distributed virtual machine (VM) lab environment that is managed by using an open-source tool called Minimega (see http://Minimega.org, https://github.com/sandia-Minimega/Minimega). Cyber Scorpion reflects a low cost of entry by being accessible from a modern browser which allows learners to train from whichever platform they chose, whether that be desktops, laptops, tablets, or phone. The virtual machine state was synchronized across all their platforms facilitating multitasking and allowing seamless transition from platform to platform. Thus, Cyber Scorpion was able to provide off-ramps for more connected learning experiences such as those supported by storytelling across different media and on-demand, self-directed learning.

Minimega was designed to easily integrate VMs into other systems, training toolkits, and front-ends through a simple scripted interface.

The Minimega platform can be installed on both commodity desktop Linux environments for individual training and on clusters of machines, which allow for large-scale team training/experimentation. Sandia National Laboratories leverages decades of supercomputing and high-performance computing (HPC) expertise to provide scale to networks. In extreme scenarios, Minimega has been able to launch experiments with over 4 million endpoints.

Between 2012 and mid 2013, Minimega supported more than 12 active projects for university and private industry use that were not involved with Sandia National Laboratories. Minimega is also used by over a dozen government sponsors for test and evaluation of hardware and software stacks in representative environments.

5.2 Software Development Approach

Cyber Scorpion focused on providing approximately 10 hours of digital content (hands-on training environment, video walk-through, and exercises) to introduce and coach learners on topics consistent with the learning objectives. Straightforward exercises were developed to incentivize learning in an immersive, realistic cyber environment. Examples of the analysis techniques, procedures used to perform offensive and defensive maneuvers, and exposure to common tools were provided.

Micro scenario exercises were designed to "get familiar with tools and techniques" while distilling "key nuggets" of information for micro training sessions, etc. Videos of "what right looks like" provided lead-ins to problem-based learning. Cyber Scorpion environment served as a "capstone" final assessment exercise for the test and demonstration.

Cyber Scorpion is a Jeopardy-style Capture the Flag interface based on the Open-Source Technology CTFd (see https://github.com/CTFd/CTFd). Identity management was handled by the Open-Source Project Keycloak, and when people logged into their machines at the start of their day for training, they did not have to log in again. Actions learners performed in the web interface, such as starting or completing a challenge, were reported to a repository. From whatever platform users chose to use (tablet, mobile, desktop, etc.), they would be presented with the responsive web page in Fig. 2.

When a challenge tile was clicked on, the learner was presented with a question and a link to open a new tab that instantly bridged users into a virtual lab where they had control of their own remote machines. These machines were required to solve the challenge and provided real-world hands-on cybersecurity experience. The following screenshot shows the virtual machine integration in the browser (Fig. 3).

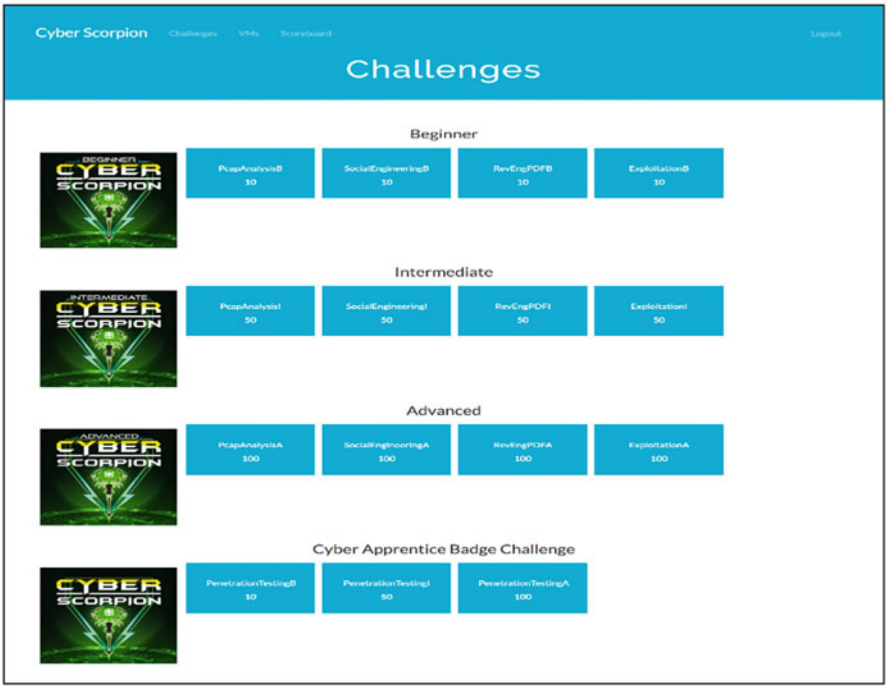

Fig. 2 Cyber Scorpion jeopardy framework (CTFd)

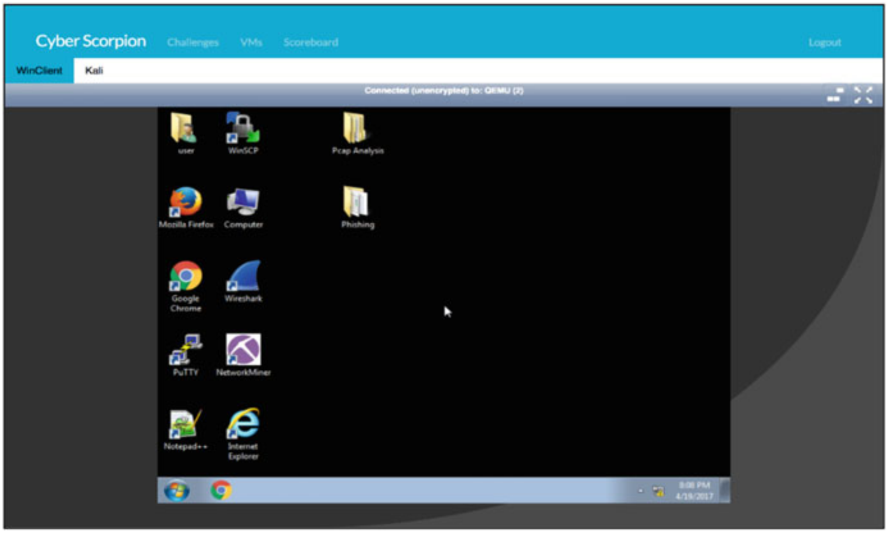

Fig. 3 Cyber Scorpion jeopardy framework (Minimega)

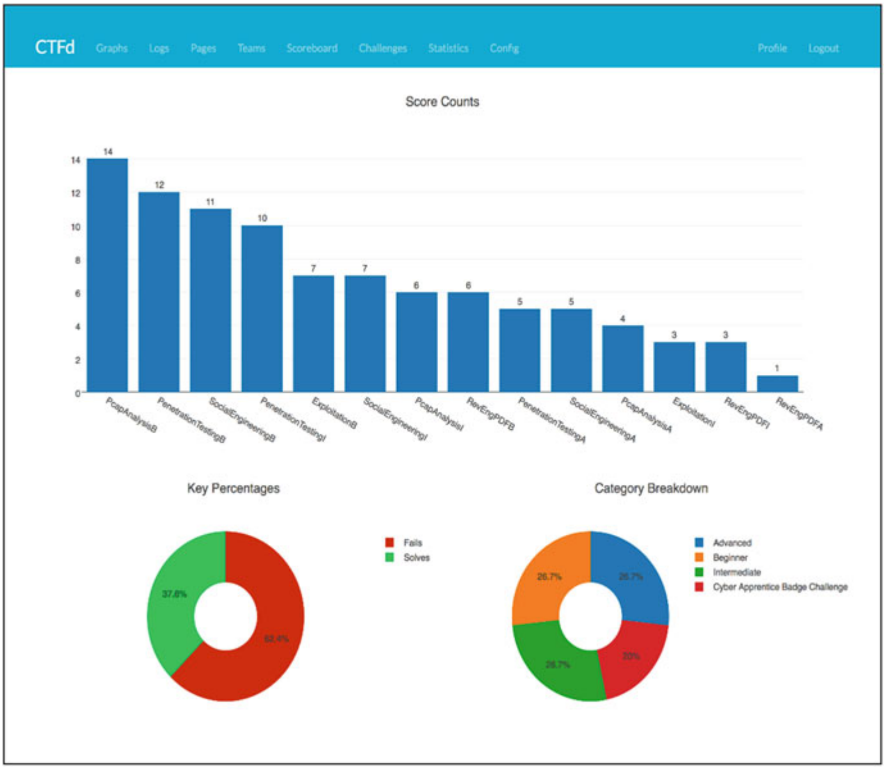

Fig. 4 Cyber Scorpion Jeopardy scoreboard

This session, where learners could control the keyboard and mouse, was shared and synced live between whatever platform learners chose to use, including a mobile phone or tablet. The remote machines had training modules with objectives that when completed netted a secret phrase, commonly referred to as a flag, hence "Capture the Flag."

This flag could then be entered by the learner into Cyber Scorpion's Jeopardy board, and when submitted, the framework would send predefined progress statements to a repository.

The CTFd Jeopardy framework also has a built-in scoreboard, and during the competition, administrators could follow what challenges were being completed and could track the progress of the learners (Fig. 4).

A pilot test was conducted a month prior to the demonstration at Ft. Bragg. During the pilot test, Cyber Scorpion was able to prove scalability, demonstrating 50 simulated learners heavily using the application. It was concluded that Cyber Scorpion would demonstrate well as the exercise environment elicited positive feedback and was proposed by the SME assisting the research team to be the culminating learning assessment environment for learners who would later pursue the network forensics training track.

6 Learner Experience Demonstration and Lessons Learned

A preliminary learning experience demonstration of Cyber Scorpion (and other technology resources) was conducted at the JFKSWCS, Ft. Bragg, NC, in the spring of 2017 during a 10-hour period of spaced exposure (2 hours per day over 4-day period). Sixty-seven learners from ages 18–30, volunteered to use the resources during the 10-hour period to increase their understanding of cybersecurity in two different areas: social engineering and network forensics. Participants used resources at their own discretion. All had prior experience with mobile phones and computer-based e-learning, but fewer were familiar with tablets, simulations, and games [14]. Some completed certain activities to achieve badges in "social engineering" and "cyber apprentice." To achieve the badge for "cyber apprentice," participants completed the pentest exercises in Cyber Scorpion as their culminating "competency" learning assessment.

Learner anecdotal feedback indicated that the ability to move from an interactive multimedia instructional (IMI) resource (i.e., game) and Cyber Scorpion (real-world hands-on cyber range lab) worked well. Participants explored a topic in the game and then tested their knowledge using Cyber Scorpion exercises.

User feedback was captured during the exercise and in one-on-one interviews conducted at the end of the demonstration to better gauge whether learners thought Cyber Scorpion could be better tailored in the future. The learners who volunteered for the test and demonstration sessions were mostly nontechnical. Teaching cybersecurity topics to people of such varying backgrounds is very difficult, and the feedback illuminated this.

For some, the exercises were too easy, while for others (without command line experience) they found the exercises appropriate. Without the ability to conduct a user needs analysis, Cyber Scorpion content was developed to be very direct and capable of being learned without much prior experience. With more information about the learners in advance, Cyber Scorpion could have been better tailored to be more in line with users' existing knowledge, skills, and abilities (KSAs). It's interesting to note that, as predicted, other learners focused on completion badges and a chance to take home a coin as a prize. These learners achieved their own training goals by being self-directed and actively sought out exercises that were interesting to them, which they felt incentivized to complete.

In general, the preliminary learning experience demonstration illuminated valuable lessons learned for future development. During this 6-month effort, we addressed the following research question, "What are the challenges associated with bringing a zero-entry, cyber range environment to future learning ecosystems that allow learners and instructors to transition among learning activities, devices, and modalities?"

A number of key observations were made during this preliminary development and demonstration cycle. First, a few factors contributed to Cyber Scorpion's successful demonstration:

1. *Leveraging open-source frameworks*. Cyber Scorpion itself is an open-source framework, and additional tools such as the scoreboard system were quickly integrated into its platform.
2. *Not attempting to be everything to everyone*. Focusing the exercises on tasks that supported learning objectives is consistent with modern cyber-education pedagogies. While there is an opportunity to iterate and improve pedagogical approaches, the "zero-entry" approach appeared to work well given the learners, the difficulty level of the content, and amount of time on task, and spaced exposure.
3. *Using contemporary technologies*. Many educational frameworks are outdated soon after deployment, and this is especially true with cyber-education frameworks. The use of a highly configurable, emulated practice environment contributed to its success.

In addition to these success indicators, we observed several challenges or areas where improvements could be made in future phases. They include:

4. *Scalability*. We provided small-scale hosting for the Ft. Bragg demonstration via an ad hoc network connection and development hardware. While successful, the need for locally hosted infrastructure, scaled to the expected audience, is critical for continued success.
5. *Atypical interfaces*. While an S&T goal is to enable personalized, data-driven, and lifelong technology-enabled learning, many of the envisioned interfaces are atypical of those most cybersecurity professionals expect to use. By providing a more generic (workstation, tablet, Android mobile phone, or other OS) accessible interface, several technical limitations could be avoided.
6. *Cybersecurity*. Due to the potential sensitivity of learner privacy and data security, a design assurance perspective (designing cybersecurity into the prototypes and subsequent iterations) is recommended when designing new systems for training and education [15]. Also see Sandia National Laboratories IDART—Information Design Assurance Red Team (http://www.idart.sandia.gov/).

7 Limitations and Future Work

Cybersecurity training is not nearly as on-demand as required, so learners do not have the opportunity to continually train as much as they should. Much of the current practice is either limited to training that is not rapidly configurable, unengaging, and stale *or* highly engaging training that is executed by face-to-face teams or via logistically complicated, over-orchestrated distributed exercises. Sandia intended to address this gap with Cyber Scorpion, a zero-entry cyber range environment offering off-ramps to auxiliary resources and activities intended to incentivize rich on-demand, self-directed, transmedia learning.

As noted previously, Capture the Flag (CTF) exercises may not provide adequate, real-time assessments of recorded events or facilitate observation of human performance without introducing artifacts into the system. Additionally, there is rarely a standardized concept or methods for offering and assessing the efficacy of cyber training, even though multiple recommendations to develop and implement standards have been made [6].

Few CTF exercises are supported with auxiliary material to enable on-demand, informal learning. Future development could better address this gap through the application of design principles and methods toward transmedia learning [1].

CTF-style measurement, in the long run, does not have sufficient fidelity to reveal much about learning that is occurring. Therefore, future research should focus on capturing and interpreting learner activity in these self-directed exercise environments.

Future work may consist the following:

- Instrument Cyber Scorpion to share (output) and leverage (ingest) learner data and/or analytics generated by other systems.
- Design and test human performance-based assessment for immersive environments.
- Develop more training modules (with varying degrees of complexity and story-driven off-ramps) for Cyber Scorpion.

8 Conclusion

In the highly VUCA environment that is cyber operations, training is obsolete as soon as it is deployed. A survey of service strategy documents highlights the shared belief of the need for training and education modernization and some congruence on how to achieve it. Modernization will require much more realistic scenarios utilizing robust models, simulations, and emulations, with adaptive, persistent, and blended live, virtual, constructive, and gaming environments. According to retired CYBERCOM Chief of Staff, Air Force Major General Jim Keffer, “We don’t have—but we need—an exercise environment where you do rehearsals, go against adversary networks, and figure out ways to better protect your own . . . the team training, the force-on-force training, that is primarily limited by a lack of a persistent training environment” [5].

This 6-month effort leveraged an existing technology (Minimega) utilized by CPT (cyber protection teams) and DOD agencies to facilitate cyber operator mission rehearsal. The resulting exercise environment, Cyber Scorpion, is a zero-entry practice/competency mastery environment.

Minimega is used by over a dozen government sponsors for test and evaluation of hardware and software stacks in representative environments. Because of this, Cyber

Scorpion can be used for training, mission rehearsal, experimentation, or testing theories and hypotheses related to training efficacy, human systems integration, learning science, visualization, and development of data-driven, learner behavior analytics.

Our technical approach to use Minimega to manage the distributed VMs for Cyber Scorpion resulted in a robust, stable software environment. Our learning science approach was successful because the exercises are purposely kept simple, approachable, and doable—to offset a potentially, unnecessarily complicated learning experience that may have otherwise introduced increased cognitive load.

In future phases, we anticipate employing better understanding of capturing learner activity in constructivist environments such as scenario-based simulations and emulated practice exercises for cybersecurity training and testing.

Acknowledgment Sandia National Laboratories is a multimission laboratory managed and operated by the National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the US Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525. This work was supported by the ADL Initiative (Contract QL6H5R66F007MP-0). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the ADL Initiative.

References

1. E.M. Raybourn, A new paradigm for serious games: Transmedia learning for more effective training & education. J. Comput. Sci. **5**(3), 471–481 (2014)
2. ADL Initiative, *xAPI-Spec* (2016). https://github.com/adlnet/xAPI-Spec/blob/1.0.1/xAPI.md. Accessed 28 Feb 2018
3. V. Shute, M. Ventura, *Stealth Assessment: Measuring and Supporting Learning in Video Games*, The John D. and Catherine T. MacArthur Foundation Reports on Digital Media and Learning (MIT Press, Cambridge, MA, 2013)
4. E.M. Raybourn, Applying simulation experience design methods to creating serious game-based adaptive training systems. Interact. Comput **19**, 207–214 (2007)
5. A. Tilghman, Without solid training options, mysterious cyber training command remains a work in progress. Military Times. (2016, 5 June), http://www.militarytimes.com/story/military/tech/2016/06/05/military-cyber-offensive-defensive-weapons-training/85033862
6. V. Urias, B. Van Leeuwen, B. Wright W. Stout, in *Emulytics™ at Sandia National Laboratories*. Proceedings of MODSIM (NTSA, Arlington, VA, 2015)
7. T. Bergin-Hill, R. Creekmore, J. Bornman, *Designing a Serious Game for Eliciting and Measuring Simulated Taxpayer Behavior* (The MITRE Corporation, McLean, VA, 2014)
8. B. Laurel, *Computers as Theater* (Addison-Wesley, Reading, MA, 1991)
9. E.M. Raybourn, in *A Metaphor for Immersive Environments: Learning Experience Design Challenges and Opportunities*. Proceedings of MODSIM (NTSA, Arlington, VA, 2016)
10. E. Hutchins, *Cognition in the Wild* (The MIT Press, Cambridge, MA, 1995)
11. J. Bruner, The narrative construction of reality. Crit. Inq. **18**(1), 1–21 (1991)
12. W. Newhouse, S. Keith, B. Scribner, G. Witte, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. NIST Special Publication 800-181 (2017). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf. Accessed 28 Feb 2018

13. Folsom-Kovarik, J.T. & Raybourn, E.M., in *Total Learning Architecture (TLA) Enables Next-Generation Learning Via Meta-Adaptation*. Proceedings of the I/ITSEC (NTSA, Arlington, VA, 2016)
14. P.S. Gallagher, J.T. Folsom-Kovarik, S. Schatz, A. Barr, S. Turkaly, in *Total Learning Architecture Development: A Design-Based Research Approach*. Proceedings of the I/ITSEC (NTSA, Arlington, VA, 2017)
15. Raybourn, E.M., Fabian, N., Davis, W., Parks, R.C., McClain, J., Trumbo, D., Regan, D., Durlach, P., in *Data Privacy and Security Considerations for Personal Assistants for Learning (PAL)*. Proceedings of the 20th International Conference on Intelligent User Interfaces Companion (2015), pp. 69–72