Inefficiencies in Cyber-Security Exercises Life-Cycle: A Position Paper

Muhammad Mudassar Yamin and Basel Katt
Department of Information Security and Communication Technology
Norwegian University of Science and Technology (NTNU), Norway
muhammad.m.yamin@ntnu.no, basel.katt@ntnu.no

Abstract

Our world is becoming digitalized day by day, this leads to an increase amount of cyber-attacks by cyber-criminals. To tackle the increasing amount of cyber-attacks, cyber-security professionals are required in a high number. However, the required number of cyber-security professionals is not present. Despite the fact that academia and industry are trying to increase the number of cyber-security professionals, however, the tools and techniques used for cyber-security professional development are ineffective, as the gap between required and available cyber-security professionals is still increasing. One of the primary tools that is used in cyber-security professional development is hands-on cyber-security exercises. In this position paper, we will analyze the inefficiencies present in conducting hands-on cyber-security exercises and what can be done to reduce and eliminate those inefficiencies.

INTRODUCTION

Cyber-security exercises run attack and defense scenarios on a virtual and physical environment. A team of individuals, known as white time, creates the environment. In the environment, a team of attackers, known as red team, tries to exploit vulnerabilities present in the environment while a team of defenders, known as a blue team, tries to defend and prevent the attacks. In a recent study (Moore, Fulton, and Likarish 2017) researchers find out that such an exercise is very beneficial in cyber-security skill development. The researcher conducted knowledge surveys on participants before and after a cyber-security exercise and they found significant improvement in network security skills like ARP-Posioning, duplication in DNS entries and firewall/routers assessment as seen in figure 1.

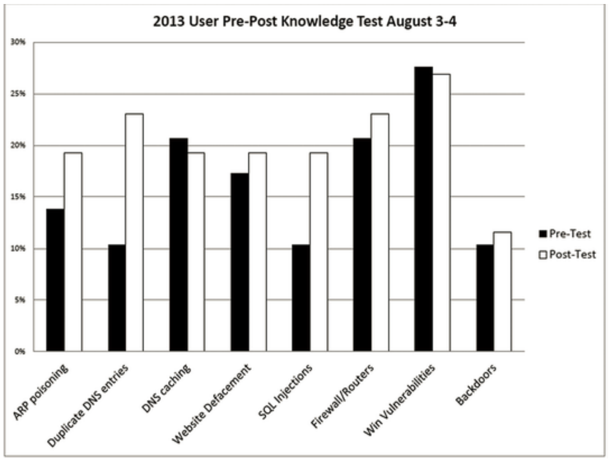

Figure 1: Participants knowledge test prior and after cyber-security exercise (Moore, Fulton, and Likarish 2017)

These cyber-security exercises are usually conducted within hours and days but the time required to prepare these cyber-security exercises often spans up to months (Vykopal et al. 2017). This makes cyber-security exercises very costly and time consuming to be used in large scale to help reducing the growing cyber-security skills gap (Furnell, Fischer, and Finch 2017). Researchers divided cyber-security exercise in five phases to get the clear picture of cyber-security exercise development and execution steps. These five phases make the cyber-security exercise development and execution life cycle (Vykopal et al. 2017):

- **Preparation** It is the lengthiest part of cyber-security exercise development and execution. It involves setting up exercise objectives, defining a story, establishing points weight-age and creating a virtual environment for the cyber security exercise.
- **Dry run** The dry run is the testing of the developed virtual environment according to exercise objective by cyber-security experts. This process also takes long time due to the changes and adjustments required for the cyber-security exercise.
- **Execution** This is the phase where the actual cyber-security exercise takes place. Teams of attackers and defenders try to achieve the set of defined objectives.

Copyright © by the papers authors. Copying permitted for private and academic purposes. In: Joseph Collins, Prithviraj Dasgupta, Ranjeev Mittu (eds.): Proceedings of the AAAI Fall 2018 Symposium on Adversary-Aware Learning Techniques and Trends in Cybersecurity, Arlington, VA, USA, 18-19 October, 2018, published at http://ceur-ws.org

Based upon the complexity of cyber-security exercise it can take hours to days.

- **Evaluation** At this phase teams performance is assessed according to the level of exercise objective completion. Feedback from participants is collected for future exercises. This phase usually takes few hours for its completion.
- **Repetition** The whole process is repeated for a set of new teams utilizing the lessons learned from the previous exercises and making necessary changes.

Conducting cyber security exercises in the described manner is a length, tedious and error-prone process (Beuran et al. 2018). Therefore, it is the position put forward that *cyber-security exercises are a good tool for cyber-security skill development but the inefficiencies in cyber-security exercise development and execution life cycle limits its ability to be widely used for cyber-security skill development.*

SURVEY OF THE LITERATURE

Researchers have been trying to reduce the inefficiencies present in conducting cyber-security exercise. In term of environment preparation phase of cyber-security exercise life cycle most of the current research is focused on reducing the time required for the preparation of virtual environment. Researchers developed multiple solutions for this problem two of them are Telelab (Willems and Meinel 2012) and SecGen (Schreuders et al. 2017) (security scenario generator). In TeleLab the researchers created multiple templates of virtual environment and developed an environment definition language, through which existing template are modified automatically to create new virtual environments for cyber security exercises. In SecGen researchers take the approach of TeleLab a bit further. Instead of defining the detailed environment schema using an environment definition language, SecGen takes the environment requirement i.e. number of machine, number of vulnerabilities, type of vulnerabilities etc. as input and randomly generate a virtual environment through the combination of existing virtual environment templates.

In the dry-run phase of cyber-security exercise recent studies (Ošlejšek et al. 2018) has shown that this phase has a lot of room for improvement. It is identified that team of human attacker and defenders does manual verification of the developed environment. That makes the process quite inefficient.

In execution phase multiple solutions in the literature are available for the execution of cyber-attacks and defense in cyber-security exercise execution. Two of the attack execution tools are Simulated Cognitive Cyber Red-team Attack Agent (SC2RAM) (Jones et al. 2015) and Scanning, Vulnerabilities, Exploits and Detection tool (SVED) (Holm and Sommestad 2016). SC2RAM is developed to mimic the red team execution steps in a cyber security-exercise. It can perform basic DoS (Denialof-Service) attack on a given network. It is still at prototyping stage and is being tested at Michigan cyber-range (Jones et al. 2015). SVED on the other hand utilizes freely available exploit tools such as metasploit and nmap and automate their operations to execute red team activities in a cyber security exercise. SVED is deployed at CRATE cyber range (Sommestad 2015). In term of cyber-defense process execution it is identified that in a cyber-security exercise skilled human professionals are required to conduct the exercise. Most of the cyber-defense research is focused on antivirus, antimalware, firewall and SIEM development, which left a lot of room for improvement in cyber-defense process execution without human involvement in a cyber-security exercise.

In term of evaluation phasen in most cyber-security exercises the theme of the exercise is CTF (Capture the flag competition). As the name suggests flags are used for point scoring and evaluation purposes. Flags contain some value of a random length when submitted to exercise or competition management systems points will be awarded. Based upon the number of points at the end of cyber security exercise or CTF competition, teams are evaluated. But the flag based evaluation mechanism is not ideal for overall performance analysis of individuals and teams. Flags only indicate that they either successful or not in completing a task, flags dont indicate at which approach they use or at which stage they feel difficult in completing the task. To tackle this problem KYPO (Čeleda et al. 2015) cyber range implemented an evaluation mechanism that is dependent upon event log monitoring. Event logs contains specific information about the activities that are being performed on a system. Based upon this information automatic evaluation is performed.

ANALYSIS AND DISCUSSION

The literature contains interesting solutions for the reduction of inefficiencies in cyber-security exercise development and execution life cycle. But these solutions have their cons as well. If we consider the autonomous generation of experimental environment by TeleLab and SecGen, we will notice that the environment which is generated is based upon an environment that is already available and if a participant already participated in an environment that is used for the creation of the environment then the participants will have unfair advantage.

The autonomous attack execution in the cyber-security exercise by SC2RAM and SVED gives a capability to the team of defenders to practice their skills without the availability of an actual attacker. But these tools are currently at an initial phase of their testing and have only basic capabilities. That makes them unsuitable for realistic training.

The scoring mechanism in KYPO cyber range is a very good approach for automatic evaluation of a participants performances in a cyber security-exercsie by monitoring the event logs created by the participants activity. However, this approach can only give a holistic view of participant performance, which is only good for calculating the overall performance of a participant, not the performance of a participant at specific phase of the cyber-security exercise.

POTENTIAL SOLUTION

Research is being carried out to address the issues present in conducting operation based cyber-security exercises. Researchers in (Jones et al. 2015) presented a novel technique to model and execute an active opposition in a cyber-security exercise. The researchers discussed the missing element in the exercise environment that is active opposition. The researchers argued that:*The environment may have static defenses, such as access control or firewalls, or a fixed set of intrusion methods to defend against, but it typically lacks any active opposition that might adapt defensive or offensive actions (e.g., monitor logs, blocked connections, exploit switching or information gathering)*

The researchers presented techniques to model cyber-attack/defense adversaries and highlighted possible approaches that can be used in the implementation of such adversaries. Based upon this research, a tool is developed for autonomous execution of highly skilled red-team attackers SC2RAM: A Deployable Cognitive Model of a Cyber Attacker (Jones et al. 2015). This tool can train blue teamers to tackle cyber-security challenges and can configure and test defensive systems. SC2RAM is deployed at Michigan cyber-range to perform basic cyber-attack simulation, as it is still at prototype stage. On the other hand tools that mimic blue teams actions in a security exercise is still need to be implemented (Jones et al. 2015). We are planning to model the roles of white, blue and red teamers with respect to each other for the development of a cyber-security exercise platform that can assist execution of cyber-security exercises in a autonomous manner by autonomously preparing the exercise environment and generating autonomous adversaries according to the exercise environment. This will effectively remove the need of human adversaries and support staff required for conducting a cyber-security exercise. By reducing these inefficiencies cyber-security exercises can be conducted regularly at a wider scale, which will help in reducing the cyber-security skill gap currently present in industry.

CONCLUSIONS

From the above discussion it can be observed that multiple phases involved in cyber-security exercise development and execution can be automated to reduce cost and time required for conducting cyber-security exercises in an efficient manner. As it was suggested earlier *inefficiencies in cyber-security exercise development and execution life cycle limit its ability to be widely used for cyber-security skill development.* We can conclude that the roles of white, blue and red teamer in a cyber-security exercise need to be executed autonomously, which will increase the efficiency of preparation, execution and evaluation phases in cyber-security exercise life cycle .This will (1) reduce the cost and time require for conducting cyber-security exercise, (2) provide better training by always-available autonomous adversaries, and (3) make cyber-exercises computationally repeatable for conducting systematic training.

References

Beuran, R.; Tang, D.; Pham, C.; Chinen, K.-i.; Tan, Y.; and Shinoda, Y. 2018. Integrated framework for hands-on cybersecurity training: Cytrone. *Computers & Security.*

Čeleda, P.; Čegan, J.; Vykopal, J.; and Tovarňák, D. 2015. Kypo–a platform for cyber defence exercises. *M&S Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence. NATO Science and Technology Organization.*

Furnell, S.; Fischer, P.; and Finch, A. 2017. Can't get the staff? the growing need for cyber-security skills. *Computer Fraud & Security* 2017(2):5–10.

Holm, H., and Sommestad, T. 2016. Sved: Scanning, vulnerabilities, exploits and detection. In *Military Communications Conference, MILCOM 2016-2016 IEEE*, 976–981. IEEE.

Jones, R. M.; OGrady, R.; Nicholson, D.; Hoffman, R.; Bunch, L.; Bradshaw, J.; and Bolton, A. 2015. Modeling and integrating cognitive agents within the emerging cyber domain. In *Proceedings of the Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC)*, volume 20. Citeseer.

Moore, E.; Fulton, S.; and Likarish, D. 2017. Evaluating a multi agency cyber security training program using pre-post event assessment and longitudinal analysis. In *IFIP World Conference on Information Security Education*, 147–156. Springer.

Ošlejšek, R.; Vykopal, J.; Burská, K.; and Rusňák, V. 2018. Evaluation of cyber defense exercises using visual analytics process.

Schreuders, Z. C.; Shaw, T.; Ravichandran, G.; Keighley, J.; Ordean, M.; et al. 2017. Security scenario generator (secgen): A framework for generating randomly vulnerable rich-scenario vms for learning computer security and hosting ctf events. In *USENIX*. USENIX Association.

Sommestad, T. 2015. Experimentation on operational cyber security in crate. NATO STO-MP-IST-133 Specialist Meeting, Copenhagen, Denmark.

Vykopal, J.; Vizváry, M.; Oslejsek, R.; Celeda, P.; and Tovarnak, D. 2017. Lessons learned from complex hands-on defence exercises in a cyber range. In *Frontiers in Education Conference (FIE)*, 1–8. IEEE.

Willems, C., and Meinel, C. 2012. Online assessment for hands-on cyber security training in a virtual lab. In *Global Engineering Education Conference (EDUCON), 2012 IEEE*, 1–10. IEEE.