Chapter 33
CYRAN:
A Hybrid Cyber Range for Testing Security on ICS/SCADA Systems

Bil Hallaq
University of Warwick, UK

Andrew Nicholson
University of Warwick, UK

Richard Smith
De Montfort University, UK

Leandros Maglaras
De Montfort University, UK

Helge Janicke
De Montfort University, UK

Kevin Jones
Airbus Group, UK

ABSTRACT

Cyber Security of ICS/SCADA systems is a major aspect of current research focus. Cyber Ranges and Test-beds can serve as means of vulnerability and threat analysis of real SCADA systems with low costs. Significantly lacking from current research, is detailed documentation of the decision process and the potential difficulties that need to be considered when undertaking the creation of a Cyber Range (CR) in order to facilitate the capture of labelled datasets which is included in this paper. This paper makes several further contributions; a review of Cyber Ranges created by Academic Institutions that influenced the criteria in creating CYRAN, the De Montfort University CYber RANge. The article presents the design implementation, the process of creating effective rules of engagement, the management and running of a Cyber Range Event (CRE) with partners from Industry and Academia and the creation of labelled datasets.

DOI: 10.4018/978-1-5225-5634-3.ch033

INTRODUCTION

Today Cyber Security is at the top of many government's agendas and extensive research is conducted (Ayres et al., 2016) with the aim of designing solutions that protect against or mitigate cyber attacks (Nickolson et al., 2012). To evaluate such solutions and to increase understanding of how cyber-attacks against organisations evolve and propagate, the replication of realistic attack and defence scenarios is paramount (Hahn et al., 2013). Technical solutions which implement low-level controls such as VPN deployment, data-diodes to ensure unidirectional information flows to the deployment of complex role-based access control mechanisms and federated identity management all serve the purpose of preventing attackers from penetrating the organization defenses. However, the development of security solutions without understanding the concrete threat or the organizations' security behaviour when faced with an incident is lacking a holistic approach to security that must bring together infrastructure, software and human variables. In this work we present the De Montfort University Cyber-Range (CYRAN) providing the infrastructure and resources in terms of scenarios and labelled data-sets to ensure that cyber security solutions are relevant to real world problems and provide insights into how cyber incident response and emergency readiness teams respond to attacks.

One of the earliest works towards the generation of attack datasets was the 1998 Defence Advanced Research Projects Agency (DARPA) in partnership with the Massachusetts Institute of Technologys Lincoln Labs (Lippmann et al., 2002). Their work produced datasets containing simulated data which replicated the traffic of a U.S. Air Force base. They undertook further work in 1999 to extend the previous datasets and released a final extension which addressed specific attack scenarios in 2000. Much research has subsequently been written regarding the shortcomings and usefulness of the DARPA datasets, McHugh (2000), Mahoney (2003), Thomas (2008). Irrespective of these works, these datasets, while innovative at their time, are now nearly 16 years old. As a result they can no longer be considered as representative of modern traffic containing examples of current Advanced Persistent Threats (APT) and Advanced Evasive Threats (AET).

Further work to address the lack of available data-sets was undertaken by Sangster (2009). In order to generate the data, they created a Capture the Flag (CTF) environment, running attack and defense scenarios. The attacking participants were limited to military and government security agencies who launched attacks across a Cyber Range (CR) over a four day period. It is logical to assume that such participants would behave with a nation-state mind set and attack and defend accordingly. Therefore, from a typical corporate enterprise and/or production environment, the subsequent datasets could be potentially viewed as not representative of typical enterprise traffic and related attack types. However, this work clearly proved the efficiency of using CRs to produce unique datasets.

Since the publication of these datasets, there has been little activity to produce and capture datasets that can be shared openly with the wider audience. Rarer still is the ability to find datasets containing traffic and industrial system protocols or specific attacks on Industrial and Automation Control Systems (IACS) and Supervisory Control and Data Acquisition (SCADA) equipment. Yet access to such data is critical to validate and test the research in intrusion detection, networking and general cyber-security, as such systems form an integral part of our IT dependent infrastructure that is increasingly connecting traditional cyber-space with physical systems. This trend is most visible in the move to incorporate and develop the Internet of Things (IoT) for Smart-Grids, Smart-Homes, and Smart-Cities which sees computing becoming pervasive. Often cited for reasons why further work and sharing of data has not been undertaken are the valid concerns around legal and privacy issues and the difficulty in anonymis-