VIRTUAL ENVIRONMENT FOR TRAINING AUDITORS WITH INFORMATION SECURITY

Fediushyn O.I., Yatsiuk O.O., Rusanov H.O.
Kharkiv National University of Radioelectronics, Kharkiv, Ukraine

At present, many universities in Ukraine are preparing specialists in the field of cybersecurity. Developing a successful educational program to train those interested in developing the cybersecurity skill set is difficult. Most institutions interested in these programs has deal with limited resources when designing an appropriate learning environment, limited teacher time to devote to maintaining systems, limited administrative support due to misunderstanding of these skills, and accidental (or deliberate) misuse of tools and skills.

Virtual machines (VM) support many of the cybersecurity competition and lab operations. Virtual laboratories allow emulating real cyber threats and rapid generation of multiple scenarios and infrastructures.

The goal of the study is to create a laboratory infrastructure that allows instructors to quickly create virtualized environments for simulating various cyber threats. The testing environment for this demo consists of a Windows 10 , Ubuntu 16.4 , Kali linux and OSSIM. OSSIM utilizes open source security tools to retrieve, organize, and display information from network assets. The sources of this information are called “data sources”. Events from data sources are parsed and normalized through plugins which associate each log event with an “Event Type,” sometimes referred to as a “plugin_sid”, which is the name of a field in the SIEM database [1, 2]. OSSIM uses database plugins which query databases and retrieve information, transforming that information into SIEM events.

The experiment is conducted in two phases. The first phase involves observing the performance of pre-selected penetration testing tools. The tools include service fingerprinting software and vulnerability scanners. Performance metrics such as number of services identified, response time, and number of vulnerabilities detected are captured and organized into various quantitative graphs and tables in order to precisely reflect the tools’ effectiveness.

In the second phase of the experiment, based on the attack surfaces provided by the first phase, various combination of attacks are deployed on the experimental hosts in order to acquire the highest privileges. Completed attacks together with potential moves are gathered and put into various attack tree diagrams for analysis so as to find out the most effective attacks against each host.

References

1. Sandeep K. B. The Operational Role of Security Information and Event Management Systems / K. B. Sandeep/ *IEEE Security and Privacy Magazine*, 2014. Vol. 12(5).–35 pp. DOI: https://doi.org/10.1109/MSP.2014.103.

2. Sievierinov O.V., Ovcharenko M.Y. Analysis of correlation rules in Security information and event management systems. *Computer and information systems and technologies.* 2020. P. 24-25.