Using Security Onion for Hands-On Cybersecurity Labs

Ronald Gonzales, Alan Watkins, Chris Simpson

National University, San Diego, CA

Abstract

Hands-on learning allows students to apply and better understand the concepts they learn during lectures and in reading assignments. Developing hands-on cybersecurity labs is challenging because many of the tools are proprietary and expensive. The creation of labs that simulate a real environment requires significant resources and planning. The use of real malware and network traffic provides a more realistic experience but can add additional risk to the laboratory network. This paper describes how we utilized the open source Linux distribution tool, Security Onion along with real malware and network traffic captures from publicly available sources to create a challenging and realistic set of hands-on cybersecurity labs. Security Onion is a Linux distribution that is used for intrusion detection, network security monitoring, and log management. It contains a variety of network security monitoring tools and is used by many organizations to monitor networks for intrusion. With its large number of pre-installed tools, Security Onion is an excellent tool to demonstrate network security monitoring concepts and provides students a hands-on experience with application tools commonly used by industry. In this paper we discuss the technical set up, development of lab objectives, data sources, and development of learning objectives. We also discuss mapping the learning objectives of the lab to the related knowledge, skills, and abilities in the National Cybersecurity Workforce Framework and to the relevant knowledge units required for designation as a National Center of Academic Excellence in Information Assurance/Cyber Defense. Use of realistic hands-on labs not only improves the students' learning experience but also better prepares them to enter the workforce.

Introduction

National University (NU) is a National Security Agency and Department of Homeland Security Center of Academic Excellence (CAE) in Information Assurance Education that offers a Master of Science degree in Cybersecurity and Information Assurance (MS-CSIA). Hands-on labs are a core component of the MS-CSIA curriculum. Providing students with labs that utilize the application tools and techniques used by industry can be expensive. The MS-CSIA program developed a set of labs utilizing the open source Network Security Monitoring tool Security Onion along with publicly available network traffic captures with malware to create a set of challenging and realistic labs.

Security Onion

Security Onion is an open source Network Security Monitoring (NSM) suite of applications used to provide full context and visibility into network traffic[1]. Network Security Monitoring is based on the collection, analysis, and escalation of indications and warnings (I&W) to detect and respond to intrusions [2].

Security Onion is designed to facilitate deploying complex open source tools with an "easy-to-use Setup wizard" [3]. The Security Onion distribution includes a set of common network security monitoring and intrusion detection tools including Snort, Suricata, Snorby, and the BRO IDS, along with network analysis tools such as Wireshark and Network Miner [3]. It also includes the Enterprise Log Search and Archive (ELSA) tool which allows for consolidated log collection and analysis [3].The integrated set up allows students to seamlessly pivot from one tool to the next to learn the effective use of different network security tools. The ease of set up allows faculty to maximize learning by giving students more opportunity to use the tool, rather than spending time installing or troubleshooting; although students must configure different tools to perform the lab tasks.

Course Information

The Security Onion labs are conducted in course CYB 606 Net Defense and Countermeasures[4]. The course is designed as an introductory network security class that provides information on intrusion detection, network security monitoring, firewalls and encryption[4]. Prior to the hands-on labs, students complete lectures and assigned readings on the concept of network security monitoring, history of intrusion detection, and an overview of the different tools. The primary textbook for this portion of the class is "The Practice of Network Security Monitoring" [2].

Lab Environment

The National University Information Security Lab Environment (ISLE) is designed to provide a robust virtual environment for students as they perform hands-on cyber security training assignments. The ISLE is used for assignments throughout most of the NU MS-CSIA classes. The ISLE is implemented in a VMware vSphere 5.5 environment. There are four VMware hosts, each with four sockets, for a total of sixteen (8-core) processors and a memory capacity of 2TB. Total storage capacity is 20TB with capability to grow. The ISLE supports multiple user enclaves, which includes the CSIA Master's program and allows for isolation when working with real malware. Each of the user enclaves has an individual security policy. The implementation of multiple security policies is made possible by the use of next generation Palo Alto (PA) firewalls. The security zone functionality of the Palo Alto firewall is used to isolate individual enclaves from each other and provide each user community with both flexibility and assurance that their equipment will not be negatively impacted by other departments using the ISLE Infrastructure and vice versa. This isolation also prevents students from collecting unauthorized network traffic. For the CYB 606 labs, student are each provided with a Security Onion virtual machine with two network interface cards (NIC). One NIC card is for network connectivity and the other NIC card is for network traffic monitoring and data collection.

A master virtual machine with Security Onion installed and preconfigured with the required lab files is used for the class. Prior to the start of the class, the master virtual machine is updated and a copy is deployed for each student. Allowing students to utilize their own virtual machine gives them the opportunity to customize the tools and download other traffic captures and files for analysis. Each student virtual machine is allocated up to 60GB of storage and 4GB of RAM.

Lab Design

The course labs were designed to provide an initial introduction to Security Onion and the tools installed in the distribution. The labs also demonstrate and reinforce the concepts of network security monitoring as discussed during lectures and with class reading assignments. Lab 1 has two parts. Part 1 is a walk-through that shows students how to utilize tools such as: Wireshark, Network Miner, squil, and Snorby. Part 2 requires students to conduct their own analysis of a second packet capture (pcap) file. The pcap files are used from a previous and publicly available Network Forensics contest [5]. Utilizing a pcap file, the students learn to extract a transmitted file and locate information in a TCP connection stream. Next, students replay a TCP file from an old honeynet scan of the monthly contest and learn how to review and analyze alerts in Snorby and squil [6]. Once students are familiar with these tools, they are given another task named "Ann Skips Bail" [7]. The purpose of this lab is to find some specific data in the pcap files. One challenge to using publicly available contests, is the easy availability of answers; especially for older contests. In addition to answering the specific question(s), students must provide a write-up of their methodology, tools as used with associated screenshots, and provide evidence supporting their conclusions. This not only provides a demonstration that students completed their own work, but helps them learn to write and document an analysis narrative and report their findings to senior management.

In the next lab, students act as an incident responder and must analyze a file with real malware. The file is from the Network Forensics Contest "Puzzle #5: Ms. Moneymany's Mysterious Malware" and contains a malicious Java Applet [8]. As with the previous lab, students must answer specific questions, such as originating URL of the file and MD5 hash of the malicious file. Students also provide an analysis in their own words.

A third lab requires students to practice creating encrypted volumes with an 'easy' password and a 'complex' password. Once completed, each student tries to crack their partner's encryption using different tools. A final lab challenges the students to practice hardening a Linux virtual machine by setting up a local firewall and running penetration testing scans against their partner's VM to observe the results. A pre-hardening scan is conducted to enable baseline results as a comparison against their probe.

Students are offered several options for a final class project. One project option is to utilize Security Onion to analyze a large packet capture. Some example of potential datasets are at the NETRESEC website [9]. As part of the project students must replay the traffic in Security Onion and use the various tools to analyze the traffic and identify such things as:

1. Network structure
2. Types of attacks
3. Phases of attacks
4. Potential preventative measures

Security Onion and NSM Display

The ability to provide over 60 custom tools, further extends the abilities, both automatically and manually, for the students to analyze the same data with different tools. . The powerful network analysis tools in the Security Onion distribution also provide a common framework for analyzing the data and provide a realistic environment for students.

Learning Objectives

Mapping student labs to achieve clear objectives not only supports learning, but allows a student to provide demonstrable skills to potential employers. With the National Initiative for Cybersecurity Careers and Studies (NICCS), the Department of Homeland Security (DHS) and the National Institute for Standards and Technology (NIST) have created the Cybersecurity Workforce Framework [10]. The purpose of this framework is to identify the common knowledge, skills, and abilities of Cybersecurity workers, along with associated job tasks [10]. Table 1 provides a list of the tasks, knowledge, skills and abilities mapped to their associated framework category that students demonstrate by completing the assigned labs.

Table 1. List of Cybersecurity Framework Tasks and KSA's Accomplished in labs

Framework Category: Protect and Defend
Framework Specialty Area: Computer Network Defense Analysis
Tasks completed in the Labs
1. Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information. 2. Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources. 3. Identify and analyze anomalies in network traffic using metadata (e.g., CENTAUR) 4. Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack. 5. Reconstruct a malicious attack or activity based off network traffic. 6. Use Computer Network Defense tools for continual monitoring and analysis of system activity to identify malicious activity. 7. Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools.
Knowledge, skills and abilities demonstrated in the labs
1. Ability to interpret and incorporate data from multiple tool sources. 2. Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution, etc.) 3. Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks, etc.) 4. Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies 5. Knowledge of intrusion detection system tools and applications 6. Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services 7. Skill in collecting data from a variety of Computer Network Defense resources 8. Skill in performing packet-level analysis (e.g., Wireshark, tcpdump, etc.) 9. Skill in reading and interpreting signatures (e.g. snort)

10. Skill in using network analysis tools to identify vulnerabilities 11. Skill in utilizing virtual networks for testing
Framework Category: Investigate
Framework Specialty Area: Investigation
Tasks completed in the Labs
1. Analyze computer-generated threats. 2. Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion. 3. Develop an investigative plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet.
Knowledge, skills and abilities demonstrated in the labs
1. Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, PL/SQL and injections, race conditions, covert channel, replay, return-oriented attacks, and malicious code)

Lessons Learned

The students' VMs are used progressively throughout the MS-CSIA courses, and in classes prior to CYB 606 they performed steps to harden their Windows and Linux systems. In starting the labs for CYB 606, some preliminary scans with Security Onion tools had very limited results, so students found they must reverse or disable some of the hardening measures in order to get more meaningful results from the vulnerability scans or penetration testing in the labs. This also taught them that, in some instances, system hardening is effective in protecting against certain types of intrusion attempts. From an instructional standpoint, because students come with such a wide variety of backgrounds and technical skills, the initial lab instructions must have clear, step-by-step procedures to help students learn about the tools and how to use them, followed by more open-ended instructions that let each student decide which tools to use to solve the lab assignment. Once students gain familiarity using the tools in week 1, they are provided less structure in week 2 and required to act as a security analyst. Students who tend to focus on a single tool should be advised to take advantage of the data linking between multiple tools to obtain the best results. Students are encouraged to compare the results obtained between the different tools to better understand each tool and to validate answers. Also because of the varied backgrounds, it is helpful to provide students with a response template for each lab, to ensure all necessary lab results data is reported in a consistent manner.

Security Onion is processor and memory intensive. During the first deployment of the labs 1GB of RAM was allocated for each virtual machine. This caused slow processing and poor video display. In subsequent labs, memory was increased to 4GB which enhanced performance and provided reasonable processing speed. Institutions without a virtual lab environment can still utilize Security Onion on local workstations or on student personal computers using a virtualization tool like VMWARE or Virtual Box.

Bibliography

1. Security-Onion. *Security Onion Website*. 2014 [cited 2014 12/3]; Available from: https://code.google.com/p/security-onion/.
2. Bejtlich, R., *The practice of network security monitoring: understanding incident detection and response*. 2013: No Starch Press.
3. Security-Onion. *Security Onion Google Code Site*. 2015 [cited 2015 1/21]; Available from: https://code.google.com/p/security-onion/.
4. University, N. *CYB606 Net Defense & Countermeasures.* 2015 [cited 2015 1/21]; Available from: http://www.nu.edu/OurPrograms/SchoolOfEngineeringAndTechnology/ComputerScienceAndInformationSystems/Courses/CYB606.html.
5. Security, L. *Netork Forensics Puzzle Contest*. 2014 [cited 2015 1/21]; Available from: http://forensicscontest.com.
6. Burks, D. *Introduction to Sguil and Squert: Part 3.* 2011; Available from: http://blog.securityonion.net/2011/01/introduction-to-sguil-and-squert-part-3.html.
7. Security, L. *Puzzle #2: Ann Skips Bail*. 2009 [cited 2015 1/21]; Available from: http://forensicscontest.com/2009/10/10/puzzle-2-ann-skips-bail.
8. Security, L. *Puzzle #5: Ms. Moneymany's Mysterious Malware*. 2010 [cited 2015 1/21]; Available from: http://forensicscontest.com/2010/04/01/ms-moneymanys-mysterious-malware.
9. NETRESEC. *Publicly available PCAP files*. 2013 [cited 2014 01/15]; Available from: http://www.netresec.com/?page=PcapFiles.
10. Security, D.o.H. *Interactive National Cybersecurity Workforce Framework*. 2015 [cited 2015 1/21]; Available from: http://niccs.us-cert.gov/training/tc/framework.