

SDN FORENSICS – A CHALLENGE

Winfield Arnott

Joseph Bull

Chris Christou

Tyler Duquette

Emre Ertekin

Michael Lundberg

Michael McAlister

Greg Starkey

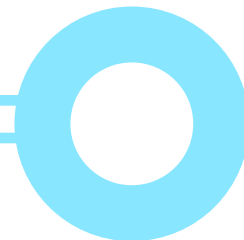
Booz | Allen | Hamilton

SOFTWARE DEFINED NETWORKING – A NEW PARADIGM

Software-defined networking (SDN) provides a new approach to networking by separating the functions of data switching and switch control. SDN permits better global network configuration and control by consolidating network topology and control information into a single controller. Information that is typically found distributed across routing and switching appliances is now used in a centralized SDN controller, permitting it to design and deploy network topology information across the physical and virtual data routing/switching infrastructure.

This new data/control paradigm presents challenges for both network forensic analysis and cybersecurity. Traditional analytics and security were based on the co-location and distribution of data and control information. SDN's separation of data and control as a strongly centralized control system will almost certainly require new procedures for analysis and protection.

To this end, digital forensics research provides the ability to evaluate the security of deployed systems by collecting and analyzing detailed information about devices and network traffic. Ultimately, researchers who perform digital forensics on devices and network traffic contribute to the advancement of emerging capabilities like SDN. The goal of the Digital Forensics Research Work Shop (DFRWS) is to bring together experts in the industry to tackle challenges related to digital forensic science. DFRWS selected SDN as the topic for this year's forensics challenge. The challenge, as stated by DFRWS, was designed to "advance the state-of-the-art in SDN forensics by focusing the community's attention on this emerging domain." We provide here the observations of a team that won the challenge.



FORENSIC ANALYSIS OF A VIRTUAL SWITCH AND ITS CONTROLLER CONNECTION

The DFRWS Challenge focused on a snapshot of memory from an SDN switch, along with a very short capture (under 2 seconds) of the southbound OpenFlow packet traffic. No other information was provided about the network. The challenge required the forensic analysis of the files and to answer the specified questions (e.g., type of SDN controller and switch, hosts connected and to which switch ports, details about flow rules). Additionally, it required the creation of an automated solution (as field-ready as possible) to support future forensic analysis.

Several tools required to successfully perform the SDN forensics analysis included:

- **Wireshark / tshark:** used to assess the packet capture (PCAP) file, including several important dissectors that supported the forensic analysis (OpenFlow version 1.0, SSL)
- **Volatility:** enabled searching the memory for artifacts and reconstructing the file system of the memory provided
- **Yara:** used to identify and enable extraction of secure socket layer (SSL)/TLS keys from memory
- **Python:** programming language that easily integrated with Wireshark and Volatility to perform the forensics necessary (also requires Pandas module and dependencies)

After some intense analysis over several weeks, our analysis of the packet capture and the memory dump data enumerated the entire network, as well as other valuable forensic information. The network consisted of an Open vSwitch and a RYU controller with two hosts directly connected to the virtual switch and five

hosts reachable via specific ports. The flow rules were reconstructed based on the analysis of the OpenFlow messages, including two dynamic rules, each with a hard timeout. Details about the flow rule actions were also captured (e.g., output to switch port, set 802.1q priority, set Ethernet source address). Diagram 1 depicts the enumerated network, which was validated as accurate by DFRWS.

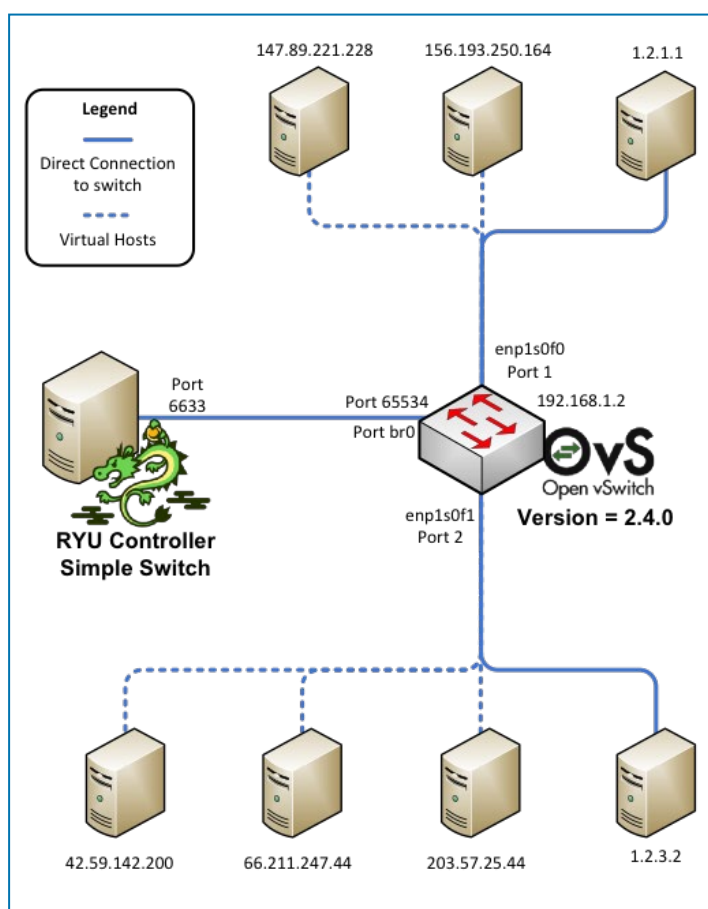


Diagram 1: Discovered Network Map

Also, while the detailed analysis can be found at the DFRWS website, Diagram 2 depicts the high-level forensic steps taken to enumerate the network based on the provided PCAP and memory dump. In the interest of space, the detailed activity will not be addressed here.



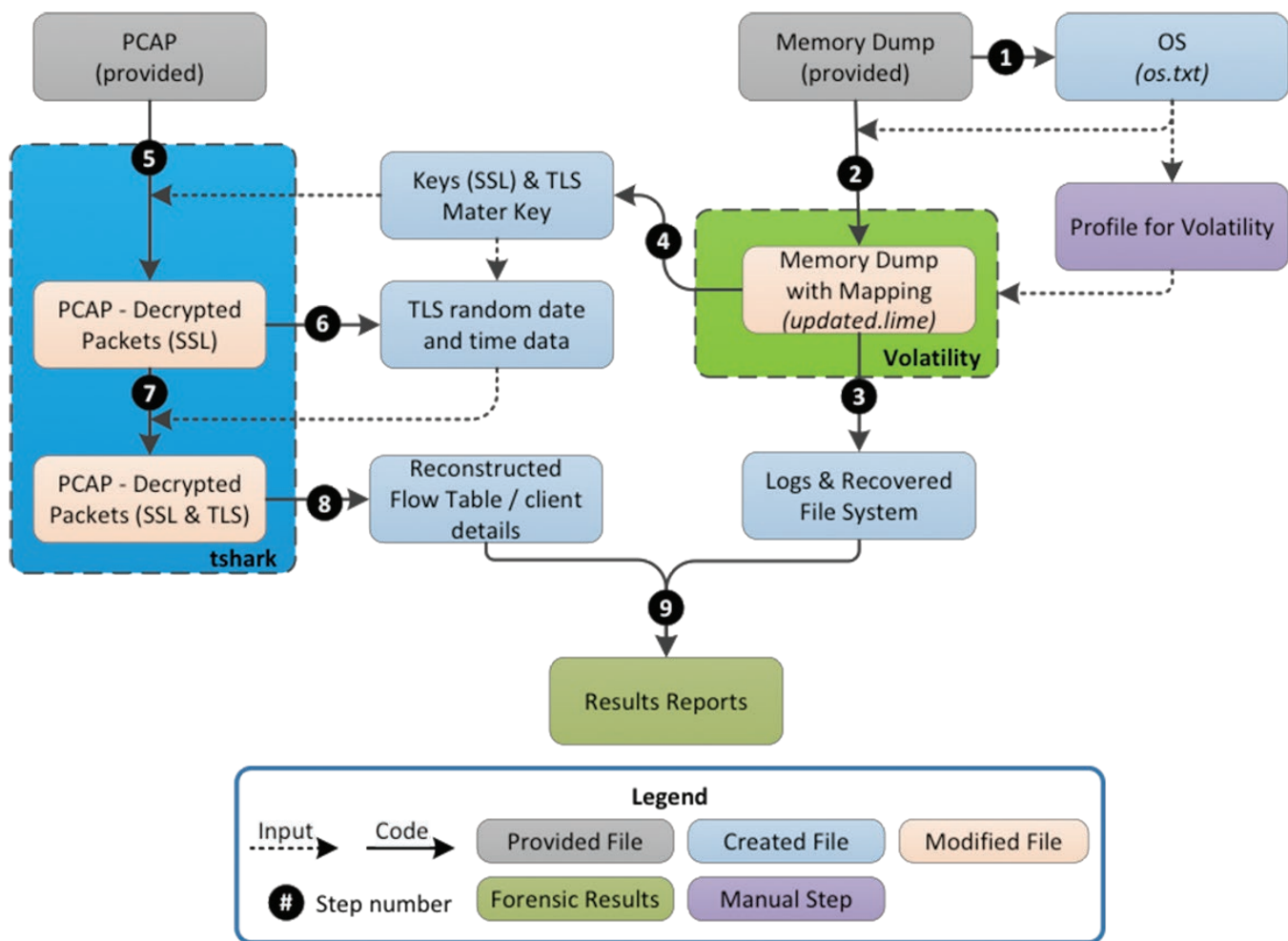


Diagram 2: High-level Forensics steps.


OBSERVATIONS ON THE FORENSIC ANALYSIS OF THE SDN SCENARIO

The DFRWS challenge provided a chance to prove SDN forensics are possible. However, due to the relative newness of SDN infrastructure, the active state of SDN development, and the complexity of the switch/controller connection, a comprehensive analysis required a team with wide-ranging skills. These skills included protocol analysis, network engineering, memory analysis, and programming/scripting. This need for a mixed team was driven home by the early discovery that the captured packets were encrypted using secure socket layer (SSL) and transport layer security (TLS) encryption. This complication forced us to look for decryption keys in the memory dump, creating deep interaction among memory, protocol analysts, and scripters. This collaboration ultimately enabled the creation of a relatively automated mechanism for discovering keys and decrypting packets, as well as several other results that would have gone unrealized in a different scenario.

The most challenging part of the forensic analysis, beyond digging into protocol specifications and fixing the memory mapping, was automating the various interdependent forensic steps as described above for decrypting the PCAP.

The existing open source tools, with some minor exceptions (e.g., incomplete OpenFlow 1.0 protocol dissector), were successful in supporting parts of the network enumeration process. The most challenging part of the forensic analysis, beyond digging into protocol specifications and fixing the memory mapping, was automating the various interdependent forensic steps as described above for decrypting the PCAP. With the continued evolution of Volatility and Wireshark in conjunction with a common framework (similar to the Python scripts applied), a field-ready solution could be deployed which provided repeatable and valuable forensic results. This would facilitate network configuration validation as well as the potential for intrusion detection. Overall, continued support of open source tools will greatly enhance digital forensics analysis, and help promote the evolution of SDN.

Initially, it was envisioned the memory dump would provide the most valuable information about the network, but in the end, the PCAP was the primary source for the network enumeration after its decryption. This was in part due to some of the valuable information from the virtual switch being paged out of memory. This also highlights that if the control plane traffic is not adequately protected, a lot of valuable network information can be recovered from the southbound traffic. Additionally, the accessibility of SSL/TLS keys in the memory needs further investigation to determine potential security risks.

DFRWS hosted a great challenge, and we hope to see several initiatives on SDN forensics in the future. For more information on automating cybersecurity using SDN, please see the article authored by Chris Christou and Michael Lundberg Spring 2016 issue of the United States Cybersecurity Magazine. 

About the Authors:

This article was authored on behalf of Booz Allen Hamilton by Winfield Arnott, Joseph Bull, Chris Christou, Tyler Duquette, Emre Ertekin, Michael Lundberg, Michael McAlister, and Greg Starkey. Booz Allen Hamilton advocates for open sourcing solutions such as this to further advance SDN and the forensics tradecraft. We are the lead developer of Project Jellyfish, an open source cloud broker and orchestration tool. As an evolution of Project Jellyfish, Booz Allen has integrated the Open Source Open Day Light (ODL) controller into the broker to automate compute and network provisioning within the cloud. Further, we are currently leading an ODL-based effort to develop an automated cyber threat response capability.

Booz | Allen | Hamilton

strategy and technology consultants

Sources

1. DFRWS 2016 Challenge - <http://www.dfrws.org/dfrws-forensic-challenge-2016>
2. <https://www.uscybersecurity.net/magazines/Spring2016/mobile/index.html#p=23>

