Demonstration showcase: Near real-time network security with an IF-MAP-based SIEM approach

Prof. Dr. Carsten Kleiner, Bastian Hellmann, Leonard Renners
(Hochschule Hannover - University of Applied Sciences and Arts)

Prof. Dr. Kai-Oliver Detken, Thomas Rix
(DECOIT GmbH)

March 11, 2015

The demonstration showcase intends to illustrate how IF-MAP open source tools of multiple vendors can be combined to smartly address the complex scenario of detecting and reacting to unwanted behavior involving the information of multiple sources. The example scenario integrates several tools by the Trust@HsH research group[1] from the University of Applied Sciences and Arts in Hanover and multiple IF-MAP-clients by DECOIT GmbH[2], a medium-sized enterprise from Bremen, Germany. The combination of these tools allows to identify threats in a detailed manner as well as a near real-time response to found incidents. The scenario is set in a medium-sized network, where an authenticated user is behaving in a malicious manner.

1 Network Overview

The security relevant components for the scenario are shown in figure 1.

Irond runs as central MAP server (MAPS) and several IF-MAP-clients (MAPC) supply information regarding the overall network state. Typical services of the network like a RADIUS server for the network access control (NAC), a DHCP server for lease information, and an e-mail-server for e-mail communication are part of the security management architecture. Additionally, security relevant components like a Nmap scanner

[1] https://github.com/trustathsh

[2] https://github.com/decoit

and an OpenVAS client are provided. These security components scan the network periodically and publish information about identified devices, services and vulnerabilities. A snort IDS monitors the network traffic and raises critical alerts.

The gathered information is stored by the MAP server irond and can be visualized by the VisITMeta dataservice component. A connected detection engine uses this information to analyze the network state and detect malicious conditions. Found incidents are communicated to the SIEM-GUI, which provides detailed information about the network security status. It presents an overview of the network behavior and can further be used for the incident management. Additionally the SIEM-GUI shows further information of the VisITMeta visualization basis.

The communication of some IF-MAP-clients with irond has been realized using the Concise Binary Object Representation (CBOR[3]) protocol of RFC 7049. CBOR uses a JSON data model and makes sufficient communication with IF-MAP possible. For example, mobile devices like Android smartphones can also addressed by IF-MAP via CBOR. An IF-MAP-client for Android is also available within the SIMU project and has been developed by the partner DECOIT GmbH, based on open source.

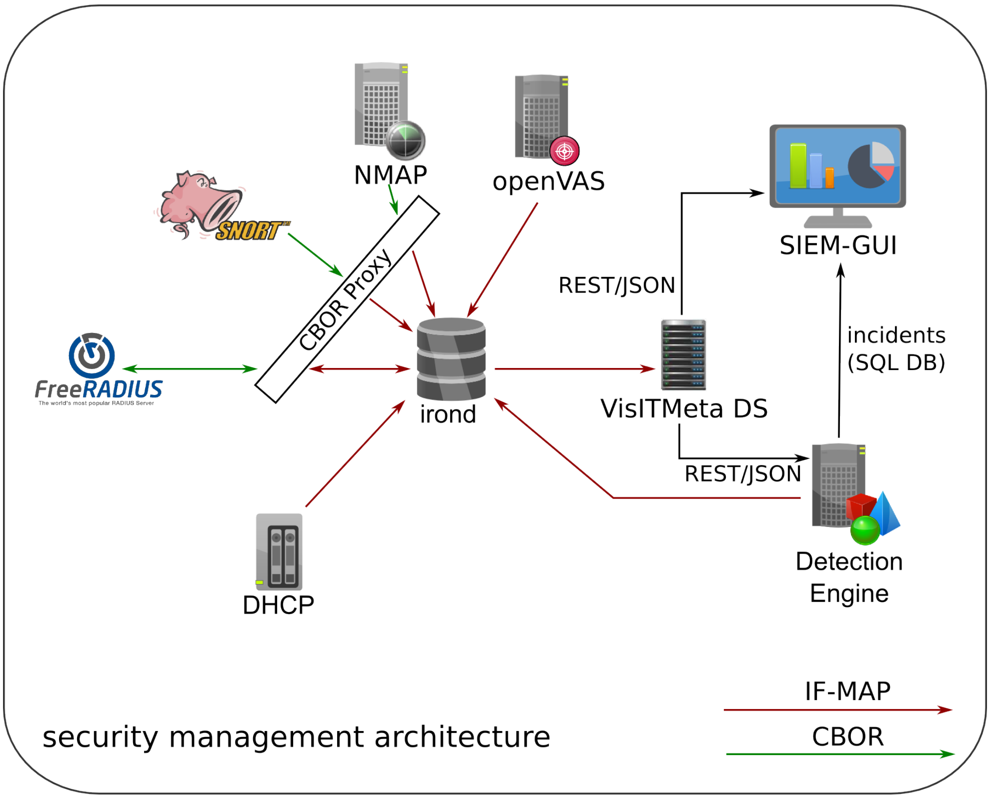

Figure 1: Management architecture of the demonstration scenario

[3] http://www.cbor.io

2 Demonstration Steps

This section describes the demonstration more in detail. The individual steps are described first, and figure 2 illustrates the resulting IF-MAP graph. The initial situation is as follows:

- The RADIUS server manages the network access based on its configuration and the company policy.
- The detection engine is equipped with rules that detect malicious patterns, e.g. brute force login attacks or SNORT-alerts in correlation with vulnerable targets.
- The SIEM-GUI is used by an administrator to monitor the network status and to react on incidents.

The demonstration itself consists of the following activities:

1. The NMAP client identifies a running SSH server.
2. OpenVAS detects a vulnerability in the version of the SSH server.
3. Later, an employee authenticates successfully at the RADIUS server and gains access to the company network.
4. SNORT monitors the network traffic and detects an attack pattern from the authenticated client's IP-address.
5. The detection engine correlates the detected attack with the information, that the server is actually vulnerable to these kind of attacks (provided by the vulnerability scanner).
6. A resulting incident is created due to the correlation and communicated towards the SIEM-GUI.
7. Due to its severity (actually vulnerable service to the specific attack), the detection engine creates an additional metadata about the malicious behavior.
8. The RADIUS server enforces the required action and publishes the results.
9. The administrator sees the (high-level) alert reporting and can react appropriately. The provided and attached information (exactly which metadata lead to the alert creation) allow for a targeted analysis.
10. After the incident has been handled appropriately, the client can be reintegrated into the company network and the employee can return to his regular work tasks.

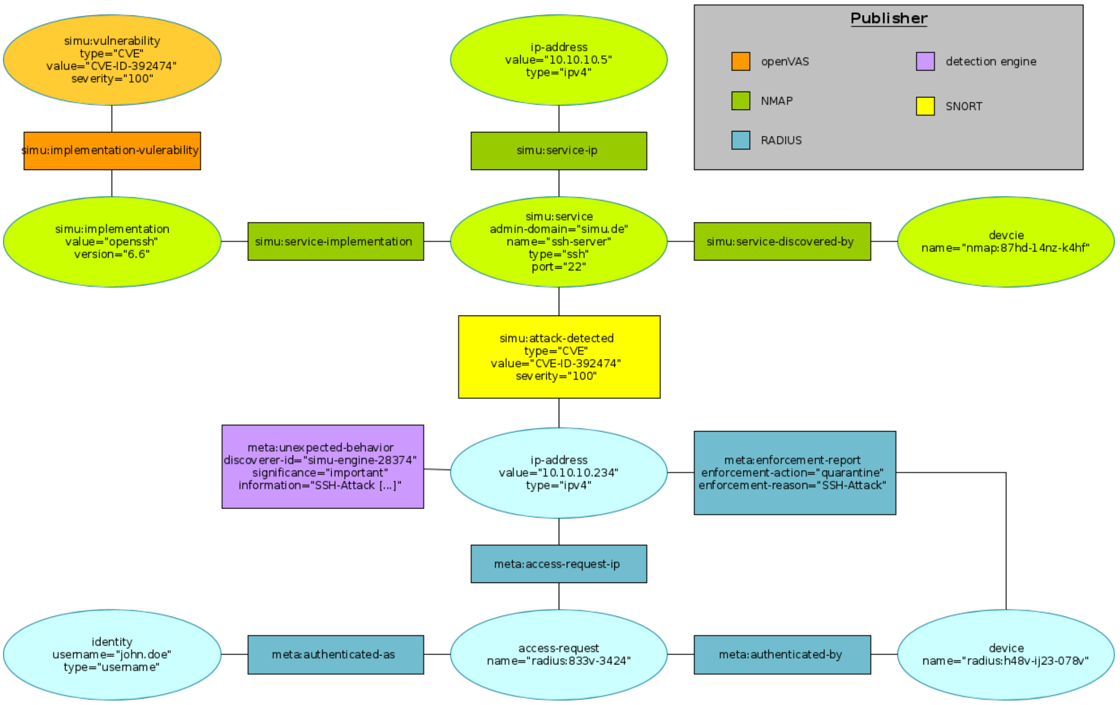

Figure 2: Metadata graph of the scenario situation

3 Summary

The demonstration shows how different open source tools can be used to build a SIEM-like system which detects and treats anomalous and malicious behavior in near real-time. Different, heterogeneous data sources allow for more complex and precise situation definition and the user-friendly GUI enables easier security management. The (optional) extension using the CBOR proxy, developed by Fraunhofer SIT, allows the deployment in environments with bandwidth or resource limited scenarios. The demonstratir also shows how open source tools, developed by different vendors, collaborate by leveraging TCG technologies, especially the IF-MAP protocol of the trusted network connect (TNC) specification[4].

[4] TCG Trusted Network Connect TNC Architecture for Interoperability: specification version 1.5, revision 3, 7 May 2012, published