SIEM, IDS and Firewall Lab Configuration

Abstract

The following document covers the process used to create a lab incorporating a Security Information and Event Management (SIEM), Intrusion Detection System and a Firewall. The purpose of this lab was to get comfortable with common enterprise technologies so that incident analysis and triage is easier in cases that involve these technologies.

The lab uses Graylog SIEM, pfSense firewall and an integrated IDS made using Suricata. These tools were chosen because of their availability and their reputation for being industry standard or at least being high quality simulations of enterprise tools.

This report will cover key aspects of the setup and configuration as well as relevant details about the tools and their usage.

1 Firewall Configuration

In this scenario the pfSense firewall is a Virtual Machine with two network cards, one configured for WAN (Internet) and LAN (VMWare Network Manager VMnet 18) which uses the IP range of 10.0.0.0/27 (30 Hosts). The pfSense firewall also serves as the primary router, providing DHCP services for connected clients (10.0.0.10 – 10.0.0.30). DNS is provided by CloudFlare using 1.1.1.1, however DNS Resolver is turned on and statically IP addressed servers were added as Host Exceptions, so pfSense will check this table before reaching out to public DNS.

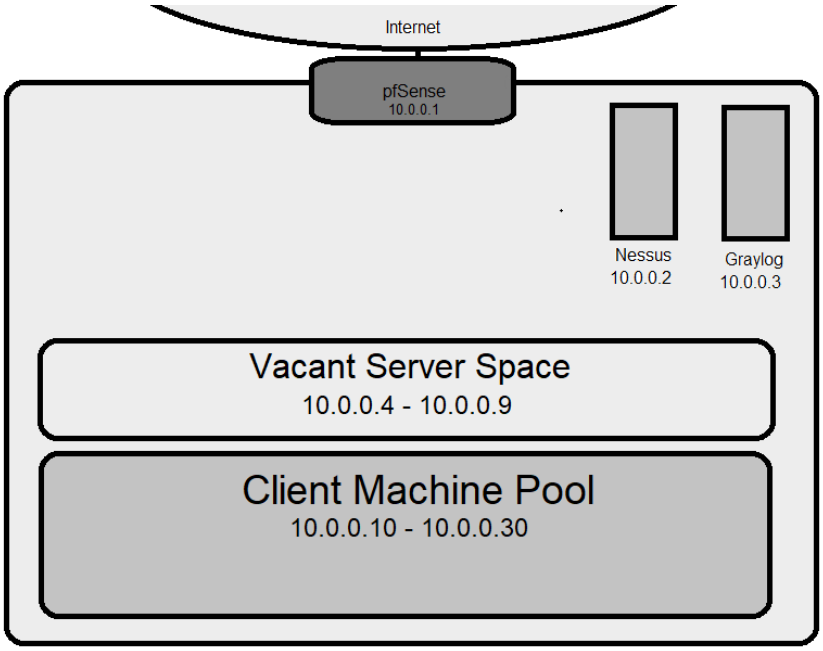

Figure A - Logical Network Diagram

2 SIEM Configuration

Using the Graylog recommended installation steps found here, Graylog was installed over a fresh copy of Ubuntu 22.04 LTS. Using Nano and the netplan file for the system, a static IP Address of 10.0.0.3 was assigned and the DNS server address was set to the IP address of the firewall. To allow system logs to be sent to the system an Input was set in the Graylog settings from **"System tab > Inputs"**, two inputs were created on TCP/UDP 1514.

Systems could then be pointed to the SIEM using the rsyslog package (for Ubuntu Clients and Servers) alongside adding **"*.* @@10.0.0.3:1514"** in their **"/etc/rsyslog.conf"** file. pfSense allows remote logging by default and was configured in **"Status > System Logs > Settings",** the option to allow remote logging should then be ticked and the IP for the SIEM provided to allow logging to SIEM.

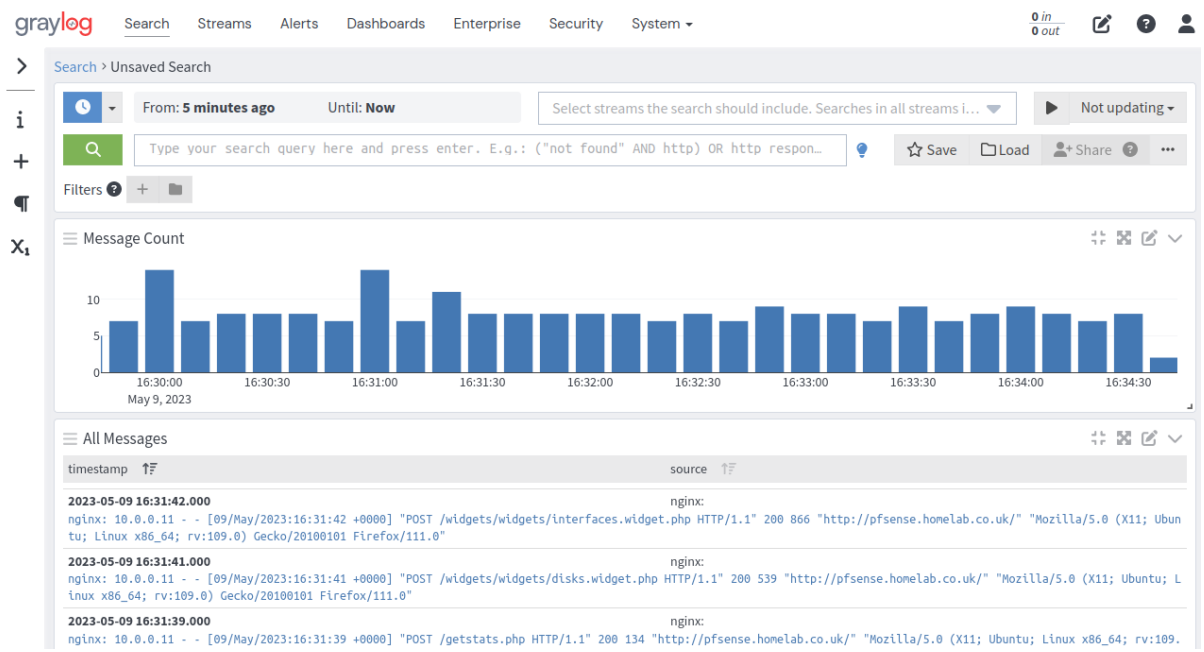

Figure B - Graylog SIEM in Action

3 Nessus Installation

To provide vulnerability scanning potential to this simulated small scale corporate network, Nessus was used, this was downloaded using the recommended steps found here. This machine is an Ubuntu 22.04 LTS server, using the static IP address of 10.0.0.2. This lab uses the Nessus Essentials free tier, providing scans for up to 16 IP addresses.

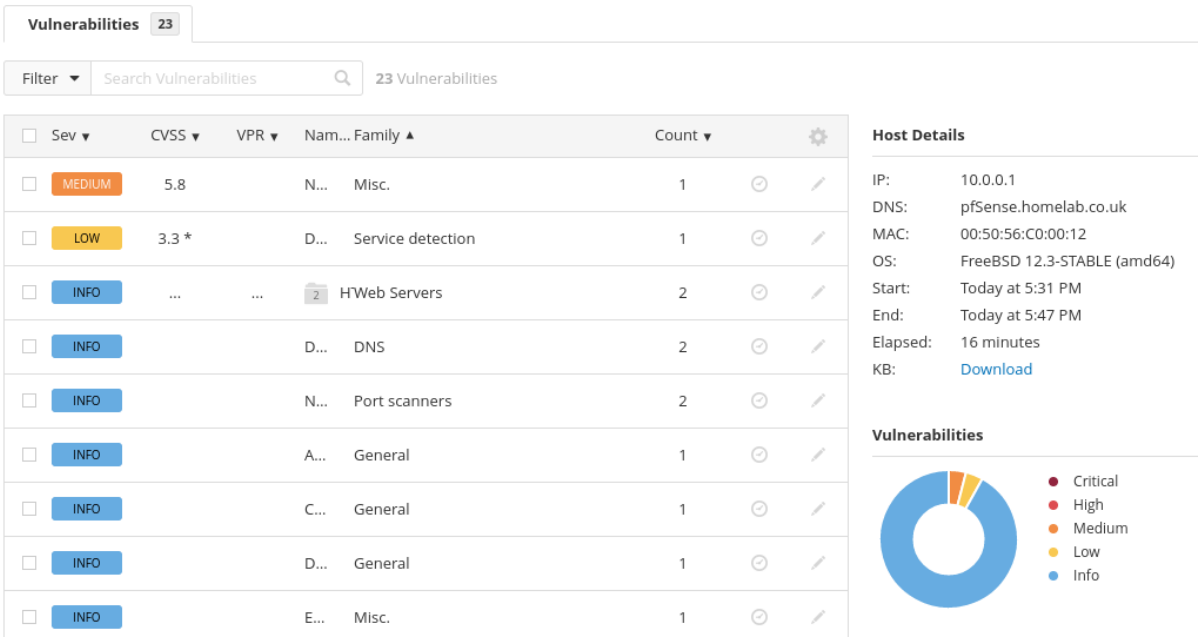

Figure C - Nessus Scan on Firewall

4 Intrusion Detection System

To secure the simulated corporate network an Intrusion Detection System was introduced to the perimeter firewall (pfSense), looking at any incoming traffic on the corporate LAN but not on the internet-facing WAN (unless it makes it into the network). Suricata IDS was installed using **"System > Package Manager"** on the firewall and searching for Suricata in the available options. The next step was to visit **"Services > Suricata"** and add it to the LAN interface and ensure that it is running, making sure that the option **"Send Alerts to System Log"** is enabled, allowing alerts to be visible to the Graylog SIEM created in section 2.

Figure D - Suricata in the SIEM

Suricata has the potential to be used as both an Intrusion Detection or Prevention system however, it is recommended to tune the IDS to the needs of a network before allowing it to block traffic. The potential for rules to misfire (cause False Positives) is massive in a fresh installation, this was show during the testing phase of this lab, as Suricata generated over 400,000 alerts in half an hour for the rule **"UDPv4 Invalid Checksum"** on System Logs travelling from pfSense to the Graylog SIEM, this rule was swiftly disabled. On the other hand, Suricata was able to detect traffic from the Vulnerability Scan shown in Section 3, which is positive, however the Nessus server was then added to the allow list, since activity from the Nessus Server may look malicious but is used to bolster the network's security posture.

Last 250 Alert Entries. (Most recent entries are listed first)

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
05/09/2023 17:41:11	⚠	3	TCP	Generic Protocol Command Decode	10.0.0.1	80	10.0.0.2	55136	1:2221010	SURICATA HTTP unable to match response to request
05/09/2023 17:39:12	⚠	3	TCP	Generic Protocol Command Decode	10.0.0.1	80	10.0.0.2	39334	1:2221010	SURICATA HTTP unable to match response to request
05/09/2023 17:39:00	⚠	3	TCP	Generic Protocol Command Decode	10.0.0.2	33876	10.0.0.1	80	1:2221014	SURICATA HTTP missing Host header
05/09/2023 17:38:52	⚠	3	TCP	Generic Protocol Command Decode	10.0.0.2	39944	10.0.0.1	80	1:2221015	SURICATA HTTP Host header ambiguous
05/09/2023 17:38:17	⚠	3	TCP	Generic Protocol Command Decode	10.0.0.2	32926	10.0.0.1	80	1:2221034	SURICATA HTTP Request unrecognized authorization method
05/09/2023 17:38:17	⚠	3	TCP	Generic Protocol Command Decode	10.0.0.2	32926	10.0.0.1	80	1:2221028	SURICATA HTTP Host header invalid

Figure E - Suricata Alerts Table (from pfSense)

To further increase the IDS's ability to secure the network, extra rulesets were downloaded from the Suricata settings including rules from Cisco Talos. The extra rules could lead to further need for tuning; however, it means that more types of attacks are likely to be caught. Auto-updating was enabled to ensure the latest rules are always available, updates were scheduled for 12:00AM when small amounts of downtime are likely to be felt.

INSTALLED RULE SET MD5 SIGNATURES

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Emerging Threats Open Rules	df7272bca1c0609f7149b8efff70bc68	Monday, 08-May-23 19:10:59 UTC
Snort Subscriber Rules	Not Enabled	Not Enabled
Snort GPLv2 Community Rules	feea5aec3629a041c89f65f066dc27e2	Monday, 08-May-23 19:10:59 UTC
Feodo Tracker Botnet C2 IP Rules		Monday, 08-May-23 19:11:00 UTC
ABUSE.ch SSL Blacklist Rules	44bcd372e119f65505a14dcba006c9e3	Monday, 08-May-23 19:10:58 UTC

Figure F - Installed Rule Sets