Security Tool Suggestions

**Firewalls:**

A good practice on web servers is to deny traffic by default and to make exceptions for traffic explicitly required for server operation, and RHEL 8 implements this by initially blocking many unnecessary ports by default. Firewalls can be helpful for modifying and expanding on this, as they allow for simplified configuration of allowed services/ports. Here is a list of RHEL 8 compatible firewalls that could be used for this effect:

Firewalld:

RHEL 8 systems come equipped with firewalld by default, and thus only starting and activating it via systemctl would be required to begin configuration. It serves as a frontend to the more complicated nftables firewall. It also contains an additional feature in network zone management, where rulesets for firewall operation can be defined based on the network conditions.

<https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/configuring_and_managing_networking/using-and-configuring-firewalld_configuring-and-managing-networking>

Uncomplicated Firewall (UFW)

UFW is designed for simplicity while still containing the features necessary in a firewall, often just being less verbose and more user-friendly. It does not contain the network zone management feature of firewalld, but given the static conditions of the web server that feature loss is unlikely to be important. It requires installing the Extra Packages for Enterprise Linux (EPEL) repository on the server, from which point it can be enabled and configured.

<https://shouts.dev/install-and-setup-ufw-firewall-on-centos-8-rhel-8>

**Intrusion Detection/Prevention Systems:**

Given the attack-and-defense basis of the project it’s likely that additional protection past the Firewall will be necessary, so a server-based Host Intrusion Detection System (HIDS) would be helpful in logging/flagging odd activity in the server and potentially shutting out invasive actions dynamically. Here are a few of the more popular open-source solutions:

Open-Source Security Event Correlator (OSSEC)

This is an open-source HIDS that’s highly popular and supported. It works through anomaly-detection and the use of logs and log analysis, and is capable of both rootkit and malware detection, file and policy integrity monitoring, and real-time response mechanisms (which allow it to function in part as an IPS as well). It would require installation of itself and some dependencies, but past that should be relatively straightforward to configure for a web server. Additional rules and plugins can be installed from its website or via community releases.

<https://www.ossec.net/about/>

Wazuh

This HIDS is essentially an extension of OSSEC. It comes with a variety of improvements in rulesets and management capabilities, at the cost of being more difficult to configure and install fully, and many of the extended features may not be necessary for this project’s scope.

<https://wazuh.com/migrating-from-ossec/>

Sagan + Snort

Sagan is an open-source, lightweight HIDS that operates with anomaly as well as signature-based detection strategies. It works by analyzing logs and allows for automatic responses to be set for specific circumstances, even allowing the execution of reactionary scripts. One notable feature it claims is the ability to geolocate IP addresses to create alerts if multiple IP addresses from a particular region generate unusual activity. It is also written to be compatible with Snort 2, a popular and broadly applicable NIDS, allowing for coordination of alert responses and a general high degree of system coverage.

<https://quadrantsec.com/sagan_log_analysis_engine/>

<https://www.snort.org/>

<https://www.dnsstuff.com/host-based-intrusion-detection-systems> (look to #6 & #7)

**Miscellaneous/Pentesting Tools:**

It’s helpful to test a server with the same approaches that attackers might be using to help patch holes. Here are some of the more popular or informative ones:

Zed Attack Proxy (ZAP)

This is an open-source tool that scans a URL and exposes a wide variety of web application weaknesses such as missing security headers, SQL injection, and XSS injection. Scans on it can be run manually or automatically through its user-friendly GUI.

<https://www.zaproxy.org/>

SQLmap

This is an open-source tool that can identify weaknesses of a wide array of SQL injection techniques on a wide array of database types.

<https://sqlmap.org/>

Nikto

This open-source tool is used as an in-house web server vulnerability scanner. It features SSL and HTTP proxy support and can scan the server’s ports, find risky configurations, and highlight problematic files amongst many other utilities. It is designed to work off Linux operating systems.

<https://geekflare.com/nikto-webserver-scanner/>

Arachni

This open-source tool is used to perform web application security scans. It’s been noted as “high performance” across multiple sites, and is capable of fingerprinting a platform, utilizing plugin extensions on scans, and detects vulnerabilities such as LFI/RFI, cross-site request forgery, and a number of injection techniques. It has a GUI and works on multiple platforms.

<https://www.arachni-scanner.com/features/framework/>

Nmap

This open-source tool is a network discovery/security auditing tool that can identify open ports, running services/devices, and available hosts amongst other things. It’s very popular to the point of it being likely used against the server, making it a good idea to use it to verify security.

<https://nmap.org/>

WordPress WordFence

This is a free-to-try security plugin for WordPress that’s designed to establish an endpoint firewall, perform security scans, establish authentication measures, and detect WordPress-sensitive malware. It’s highly reviewed and has a GUI-based management tool to overview the site. There is a premium version available with additional real-time functionality, but given our project’s scope and periodic checks it’s unlikely to be necessary for our purposes. Given the use of WordPress for this project, this tool would likely be helpful specifically for our website’s security coverage alongside making a few WordPress configuration changes.

<https://wordpress.org/plugins/wordfence/>

WPScan

This is an free-to-try security plugin for WordPress that scans a site against a specially curated and updated WordPress Vulnerability database for holes in WordPress itself, plugins, or themes. Given the popularity of the tool, its offensive capabilities, and our use of WordPress it’s likely that this tool could be used against us, so it could be very helpful to run the scans ourselves with it first. There is a limit to 25 API requests a day with the tool, but that should be more than enough for our one site.

<https://wordpress.org/plugins/wpscan/>

**Additional Helpful Links:**

Red Hat Enterprise Linux 8 “Security Hardening” Guide:

<https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/pdf/security_hardening/red_hat_enterprise_linux-8-security_hardening-en-us.pdf>

Web Server Hardening Best Practices:

<https://resources.infosecinstitute.com/topic/web-server-security-web-server-hardening/>

Hardening WordPress:

<https://wordpress.org/support/article/hardening-wordpress/>