Wazuh Ruleset

Rule	Description	Source	Updated by Wazuh
apache	Apache is the world's most used web server software.	Out of the box	✓
apparmor	AppArmor is a Linux kernel security module that allows the system administrator to restrict programs's capabilities with per-program profiles.	Out of the box	✓
arpwatch	ARPWatch is a computer software tool for monitoring Address Resolution Protocol traffic on a computer network.	Out of the box	✓
asterisk	Asterisk is a software implementation of a telephone private branch exchange (PBX).	Out of the box	✓
attack_rules.xml	Signatures of different attacks detected by Wazuh	Out of the box	✓
cimserver	Compaq Insight Manager Server	Out of the box	✓
cisco-ios	Cisco IOS is a software used on most Cisco Systems routers and current Cisco network switches.	Out of the box	✓
clam_av	Clam AntiVirus (ClamAV) is a free and open-source, cross-platform antivirus software tool-kit able to detect many types of malicious software.	Out of the box	✓
courier	IMAP/POP3 server	Out of the box	✓
dovecot	Dovecot is an open-source IMAP and POP3 server for Linux/UNIX-like systems, written primarily with security in mind.	Out of the box	✓
dropbear	Dropbear is a software package that provides a Secure Shell-compatible server and client. It is designed as a replacement for standard OpenSSH for environments with low memory and processor resources, such as embedded systems.	Out of the box	✓
firewalld	FirewallD provides a dynamically managed firewall with support for network/firewall zones to define the trust level of network connections or interfaces. Default firewall management tool RHEL and Fedora.	Out of the box	✓
firewall_rules.xml	Firewall events detected by Wazuh	Out of the box	✓
ftpd	Simple FTP server.	Out of the box	✓
hordeimp	IMP is the Internet Messaging Program and provides webmail access to IMAP and POP3 accounts.	Out of the box	✓
ids_rules.xml	IDS events detected by Wazuh	Out of the box	✓
imapd	imapd is the Courier IMAP server that provides IMAP access to Maildir mailboxes	Out of the box	✓
mailscanner	MailScanner is a highly respected open source email security system design for Linux-based email gateways	Out of the box	✓
mcafee_av	McAfee is an antivirus program.	Out of the box	✓
ms-exchange	Microsoft Exchange Server is a calendaring and mail server developed by Microsoft	Out of the box	✓
ms-se	Microsoft Security Essentials (MSE) is an antivirus software (AV) product that provides protection against different types of malicious software.	Out of the box	✓
msauth_rules.xml	Microsoft Windows events deteced by Wazuh.	Out of the box	✓
ms_dhcp	Microsoft DHCP rules.	Out of the box	✓
ms_ftpd	Microsoft FTP rules.	Out of the box	✓
mysql	MySQL is an open-source relational database management system (RDBMS).	Out of the box	✓
named	named is a Domain Name System (DNS) server.	Out of the box	✓
netscreenfw	Netscreen is a high performance firewall.	Out of the box	✓
nginx	Nginx is a web server with a strong focus on high concurrency, performance and low memory usage.	Out of the box	✓
openbsd	OpenBSD is a Unix-like computer operating system descended from BSD.	Out of the box	✓
ossec_rules.xml	Main rules	Out of the box	✓

Rule	Description	Source	Updated by Wazuh
pam	A pluggable authentication module (PAM) is a mechanism to integrate multiple low-level authentication schemes into a high-level application programming interface (API).	Out of the box	✓
php	PHP is a server-side scripting language designed for web development but also used as a general-purpose programming language.	Out of the box	✓
pix	Cisco PIX (Private Internet eXchange) is a popular IP firewall and network address translation (NAT) appliance.	Out of the box	✓
policy_rules.xml	Policy rules (login during weekends, non-business hours)	Out of the box	✓
postfix	Postfix is a free and open-source mail transfer agent (MTA) that routes and delivers electronic mail.	Out of the box	✓
postgresql	PostgreSQL is an object-relational database management system (ORDBMS) with an emphasis on extensibility and on standards-compliance.	Out of the box	✓
proftpd	ProFTPD is an FTP serve	Out of the box	✓
pure-ftpd	Pure-FTPd is a free (BSD license) FTP Server	Out of the box	✓
racoon	Racoon is a key management daemon used for VPN connections.	Out of the box	✓
roundcube	Roundcube is a web-based IMAP email client.	Out of the box	✓
rules_config.xml	Main rules	Out of the box	✕
sendmail	Sendmail is a general purpose internetwork email routing facility that supports many kinds of mail-transfer and delivery methods, including SMTP used for email transport over the Internet.	Out of the box	✓
smbd	SMBD is a server that can provide most SMB services. The server provides filespace and printer services to clients using the SMB protocol.	Out of the box	✓
solaris_bsm	Solaris Basic Security Module (BSM) can create an extremely detailed audit trail for all processes on the system.	Out of the box	✓
sonicwall	SonicWall is a network firewall.	Out of the box	✓
spamd	spamd is a ISC-licensed lightweight spam-deferral daemon written under the umbrella of the OpenBSD project. spamd works directly with smtp connections, and supports features such as greylisting, minimising false positives compared to a system that does full-body analysis.	Out of the box	✕
squid	Squid is a caching and forwarding web proxy.	Out of the box	✓
sshd	sshd (SSH Daemon) is the daemon program for ssh.	Out of the box	✓
symantec-av	Symantec is an antivirus program.	Out of the box	✓
symantec-ws	Symantec Web Security	Out of the box	✓
syslog_rules.xml	Rules to analyze syslog messages	Out of the box	✓
sysmon_rules.xml	Rules to detect Windows Process Anomalies	Out of the box	✓
systemd	Systemd is a software suite for central management and configuration of the GNU/Linux operating system.	Out of the box	✕
telnetd	Telnet protocol daemon	Out of the box	✕
trend-osce	Trend Micro OSCE (Office Scan) rules	Out of the box	✓
unbound	Unbound is a validating, recursive, and caching DNS server software.	Out of the box	✕
vmpop3d	vm-pop3d is a POP3 server.	Out of the box	✓
vmware	VMware is a virtualization software .	Out of the box	✓
vpn_concentrator	Cisco VPN Concentrator	Out of the box	✓

Rule	Description	Source	Updated by Wazuh
vpopmail	vpopmail is a free GPL software package, to provide a way to manage virtual e-mail domains and non /etc/passwd e-mail accounts on qmail mail servers.	Out of the box	✓
vsftpd	vsftpd is an FTP server for Unix-like systems, including Linux.	Out of the box	✓
web_appsec_rules.xm	Rules for vulnerabilities and attacks related with web	Out of the box	✓
web_rules.xml	Web access rules	Out of the box	✓
wordpress	WordPress is a free and open-source content management system (CMS) based on PHP and MySQL.	Out of the box	✓
zeus	Zeus is a lite Web Server	Out of the box	✓
Puppet	Puppet is an open-source configuration management utility.	Created by Wazuh	✓
Netscaler	NetScaler is a hardware device (or network appliance) manufactured by Citrix, which primary role is to provide Level 4 Load Balancing. It also supports Firewall, proxy and VPN functions.	Created by Wazuh	✓