CIS Benchmarks

For

Wazuh

Contents

Summary of CIS benchmarks

CIS benchmarks - Center for Internet Security (CIS) Benchmarks
CIS benchmarks are consensus-based, best-practice security configuration guides developed and accepted by the government, business industry and academia.
CIS critical security controls:
Top 18 top-level CIS controls

- Inventory and control of enterprise assets
- Inventory and control of software assets
- Data Protection
- Secure configuration of enterprise assets and software
- Account management
- Access Control Management
- Continuous vulnerability management
- Audit log management
- Email and web browser protection
- Malware Defenses
- Data Recovery
- Network infrastructure management
- Network monitoring and defence
- Security awareness and skills training
- Service provider management

- Application software security
- Incident response management
- Penetration testing
-

Outlined goals of testing against CIS Benchmarks

- Ubuntu Linux
- Windows 10 pro
- Scanning wazuh
- Scanning Nessus

Ongoing security operations -
Continuous vulnerability scanning
Log review and compliance - within wazuh security teams will be alerted when critical events related to CIS Standards occur
CIS updates - ensure§ the server configurations reflect the latest CIS benchmarks as they are revised. Monitor changes in the benchmark and adapt scanning and monitoring methods as needed.

Ubuntu - scanning wazuh and Nessus good files etc
Windows - scanning wazuh and Nessus bad files etc
Comparison in the end

Friday 14th February 2025
L/O - Today's objective is to start looking at scanning the gaming log files which have been created by a following team member.

Server outlines from the creator - Ivan Urdev
The first server simulates brute force attacks, SQL injection, cross-site scripting attacks, and out-of-bounds memory writes, exposing sensitive game states and rate limit abuse.

The third server has been set with remote code execution (RCE), Buffer overflow attacks, privilege escalation attempts, Brute force attacks, SQL injection, cross-site scripting, and Denial-of-service.

- The script is not set to run automatically. If needs to be run again type the following command sudo ./game_log.sh
- The script will continue running unless manually stopped, press ctrl+C
- To view the security report that the script has generated

- Cat /var/log/game_and_security_logs/security_report.txt
- Will display the attacks against the server

Objectives of scanning

- Outline the risk factors - Penn test report?
- Scan the servers against CIS CAT
- Compare the benchmark results to the report
- Scan on wazuh
- Scan on Openvas
- Dashboard of results ??

Security Automation Servers - Initial overlook

- Ubuntu server 22.04 Security Automation
- Machine IP address - 192.168.123.30/24
- Sudo ./game_log.sh - simulating an indefinite number of players in the game
- Fail2Ban attempt? - unable to download
- Ubuntu server 22.04 Security Automation server 2
- Machine IP address - 192.168.123.20/24
- Ubuntu server 22.04 Security Automation Server 3
- Machine IP Address - 192.168.123.10/24
- Brute force command not found
- Everything else is loading correctly
- Is it supposed to take a while to load?
- Didn't know when it ended - need clarification

Ubuntu server 22.04 Security Automation Server 3 Report output
Examples of what came from the report

- XSS - vulnerability detected. Ensure proper sanitation
- SQL - Injection attempt detected. Check input validation
- Why is it only releasing two in the reports?
- Very brief description of what could be the problem

Friday 12th February 2025

Wazuh scans monitor endpoints using the CIS benchmarks. Wazuh uses the SCA module to generate this report.

- Scan each of the servers
- Penn test report formats
- How these reports are configured.
- Schedule weekly scans

Wazuh - https://172.16.252.128
Greenbone - https://172.16.252.128:9392

Wazuh log in - admin
SecretPassword

CIS benchmarks dashboard image - what some of the benchmarks mean

CIS Ubuntu 22.04 LTS BENCHMARK v1.0.0 - Server one

Summary of the file scan - 75 passed, 105 failed, 2 not applicable and 41% score

Critical

- Ensure the password hashing algorithm is up to date with the latest standards
- Ensure the inactive password lock is 30 days or less
- Ensure XDMCP is not enabled

High

- Ensure lockout for failed password attempts is configured
- Ensure password expiration is 365 days or less
- Ensure pre-link is not installed
- Ensure systemd-timesyncd is enabled and running
- Ensure the NIS server is not installed - can lead to DOS attacks
- Ensure rsh client is not installed - contains numerous security exposures
- Ensure talk client is not installed - presents security risks as uses encrypted protocols for communication
- Ensure LDAP client and RPC are not installed - (potential attack surface), (Remote attack surface)

Medium

- Ensure password requirements are configured
- Ensure password reuse is limited
- Ensure Apparmor is installed
- Ensure permissions on /etc/motd are configured correctly
- Ensure permissions on /etc/issue are configured correctly
- Ensure permissions on /etc/issue.net are configured correctly
- Ensure window X is not installed - unless the organisation require it
- Ensure the Avahi server is not installed
- Ensure CUPS isn't installed
- Ensure DHCP, LDAP, NFS, DNS, FTP, IMAP, POP3 isn't installed

Info (not applicable) - Ensure ntp access control is configured

- Ensure only authorised groups are assigned ownership of Audit log file

CIS benchmarks overview

Within Wazuh it offers a security configuration module which allows you to automatically check the server which has been running on the wazuh against the CIS benchmarks. In addition to being able to check the server against the benchmarks you are able to visualize the results within a dashboard under section CIS Docker Benchmark v1.7.0.
From each of the three servers we have taken three things which have failed against the CISbenchmarks and what is important is that they are in place.

Server one -

- Ensure bootloader password is set - Enhances security by preventing unauthorised access from modifying boot settings or booting the server into recovery mode.
- Ensure core dumps are restricted - enhances security by preventing sensitive information (such as passwords, encryption keys, or memory contents) from being exposed in crash dump files
- Ensure audit tools are owned by root - Ensuring that audit tools are owned by the root is highly important for security as it prevents unauthorized users from modifying or disabling them

Server two -

- Ensure IMAP and POP3 server are not installed - IMAP and POP3 increase various security and operational risks which include; increased attack surface, risk of data exposure, unnecessary resource consumption, compliance and security policy violations and risk of unauthorised email relay(spam and phishing)

- Ensure chrony is enabled and running - chrony needs to be running because it is critical for system security, logging, and authentication. If Chrony is not running, the system clock may drift, causing various issues, including failed security checks and incorrect timestamps.
- Disable automounting - Disabling automounting is a crucial security step to prevent the automatic execution of malicious code, unauthorized data transfer, and various other types of attacks.

Server three -

- Ensure XDMCP is not enabled - XDMCP enables remote users to access the graphical login screen of a Linux or Unix system. Although it may be helpful for specific administrative tasks, enabling XDMCP poses considerable security risks by providing remote access to the graphical user interface (GUI) without adequate security protections.
- Ensure iptables-persistent is not installed with ufw -While UFW is a frontend for managing firewall rules easily, iptables-persistent is used to save and restore iptables rules, which can override UFW's settings or create unexpected behavior.
- Ensure ip6tables default deny firewall policy - ip6tables (IPv6 firewall) is enabled with a default deny policy, it can result in several potential problems if not properly configured

Breakdown of the wazuh rule classification

Within the wazuh documentation there is a rules classification section, which the rules are categorized into multiple levels which start from level 0 all the way to level 16 which is noticed as the highest level there is within the wazuh rules classification.

Level 15 or higher -

- 15 - severe attack - no chances of false positives, immediate attention is necessary

Levels 12 to 14 -

- 12 - High importance event - These include error or warning messages from the system, kernel etc. THese may indicate an attack against a specific application.
- 13 - unusual error (high importance) - it matches a common attack pattern most of the time
- 14 - High importance security event - it is triggered with correlation most of the time, and it indicates an attack

Levels 7 to 11 -

- 7 - bad word matching - These include the words like ‘bad’, ‘error’, etc. These events are most of the time unclassified and may have some security relevance.
- 8 - First time seen - includes first time seen events. First time an IDS event is fired or the first time a user logs in. It also includes security relevant actions such as the activation of a sniffer or similar activities.
- 9 - Error from invalid source - includes attempt to login as as unknown user or from an invalid source.
- 10 - Multiple user generated errors - The include multiple bad passwords, multiple failed logins.
- 11 - integrity checking warning - These include messages regarding the modification of binaries or the presence of rootkits (by root check)

Levels 0 to 6

- 0 - No action taken. Used to avoid false positives
- 2 - system low priority - system notification or status message
- 3 - Successful/Authorized events - These include successful log in attempts, firewall allow events etc.
- 4 - System low priority error - Errors related to bad configuration or unused device/applications. These have no security relevance and are usually caused by default installations or software testing
- 5 - user generated error - These include missed passwords, denied actions etc. By themselves, these have no security relevance
- 6 - low relevance attack - These indicate a worm or a virus that has no effect on the system, (like code red for apache servers). Also include frequent IDS events and frequent errors

Table of Dashboard overview

	Server one	Server Two	Server Three
Vulnerability Detection	• 79 critical • 1,886 High • 3,753 Medium • 74 Low	• 79 critical • 1,886 High • 3,753 Medium • 74 Low	• 155 critical • 2,175 High • 4,790 Medium • 148 Low

MITRE ATT&CK - Top Targets -	No MITRE ATT&CK results were found in the selected time range	No MITRE ATT&CK results were found in the selected time range	• Defence evasion - 2 • Privilege escalation - 2 • Initial Access - 1 • Persistence - 1
Top 5 Packages	• Linux-image-5.15.0-50-generic count: 3678 • Linux-image-5.15.0-60-generic count 3555 • Linux-image-5.15.0-134-generic count 1783 • Libcurl13-gnutls count 24 • OpenSSL count 23	• Linux-image-5.15.0-50-generic count: 3678 • Linux-image-5.15.0-60-generic count 3555 • Linux-image-5.15.0-134-generic count 1783 • Libcurl13-gnutls count 24 • OpenSSL count 23	• Linux-image-5.15.0-50-generic • Linux-image-5.15.0-60-generic • Mysql-client-8.0 • Mysql-client-core-8.0 • MySQL-server
Compliance	• 10.2.5 (2,908) • 10.2.4(2,908) • 10.2.6(1) • 10.2.6(1)	• 10.2.5 (1,1800) • 10.2.4(1,798) • 10.6.1(253) • 10.2.7(252) • 10.2.6(1)	• 10.2.5 (2,203) • 10.2.4(2,200) • 10.6.1(838) • 10.2.7(832) • 10.2.6(1)

Wazuh Dashboard Breakdown

The wazuh dashboard is broken down into 6 components which include vulnerability detection, MITRE ATT&CK, top 5 packages, compliance, events count evolution and Latest scans. Even though events count evolution and latest scans can be important when scanning a vulnerable server for the purpose of this breakdown it isn't important because although it has been

scanned for vulnerabilities we aren't running weekly scans on wazuh as we have another server which is set up to run weekly scans on all three of the servers we have set up.
So therefore on the wazuh dashboard there isn't going to be any change of the dashboard all round.

So the four main sections which are relevant to our project include vulnerability detection, MITRE ATT&CK, top 5 packages and compliance.
Vulnerability detection - The vulnerability detection module which is displayed within the wazuh dashboard is designed to show the users the vulnerabilities in the operating system which wazuh is scanning/scanned, in our instance a server,
The module functions using one of the following vulnerability sources:

- Wazuh vulnerabilities repository in our cyber threat intelligence (CTI) platform
- Offline local vulnerabilities repository

Wazuh also uses vulnerability data which is externally sourced from canonical,Debian,Red Hat, Arch Linux, Amazon Linux advisories Security (ALAS), Microsoft, CISA and the national vulnerability database (NVD).

MITRE ATT&CK - one of the frameworks which is displayed is the MITRE ATT&CK framework and it stands for MITRE adversarial tactics, techniques and common knowledge. It is a globally accessible collection of real world threat actions and behaviour. The reason it is implemented onto the wazuh dashboard is that it allows users to map alerts generated by wazuh to specific tactics and techniques. This gives security teams a better understanding of the nature of the security threats that the server may be facing and helps them to develop mitigation strategies.

Top 5 packages - Wazuh integrates with various tools such as OSSEC, security intelligence feeds, and vulnerability scanners to monitor and analyze the behavior of these packages, providing valuable insights.

These insights include; top installed packages, most vulnerable packages, most analysed:
Compliance - The compliance section of the wazuh dashboard implements compliance requirements for regular compliance support and visibility. Wazuh ruleset provides support for PCI DSS, HIPAA, NIST 800-53, TSC, and GDPR frameworks and standards

References

Scanning Docker infrastructure against CIS Benchmark with Wazuh | Wazuh - Cisbenchmarks overview
Vulnerability detection - Capabilities · Wazuh documentation - Page 8 - wazuh dashboard breakdown
MITRE ATT&CK framework - Data analysis · Wazuh documentation - Page 8 - wazuh dashboard breakdown
Regulatory compliance · Wazuh documentation - Page 8 - wazuh dashboard breakdown

ChatGPT - Top 5 packages meaning on wazuh dashboard - 14/03/2025 - page 8 - wazuh dashboard breakdown

ChatGPT 21/03/2025 - CIS Benchmarks breakdown for what each of the failed components mean