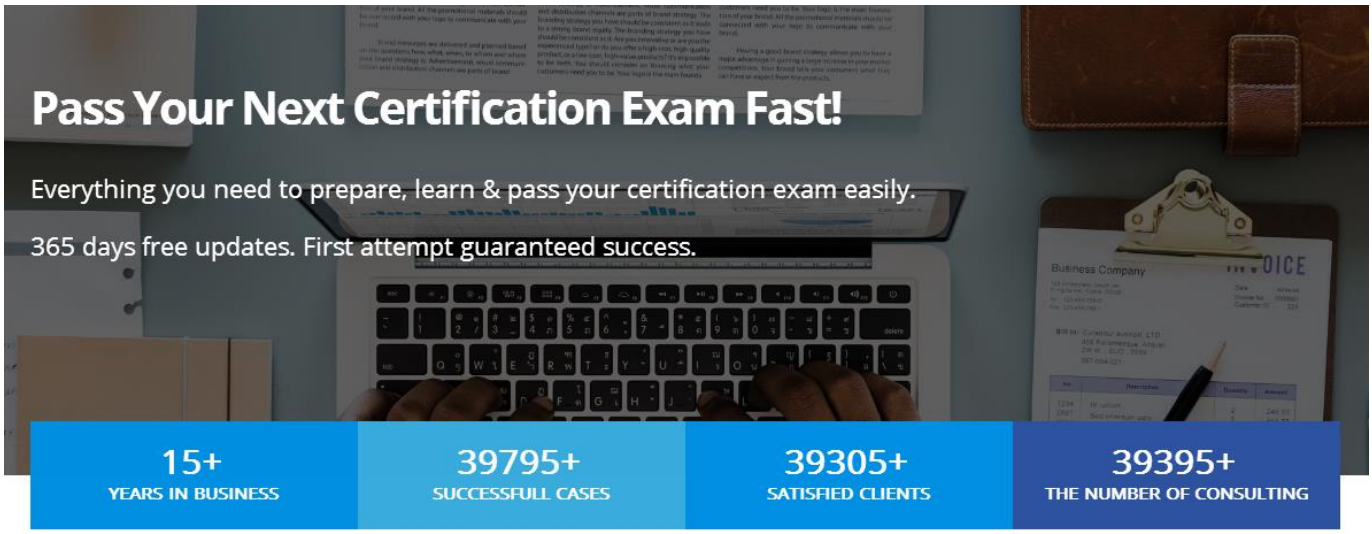
PracticeVCE



TRY BEFORE YOU BUY

Download a free sample of any of our exam questions and answers

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.

http://www.practicevce.com

Professional Study Tool and Reliable Exam Practice Material

Exam : **312-97**

Title : EC-Council Certified DevSecOps Engineer (ECDE)

Vendor : ECCouncil

Version : DEMO

NO.1 (Kenneth Danziger is a certified DevSecOps engineer, and he recently got a job in an IT company that develops software products related to the healthcare industry. To identify security and compliance issues in the source code and quickly fix them before they impact the source code, Kenneth would like to integrate WhiteSource SCA tool with AWS. Therefore, to integrate WhiteSource SCA Tool in AWS CodeBuild for initiating scanning in the code repository, he built a buildspec.yml file to the source code root directory and added the following command to pre-build phase curl -LJOhttps://github.com/whitesource/unified-agent-distribution/raw/master/standAlone/wss_agent.sh. Which of the following script files will the above step download in Kenneth organization's CodeBuild server?.)

A. wss_agent.sh.

B. ssw_agent.sh.

C. cbs_agent.sh.

D. aws_agent.sh.

Answer: A

Explanation:

The command shown in the pre-build phase explicitly targets a script namedwss_agent.sh. The curl -LJO flags mean: -L follows redirects, -J honors the server-provided filename in the Content-Disposition header (when present), and -O writes output to a local file using the remote name. Since the requested path ends with wss_agent.sh, the downloaded file on the AWS CodeBuild server will be wss_agent.sh. This script is the WhiteSource (now commonly referred to as Mend in many environments) unified agent shell wrapper used to run SCA scans as part of a CI pipeline. Integrating SCA during the Build and Test stage helps detect vulnerable open-source dependencies and licensing/compliance issues early, when fixes are cheapest. The other filenames (ssw_agent.sh, cbs_agent.sh, aws_agent.sh) are distractors; they are not referenced by the provided command and would not be downloaded by that step.

========

NO.2 (Rachel Maddow has been working at RuizSoft Solution Pvt. Ltd. for the past 7 years as a senior DevSecOps engineer. To develop software products quickly and securely, her organization has been using AWS DevOps services. On January 1, 2022, the software development team of her organization developed a spring boot application with microservices and deployed it in AWS EC2 instance. Which of the following AWS services should Rachel use to scan the AWS workloads in EC2 instance for security issues and unintended network exposures?.)

A. AWS Inspector.

B. AWS WAF.

C. AWS Config.

D. Amazon CloudWatch.

Answer: A

Explanation:

AWS Inspector is a managed vulnerability assessment service designed specifically to scan workloads running on Amazon EC2 instances and container images for security vulnerabilities and unintended network exposures. It automatically evaluates instances against known vulnerabilities and security best practices, providing detailed findings and risk severity levels. AWS WAF protects web applications from common web exploits but does not perform host-based vulnerability scanning. AWS Config tracks configuration changes and compliance but does not actively scan workloads for

vulnerabilities. Amazon CloudWatch focuses on monitoring logs, metrics, and alarms rather than security scanning. For a Spring Boot microservices application deployed on EC2, AWS Inspector is the correct choice to continuously assess security posture during the Build, Deploy, and Operate phases of the DevSecOps pipeline.
========

NO.3 (Lara Grice has been working as a DevSecOps engineer in an IT company located in Denver, Colorado. Her team leader has told her to save all the container images in the centos repository to centos-all.tar. Which of the following is a STDOUT command that Lara can use to save all the container images in the centos repository to centos-all.tar?.)

A. # docker save centos > centos all.tar.

B. # docker save centos > centos-all.tar.

C. # docker save centos < centos all.tar.

D. # docker save centos < centos-all.tar.

Answer: B

Explanation:
The docker save command exports one or more Docker images to a tar archive by writing the image data to standard output (STDOUT). To redirect this output into a file, the > redirection operator is used. The correct syntax is docker save <image> > <filename>.tar. In this scenario, the image repository name is centos, and the desired archive file is centos-all.tar, making option B correct. Options C and D incorrectly use input redirection (<) instead of output redirection. Option A includes a space in the filename (centos all.tar), which would be interpreted as two separate arguments and cause an error unless quoted. Saving images to a tar archive is a common operational task used for backups, transfers between environments, or offline analysis during the Operate and Monitor stage.
========

NO.4 (Matt LeBlanc has been working as a DevSecOps engineer in an IT company that develops software products and web applications for IoT devices. His team leader has asked him to use GitRob tool to find sensitive data in the organizational public GitHub repository. To install GitRob, Matt ensured that he has correctly configured Go >= 1.8 environment and that $GOPATH/bin is in his $PATH. The GitHub repository URL from which he is supposed to install the tool ishttps://github.com/michenriksen/gitrob. Which of the following command should Matt use to install GitRob?.)

A. $ go get github.com/michenriksen/gitrob.

B. $ go get gitrob github.com/michenriksen/gitrob.

C. $ go git github.com/michenriksen/gitrob.

D. $ go git gitrob github.com/michenriksen/gitrob.

Answer: A

Explanation:
In Go-based tool installation, the standard method to download, compile, and install a Go package is using the go get command followed by the repository import path. Since Matt has already ensured that Go version 1.8 or later is installed and that $GOPATH/bin is included in the system PATH, running go get github.com
/michenriksen/gitrob will fetch the GitRob source code, build the binary, and place it in the appropriate bin directory. Options B, C, and D are invalid because go get does not accept multiple

positional arguments in that manner, and go git is not a valid Go command. Installing GitRob during the Code stage enables DevSecOps teams to scan repositories for accidentally committed credentials, API keys, and other sensitive information, helping prevent data leakage from public repositories.
========

NO.5 (Lisa Kramer carries an experience of 4 years as a DevSecOps engineer in an IT company. The software development team of her organization has developed a Ruby on Rails web application and would like to find vulnerabilities in Ruby dependencies. Therefore, the team leader of the software development team approached Lisa for help in this regard. Which of the following SCA tool should Lisa use to detect vulnerabilities in Ruby dependencies?)

A. Bandit.

B. Bundler-Audit.

C. Retire.js.

D. Tenable.io.

Answer: B

Explanation:
Bundler-Audit is an SCA tool designed specifically for Ruby applications. It analyzes the Gemfile and Gemfile.lock to identify dependencies and checks them against known vulnerability databases. Bandit is intended for Python code analysis, Retire.js targets JavaScript libraries, and Tenable.io focuses on infrastructure-level vulnerabilities. By using Bundler-Audit during the Code stage, DevSecOps teams can detect vulnerable Ruby gems early and ensure that only secure dependencies are used. This reduces the risk of exploiting known vulnerabilities in third-party libraries and supports secure dependency management throughout the development lifecycle.
========

NO.6 (Joyce Vincent has been working as a senior DevSecOps engineer at MazeSoft Solution Pvt. Ltd. She would like to integrate Trend Micro Cloud One RASP tool with Microsoft Azure to secure container-based application by inspecting the traffic, detecting vulnerabilities, and preventing threats. In Microsoft Azure PowerShell, Joyce created the Azure container instance in a resource group (ACI) (named "aci-test-closh") and loaded the container image to it. She then reviewed the deployment of the container instance. Which of the following commands should Joyce use to get the logging information from the container?.)

A. az container logs --resource-group ACI --name aci-test-closh.

B. az container logs -resource-group ACI -name aci-test-closh.

C. azure container logs --resource-group ACI --name aci-test-closh.

D. azure container logs -resource-group ACI -name aci-test-closh.

Answer: A

Explanation:
Azure Container Instances (ACI) exposes container logs via the Azure CLI using the az container logs command. To retrieve logs, you must provide the resource group and the container group name using the long- form parameters --resource-group and --name. Option A matches the correct CLI structure and parameter format: az container logs --resource-group ACI --name aci-test-closh. Options B and D incorrectly use single- dash forms (-resource-group and -name), which are not valid for these long option names. Options C and D incorrectly use azure instead of az; the Azure CLI command group is invoked with az, not azure. Getting logs after deployment review is a critical

Operate and Monitor activity: it helps confirm the container started correctly, diagnose runtime errors, and validate that runtime protection (such as a RASP/micro-agent) is functioning. This visibility supports faster incident response and helps ensure the containerized workload remains secure and stable in its runtime environment.
========

NO.7 (Charlotte Flair is a DevSecOps engineer at Egma Soft Solution Pvt. Ltd. Her organization develops software and applications related to supply chain management. Charlotte would like to integrate Sqreen RASP tool with Slack to monitor the application at runtime for malicious activities and block them before they can damage the application. Therefore, she created a Sqreen account and installed Sqreen Microagent. Now, she would like to install the PHP microagent. To do so, she reviewed the PHP microagent's compatibility, then she signed in to Sqreen account and noted the token in Notepad. Which of the following commands should Charlotte run in the terminal to install the PHP extension and the Sqreen daemon?.)

A. curl -shttps://download.sqreen.com/php/install.sh> sqreen-install.sh \ && bash sqreen-install.sh [CHARLOTTE'S ORG TOKEN HERE] "[CHARLOTTE'S APP NAME HERE]".

B. curl -shttps://download.sqreen.com/php/install.sh< sqreen-install.sh \ && bash sqreen-install.sh [CHARLOTTE'S ORG TOKEN HERE] "[CHARLOTTE'S APP NAME HERE]".

C. curl -ihttps://download.sqreen.com/php/install.sh> sqreen-install.sh \ && bash sqreen-install.sh [CHARLOTTE'S ORG TOKEN HERE] "[CHARLOTTE'S APP NAME HERE]".

D. curl -ihttps://download.sqreen.com/php/install.sh< sqreen-install.sh \ && bash sqreen-install.sh [CHARLOTTE'S ORG TOKEN HERE] "[CHARLOTTE'S APP NAME HERE]".

Answer: A

Explanation:

The correct installation procedure for the Sqreen PHP microagent involves downloading the installer script and executing it with the organization token and application name. The curl -s option downloads the script silently, while the > redirection operator saves it locally as sqreen-install.sh. The script is then executed using bash, passing the required token and app name as parameters. Options using input redirection (<) are incorrect because they do not save the downloaded script to a file. The -i option includes HTTP headers in the output, which is unnecessary and could corrupt the script. Installing the microagent correctly enables runtime monitoring, attack detection, and automatic blocking, supporting strong runtime security during the Operate and Monitor stage.
========

NO.8 (Richard Branson has been working as a DevSecOps engineer in an IT company since the past 7 years. He has launched an application in a container one month ago. Recently, he modified the container and would like to commit the changes to a new image. Which of the following commands should Branson use to save the current state of the container as a new image?.)

A. container commit.

B. docker push.

C. container push.

D. docker commit.

Answer: D

Explanation:

The docker commit command is used to create a new Docker image from the current state of a

running or stopped container. This is useful when changes have been made interactively inside a container and need to be preserved as a reusable image. Commands such as docker push are used to upload images to a registry, not to create them, and container commit or container push are not valid Docker CLI commands. While docker commit can be helpful for quick snapshots or debugging, it is generally recommended to use Dockerfiles for reproducible builds in production pipelines. In the Build and Test stage, understanding docker commit helps DevSecOps engineers capture container changes for analysis, testing, or troubleshooting.
========

NO.9 (James Harden has been working as a senior DevSecOps engineer in an IT company located in Oakland, California. To detect vulnerabilities and to evaluate attack vectors compromising web applications, he would like to integrate Burp Suite with Jenkins. He downloaded the Burp Suite Jenkins plugins and then uploaded the plugin and successfully integrated Burp Suite with Jenkins. After integration, he would like to scan web application using Burp Suite; therefore, he navigated to Jenkins' dashboard, opened an existing project, and clicked on Configure. Then, he navigated to the Build tab and selected Execute shell from Add build step.
Which of the following commands should James enter under the Execute shell?.)

A. sudo BURP_SCAN_URL =http://target-website.com.

B. grep BURP_SCAN_URL =http://target-website.com.

C. cat BURP_SCAN_URL =http://target-website.com.

D. echo BURP_SCAN_URL =http://target-website.com.

Answer: D

Explanation:
When
configuring Burp Suite scans in Jenkins using an Execute shell build step, environment variables are often set or echoed so that subsequent scan steps can consume them. The echo command is used to output or define values in the shell context. In this case, echo BURP_SCAN_URL = http://target-website.com correctly defines the target URL for Burp Suite scanning. Commands like grep and cat are used for searching or displaying file contents and are not appropriate for setting scan parameters. The sudo command is unnecessary and incorrect in this context. Using the correct shell command ensures that Burp Suite receives the proper target information during the Build and Test stage, enabling accurate dynamic application security testing.
========

NO.10 (Peter McCarthy is working in TetraVerse Soft Solution Pvt. Ltd. as a DevSecOps engineer. His organization develops customized software products and web applications. To develop software products quickly and securely, his organization has been using AWS cloud-based services, including AWS DevOps services. Peter would like to use CloudMapper to examine the AWS cloud environment and perform auditing for security issues. Which of the following privileges should Peter possess in order to collect information about the AWS account?.)

A. arn:aws:iam::aws:policy/SecurityAudit arn:aws:iam::aws:policy/job-function/ViewOnlyAccess.

B. arn:aws:iam::aws:policy/SecurityCheck arn:aws:iam::aws:policy/job-function/ViewOnlyAccess:: EditOnlyAccess.

C. arn:aws:iam::aws:policy/SecurityAudit::SecurityCheck arn:aws:iam::aws:policy/job-role /ViewOnlyAccess:: EditOnlyAccess.

D. arn:aws:iam::aws:policy/AWSLambdaFullAccess arn:aws:iam::aws:policy/job-role/ViewOnlyAccess.

Answer: A

Explanation:

CloudMapper requires read-only access to AWS resources in order to collect metadata, visualize architectures, and perform security analysis without modifying infrastructure. The AWS-managed policy SecurityAuditprovides permissions to view security-related configuration across services, while ViewOnlyAccessallows read-only access to AWS resources more broadly. Together, these policies enable CloudMapper to gather comprehensive information about the AWS environment without granting write privileges. The other options either reference invalid policy names, incorrect formatting, or excessive permissions such as AWSLambdaFullAccess, which are unnecessary and violate least-privilege principles.

Granting SecurityAudit and ViewOnlyAccess aligns with secure auditing practices during the Operate and Monitor stage.

========