Exam Report: 7.3.3 Practice Questions

Date: 5/2/2020 6:33:46 pm
Time Spent: 0:34

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 14%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

Which of the following are the three metrics used to determine a CVSS score?

- Base, temporal, and environmental
- Risk, change, and severity
- ~~Risk, temporal, and severity~~
- Base, change, and environmental

Explanation

The base metric denotes a vulnerability's unique characteristics.

The temporal metric denotes the changeable attributes of a vulnerability.

The environmental metric denotes vulnerabilities that are present only in certain environments or implementations.

Risk, change, and severity are not metrics used to determine a CVSS score.

References

TestOut Ethical Hacker Pro - 7.3 Vulnerability Scoring Systems
[e_vuln_scoring_systems_eh1.exam.xml Q_VULN_SCORING_SYS_CVSS_CALC_01_EH1]

Question 2: Incorrect

Jessica, an employee, has come to you with a new software package she would like to use. Before you purchase and install the software, you would like to know if there are any known security-related flaws or if it is commonly misconfigured in a way that would make it vulnerable to attack. You only know the name and version of the software package. Which of the following government resources would you consider using to find an answer to your question?

- NVD
- CVSS
- ~~CVE~~
- CWE

Explanation

NVD, or the National Vulnerability Database, was originally created in 2000. You can find it at nvd.nist.gov. The NVD list includes more specific information for each entry than the CVE list, such as fix information, severity scores, and impact ratings. It is searchable by product name or version number, vendor, operating system, impact, severity, and related exploit range.

CVE is a list of standardized identifiers for known software vulnerabilities and exposures.

CVSS is a scoring system that creates a way to organize and prioritize vulnerabilities that you look for and discover in your work as an ethical hacker.

CWE is a community-developed list of common software security weaknesses.

References

TestOut Ethical Hacker Pro - 7.3 Vulnerability Scoring Systems
[e_vuln_scoring_systems_eh1.exam.xml Q_VULN_SCORING_SYS_VULN_GOV_RESOURCES_02_EH1]

Question 3: Incorrect

This government resource is a community-developed list of common software security weaknesses. They strive to create commonality in the descriptions of weaknesses of software security. Which of the following government resources is described?

- NVD
- ~~CVE~~
- CWE
- CISA

Explanation

CWE is a community-developed list of common software security weaknesses. This creates a reference for identification, mitigation, and prevention of vulnerabilities. This list provides a standardization for evaluating assessment tools. This site combines the diverse ideas and perspectives from professionals, academics, and government sources to create a unified standard on cybersecurity.

The CVE is a list of standardized identifiers for known software vulnerabilities and exposures. It is free to use and publicly available at cve.mitre.org.

The National Vulnerability Database, or NVD, is a government-sponsored, detailed database of known vulnerabilities.

CISA is a government agency. This government site provides information exchange, training and exercises, risk and vulnerability assessments, data synthesis and analysis, operational planning and coordination, watch operations, and incident response and recovery.

References

TestOut Ethical Hacker Pro - 7.3 Vulnerability Scoring Systems
[e_vuln_scoring_systems_eh1.exam.xml Q_VULN_SCORING_SYS_VULN_GOV_RESOURCES_03_EH1]

Question 4: Incorrect

Which of the following government resources is a directory of known patterns of cyberattacks used by hackers?

- CISA
- ~~CVE~~
- CWE
- CAPEC

Explanation

CAPEC is a dictionary of known patterns of cyberattack used by hackers. Its website is capec.mitre.org. You can search this list by mechanisms of attack or domains of attack, as well as by key terms and CAPEC ID numbers. This resource is valuable because you can browse through it to see common attacks used by hackers, and you can search for specific patterns of attack.

The CVE is a list of standardized identifiers for known software vulnerabilities and exposures. It is free to use and publicly available at cve.mitre.org.

CWE is a community-developed list of common software security weaknesses. Its website is

cwe.mitre.org.

CISA is a government agency. This government site provides information exchange, training and exercises, risk and vulnerability assessments, data synthesis and analysis, operational planning and coordination, watch operations, and incident response and recovery.

References

TestOut Ethical Hacker Pro - 7.3 Vulnerability Scoring Systems
[e_vuln_scoring_systems_eh1.exam.xml Q_VULN_SCORING_SYS_VULN_GOV_RESOURCES_04_EH1]

Question 5: Incorrect

The list of cybersecurity resources below are provided by which of the following government sites?

- Information exchange
- Training and exercises
- Risk and vulnerability assessments
- Data synthesis and analysis
- Operational planning and coordination
- Watch operations
- Incident response and recovery

- CAPEC
- CISA
- CWE
- ~~CVE~~

Explanation

Cybersecurity and Infrastructure Security Agency (CISA) is a large government-sponsored organization that provides many resources for cyber security.

This government site provides:

- Information exchange
- Training and exercises
- Risk and vulnerability assessments
- Data synthesis and analysis
- Operational planning and coordination
- Watch operations
- Incident response and recovery

CAPEC is a dictionary of known patterns of cyberattack used by hackers.

The CVE is a list of standardized identifiers for known software vulnerabilities and exposures. It is free to use and publicly available.

CWE is a community-developed list of common software security weaknesses.

References

TestOut Ethical Hacker Pro - 7.3 Vulnerability Scoring Systems
[e_vuln_scoring_systems_eh1.exam.xml Q_VULN_SCORING_SYS_VULN_GOV_RESOURCES_05_EH1]

Question 6: Correct

There are two non-government sites that provide lists of valuable information for ethical hackers. Which of the following best describes the Full Disclosure site?

- A list of standardized identifiers for known software vulnerabilities and exposures.
- A mailing list that often shows the newest vulnerabilities before other sources.
- A community-developed list of common software security weaknesses.
- A list searchable by mechanisms of attack or domains of attack.

Explanation

Full Disclosure is a mailing list from Nmap. This mailing list often shows the newest vulnerabilities before other sources.

The CVE is a list of standardized identifiers for known software vulnerabilities and exposures.

CAPEC is a dictionary of known patterns of cyberattack used by hackers. Its website is capec.mitre.org. This list is searchable by mechanisms of attack or domains of attack, as well as by key terms and CAPEC ID numbers.

CWE is a community-developed list of common software security weaknesses.

References

TestOut Ethical Hacker Pro - 7.3 Vulnerability Scoring Systems
[e_vuln_scoring_systems_eh1.exam.xml Q_VULN_SCORING_SYS_VULN_NON-GOV_RESOURCE_01_EH1]

Question 7: Incorrect

As an ethical hacker, you are looking for a way to organize and prioritize vulnerabilities that were discovered in your work. Which of the following scoring systems could you use?

- CISA
- ~~CVE~~
- CVSS
- CAPEC

Explanation

The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities.

The Common Vulnerabilities and Exposure (CVE) is a list of standardized identifiers for known software vulnerabilities and exposures.

CISA is a government agency. This government site provides information exchange, training and exercises, risk and vulnerability assessments, data synthesis and analysis, operational planning and coordination, watch operations, and incident response and recovery.

Common Attack Pattern Enumeration & Classification (CAPEC) is a dictionary of known patterns of cyberattack used by hackers.

References

TestOut Ethical Hacker Pro - 7.3 Vulnerability Scoring Systems
[e_vuln_scoring_systems_eh1.exam.xml Q_VULN_SCORING_SYS_VULN_SCORE_SYS_01_EH1]