Certified Ethical Hacker v9

Number: 312-50v9
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

http://www.gratisexam.com/

Exam A

QUESTION 1
The program snow is used for:

A. Password attacks
B. Spyware
C. Steganography
D. Sniffing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Information may be hidden into the slack space of a file.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
What software can be used to alter an image in stenography?

A. Photoshop
B. Firefox
C. Explorer
D. S-Tools

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
It is possible to hide a text message in _.

A. All of these
B. A graphic file
C. An audio file
D. Another message

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Steganography is used by:

GRATIS EXAM
Free Practice Exams

http://www.gratisexam.com/

A. Artists/Owners
B. All of these
C. Hackers
D. Terrorists

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 6
Steganography can be used for legitimate purposes.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
LSB insertion can serve as a steganographic technique to hide messages in audio files.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Steganography can be used to pass messages through uploaded photos on Facebook. True or False?

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Secret communications where the existence of the message is hidden is known as .

http://www.gratisexam.com/

A. Concealment Cipher
B. Image Processing
C. Running Cipher
D. Steganography

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Lossless compression are considered best for those applications where the integrity of an original information can be maintained. True or false?
// True

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Steganography can be detected by certain programs.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
The term that is best described as a process of replacing unwanted bits in an image and its source files with the secret data is known as_____.

A. Forensic Analysis
B. Steganography
C. Network Analysis
D. Cryptography

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which of these is a potential carrier file?

A. All of these
B. Executable file
C. Audio file
D. Image file

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Which of the layered approaches to security hides data in ICMP traffic:

A. Covert channels
B. Unique
C. Hiding directories
D. Encryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Information may be hidden into the slack space of a file.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following represents a form of steganography technique?

A. Password protection
B. Encryption

C. Highlight
D. Digital watermarking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which form of steganography generally includes a replication of an image so that any document source can be authenticated in a partial manner?

A. BMP tagging
B. Time stamp
C. Digital watermarking
D. Date stamp

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
JPEG images use discrete cosine transformation to achieve an optimal compression. True or false?

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19

The color of every 50th pixel in a video file corresponds to a letter in the alphabet. This is an example of steganography.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
True or false, Steganalysis detection performance is specified by the receiver operating characteristic or OC curve. The Operating Characteristic (OC) curve is the probability of detection versus the cumulative distribution.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
True or false, JPEG images use the discrete cosine transform to achieve compression?

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22

In steganography, it is crucial that only those people who are expecting the message know the message exists.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
True or false, lossless compression is better suited to applications where the integrity of the original information must be maintained?

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which of the following bit size images provides the most hiding space for information?

A. Single bit
B. 16-bit
C. 24-bit
D. 8-bit

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which of the following are three primary colors that are normally used in image analysis?

A. Peach, yellow, pink
B. Brown, red, orange
C. Red, green, blue
D. Black, white, gray

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following normally uses a layered approach for hiding the data in ICMP traffic?

A. Unique
B. Encryption
C. Hiding directories
D. Covert channels

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which of these is used during steganography to withstand statistical steganalysis?

A. Stream-based cryptography process
B. Data whitening process
C. Data encoding process
D. All of these

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
A stego is sent as a secret information that is embedded in normal traffic. Which of the following method is used?

A. Hidden active directory
B. Punching
C. Encryption
D. Covert channels

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Which process uses a GIF and BMP file that allows software to exactly reconstruct an original image?

A. Lost
B. Lossless
C. Laid compression
D. Wasteless

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Of these answers, which best describes the art of steganography?

A. The act of scrambling data using complex algorithms and special keys in order to secure and conceal data.
B. A malicious act where an insider-threat uses encryption and compression to smuggle data from a secured network
C. The process by which programmers break down and analyze code that is encrypted.
D. The process of injecting or concealing secret data or code into a common, easily-readable file so that the secret cannot be easily detected by ordinary means.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which of the choices is a form of steganography?

A. Video recordings
B. Digital watermarking
C. Audio tapes
D. Password protection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which of the following is the main use of digital watermarks and digital fingerprinting?

A. Monitoring patent applications
B. Track copyright issues
C. Develop a covert communication
D. Enhance duplication

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 33
Which of these choices is a form of steganography?

A. Digital watermarking
B. Video recordings
C. Audio tapes
D. Password protection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
What are noisy areas in steganography realm?

A. Grayscale color area
B. Black areas
C. Areas with a great deal of natural color variation
D. Areas with little color variation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
The tool 'snow' is a steganography tool.

A. whitespace

B. blackspace
C. deep
D. deadspace

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Which type of stenography includes the replication of an image, text, or logo, so that the source of the document can be partially authenticated?

A. Date stamping
B. JPEG tagging
C. Digital watermarking
D. Time stamping

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Adding identifiable information into a file or document is known as_____.

A. Copyright hiding
B. Counterfeiting
C. Watermarking
D. None of these

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
True or false stenography's niche in security of information is to replace cryptography?

A. True
B. False

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
The study of discovering messages that were hidden using the process of steganography is known as_____.

A. None of these
B. Steganographics
C. Steganographism
D. Steganalysis

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Steganography that is using a carrier chain would fail to reconstruct a message when:

A. Any of these
B. A carrier is modified
C. Carriers are processed in the wrong order
D. A carrier is unavailable

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which method is used where a stego is sent in information embedded within normal traffic?

A. Covert channels
B. Encryption
C. Hidden directory
D. Cipher text

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which layered approach to security hides data in ICMP traffic?

A. Hiding directories
B. Encryption
C. Covert channels
D. Unique

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
True or false. The robustness of spread spectrum steganography against active text comes at the cost of low and embedding capacity.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Steganalysis is not the method that is used to detect stenography.

A. True
B. False

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which of the following methods would help best in preventing the malicious steganography?

A. Routine server analysis
B. Specialized training
C. Hiring of internal developers
D. Policy that restricts installation of unauthorized programs on company's computers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46

True or false the properties of single files and entire directories can be changed to a hidden status to hide messages using the stego process?

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Traffic security can be correctly categorized under:

A. Traffic intelligence
B. Electric intelligence
C. Electronic security
D. Communication security

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
What is the main use of digital watermarks and digital fingerprinting today?

A. Track copyright issues
B. To develop covert communications
C. To monitor patent applications
D. To enhance duplication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Steganography noticeably changes the carrier file.

A. True
B. False

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Which of the following activities is not considered to be anti-forensics?

A. Data sanitizing
B. Trail obfuscation
C. Artifact wiping
D. Data hiding

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
How can a rootkit bypass Windows 7 operating system's kernel mode, code signing policy?

A. Attaching itself to the master boot record in a hard drive and changing the machine's boot sequence/options.
B. Replacing patch system calls with its own version that hides the rootkit (attacker's) actions.
C. Performing common services for the application process and replacing real applications with fake ones.
D. Defeating the scanner from detecting any code change at the kernel.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Which of these rootkits would you rate as the most effective?

A. Kernel level
B. Application level
C. Physical level
D. Library level

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which of the following is considered the most dangerous type of rootkit?

A. System level
B. Library level
C. Kernel level
D. Application level

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Rootkits are harder to detect than other malware.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
A rootkit is capable of:

A. Hiding processes
B. Hiding registry keys
C. All of these
D. Hiding files

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
What is a rootkit?

A. It's malware that intercepts packets in transit without being stored onto a target machine
B. It's malware that propagates without a specific target
C. It's malware that's used to gain access to a computer or computer system while being undetected
D. It's malware that uses social engineering techniques

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
You are doing a pen test against an organization that has just recovered from a major cyber-attack. The CISO and CIO want to completely and totally eliminate risk. What is one of the first things you should explain to these individuals?

GRATISEXAM
Free Practice Exams

http://www.gratisexam.com/

A. Explain that you cannot eliminate all risk but you will be able to reduce risk to acceptable levels.
B. Explain to them that they need to buy more services.
C. Tell him everything is going to a ok and collect that check!
D. Start the Wireshark application to sniff traffic

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
What should you do if a friend asks you to perform and penetration test as a favor outside your normal job of being a pen tester for a consulting company?

A. Start the test immediately
B. Start foot printing the friend's network
C. Start social engineering the friends company
D. Ask your employer for permission to perform the test outside of your normal work

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Which solution can be used to emulate real services such as ftp, mail, etc and capture login attempts and related information? They're often used to study hacker's activities.

A. Layer 4 switch
B. Core server
C. Honeypot
D. Firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
You need to monitor all traffic on your local network for suspicious activity and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?

A. Host based IDS
B. Proxy
C. Network based IDS
D. Firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Which property or concept ensures that a hash function will not produce the same hashed value for two different messages?

A. Key strength
B. Entropy

C. Bit length
D. Collision resistance

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
What is this Shellshock bash vulnerability attempting to do on this vulnerable Linux host? env x='(){:;};echo exploit' bash -c 'cat /etc/passwd'

A. Change all password in passwd
B. Remove the passwd file.
C. Add new user to the passwd file
D. Display passwd contents to prompt

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
During a routine assessment you discover information that suggests the customer is involved in human trafficking.

A. Ignore the data complete the job collect a check. Keep it moving!
B. Immediately stop work and contact the proper legal authorities
C. Copy the data to a thumb drive and keep it as leverage.
D. Confront the client in a respectful manner and ask about the data

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
What is the best description of SQL Injection?

A. It is an attack used to modify the code in an application
B. It is a Denial of Service Attack (DoS)
C. It is a MiTM attack
D. It is an attack used to gain unauthorized access to a database

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Which of the following defines the role of a root Certificate Authority (CA) in a Public Key Infrastructure (PKI)?

A. The root CA stores the user's hash value for safekeeping.
B. The root CA is the recovery agent used to encrypt data when a user's certificate is lost
C. The root CA is used to encrypt email messages to prevent unintended disclosure of data
D. The CA is the trusted root that issues certificates

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

A. Impact Risk
B. Inherent Risk
C. Deferred Risk
D. Residual Risk

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Which of the following problems can be solved by using Wireshark?

A. Resetting the administrator password on multiple systems
B. Troubleshooting communication resets between two systems
C. Tracking version changes of source code
D. Checking creation dates on all webpages on a server

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
This kind of malware is installed by criminals on your computer so they can lock it from a remote location. This malware generates a popup window, webpage, or email warning from what looks like an official authority such as the FBI. It explains your computer has been locked because of possible illegal activities and demands payment before you can access your files and programs again. Which term best matches this definition?

A. Ransomware
B. Adware
C. Riskware
D. Spyware

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Which of the following is a hashing algorithm?

A. PGP
B. DES
C. ROT13
D. MD5

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
An attacker gains access to a Web server's database and displays the contents of the table that holds all of the names, passwords, and other user information. The attacker did this by entering information into the Web site's user login page that the software's designers did not expect to be entered. This is an example of what kind of software design problem/issue?

A. Insufficient firewall rules
B. Insufficient input validation
C. Insufficient exception handling
D. Insufficient anti-virus detection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
What is the best way to defend against network sniffing?

A. Register all machines MAC address in a Centralized Database and
B. limit network connection to those machines
C. Use Static IP's
D. Using encryption protocols on network communications

E. Restrict physical access to server rooms host critical servers.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
What is a collision attack in cryptography?

A. Collision attacks try to break the hash into two parts with the same bytes in each part to get the private key
B. Collision attacks try to get the public key
C. Collision attacks try to find two inputs that produce the same hash
D. Collision attacks try to break the hash into three parts.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Which of the following is an example of the principle of least privilege as a system security control?

A. User should have limited access to the information regardless of its purpose
B. User must be able to access only the information and resources that are necessary for legitimate purpose
C. User should access all the information stored in the business to best execute their functions
D. Companies should have only a few employees

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Which tool queries publicly available databases that contain domain name registration contact information?

A. netstat
B. ifconfig
C. WHOIS
D. nslookup

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
The TJ Max breach happened in part because this type of weak wireless security was implemented.

A. WiFi Protected Access (WPA)
B. TKIP
C. Wired Equivalent Privacy (WEP)
D. WPA2

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Which wireless hacking tool attacks WEP and WPA-PSK?

GRATIS EXAM
Free Practice Exams
http://www.gratisexam.com/

A. Airguard
B. wificracker
C. Aircrack-ng
D. WLAN-crack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Which of the following techniques will identify if computer files have been changed?

A. Network sniffing
B. Integrity checking hashes
C. Firewall alerts
D. Permissions sets

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Nation-state threat actors often discover vulnerabilities and hold on to them until they want to launch a sophisticated attack. Stuxnet attack was an unprecedented style of attack because it used four types of this vulnerability. What is this style of attack called?

A. zero-sum
B. zero-day
C. no-day
D. zero-hour

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
You are doing a pen test against an organization that has just recovered from a major cyber-attack. The CISO and CIO want to completely and totally eliminate risk. What is one of the first things you should explain to these individuals?

A. Start the Wireshark application to sniff traffic
B. Tell him everything is going to A ok and collect that check!
C. Explain to them that they need to buy more services.
D. Explain that you cannot eliminate all risk but you will be able to reduce risk to acceptable levels.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
What should you do if a friend asks you to perform and penetration test as a favor outside your normal job of being a pentester for a consulting company?

A. Ask your employer for permission to perform the test outside of your normal work
B. Start social engineering the friends company
C. Start foot printing the friends' network
D. Start the test immediately

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Which solution can be used to emulate real services such as ftp, mail, etc and capture login attempts and related information? They're often used to study hacker's activities.

A. Honeypot
B. Layer 4 switch
C. Core server
D. Firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
You need to monitor all traffic on your local network for suspicious activity and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?

A. Host based IDS
B. Proxy
C. Network based IDS
D. Firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83

Which property or concept ensures that a hash function will not produce the same hashed value for two different messages?

A. Key strength
B. Bit length
C. Entropy
D. Collision resistance

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
During a routine assessment you discover information that suggests the customer is involved in human trafficking.

A. Copy the data to a thumb drive and keep it as leverage.
B. Immediately stop work and contact the proper legal authorities
C. Ignore the data complete the job collect a check. Keep it moving!
D. Confront the client in a respectful manner and ask about the data

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
What is the best description of SQL Injection?

A. It is an attack used to modify the code in an application
B. It is a Denial of Service Attack (DoS)
C. It is a MiTM attack
D. It is an attack used to gain unauthorized access to a database

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Which of the following defines the role of a root Certificate Authority (CA) in a Public Key Infrastructure (PKI)?

A. The root CA is the recovery agent used to encrypt data when a user's certificate is lost
B. The CA is the trusted root that issues certificates
C. The root CA is used to encrypt email messages to prevent unintended disclosure of data
D. The root CA stores the user's hash value for safekeeping.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

A. Impact Risk
B. Inherent Risk
C. Deferred Risk
D. Residual Risk

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which of the following problems can be solved by using Wireshark?

A. Troubleshooting communication resets between two systems
B. Tracking version changes of source code
C. Resetting the administrator password on multiple systems
D. Checking creation dates on all webpages on a server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
This kind of malware is installed by criminals on your computer so they can lock it from a remote location. This malware generates a popup window, webpage, or email warning from what looks like an official authority such as the FBI. It explains your computer has been locked because of possible illegal activities and demands payment before you can access your files and programs again. Which term best matches this definition?

A. Spyware
B. Riskware
C. Adware
D. Ransomware

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Which of the following is a hashing algorithm?

A. DES
B. ROT13
C. MD5
D. PGP

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 91
Which of the following is an example of the principle of least privilege as a system security control?

A. User should access all the information stored in the business to best execute their functions
B. Companies should have only a few employees
C. User should have limited access to the information regardless of its purpose
D. User must be able to access only the information and resources that are necessary for legitimate purpose

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
An individual who aims to bring down critical infrastructure for a "cause" and is not worried about facing 30 years in jail for their action.

A. Black Hat
B. Suicide Hacker
C. Gray Hat
D. White Hat

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
During a security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do?

A. Terminate the audit
B. Identify and evaluate existing practices
C. Create a procedures document
D. Conduct compliance testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing. What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?

A. Project Scope
B. Rules of Engagement
C. Service Level Agreement
D. Non- Disclosure Agreement

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up. What is the most likely cause?

A. The attacker altered or erased events from the logs.
B. Proper chain of custody was not observed while collecting the logs.
C. The security breach was a false positive.
D. The network devices are not all synchronized.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place. What Web browser-based security vulnerability was exploited to compromise the user?

A. Web form input validation
B. Cross-Site Request Forgery
C. Clickjacking
D. Cross-Site Scripting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
This phase will increase the odds of success in later phases of the penetration test. It is also the very first step in Information Gathering, and it will tell you what the "landscape" looks like. What is the most important phase of ethical hacking in which you need to spend a considerable amount of time?

A. Gaining access
B. Escalating privileges
C. Network mapping
D. Footprinting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Which of the following is a command line packet analyzer similar to GUI- based Wireshark?

A. Ethereal
B. Nessus
C. Tcpdump
D. Jack the ripper

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?

GRATIS EXAM
Free Practice Exams

http://www.gratisexam.com/

A. SOA
B. Biometrics
C. PKI
D. Single sign on

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?

A. Containment phase
B. Recovery phase
C. Identification phase
D. Preparation phase

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
After trying multiple exploits, you've gained root access to a Centos 6 server. To ensure you maintain access, what would you do first?

A. Disable Key Services
B. Create User Account
C. Disable IPTables
D. Download and Install Netcat

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
This international organization regulates billions of transactions daily and provides security guidelines to protect personally identifiable information (PII). These security controls provide a baseline and prevent low-level hackers sometimes known as script kiddies from causing a data breach. Which of the following organizations is being described?

A. International Security Industry Organization (ISIO)
B. Payment Card Industry (PCI)

C. Institute of Electrical and Electronics Engineers (IEEE)
D. Center for Disease Control (CDC)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
What is the process of logging, recording, and resolving events that take place in an organization?

A. Security Policy
B. Internal Procedure
C. Incident Management Process
D. Metrics

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
env x=`(){ :;};echo exploit` bash -c 'cat /etc/passwd'
What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?

A. Display passwd content to prompt
B. Changes all passwords in passwd
C. Add new user to the passwd file
D. Removes the passwd file

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
You work as a Security Analyst for a retail organization. In securing the company's network, you set up a firewall and an IDS. However, hackers are able to attack the network. After investigating, you discover that your IDS is not configured properly and therefore is unable to trigger alarms when needed. What type of alert is the IDS giving?

A. True Positive
B. True Negative
C. False Negative
D. False Positive

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
What does a firewall check to prevent particular ports and applications from getting packets into an organization?

A. Application layer port numbers and the transport layer headers
B. Transport layer port numbers and application layer headers
C. Presentation layer headers and the session layer port numbers
D. Network layer headers and the session layer port numbers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners. What proxy tool will help you find web vulnerabilities?

A. Burpsuite
B. Proxy chains
C. Dimitry
D. Maskgen

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
You have successfully gained access to your client's internal network and successfully comprised a Linux server which is part of the internal IP network. You want to know which Microsoft Windows workstations have file sharing enabled.
Which port would you see listening on these Windows machines in the network?

A. 1433
B. 161
C. 3389
D. 445

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
Which of the following is a component of a risk assessment?

A. Administrative safeguards
B. Logical interface
C. DMZ
D. Physical security

Correct Answer:
Section: (none)

Explanation

Explanation/Reference:

QUESTION 110
Using Windows CMD, how would an attacker list all the shares to which the current user context has access?

GRATIS EXAM
Free Practice Exams

http://www.gratisexam.com/

A. NET FILE
B. NET USE
C. NET VIEW
D. NET CONFIG

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
Perspective clients want to see sample reports from previous penetration tests. What should you do next?

A. Decline, just provide the details of the components that will be there in the report.
B. Share full reports, not redacted.
C. Decline, just provide references.
D. Share sample reports with redactions after NDA is signed.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
Your team has won a contract to infiltrate an organization. The company wants to have the attack be as realistic as possible; therefore, they did not provide any information besides the company name. What should be the first step in security testing the client?

A. Scanning
B. Enumeration
C. Escalation
D. Reconnaissance

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
The Open Web Application Security Project (OWASP) is the worldwide not- for-profit charitable organization focused on improving the security of software. What item is the primary concern on OWASP's Top Ten Project Most Critical Web Application Security Risks?

A. Cross Site Scripting
B. Cross Site Request Forgery
C. Injection
D. Path disclosure

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
Which regulation defines security and privacy controls for Federal information systems and organizations?

A. EU Safe Harbor
B. PCI-DSS
C. HIPAA
D. NIST-800-53

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
When you are collecting information to perform a data analysis, Google commands are very useful to find sensitive information and files. These files may contain information about passwords, system functions, or documentation. What command will help you to search files using Google as a search engine?

A. inurl: target.com filename:xls username password email
B. site: target.com filetype:xls username password email site:
C. target.com file:xls username password email domain:
D. target.com archive:xls username password email

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
You have successfully gained access to a linux server and would like to ensure that the succeeding outgoing traffic from this server will not be caught by a Network Based Intrusion Detection Systems (NIDS).
What is the best way to evade the NIDS?

A. Out of band signaling
B. Alternate Data Streams
C. Protocol Isolation
D. Encryption

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very Difficult for an IDS to detect the attack signatures. Which tool can be used to perform session splicing attacks?

A. Burp
B. Hydra
C. Whisker
D. TCP splice

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
It is a regulation that has a set of guidelines, which should be adhered to by anyone who handles any electronic medical data. These guidelines stipulate that all medical practices must ensure that all necessary measures are in place while saving, accessing, and sharing any electronic medical data to keep patient data secure.
Which of the following regulations best matches the description?

A. ISO/IEC 27002
B. HIPAA
C. FISMA
D. COBIT

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

A. ESP transport
B. mode AH Tunnel
C. mode ESP
D. AH promiscuous

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
A regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server. Based on this information, what should be one of your key recommendations to the bank?

A. Require all employees to change their anti-virus program with a new one
B. Move the financial data to another server on the same IP subnet
C. Issue new certificates to the web servers from the root certificate authority
D. Place a front-end web server in a demilitarized zone that only handles external web traffic

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
Which of the following is one of the most effective ways to prevent Cross- site Scripting (XSS) flaws in software applications?

A. Use digital certificates to authenticate a server prior to sending data
B. Use security policies and procedures to define and implement proper security settings
C. Validate and escape all information sent to a server
D. Verify access right before allowing access to protected information and UI controls

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
You are the Systems Administrator for a large corporate organization. You need to monitor all network traffic on your local network for suspicious activities and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?

A. Firewall
B. Proxy
C. Network-based
D. IDS Host-based IDS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft through a technique known as war driving. Which Algorithm is this referring to?

A. Wi-Fi Protected Access 2 (WPA2)
B. Wi-Fi Protected Access (WPA)
C. Temporal Key Integrity Protocol (TKIP)
D. Wired Equivalent Privacy (WEP)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
Which of the following tools can be used for passive OS fingerprinting?

A. tracert
B. ping
C. nmap
D. tcpdump

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run Wireshark in the snort machine to check if the messages are going to the kiwi syslog machine.
What Wireshark filter will show the connections from the snort machine to kiwi syslog machine?

A. tcp.dstport==514 && ip.dst==192.168.0.99
B. tcp.srcport==514 && ip.src==192.168.150
C. tcp.dstport==514 && ip.dst==192.168.0.150
D. tcp.srcport==514 && ip.src==192.168.0.99

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
You have compromised a server and successfully gained a root access. You want to pivot and pass traffic undetected over the network and evade any possible Intrusion Detection System. What is the best approach?

A. Install and use Telnet to encrypt all outgoing traffic from this server.
B. Use Alternate Data Streams to hide the outgoing packets from this server.

C. Install Cryptcat and encrypt outgoing packets from this server.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems. The security concept of "separation of duties" is most similar to the operation of which type of security device?

A. Bastion host
B. Honeypot
C. Firewall
D. Intrusion Detection System

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
An attacker gains access to a Web server's database and displays the contents of the table that holds all of the names, passwords, and other user information. The attacker did this by entering information into the Web site's user login page that the software's designers did not expect to be entered. This is an example of what kind of software design problem?

A. Insufficient security management
B. Insufficient exception handling
C. Insufficient database hardening
D. Insufficient input validation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
Which of the following is not a Bluetooth attack?

A. Bluedriving
B. Bluesmacking
C. Bluesnarfing
D. Bluejacking

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security policies. Which one of the following tools would most likely be used in such an audit?

A. Intrusion Detection System
B. Protocol analyzer
C. Vulnerability scanner
D. Port scanner

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
What is a "Collision attack" in cryptography?

A. Collision attacks try to get the public key
B. Collision attacks try to find two inputs producing the same hash.

C. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key.
D. Collision attacks try to break the hash into three parts to get the plaintext value.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
Which of the following is the greatest threat posed by backups?

A. A backup is incomplete because no verification was performed
B. A backup is unavailable during disaster recovery
C. A backup is the source of Malware or illicit information.
D. An un-encrypted backup can be misplaced or stolen

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

A. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.
B. Attempts by attackers to access passwords stored on the user's computer without the user's knowledge.
C. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.
D. Attempts by attackers to access the user and password information stored in the company's SQL database.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
You have compromised a server on a network and successfully opened a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the network using the nmap syntax below, it is not going through. invictus@victim_server:
~$ nmap -T4 -O 10.10.0.0/24
TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx. QUITTING!
What seems to be wrong?

A. OS Scan requires root privileges.
B. The nmap syntax is wrong.
C. This is a common behavior for a corrupted nmap application.
D. The outgoing TCP/IP fingerprinting is blocked by the host firewall.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network. What is this type of DNS configuration commonly called?

A. Split DNS
B. DNSSEC
C. DNS Scheme
D. DynDNS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136

It is a kind of malware (malicious software) that criminals install on your computer so they can lock it from a remote location. This malware generates a pop-up window, webpage, or email warning from what looks like an official authority. It explains that your computer has been locked because of possible illegal activities on it and demands payment before you can access your files and programs again. Which of the following terms best matches the definition?

GRATIS EXAM
Free Practice Exams

http://www.gratisexam.com/

A. Ransomware
B. Spyware
C. Riskware
D. Adware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
Which of these options is the most secure procedure for storing backup tapes?

A. In a cool dry environment
B. In a climate controlled facility offsite
C. Inside the data center for faster retrieval in a fireproof safe
D. On a different floor in the same building

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
Which tool allows analysts and pen testers to examine links between data using graphs and link analysis?

A. Wireshark
B. Cain & Abel
C. Maltego
D. Metasploit

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?

A. Dsniff
B. John the Ripper
C. Snort
D. Nikto

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
Which of the following describes the characteristics of a Boot Sector Virus?

A. Overwrites the original MBR and only executes the new virus code
B. Modifies directory table entries so that directory entries point to the virus code instead of the actual program
C. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR
D. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
You are performing a penetration test. You achieved access via a buffer overflow exploit and you proceed to find interesting data, such as files with usernames and passwords. You find a hidden folder that has the administrator's bank account password and login information for the administrator's bitcoin account. What should you do?

A. Transfer money from the administrator's account to another account
B. Do not report it and continue the penetration test
C. Report immediately to the administrator
D. Do not transfer the money but steal the bitcoins

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
It is a vulnerability in GNU's bash shell, discovered in September of 2014 that gives attackers access to run remote commands on a vulnerable system. The malicious software can take control of an infected machine, launch denial-of-service attacks to disrupt websites, and scan for other vulnerable devices (including routers).
Which of the following vulnerabilities is being described?

A. Shellbash
B. Rootshock
C. Shellshock
D. Rootshell

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
Which of the following is designed to identify malicious attempts to penetrate systems?

A. Intrusion Detection System
B. Router
C. Proxy
D. Firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
Which of the following security operations is used for determining the attack surface of an organization?

A. Using configuration management to determine when and where to apply security patches
B. Training employees on the security policy regarding social engineering
C. Reviewing the need for a security clearance for each employee
D. Running a network scan to detect network services in the corporate DMZ

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
How does the Address Resolution Protocol (ARP) work?

A. It sends a request packet to all the network elements, asking for the domain name from a specific IP.

B. It sends a request packet to all the network elements, asking for the MAC address from a specific IP.
C. It sends a reply packet for a specific IP, asking for the MAC address.
D. It sends a reply packet to all the network elements, asking for the MAC address from a specific IP.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
Which of the following types of firewalls ensures that the packets are part of the established session?

GRATIS EXAM
Free Practice Exams
http://www.gratisexam.com/

A. Stateful inspection firewall
B. Application-level firewall
C. Circuit-level firewall
D. Switch-level firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
Ricardo wants to send secret messages to a competitor company. To secure these messages, he uses a technique of hiding a secret message within an ordinary message. The technique provides 'security through obscurity'. What technique is Ricardo using?

A. Encryption

B. Public-key cryptography
C. RSA algorithm
D. Steganography

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, and TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, PUT, DELETE, TRACE) using NMAP script engine. What nmap script will help you with this task?

A. http-git
B. http-methods
C. http-headers
D. http enum

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
The "black box testing" methodology enforces which kind of restriction?

A. Only the internal operation of a system is known to the tester.
B. The internal operation of a system is only partly accessible to the tester.
C. Only the external operation of a system is accessible to the tester.
D. The internal operation of a system is completely known to the tester.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file. What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

A. Protocol analyzer
B. Network sniffer
C. Intrusion Prevention System (IPS)
D. Vulnerability scanner

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
Jesse receives an email with an attachment labeled “Court_Notice_21206.zip”. Inside the zip file is a file named “Court_Notice_21206.docx.exe” disguised as a word document. Upon execution, a window appears stating, “This word document is corrupt.” In the background, the file copies itself to Jesse APPDATA\local directory and begins to beacon to a C2 server to download additional malicious binaries. What type of malware has Jesse encountered?

A. Macro Virus
B. Trojan
C. Key-Logger
D. Worm

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
Risks = Threats x Vulnerabilities is referred to as the:

A. Threat assessment
B. Risk equation
C. BIA equation
D. Disaster recovery formula

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
The purpose of a
networks and other information assets by unauthorized wireless devices.

A. Wireless Access Control List
B. Wireless Analyzer
C. Wireless Access Point
D. Wireless Jammer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program.
What term is commonly used when referring to this type of testing?

A. Mutating

B. Randomizing
C. Fuzzing
D. Bounding

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
The "gray box testing" methodology enforces what kind of restriction?

A. The internal operation of a system is only partly accessible to the tester.
B. Only the external operation of a system is accessible to the tester.
C. The internal operation of a system is completely known to the tester.
D. Only the internal operation of a system is known to the tester

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
You have several plain-text firewall logs that you must review to evaluate network traffic. You know that in order to do fast, efficient searches of the logs you must use regular expressions.
Which command-line utility are you most likely to use?

A. Grep
B. Relational Database
C. Notepad
D. MS Excel

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
You have successfully compromised a machine on the network and found a server that is alive on the same network. You tried to ping it but you didn't get any response back. What is happening?

A. The ARP is disabled on the target server.
B. ICMP could be disabled on the target server.
C. TCP/IP doesn't support ICMP.
D. You need to run the ping command with root privileges.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE- 2014- 0160. This bug affects the OpenSSL implementation of the transport layer security (TLS) protocols defined in RFC6520. What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?

A. Root
B. Private
C. Public
D. Shared

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
When you return to your desk after a lunch break, you notice a strange email in your inbox. The sender is someone you did business with recently, but the subject line has strange characters in it.

What should you do?

http://www.gratisexam.com/

A. Delete the email and pretend nothing happened.
B. Reply to the sender and ask them for more information about the message contents.
C. Forward the message to your company's security response team and permanently delete the message from your computer.
D. Forward the message to your supervisor and ask for her opinion on how to handle the situation.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
Under the "Post-attack Phase and Activities," it is the responsibility of the tester to restore the systems to a pre-test state.
Which of the following activities should not be included in this phase? Removing all files uploaded on the system
I. Cleaning all registry entries
II. Mapping of network state
III. Removing all tools and maintaining backdoor for reporting

A. III
B. III and IV
C. IV
D. All should be included

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
A medium-sized healthcare IT business decides to implement a risk management strategy.
Which of the following is NOT one of the five basic responses to risk?

A. Avoid
B. Mitigate
C. Accept
D. Delegate

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
An Internet Service Provider (ISP) has a need to authenticate users connecting using analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network.
Which AAA protocol is most likely able to handle this requirement?

A. RADIUS
B. Kerberos
C. DIAMETER
D. TACACS+

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
Your company was hired by a small healthcare provider to perform
a technical assessment on the network.
What is the best approach for discovering vulnerabilities on a Windows- based computer?

A. Use the built-in Windows Update tool
B. Create a disk image of a clean Windows installation
C. Check MITRE.org for the latest list of CVE findings
D. Use a scan tool like Nessus

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
You are performing information gathering for an important penetration test. You have found pdf, doc, and images in your objective. You decide to extract metadata from these files and analyze it. What tool will help you with the task?

A. cdpsnarf
B. Metagoofil
C. Armitage
D. Dimitry

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application. What kind of Web application vulnerability likely exists in their software?

A. Cross-site Request Forgery vulnerability
B. SQL injection vulnerability
C. Cross-site scripting vulnerability
D. Session management vulnerability

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the central processing unit (CPU), rather than passing only the frames that the controller is intended to receive. Which of the following is being described?

A. Port forwarding
B. Multi-cast mode
C. WEP
D. promiscuous mode

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167
A hacker has successfully infected an internet-facing server which he will then use to send junk mail, take part in coordinated attacks, or host junk email content. Which sort of Trojan infects this server?

A. Turtle Trojans
B. Ransomware Trojans
C. Botnet Trojan
D. Banking Trojans

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168

Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

A. tcptrace
B. Tcptraceroute
C. OpenVAS
D. Nessus

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
Which of the following parameters describe LM Hash?
I - The maximum password length is 14 characters.
II - There are no distinctions between uppercase and lowercase.
III - The password is split into two 7-byte halves.

A. I
B. II
C. I, II and III
D. I and II

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com", that the user is directed to a phishing site.
Which file does the attacker need to modify?

A. Hosts
B. Sudoers

C. Boot.ini
D. Networks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
Which of the following statements regarding ethical hacking is incorrect?

A. Ethical hacking should not involve writing to or modifying the target systems.
B. An organization should use ethical hackers who do not sell vendor hardware/software or other consulting services.
C. Testing should be remotely performed offsite.
D. Ethical hackers should never use tools or methods that have the potential of exploiting vulnerabilities in an organization's systems.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
What is the benefit of performing an unannounced Penetration Testing?

A. It is best approach to catch critical infrastructure unpatched.
B. The tester could easily acquire a complete overview of the infrastructure of the organization.
C. The tester will get a clearer picture of measures applied to information and system security of the organization.
D. The tester can test the response capabilities of the target organization.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
Which of the following is the BEST way to defend against network sniffing?

A. Use Static IP Address
B. Register all machines MAC Address in a Centralized Database
C. Restrict Physical Access to Server Rooms hosting Critical Servers
D. Using encryption protocols to secure network communications

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The ps command shows that the nc file is running as process, and the netstat command shows the nc process is listening on a network port. What kind of vulnerability must be present to make this remote attack possible?

A. File system permissions
B. Directory traversal
C. Brute force login
D. Privilege escalation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
While using your bank's online servicing you notice the following string in the URL bar:

http://www.MyPersonalBank.com/account?id=368940911028389&Damount=10980&Camount=21”

You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflect the changes. Which type of vulnerability is present on this site?

A. Cookie Tampering
B. XSS Reflection
C. SQL injection
D. Web Parameter Tampering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
This tool is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the PTW attack, thus making the attack much faster compared to other WEP cracking tools.
Which of the following tools is being described?

A. Aircrack-ng
B. Wificracker
C. Airguard
D. WLAN-crack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
Which of the following is the successor of SSL?

A. IPSec
B. TLS
C. GRE
D. RSA

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
In Risk Management, how is the term "likelihood" related to the concept of "threat?"

A. Likelihood is a possible threat-source that may exploit a vulnerability.
B. Likelihood is the likely source of a threat that could exploit a vulnerability.
C. Likelihood is the probability that a vulnerability is a threat-source.
D. Likelihood is the probability that a threat-source will exploit a vulnerability.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
Which of the following is a low-tech way of gaining unauthorized access to systems?

A. Social Engineering
B. Eavesdropping
C. Scanning
D. Sniffing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180
You are attempting to man-in-the-middle a session. Which protocol will allow you to guess a sequence number?

A. ICMP
B. TCP
C. UPX
D. UPD

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
During a black box pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded.
What type of firewall is inspecting outbound traffic?

A. Packet Filtering
B. Application
C. Circuit
D. Stateful

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
Which of the following is considered the best way to protect Personally Identifiable Information (PII) from Web application vulnerabilities?

A. Use a security token to log into all Web applications that use PII
B. Use full disk encryption on all hard drives to protect PII
C. Use encrypted communications protocols to transmit PII
D. Store all PII in encrypted format

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
Which method of password cracking takes the most time and effort?

A. Rainbow tables
B. Shoulder surfing
C. Brute force
D. Dictionary attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
It is a short-range wireless communication technology intended to replace the cables connecting portable of fixed devices while maintaining high levels of security. It allows mobile phones, computers and other devices to connect and communicate using a short-range wireless connection. Which of the following terms best matches the definition?

A. Bluetooth
B. InfraRed
C. Radio-Frequency Identification
D. WLAN

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 185
A common cryptographical tool is the use of XOR. XOR the following
binary values:
10110001
00111010

A. 10001011
B. 11011000
C. 10111100
D. 10011101

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186
Port scanning can be used as part of a technical assessment to determine network vulnerabilities. The TCP XMAS scan is used to identify listening ports on the targeted system. If a scanned port is open, what happens?

A. The port will ignore the packets
B. The port will send an RST
C. The port will send a SYN
D. The port will send an ACK

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187

Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?

A. Fingerprints
B. Height and Weight
C. Iris patterns
D. Voice

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188
It is an entity or event with the potential to adversely impact a system through unauthorized access, destruction, disclosure, denial of service or modification of data. Which of the following terms best matches the definition?

A. Threat
B. Attack
C. Vulnerability
D. Risk

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 189
> NMAP -sn 192.168.11.200-215
The NMAP command above performs which of the following?

A. A trace sweep
B. An operating system detect
C. A ping scan
D. A port scan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190
Nation-state threat actors often discover vulnerabilities and hold on to them until they want to launch a sophisticated attack. The Sutxnet attack was an unprecedented style of attack because it used four types of vulnerability.
What is this style of attack called?

A. zero-sum
B. no-day
C. zero-day
D. zero-hour

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191
You've just been hired to perform a pen test on an organization that has been subjected to a large-scale attack. The CIO is concerned with mitigating threats and vulnerabilities to totally eliminate risk. What is one of the first things you should do when given the job?

A. Explain to the CIO that you cannot eliminate all risk, but you will be able to reduce risk to acceptable levels.
B. Interview all employees in the company to rule out possible insider threats
C. Establish attribution to suspected attackers
D. Start the Wireshark application to start sniffing network traffic.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
Initiating an attack against targeted businesses and organizations, threat actors compromise a carefully selected website by inserting an exploit resulting in malware infection. The attackers run exploits on well-known and trusted sites likely to be visited by their targeted victims. Aside from carefully choosing sites to compromise, these attacks are known to incorporate zero-day exploits that target unpatched vulnerabilities. Thus, the targeted entities are left with little or no defense against these exploits. What type of attack is outlined in the scenario?

A. Watering Hole Attack
B. Shellshock Attack
C. Spear Phishing Attack
D. Heartbleed Attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 193
A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering the NMAP result below, which of the following is likely to be installed on the target machine by the OS?
Starting NMAP 5.21 at 2011-03-15 11:06 NMAP scan report for 172.16.40.65 Host is up (1.00s latency).Not shown: 993 closed ports PORT STATE SERVICE 21/ tcp open ftp 23/tcp open telnet 80/tcp open http 139/tcp open netbios-ssn 515/tcp open 631/tcp open ipp 9100/tcp open MAC Address: 00:00:48:0D:EE:8

A. The host is likely a Windows machine
B. The host is likely a Linux machine.
C. The host is likely a router.
D. The host is likely a printer.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 194
This asymmetry cipher is based on factoring the product of two large prime numbers. What cipher is described above?

A. RC5
B. MD5
C. RSA
D. SHA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 195
The "white box testing" methodology enforces what kind of restriction?

A. The internal operation of a system is only partly accessible to the tester.
B. Only the internal operation of a system is known to the tester.
C. Only the external operation of a system is accessible to the tester.
D. The internal operation of a system is completely known to the tester.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 196
What is the best description of SQL Injection?

A. It is an attack used to gain unauthorized access to a database.
B. It is an attack used to modify code in an application.
C. It is a Man-in-the-Middle attack between your SQL Server and Web App Server.
D. It is a Denial of Service Attack.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197
You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from command line. Which command would you use?

A. c:\ncpa.cpl
B. c:\services.msc
C. c:\gpedit
D. c:\compmgmt.msc

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 198
You are using NMAP to resolve domain names into IP addresses for a ping sweep later. Which of the following commands looks for IP addresses?

A. >host -t AXFR hackeddomain.com
B. >host -t a hackeddomain.com
C. >host -t soa hackeddomain.com
D. >host -t ns hackeddomain.com

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 199
Which of the following countermeasure can specifically protect against both the MAC Flood and MAC Spoofing attacks?

A. Configure Port Security on the switch

B. Configure Port Recon on the switch
C. Configure Switch Mapping
D. Configure Multiple Recognition on the switch

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 200
This IDS defeating technique works by splitting a datagram (or packet) into multiple fragments and the IDS will not spot the true nature of the fully assembled datagram. The datagram is not reassembled until it reaches its final destination. It would be a processor-intensive task for IDS to reassemble all fragments itself, and on a busy system the packet will slip through the IDS onto the network. What is this technique called?

A. IP Routing or Packet Dropping
B. IDS Spoofing or Session Assembly
C. IP Fragmentation or Session
D. Splicing IP Splicing or Packet Reassembly

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 201
This type of Port Scanning technique splits TCP header into several packets so that the packet filters are not able to detect what the packets intends to do?

A. UDP Scanning
B. IP Fragment Scanning
C. Inverse TCP flag scanning
D. ACK flag scanning

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 202
Joel and her team have been going through tons of garbage, recycled paper, and other rubbish in order to find Some information about the target they are attempting to penetrate. How would you call this type of activity?

A. Dumpster Diving
B. Scanning
C. CI Gathering
D. Garbage Scooping

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 203
Hacker wants to break into Brown Co.'s computers and obtain their secret double fudge cookie recipe. Jack calls Jane, an accountant at Brown Co., pretending to be an administrator from Brown Co. Jack tells Jane that there has been a problem with some accounts and asks her to verify her password with him "just to double check our records." Jane does not suspect anything amiss, and parts with her password. Jack can now access Brown Co.'s computers with a valid user name and password, to steal the cookie recipe. What kind of attack is being illustrated here?

A. Reverse Psychology Reverse Engineering
B. Social Engineering
C. Spoofing Identity
D. Faking Identity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 204
TCP SYN Flood attack uses the three-way handshake mechanism.

1. An attacker at system A sends a SYN packet to victim at system B. 2. System B sends a SYN/ACK packet to victim A.
3. As a normal three-way handshake mechanism system A should send an ACK packet to system B, however, system A does not send an ACK packet to system B. In this case client B is waiting for an ACK packet from client A.
This status of client B is called _____

A. "half-closed"
B. "half open"
C. "full-open"
D. "xmas-open"

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 205
How do you defend against Privilege Escalation?

A. Use encryption to protect sensitive data
B. Restrict the interactive logon privileges
C. Run services as unprivileged accounts
D. Allow security settings of IE to zero or Low
E. Run users and applications on the least privileges

Correct Answer: ABCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 206
What does ICMP (type 11, code 0) denote?

A. Source Quench
B. Destination Unreachable
C. Time Exceeded

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 207
More sophisticated IDSs look for common shellcode signatures. But even these systems can be bypassed, by using polymorphic shellcode. This is a technique common among virus writers? It basically hides the true nature of the shellcode in different disguises. How does a polymorphic shellcode work?

A. They encrypt the shellcode by XORing values over the shellcode, using loader code to decrypt the shellcode, and then executing the decrypted shellcode
B. They convert the shellcode into Unicode, using loader to convert back to machine code then executing them
C. They reverse the working instructions into opposite order by masking the IDS signatures
D. They compress shellcode into normal instructions, uncompressed the shellcode using loader code and then executing the shellcode

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 208
The FIN flag is set and sent from host A to host B when host A has no more data to transmit (Closing a TCP connection). This flag releases the connection resources. However, host A can continue to receive data as long as the SYN sequence numbers of transmitted packets from host B are lower than the packet segment containing the set FIN flag

GRATIS EXAM
Free Practice Exams
http://www.gratisexam.com/

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 209
When setting up a wireless network, an administrator enters a pre-shared key for security. Which of the following is true?

A. The key entered is a symmetric key used to encrypt the wireless data.
B. The key entered is a hash that is used to prove the integrity of the wireless data.
C. The key entered is based on the Diffie-Hellman method.
D. The key is an RSA key used to encrypt the wireless data.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 210
Which of the following defines the role of a root Certificate Authority (CA) in a Public Key Infrastructure (PKI)?

A. The root CA is the recovery agent used to encrypt data when a user's certificate is lost.
B. The root CA stores the user's hash value for safekeeping.
C. The CA is the trusted root that issues certificates.
D. The root CA is used to encrypt email messages to prevent unintended disclosure of data.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 211

Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results?
TCP port 21 no response TCP port 22 no response TCP port 23 Time-to- live exceeded.

A. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host.
B. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server.
C. The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall.
D. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 212
A security engineer has been asked to deploy a secure remote access solution that will allow employees to connect to the company's internal network. Which of the following can be implemented to minimize the opportunity for the man-in-the-middle attack to occur?

A. SSL
B. Mutual authentication
C. IPSec
D. Static IP addresses

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 213
Using a swipe code is one way to increase mobile device security

A. True
B. False

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 214
A rooted Android device is usually less secure than an unrooted Android device. True or false?

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 215
Windows Phone 8 devices boot with Secure UEFI. True or false?

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 216
True or False: it is important to assess end-user security awareness on mobile devices.

A. True
B. False

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 217
Which devices are causing difficulty for security administrators in the workplace to maintain secure networks?

A. copiers
B. laptops
C. scanners
D. Employees' personal devices

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 218
A jailbroken iOS device is usually less secure than an unjailbroken iOS device. True or false?

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 219
It is common for buffer overflows to occur in the heap memory space. Application dynamically allocates heap memory as needed through a function. This function is called what?

A. strncopy()
B. strprint()

C. strcopy()
D. malloc()

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 220
What technique is used to ensure a buffer overflow will successfully execute the desired code by creating a padding in memory?

A. NOP sled
B. Heap sled
C. Heap spray

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 221
Which of the following programming languages are less vunerable to buffer overflow attacks? (select 3)

A. Ruby
B. C
C. C++
D. Assembly
E. Java
F. Python

Correct Answer: AEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 222
Which of these is present in BOTH Windows and Linux:

A. Program code
B. All of these
C. Stack segment
D. Heap address space

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 223
Which of the following programming languages is commonly associated with buffer overflows?

A. Flash
B. HTML
C. Crash
D. C and C++
E. Visual Basic

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 224
In the C++ Object-oriented programming language, which of these situations can result in a buffer overflow?

A. When an object returns a null (empty) value
B. When a program fails to compile properly
C. When a program returns an incorrect output

D. When the length of some input data is not correctly checked

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 225
Will buffer overflows lead to remote code executions.

A. True
B. False

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 226
which one of these BEST describes a Buffer Overflow attack that allows access to a remote system?

A. The attacker attempts to have the receiving server pass information to a back-end database from which it can compromise the stored information
B. The attacker overwhelms a system or application, causing a crash and bringing the server down to cause an outage
C. The attacker overwhelms a system or application, causing it to crash, and then redirects the memory address to read from a location holding the payload
D. The attacker attempts to have the receiving server run a payload using programming commonly found on web servers

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 227
From a security perspective, there is no problem in using the '>>' operator.

A. True
B. False

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 228
What is considered to be a violation of memory safety?

A. HTML
B. Null Characters
C. C++
D. Programming language
E. Buffer Overrun

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 229
What technique is used to ensure a buffer overflow will successfully execute the desired code by creating a padding in memory?

A. NOP sled
B. Heap spray
C. Heap sled

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 230
Which programming language is the most likely to be susceptible to a buffer overflow attack?

A. Java
B. Python
C. C
D. C#

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 231
You are performing a penetration test. You achieved access via a buffer overflow exploit and you proceed to find interesting data, such as files with usernames and passwords. You find a hidden folder that has the administrators bank account password and login information for the administrators bitcoin account. What should you do?

A. Transfer money from the administrator's account to another account
B. Report immediately to the administrator
C. Do not transfer the money but steal the bitcoins
D. Do not report it immediately, continue the penetration test, and add it to the report submitted when testing is complete

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 232
As a countermeasure to buffer overflows, bounds checking should be performed.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 233
When performing a buffer overflow attack against a system protected by SafeSEH - If the canary is known, an attacker could potentially pass the canary check code by overwriting the canary with its known value, and controlling information with mismatched values.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 234
It is possible to prevent buffer overflows by adding bounds checking to all buffers.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 235
Which of the following are types of buffer overflow?

A. Heap-based
B. Stack-based
C. Both Stack-based and Heap-based

D. Dynamic-based

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 236
By manipulating a buffer overflow, an attacker can jump:

A. To a function in the program
B. To one of the program's libraries
C. To a buffer he/she has created
D. All of these

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 237
Buffer overflows can be used to perform DoS attacks. True or false?

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 238
StackGuard can use the value of "0" as the canary value even though it is easily guessed by the attacker.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 239
Which of these attacks does bounds checking prevent:

A. SQL injection
B. DoS
C. Buffer overflow
D. Memory overflow

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 240
Canaries are known values that are placed between a buffer and control data on the stack to monitor buffer overflows.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 241

Which of these should be avoided to prevent a buffer overflow:

A. streadd()
B. strcpy()
C. strcat()
D. All of these

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 242
Attackers may place a Null Operation (NOP) instruction code at the beginning of a string in the buffer overflow attack process. True or false?

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 243
In the case of C and C++ languages, there are no automatic bounds checks on buffers.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 244
Splint is a source code analyzer that is capable of detecting a _____

A. XSRF
B. XSS
C. Buffer overflow
D. SQL injection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 245
Stack buffer overflows are also known as _____.

A. Stack smashing
B. Address space layout randomization
C. Shell injection
D. NOP sled

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 246
Which of these is NOT a countermeasure against a buffer overflow attack?

A. All of the choices are countermeasures against a buffer overflow attack
B. Canary (security cookie)
C. Address space layout randomization
D. Setting the NX bit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 247
Which of these is the best defense against a buffer overflow attack?

A. Stack execute invalidation
B. Compiler tools
C. Write secure code
D. Dynamic runtime checks

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 248
Which of the following programming languages is not susceptible to a stack-based buffer overflow attack?

A. C++
B. C
C. Assembler
D. Java

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 249
It is possible to make the stack non-executable.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 250
What is the best way a designer can mitigate buffer overflow from occurring in their code? Choose all that apply.

A. Write code using boundary checks within the code.
B. Write code without boundary scans.
C. Write code that uses C++ and everything will be great, no worries.
D. Use a protocol robustness test to verify the code meets qualifications for proper boundary and common key stroke entries.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 251
What's stack smashing?

A. It's when code is executed from a default heap.
B. It's when an attacker gets to a stack after they're done with the pumpkins.
C. A buffer overflow that overwrites the return address
D. The input of No Operation instruction code in a string

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 252
In StackGuard, whenever a function is called, code is added that pushes a small value called a ___ value over to the stack.

A. Stackgap
B. Runtime bound checkers
C. Canary
D. CRED

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 253
Which of these functions are vulnerable to buffer overflows?

A. gets
B. sprintf
C. strcpy
D. All of these

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 254
Splint is a source code analyzer that is capable of detecting a _____

A. XSRF
B. XSS
C. Buffer overflow
D. SQL injection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 255
Which of these is the best defense against a buffer overflow attack?

A. Dynamic runtime checks
B. Stack execute invalidation
C. Compiler tools
D. Write secure code

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 256
What is the best way a designer can mitigate buffer overflow from occurring in their code? Choose all that apply.

A. Use a protocol robustness test to verify the code meets qualifications for proper boundary and common key stroke entries.
B. Write code without boundary scans.
C. Write code that uses C++ and everything will be great, no worries.
D. Write code using boundary checks within the code.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 257

What's stack smashing?

A. The input of No Operation instruction code in a string
B. A buffer overflow that overwrites the return address
C. It's when code is executed from a default heap.
D. It's when an attacker gets to a stack after they're done with the pumpkins.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 258
Which of the following languages are the primary targets of cross-site scripting? (Choose two.)

A. HTML
B. SQL
C. XSLT
D. Javascript

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 259
What does Cross-Site Scripting allow an attacker to do to a computer system?

A. Defend themselves
B. Call people
C. Agree with policies
D. Delete information
E. Inject script into web pages

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 260
An effective countermeasure for Server Side Includes (SSI) is to use a preparser to filter out unauthorized SSI lines before passing it to the host. True or false?

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

GRATIS EXAM
Free Practice Exams
http://www.gratisexam.com/