

312-50v10 Dumps

Certified Ethical Hacker v10

<https://www.certleader.com/312-50v10-dumps.html>



NEW QUESTION 1

- (Exam Topic 1)

What does the -oX flag do in an Nmap scan?

- A. Perform an express scan
- B. Output the results in truncated format to the screen
- C. Perform an Xmas scan
- D. Output the results in XML format to a file

Answer: D

NEW QUESTION 2

- (Exam Topic 1)

What would you enter, if you wanted to perform a stealth scan using Nmap?

- A. nmap -sU
- B. nmap -sS
- C. nmap -sM
- D. nmap -sT

Answer: B

NEW QUESTION 3

- (Exam Topic 1)

The Payment Card Industry Data Security Standard (PCI DSS) contains six different categories of control objectives. Each objective contains one or more requirements, which must be followed in order to achieve compliance. Which of the following requirements would best fit under the objective, "Implement strong access control measures"?

- A. Regularly test security systems and processes.
- B. Encrypt transmission of cardholder data across open, public networks.
- C. Assign a unique ID to each person with computer access.
- D. Use and regularly update anti-virus software on all systems commonly affected by malware.

Answer: C

NEW QUESTION 4

- (Exam Topic 1)

Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occurring during non-business hours. After further examination of all login activities, it is noticed that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem realizes the system time on the Linux server is wrong by more than twelve hours. What protocol used on Linux servers to synchronize the time has stopped working?

- A. Time Keeper
- B. NTP
- C. PPP
- D. OSPP

Answer: B

NEW QUESTION 5

- (Exam Topic 1)

Which of the following cryptography attack is an understatement for the extraction of cryptographic secrets (the password to an encrypted file) from a person by a coercion or torture?

- A. Chosen-Cipher text Attack
- B. Ciphertext-only Attack
- C. Timing Attack
- D. Rubber Hose Attack

Answer: D

NEW QUESTION 6

- (Exam Topic 1)

Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

- A. Omnidirectional antenna
- B. Dipole antenna
- C. Yagi antenna
- D. Parabolic grid antenna

Answer: C

NEW QUESTION 7

- (Exam Topic 1)

Vlady works in a fishing company where the majority of the employees have very little understanding of IT let alone IT Security. Several information security issues

that Vlady often found includes, employees sharing password, writing his/her password on a post it note and stick it to his/her desk, leaving the computer unlocked, didn't log out from emails or other social media accounts, and etc.

After discussing with his boss, Vlady decided to make some changes to improve the security environment in his company. The first thing that Vlady wanted to do is to make the employees understand the importance of keeping confidential information, such as password, a secret and they should not share it with other persons. Which of the following steps should be the first thing that Vlady should do to make the employees in his company understand to importance of keeping confidential information a secret?

- A. Warning to those who write password on a post it note and put it on his/her desk
- B. Developing a strict information security policy
- C. Information security awareness training
- D. Conducting a one to one discussion with the other employees about the importance of information security

Answer: A

NEW QUESTION 8

- (Exam Topic 1)

Which of the below hashing functions are not recommended for use?

- A. SHA-1.ECC
- B. MD5, SHA-1
- C. SHA-2. SHA-3
- D. MD5. SHA-5

Answer: A

NEW QUESTION 9

- (Exam Topic 1)

If an attacker uses the command `SELECT*FROM user WHERE name = 'x' AND userid IS NULL; --'`; which type of SQL injection attack is the attacker performing?

- A. End of Line Comment
- B. UNION SQL Injection
- C. Illegal/Logically Incorrect Query
- D. Tautology

Answer: D

NEW QUESTION 10

- (Exam Topic 1)

Security Policy is a definition of what it means to be secure for a system, organization or other entity. For Information Technologies, there are sub-policies like Computer Security Policy, Information Protection Policy, Information Security Policy, network Security Policy, Physical Security Policy, Remote Access Policy, and User Account Policy.

What is the main theme of the sub-policies for Information Technologies?

- A. Availability, Non-repudiation, Confidentiality
- B. Authenticity, Integrity, Non-repudiation
- C. Confidentiality, Integrity, Availability
- D. Authenticity, Confidentiality, Integrity

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

Assume a business-crucial web-site of some company that is used to sell handsets to the customers worldwide. All the developed components are reviewed by the security team on a monthly basis. In order to drive business further, the web-site developers decided to add some 3rd party marketing tools on it. The tools are written in JavaScript and can track the customer's activity on the site. These tools are located on the servers of the marketing company.

What is the main security risk associated with this scenario?

- A. External script contents could be maliciously modified without the security team knowledge
- B. External scripts have direct access to the company servers and can steal the data from there
- C. There is no risk at all as the marketing services are trustworthy
- D. External scripts increase the outbound company data traffic which leads greater financial losses

Answer: A

NEW QUESTION 11

- (Exam Topic 1)

Code injection is a form of attack in which a malicious user:

- A. Inserts text into a data field that gets interpreted as code
- B. Gets the server to execute arbitrary code using a buffer overflow
- C. Inserts additional code into the JavaScript running in the browser
- D. Gains access to the codebase on the server and inserts new code

Answer: A

NEW QUESTION 16

- (Exam Topic 1)

Based on the below log, which of the following sentences are true?

Mar 1, 2016, 7:33:28 AM 10.240.250.23 – 54373 10.249.253.15 – 22 tcp_ip

- A. SSH communications are encrypted it's impossible to know who is the client or the server
- B. Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server
- C. Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server
- D. Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the server

Answer: C

NEW QUESTION 17

- (Exam Topic 1)

Darius is analysing IDS logs. During the investigation, he noticed that there was nothing suspicious found and an alert was triggered on normal web application traffic. He can mark this alert as:

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

Answer: A

NEW QUESTION 20

- (Exam Topic 1)

Which of the following scanning method splits the TCP header into several packets and makes it difficult for packet filters to detect the purpose of the packet?

- A. ICMP Echo scanning
- B. SYN/FIN scanning using IP fragments
- C. ACK flag probe scanning
- D. IPID scanning

Answer: B

NEW QUESTION 21

- (Exam Topic 1)

Which of the following attacks exploits web age vulnerabilities that allow an attacker to force an unsuspecting user's browser to send malicious requests they did not intend?

- A. Command Injection Attacks
- B. File Injection Attack
- C. Cross-Site Request Forgery (CSRF)
- D. Hidden Field Manipulation Attack

Answer: C

NEW QUESTION 22

- (Exam Topic 1)

Which of the following DoS tools is used to attack target web applications by starvation of available sessions on the web server?

The tool keeps sessions at halt using never-ending POST transmissions and sending an arbitrarily large content-length header value.

- A. My Doom
- B. Astacheldraht
- C. R-U-Dead-Yet?(RUDY)
- D. LOIC

Answer: C

NEW QUESTION 27

- (Exam Topic 1)

Which is the first step followed by Vulnerability Scanners for scanning a network?

- A. TCP/UDP Port scanning
- B. Firewall detection
- C. OS Detection
- D. Checking if the remote host is alive

Answer: D

NEW QUESTION 30

- (Exam Topic 1)

You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise in order to evade IDS?

- A. nmap -A - Pn
- B. nmap -sP -p-65535-T5
- C. nmap -sT -O -T0

D. nmap -A --host-timeout 99-T1

Answer: C

NEW QUESTION 33

- (Exam Topic 1)

DHCP snooping is a great solution to prevent rogue DHCP servers on your network. Which security feature on switches leverages the DHCP snooping database to help prevent man-in-the-middle attacks?

- A. Port security
- B. A Layer 2 Attack Prevention Protocol (LAPP)
- C. Dynamic ARP inspection (DAI)
- D. Spanning tree

Answer: C

NEW QUESTION 38

- (Exam Topic 1)

You are looking for SQL injection vulnerability by sending a special character to web applications. Which of the following is the most useful for quick validation?

- A. Double quotation
- B. Backslash
- C. Semicolon
- D. Single quotation

Answer: D

NEW QUESTION 42

- (Exam Topic 1)

Which of the following Secure Hashing Algorithm (SHA) produces a 160-bit digest from a message with a maximum length of (264-1) bits and resembles the MD5 algorithm?

- A. SHA-2
- B. SHA-3
- C. SHA-1
- D. SHA-0

Answer: C

NEW QUESTION 44

- (Exam Topic 1)

You are working as a Security Analyst in a company XYZ that owns the whole subnet range of 23.0.0.0/8 and 192.168.0.0/8.

While monitoring the data, you find a high number of outbound connections. You see that IP's owned by XYZ (Internal) and private IP's are communicating to a Single Public IP. Therefore, the Internal IP's are sending data to the Public IP.

After further analysis, you find out that this Public IP is a blacklisted IP, and the internal communicating devices are compromised.

What kind of attack does the above scenario depict?

- A. Botnet Attack
- B. Spear Phishing Attack
- C. Advanced Persistent Threats
- D. Rootkit Attack

Answer: A

NEW QUESTION 46

- (Exam Topic 1)

What is the main security service a cryptographic hash provides?

- A. Integrity and ease of computation
- B. Message authentication and collision resistance
- C. Integrity and collision resistance
- D. Integrity and computational in-feasibility

Answer: D

NEW QUESTION 47

- (Exam Topic 1)

Which protocol is used for setting up secure channels between two devices, typically in VPNs?

- A. PPP
- B. IPSEC
- C. PEM
- D. SET

Answer: B

NEW QUESTION 50

- (Exam Topic 1)

Which of the following provides a security professional with most information about the system's security posture?

- A. Wardriving, warchalking, social engineering
- B. Social engineering, company site browsing, tailgating
- C. Phishing, spamming, sending trojans
- D. Port scanning, banner grabbing, service identification

Answer: D

NEW QUESTION 53

- (Exam Topic 1)

When a security analyst prepares for the formal security assessment - what of the following should be done in order to determine inconsistencies in the secure assets database and verify that system is compliant to the minimum security baseline?

- A. Data items and vulnerability scanning
- B. Interviewing employees and network engineers
- C. Reviewing the firewalls configuration
- D. Source code review

Answer: A

NEW QUESTION 55

- (Exam Topic 1)

You are monitoring the network of your organizations. You notice that: Which of the following solution will you suggest?

- A. Block the Blacklist IP's @ Firewall
- B. Update the Latest Signatures on your IDS/IPS
- C. Clean the Malware which are trying to Communicate with the External Blacklist IP's
- D. Both B and C

Answer: D

NEW QUESTION 56

- (Exam Topic 1)

Trinity needs to scan all hosts on a /16 network for TCP port 445 only. What is the fastest way she can accomplish this with Nmap? Stealth is not a concern.

- A. `nmap -sn -sF 10.1.0.0/16 445`
- B. `nmap -p 445 -n -T4 --open 10.1.0.0/16`
- C. `nmap -s 445 -sU -T5 10.1.0.0/16`
- D. `nmap -p 445 --max -Pn 10.1.0.0/16`

Answer: B

NEW QUESTION 61

- (Exam Topic 1)

DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed.

What command is used to determine if the entry is present in DNS cache?

- A. `nslookup -fullrecursive update.antivirus.com`
- B. `dnsnoping -rt update.antivirus.com`
- C. `nslookup -norecursive update.antivirus.com`
- D. `dns --snoop update.antivirus.com`

Answer: C

NEW QUESTION 65

- (Exam Topic 1)

Firewalls are the software or hardware systems that are able to control and monitor the traffic coming in and out the target network based on pre-defined set of rules.

Which of the following types of firewalls can protect against SQL injection attacks?

- A. Data-driven firewall
- B. Stateful firewall
- C. Packet firewall
- D. Web application firewall

Answer: D

NEW QUESTION 66

- (Exam Topic 1)

Which one of the following Google advanced search operators allows an attacker to restrict the results to those websites in the given domain?

- A. `[cache:]`
- B. `[site:]`

- C. [inurl:]
- D. [link:]

Answer: B

NEW QUESTION 71

- (Exam Topic 1)

Why containers are less secure than virtual machines?

- A. Host OS on containers has a larger surface attack.
- B. Containers may fill disk space of the host.
- C. A compromised container may cause a CPU starvation of the host.
- D. Containers are attached to the same virtual network.

Answer: A

NEW QUESTION 75

- (Exam Topic 1)

What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?

- A. Symmetric algorithms such as AES provide a failsafe when asymmetric methods fail.
- B. Asymmetric cryptography is computationally expensive in comparison.
- C. However, it is well-suited to securely negotiate keys for use with symmetric cryptography.
- D. Symmetric encryption allows the server to securely transmit the session keys out-of-band.
- E. Supporting both types of algorithms allows less-powerful devices such as mobile phones to use symmetric encryption instead.

Answer: D

NEW QUESTION 77

- (Exam Topic 1)

Which of the following types of jailbreaking allows user-level access but does not allow iBoot-level access?

- A. Bootrom Exploit
- B. iBoot Exploit
- C. Sandbox Exploit
- D. Userland Exploit

Answer: D

NEW QUESTION 82

- (Exam Topic 1)

An attacker, using a rogue wireless AP, performed a MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections. When users accessed any page, the applet ran and exploited many machines. Which one of the following tools the hacker probably used to inject HTML code?

- A. Wireshark
- B. Ettercap
- C. Aircrack-ng
- D. Tcpdump

Answer: B

NEW QUESTION 84

- (Exam Topic 1)

Email is transmitted across the Internet using the Simple Mail Transport Protocol. SMTP does not encrypt email, leaving the information in the message vulnerable to being read by an unauthorized person. SMTP can upgrade a connection between two mail servers to use TLS. Email transmitted by SMTP over TLS is encrypted. What is the name of the command used by SMTP to transmit email over TLS?

- A. OPPORTUNISTIC TLS STARTTLS
- B. FORCETLS
- C. UPGRADE TLS

Answer: B

NEW QUESTION 89

- (Exam Topic 1)

You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity, what tool would you most likely select?

- A. Nmap
- B. Cain & Abel
- C. Nessus
- D. Snort

Answer: D

NEW QUESTION 94

- (Exam Topic 1)

Why should the security analyst disable/remove unnecessary ISAPI filters?

- A. To defend against social engineering attacks
- B. To defend against webserver attacks
- C. To defend against jailbreaking
- D. To defend against wireless attacks

Answer: B

NEW QUESTION 96

- (Exam Topic 1)

A virus that attempts to install itself inside the file it is infecting is called?

- A. Tunneling virus
- B. Cavity virus
- C. Polymorphic virus
- D. Stealth virus

Answer: B

NEW QUESTION 100

- (Exam Topic 1)

In which of the following password protection technique, random strings of characters are added to the password before calculating their hashes?

- A. Keyed Hashing
- B. Key Stretching
- C. Salting
- D. Double Hashing

Answer: C

NEW QUESTION 102

- (Exam Topic 1)

Identify the UDP port that Network Time Protocol (NTP) uses as its primary means of communication?

- A. 123
- B. 161
- C. 69
- D. 113

Answer: A

NEW QUESTION 105

- (Exam Topic 1)

Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students. He identified this when the IDS alerted for malware activities in the network. What should Bob do to avoid this problem?

- A. Disable unused ports in the switches
- B. Separate students in a different VLAN
- C. Use the 802.1x protocol
- D. Ask students to use the wireless network

Answer: C

NEW QUESTION 109

- (Exam Topic 1)

If you want only to scan fewer ports than the default scan using Nmap tool, which option would you use?

- A. -sP
- B. -P
- C. -r
- D. -F

Answer: B

NEW QUESTION 112

- (Exam Topic 1)

Which of the following statements is TRUE?

- A. Sniffers operate on Layer 2 of the OSI model
- B. Sniffers operate on Layer 3 of the OSI model
- C. Sniffers operate on both Layer 2 & Layer 3 of the OSI model.
- D. Sniffers operate on the Layer 1 of the OSI model.

Answer: A

NEW QUESTION 114

- (Exam Topic 1)

In the field of cryptanalysis, what is meant by a "rubber-hose" attack?

- A. Attempting to decrypt cipher text by making logical assumptions about the contents of the original plain text.
- B. Extraction of cryptographic secrets through coercion or torture.
- C. Forcing the targeted key stream through a hardware-accelerated device such as an ASIC.
- D. A backdoor placed into a cryptographic algorithm by its creator.

Answer: B

NEW QUESTION 117

- (Exam Topic 1)

A pen tester is configuring a Windows laptop for a test. In setting up Wireshark, what driver and library are required to allow the NIC to work in promiscuous mode?

- A. Libpcap
- B. Awinpcap
- C. Winprom
- D. Winpcap

Answer: D

NEW QUESTION 121

- (Exam Topic 1)

These hackers have limited or no training and know how to use only basic techniques or tools. What kind of hackers are we talking about?

- A. Black-Hat Hackers A
- B. Script Kiddies
- C. White-Hat Hackers
- D. Gray-Hat Hacker

Answer: C

NEW QUESTION 124

- (Exam Topic 1)

Which of the following options represents a conceptual characteristic of an anomaly-based IDS over a signature-based IDS?

- A. Produces less false positives
- B. Can identify unknown attacks
- C. Requires vendor updates for a new threat
- D. Cannot deal with encrypted network traffic

Answer: B

NEW QUESTION 126

- (Exam Topic 1)

A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wire shark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?

- A. tcp.port != 21
- B. tcp.port = 23
- C. tcp.port ==21
- D. tcp.port ==21 || tcp.port ==22

Answer: D

NEW QUESTION 131

- (Exam Topic 1)

Cross-site request forgery involves:

- A. A request sent by a malicious user from a browser to a server
- B. Modification of a request by a proxy between client and server
- C. A browser making a request to a server without the user's knowledge
- D. A server making a request to another server without the user's knowledge

Answer: C

NEW QUESTION 132

- (Exam Topic 1)

During the process of encryption and decryption, what keys are shared? During the process of encryption and decryption, what keys are shared?

- A. Private keys
- B. User passwords
- C. Public keys

D. Public and private keys

Answer: C

NEW QUESTION 133

- (Exam Topic 1)

A hacker named Jack is trying to compromise a bank's computer system. He needs to know the operating system of that computer to launch further attacks. What process would help him?

- A. Banner Grabbing
- B. IDLE/IPID Scanning
- C. SSDP Scanning
- D. UDP Scanning

Answer: A

NEW QUESTION 136

- (Exam Topic 1)

In Wireshark, the packet bytes panes show the data of the current packet in which format?

- A. Decimal
- B. ASCII only
- C. Binary
- D. Hexadecimal

Answer: D

NEW QUESTION 141

- (Exam Topic 1)

What type of vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?

- A. Cross-site request forgery
- B. Cross-site scripting
- C. Session hijacking
- D. Server side request forgery

Answer: A

NEW QUESTION 145

- (Exam Topic 1)

Bob finished a C programming course and created a small C application to monitor the network traffic and produce alerts when any origin sends "many" IP packets, based on the average number of packets sent by all origins and using some thresholds.

In concept, the solution developed by Bob is actually:

- A. Just a network monitoring tool
- B. A signature-based IDS
- C. A hybrid IDS
- D. A behavior-based IDS

Answer: A

NEW QUESTION 146

- (Exam Topic 2)

Which of the following processes evaluates the adherence of an organization to its stated security policy?

- A. Vulnerability assessment
- B. Penetration testing
- C. Risk assessment
- D. Security auditing

Answer: D

NEW QUESTION 147

- (Exam Topic 2)

The precaution of prohibiting employees from bringing personal computing devices into a facility is what type of security control?

- A. Physical
- B. Procedural
- C. Technical
- D. Compliance

Answer: B

NEW QUESTION 149

- (Exam Topic 2)

Which of the following tools will scan a network to perform vulnerability checks and compliance auditing?

- A. NMAP
- B. Metasploit
- C. Nessus
- D. BeEF

Answer: C

NEW QUESTION 151

- (Exam Topic 2)

Which tool would be used to collect wireless packet data?

- A. NetStumbler
- B. John the Ripper
- C. Nessus
- D. Netcat

Answer: A

NEW QUESTION 155

- (Exam Topic 2)

Which of the following open source tools would be the best choice to scan a network for potential targets?

- A. NMAP
- B. NIKTO
- C. CAIN
- D. John the Ripper

Answer: A

NEW QUESTION 158

- (Exam Topic 2)

Which of the following is an application that requires a host application for replication?

- A. Micro
- B. Worm
- C. Trojan
- D. Virus

Answer: D

Explanation:

Computer viruses infect a variety of different subsystems on their hosts. A computer virus is a malware that, when executed, replicates by reproducing itself or infecting other programs by modifying them. Infecting computer programs can include as well, data files, or the boot sector of the hard drive. When this replication succeeds, the affected areas are then said to be "infected".

References: https://en.wikipedia.org/wiki/Computer_virus

NEW QUESTION 163

- (Exam Topic 2)

A tester has been hired to do a web application security test. The tester notices that the site is dynamic and must make use of a back end database. In order for the tester to see if SQL injection is possible, what is the first character that the tester should use to attempt breaking a valid SQL request?

- A. Semicolon
- B. Single quote
- C. Exclamation mark
- D. Double quote

Answer: B

NEW QUESTION 164

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 169

- (Exam Topic 2)

A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed. Which security policy must the security analyst check to see if dial-out modems are allowed?

- A. Firewall-management policy

- B. Acceptable-use policy
- C. Remote-access policy
- D. Permissive policy

Answer: C

NEW QUESTION 174

- (Exam Topic 2)

Which type of access control is used on a router or firewall to limit network activity?

- A. Mandatory
- B. Discretionary
- C. Rule-based
- D. Role-based

Answer: C

NEW QUESTION 177

- (Exam Topic 2)

A developer for a company is tasked with creating a program that will allow customers to update their billing and shipping information. The billing address field used is limited to 50 characters. What pseudo code would the developer use to avoid a buffer overflow attack on the billing address field?

- A. if (billingAddress = 50) {update field} else exit
- B. if (billingAddress != 50) {update field} else exit
- C. if (billingAddress >= 50) {update field} else exit
- D. if (billingAddress <= 50) {update field} else exit

Answer: D

NEW QUESTION 180

- (Exam Topic 2)

Which of the following is a hashing algorithm?

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

Answer: A

NEW QUESTION 181

- (Exam Topic 2)

Which protocol and port number might be needed in order to send log messages to a log analysis tool that resides behind a firewall?

- A. UDP 123
- B. UDP 541
- C. UDP 514
- D. UDP 415

Answer: C

NEW QUESTION 184

- (Exam Topic 2)

During a wireless penetration test, a tester detects an access point using WPA2 encryption. Which of the following attacks should be used to obtain the key?

- A. The tester must capture the WPA2 authentication handshake and then crack it.
- B. The tester must use the tool inSSIDer to crack it using the ESSID of the network.
- C. The tester cannot crack WPA2 because it is in full compliance with the IEEE 802.11i standard.
- D. The tester must change the MAC address of the wireless network card and then use the AirTraf tool to obtain the key.

Answer: A

NEW QUESTION 185

- (Exam Topic 2)

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

Answer: C

NEW QUESTION 187

- (Exam Topic 2)

What is the main disadvantage of the scripting languages as opposed to compiled programming languages?

- A. Scripting languages are hard to learn.
- B. Scripting languages are not object-oriented.
- C. Scripting languages cannot be used to create graphical user interfaces.
- D. Scripting languages are slower because they require an interpreter to run the code.

Answer: D

NEW QUESTION 191

- (Exam Topic 2)

A hacker, who posed as a heating and air conditioning specialist, was able to install a sniffer program in a switched environment network. Which attack could the hacker use to sniff all of the packets in the network?

- A. Fraggles
- B. MAC Flood
- C. Smurf
- D. Tear Drop

Answer: B

NEW QUESTION 195

- (Exam Topic 2)

A botnet can be managed through which of the following?

- A. IRC
- B. E-Mail
- C. LinkedIn and Facebook
- D. A vulnerable FTP server

Answer: A

NEW QUESTION 199

- (Exam Topic 2)

Which type of intrusion detection system can monitor and alert on attacks, but cannot stop them?

- A. Detective
- B. Passive
- C. Intuitive
- D. Reactive

Answer: B

NEW QUESTION 202

- (Exam Topic 2)

Which of the following lists are valid data-gathering activities associated with a risk assessment?

- A. Threat identification, vulnerability identification, control analysis
- B. Threat identification, response identification, mitigation identification
- C. Attack profile, defense profile, loss profile
- D. System profile, vulnerability identification, security determination

Answer: A

NEW QUESTION 203

- (Exam Topic 2)

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

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

Answer: B

Explanation:

A boot sector virus is a computer virus that infects a storage device's master boot record (MBR). The virus moves the boot sector to another location on the hard drive.

References: <https://www.techopedia.com/definition/26655/boot-sector-virus>

NEW QUESTION 208

- (Exam Topic 2)

When an alert rule is matched in a network-based IDS like snort, the IDS does which of the following?

- A. Drops the packet and moves on to the next one
- B. Continues to evaluate the packet until all rules are checked

- C. Stops checking rules, sends an alert, and lets the packet continue
- D. Blocks the connection with the source IP address in the packet

Answer: B

NEW QUESTION 209

- (Exam Topic 2)

A hacker is attempting to use nslookup to query Domain Name Service (DNS). The hacker uses the nslookup interactive mode for the search. Which command should the hacker type into the command shell to request the appropriate records?

- A. Locate type=ns
- B. Request type=ns
- C. Set type=ns
- D. Transfer type=ns

Answer: C

NEW QUESTION 213

- (Exam Topic 2)

A company has publicly hosted web applications and an internal Intranet protected by a firewall. Which technique will help protect against enumeration?

- A. Reject all invalid email received via SMTP.
- B. Allow full DNS zone transfers.
- C. Remove A records for internal hosts.
- D. Enable null session pipes.

Answer: C

NEW QUESTION 217

- (Exam Topic 2)

If the final set of security controls does not eliminate all risk in a system, what could be done next?

- A. Continue to apply controls until there is zero risk.
- B. Ignore any remaining risk.
- C. If the residual risk is low enough, it can be accepted.
- D. Remove current controls since they are not completely effective.

Answer: C

NEW QUESTION 220

- (Exam Topic 2)

Which NMAP command combination would let a tester scan every TCP port from a class C network that is blocking ICMP with fingerprinting and service detection?

- A. NMAP -PN -A -O -sS 192.168.2.0/24
- B. NMAP -P0 -A -O -p1-65535 192.168.0/24
- C. NMAP -P0 -A -sT -p0-65535 192.168.0/16
- D. NMAP -PN -O -sS -p 1-1024 192.168.0/8

Answer: B

NEW QUESTION 224

- (Exam Topic 2)

A company is using Windows Server 2003 for its Active Directory (AD). What is the most efficient way to crack the passwords for the AD users?

- A. Perform a dictionary attack.
- B. Perform a brute force attack.
- C. Perform an attack with a rainbow table.
- D. Perform a hybrid attack.

Answer: C

NEW QUESTION 227

- (Exam Topic 2)

What is the best defense against privilege escalation vulnerability?

- A. Patch systems regularly and upgrade interactive login privileges at the system administrator level.
- B. Run administrator and applications on least privileges and use a content registry for tracking.
- C. Run services with least privileged accounts and implement multi-factor authentication and authorization.
- D. Review user roles and administrator privileges for maximum utilization of automation services.

Answer: C

NEW QUESTION 232

- (Exam Topic 2)

How is sniffing broadly categorized?

- A. Active and passive
- B. Broadcast and unicast
- C. Unmanaged and managed
- D. Filtered and unfiltered

Answer: A

NEW QUESTION 237

- (Exam Topic 2)

Which tool can be used to silently copy files from USB devices?

- A. USB Grabber
- B. USB Dumper
- C. USB Sniffer
- D. USB Snoopy

Answer: B

NEW QUESTION 240

- (Exam Topic 2)

Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Which of the following is the correct bit size of the Diffie-Hellman (DH) group 5?

- A. 768 bit key
- B. 1025 bit key
- C. 1536 bit key
- D. 2048 bit key

Answer: C

NEW QUESTION 242

- (Exam Topic 2)

What type of OS fingerprinting technique sends specially crafted packets to the remote OS and analyzes the received response?

- A. Passive
- B. Reflective
- C. Active
- D. Distributive

Answer: C

NEW QUESTION 244

- (Exam Topic 2)

Which type of scan measures a person's external features through a digital video camera?

- A. Iris scan
- B. Retinal scan
- C. Facial recognition scan
- D. Signature kinetics scan

Answer: C

NEW QUESTION 245

- (Exam Topic 2)

Which of the following is a strong post designed to stop a car?

- A. Gate
- B. Fence
- C. Bollard
- D. Reinforced rebar

Answer: C

NEW QUESTION 248

- (Exam Topic 2)

An NMAP scan of a server shows port 25 is open. What risk could this pose?

- A. Open printer sharing
- B. Web portal data leak
- C. Clear text authentication
- D. Active mail relay

Answer: D

NEW QUESTION 250

- (Exam Topic 2)

To send a PGP encrypted message, which piece of information from the recipient must the sender have before encrypting the message?

- A. Recipient's private key
- B. Recipient's public key
- C. Master encryption key
- D. Sender's public key

Answer: B

NEW QUESTION 253

- (Exam Topic 2)

Which of the following conditions must be given to allow a tester to exploit a Cross-Site Request Forgery (CSRF) vulnerable web application?

- A. The victim user must open the malicious link with an Internet Explorer prior to version 8.
- B. The session cookies generated by the application do not have the HttpOnly flag set.
- C. The victim user must open the malicious link with a Firefox prior to version 3.
- D. The web application should not use random tokens.

Answer: D

NEW QUESTION 257

- (Exam Topic 2)

Which of the following does proper basic configuration of snort as a network intrusion detection system require?

- A. Limit the packets captured to the snort configuration file.
- B. Capture every packet on the network segment.
- C. Limit the packets captured to a single segment.
- D. Limit the packets captured to the /var/log/snort directory.

Answer: A

NEW QUESTION 259

- (Exam Topic 2)

A penetration tester is attempting to scan an internal corporate network from the internet without alerting the border sensor. Which is the most efficient technique should the tester consider using?

- A. Spoofing an IP address
- B. Tunneling scan over SSH
- C. Tunneling over high port numbers
- D. Scanning using fragmented IP packets

Answer: B

NEW QUESTION 260

- (Exam Topic 2)

What results will the following command yield: 'NMAP -sS -O -p 123-153 192.168.100.3'?

- A. A stealth scan, opening port 123 and 153
- B. A stealth scan, checking open ports 123 to 153
- C. A stealth scan, checking all open ports excluding ports 123 to 153
- D. A stealth scan, determine operating system, and scanning ports 123 to 153

Answer: D

NEW QUESTION 265

- (Exam Topic 2)

John the Ripper is a technical assessment tool used to test the weakness of which of the following?

- A. Usernames
- B. File permissions
- C. Firewall rulesets
- D. Passwords

Answer: D

NEW QUESTION 269

- (Exam Topic 2)

How can rainbow tables be defeated?

- A. Password salting
- B. Use of non-dictionary words
- C. All uppercase character passwords
- D. Lockout accounts under brute force password cracking attempts

Answer: A

NEW QUESTION 274

- (Exam Topic 2)

Bluetooth uses which digital modulation technique to exchange information between paired devices?

- A. PSK (phase-shift keying)
- B. FSK (frequency-shift keying)
- C. ASK (amplitude-shift keying)
- D. QAM (quadrature amplitude modulation)

Answer: A

Explanation:

Phase shift keying is the form of Bluetooth modulation used to enable the higher data rates achievable with Bluetooth 2 EDR (Enhanced Data Rate). Two forms of PSK are used: /4 DQPSK, and 8DPSK.

References:

<http://www.radio-electronics.com/info/wireless/bluetooth/radio-interface-modulation.php>

NEW QUESTION 277

- (Exam Topic 2)

Which command line switch would be used in NMAP to perform operating system detection?

- A. -OS
- B. -sO
- C. -sP
- D. -O

Answer: D

NEW QUESTION 281

- (Exam Topic 2)

Which of the following programming languages is most vulnerable to buffer overflow attacks?

- A. Perl
- B. C++
- C. Python
- D. Java

Answer: B

NEW QUESTION 286

- (Exam Topic 2)

A hacker searches in Google for filetype:pcf to find Cisco VPN config files. Those files may contain connectivity passwords that can be decoded with which of the following?

- A. Cupp
- B. Nessus
- C. Cain and Abel
- D. John The Ripper Pro

Answer: C

NEW QUESTION 287

- (Exam Topic 2)

An engineer is learning to write exploits in C++ and is using the exploit tool Backtrack. The engineer wants to compile the newest C++ exploit and name it calc.exe. Which command would the engineer use to accomplish this?

- A. g++ hackersExploit.cpp -o calc.exe
- B. g++ hackersExploit.py -o calc.exe
- C. g++ -i hackersExploit.pl -o calc.exe
- D. g++ --compile -i hackersExploit.cpp -o calc.exe

Answer: A

NEW QUESTION 289

- (Exam Topic 2)

Which of the following scanning tools is specifically designed to find potential exploits in Microsoft Windows products?

- A. Microsoft Security Baseline Analyzer
- B. Retina
- C. Core Impact
- D. Microsoft Baseline Security Analyzer

Answer: D

NEW QUESTION 292

- (Exam Topic 2)

Which solution can be used to emulate computer services, such as mail and ftp, and to capture information related to logins or actions?

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

Answer: B

NEW QUESTION 297

- (Exam Topic 2)

ICMP ping and ping sweeps are used to check for active systems and to check

- A. if ICMP ping traverses a firewall.
- B. the route that the ICMP ping took.
- C. the location of the switchport in relation to the ICMP ping.
- D. the number of hops an ICMP ping takes to reach a destination.

Answer: A

NEW QUESTION 300

- (Exam Topic 2)

A recently hired network security associate at a local bank was given the responsibility to perform daily scans of the internal network to look for unauthorized devices. The employee decides to write a script that will scan the network for unauthorized devices every morning at 5:00 am.

Which of the following programming languages would most likely be used?

- A. PHP
- B. C#
- C. Python
- D. ASP.NET

Answer: C

NEW QUESTION 305

- (Exam Topic 2)

What is the correct PCAP filter to capture all TCP traffic going to or from host 192.168.0.125 on port 25?

- A. tcp.src == 25 and ip.host == 192.168.0.125
- B. host 192.168.0.125:25
- C. port 25 and host 192.168.0.125
- D. tcp.port == 25 and ip.host == 192.168.0.125

Answer: D

NEW QUESTION 308

- (Exam Topic 2)

A penetration tester is hired to do a risk assessment of a company's DMZ. The rules of engagement states that the penetration test be done from an external IP address with no prior knowledge of the internal IT systems. What kind of test is being performed?

- A. white box
- B. grey box
- C. red box
- D. black box

Answer: D

NEW QUESTION 310

- (Exam Topic 2)

Which statement is TRUE regarding network firewalls preventing Web Application attacks?

- A. Network firewalls can prevent attacks because they can detect malicious HTTP traffic.
- B. Network firewalls cannot prevent attacks because ports 80 and 443 must be opened.
- C. Network firewalls can prevent attacks if they are properly configured.
- D. Network firewalls cannot prevent attacks because they are too complex to configure.

Answer: B

Explanation:

Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. To prevent Web Application attacks an Application layer firewall would be required.

References: [https://en.wikipedia.org/wiki/Firewall_\(computing\)#Network_layer_or_packet_filters](https://en.wikipedia.org/wiki/Firewall_(computing)#Network_layer_or_packet_filters)

NEW QUESTION 312

- (Exam Topic 2)

A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

- A. Perform a vulnerability scan of the system.
- B. Determine the impact of enabling the audit feature.
- C. Perform a cost/benefit analysis of the audit feature.
- D. Allocate funds for staffing of audit log review.

Answer: B

NEW QUESTION 316

- (Exam Topic 2)

Which of the following programs is usually targeted at Microsoft Office products?

- A. Polymorphic virus
- B. Multipart virus
- C. Macro virus
- D. Stealth virus

Answer: C

Explanation:

A macro virus is a virus that is written in a macro language: a programming language which is embedded inside a software application (e.g., word processors and spreadsheet applications). Some applications, such as Microsoft Office, allow macro programs to be embedded in documents such that the macros are run automatically when the document is opened, and this provides a distinct mechanism by which malicious computer instructions can spread.

References: https://en.wikipedia.org/wiki/Macro_virus

NEW QUESTION 320

- (Exam Topic 2)

What information should an IT system analysis provide to the risk assessor?

- A. Management buy-in
- B. Threat statement
- C. Security architecture
- D. Impact analysis

Answer: C

NEW QUESTION 324

- (Exam Topic 2)

A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the corporate network. What tool should the analyst use to perform a Blackjacking attack?

- A. Paros Proxy
- B. BBProxy
- C. BBCrack
- D. Blooover

Answer: B

Explanation:

Blackberry users warned of hacking tool threat.

Users have been warned that the security of Blackberry wireless e-mail devices is at risk due to the availability this week of a new hacking tool. Secure Computing Corporation said businesses that have installed Blackberry servers behind their gateway security devices could be vulnerable to a hacking attack from a tool call BBProxy.

References:

<http://www.computerweekly.com/news/2240062112/Technology-news-in-brief>

NEW QUESTION 329

- (Exam Topic 2)

Least privilege is a security concept that requires that a user is

- A. limited to those functions required to do the job.
- B. given root or administrative privileges.
- C. trusted to keep all data and access to that data under their sole control.
- D. given privileges equal to everyone else in the department.

Answer: A

NEW QUESTION 334

- (Exam Topic 2)

Which of the following parameters enables NMAP's operating system detection feature?

- A. NMAP -sV
- B. NMAP -oS
- C. NMAP -sR
- D. NMAP -O

Answer: D

NEW QUESTION 337

- (Exam Topic 2)

Which of the following is a symmetric cryptographic standard?

- A. DSA
- B. PKI
- C. RSA
- D. 3DES

Answer: D

NEW QUESTION 338

- (Exam Topic 2)

Which of the following settings enables Nessus to detect when it is sending too many packets and the network pipe is approaching capacity?

- A. Netstat WMI Scan
- B. Silent Dependencies
- C. Consider unscanned ports as closed
- D. Reduce parallel connections on congestion

Answer: D

NEW QUESTION 341

- (Exam Topic 2)

What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room?

- A. Set a BIOS password.
- B. Encrypt the data on the hard drive.
- C. Use a strong logon password to the operating system.
- D. Back up everything on the laptop and store the backup in a safe place.

Answer: B

NEW QUESTION 345

- (Exam Topic 2)

A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted.

Which cryptography attack is the student attempting?

- A. Man-in-the-middle attack
- B. Brute-force attack
- C. Dictionary attack
- D. Session hijacking

Answer: C

NEW QUESTION 347

- (Exam Topic 2)

What is the main advantage that a network-based IDS/IPS system has over a host-based solution?

- A. They do not use host system resources.
- B. They are placed at the boundary, allowing them to inspect all traffic.
- C. They are easier to install and configure.
- D. They will not interfere with user interfaces.

Answer: A

NEW QUESTION 350

- (Exam Topic 3)

Which vital role does the U.S. Computer Security Incident Response Team (CSIRT) provide?

- A. Incident response services to any user, company, government agency, or organization in partnership with the Department of Homeland Security
- B. Maintenance of the nation's Internet infrastructure, builds out new Internet infrastructure, and decommissions old Internet infrastructure
- C. Registration of critical penetration testing for the Department of Homeland Security and public and private sectors
- D. Measurement of key vulnerability assessments on behalf of the Department of Defense (DOD) and State Department, as well as private sectors

Answer: A

NEW QUESTION 355

- (Exam Topic 3)

A certified ethical hacker (CEH) is approached by a friend who believes her husband is cheating. She offers to pay to break into her husband's email account in order to find proof so she can take him to court. What is the ethical response?

- A. Say no; the friend is not the owner of the account.
- B. Say yes; the friend needs help to gather evidence.
- C. Say yes; do the job for free.

D. Say no; make sure that the friend knows the risk she's asking the CEH to take.

Answer: A

NEW QUESTION 356

- (Exam Topic 3)

An ethical hacker for a large security research firm performs penetration tests, vulnerability tests, and risk assessments. A friend recently started a company and asks the hacker to perform a penetration test and vulnerability assessment of the new company as a favor. What should the hacker's next step be before starting work on this job?

- A. Start by foot printing the network and mapping out a plan of attack.
- B. Ask the employer for authorization to perform the work outside the company.
- C. Begin the reconnaissance phase with passive information gathering and then move into active information gathering.
- D. Use social engineering techniques on the friend's employees to help identify areas that may be susceptible to attack.

Answer: B

NEW QUESTION 358

- (Exam Topic 3)

If an e-commerce site was put into a live environment and the programmers failed to remove the secret entry point that was used during the application development, what is this secret entry point known as?

- A. SDLC process
- B. Honey pot
- C. SQL injection
- D. Trap door

Answer: D

NEW QUESTION 363

- (Exam Topic 3)

The fundamental difference between symmetric and asymmetric key cryptographic systems is that symmetric key cryptography uses which of the following?

- A. Multiple keys for non-repudiation of bulk data
- B. Different keys on both ends of the transport medium
- C. Bulk encryption for data transmission over fiber
- D. The same key on each end of the transmission medium

Answer: D

NEW QUESTION 364

- (Exam Topic 3)

Which of the following network attacks relies on sending an abnormally large packet size that exceeds TCP/IP specifications?

- A. Ping of death
- B. SYN flooding
- C. TCP hijacking
- D. Smurf attack

Answer: A

NEW QUESTION 369

- (Exam Topic 3)

Which of the following is an advantage of utilizing security testing methodologies to conduct a security audit?

- A. They provide a repeatable framework.
- B. Anyone can run the command line scripts.
- C. They are available at low cost.
- D. They are subject to government regulation.

Answer: A

NEW QUESTION 371

- (Exam Topic 3)

For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. While using a digital signature, the message digest is encrypted with which key?

- A. Sender's public key
- B. Receiver's private key
- C. Receiver's public key
- D. Sender's private key

Answer: D

NEW QUESTION 372

- (Exam Topic 3)

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.

Answer: C

NEW QUESTION 376

- (Exam Topic 3)

An attacker has captured a target file that is encrypted with public key cryptography. Which of the attacks below is likely to be used to crack the target file?

- A. Timing attack
- B. Replay attack
- C. Memory trade-off attack
- D. Chosen plain-text attack

Answer: D

NEW QUESTION 379

- (Exam Topic 3)

Which initial procedure should an ethical hacker perform after being brought into an organization?

- A. Begin security testing.
- B. Turn over deliverables.
- C. Sign a formal contract with non-disclosure.
- D. Assess what the organization is trying to protect.

Answer: C

NEW QUESTION 380

- (Exam Topic 3)

Which of the following is a primary service of the U.S. Computer Security Incident Response Team (CSIRT)?

- A. CSIRT provides an incident response service to enable a reliable and trusted single point of contact for reporting computer security incidents worldwide.
- B. CSIRT provides a computer security surveillance service to supply a government with important intelligence information on individuals travelling abroad.
- C. CSIRT provides a penetration testing service to support exception reporting on incidents worldwide by individuals and multi-national corporations.
- D. CSIRT provides a vulnerability assessment service to assist law enforcement agencies with profiling an individual's property or company's asset.

Answer: A

NEW QUESTION 385

- (Exam Topic 3)

Employees in a company are no longer able to access Internet web sites on their computers. The network administrator is able to successfully ping IP address of web servers on the Internet and is able to open web sites by using an IP address in place of the URL. The administrator runs the nslookup command for www.eccouncil.org and receives an error message stating there is no response from the server. What should the administrator do next?

- A. Configure the firewall to allow traffic on TCP ports 53 and UDP port 53.
- B. Configure the firewall to allow traffic on TCP ports 80 and UDP port 443.
- C. Configure the firewall to allow traffic on TCP port 53.
- D. Configure the firewall to allow traffic on TCP port 8080.

Answer: A

NEW QUESTION 387

- (Exam Topic 3)

A Certificate Authority (CA) generates a key pair that will be used for encryption and decryption of email. The integrity of the encrypted email is dependent on the security of which of the following?

- A. Public key
- B. Private key
- C. Modulus length
- D. Email server certificate

Answer: B

NEW QUESTION 389

- (Exam Topic 3)

The intrusion detection system at a software development company suddenly generates multiple alerts regarding attacks against the company's external webserver, VPN concentrator, and DNS servers. What should the security team do to determine which alerts to check first?

- A. Investigate based on the maintenance schedule of the affected systems.
- B. Investigate based on the service level agreements of the systems.
- C. Investigate based on the potential effect of the incident.
- D. Investigate based on the order that the alerts arrived in.

Answer: C

NEW QUESTION 393

- (Exam Topic 3)

Which of the following network attacks takes advantage of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

- A. Teardrop
- B. SYN flood
- C. Smurf attack
- D. Ping of death

Answer: A

NEW QUESTION 396

- (Exam Topic 3)

How do employers protect assets with security policies pertaining to employee surveillance activities?

- A. Employers promote monitoring activities of employees as long as the employees demonstrate trustworthiness.
- B. Employers use informal verbal communication channels to explain employee monitoring activities to employees.
- C. Employers use network surveillance to monitor employee email traffic, network access, and to record employee keystrokes.
- D. Employers provide employees written statements that clearly discuss the boundaries of monitoring activities and consequences.

Answer: D

NEW QUESTION 401

- (Exam Topic 3)

Company A and Company B have just merged and each has its own Public Key Infrastructure (PKI). What must the Certificate Authorities (CAs) establish so that the private PKIs for Company A and Company B trust one another and each private PKI can validate digital certificates from the other company?

- A. Poly key exchange
- B. Cross certification
- C. Poly key reference
- D. Cross-site exchange

Answer: B

NEW QUESTION 403

- (Exam Topic 3)

An IT security engineer notices that the company's web server is currently being hacked. What should the engineer do next?

- A. Unplug the network connection on the company's web server.
- B. Determine the origin of the attack and launch a counterattack.
- C. Record as much information as possible from the attack.
- D. Perform a system restart on the company's web server.

Answer: C

NEW QUESTION 406

- (Exam Topic 3)

Which statement best describes a server type under an N-tier architecture?

- A. A group of servers at a specific layer
- B. A single server with a specific role
- C. A group of servers with a unique role
- D. A single server at a specific layer

Answer: C

NEW QUESTION 409

- (Exam Topic 3)

Which of the following items is unique to the N-tier architecture method of designing software applications?

- A. Application layers can be separated, allowing each layer to be upgraded independently from other layers.
- B. It is compatible with various databases including Access, Oracle, and SQL.
- C. Data security is tied into each layer and must be updated for all layers when any upgrade is performed.
- D. Application layers can be written in C, ASP.NET, or Delphi without any performance loss.

Answer: A

NEW QUESTION 413

- (Exam Topic 3)

What are the three types of compliance that the Open Source Security Testing Methodology Manual (OSSTMM) recognizes?

- A. Legal, performance, audit
- B. Audit, standards based, regulatory

- C. Contractual, regulatory, industry
- D. Legislative, contractual, standards based

Answer: D

NEW QUESTION 418

- (Exam Topic 3)

Which of the following can take an arbitrary length of input and produce a message digest output of 160 bit?

- A. SHA-1
- B. MD5
- C. HAVAL
- D. MD4

Answer: A

NEW QUESTION 421

- (Exam Topic 3)

Which type of security document is written with specific step-by-step details?

- A. Process
- B. Procedure
- C. Policy
- D. Paradigm

Answer: B

NEW QUESTION 426

- (Exam Topic 3)

A certified ethical hacker (CEH) completed a penetration test of the main headquarters of a company almost two months ago, but has yet to get paid. The customer is suffering from financial problems, and the CEH is worried that the company will go out of business and end up not paying. What actions should the CEH take?

- A. Threaten to publish the penetration test results if not paid.
- B. Follow proper legal procedures against the company to request payment.
- C. Tell other customers of the financial problems with payments from this company.
- D. Exploit some of the vulnerabilities found on the company webserver to deface it.

Answer: B

NEW QUESTION 428

- (Exam Topic 3)

A network security administrator is worried about potential man-in-the-middle attacks when users access a corporate web site from their workstations. Which of the following is the best remediation against this type of attack?

- A. Implementing server-side PKI certificates for all connections
- B. Mandating only client-side PKI certificates for all connections
- C. Requiring client and server PKI certificates for all connections
- D. Requiring strong authentication for all DNS queries

Answer: C

NEW QUESTION 432

- (Exam Topic 3)

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.

Answer: A

NEW QUESTION 436

- (Exam Topic 4)

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. Payment Card Industry (PCI)
- B. Center for Disease Control (CDC)
- C. Institute of Electrical and Electronics Engineers (IEEE)
- D. International Security Industry Organization (ISIO)

Answer: A

Explanation:

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB. The PCI DSS standards are very explicit about the requirements for the back end storage and access of PII (personally identifiable information).

References: https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

NEW QUESTION 441

- (Exam Topic 4)

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

Answer: A

Explanation:

Metagoofil is an information gathering tool designed for extracting metadata of public documents (pdf,doc,xls,ppt,docx,pptx,xlsx) belonging to a target company. Metagoofil will perform a search in Google to identify and download the documents to local disk and then will extract the metadata with different libraries like Hachoir, PdfMiner? and others. With the results it will generate a report with usernames, software versions and servers or machine names that will help Penetration testers in the information gathering phase.

References:

<http://www.edge-security.com/metagoofil.php>

NEW QUESTION 443

- (Exam Topic 4)

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

- A. Decline but, provide references.
- B. Share full reports, not redacted.
- C. Share full reports with redactions.
- D. Share reports, after NDA is signed.

Answer: A

Explanation:

Penetration tests data should not be disclosed to third parties.

NEW QUESTION 444

- (Exam Topic 4)

How does the Address Resolution Protocol (ARP) work?

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

Answer: A

Explanation:

When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address. The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it. A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

References:

<http://searchnetworking.techtarget.com/definition/Address-Resolution-Protocol-ARP>

NEW QUESTION 449

- (Exam Topic 4)

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==192.168.0.150
- B. tcp.srcport==514 && ip.src==192.168.0.99
- C. tcp.dstport==514 && ip.dst==192.168.0.0/16
- D. tcp.srcport==514 && ip.src==192.168.150

Answer: A

Explanation:

We need to configure destination port at destination ip. The destination ip is 192.168.0.150, where the kiwi syslog is installed.

References: <https://wiki.wireshark.org/DisplayFilters>

NEW QUESTION 452

- (Exam Topic 4)

> NMAP -sn 192.168.11.200-215

The NMAP command above performs which of the following?

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

Answer: A

Explanation:

NMAP -sn (No port scan)

This option tells Nmap not to do a port scan after host discovery, and only print out the available hosts that responded to the host discovery probes. This is often known as a "ping scan", but you can also request that traceroute and NSE host scripts be run.

References: <https://nmap.org/book/man-host-discovery.html>

NEW QUESTION 455

- (Exam Topic 4)

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

Answer: A

Explanation:

The data obtained by a Heartbleed attack may include unencrypted exchanges between TLS parties likely to be confidential, including any form post data in users' requests. Moreover, the confidential data exposed could include authentication secrets such as session cookies and passwords, which might allow attackers to impersonate a user of the service.

An attack may also reveal private keys of compromised parties. References: <https://en.wikipedia.org/wiki/Heartbleed>

NEW QUESTION 456

- (Exam Topic 4)

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. Notepad
- C. MS Excel
- D. Relational Database

Answer: A

Explanation:

grep is a command-line utility for searching plain-text data sets for lines matching a regular expression. References: <https://en.wikipedia.org/wiki/Grep>

NEW QUESTION 458

- (Exam Topic 4)

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?

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

Answer: A

Explanation:

By setting up an email address for your users to forward any suspicious email to, the emails can be automatically scanned and replied to, with security incidents created to follow up on any emails with attached malware or links to known bad websites.

References:

https://docs.servicenow.com/bundle/helsinki-security-management/page/product/threat-intelligence/task/t_Confi

NEW QUESTION 461

- (Exam Topic 4)

Which of the following is not a Bluetooth attack?

- A. Bluedriving
- B. Bluejacking
- C. Bluesmacking

D. Bluesnarfing

Answer: A

NEW QUESTION 463

- (Exam Topic 4)

It is a short-range wireless communication technology intended to replace the cables connecting portable or 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. Radio-Frequency Identification
- C. WLAN
- D. InfraRed

Answer: A

Explanation:

Bluetooth is a standard for the short-range wireless interconnection of mobile phones, computers, and other electronic devices.

References:

<http://www.bbc.co.uk/webwise/guides/about-bluetooth>

NEW QUESTION 468

- (Exam Topic 4)

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

Answer: A

NEW QUESTION 469

- (Exam Topic 4)

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.

Answer: A

Explanation:

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).

References: https://en.wikipedia.org/wiki/SQL_injection

NEW QUESTION 473

- (Exam Topic 4)

Which of the following is a design pattern based on distinct pieces of software providing application functionality as services to other applications?

- A. Service Oriented Architecture
- B. Object Oriented Architecture
- C. Lean Coding
- D. Agile Process

Answer: A

Explanation:

A service-oriented architecture (SOA) is an architectural pattern in computer software design in which application components provide services to other components via a communications protocol, typically over a network.

References: https://en.wikipedia.org/wiki/Service-oriented_architecture

NEW QUESTION 476

- (Exam Topic 4)

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 wardriving.

Which Algorithm is this referring to?

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

Answer: A

Explanation:

WEP is the currently most used protocol for securing 802.11 networks, also called wireless lans or wlans. In 2007, a new attack on WEP, the PTW attack, was discovered, which allows an attacker to recover the secret key in less than 60 seconds in some cases.

Note: Wardriving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, smartphone or personal digital assistant (PDA).

References: <https://events.ccc.de/camp/2007/Fahrplan/events/1943.en.html>

NEW QUESTION 479

- (Exam Topic 4)

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

Answer: A

NEW QUESTION 484

- (Exam Topic 4)

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

Answer: A

Explanation:

Phases of hacking

Phase 1—Reconnaissance Phase 2—Scanning

Phase 3—Gaining Access Phase 4—Maintaining Access Phase 5—Covering Tracks

Phase 1: Passive and Active Reconnaissance

References:

<http://hack-o-crack.blogspot.se/2010/12/five-stages-of-ethical-hacking.html>

NEW QUESTION 487

- (Exam Topic 4)

Which of the following is assured by the use of a hash?

- A. Integrity
- B. Confidentiality
- C. Authentication
- D. Availability

Answer: A

Explanation:

An important application of secure hashes is verification of message integrity. Determining whether any changes have been made to a message (or a file), for example, can be accomplished by comparing message digests calculated before, and after, transmission (or any other event).

References: https://en.wikipedia.org/wiki/Cryptographic_hash_function#Verifying_the_integrity_of_files_or_messages

NEW QUESTION 489

- (Exam Topic 4)

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

Answer: A

Explanation:

A DMZ or demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node only has direct access to equipment in the DMZ, rather than any other part of the network.

References: [https://en.wikipedia.org/wiki/DMZ_\(computing\)](https://en.wikipedia.org/wiki/DMZ_(computing))

NEW QUESTION 492

- (Exam Topic 4)

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

- A. tcpdump
- B. nessus
- C. etherea
- D. Jack the ripper

Answer: A

Explanation:

tcpdump is a common packet analyzer that runs under the command line. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. References: <https://en.wikipedia.org/wiki/Tcpdump>

NEW QUESTION 497

- (Exam Topic 4)

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

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

Answer: D

Explanation:

If the data written on the backup media is properly encrypted, it will be useless for anyone without the key.

References:

<http://resources.infosecinstitute.com/backup-media-encryption/>

NEW QUESTION 498

- (Exam Topic 4)

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

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

Answer: A

Explanation:

The activities within the incident management process include:

References: [https://en.wikipedia.org/wiki/Incident_management_\(ITSM\)#Incident_management_procedure](https://en.wikipedia.org/wiki/Incident_management_(ITSM)#Incident_management_procedure)

NEW QUESTION 500

- (Exam Topic 4)

Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it begins to close.

What just happened?

- A. Piggybacking
- B. Masquading
- C. Phishing
- D. Whaling

Answer: A

Explanation:

In security, piggybacking refers to when a person tags along with another person who is authorized to gain entry into a restricted area, or pass a certain checkpoint.

References: [https://en.wikipedia.org/wiki/Piggybacking_\(security\)](https://en.wikipedia.org/wiki/Piggybacking_(security))

NEW QUESTION 501

- (Exam Topic 4)

You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration?
alert tcp any any -> 192.168.100.0/24 21 (msg: "FTP on the network!");

- A. An Intrusion Detection System
- B. A firewall IPTable
- C. A Router IPTable
- D. FTP Server rule

Answer: A

Explanation:

Snort is an open source network intrusion detection system (NIDS) for networks . Snort rule example:

This example is a rule with a generator id of 1000001.

alert tcp any any -> any 80 (content:"BOB"; gid:1000001; sid:1; rev:1;)

References:

<http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node31.html>

NEW QUESTION 503

- (Exam Topic 4)

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?

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

Answer: A

Explanation:

Ransomware is a type of malware that can be covertly installed on a computer without knowledge or intention of the user that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction. Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying. Ransomware typically propagates as a Trojan.

References: <https://en.wikipedia.org/wiki/Ransomware>

NEW QUESTION 505

- (Exam Topic 4)

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

Answer: A

Explanation:

A threat is at any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

References: [https://en.wikipedia.org/wiki/Threat_\(computer\)](https://en.wikipedia.org/wiki/Threat_(computer))

NEW QUESTION 506

- (Exam Topic 4)

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

Answer: A

Explanation:

The Web Parameter Tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.

References: https://www.owasp.org/index.php/Web_Parameter_Tampering

NEW QUESTION 507

- (Exam Topic 4)

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

Answer: A

Explanation:

The hosts file is a computer file used by an operating system to map hostnames to IP addresses. The hosts file contains lines of text consisting of an IP address in

the first text field followed by one or more host names.
References: [https://en.wikipedia.org/wiki/Hosts_\(file\)](https://en.wikipedia.org/wiki/Hosts_(file))

NEW QUESTION 510

- (Exam Topic 4)

You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email(boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network.
What testing method did you use?

- A. Social engineering
- B. Tailgating
- C. Piggybacking
- D. Eavesdropping

Answer: A

Explanation:

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

NEW QUESTION 511

- (Exam Topic 4)

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 an ACK.
- D. The port will send a SYN.

Answer: A

Explanation:

An attacker uses a TCP XMAS scan to determine if ports are closed on the target machine. This scan type is accomplished by sending TCP segments with the all flags sent in the packet header, generating packets that are illegal based on RFC 793. The RFC 793 expected behavior is that any TCP segment with an out-of-state Flag sent to an open port is discarded, whereas segments with out-of-state flags sent to closed ports should be handled with a RST in response. This behavior should allow an attacker to scan for closed ports by sending certain types of rule-breaking packets (out of sync or disallowed by the TCB) and detect closed ports via RST packets.

References: <https://capec.mitre.org/data/definitions/303.html>

NEW QUESTION 513

- (Exam Topic 4)

The network administrator contacts you and tells you that she noticed the temperature on the internal wireless router increases by more than 20% during weekend hours when the office was closed. She asks you to investigate the issue because she is busy dealing with a big conference and she doesn't have time to perform the task.

What tool can you use to view the network traffic being sent and received by the wireless router?

- A. Wireshark
- B. Nessus
- C. Netcat
- D. Netstat

Answer: A

Explanation:

Wireshark is a Free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

NEW QUESTION 514

- (Exam Topic 4)

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

Answer: A

Explanation:

Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools.

The Nessus server is currently available for Unix, Linux and FreeBSD. The client is available for Unix- or Windows-based operating systems.

Note: Significant capabilities of Nessus include: References: <http://searchnetworking.techtarget.com/definition/Nessus>

NEW QUESTION 518

- (Exam Topic 5)

Risks = Threats x Vulnerabilities is referred to as the:

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

Answer: A

Explanation:

The most effective way to define risk is with this simple equation: Risk = Threat x Vulnerability x Cost

This equation is fundamental to all information security. References: http://www.icharter.org/articles/risk_equation.html

NEW QUESTION 522

- (Exam Topic 5)

A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client.

What is a possible source of this problem?

- A. The WAP does not recognize the client's MAC address
- B. The client cannot see the SSID of the wireless network
- C. Client is configured for the wrong channel
- D. The wireless client is not configured to use DHCP

Answer: A

Explanation:

MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network. MAC Filtering is often used on wireless networks.

References: https://en.wikipedia.org/wiki/MAC_filtering

NEW QUESTION 527

- (Exam Topic 5)

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

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

Answer: A

Explanation:

Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings.

References: https://en.wikipedia.org/wiki/Black-box_testing

NEW QUESTION 532

- (Exam Topic 5)

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

Answer: A

Explanation:

Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the website trusts.

Example and characteristics

If an attacker is able to find a reproducible link that executes a specific action on the target page while the victim is being logged in there, he is able to embed such link on a page he controls and trick the victim into opening it. The attack carrier link may be placed in a location that the victim is likely to visit while logged into the target site (e.g. a discussion forum), sent in a HTML email body or attachment.

NEW QUESTION 534

- (Exam Topic 5)

Which of the following is a protocol specifically designed for transporting event messages?

- A. SYSLOG
- B. SMS

- C. SNMP
- D. ICMP

Answer: A

Explanation:

syslog is a standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, indicating the software type generating the message, and assigned a severity label. References: https://en.wikipedia.org/wiki/Syslog#Network_protocol

NEW QUESTION 536

- (Exam Topic 5)

Internet Protocol Security IPSec is actually a suite of protocols. Each protocol within the suite provides different functionality. Collective IPSec does everything except.

- A. Protect the payload and the headers
- B. Authenticate
- C. Encrypt
- D. Work at the Data Link Layer

Answer: D

NEW QUESTION 538

- (Exam Topic 5)

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

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

Answer: A

Explanation:

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station. References: https://en.wikipedia.org/wiki/Intrusion_detection_system

NEW QUESTION 540

- (Exam Topic 5)

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

- A. tcpdump
- B. nmap
- C. ping
- D. tracer

Answer: A

Explanation:

The passive operating system fingerprinting is a feature built into both the pf and tcpdump tools. References: <http://geek00l.blogspot.se/2007/04/tcpdump-privilege-dropping-passive-os.html>

NEW QUESTION 542

- (Exam Topic 5)

The company ABC recently discovered that their new product was released by the opposition before their premiere. They contract an investigator who discovered that the maid threw away papers with confidential information about the new product and the opposition found it in the garbage. What is the name of the technique used by the opposition?

- A. Hack attack
- B. Sniffing
- C. Dumpster diving
- D. Spying

Answer: C

NEW QUESTION 545

- (Exam Topic 5)

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

Answer:

A

Explanation:

A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications for weaknesses. They can be run either as part of vulnerability management by those tasked with protecting systems - or by black hat attackers looking to gain unauthorized access.

References: https://en.wikipedia.org/wiki/Vulnerability_scanner

NEW QUESTION 550

- (Exam Topic 5)

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 scripting vulnerability
- B. Cross-site Request Forgery vulnerability
- C. SQL injection vulnerability
- D. Web site defacement vulnerability

Answer: A

Explanation:

Many operators of particular web applications (e.g. forums and webmail) allow users to utilize a limited subset of HTML markup. When accepting HTML input from users (say, `very large`), output encoding (such as `very large`) will not suffice since the user input needs to be rendered as HTML by the browser (so it shows as "very large", instead of "`very large`"). Stopping an XSS attack when accepting HTML input from users is much more complex in this situation. Untrusted HTML input must be run through an HTML sanitization engine to ensure that it does not contain cross-site scripting code.

References: https://en.wikipedia.org/wiki/Cross-site_scripting#Safely_validating_untrusted_HTML_input

NEW QUESTION 551

- (Exam Topic 5)

The establishment of a TCP connection involves a negotiation called 3 way handshake. What type of message sends the client to the server in order to begin this negotiation?

- A. RST
- B. ACK
- C. SYN-ACK
- D. SYN

Answer: D

NEW QUESTION 556

- (Exam Topic 5)

What is the most common method to exploit the "Bash Bug" or "ShellShock" vulnerability?

- A. Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server
- B. Manipulate format strings in text fields
- C. SSH
- D. SYN Flood

Answer: A

Explanation:

Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell. One specific exploitation vector of the Shellshock bug is CGI-based web servers.

Note: When a web server uses the Common Gateway Interface (CGI) to handle a document request, it passes various details of the request to a handler program in the environment variable list. For example, the variable `HTTP_USER_AGENT` has a value that, in normal usage, identifies the program sending the request. If the request handler is a Bash script, or if it executes one for example using the system call, Bash will receive the environment variables passed by the server and will process them. This provides a means for an attacker to trigger the Shellshock vulnerability with a specially crafted server request.

References: [https://en.wikipedia.org/wiki/Shellshock_\(software_bug\)#Specific_exploitation_vectors](https://en.wikipedia.org/wiki/Shellshock_(software_bug)#Specific_exploitation_vectors)

NEW QUESTION 557

- (Exam Topic 5)

An attacker is trying to redirect the traffic of a small office. That office is using their own mail server, DNS server and NTP server because of the importance of their job. The attacker gains access to the DNS server and redirects the direction `www.google.com` to his own IP address. Now when the employees of the office want to go to Google they are being redirected to the attacker machine. What is the name of this kind of attack?

- A. ARP Poisoning
- B. Smurf Attack
- C. DNS spoofing
- D. MAC Flooding

Answer: C

NEW QUESTION 561

- (Exam Topic 5)

The chance of a hard drive failure is once every three years. The cost to buy a new hard drive is \$300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns \$10/hour. Calculate the SLE, ARO, and ALE. Assume the $EF = 1$ (100%).

What is the closest approximate cost of this replacement and recovery operation per year?

- A. \$146
- B. \$1320
- C. \$440
- D. \$100

Answer: A

Explanation:

The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE).

Suppose that an asset is valued at \$100,000, and the Exposure Factor (EF) for this asset is 25%. The single loss expectancy (SLE) then, is 25% * \$100,000, or \$25,000.

In our example the ARO is 33%, and the SLE is 300+14*10 (as EF=1). The ALO is thus: 33%*(300+14*10) which equals 146.

References: https://en.wikipedia.org/wiki/Annualized_loss_expectancy

NEW QUESTION 563

- (Exam Topic 5)

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

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

Answer: A

Explanation:

The ability to analyze the likelihood of threats within the organization is a critical step in building an effective security program. The process of assessing threat probability should be well defined and incorporated into a broader threat analysis process to be effective.

References:

<http://www.mcafee.com/campaign/securitybattleground/resources/chapter5/whitepaper-on-assessing-threat-attac>

NEW QUESTION 564

- (Exam Topic 5)

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

Answer: A

Explanation:

The most common web application security weakness is the failure to properly validate input coming from the client or from the environment before using it. This weakness leads to almost all of the major vulnerabilities in web applications, such as cross site scripting, SQL injection, interpreter injection, locale/Unicode attacks, file system attacks, and buffer overflows.

References: https://www.owasp.org/index.php/Testing_for_Input_Validation

NEW QUESTION 566

- (Exam Topic 5)

What two conditions must a digital signature meet?

- A. Has to be unforgeable, and has to be authentic.
- B. Has to be legible and neat.
- C. Must be unique and have special characters.
- D. Has to be the same number of characters as a physical signature and must be unique.

Answer: A

NEW QUESTION 570

- (Exam Topic 5)

Which protocol is used for setting up secured channels between two devices, typically in VPNs?

- A. IPSEC
- B. PEM
- C. SET
- D. PPP

Answer: A

NEW QUESTION 574

- (Exam Topic 5)

A large mobile telephony and data network operator has a data center that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with firewalls and IPS systems. What is the best security policy concerning this setup?

- A. Network elements must be hardened with user ids and strong password
- B. Regular security tests and audits should be performed.
- C. As long as the physical access to the network elements is restricted, there is no need for additional measures.
- D. There is no need for specific security measures on the network elements as long as firewalls and IPS systems exist.
- E. The operator knows that attacks and down time are inevitable and should have a backup site.

Answer: A

NEW QUESTION 575

- (Exam Topic 5)

Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?

- A. Kismet
- B. Nessus
- C. Netstumbler
- D. Abel

Answer: A

Explanation:

Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic. The program runs under Linux, FreeBSD, NetBSD, OpenBSD, and Mac OS X.
References: [https://en.wikipedia.org/wiki/Kismet_\(software\)](https://en.wikipedia.org/wiki/Kismet_(software))

NEW QUESTION 577

- (Exam Topic 5)

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

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

Answer: A

Explanation:

Brute-force cracking, in which a computer tries every possible key or password until it succeeds, is typically very time consuming. More common methods of password cracking, such as dictionary attacks, pattern checking, word list substitution, etc. attempt to reduce the number of trials required and will usually be attempted before brute force.

References: https://en.wikipedia.org/wiki/Password_cracking

NEW QUESTION 580

- (Exam Topic 5)

By using a smart card and pin, you are using a two-factor authentication that satisfies

- A. Something you know and something you are
- B. Something you have and something you know
- C. Something you have and something you are
- D. Something you are and something you remember

Answer: B

NEW QUESTION 582

- (Exam Topic 5)

What is the correct process for the TCP three-way handshake connection establishment and connection termination?

- A. Connection Establishment: FIN, ACK-FIN, ACK
Connection Termination: SYN, SYN-ACK, ACK
- B. Connection Establishment: SYN, SYN-ACK, ACK
Connection Termination: ACK, ACK-SYN, SYN
- C. Connection Establishment: ACK, ACK-SYN, SYN
Connection Termination: FIN, ACK-FIN, ACK
- D. Connection Establishment: SYN, SYN-ACK, ACK
Connection Termination: FIN, ACK-FIN, ACK

Answer: D

NEW QUESTION 583

- (Exam Topic 5)

The company ABC recently contracted a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. What of the following options can be useful to ensure the integrity of the data?

- A. The document can be sent to the accountant using an exclusive USB for that document.
- B. The CFO can use a hash algorithm in the document once he approved the financial statements.
- C. The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure it is the same document.
- D. The CFO can use an excel file with a password.

Answer: B

NEW QUESTION 585

- (Exam Topic 5)

You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?

- A. hping2 host.domain.com
- B. hping2 --set-ICMP host.domain.com
- C. hping2 -i host.domain.com
- D. hping2 -1 host.domain.com

Answer: D

NEW QUESTION 590

- (Exam Topic 5)

Which of the following is a passive wireless packet analyzer that works on Linux-based systems?

- A. Burp Suite
- B. OpenVAS
- C. tshark
- D. Kismet

Answer: D

NEW QUESTION 595

- (Exam Topic 5)

The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124.

An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is: nmap 192.168.1.64/28.

Why he cannot see the servers?

- A. The network must be down and the nmap command and IP address are ok.
- B. He needs to add the command ""ip address"" just before the IP address.
- C. He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range.
- D. He needs to change the address to 192.168.1.0 with the same mask.

Answer: C

NEW QUESTION 597

- (Exam Topic 5)

Which of the following statements regarding ethical hacking is incorrect?

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

Answer: A

Explanation:

Ethical hackers use the same methods and techniques, including those that have the potential of exploiting vulnerabilities, to test and bypass a system's defenses as their less-principled counterparts, but rather than taking advantage of any vulnerabilities found, they document them and provide actionable advice on how to fix them so the organization can improve its overall security.

References:

<http://searchsecurity.techtarget.com/definition/ethical-hacker>

NEW QUESTION 600

- (Exam Topic 5)

_____ is a set of extensions to DNS that provide to DNS clients (resolvers) origin authentication of DNS data to reduce the threat of DNS poisoning, spoofing, and similar attacks types.

- A. DNSSEC
- B. Zone transfer
- C. Resource transfer
- D. Resource records

Answer: A

NEW QUESTION 603

- (Exam Topic 5)

Sophia travels a lot and worries that her laptop containing confidential documents might be stolen. What is the best protection that will work for her?

- A. Password protected files
- B. Hidden folders
- C. BIOS password
- D. Full disk encryption.

Answer: D

NEW QUESTION 604

- (Exam Topic 5)

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

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

Answer: A

Explanation:

Newer firewalls can filter traffic based on many packet attributes like source IP address, source port, destination IP address or transport layer port, destination service like WWW or FTP. They can filter based on protocols, TTL values, netblock of originator, of the source, and many other attributes. Application layer firewalls are responsible for filtering at 3, 4, 5, 7 layer. Because they analyze the application layer headers, most firewall control and filtering is performed actually in the software.

References: [https://en.wikipedia.org/wiki/Firewall_\(computing\)#Network_layer_or_packet_filters](https://en.wikipedia.org/wiki/Firewall_(computing)#Network_layer_or_packet_filters)

<http://howdoesinternetnetwork.com/2012/application-layer-firewalls>

NEW QUESTION 606

- (Exam Topic 5)

Which tier in the N-tier application architecture is responsible for moving and processing data between the tiers?

- A. Application Layer
- B. Data tier
- C. Presentation tier
- D. Logic tier

Answer: D

NEW QUESTION 610

- (Exam Topic 5)

Bob learned that his username and password for a popular game has been compromised. He contacts the company and resets all the information. The company suggests he use two-factor authentication, which option below offers that?

- A. A new username and password
- B. A fingerprint scanner and his username and password.
- C. Disable his username and use just a fingerprint scanner.
- D. His username and a stronger password.

Answer: B

NEW QUESTION 611

- (Exam Topic 5)

Which Intrusion Detection System is best applicable for large environments where critical assets on the network need extra security and is ideal for observing sensitive network segments?

- A. Network-based intrusion detection system (NIDS)
- B. Host-based intrusion detection system (HIDS)
- C. Firewalls
- D. Honey pots

Answer: A

NEW QUESTION 614

- (Exam Topic 5)

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

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

Answer: A

Explanation:

As a matter of good practice any PII should be protected with strong encryption.

References: <https://cuit.columbia.edu/cuit/it-security-practices/handling-personally-identifying-information>

NEW QUESTION 615

- (Exam Topic 5)

Sid is a judge for a programming contest. Before the code reaches him it goes through a restricted OS and is tested there. If it passes, then it moves onto Sid. What is this middle step called?

- A. Fuzzy-testing the code
- B. Third party running the code
- C. Sandboxing the code
- D. String validating the code

Answer: A

NEW QUESTION 620

- (Exam Topic 5)

When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best describes what it is meant by processing?

- A. The amount of time it takes to convert biometric data into a template on a smart card.
- B. The amount of time and resources that are necessary to maintain a biometric system.
- C. The amount of time it takes to be either accepted or rejected form when an individual provides Identification and authentication information.
- D. How long it takes to setup individual user accounts.

Answer: C

NEW QUESTION 625

- (Exam Topic 5)

Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications and unpatched security flaws in a computer system?

- A. Wireshark
- B. Maltego
- C. Metasploit
- D. Nessus

Answer: C

NEW QUESTION 629

- (Exam Topic 5)

What is correct about digital signatures?

- A. A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.
- B. Digital signatures may be used in different documents of the same type.
- C. A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.
- D. Digital signatures are issued once for each user and can be used everywhere until they expire.

Answer: A

NEW QUESTION 634

- (Exam Topic 5)

Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?

- A. A biometric system that bases authentication decisions on behavioral attributes.
- B. A biometric system that bases authentication decisions on physical attributes.
- C. An authentication system that creates one-time passwords that are encrypted with secret keys.
- D. An authentication system that uses passphrases that are converted into virtual passwords.

Answer: C

NEW QUESTION 637

- (Exam Topic 5)

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

- A. Residual risk
- B. Inherent risk
- C. Deferred risk
- D. Impact risk

Answer: A

Explanation:

The residual risk is the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied (scientifically conceivable measures); in other words, the amount of risk left over after natural or inherent risks have been reduced by risk controls.

References: https://en.wikipedia.org/wiki/Residual_risk

NEW QUESTION 639

- (Exam Topic 5)

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

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

Answer: A

Explanation:

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access.

References: [https://en.wikipedia.org/wiki/Social_engineering_\(security\)](https://en.wikipedia.org/wiki/Social_engineering_(security))

NEW QUESTION 640

- (Exam Topic 5)

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

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

Answer: A

Explanation:

A stateful firewall is a network firewall that tracks the operating state and characteristics of network connections traversing it. The firewall is configured to distinguish legitimate packets for different types of connections. Only packets matching a known active connection (session) are allowed to pass the firewall.

References: https://en.wikipedia.org/wiki/Stateful_firewall

NEW QUESTION 641

- (Exam Topic 5)

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

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

Answer: A

Explanation:

Contextual output encoding/escaping could be used as the primary defense mechanism to stop Cross-site Scripting (XSS) attacks.

References:

https://en.wikipedia.org/wiki/Cross-site_scripting#Contextual_output_encoding.2Fescaping_of_string_input

NEW QUESTION 644

- (Exam Topic 5)

A well-intentioned researcher discovers a vulnerability on the web site of a major corporation. What should he do?

- A. Ignore it.
- B. Try to sell the information to a well-paying party on the dark web.
- C. Notify the web site owner so that corrective action be taken as soon as possible to patch the vulnerability.
- D. Exploit the vulnerability without harming the web site owner so that attention be drawn to the problem.

Answer: C

NEW QUESTION 648

- (Exam Topic 5)

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

Answer: A

Explanation:

A false negative error, or in short false negative, is where a test result indicates that a condition failed, while it actually was successful. I.e. erroneously no effect has been assumed.

References: https://en.wikipedia.org/wiki/False_positives_and_false_negatives#False_negative_error

NEW QUESTION 650

- (Exam Topic 5)

Which of these is capable of searching for and locating rogue access points?

- A. HIDS
- B. WISS
- C. WIPS
- D. NIDS

Answer: C

NEW QUESTION 652

- (Exam Topic 5)

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

Answer: A

Explanation:

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.

References: <https://en.wikipedia.org/wiki/Steganography>

NEW QUESTION 653

- (Exam Topic 5)

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. Intrusion Prevention System (IPS)
- C. Network sniffer
- D. Vulnerability scanner

Answer: A

Explanation:

A packet analyzer (also known as a network analyzer, protocol analyzer or packet sniffer—or, for particular types of networks, an Ethernet sniffer or wireless sniffer) is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network. A packet analyzer can analyze packet traffic saved in a PCAP file.

References: https://en.wikipedia.org/wiki/Packet_analyzer

NEW QUESTION 656

- (Exam Topic 5)

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. Fuzzing
- B. Randomizing
- C. Mutating
- D. Bounding

Answer: A

Explanation:

Fuzz testing or fuzzing is a software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes, or failing built-in code assertions or for finding potential memory leaks. Fuzzing is commonly used to test for security problems in software or computer systems. It is a form of random testing which has been used for testing hardware or software.

References: https://en.wikipedia.org/wiki/Fuzz_testing

NEW QUESTION 657

- (Exam Topic 6)

What type of malware is it that restricts access to a computer system that it infects and demands that the user pay a certain amount of money, cryptocurrency, etc. to the operators of the malware to remove the restriction?

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

Answer: A

NEW QUESTION 661

- (Exam Topic 6)

Matthew received an email with an attachment named "YouWon\$10Grand.zip." The zip file contains a file named "HowToClaimYourPrize.docx.exe." Out of excitement and curiosity, Matthew opened the said file. Without his knowledge, the file copies itself to Matthew's APPDATA\local directory and begins to beacon to a Command-and-control server to download additional malicious binaries. What type of malware has Matthew encountered?

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

Answer: B

NEW QUESTION 663

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 312-50v10 Exam with Our Prep Materials Via below:

<https://www.certleader.com/312-50v10-dumps.html>