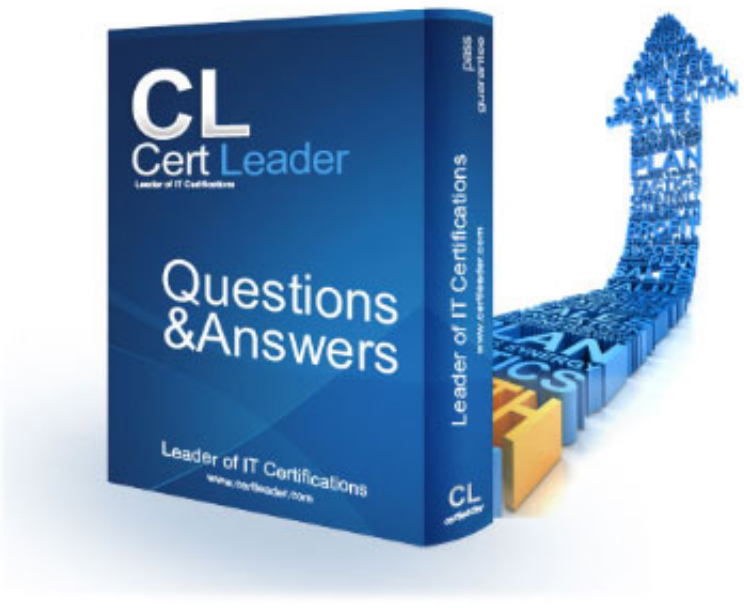
312-50v10 Dumps

Certified Ethical Hacker v10

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



NEW QUESTION 1
- (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 2
- (Exam Topic 1)
You are a security officer of a company. You had an alert from IDS that indicates that one PC on your Intranet is connected to a blacklisted IP address (C2 Server) on the Internet. The IP address was blacklisted just before the alert. You are staring an investigation to roughly analyze the severity of the situation. Which of the following is appropriate to analyze?

A. Event logs on the PC
B. Internet Firewall/Proxy log
C. IDS log
D. Event logs on domain controller

Answer: B

NEW QUESTION 3
- (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 4
- (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 5
- (Exam Topic 1)
You perform a scan of your company’s network and discover that TCP port 123 is open. What services by default run on TCP port 123?

A. Telnet
B. POP3
C. Network Time Protocol
D. DNS

Answer: C

NEW QUESTION 6
- (Exam Topic 1)
Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access.
A camera captures people walking and identifies the individuals using Steve’s approach.
After that, people must approximate their RFID badges. Both the identifications are required to open the door.
In this case, we can say:

A. Although the approach has two phases, it actually implements just one authentication factor
B. The solution implements the two authentication factors: physical object and physical characteristic
C. The solution will have a high level of false positives
D. Biological motion cannot be used to identify people

Answer: B

NEW QUESTION 7
- (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 8
- (Exam Topic 1)
Which of the following is considered as one of the most reliable forms of TCP scanning?

A. TCP Connect/Full Open Scan
B. Half-open Scan
C. NULL Scan
D. Xmas Scan

Answer: A

NEW QUESTION 9
- (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 10
- (Exam Topic 1)
On performing a risk assessment, you need to determine the potential impacts when some of the critical business process of the company interrupt its service.
What is the name of the process by which you can determine those critical business?

A. Risk Mitigation
B. Emergency Plan Response (EPR)
C. Disaster Recovery Planning (DRP)
D. Business Impact Analysis (BIA)

Answer: D

NEW QUESTION 10
- (Exam Topic 1)
Which component of IPsec performs protocol-level functions that are required to encrypt and decrypt the packets?

A. Internet Key Exchange (IKE)
B. Oakley
C. IPsec Policy Agent
D. IPsec driver

Answer: A

NEW QUESTION 13
- (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 14
- (Exam Topic 1)
Some clients of TPNQM SA were redirected to a malicious site when they tried to access the TPNQM main site. Bob, a system administrator at TPNQM SA, found that they were victims of DNS Cache Poisoning.
What should Bob recommend to deal with such a threat?

A. The use of security agents in clients' computers

B. The use of DNSSEC
C. The use of double-factor authentication
D. Client awareness

Answer: B

NEW QUESTION 16
- (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 19
- (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 20
- (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 21
- (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 26
- (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 28
- (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 31

- (Exam Topic 1)
Which of the following is the best countermeasure to encrypting ransomwares?

A. Use multiple antivirus softwares
B. Keep some generation of off-line backup
C. Analyze the ransomware to get decryption key of encrypted data
D. Pay a ransom

Answer: B

NEW QUESTION 33
- (Exam Topic 1)
Which of the following steps for risk assessment methodology refers to vulnerability identification?

A. Determines if any flaws exist in systems, policies, or procedures
B. Assigns values to risk probabilities; Impact values.
C. Determines risk probability that vulnerability will be exploited (Hig
D. Medium, Low)
E. Identifies sources of harm to an IT syste
F. (Natural, Huma
G. Environmental)

Answer: C

NEW QUESTION 36
- (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 41
- (Exam Topic 1)
A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer's software and hardware without the owner’s permission. Their intention can either be to simply gain knowledge or to illegally make changes. Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?

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

Answer: D

NEW QUESTION 44
- (Exam Topic 1)
Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key.
Suppose a malicious user Rob tries to get access to the account of a benign user Ned.
Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

A. “GET/restricted/goldtransfer?to=Rob&from=1 or 1=1’ HTTP/1.1Host: westbank.com”
B. “GET/restricted/accounts/?name=Ned HTTP/1.1 Host: westbank.com”
C. “GET/restricted/bank.getaccount(‘Ned’) HTTP/1.1 Host: westbank.com”
D. “GET/restricted/\r\n\%00account%00Ned%00access HTTP/1.1 Host: westbank.com”

Answer: B

NEW QUESTION 49
- (Exam Topic 1)
When tuning security alerts, what is the best approach?

A. Tune to avoid False positives and False Negatives
B. Rise False positives Rise False Negatives
C. Decrease the false positives
D. Decrease False negatives

Answer: A

NEW QUESTION 50
- (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 53
- (Exam Topic 1)
Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days. Bob denies that he had ever sent a mail. What do you want to ""know"" to prove yourself that it was Bob who had send a mail?

A. Authentication
B. Confidentiality
C. Integrity
D. Non-Repudiation

Answer: D

NEW QUESTION 55
- (Exam Topic 1)
Alice encrypts her data using her public key PK and stores the encrypted data in the cloud. Which of the following attack scenarios will compromise the privacy of her data?

A. None of these scenarios compromise the privacy of Alice's data
B. Agent Andrew subpoenas Alice, forcing her to reveal her private ke
C. However, the cloud server successfully resists Andrew's attempt to access the stored data
D. Hacker Harry breaks into the cloud server and steals the encrypted data
E. Alice also stores her private key in the cloud, and Harry breaks into the cloud server as before

Answer: D

NEW QUESTION 59
- (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 61
- (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 62
- (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 67
- (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 72
- (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 75
- (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 79
- (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 83
- (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 87
- (Exam Topic 1)
Which of the following is an adaptive SQL Injection testing technique used to discover coding errors by inputting massive amounts of random data and observing the changes in the output?

A. Function Testing
B. Dynamic Testing
C. Static Testing
D. Fuzzing Testing

Answer: D

NEW QUESTION 90
- (Exam Topic 1)
Company XYZ has asked you to assess the security of their perimeter email gateway. From your office in New York, you craft a specially formatted email message and send it across the Internet to an employee of Company XYZ. The employee of Company XYZ is aware of your test.
Your email message looks like this: From: jim_miller@companyxyz.com
To: michelle_saunders@companyxyz.com Subject: Test message
Date: 4/3/2017 14:37
The employee of Company XYZ receives your email message. This proves that Company XYZ's email gateway doesn't prevent what?

A. Email Phishing
B. Email Masquerading
C. Email Spoofing
D. Email Harvesting

Answer: C

NEW QUESTION 92
- (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 93
- (Exam Topic 1)
Your business has decided to add credit card numbers to the data it backs up to tape. Which of the following represents the best practice your business should observe?

A. Hire a security consultant to provide direction.
B. Do not back up cither the credit card numbers or then hashes.
C. Back up the hashes of the credit card numbers not the actual credit card numbers.
D. Encrypt backup tapes that are sent off-site.

Answer: A

NEW QUESTION 96
- (Exam Topic 1)
Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations.
Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.
In this context, what can you say?

A. Bob can be right since DMZ does not make sense when combined with stateless firewalls
B. Bob is partially righ
C. He does not need to separate networks if he can create rules by destination IPs, one by one
D. Bob is totally wron
E. DMZ is always relevant when the company has internet servers and workstations
F. Bob is partially righ
G. DMZ does not make sense when a stateless firewall is available

Answer: C

NEW QUESTION 100
- (Exam Topic 1)
You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for.
Which of the below scanning technique will you use?

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

Answer: C

NEW QUESTION 105
- (Exam Topic 1)
In which of the following cryptography attack methods, the attacker makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions?

A. Chosen-plaintext attack
B. Ciphertext-only attack
C. Adaptive chosen-plaintext attack
D. Known-plaintext attack

Answer: A

NEW QUESTION 110
- (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 111
- (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 114
- (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 119
- (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 120
- (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 124
- (Exam Topic 2)
An attacker has been successfully modifying the purchase price of items purchased on the company's web site. The security administrators verify the web server and Oracle database have not been compromised directly. They have also verified the Intrusion Detection System (IDS) logs and found no attacks that could have caused this. What is the mostly likely way the attacker has been able to modify the purchase price?

A. By using SQL injection
B. By changing hidden form values
C. By using cross site scripting
D. By utilizing a buffer overflow attack

Answer: B

NEW QUESTION 127
- (Exam Topic 2)
An organization hires a tester to do a wireless penetration test. Previous reports indicate that the last test did not contain management or control packets in the submitted traces. Which of the following is the most likely reason for lack of management or control packets?

A. The wireless card was not turned on.
B. The wrong network card drivers were in use by Wireshark.
C. On Linux and Mac OS X, only 802.11 headers are received in promiscuous mode.
D. Certain operating systems and adapters do not collect the management or control packets.

Answer: D

NEW QUESTION 132
- (Exam Topic 2)
Which of the following is a preventive control?

A. Smart card authentication
B. Security policy
C. Audit trail
D. Continuity of operations plan

Answer: A

NEW QUESTION 137
- (Exam Topic 2)
Which of the following problems can be solved by using Wireshark?

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

Answer: D

NEW QUESTION 140
- (Exam Topic 2)
How can a rootkit bypass Windows 7 operating system’s kernel mode, code signing policy?

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

Answer: D

NEW QUESTION 144
- (Exam Topic 2)
After gaining access to the password hashes used to protect access to a web based application, knowledge of which cryptographic algorithms would be useful to gain access to the application?

A. SHA1
B. Diffie-Helman
C. RSA
D. AES

Answer: A

NEW QUESTION 149
- (Exam Topic 2)
A security consultant decides to use multiple layers of anti-virus defense, such as end user desktop anti-virus and E-mail gateway. This approach can be used to mitigate which kind of attack?

A. Forensic attack
B. ARP spoofing attack
C. Social engineering attack
D. Scanning attack

Answer: C

NEW QUESTION 152
- (Exam Topic 2)
When utilizing technical assessment methods to assess the security posture of a network, which of the following techniques would be most effective in determining whether end-user security training would be beneficial?

A. Vulnerability scanning
B. Social engineering
C. Application security testing
D. Network sniffing

Answer: B

NEW QUESTION 154
- (Exam Topic 2)
What is a successful method for protecting a router from potential smurf attacks?

A. Placing the router in broadcast mode
B. Enabling port forwarding on the router
C. Installing the router outside of the network's firewall
D. Disabling the router from accepting broadcast ping messages

Answer: D

NEW QUESTION 159
- (Exam Topic 2)
Which type of scan is used on the eye to measure the layer of blood vessels?

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

Answer: B

NEW QUESTION 164
- (Exam Topic 2)
An attacker uses a communication channel within an operating system that is neither designed nor intended to transfer information. What is the name of the communications channel?

A. Classified
B. Overt
C. Encrypted
D. Covert

Answer: D

NEW QUESTION 168
- (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 170
- (Exam Topic 2)
Low humidity in a data center can cause which of the following problems?

A. Heat
B. Corrosion
C. Static electricity
D. Airborne contamination

Answer: C

NEW QUESTION 174
- (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 179
- (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 181
- (Exam Topic 2)
Which of the following can the administrator do to verify that a tape backup can be recovered in its entirety?

A. Restore a random file.
B. Perform a full restore.
C. Read the first 512 bytes of the tape.
D. Read the last 512 bytes of the tape.

Answer: B

Explanation:
A full restore is required.

NEW QUESTION 183
- (Exam Topic 2)

A security consultant is trying to bid on a large contract that involves penetration testing and reporting. The company accepting bids wants proof of work so the consultant prints out several audits that have been performed. Which of the following is likely to occur as a result?

A. The consultant will ask for money on the bid because of great work.
B. The consultant may expose vulnerabilities of other companies.
C. The company accepting bids will want the same type of format of testing.
D. The company accepting bids will hire the consultant because of the great work performed.

Answer: B

NEW QUESTION 188
- (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 191
- (Exam Topic 2)
What is the outcome of the comm”nc -l -p 2222 | nc 10.1.0.43 1234"?

A. Netcat will listen on the 10.1.0.43 interface for 1234 seconds on port 2222.
B. Netcat will listen on port 2222 and output anything received to a remote connection on 10.1.0.43 port 1234.
C. Netcat will listen for a connection from 10.1.0.43 on port 1234 and output anything received to port 2222.
D. Netcat will listen on port 2222 and then output anything received to local interface 10.1.0.43.

Answer: B

NEW QUESTION 196
- (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 199
- (Exam Topic 2)
Which set of access control solutions implements two-factor authentication?

A. USB token and PIN
B. Fingerprint scanner and retina scanner
C. Password and PIN
D. Account and password

Answer: A

NEW QUESTION 203
- (Exam Topic 2)
A consultant is hired to do physical penetration testing at a large financial company. In the first day of his assessment, the consultant goes to the company`s building dressed like an electrician and waits in the lobby for an employee to pass through the main access gate, then the consultant follows the employee behind to get into the restricted area. Which type of attack did the consultant perform?

A. Man trap
B. Tailgating
C. Shoulder surfing
D. Social engineering

Answer: B

NEW QUESTION 206
- (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)
While checking the settings on the internet browser, a technician finds that the proxy server settings have been checked and a computer is trying to use itself as a proxy server. What specific octet within the subnet does the technician see?

A. 10.10.10.10
B. 127.0.0.1
C. 192.168.1.1
D. 192.168.168.168

Answer: B

NEW QUESTION 210
- (Exam Topic 2)
One advantage of an application-level firewall is the ability to

A. filter packets at the network level.
B. filter specific commands, such as http:post.
C. retain state information for each packet.
D. monitor tcp handshaking.

Answer: B

NEW QUESTION 211
- (Exam Topic 2)
Which of the following is used to indicate a single-line comment in structured query language (SQL)?

A. --
B. ||
C. %%
D. "

Answer: A

NEW QUESTION 212
- (Exam Topic 2)
What technique is used to perform a Connection Stream Parameter Pollution (CSPP) attack?

A. Injecting parameters into a connection string using semicolons as a separator
B. Inserting malicious Javascript code into input parameters
C. Setting a user's session identifier (SID) to an explicit known value
D. Adding multiple parameters with the same name in HTTP requests

Answer: A

NEW QUESTION 213
- (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 217
- (Exam Topic 2)
A hacker is attempting to see which ports have been left open on a network. Which NMAP switch would the hacker use?

A. -sO
B. -sP
C. -sS
D. -sU

Answer: A

NEW QUESTION 219
- (Exam Topic 2)
Which of the following types of firewall inspects only header information in network traffic?

A. Packet filter
B. Stateful inspection
C. Circuit-level gateway
D. Application-level gateway

Answer: A

NEW QUESTION 220
- (Exam Topic 2)
Which of the following is an example of an asymmetric encryption implementation?

A. SHA1
B. PGP
C. 3DES
D. MD5

Answer: B

NEW QUESTION 223
- (Exam Topic 2)
A penetration tester was hired to perform a penetration test for a bank. The tester began searching for IP ranges owned by the bank, performing lookups on the bank's DNS servers, reading news articles online about the bank, watching what times the bank employees come into work and leave from work, searching the bank's job postings (paying special attention to IT related jobs), and visiting the local dumpster for the bank's corporate office. What phase of the penetration test is the tester currently in?

A. Information reporting
B. Vulnerability assessment
C. Active information gathering
D. Passive information gathering

Answer: D

NEW QUESTION 228
- (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 229
- (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 234
- (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 238
- (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 243
- (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 246
- (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 248
- (Exam Topic 2)
Which technical characteristic do Ethereal/Wireshark, TCPDump, and Snort have in common?

A. They are written in Java.
B. They send alerts to security monitors.
C. They use the same packet analysis engine.
D. They use the same packet capture utility.

Answer: D

NEW QUESTION 249
- (Exam Topic 2)
A hacker is attempting to see which IP addresses are currently active on a network. Which NMAP switch would the hacker use?

A. -sO
B. -sP
C. -sS
D. -sU

Answer: B

NEW QUESTION 253
- (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 254
- (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 257
- (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 261
- (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 266
- (Exam Topic 2)
An NMAP scan of a server shows port 69 is open. What risk could this pose?

A. Unauthenticated access
B. Weak SSL version
C. Cleartext login
D. Web portal data leak

Answer: A

NEW QUESTION 269
- (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 271
- (Exam Topic 2)
Which of the following cryptography attack methods is usually performed without the use of a computer?

A. Ciphertext-only attack
B. Chosen key attack
C. Rubber hose attack
D. Rainbow table attack

Answer: C

NEW QUESTION 276
- (Exam Topic 2)
What is the main difference between a “Normal” SQL Injection and a “Blind” SQL Injection vulnerability?

A. The request to the web server is not visible to the administrator of the vulnerable application.
B. The attack is called “Blind” because, although the application properly filters user input, it is still vulnerable to code injection.
C. The successful attack does not show an error message to the administrator of the affected application.
D. The vulnerable application does not display errors with information about the injection results to the attacker.

Answer: D

NEW QUESTION 280
- (Exam Topic 2)
Passive reconnaissance involves collecting information through which of the following?

A. Social engineering
B. Network traffic sniffing
C. Man in the middle attacks
D. Publicly accessible sources

Answer: D

NEW QUESTION 282
- (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 286
- (Exam Topic 2)
Which tool is used to automate SQL injections and exploit a database by forcing a given web application to connect to another database controlled by a hacker?

A. DataThief
B. NetCat
C. Cain and Abel
D. SQLInjector

Answer: A

NEW QUESTION 291
- (Exam Topic 2)
Which of the following is a component of a risk assessment?

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

Answer: B

NEW QUESTION 293
- (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)
Which of the following is considered an acceptable option when managing a risk?

A. Reject the risk.
B. Deny the risk.
C. Mitigate the risk.
D. Initiate the risk.

Answer: C

NEW QUESTION 301
- (Exam Topic 2)
Which of the following items of a computer system will an anti-virus program scan for viruses?

A. Boot Sector
B. Deleted Files
C. Windows Process List
D. Password Protected Files

Answer: A

NEW QUESTION 303
- (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

NEW QUESTION 306
- (Exam Topic 2)
Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

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

Answer: D

NEW QUESTION 309
- (Exam Topic 2)
Which of the statements concerning proxy firewalls is correct?

A. Proxy firewalls increase the speed and functionality of a network.
B. Firewall proxy servers decentralize all activity for an application.
C. Proxy firewalls block network packets from passing to and from a protected network.
D. Computers establish a connection with a proxy firewall which initiates a new network connection for the client.

Answer: D

NEW QUESTION 314
- (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 315
- (Exam Topic 2)
Which of the following is a hardware requirement that either an IDS/IPS system or a proxy server must have in order to properly function?

A. Fast processor to help with network traffic analysis
B. They must be dual-homed
C. Similar RAM requirements
D. Fast network interface cards

Answer: B

Explanation:
Dual-homed or dual-homing can refer to either an Ethernet device that has more than one network interface, for redundancy purposes, or in firewall technology, dual-homed is one of the firewall architectures, such as an IDS/IPS system, for implementing preventive security.
References: https://en.wikipedia.org/wiki/Dual-homed

NEW QUESTION 318
- (Exam Topic 2)
Which system consists of a publicly available set of databases that contain domain name registration contact information?

A. WHOIS
B. IANA
C. CAPTCHA
D. IETF

Answer: A

NEW QUESTION 319
- (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 322
- (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 327
- (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 328
- (Exam Topic 2)
When creating a security program, which approach would be used if senior management is supporting and enforcing the security policy?

A. A bottom-up approach
B. A top-down approach
C. A senior creation approach
D. An IT assurance approach

Answer: B

NEW QUESTION 333
- (Exam Topic 3)
Which of the following describes a component of Public Key Infrastructure (PKI) where a copy of a private key is stored to provide third-party access and to facilitate recovery operations?

A. Key registry
B. Recovery agent
C. Directory
D. Key escrow

Answer: D

NEW QUESTION 336
- (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 337
- (Exam Topic 3)
When comparing the testing methodologies of Open Web Application Security Project (OWASP) and Open Source Security Testing Methodology Manual (OSSTMM) the main difference is

A. OWASP is for web applications and OSSTMM does not include web applications.
B. OSSTMM is gray box testing and OWASP is black box testing.
C. OWASP addresses controls and OSSTMM does not.
D. OSSTMM addresses controls and OWASP does not.

Answer: D

NEW QUESTION 338
- (Exam Topic 3)
To reduce the attack surface of a system, administrators should perform which of the following processes to remove unnecessary software, services, and insecure configuration settings?

A. Harvesting
B. Windowing
C. Hardening

D. Stealthing

Answer: C

NEW QUESTION 342
- (Exam Topic 3)
Some passwords are stored using specialized encryption algorithms known as hashes. Why is this an appropriate method?

A. It is impossible to crack hashed user passwords unless the key used to encrypt them is obtained.
B. If a user forgets the password, it can be easily retrieved using the hash key stored by administrators.
C. Hashing is faster compared to more traditional encryption algorithms.
D. Passwords stored using hashes are non-reversible, making finding the password much more difficult.

Answer: D

NEW QUESTION 345
- (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 346
- (Exam Topic 3)
Which of the following algorithms provides better protection against brute force attacks by using a 160-bit message digest?

A. MD5
B. SHA-1
C. RC4
D. MD4

Answer: B

NEW QUESTION 349
- (Exam Topic 3)
SOAP services use which technology to format information?

A. SATA
B. PCI
C. XML
D. ISDN

Answer: C

NEW QUESTION 352
- (Exam Topic 3)
Which of the following is a characteristic of Public Key Infrastructure (PKI)?

A. Public-key cryptosystems are faster than symmetric-key cryptosystems.
B. Public-key cryptosystems distribute public-keys within digital signatures.
C. Public-key cryptosystems do not require a secure key distribution channel.
D. Public-key cryptosystems do not provide technical non-repudiation via digital signatures.

Answer: B

NEW QUESTION 354
- (Exam Topic 3)
A consultant has been hired by the V.P. of a large financial organization to assess the company's security posture. During the security testing, the consultant comes across child pornography on the V.P.'s computer. What is the consultant's obligation to the financial organization?

A. Say nothing and continue with the security testing.
B. Stop work immediately and contact the authorities.
C. Delete the pornography, say nothing, and continue security testing.
D. Bring the discovery to the financial organization's human resource department.

Answer: B

NEW QUESTION 359
- (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 361
- (Exam Topic 3)
Which method can provide a better return on IT security investment and provide a thorough and comprehensive assessment of organizational security covering policy, procedure design, and implementation?

A. Penetration testing
B. Social engineering
C. Vulnerability scanning
D. Access control list reviews

Answer: A

NEW QUESTION 362
- (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 importantintelligence 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 367
- (Exam Topic 3)
While testing the company's web applications, a tester attempts to insert the following test script into the search area on the company's web site:
<script>alert(" Testing Testing Testing ")</script>
Afterwards, when the tester presses the search button, a pop-up box appears on the screen with the text: "Testing Testing Testing". Which vulnerability has been detected in the web application?

A. Buffer overflow
B. Cross-site request forgery
C. Distributed denial of service
D. Cross-site scripting

Answer: D

NEW QUESTION 371
- (Exam Topic 3)
Which of the following ensures that updates to policies, procedures, and configurations are made in a controlled and documented fashion?

A. Regulatory compliance
B. Peer review
C. Change management
D. Penetration testing

Answer: C

NEW QUESTION 373
- (Exam Topic 3)
Which of the following is optimized for confidential communications, such as bidirectional voice and video?

A. RC4
B. RC5
C. MD4
D. MD5

Answer: A

NEW QUESTION 376
- (Exam Topic 3)
Which Open Web Application Security Project (OWASP) implements a web application full of known vulnerabilities?

A. WebBugs
B. WebGoat
C. VULN_HTML
D. WebScarab

Answer: B

NEW QUESTION 379
- (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 382
- (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 386
- (Exam Topic 3)
An attacker sniffs encrypted traffic from the network and is subsequently able to decrypt it. The attacker can now use which cryptanalytic technique to attempt to discover the encryption key?

A. Birthday attack
B. Plaintext attack
C. Meet in the middle attack
D. Chosen ciphertext attack

Answer: D

NEW QUESTION 387
- (Exam Topic 3)
Which United States legislation mandates that the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) must sign statements verifying the completeness and accuracy of financial reports?

A. Sarbanes-Oxley Act (SOX)
B. Gramm-Leach-Bliley Act (GLBA)
C. Fair and Accurate Credit Transactions Act (FACTA)
D. Federal Information Security Management Act (FISMA)

Answer: A

NEW QUESTION 388
- (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 391
- (Exam Topic 3)
International Organization for Standardization (ISO) standard 27002 provides guidance for compliance by outlining

A. guidelines and practices for security controls.
B. financial soundness and business viability metrics.
C. standard best practice for configuration management.
D. contract agreement writing standards.

Answer: A

NEW QUESTION 394
- (Exam Topic 3)
Which of the following tools would be the best choice for achieving compliance with PCI Requirement 11?

A. Truecrypt
B. Sub7
C. Nessus
D. Clamwin

Answer: C

NEW QUESTION 397
- (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 400
- (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 404
- (Exam Topic 4)
Which of the following is a component of a risk assessment?

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

Answer: A

Explanation:
Risk assessment include:
References: https://en.wikipedia.org/wiki/IT_risk_management#Risk_assessment

NEW QUESTION 405
- (Exam Topic 4)
You have successfully gained access to your client's internal network and successfully comprised a Linux server which is part of the internal IP network. You want to know which Microsoft Windows workstations have file sharing enabled.
Which port would you see listening on these Windows machines in the network?

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

Answer: A

Explanation:
The following ports are associated with file sharing and server message block (SMB) communications: References: https://support.microsoft.com/en-us/kb/298804

NEW QUESTION 409
- (Exam Topic 4)
You have successfully gained access to a linux server and would like to ensure that the succeeding outgoing traffic from this server will not be caught by a Network Based Intrusion Detection Systems (NIDS).
What is the best way to evade the NIDS?

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

Answer: A

Explanation:
When the NIDS encounters encrypted traffic, the only analysis it can perform is packet level analysis, since the application layer contents are inaccessible. Given that exploits against today's networks are primarily targeted against network services (application layer entities), packet level analysis ends up doing very little to protect our core business assets.
References:
http://www.techrepublic.com/article/avoid-these-five-common-ids-implementation-errors/

NEW QUESTION 414
- (Exam Topic 4)
What is a "Collision attack" in cryptography?

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

Answer: A

Explanation:
A Collision Attack is an attempt to find two input strings of a hash function that produce the same hash result. References: https://learncryptography.com/hash-functions/hash-collision-attack

NEW QUESTION 415
- (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 417
- (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 419
- (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 424
- (Exam Topic 4)
env x=`(){ :;};echo exploit` bash -c 'cat /etc/passwd'
What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?

A. Display passwd content to prompt
B. Removes the passwd file

C. Changes all passwords in passwd
D. Add new user to the passwd file

Answer: A

Explanation:
To extract private information, attackers are using a couple of techniques. The simplest extraction attacks are in the form:
() {:;}; /bin/cat /etc/passwd
That reads the password file /etc/passwd, and adds it to the response from the web server. So an attacker injecting this code through the Shellshock vulnerability would see the password file dumped out onto their screen as part of the web page returned.
References: https://blog.cloudflare.com/inside-shellshock/

NEW QUESTION 428
- (Exam Topic 4)
Which of the following describes the characteristics of a Boot Sector Virus?

A. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR
B. Moves the MBR to another location on the RAM 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: A

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 430
- (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 431
- (Exam Topic 4)
Which of the following is not a Bluetooth attack?

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

Answer: A

NEW QUESTION 436
- (Exam Topic 4)
You've gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your tool kit you have an Ubuntu 9.10 Linux LiveCD. Which Linux based tool has the ability to change any user's password or to activate disabled Windows accounts?

A. CHNTPW
B. Cain & Abel
C. SET
D. John the Ripper

Answer: A

Explanation:
chntpw is a software utility for resetting or blanking local passwords used by Windows NT, 2000, XP, Vista, 7, 8 and 8.1. It does this by editing the SAM database where Windows stores password hashes.
References: https://en.wikipedia.org/wiki/Chntpw

NEW QUESTION 441

- (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 446
- (Exam Topic 4)
You are attempting to man-in-the-middle a session. Which protocol will allow you to guess a sequence number?

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

Answer: A

Explanation:
At the establishment of a TCP session the client starts by sending a SYN-packet (SYN=synchronize) with a sequence number. To hijack a session it is required to send a packet with a right seq-number, otherwise they are dropped.
References: https://www.exploit-db.com/papers/13587/

NEW QUESTION 447
- (Exam Topic 4)
Which of the following is the successor of SSL?

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

Answer: A

Explanation:
Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as 'SSL', are cryptographic protocols that provide communications security over a computer network.
References: https://en.wikipedia.org/wiki/Transport_Layer_Security

NEW QUESTION 448
- (Exam Topic 4)
During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network.
What is this type of DNS configuration commonly called?

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

Answer: A

Explanation:
In a split DNS infrastructure, you create two zones for the same domain, one to be used by the internal network, the other used by the external network. Split DNS directs internal hosts to an internal domain name server for name resolution and external hosts are directed to an external domain name server for name resolution.
References:
http://www.webopedia.com/TERM/S/split_DNS.html

NEW QUESTION 450
- (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 454
- (Exam Topic 4)
Which regulation defines security and privacy controls for Federal information systems and organizations?

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

Answer: A

Explanation:
NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," provides a catalog of security controls for all U.S. federal information systems except those related to national security.
References: https://en.wikipedia.org/wiki/NIST_Special_Publication_800-53

NEW QUESTION 459
- (Exam Topic 4)
When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners.
What proxy tool will help you find web vulnerabilities?

A. Burpsuite
B. Maskgen
C. Dimitry
D. Proxychains

Answer: A

Explanation:
Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.
References: https://portswigger.net/burp/

NEW QUESTION 461
- (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 465
- (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 470
- (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

NEW QUESTION 475
- (Exam Topic 4)
Using Windows CMD, how would an attacker list all the shares to which the current user context has access?

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

Answer: A

Explanation:
Connects a computer to or disconnects a computer from a shared resource, or displays information about computer connections. The command also controls persistent net connections. Used without parameters, net use retrieves a list of network connections.
References: https://technet.microsoft.com/en-us/library/bb490717.aspx

NEW QUESTION 476
- (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)

NEW QUESTION 478
- (Exam Topic 4)
An attacker changes the profile information of a particular user (victim) on the target website. The attacker uses this string to update the victim's profile to a text file and then submit the data to the attacker's database.
<iframe src="http://www.vulnweb.com/updateif.php" style="display:none"></iframe>
What is this type of attack (that can use either HTTP GET or HTTP POST) called?

A. Cross-Site Request Forgery
B. Cross-Site Scripting
C. SQL Injection
D. Browser Hacking

Answer: A

Explanation:
Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf) or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the website trusts.
Different HTTP request methods, such as GET and POST, have different level of susceptibility to CSRF attacks and require different levels of protection due to their different handling by web browsers.
References: https://en.wikipedia.org/wiki/Cross-site_request_forgery

NEW QUESTION 479
- (Exam Topic 4)
Your company performs penetration tests and security assessments for small and medium-sized business in the local area. During a routine security assessment, you discover information that suggests your client is involved with human trafficking.
What should you do?

A. Immediately stop work and contact the proper legal authorities.
B. Copy the data to removable media and keep it in case you need it.
C. Confront the client in a respectful manner and ask her about the data.
D. Ignore the data and continue the assessment until completed as agreed.

Answer: A

NEW QUESTION 483
- (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 487
- (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 491
- (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 496
- (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 497
- (Exam Topic 5)
An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?

A. He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.
B. He will activate OSPF on the spoofed root bridge.
C. He will repeat the same attack against all L2 switches of the network.
D. He will repeat this action so that it escalates to a DoS attack.

Answer: A

NEW QUESTION 499
- (Exam Topic 5)
Which of the following tools can be used for passive OS fingerprinting?

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

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 500
- (Exam Topic 5)
What network security concept requires multiple layers of security controls to be placed throughout an IT infrastructure, which improves the security posture of an organization to defend against malicious attacks or potential vulnerabilities?

A. Security through obscurity
B. Host-Based Intrusion Detection System
C. Defense in depth
D. Network-Based Intrusion Detection System

Answer: C

NEW QUESTION 503
- (Exam Topic 5)
A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The ps command shows that the nc file is running as process, and the netstat command shows the nc process is listening on a network port.
What kind of vulnerability must be present to make this remote attack possible?

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

Answer: A

Explanation:
To upload files the user must have proper write file permissions.
References:
http://codex.wordpress.org/Hardening_WordPress

NEW QUESTION 505
- (Exam Topic 5)
What is the way to decide how a packet will move from an untrusted outside host to a protected inside that is behind a firewall, which permits the hacker to determine which ports are open and if the packets can pass through the packet-filtering of the firewall?

A. Firewalking
B. Session hijacking
C. Network sniffing
D. Man-in-the-middle attack

Answer: A

NEW QUESTION 509
- (Exam Topic 5)
In both pharming and phishing attacks an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?

A. In a pharming attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DN
B. In a phishing attack an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name.
C. Both pharming and phishing attacks are purely technical and are not considered forms of social engineering.
D. Both pharming and phishing attacks are identical.
E. In a phishing attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DN
F. In a pharming attack an attacker provides the victim with a URL that is either misspelled or looks very similar to the actual websites domain name.

Answer: A

NEW QUESTION 511
- (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 516
- (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)

NEW QUESTION 517
- (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 519
- (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 524
- (Exam Topic 5)
Which of the following security operations is used for determining the attack surface of an organization?

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

Answer: A

Explanation:
For a network scan the goal is to document the exposed attack surface along with any easily detected vulnerabilities.
References:
http://meisecurity.com/home/consulting/consulting-network-scanning/

NEW QUESTION 529
- (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 530
- (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 532
- (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 537
- (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
http://howdoesinternetwork.com/2012/application-layer-firewalls

NEW QUESTION 538
- (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 543
- (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 547
- (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. Honeypots

Answer: A

NEW QUESTION 548
- (Exam Topic 5)
What mechanism in Windows prevents a user from accidentally executing a potentially malicious batch (.bat) or PowerShell (.ps1) script?

A. User Access Control (UAC)
B. Data Execution Prevention (DEP)
C. Address Space Layout Randomization (ASLR)
D. Windows firewall

Answer: B

NEW QUESTION 549
- (Exam Topic 5)
An attacker attaches a rogue router in a network. He wants to redirect traffic to a LAN attached to his router as part of a man-in-the-middle attack. What measure on behalf of the legitimate admin can mitigate this attack?

A. Only using OSPFv3 will mitigate this risk.
B. Make sure that legitimate network routers are configured to run routing protocols with authentication.
C. Redirection of the traffic cannot happen unless the admin allows it explicitly.
D. Disable all routing protocols and only use static routes.

Answer: B

NEW QUESTION 553
- (Exam Topic 5)
A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

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

Answer: A

Explanation:
Cookies can store passwords and form content a user has previously entered, such as a credit card number or an address.
Cookies can be stolen using a technique called cross-site scripting. This occurs when an attacker takes advantage of a website that allows its users to post unfiltered HTML and JavaScript content.
References: https://en.wikipedia.org/wiki/HTTP_cookie#Cross-site_scripting_.E2.80.93_cookie_theft

NEW QUESTION 556
- (Exam Topic 5)
Which of these options is the most secure procedure for storing backup tapes?

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

Answer: A

Explanation:
An effective disaster data recovery strategy should consist of producing backup tapes and housing them in an offsite storage facility. This way the data isn't compromised if a natural disaster affects the business' office. It is highly recommended that the backup tapes be handled properly and stored in a secure, climate controlled facility. This provides peace of mind, and gives the business almost immediate stability after a disaster.
References:
http://www.entrustrm.com/blog/1132/why-is-offsite-tape-storage-the-best-disaster-recovery-strategy

NEW QUESTION 557
- (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 561
- (Exam Topic 5)
The "white box testing" methodology enforces what kind of restriction?

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

Answer: A

Explanation:
White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases.
References: https://en.wikipedia.org/wiki/White-box_testing

NEW QUESTION 562
- (Exam Topic 5)
Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?

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

Answer: A

Explanation:
Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/CGIs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.
References: https://en.wikipedia.org/wiki/Nikto_Web_Scanner

NEW QUESTION 565
- (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 567
- (Exam Topic 5)
During a security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do?

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

Answer: A

Explanation:
The auditor should first evaluated existing policies and practices to identify problem areas and opportunities.

NEW QUESTION 568
- (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 570
- (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 573
- (Exam Topic 5)
What is not a PCI compliance recommendation?

A. Limit access to card holder data to as few individuals as possible.
B. Use encryption to protect all transmission of card holder data over any public network.
C. Rotate employees handling credit card transactions on a yearly basis to different departments.
D. Use a firewall between the public network and the payment card data.

Answer: C

NEW QUESTION 574
- (Exam Topic 6)
While you were gathering information as part of security assessments for one of your clients, you were able to gather data that show your client is involved with fraudulent activities. What should you do?

A. Immediately stop work and contact the proper legal authorities
B. Ignore the data and continue the assessment until completed as agreed
C. Confront the client in a respectful manner and ask her about the data
D. Copy the data to removable media and keep it in case you need it

Answer: A

NEW QUESTION 576
- (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 577
- (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 579
- (Exam Topic 6)
Which type of security feature stops vehicles from crashing through the doors of a building?

A. Turnstile
B. Bollards
C. Mantrap
D. Receptionist

Answer: B

NEW QUESTION 583
- (Exam Topic 6)
A new wireless client that is 802.11 compliant cannot connect to a wireless network given that the client can see the network and it has compatible hardware and software installed. Upon further tests and investigation, it was found out that the Wireless Access Point (WAP) was not responding to the association requests being sent by the wireless client. What MOST likely is the issue on this scenario?

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

Answer: B

NEW QUESTION 585
- (Exam Topic 6)
Neil notices that a single address is generating traffic from its port 500 to port 500 of several other machines on the network. This scan is eating up most of the network bandwidth and Neil is concerned. As a security professional, what would you infer from this scan?

A. It is a network fault and the originating machine is in a network loop
B. It is a worm that is malfunctioning or hardcoded to scan on port 500
C. The attacker is trying to detect machines on the network which have SSL enabled
D. The attacker is trying to determine the type of VPN implementation and checking for IPSec

Answer: D

NEW QUESTION 588
- (Exam Topic 6)
When security and confidentiality of data within the same LAN is of utmost priority, which IPSec mode should you implement?

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

Answer: C

NEW QUESTION 592
- (Exam Topic 6)
As an Ethical Hacker you are capturing traffic from your customer network with Wireshark and you need to find and verify just SMTP traffic. What command in Wireshark will help you to find this kind of traffic?

A. request smtp 25
B. tcp.port eq 25
C. smtp port
D. tcp.contains port 25

Answer: B

NEW QUESTION 596
- (Exam Topic 6)
Which of the following BEST describes the mechanism of a Boot Sector Virus?

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

Answer: A

NEW QUESTION 598
- (Exam Topic 6)
.....is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.
Fill in the blank with appropriate choice.

A. Collision Attack
B. Evil Twin Attack
C. Sinkhole Attack

D. Signal Jamming Attack

Answer: B

NEW QUESTION 601
- (Exam Topic 6)
What would you type on the Windows command line in order to launch the Computer Management Console provided that you are logged in as an admin?

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

Answer: A

NEW QUESTION 602
- (Exam Topic 6)
Which of the following commands runs snort in packet logger mode?

A. ./snort -dev -h ./log
B. ./snort -dev -l ./log
C. ./snort -dev -o ./log
D. ./snort -dev -p ./log

Answer: B

NEW QUESTION 605
- (Exam Topic 6)
SNMP is a protocol used to query hosts, servers, and devices about performance or health status data. This protocol has long been used by hackers to gather great amount of information about remote hosts. Which of the following features makes this possible? (Choose two.)

A. It used TCP as the underlying protocol.
B. It uses community string that is transmitted in clear text.
C. It is susceptible to sniffing.
D. It is used by all network devices on the market.

Answer: BD

NEW QUESTION 607
- (Exam Topic 6)
In which phase of the ethical hacking process can Google hacking be employed? This is a technique that involves manipulating a search string with specific operators to search for vulnerabilities.
Example:
allintitle: root passwd

A. Maintaining Access
B. Gaining Access
C. Reconnaissance
D. Scanning and Enumeration

Answer: C

NEW QUESTION 608
- (Exam Topic 6)
While performing ping scans into a target network you get a frantic call from the organization's security team. They report that they are under a denial of service attack. When you stop your scan, the smurf attack event stops showing up on the organization's IDS monitor.
How can you modify your scan to prevent triggering this event in the IDS?

A. Scan more slowly.
B. Do not scan the broadcast IP.
C. Spoof the source IP address.
D. Only scan the Windows systems.

Answer: B

NEW QUESTION 612
- (Exam Topic 6)
Which among the following is a Windows command that a hacker can use to list all the shares to which the current user context has access?

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

Answer: B

NEW QUESTION 615
- (Exam Topic 6)
Backing up data is a security must. However, it also has certain level of risks when mishandled. 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 incomplete because no verification was performed
C. A backup is unavailable during disaster recovery
D. An unencrypted backup can be misplaced or stolen

Answer: D

NEW QUESTION 619
- (Exam Topic 6)
You want to analyze packets on your wireless network. Which program would you use?

A. Wireshark with Airpcap
B. Airsnort with Airpcap
C. Wireshark with Winpcap
D. Ethereal with Winpcap

Answer: A

NEW QUESTION 621
- (Exam Topic 6)
Which of the following is a restriction being enforced in “white box testing?”

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

Answer: B

NEW QUESTION 625
- (Exam Topic 6)
In order to prevent particular ports and applications from getting packets into an organization, what does a firewall check?

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

Answer: D

NEW QUESTION 627
- (Exam Topic 6)
XOR is a common cryptographic tool. 10110001 XOR 00111010 is?

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

Answer: D

NEW QUESTION 631
- (Exam Topic 6)
What tool and process are you going to use in order to remain undetected by an IDS while pivoting and passing traffic over a server you’ve compromised and gained root access to?

A. Install Cryptcat and encrypt outgoing packets from this server.
B. Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.
C. Use Alternate Data Streams to hide the outgoing packets from this server.

Answer: B

NEW QUESTION 634
- (Exam Topic 6)
A distributed port scan operates by:

A. Blocking access to the scanning clients by the targeted host
B. Using denial-of-service software against a range of TCP ports
C. Blocking access to the targeted host by each of the distributed scanning clients
D. Having multiple computers each scan a small number of ports, then correlating the results

Answer: D

NEW QUESTION 638
- (Exam Topic 6)
Which of the following Nmap commands would be used to perform a stack fingerprinting?

A. Nmap -O -p80 <host(s.>
B. Nmap -hU -Q<host(s.>
C. Nmap -sT -p <host(s.>
D. Nmap -u -o -w2 <host>
E. Nmap -sS -0p targe

Answer: B

NEW QUESTION 642
- (Exam Topic 6)
Defining rules, collaborating human workforce, creating a backup plan, and testing the plans are within what phase of the Incident Handling Process?

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

Answer: A

NEW QUESTION 643
- (Exam Topic 6)
It is a widely used 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. This protocol is specifically designed for transporting event messages. Which of the following is being described?

A. SNMP
B. ICMP
C. SYSLOG
D. SMS

Answer: C

NEW QUESTION 644
- (Exam Topic 6)
What does a type 3 code 13 represent? (Choose two.)

A. Echo request
B. Destination unreachable
C. Network unreachable
D. Administratively prohibited
E. Port unreachable
F. Time exceeded

Answer: BD

NEW QUESTION 649
- (Exam Topic 6)
Security and privacy of/on information systems are two entities that requires lawful regulations. Which of the following regulations defines security and privacy controls for Federal information systems and organizations?

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

Answer: A

NEW QUESTION 650
- (Exam Topic 6)
What tool should you use when you need to analyze extracted metadata from files you collected when you were in the initial stage of penetration test (information gathering)?

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

Answer: C

NEW QUESTION 651
- (Exam Topic 6)
There are several ways to gain insight on how a cryptosystem works with the goal of reverse engineering the process. A term describes when two pieces of data result in the same value is?

A. Collision
B. Collusion
C. Polymorphism
D. Escrow

Answer: A

NEW QUESTION 652
- (Exam Topic 6)
Name two software tools used for OS guessing? (Choose two.)

A. Nmap
B. Snadboy
C. Queso
D. UserInfo
E. NetBus

Answer: AC

NEW QUESTION 655
- (Exam Topic 6)
Which of the following is designed to verify and authenticate individuals taking part in a data exchange within an enterprise?

A. SOA
B. Single-Sign On
C. PKI
D. Biometrics

Answer: C

NEW QUESTION 656
- (Exam Topic 6)
A possibly malicious sequence of packets that were sent to a web server has been captured by an Intrusion Detection System (IDS) and was saved to a PCAP file. As a network administrator, you need to determine whether this packets are indeed malicious. What tool are you going to use?

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

Answer: C

NEW QUESTION 657
- (Exam Topic 6)
Knowing the nature of backup tapes, which of the following is the MOST RECOMMENDED way of storing backup tapes?

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

Answer: C

NEW QUESTION 661
- (Exam Topic 6)
A recent security audit revealed that there were indeed several occasions that the company’s network was breached. After investigating, you discover that your IDS is not configured properly and therefore is unable to trigger alarms when needed. What type of alert is the IDS giving?

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

Answer: B

NEW QUESTION 663
- (Exam Topic 6)
The following are types of Bluetooth attack EXCEPT ?

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

Answer: D

NEW QUESTION 664
- (Exam Topic 6)
Jack was attempting to fingerprint all machines in the network using the following Nmap syntax: invictus@victim_server:~$ nmap -T4 -0 10.10.0.0/24
TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx. QUITTING! Obviously, it is not going through. What is the issue here?

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

Answer: A

NEW QUESTION 667
- (Exam Topic 6)
What are two things that are possible when scanning UDP ports? (Choose two.)

A. A reset will be returned
B. An ICMP message will be returned
C. The four-way handshake will not be completed
D. An RFC 1294 message will be returned
E. Nothing

Answer: BE

NEW QUESTION 670
- (Exam Topic 6)
What is the best Nmap command to use when you want to list all devices in the same network quickly after you successfully identified a server whose IP address is 10.10.0.5?

A. nmap -T4 -F 10.10.0.0/24
B. nmap -T4 -q 10.10.0.0/24
C. nmap -T4 -O 10.10.0.0/24
D. nmap -T4 -r 10.10.1.0/24

Answer: A

NEW QUESTION 673
- (Exam Topic 6)
One of the Forbes 500 companies has been subjected to a large scale attack. You are one of the shortlisted pen testers that they may hire. During the interview with the CIO, he emphasized that he wants to totally eliminate all risks. What is one of the first things you should do when hired?

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

Answer: C

NEW QUESTION 674
- (Exam Topic 6)
You’ve just discovered a server that is currently active within the same network with the machine you recently compromised. You ping it but it did not respond. What could be the case?

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

Answer: C

NEW QUESTION 678
- (Exam Topic 6)
While doing a Black box pen test via the TCP port (80), you noticed that the traffic gets blocked when you tried to pass IRC traffic from a web enabled host. However, you also noticed that outbound HTTP traffic is being allowed. What type of firewall is being utilized for the outbound traffic?

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

Answer: B

NEW QUESTION 679
- (Exam Topic 6)
What is the approximate cost of replacement and recovery operation per year of a hard drive that has a value of $300 given that the technician who charges $10/hr would need 10 hours to restore OS and Software and needs further 4 hours to restore the database from the last backup to the new hard disk? Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%).

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

Answer: D

NEW QUESTION 680
- (Exam Topic 7)
Every company needs a formal written document which spells out to employees precisely what they are allowed to use the company's systems for, what is prohibited, and what will happen to them if they break the rules. Two printed copies of the policy should be given to every employee as soon as possible after they join the organization. The employee should be asked to sign one copy, which should be safely filed by the company. No one should be allowed to use the company's computer systems until they have signed the policy in acceptance of its terms.
What is this document called?

A. Information Audit Policy (IAP)
B. Information Security Policy (ISP)
C. Penetration Testing Policy (PTP)
D. Company Compliance Policy (CCP)

Answer: B

NEW QUESTION 685
- (Exam Topic 7)
What is the proper response for a NULL scan if the port is open?

A. SYN
B. ACK
C. FIN
D. PSH
E. RST
F. No response

Answer: F

NEW QUESTION 686
- (Exam Topic 7)
Bob is doing a password assessment for one of his clients. Bob suspects that security policies are not in place. He also suspects that weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weaknesses and key loggers.
Which of the following options best represents the means that Bob can adopt to retrieve passwords from his clients hosts and servers?

A. Hardware, Software, and Sniffing.
B. Hardware and Software Keyloggers.
C. Passwords are always best obtained using Hardware key loggers.
D. Software only, they are the most effective.

Answer: A

NEW QUESTION 687
- (Exam Topic 7)
Which of the following statements about a zone transfer is correct? (Choose three.)

A. A zone transfer is accomplished with the DNS
B. A zone transfer is accomplished with the nslookup service
C. A zone transfer passes all zone information that a DNS server maintains
D. A zone transfer passes all zone information that a nslookup server maintains
E. A zone transfer can be prevented by blocking all inbound TCP port 53 connections
F. Zone transfers cannot occur on the Internet

Answer: ACE

NEW QUESTION 691
- (Exam Topic 7)
How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?

A. There is no way to tell because a hash cannot be reversed
B. The right most portion of the hash is always the same
C. The hash always starts with AB923D
D. The left most portion of the hash is always the same
E. A portion of the hash will be all 0's

Answer: B

NEW QUESTION 696
- (Exam Topic 7)
In the context of Windows Security, what is a 'null' user?

A. A user that has no skills
B. An account that has been suspended by the admin
C. A pseudo account that has no username and password
D. A pseudo account that was created for security administration purpose

Answer: C

NEW QUESTION 697
- (Exam Topic 7)
What did the following commands determine?

```
C: user2sid \earth guest
S-1-5-21-343818398-789336058-1343024091-501
C:sid2user 5 21 343818398 789336058 1343024091 500
Name is Joe
Domain is EARTH
```

A. That the Joe account has a SID of 500
B. These commands demonstrate that the guest account has NOT been disabled
C. These commands demonstrate that the guest account has been disabled
D. That the true administrator is Joe
E. Issued alone, these commands prove nothing

Answer: D

NEW QUESTION 698
- (Exam Topic 7)
An LDAP directory can be used to store information similar to a SQL database. LDAP uses a database structure instead of SQL's structure. Because of this, LDAP has difficulty representing many-to-one relationships.

A. Relational, Hierarchical
B. Strict, Abstract
C. Hierarchical, Relational
D. Simple, Complex

Answer: C

NEW QUESTION 703
- (Exam Topic 7)
Eric has discovered a fantastic package of tools named Dsniff on the Internet. He has learnt to use these tools in his lab and is now ready for real world exploitation. He was able to effectively intercept communications between the two entities and establish credentials with both sides of the connections. The two remote ends of the communication never notice that Eric is relaying the information between the two. What would you call this attack?

A. Interceptor
B. Man-in-the-middle
C. ARP Proxy
D. Poisoning Attack

Answer: B

NEW QUESTION 705
- (Exam Topic 7)
One of your team members has asked you to analyze the following SOA record. What is the version? Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.) (Choose four.)

A. 200303028
B. 3600
C. 604800
D. 2400
E. 60
F. 4800

Answer: A

NEW QUESTION 706
.....

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