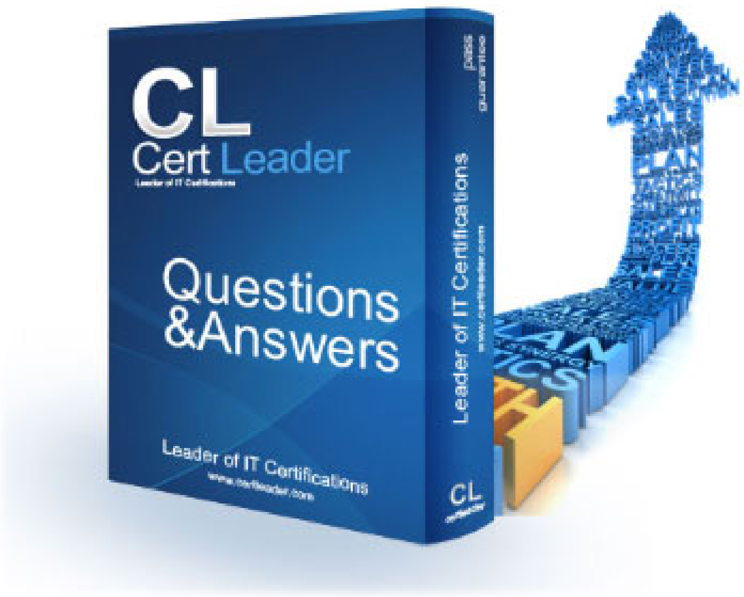
312-50v10 Dumps

Certified Ethical Hacker v10

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



NEW QUESTION 1
- (Exam Topic 1)
What does the -oX flag do in an Nmap scan?

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

Answer: D

NEW QUESTION 2
- (Exam Topic 1)
Chandler works as a pen-tester in an IT-firm in New York. As a part of detecting viruses in the systems, he uses a detection method where the anti-virus executes the malicious codes on a virtual machine to simulate CPU and memory activities.
Which type of virus detection method did Chandler use in this context?

A. Heuristic Analysis
B. Code Emulation
C. Integrity checking
D. Scanning

Answer: B

NEW QUESTION 3
- (Exam Topic 1)
Which of the following cryptography attack is an understatement for the extraction of cryptographic secrets
the password to an encrypted file) from a person by a coercion or torture?

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

Answer: D

NEW QUESTION 4
- (Exam Topic 1)
If an attacker uses the command SELECT*FROM user WHERE name = ‘x’ AND userid IS NULL; --‘; which type of SQL injection attack is the attacker performing?

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

Answer: D

NEW QUESTION 5
- (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 6
- (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 7

- (Exam Topic 1)
Based on the below log, which of the following sentences are true?
Mar 1, 2016, 7:33:28 AM 10.240.250.23 – 54373 10.249.253.15 – 22 tcp_ip

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

Answer: C

NEW QUESTION 8
- (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 9
- (Exam Topic 1)
Which of the following scanning method splits the TCP header into several packets and makes it difficult for packet filters to detect the purpose of the packet?

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

Answer: B

NEW QUESTION 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 10
- (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 11
- (Exam Topic 1)
DHCP snooping is a great solution to prevent rogue DHCP servers on your network. Which security feature on switches leverages the DHCP snooping database to help prevent man-in-the-middle attacks?

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

Answer: C

NEW QUESTION 12
- (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 15
- (Exam Topic 1)
The collection of potentially actionable, overt, and publicly available information is known as

A. Open-source intelligence
B. Human intelligence
C. Social intelligence
D. Real intelligence

Answer: A

NEW QUESTION 16
- (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 18
- (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 23
- (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 27
- (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 35
- (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 40
- (Exam Topic 1)
Identify the web application attack where the attackers exploit vulnerabilities in dynamically generated web pages to inject client-side script into web pages viewed by other users.

A. SQL injection attack
B. Cross-Site Scripting (XSS)
C. LDAP Injection attack
D. Cross-Site Request Forgery (CSRF)

Answer: B

NEW QUESTION 44
- (Exam Topic 1)
DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed.
What command is used to determine if the entry is present in DNS cache?

A. nslookup -fullrecursive update.antivirus.com
B. dnsnooping –rt update.antivirus.com
C. nslookup -norecursive update.antivirus.com
D. dns --snoop update.antivirus.com

Answer: C

NEW QUESTION 47
- (Exam Topic 1)
An attacker scans a host with the below command. Which three flags are set? (Choose three.)
#nmap –sX host.domain.com

A. This is ACK sca
B. ACK flag is set
C. This is Xmas sca
D. SYN and ACK flags are set
E. This is Xmas sca
F. URG, PUSH and FIN are set
G. This is SYN sca
H. SYN flag is set

Answer: C

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 54
- (Exam Topic 1)
Firewalls are the software or hardware systems that are able to control and monitor the traffic coming in and out the target network based on pre-defined set of rules.
Which of the following types of firewalls can protect against SQL injection attacks?

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

Answer: D

NEW QUESTION 59
- (Exam Topic 1)
What is the purpose of a demilitarized zone on a network?

A. To scan all traffic coming through the DMZ to the internal network
B. To only provide direct access to the nodes within the DMZ and protect the network behind it

C. To provide a place to put the honeypot
D. To contain the network devices you wish to protect

Answer: B

NEW QUESTION 62
- (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 63
- (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 64
- (Exam Topic 1)
How is the public key distributed in an orderly, controlled fashion so that the users can be sure of the sender's identity?

A. Hash value
B. Private key
C. Digital signature
D. Digital certificate

Answer: D

NEW QUESTION 66
- (Exam Topic 1)
Why containers are less secure that virtual machines?

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

Answer: A

NEW QUESTION 70
- (Exam Topic 1)
An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections.
When users accessed any page, the applet ran and exploited many machines. Which one of the following tools the hacker probably used to inject HTML code?

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

Answer: B

NEW QUESTION 74
- (Exam Topic 1)
You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity, what tool would you most likely select?

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

Answer: D

NEW QUESTION 75

- (Exam Topic 1)
You need to deploy a new web-based software package for your organization. The package requires three separate servers and needs to be available on the Internet. What is the recommended architecture in terms of server placement?

A. All three servers need to be placed internally
B. A web server facing the Internet, an application server on the internal network, a database server on the internal network
C. A web server and the database server facing the Internet, an application server on the internal network
D. All three servers need to face the Internet so that they can communicate between themselves

Answer: B

NEW QUESTION 77
- (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 80
- (Exam Topic 1)
The network team has well-established procedures to follow for creating new rules on the firewall. This includes having approval from a manager prior to implementing any new rules. While reviewing the firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it. What would be a good step to have in the procedures for a situation like this?

A. Have the network team document the reason why the rule was implemented without prior manager approval.
B. Monitor all traffic using the firewall rule until a manager can approve it.
C. Do not roll back the firewall rule as the business may be relying upon it, but try to get manager approval as soon as possible.
D. Immediately roll back the firewall rule until a manager can approve it

Answer: D

NEW QUESTION 85
- (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 90
- (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 93
- (Exam Topic 1)
A pen tester is configuring a Windows laptop for a test. In setting up Wireshark, what river and library are required to allow the NIC to work in promiscuous mode?

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

Answer: D

NEW QUESTION 96
- (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 97
- (Exam Topic 1)
Cross-site request forgery involves:

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

Answer: C

NEW QUESTION 99
- (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 102
- (Exam Topic 1)
Which of the following Bluetooth hacking techniques does an attacker use to send messages to users without the recipient's consent, similar to email spamming?

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

Answer: D

NEW QUESTION 104
- (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 107
- (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 109
- (Exam Topic 1)
What type of vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?

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

Answer: A

NEW QUESTION 112
- (Exam Topic 2)
The use of technologies like IPSec can help guarantee the following: authenticity, integrity, confidentiality and

A. non-repudiation.
B. operability.
C. security.
D. usability.

Answer: A

NEW QUESTION 113
- (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 115
- (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 of the following tools will scan a network to perform vulnerability checks and compliance auditing?

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

Answer: C

NEW QUESTION 125
- (Exam Topic 2)
On a Linux device, which of the following commands will start the Nessus client in the background so that the Nessus server can be configured?

A. nessus +
B. nessus *s
C. nessus &
D. nessus -d

Answer: C

NEW QUESTION 126
- (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 130
- (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 133
- (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 135
- (Exam Topic 2)
What are the three types of authentication?

A. Something you: know, remember, prove
B. Something you: have, know, are
C. Something you: show, prove, are
D. Something you: show, have, prove

Answer: B

NEW QUESTION 140
- (Exam Topic 2)
Which of the following is an application that requires a host application for replication?

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

Answer: D

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

NEW QUESTION 143
- (Exam Topic 2)
The network administrator for a company is setting up a website with e-commerce capabilities. Packet sniffing is a concern because credit card information will be sent electronically over the Internet. Customers visiting the site will need to encrypt the data with HTTPS. Which type of certificate is used to encrypt and decrypt the data?

A. Asymmetric
B. Confidential
C. Symmetric
D. Non-confidential

Answer: A

NEW QUESTION 145
- (Exam Topic 2)
Which of the following resources does NMAP need to be used as a basic vulnerability scanner covering several vectors like SMB, HTTP and FTP?

A. Metasploit scripting engine
B. Nessus scripting engine
C. NMAP scripting engine
D. SAINT scripting engine

Answer: C

NEW QUESTION 146
- (Exam Topic 2)
A tester has been hired to do a web application security test. The tester notices that the site is dynamic and must make use of a back end database.
In order for the tester to see if SQL injection is possible, what is the first character that the tester should use to attempt breaking a valid SQL request?

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

Answer: B

NEW QUESTION 150

- (Exam Topic 2)
A person approaches a network administrator and wants advice on how to send encrypted email from home. The end user does not want to have to pay for any license fees or manage server services. Which of the following is the most secure encryption protocol that the network administrator should recommend?

A. IP Security (IPSEC)
B. Multipurpose Internet Mail Extensions (MIME)
C. Pretty Good Privacy (PGP)
D. Hyper Text Transfer Protocol with Secure Socket Layer (HTTPS)

Answer: C

NEW QUESTION 151
- (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 152
- (Exam Topic 2)
Which protocol and port number might be needed in order to send log messages to a log analysis tool that resides behind a firewall?

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

Answer: C

NEW QUESTION 157
- (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 158
- (Exam Topic 2)
At a Windows Server command prompt, which command could be used to list the running services?

A. Sc query type= running
B. Sc query \\servername
C. Sc query
D. Sc config

Answer: C

NEW QUESTION 162
- (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 165
- (Exam Topic 2)
A hacker, who posed as a heating and air conditioning specialist, was able to install a sniffer program in a switched environment network. Which attack could the hacker use to sniff all of the packets in the network?

A. Fraggle
B. MAC Flood
C. Smurf
D. Tear Drop

Answer: B

NEW QUESTION 167
- (Exam Topic 2)
While conducting a penetration test, the tester determines that there is a firewall between the tester's machine and the target machine. The firewall is only monitoring TCP handshaking of packets at the session layer of the OSI model. Which type of firewall is the tester trying to traverse?

A. Packet filtering firewall
B. Application-level firewall
C. Circuit-level gateway firewall
D. Stateful multilayer inspection firewall

Answer: C

NEW QUESTION 171
- (Exam Topic 2)
Which results will be returned with the following Google search query? site:target.com -site:Marketing.target.com accounting

A. Results matching all words in the query
B. Results matching “accounting” in domain target.com but not on the site Marketing.target.com
C. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting
D. Results for matches on target.com and Marketing.target.com that include the word “accounting”

Answer: B

NEW QUESTION 172
- (Exam Topic 2)
Which type of intrusion detection system can monitor and alert on attacks, but cannot stop them?

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

Answer: B

NEW QUESTION 173
- (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 178
- (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 180
- (Exam Topic 2)
Which of the following describes the characteristics of a Boot Sector Virus?

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

Answer: B

Explanation:
A boot sector virus is a computer virus that infects a storage device's master boot record (MBR). The virus moves the boot sector to another location on the hard drive.
References: https://www.techopedia.com/definition/26655/boot-sector-virus

NEW QUESTION 181
- (Exam Topic 2)
A hacker is attempting to use nslookup to query Domain Name Service (DNS). The hacker uses the nslookup interactive mode for the search. Which command should the hacker type into the command shell to request the appropriate records?

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

Answer: C

NEW QUESTION 182
- (Exam Topic 2)
How can telnet be used to fingerprint a web server?

A. telnet webserverAddress 80HEAD / HTTP/1.0
B. telnet webserverAddress 80PUT / HTTP/1.0
C. telnet webserverAddress 80HEAD / HTTP/2.0
D. telnet webserverAddress 80PUT / HTTP/2.0

Answer: A

NEW QUESTION 184
- (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 185
- (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 190
- (Exam Topic 2)
What is the main reason the use of a stored biometric is vulnerable to an attack?

A. The digital representation of the biometric might not be unique, even if the physical characteristic is unique.
B. Authentication using a stored biometric compares a copy to a copy instead of the original to a copy.
C. A stored biometric is no longer "something you are" and instead becomes "something you have".
D. A stored biometric can be stolen and used by an attacker to impersonate the individual identified by the biometric.

Answer: D

NEW QUESTION 193
- (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 197
- (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 202
- (Exam Topic 2)
A company has five different subnets: 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0 and 192.168.5.0.
How can NMAP be used to scan these adjacent Class C networks?

A. NMAP -P 192.168.1-5.
B. NMAP -P 192.168.0.0/16
C. NMAP -P 192.168.1.0,2.0,3.0,4.0,5.0
D. NMAP -P 192.168.1/17

Answer: A

NEW QUESTION 207
- (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 212
- (Exam Topic 2)
Which tool can be used to silently copy files from USB devices?

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

Answer: B

NEW QUESTION 216
- (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 218
- (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 222
- (Exam Topic 2)
An NMAP scan of a server shows port 25 is open. What risk could this pose?

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

Answer: D

NEW QUESTION 225
- (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 227
- (Exam Topic 2)
Which of the following does proper basic configuration of snort as a network intrusion detection system require?

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

Answer: A

NEW QUESTION 232
- (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 237
- (Exam Topic 2)
During a penetration test, the tester conducts an ACK scan using NMAP against the external interface of the DMZ firewall. NMAP reports that port 80 is unfiltered. Based on this response, which type of packet inspection is the firewall conducting?

A. Host
B. Stateful
C. Stateless
D. Application

Answer: C

NEW QUESTION 242
- (Exam Topic 2)
How does an operating system protect the passwords used for account logins?

A. The operating system performs a one-way hash of the passwords.
B. The operating system stores the passwords in a secret file that users cannot find.
C. The operating system encrypts the passwords, and decrypts them when needed.
D. The operating system stores all passwords in a protected segment of non-volatile memory.

Answer: A

NEW QUESTION 243
- (Exam Topic 2)
What is the name of the international standard that establishes a baseline level of confidence in the security functionality of IT products by providing a set of requirements for evaluation?

A. Blue Book
B. ISO 26029
C. Common Criteria
D. The Wassenaar Agreement

Answer: C

NEW QUESTION 246
- (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 250
- (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 255
- (Exam Topic 2)
Which of the following business challenges could be solved by using a vulnerability scanner?

A. Auditors want to discover if all systems are following a standard naming convention.
B. A web server was compromised and management needs to know if any further systems were compromised.
C. There is an emergency need to remove administrator access from multiple machines for an employee that quit.
D. There is a monthly requirement to test corporate compliance with host application usage and security policies.

Answer: D

NEW QUESTION 256
- (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 261
- (Exam Topic 2)
Windows file servers commonly hold sensitive files, databases, passwords and more. Which of the following choices would be a common vulnerability that usually exposes them?

A. Cross-site scripting
B. SQL injection
C. Missing patches
D. CRLF injection

Answer: C

NEW QUESTION 265
- (Exam Topic 2)
During a penetration test, a tester finds a target that is running MS SQL 2000 with default credentials. The tester assumes that the service is running with Local System account. How can this weakness be exploited to access the system?

A. Using the Metasploit psexec module setting the SA / Admin credential
B. Invoking the stored procedure xp_shell to spawn a Windows command shell
C. Invoking the stored procedure cmd_shell to spawn a Windows command shell
D. Invoking the stored procedure xp_cmdshell to spawn a Windows command shell

Answer: D

NEW QUESTION 270
- (Exam Topic 2)
Which of the following programming languages is most vulnerable to buffer overflow attacks?

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

Answer: B

NEW QUESTION 274
- (Exam Topic 2)
Which of the following is a detective control?

A. Smart card authentication

B. Security policy
C. Audit trail
D. Continuity of operations plan

Answer: C

NEW QUESTION 279
- (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 283
- (Exam Topic 2)
An engineer is learning to write exploits in C++ and is using the exploit tool Backtrack. The engineer wants to compile the newest C++ exploit and name it calc.exe. Which command would the engineer use to accomplish this?

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

Answer: A

NEW QUESTION 287
- (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 292
- (Exam Topic 2)
A company has hired a security administrator to maintain and administer Linux and Windows-based systems. Written in the nightly report file is the following:
Firewall log files are at the expected value of 4 MB. The current time is 12am. Exactly two hours later the size has decreased considerably. Another hour goes by and the log files have shrunk in size again.
Which of the following actions should the security administrator take?

A. Log the event as suspicious activity and report this behavior to the incident response team immediately.
B. Log the event as suspicious activity, call a manager, and report this as soon as possible.
C. Run an anti-virus scan because it is likely the system is infected by malware.
D. Log the event as suspicious activity, continue to investigate, and act according to the site's security policy.

Answer: D

NEW QUESTION 296
- (Exam Topic 2)
Pentest results indicate that voice over IP traffic is traversing a network. Which of the following tools will decode a packet capture and extract the voice conversations?

A. Cain
B. John the Ripper
C. Nikto
D. Hping

Answer: A

NEW QUESTION 298
- (Exam Topic 2)
ICMP ping and ping sweeps are used to check for active systems and to check

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

Answer: A

NEW QUESTION 299
- (Exam Topic 2)
During a penetration test, a tester finds that the web application being analyzed is vulnerable to Cross Site Scripting (XSS). Which of the following conditions must be met to exploit this vulnerability?

A. The web application does not have the secure flag set.
B. The session cookies do not have the HttpOnly flag set.
C. The victim user should not have an endpoint security solution.
D. The victim's browser must have ActiveX technology enabled.

Answer: B

NEW QUESTION 303
- (Exam Topic 2)
One way to defeat a multi-level security solution is to leak data via

A. a bypass regulator.
B. steganography.
C. a covert channel.
D. asymmetric routing.

Answer: C

NEW QUESTION 306
- (Exam Topic 2)
A penetration tester is hired to do a risk assessment of a company's DMZ. The rules of engagement states that the penetration test be done from an external IP address with no prior knowledge of the internal IT systems. What kind of test is being performed?

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

Answer: D

NEW QUESTION 311
- (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 312
- (Exam Topic 2)
A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

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

Answer: B

NEW QUESTION 317
- (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 318

- (Exam Topic 2)
A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the corporate network. What tool should the analyst use to perform a Blackjacking attack?

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

Answer: B

Explanation:
Blackberry users warned of hacking tool threat.
Users have been warned that the security of Blackberry wireless e-mail devices is at risk due to the availability this week of a new hacking tool. Secure Computing Corporation said businesses that have installed Blackberry servers behind their gateway security devices could be vulnerable to a hacking attack from a tool call BBProxy.
References:
http://www.computerweekly.com/news/2240062112/Technology-news-in-brief

NEW QUESTION 321
- (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 323
- (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 327
- (Exam Topic 2)
Which of the following is a symmetric cryptographic standard?

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

Answer: D

NEW QUESTION 332
- (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 334
- (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 338
- (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 342
- (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 346
- (Exam Topic 2)
While performing data validation of web content, a security technician is required to restrict malicious input. Which of the following processes is an efficient way of restricting malicious input?

A. Validate web content input for query strings.
B. Validate web content input with scanning tools.
C. Validate web content input for type, length, and range.
D. Validate web content input for extraneous queries.

Answer: C

NEW QUESTION 347
- (Exam Topic 2)
What is the main advantage that a network-based IDS/IPS system has over a host-based solution?

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

Answer: A

NEW QUESTION 350
- (Exam Topic 2)
Which of the following identifies the three modes in which Snort can be configured to run?

A. Sniffer, Packet Logger, and Network Intrusion Detection System
B. Sniffer, Network Intrusion Detection System, and Host Intrusion Detection System
C. Sniffer, Host Intrusion Prevention System, and Network Intrusion Prevention System
D. Sniffer, Packet Logger, and Host Intrusion Prevention System

Answer: A

NEW QUESTION 354
- (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 359
- (Exam Topic 2)
A covert channel is a channel that

A. transfers information over, within a computer system, or network that is outside of the security policy.
B. transfers information over, within a computer system, or network that is within the security policy.
C. transfers information via a communication path within a computer system, or network for transfer of data.
D. transfers information over, within a computer system, or network that is encrypted.

Answer: A

NEW QUESTION 364
- (Exam Topic 3)
When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?

A. At least once a year and after any significant upgrade or modification
B. At least once every three years or after any significant upgrade or modification
C. At least twice a year or after any significant upgrade or modification
D. At least once every two years and after any significant upgrade or modification

Answer: A

NEW QUESTION 365
- (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 370
- (Exam Topic 3)
A certified ethical hacker (CEH) is approached by a friend who believes her husband is cheating. She offers to pay to break into her husband's email account in order to find proof so she can take him to court. What is the ethical response?

A. Say no; the friend is not the owner of the account.
B. Say yes; the friend needs help to gather evidence.
C. Say yes; do the job for free.
D. Say no; make sure that the friend knows the risk she’s asking the CEH to take.

Answer: A

NEW QUESTION 375
- (Exam Topic 3)
A computer technician is using a new version of a word processing software package when it is discovered that a special sequence of characters causes the entire computer to crash. The technician researches the bug and discovers that no one else experienced the problem. What is the appropriate next step?

A. Ignore the problem completely and let someone else deal with it.
B. Create a document that will crash the computer when opened and send it to friends.
C. Find an underground bulletin board and attempt to sell the bug to the highest bidder.
D. Notify the vendor of the bug and do not disclose it until the vendor gets a chance to issue a fix.

Answer: D

NEW QUESTION 377
- (Exam Topic 3)
Which of the following guidelines or standards is associated with the credit card industry?

A. Control Objectives for Information and Related Technology (COBIT)
B. Sarbanes-Oxley Act (SOX)
C. Health Insurance Portability and Accountability Act (HIPAA)
D. Payment Card Industry Data Security Standards (PCI DSS)

Answer: D

NEW QUESTION 378
- (Exam Topic 3)
How can a policy help improve an employee's security awareness?

A. By implementing written security procedures, enabling employee security training, and promoting the benefits of security
B. By using informal networks of communication, establishing secret passing procedures, and immediately terminating employees
C. By sharing security secrets with employees, enabling employees to share secrets, and establishing a consultative help line
D. By decreasing an employee's vacation time, addressing ad-hoc employment clauses, and ensuring that managers know employee strengths

Answer: A

NEW QUESTION 379
- (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 380
- (Exam Topic 3)
Which of the following network attacks relies on sending an abnormally large packet size that exceeds TCP/IP specifications?

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

Answer: A

NEW QUESTION 381
- (Exam Topic 3)
Which of the following is a common Service Oriented Architecture (SOA) vulnerability?

A. Cross-site scripting
B. SQL injection
C. VPath injection
D. XML denial of service issues

Answer: D

NEW QUESTION 385
- (Exam Topic 3)
Which of the following is an advantage of utilizing security testing methodologies to conduct a security audit?

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

Answer: A

NEW QUESTION 387
- (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 391
- (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 392
- (Exam Topic 3)
Which security strategy requires using several, varying methods to protect IT systems against attacks?

A. Defense in depth
B. Three-way handshake
C. Covert channels
D. Exponential backoff algorithm

Answer: A

NEW QUESTION 393
- (Exam Topic 3)
Which of the following defines the role of a root Certificate Authority (CA) in a Public Key Infrastructure (PKI)?

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

Answer: C

NEW QUESTION 396
- (Exam Topic 3)
Which initial procedure should an ethical hacker perform after being brought into an organization?

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

Answer: C

NEW QUESTION 400
- (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 401
- (Exam Topic 3)
In the OSI model, where does PPTP encryption take place?

A. Transport layer
B. Application layer
C. Data link layer
D. Network layer

Answer: C

NEW QUESTION 402
- (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 406
- (Exam Topic 3)
A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?

A. The gateway is not routing to a public IP address.
B. The computer is using an invalid IP address.
C. The gateway and the computer are not on the same network.
D. The computer is not using a private IP address.

Answer: A

NEW QUESTION 411
- (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 413
- (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 416
- (Exam Topic 3)
The intrusion detection system at a software development company suddenly generates multiple alerts regarding attacks against the company's external webserver, VPN concentrator, and DNS servers. What should the security team do to determine which alerts to check first?

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

Answer: C

NEW QUESTION 417
- (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 422
- (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 424
- (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 426
- (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 430
- (Exam Topic 3)
Which statement best describes a server type under an N-tier architecture?

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

Answer: C

NEW QUESTION 435
- (Exam Topic 3)
What is the primary drawback to using advanced encryption standard (AES) algorithm with a 256 bit key to share sensitive data?

A. Due to the key size, the time it will take to encrypt and decrypt the message hinders efficient communication.
B. To get messaging programs to function with this algorithm requires complex configurations.
C. It has been proven to be a weak cipher; therefore, should not be trusted to protect sensitive data.
D. It is a symmetric key algorithm, meaning each recipient must receive the key through a different channel than the message.

Answer: D

NEW QUESTION 440
- (Exam Topic 3)
Which type of security document is written with specific step-by-step details?

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

Answer: B

NEW QUESTION 442
- (Exam Topic 3)
A certified ethical hacker (CEH) completed a penetration test of the main headquarters of a company almost two months ago, but has yet to get paid. The customer is suffering from financial problems, and the CEH is worried that the company will go out of business and end up not paying. What actions should the CEH take?

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

Answer: B

NEW QUESTION 447
- (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 451
- (Exam Topic 3)
Which of the following is an example of IP spoofing?

A. SQL injections
B. Man-in-the-middle
C. Cross-site scripting
D. ARP poisoning

Answer: B

NEW QUESTION 453
- (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 455
- (Exam Topic 3)
Which cipher encrypts the plain text digit (bit or byte) one by one?

A. Classical cipher
B. Block cipher
C. Modern cipher
D. Stream cipher

Answer: D

NEW QUESTION 457
- (Exam Topic 4)
This international organization regulates billions of transactions daily and provides security guidelines to protect personally identifiable information (PII). These security controls provide a baseline and prevent low-level hackers sometimes known as script kiddies from causing a data breach.
Which of the following organizations is being described?

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

Answer: A

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

NEW QUESTION 460
- (Exam Topic 4)
Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?

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

Answer: A

Explanation:
There are two main types of biometric identifiers:
Examples of physiological characteristics used for biometric authentication include fingerprints; DNA; face, hand, retina or ear features; and odor. Behavioral characteristics are related to the pattern of the behavior of a person, such as typing rhythm, gait, gestures and voice.
References:
http://searchsecurity.techtarget.com/definition/biometrics

NEW QUESTION 465
- (Exam Topic 4)
You are performing information gathering for an important penetration test. You have found pdf, doc, and images in your objective. You decide to extract metadata from these files and analyze it.
What tool will help you with the task?

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

Answer: A

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

NEW QUESTION 468
- (Exam Topic 4)
You've just been hired to perform a pen test on an organization that has been subjected to a large-scale attack. The CIO is concerned with mitigating threats and vulnerabilities to totally eliminate risk.
What is one of the first things you should do when given the job?

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

Answer: A

Explanation:
The goals of penetration tests are:
References: https://en.wikipedia.org/wiki/Penetration_test

NEW QUESTION 470
- (Exam Topic 4)
Perspective clients want to see sample reports from previous penetration tests. What should you do next?

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

Answer: A

Explanation:
Penetration tests data should not be disclosed to third parties.

NEW QUESTION 473
- (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 476
- (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 481
- (Exam Topic 4)
When you are collecting information to perform a data analysis, Google commands are very useful to find sensitive information and files. These files may contain information about passwords, system functions, or documentation.
What command will help you to search files using Google as a search engine?

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

Answer: A

Explanation:
If you include site: in your query, Google will restrict your search results to the site or domain you specify. If you include filetype:suffix in your query, Google will restrict the results to pages whose names end in
suffix. For example, [web page evaluation checklist filetype:pdf] will return Adobe Acrobat pdf files that match the terms “web,” “page,” “evaluation,” and

"checklist."
References:
http://www.googleguide.com/advanced_operators_reference.html

NEW QUESTION 482
- (Exam Topic 4)
A common cryptographical tool is the use of XOR. XOR the following binary values:
10110001
00111010

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

Answer: A

Explanation:
The XOR gate is a digital logic gate that implements an exclusive or; that is, a true output (1/HIGH) results if one, and only one, of the inputs to the gate is true. If both inputs are false (0/LOW) or both are true, a false output results. XOR represents the inequality function, i.e., the output is true if the inputs are not alike otherwise the output is false. A way to remember XOR is "one or the other but not both".
References: https://en.wikipedia.org/wiki/XOR_gate

NEW QUESTION 485
- (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 486
- (Exam Topic 4)
You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine.
What wireshark filter will show the connections from the snort machine to kiwi syslog machine?

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

Answer: A

Explanation:
We need to configure destination port at destination ip. The destination ip is 192.168.0.150, where the kiwi syslog is installed.
References: https://wiki.wireshark.org/DisplayFilters

NEW QUESTION 488
- (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 492
- (Exam Topic 4)
You have successfully compromised a machine on the network and found a server that is alive on the same network. You tried to ping it but you didn't get any response back.
What is happening?

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

Answer: A

Explanation:
The ping utility is implemented using the ICMP "Echo request" and "Echo reply" messages.
Note: The Internet Control Message Protocol (ICMP) is one of the main protocols of the internet protocol suite. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.
References: https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

NEW QUESTION 495
- (Exam Topic 4)
During a blackbox pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded.
What type of firewall is inspecting outbound traffic?

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

Answer: A

Explanation:
An application firewall is an enhanced firewall that limits access by applications to the operating system (OS) of a computer. Conventional firewalls merely control the flow of data to and from the central processing unit (CPU), examining each packet and determining whether or not to forward it toward a particular destination. An application firewall offers additional protection by controlling the execution of files or the handling of data by specific applications.
References:
http://searchsoftwarequality.techtarget.com/definition/application-firewall

NEW QUESTION 500
- (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 504
- (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 507
- (Exam Topic 4)
This asymmetry cipher is based on factoring the product of two large prime numbers. What cipher is described above?

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

Answer: A

Explanation:
RSA is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.
Note: A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message.
References: https://en.wikipedia.org/wiki/RSA_(cryptosystem)

NEW QUESTION 510
- (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 513
- (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 514
- (Exam Topic 4)
You are using NMAP to resolve domain names into IP addresses for a ping sweep later.
Which of the following commands looks for IP addresses?

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

Answer: A

Explanation:
The A record is an Address record. It returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host.
References: https://en.wikipedia.org/wiki/List_of_DNS_record_types

NEW QUESTION 515
- (Exam Topic 4)
This phase will increase the odds of success in later phases of the penetration test. It is also the very first step in Information Gathering, and it will tell you what the "landscape" looks like.
What is the most important phase of ethical hacking in which you need to spend a considerable amount of time?

A. footprinting
B. network mapping
C. gaining access
D. escalating privileges

Answer: A

Explanation:
Footprinting is a first step that a penetration tester used to evaluate the security of any IT infrastructure, footprinting means to gather the maximum information about the computer system or a network and about the devices that are attached to this network.

References:
http://www.ehacking.net/2011/02/footprinting-first-step-of-ethical.html

NEW QUESTION 516
- (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 520
- (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 522
- (Exam Topic 4)
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

Explanation:
The OSI layer 2 is where packet sniffers collect their data. References: https://en.wikipedia.org/wiki/Ethernet_frame

NEW QUESTION 527
- (Exam Topic 4)
This tool is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the PTW attack, thus making the attack much faster compared to other WEP cracking tools.
Which of the following tools is being described?

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

Answer: A

Explanation:
Aircrack-ng is a complete suite of tools to assess WiFi network security.
The default cracking method of Aircrack-ng is PTW, but Aircrack-ng can also use the FMS/KoreK method, which incorporates various statistical attacks to discover the WEP key and uses these in combination with brute forcing.
References:
http://www.aircrack-ng.org/doku.php?id=aircrack-ng

NEW QUESTION 529
- (Exam Topic 4)
Initiating an attack against targeted businesses and organizations, threat actors compromise a carefully selected website by inserting an exploit resulting in malware infection. The attackers run exploits on well-known and trusted sites likely to be visited by their targeted victims. Aside from carefully choosing sites to compromise, these attacks are known to incorporate zero-day exploits that target unpatched vulnerabilities. Thus, the targeted entities are left with little or no defense against these exploits.
What type of attack is outlined in the scenario?

A. Watering Hole Attack

B. Heartbleed Attack
C. Shellshock Attack
D. Spear Phising Attack

Answer: A

Explanation:
Watering Hole is a computer attack strategy, in which the victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group gets infected.

NEW QUESTION 532
- (Exam Topic 4)
A regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server.
Based on this information, what should be one of your key recommendations to the bank?

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

Answer: A

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

NEW QUESTION 533
- (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 534
- (Exam Topic 4)
It is a kind of malware (malicious software) that criminals install on your computer so they can lock it from a remote location. This malware generates a pop-up window, webpage, or email warning from what looks like an official authority. It explains that your computer has been locked because of possible illegal activities on it and demands payment before you can access your files and programs again.
Which of the following terms best matches the definition?

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

Answer: A

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

NEW QUESTION 535
- (Exam Topic 4)
An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com", that the user is directed to a phishing site.
Which file does the attacker need to modify?

A. Hosts
B. Sudoers
C. Boot.ini
D. Networks

Answer: A

Explanation:
The hosts file is a computer file used by an operating system to map hostnames to IP addresses. The hosts file contains lines of text consisting of an IP address in the first text field followed by one or more host names.
References: https://en.wikipedia.org/wiki/Hosts_(file)

NEW QUESTION 540
- (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 545
- (Exam Topic 4)
You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email(boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network.
What testing method did you use?

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

Answer: A

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

NEW QUESTION 549
- (Exam Topic 4)
You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.
What is the best nmap command you will use?

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

Answer: A

Explanation:
command = nmap -T4 -F
description = This scan is faster than a normal scan because it uses the aggressive timing template and scans fewer ports.
References: https://svn.nmap.org/nmap/zenmap/share/zenmap/config/scan_profile.usp

NEW QUESTION 550
- (Exam Topic 4)
The network administrator contacts you and tells you that she noticed the temperature on the internal wireless router increases by more than 20% during weekend hours when the office was closed. She asks you to investigate the issue because she is busy dealing with a big conference and she doesn't have time to perform the task.
What tool can you use to view the network traffic being sent and received by the wireless router?

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

Answer: A

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

education.

NEW QUESTION 552
- (Exam Topic 4)
The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the central processing unit (CPU), rather than passing only the frames that the controller is intended to receive.
Which of the following is being described?

A. promiscuous mode
B. port forwarding
C. multi-cast mode
D. WEM

Answer: A

Explanation:
Promiscuous mode refers to the special mode of Ethernet hardware, in particular network interface cards (NICs), that allows a NIC to receive all traffic on the network, even if it is not addressed to this NIC. By default, a NIC ignores all traffic that is not addressed to it, which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a. MAC) of the device. While this makes perfect sense for networking, non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting.
References: https://www.tamos.com/htmlhelp/monitoring/

NEW QUESTION 554
- (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 556
- (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 560
- (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 564
- (Exam Topic 5)
Which of the following areas is considered a strength of symmetric key cryptography when compared with asymmetric algorithms?

A. Scalability

B. Speed
C. Key distribution
D. Security

Answer: B

NEW QUESTION 569
- (Exam Topic 5)
Which of the following is a protocol specifically designed for transporting event messages?

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

Answer: A

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

NEW QUESTION 570
- (Exam Topic 5)
Internet Protocol Security IPSec is actually a suite of protocols. Each protocol within the suite provides different functionality. Collective IPSec does everything except.

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

Answer: D

NEW QUESTION 571
- (Exam Topic 5)
The "gray box testing" methodology enforces what kind of restriction?

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

Answer: A

Explanation:
A black-box tester is unaware of the internal structure of the application to be tested, while a white-box tester has access to the internal structure of the application. A gray-box tester partially knows the internal structure, which includes access to the documentation of internal data structures as well as the algorithms used.
References: https://en.wikipedia.org/wiki/Gray_box_testing

NEW QUESTION 572
- (Exam Topic 5)
An IT employee got a call from one of our best customers. The caller wanted to know about the company's network infrastructure, systems, and team. New opportunities of integration are in sight for both company and customer. What should this employee do?

A. Since the company's policy is all about Customer Service, he/she will provide information.
B. Disregarding the call, the employee should hang up.
C. The employee should not provide any information without previous management authorization.
D. The employees can not provide any information; but, anyway, he/she will provide the name of the person in charge.

Answer: C

NEW QUESTION 573
- (Exam Topic 5)
To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security policies. Which one of the following tools would most likely be used in such an audit?

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

Answer: A

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

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

NEW QUESTION 577
- (Exam Topic 5)
A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.
What kind of Web application vulnerability likely exists in their software?

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

Answer: A

Explanation:
Many operators of particular web applications (e.g. forums and webmail) allow users to utilize a limited subset of HTML markup. When accepting HTML input from users (say, <b>very</b> large), output encoding (such as &lt;b&gt;very&lt;/b&gt; large) will not suffice since the user input needs to be rendered as HTML by the browser (so it shows as "very large", instead of "<b>very</b> large"). Stopping an XSS attack when accepting HTML input from users is much more complex in this situation. Untrusted HTML input must be run through an HTML sanitization engine to ensure that it does not contain cross-site scripting code.
References: https://en.wikipedia.org/wiki/Cross-site_scripting#Safely_validating_untrusted_HTML_input

NEW QUESTION 579
- (Exam Topic 5)
Craig received a report of all the computers on the network that showed all the missing patches and weak passwords. What type of software generated this report?

A. a port scanner
B. a vulnerability scanner
C. a virus scanner
D. a malware scanner

Answer: B

NEW QUESTION 582
- (Exam Topic 5)
What is the most common method to exploit the “Bash Bug” or “ShellShock" vulnerability?

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

Answer: A

Explanation:
Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell. One specific exploitation vector of the Shellshock bug is CGI-based web servers.
Note: When a web server uses the Common Gateway Interface (CGI) to handle a document request, it passes various details of the request to a handler program in the environment variable list. For example, the variable HTTP_USER_AGENT has a value that, in normal usage, identifies the program sending the request. If the request handler is a Bash script, or if it executes one for example using the system call, Bash will receive the environment variables passed by the server and will process them. This provides a means for an attacker to trigger the Shellshock vulnerability with a specially crafted server request.
References: https://en.wikipedia.org/wiki/Shellshock_(software_bug)#Specific_exploitation_vectors

NEW QUESTION 587
- (Exam Topic 5)
PGP, SSL, and IKE are all examples of which type of cryptography?

A. Public Key
B. Secret Key
C. Hash Algorithm
D. Digest

Answer: A

Explanation:
Public-key algorithms are fundamental security ingredients in cryptosystems, applications and protocols. They underpin various Internet standards, such as Secure Sockets Layer (SSL),Transport Layer Security (TLS), S/MIME, PGP, Internet Key Exchange (IKE or IKEv2), and GPG.
References: https://en.wikipedia.org/wiki/Public-key_cryptography

NEW QUESTION 590
- (Exam Topic 5)
An attacker is trying to redirect the traffic of a small office. That office is using their own mail server, DNS server and NTP server because of the importance of their job. The attacker gains access to the DNS server and redirects the direction www.google.com to his own IP address. Now when the employees of the office want to go to Google they are being redirected to the attacker machine. What is the name of this kind of attack?

A. ARP Poisoning
B. Smurf Attack

C. DNS spoofing
D. MAC Flooding

Answer: C

NEW QUESTION 595
- (Exam Topic 5)
In Risk Management, how is the term "likelihood" related to the concept of "threat?"

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

Answer: A

Explanation:
The ability to analyze the likelihood of threats within the organization is a critical step in building an effective security program. The process of assessing threat probability should be well defined and incorporated into a broader threat analysis process to be effective.
References:
http://www.mcafee.com/campaign/securitybattleground/resources/chapter5/whitepaper-on-assessing-threat-attac

NEW QUESTION 597
- (Exam Topic 5)
If executives are found liable for not properly protecting their company's assets and information systems, what type of law would apply in this situation?

A. Civil
B. International
C. Criminal
D. Common

Answer: A

NEW QUESTION 601
- (Exam Topic 5)
An attacker gains access to a Web server's database and displays the contents of the table that holds all of the names, passwords, and other user information. The attacker did this by entering information into the Web site's user login page that the software's designers did not expect to be entered. This is an example of what kind of software design problem?

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

Answer: A

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

NEW QUESTION 602
- (Exam Topic 5)
What two conditions must a digital signature meet?

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

Answer: A

NEW QUESTION 604
- (Exam Topic 5)
Seth is starting a penetration test from inside the network. He hasn't been given any information about the network. What type of test is he conducting?

A. Internal Whitebox
B. External, Whitebox
C. Internal, Blackbox
D. External, Blackbox

Answer: C

NEW QUESTION 609
- (Exam Topic 5)

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

A. Whisker
B. tcpsplice
C. Burp
D. Hydra

Answer: A

Explanation:
One basic technique is to split the attack payload into multiple small packets, so that the IDS must reassemble the packet stream to detect the attack. A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads. The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.
References: https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques#Fragmentation_and_small_packe

NEW QUESTION 611
- (Exam Topic 5)
Due to a slowdown of normal network operations, IT department decided to monitor internet traffic for all of the employees. From a legal stand point, what would be troublesome to take this kind of measure?

A. All of the employees would stop normal work activities
B. IT department would be telling employees who the boss is
C. Not informing the employees that they are going to be monitored could be an invasion of privacy.
D. The network could still experience traffic slow down.

Answer: C

NEW QUESTION 614
- (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 619
- (Exam Topic 5)
Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

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

Answer: A

Explanation:
tcptrace is a tool for analysis of TCP dump files. It can take as input the files produced by several popular packet-capture programs, including tcpdump/WinDump/Wireshark, snoop, EtherPeek, and Agilent NetMetrix.
References: https://en.wikipedia.org/wiki/Tcptrace

NEW QUESTION 621
- (Exam Topic 5)
If there is an Intrusion Detection System (IDS) in intranet, which port scanning technique cannot be used?

A. Spoof Scan
B. TCP Connect scan
C. TCP SYN
D. Idle Scan

Answer: C

NEW QUESTION 626
- (Exam Topic 5)
What is the correct process for the TCP three-way handshake connection establishment and connection termination?

A. Connection Establishment: FIN, ACK-FIN, ACKConnection Termination: SYN, SYN-ACK, ACK

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

Answer: D

NEW QUESTION 627
- (Exam Topic 5)
You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?

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

Answer: D

NEW QUESTION 630
- (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 635
- (Exam Topic 5)
The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124.
An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is: nmap 192.168.1.64/28.
Why he cannot see the servers?

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

Answer: C

NEW QUESTION 639
- (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 640
- (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 641
- (Exam Topic 5)
Which of the following is considered the best way to protect Personally Identifiable Information (PII) from Web application vulnerabilities?

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

Answer: A

Explanation:
As a matter of good practice any PII should be protected with strong encryption.
References: https://cuit.columbia.edu/cuit/it-security-practices/handling-personally-identifying-information

NEW QUESTION 642
- (Exam Topic 5)
Sid is a judge for a programming contest. Before the code reaches him it goes through a restricted OS and is tested there. If it passes, then it moves onto Sid. What is this middle step called?

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

Answer: A

NEW QUESTION 643
- (Exam Topic 5)
Attempting an injection attack on a web server based on responses to True/False questions is called which of the following?

A. Blind SQLi
B. DMS-specific SQLi
C. Classic SQLi
D. Compound SQLi

Answer: A

NEW QUESTION 648
- (Exam Topic 5)
When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best describes what it is meant by processing?

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

Answer: C

NEW QUESTION 651
- (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 655
- (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 658
- (Exam Topic 5)
Scenario:
What is the name of the attack which is mentioned in the scenario?

A. HTTP Parameter Pollution
B. HTML Injection
C. Session Fixation

D. ClickJacking Attack

Answer: D

NEW QUESTION 662
- (Exam Topic 5)
In order to have an anonymous Internet surf, which of the following is best choice?

A. Use SSL sites when entering personal information
B. Use Tor network with multi-node
C. Use shared WiFi
D. Use public VPN

Answer: B

NEW QUESTION 664
- (Exam Topic 5)
Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?

A. msfpayload
B. msfcli
C. msfencode
D. msfd

Answer: C

NEW QUESTION 668
- (Exam Topic 5)
Which of the following types of firewalls ensures that the packets are part of the established session?

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

Answer: A

Explanation:
A stateful firewall is a network firewall that tracks the operating state and characteristics of network connections traversing it. The firewall is configured to distinguish legitimate packets for different types of connections. Only packets matching a known active connection (session) are allowed to pass the firewall.
References: https://en.wikipedia.org/wiki/Stateful_firewall

NEW QUESTION 673
- (Exam Topic 5)
You're doing an internal security audit and you want to find out what ports are open on all the servers. What is the best way to find out?

A. Scan servers with Nmap
B. Physically go to each server
C. Scan servers with MBSA
D. Telent to every port on each server

Answer: A

NEW QUESTION 678
- (Exam Topic 5)
Which of the following is one of the most effective ways to prevent Cross-site Scripting (XSS) flaws in software applications?

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

Answer: A

Explanation:
Contextual output encoding/escaping could be used as the primary defense mechanism to stop Cross-site Scripting (XSS) attacks.
References:
https://en.wikipedia.org/wiki/Cross-site_scripting#Contextual_output_encoding.2Fescaping_of_string_input

NEW QUESTION 679
- (Exam Topic 5)
Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it begins to close.
What just happened?

A. Phishing

B. Whaling
C. Tailgating
D. Masquerading

Answer: C

NEW QUESTION 681
- (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 682
- (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 686
......