EC-Council

Exam Questions 312-50v10

Certified Ethical Hacker v10

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

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

Answer: D

NEW QUESTION 2
- (Exam Topic 1)
What would you enter, if you wanted to perform a stealth scan using Nmap?

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

Answer: B

NEW QUESTION 3
- (Exam Topic 1)
You are a security officer of a company. You had an alert from IDS that indicates that one PC on your Intranet is connected to a blacklisted IP address (C2 Server) on the Internet. The IP address was blacklisted just before the alert. You are staring an investigation to roughly analyze the severity of the situation. Which of the following is appropriate to analyze?

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

Answer: B

NEW QUESTION 4
- (Exam Topic 1)
Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occurring during non-business hours. After further examination of all login activities, it is noticed that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem realizes the system time on the Linux server is wrong by more than twelve hours. What protocol used on Linux servers to synchronize the time has stopped working?

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

Answer: B

NEW QUESTION 5
- (Exam Topic 1)
Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

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

Answer: C

NEW QUESTION 6
- (Exam Topic 1)
Vlady works in a fishing company where the majority of the employees have very little understanding of IT let alone IT Security. Several information security issues that Vlady often found includes, employees sharing password, writing his/her password on a post it note and stick it to his/her desk, leaving the computer unlocked, didn't log out from emails or other social media accounts, and etc.
After discussing with his boss, Vlady decided to make some changes to improve the security environment in his company. The first thing that Vlady wanted to do is to make the employees understand the importance of keeping confidential information, such as password, a secret and they should not share it with other persons.
Which of the following steps should be the first thing that Vlady should do to make the employees in his company understand to importance of keeping confidential information a secret?

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

Answer: A

NEW QUESTION 7
- (Exam Topic 1)
Security Policy is a definition of what it means to be secure for a system, organization or other entity. For Information Technologies, there are sub-policies like Computer Security Policy, Information Protection Policy, Information Security Policy, network Security Policy, Physical Security Policy, Remote Access Policy, and User Account Policy.
What is the main theme of the sub-policies for Information Technologies?

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

Answer: C

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

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

Answer: A

NEW QUESTION 9
- (Exam Topic 1)
Which of the following act requires employer's standard national numbers to identify them on standard transactions?

A. SOX
B. HIPAA
C. DMCA
D. PCI-DSS

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

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

Answer: C

NEW QUESTION 11
- (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 15
- (Exam Topic 1)
What is the main security service a cryptographic hash provides?

A. Integrity and ease of computation

B. Message authentication and collision resistance
C. Integrity and collision resistance
D. Integrity and computational in-feasibility

Answer: D

NEW QUESTION 20
- (Exam Topic 1)
Which of the following steps for risk assessment methodology refers to vulnerability identification?

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

Answer: C

NEW QUESTION 22
- (Exam Topic 1)
Nedved is an IT Security Manager of a bank in his country. One day. he found out that there is a security breach to his company's email server based on analysis of a suspicious connection from the email server to an unknown IP Address.
What is the first thing that Nedved needs to do before contacting the incident response team?

A. Leave it as it Is and contact the incident response te3m right away
B. Block the connection to the suspicious IP Address from the firewall
C. Disconnect the email server from the network
D. Migrate the connection to the backup email server

Answer: C

NEW QUESTION 26
- (Exam Topic 1)
Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key.
Suppose a malicious user Rob tries to get access to the account of a benign user Ned.
Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

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

Answer: B

NEW QUESTION 28
- (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 29
- (Exam Topic 1)
What network security concept requires multiple layers of security controls to be placed throughout an IT infrastructure, which improves the security posture of an organization to defend against malicious attacks or potential vulnerabilities?
What kind of Web application vulnerability likely exists in their software?

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

Answer: C

NEW QUESTION 33
- (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 38
- (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 41
- (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 42
- (Exam Topic 1)
Alice encrypts her data using her public key PK and stores the encrypted data in the cloud. Which of the following attack scenarios will compromise the privacy of her data?

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

Answer: D

NEW QUESTION 47
- (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 50
- (Exam Topic 1)
What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?

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

Answer: D

NEW QUESTION 51
- (Exam Topic 1)
Which of the following types of jailbreaking allows user-level access but does not allow iboot-level access?

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

Answer: D

NEW QUESTION 55
- (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 60
- (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 64
- (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 69
- (Exam Topic 1)
Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students.
He identified this when the IDS alerted for malware activities in the network. What should Bob do to avoid this problem?

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

Answer: C

NEW QUESTION 71
- (Exam Topic 1)
In the field of cryptanalysis, what is meant by a "rubber-hose" attack?

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

Answer: B

NEW QUESTION 73
- (Exam Topic 1)
Company XYZ has asked you to assess the security of their perimeter email gateway. From your office in New York, you craft a specially formatted email message and send it across the Internet to an employee of Company XYZ. The employee of Company XYZ is aware of your test.
Your email message looks like this: From: jim_miller@companyxyz.com
To: michelle_saunders@companyxyz.com Subject: Test message
Date: 4/3/2017 14:37
The employee of Company XYZ receives your email message. This proves that Company XYZ's email gateway doesn't prevent what?

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

Answer: C

NEW QUESTION 78

- (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 83
- (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 88
- (Exam Topic 1)
Darius is analysing logs from IDS. He want to understand what have triggered one alert and verify if it's true positive or false positive. Looking at the logs he copy and paste basic details like below:
source IP: 192.168.21.100
source port: 80
destination IP: 192.168.10.23
destination port: 63221
What is the most proper answer.

A. This is most probably true negative.
B. This is most probably true positive which triggered on secure communication between client and server.
C. This is most probably false-positive, because an alert triggered on reversed traffic.
D. This is most probably false-positive because IDS is monitoring one direction traffic.

Answer: A

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

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

Answer: A

NEW QUESTION 96
- (Exam Topic 1)
When conducting a penetration test, it is crucial to use all means to get all available information about the target network. One of the ways to do that is by sniffing the network. Which of the following cannot be performed by the passive network sniffing?

A. Identifying operating systems, services, protocols and devices
B. Modifying and replaying captured network traffic
C. Collecting unencrypted information about usernames and passwords
D. Capturing a network traffic for further analysis

Answer: B

NEW QUESTION 101
- (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 106
- (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 109
- (Exam Topic 1)
A hacker named Jack is trying to compromise a bank's computer system. He needs to know the operating
system of that computer to launch further attacks. What process would help him?

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

Answer: A

NEW QUESTION 111
- (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 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 117
- (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 121
- (Exam Topic 2)
Which property ensures that a hash function will not produce the same hashed value for two different messages?

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

Answer: A

NEW QUESTION 124
- (Exam Topic 2)
What is one thing a tester can do to ensure that the software is trusted and is not changing or tampering with critical data on the back end of a system it is loaded on?

A. Proper testing
B. Secure coding principles
C. Systems security and architecture review

D. Analysis of interrupts within the software

Answer: D

NEW QUESTION 127
- (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 132
- (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 134
- (Exam Topic 2)
Which of the following techniques will identify if computer files have been changed?

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

Answer: C

NEW QUESTION 135
- (Exam Topic 2)
A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed. Which security policy must the security analyst check to see if dial-out modems are allowed?

A. Firewall-management policy
B. Acceptable-use policy
C. Remote-access policy
D. Permissive policy

Answer: C

NEW QUESTION 139
- (Exam Topic 2)
WPA2 uses AES for wireless data encryption at which of the following encryption levels?

A. 64 bit and CCMP
B. 128 bit and CRC
C. 128 bit and CCMP
D. 128 bit and TKIP

Answer: C

NEW QUESTION 141
- (Exam Topic 2)
What is a successful method for protecting a router from potential smurf attacks?

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

Answer: D

NEW QUESTION 142
- (Exam Topic 2)

Which of the following is a hashing algorithm?

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

Answer: A

NEW QUESTION 146
- (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 148
- (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 150
- (Exam Topic 2)
During a wireless penetration test, a tester detects an access point using WPA2 encryption. Which of the following attacks should be used to obtain the key?

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

Answer: A

NEW QUESTION 153
- (Exam Topic 2)
A security engineer has been asked to deploy a secure remote access solution that will allow employees to connect to the company's internal network. Which of the following can be implemented to minimize the opportunity for the man-in-the-middle attack to occur?

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

Answer: C

NEW QUESTION 154
- (Exam Topic 2)
A security consultant is trying to bid on a large contract that involves penetration testing and reporting. The company accepting bids wants proof of work so the consultant prints out several audits that have been performed. Which of the following is likely to occur as a result?

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

Answer: B

NEW QUESTION 158
- (Exam Topic 2)
A botnet can be managed through which of the following?

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

Answer: A

NEW QUESTION 159
- (Exam Topic 2)
What is the outcome of the comm"nc -l -p 2222 | nc 10.1.0.43 1234"?

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

Answer: B

NEW QUESTION 160
- (Exam Topic 2)
The use of alert thresholding in an IDS can reduce the volume of repeated alerts, but introduces which of the following vulnerabilities?

A. An attacker, working slowly enough, can evade detection by the IDS.
B. Network packets are dropped if the volume exceeds the threshold.
C. Thresholding interferes with the IDS' ability to reassemble fragmented packets.
D. The IDS will not distinguish among packets originating from different sources.

Answer: A

NEW QUESTION 161
- (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 162
- (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 165
- (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 170
- (Exam Topic 2)
A company has publicly hosted web applications and an internal Intranet protected by a firewall. Which technique will help protect against enumeration?

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

Answer: C

NEW QUESTION 172
- (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 174
- (Exam Topic 2)
A company is using Windows Server 2003 for its Active Directory (AD). What is the most efficient way to crack the passwords for the AD users?

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

Answer: C

NEW QUESTION 175
- (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 177
- (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 180
- (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 183
- (Exam Topic 2)
Which technical characteristic do Ethereal/Wireshark, TCPDump, and Snort have in common?

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

Answer: D

NEW QUESTION 187
- (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 192
- (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 197
- (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 200
- (Exam Topic 2)
John the Ripper is a technical assessment tool used to test the weakness of which of the following?

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

Answer: D

NEW QUESTION 203
- (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 207
- (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 211
- (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 215
- (Exam Topic 2)
Which of the following cryptography attack methods is usually performed without the use of a computer?

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

Answer: C

NEW QUESTION 219
- (Exam Topic 2)
A network administrator received an administrative alert at 3:00 a.m. from the intrusion detection system. The alert was generated because a large number of packets were coming into the network over ports 20 and 21. During analysis, there were no signs of attack on the FTP servers. How should the administrator classify this situation?

A. True negatives
B. False negatives
C. True positives
D. False positives

Answer: D

NEW QUESTION 221
- (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 222
- (Exam Topic 2)
Passive reconnaissance involves collecting information through which of the following?

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

Answer: D

NEW QUESTION 223
- (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 227
- (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 232
- (Exam Topic 2)
Which of the following scanning tools is specifically designed to find potential exploits in Microsoft Windows products?

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

Answer: D

NEW QUESTION 234
- (Exam Topic 2)
When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's computer to update the router configuration. What type of an alert is this?

A. False positive
B. False negative

C. True positve
D. True negative

Answer: A

NEW QUESTION 239
- (Exam Topic 2)
A security engineer is attempting to map a company's internal network. The engineer enters in the following NMAP command:
NMAP –n –sS –P0 –p 80 ***.***.**.** What type of scan is this?

A. Quick scan
B. Intense scan
C. Stealth scan
D. Comprehensive scan

Answer: C

NEW QUESTION 241
- (Exam Topic 2)
Which of the following is considered an acceptable option when managing a risk?

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

Answer: C

NEW QUESTION 246
- (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 250
- (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 255
- (Exam Topic 2)
What is the correct PCAP filter to capture all TCP traffic going to or from host 192.168.0.125 on port 25?

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

Answer: D

NEW QUESTION 258
- (Exam Topic 2)
Which of the following is a client-server tool utilized to evade firewall inspection?

A. tcp-over-dns
B. kismet
C. nikto
D. hping

Answer: A

NEW QUESTION 259
- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 264
- (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 269
- (Exam Topic 2)
Which of the following parameters enables NMAP's operating system detection feature?

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

Answer: D

NEW QUESTION 274
- (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 277
- (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 280
- (Exam Topic 2)
Which of the following settings enables Nessus to detect when it is sending too many packets and the network pipe is approaching capacity?

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

Answer: D

NEW QUESTION 282
- (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 285
- (Exam Topic 2)
A pentester is using Metasploit to exploit an FTP server and pivot to a LAN. How will the pentester pivot using Metasploit?

A. Issue the pivot exploit and set the meterpreter.
B. Reconfigure the network settings in the meterpreter.
C. Set the payload to propagate through the meterpreter.
D. Create a route statement in the meterpreter.

Answer: D

NEW QUESTION 289
- (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 291
- (Exam Topic 3)
Which vital role does the U.S. Computer Security Incident Response Team (CSIRT) provide?

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

Answer: A

NEW QUESTION 296
- (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 297
- (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 301
- (Exam Topic 3)
If an e-commerce site was put into a live environment and the programmers failed to remove the secret entry point that was used during the application development, what is this secret entry point known as?

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

Answer: D

NEW QUESTION 305
- (Exam Topic 3)
The fundamental difference between symmetric and asymmetric key cryptographic systems is that symmetric key cryptography uses which of the following?

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

Answer: D

NEW QUESTION 310
- (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 315
- (Exam Topic 3)
Which element of Public Key Infrastructure (PKI) verifies the applicant?

A. Certificate authority
B. Validation authority
C. Registration authority
D. Verification authority

Answer: C

NEW QUESTION 317
- (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 322
- (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 327
- (Exam Topic 3)
Which of the following descriptions is true about a static NAT?

A. A static NAT uses a many-to-many mapping.
B. A static NAT uses a one-to-many mapping.
C. A static NAT uses a many-to-one mapping.
D. A static NAT uses a one-to-one mapping.

Answer: D

NEW QUESTION 330
- (Exam Topic 3)
Which of the following processes of PKI (Public Key Infrastructure) ensures that a trust relationship exists and that a certificate is still valid for specific operations?

A. Certificate issuance
B. Certificate validation
C. Certificate cryptography
D. Certificate revocation

Answer: B

NEW QUESTION 334

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

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

Answer: B

NEW QUESTION 335
- (Exam Topic 3)
An attacker has captured a target file that is encrypted with public key cryptography. Which of the attacks below is likely to be used to crack the target file?

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

Answer: D

NEW QUESTION 336
- (Exam Topic 3)
Which method can provide a better return on IT security investment and provide a thorough and comprehensive assessment of organizational security covering policy, procedure design, and implementation?

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

Answer: A

NEW QUESTION 338
- (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 342
- (Exam Topic 3)
Which NMAP feature can a tester implement or adjust while scanning for open ports to avoid detection by the network's IDS?

A. Timing options to slow the speed that the port scan is conducted
B. Fingerprinting to identify which operating systems are running on the network
C. ICMP ping sweep to determine which hosts on the network are not available
D. Traceroute to control the path of the packets sent during the scan

Answer: A

NEW QUESTION 346
- (Exam Topic 3)
A Certificate Authority (CA) generates a key pair that will be used for encryption and decryption of email. The integrity of the encrypted email is dependent on the security of which of the following?

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

Answer: B

NEW QUESTION 349
- (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 351
- (Exam Topic 3)
Which United States legislation mandates that the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) must sign statements verifying the completeness and accuracy of financial reports?

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

Answer: A

NEW QUESTION 356
- (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 358
- (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 362
- (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 366
- (Exam Topic 3)
Which of the following can take an arbitrary length of input and produce a message digest output of 160 bit?

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

Answer: A

NEW QUESTION 371
- (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 373
- (Exam Topic 3)
Advanced encryption standard is an algorithm used for which of the following?

A. Data integrity
B. Key discovery
C. Bulk data encryption
D. Key recovery

Answer: C

NEW QUESTION 374
- (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 375
- (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 378
- (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 383
- (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 384
- (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 385
- (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 387
- (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 392
- (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 394
- (Exam Topic 4)
What is a "Collision attack" in cryptography?

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

Answer: A

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

NEW QUESTION 399
- (Exam Topic 4)
It is a vulnerability in GNU's bash shell, discovered in September of 2014, that gives attackers access to run remote commands on a vulnerable system. The malicious software can take control of an infected machine, launch denial-of-service attacks to disrupt websites, and scan for other vulnerable devices (including routers).
Which of the following vulnerabilities is being described?

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

Answer: A

Explanation:
Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell, the first of which was disclosed on 24 September 2014.
References: https://en.wikipedia.org/wiki/Shellshock_(software_bug)

NEW QUESTION 400
- (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 404
- (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 408
- (Exam Topic 4)
> NMAP -sn 192.168.11.200-215
The NMAP command above performs which of the following?

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

Answer: A

Explanation:
NMAP -sn (No port scan)
This option tells Nmap not to do a port scan after host discovery, and only print out the available hosts that responded to the host discovery probes. This is often known as a "ping scan", but you can also request that traceroute and NSE host scripts be run.
References: https://nmap.org/book/man-host-discovery.html

NEW QUESTION 411
- (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 415
- (Exam Topic 4)
You have compromised a server and successfully gained a root access. You want to pivot and pass traffic undetected over the network and evade any possible Intrusion Detection System.
What is the best approach?

A. Install Cryptcat and encrypt outgoing packets from this server.
B. Install and use Telnet to encrypt all outgoing traffic from this server.

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

Answer: A

Explanation:
Cryptcat enables us to communicate between two systems and encrypts the communication between them with twofish.
References:
http://null-byte.wonderhowto.com/how-to/hack-like-pro-create-nearly-undetectable-backdoor-with-cryptcat-014

NEW QUESTION 417
- (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 419
- (Exam Topic 4)
You've gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your tool kit you have an Ubuntu 9.10 Linux LiveCD. Which Linux based tool has the ability to change any user's password or to activate disabled Windows accounts?

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

Answer: A

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

NEW QUESTION 424
- (Exam Topic 4)
It is a short-range wireless communication technology intended to replace the cables connecting portable of fixed devices while maintaining high levels of security. It allows mobile phones, computers and other devices to connect and communicate using a short-range wireless connection.
Which of the following terms best matches the definition?

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

Answer: A

Explanation:
Bluetooth is a standard for the short-range wireless interconnection of mobile phones, computers, and other electronic devices.
References:
http://www.bbc.co.uk/webwise/guides/about-bluetooth

NEW QUESTION 425
- (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 430
- (Exam Topic 4)
You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from command line.
Which command would you use?

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

Answer: A

Explanation:
To start the Computer Management Console from command line just type compmgmt.msc
/computer:computername in your run box or at the command line and it should automatically open the Computer Management console.
References:
http://www.waynezim.com/tag/compmgmtmsc/

NEW QUESTION 433
- (Exam Topic 4)
Which regulation defines security and privacy controls for Federal information systems and organizations?

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

Answer: A

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

NEW QUESTION 438
- (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 443
- (Exam Topic 4)
Which of the following is assured by the use of a hash?

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

Answer: A

Explanation:
An important application of secure hashes is verification of message integrity. Determining whether any changes have been made to a message (or a file), for example, can be accomplished by comparing message digests calculated before, and after, transmission (or any other event).
References: https://en.wikipedia.org/wiki/Cryptographic_hash_function#Verifying_the_integrity_of_files_or_messages

NEW QUESTION 446
- (Exam Topic 4)
Which tool allows analysts and pen testers to examine links between data using graphs and link analysis?

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

Answer: A

Explanation:
Maltego is proprietary software used for open-source intelligence and forensics, developed by Paterva. Maltego focuses on providing a library of transforms for discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining.
References: https://en.wikipedia.org/wiki/Maltego

NEW QUESTION 451
- (Exam Topic 4)
Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?

A. PKI
B. single sign on
C. biometrics
D. SOA

Answer: A

Explanation:
A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates [1] and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-c commerce, internet banking and confidential email.
References: https://en.wikipedia.org/wiki/Public_key_infrastructure

NEW QUESTION 452
- (Exam Topic 4)
What is the process of logging, recording, and resolving events that take place in an organization?

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

Answer: A

Explanation:
The activities within the incident management process include:
References: https://en.wikipedia.org/wiki/Incident_management_(ITSM)#Incident_management_procedure

NEW QUESTION 453
- (Exam Topic 4)
You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration?
alert tcp any any -> 192.168.100.0/24 21 (msg: "FTP on the network!";)

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

Answer: A

Explanation:
Snort is an open source network intrusion detection system (NIDS) for networks . Snort rule example:
This example is a rule with a generator id of 1000001.
alert tcp any any -> any 80 (content:"BOB"; gid:1000001; sid:1; rev:1;)
References:
http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node31.html

NEW QUESTION 458
- (Exam Topic 4)
It is a regulation that has a set of guidelines, which should be adhered to by anyone who handles any electronic medical data. These guidelines stipulate that all medical practices must ensure that all necessary measures are in place while saving, accessing, and sharing any electronic medical data to keep patient data secure.
Which of the following regulations best matches the description?

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

Answer: A

Explanation:

The HIPAA Privacy Rule regulates the use and disclosure of Protected Health Information (PHI) held by "covered entities" (generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions.)[15] By regulation, the Department of Health and Human Services extended the HIPAA privacy rule to independent contractors of covered entities who fit within the definition of "business associates".
References: https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Privacy_Rule

NEW QUESTION 460
- (Exam Topic 4)
Port scanning can be used as part of a technical assessment to determine network vulnerabilities. The TCP XMAS scan is used to identify listening ports on the targeted system.
If a scanned port is open, what happens?

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

Answer: A

Explanation:
An attacker uses a TCP XMAS scan to determine if ports are closed on the target machine. This scan type is accomplished by sending TCP segments with the all flags sent in the packet header, generating packets that are illegal based on RFC 793. The RFC 793 expected behavior is that any TCP segment with an out-of-state Flag sent to an open port is discarded, whereas segments with out-of-state flags sent to closed ports should be handled with a RST in response. This behavior should allow an attacker to scan for closed ports by sending certain types of rule-breaking packets (out of sync or disallowed by the TCB) and detect closed ports via RST packets.
References: https://capec.mitre.org/data/definitions/303.html

NEW QUESTION 464
- (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 466
- (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 468
- (Exam Topic 4)
You are performing a penetration test. You achieved access via a buffer overflow exploit and you proceed to find interesting data, such as files with usernames and passwords. You find a hidden folder that has the administrator's bank account password and login information for the administrator's bitcoin account.
What should you do?

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

Answer: A

NEW QUESTION 473
- (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 475
- (Exam Topic 5)
An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?

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

Answer: A

NEW QUESTION 480
- (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 481
- (Exam Topic 5)
A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The ps command shows that the nc file is running as process, and the netstat command shows the nc process is listening on a network port.
What kind of vulnerability must be present to make this remote attack possible?

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

Answer: A

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

NEW QUESTION 483
- (Exam Topic 5)
What is the way to decide how a packet will move from an untrusted outside host to a protected inside that is behind a firewall, which permits the hacker to determine which ports are open and if the packets can pass through the packet-filtering of the firewall?

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

Answer: A

NEW QUESTION 485
- (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 488
- (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 491
- (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 492
- (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 497
- (Exam Topic 5)
You are an Ethical Hacker who is auditing the ABC company. When you verify the NOC one of the machines has 2 connections, one wired and the other wireless. When you verify the configuration of this Windows system you find two static routes.
route add 10.0.0.0 mask 255.0.0.0 10.0.0.1
route add 0.0.0.0 mask 255.0.0.0 199.168.0.1 What is the main purpose of those static routes?

A. Both static routes indicate that the traffic is external with different gateway.
B. The first static route indicates that the internal traffic will use an external gateway and the second static route indicates that the traffic will be rerouted.
C. Both static routes indicate that the traffic is internal with different gateway.
D. The first static route indicates that the internal addresses are using the internal gateway and the second static route indicates that all the traffic that is not internal must go to an external gateway.

Answer: D

NEW QUESTION 501
- (Exam Topic 5)
Rebecca commonly sees an error on her Windows system that states that a Data Execution Prevention (DEP) error has taken place. Which of the following is most likely taking place?

A. A race condition is being exploited, and the operating system is containing the malicious process.
B. A page fault is occurring, which forces the operating system to write data from the hard drive.
C. Malware is executing in either ROM or a cache memory area.
D. Malicious code is attempting to execute instruction in a non-executable memory region.

Answer: D

NEW QUESTION 505
- (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 506
- (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 507
- (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 511
- (Exam Topic 5)
Which of the following security operations is used for determining the attack surface of an organization?

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

Answer: A

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

NEW QUESTION 516
- (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 521
- (Exam Topic 5)
The company ABC recently contracted a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. What of the following options can be useful to ensure the integrity of the data?

A. The document can be sent to the accountant using an exclusive USB for that document.

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

Answer: B

NEW QUESTION 526
- (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 528
- (Exam Topic 5)
Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?

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

Answer: A

Explanation:
There are several key elements to have implemented in preparation phase in order to help mitigate any potential problems that may hinder one's ability to handle an incident. For the sake of brevity, the following should be performed:
References: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

NEW QUESTION 530
- (Exam Topic 5)
An attacker is using nmap to do a ping sweep and a port scanning in a subnet of 254 addresses. In which order should he perform these steps?

A. The sequence does not matte
B. Both steps have to be performed against all hosts.
C. First the port scan to identify interesting services and then the ping sweep to find hosts responding to icmp echo requests.
D. First the ping sweep to identify live hosts and then the port scan on the live host
E. This way he saves time.
F. The port scan alone is adequat
G. This way he saves time.

Answer: C

NEW QUESTION 533
- (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 538
- (Exam Topic 5)
Sophia travels a lot and worries that her laptop containing confidential documents might be stolen. What is the best protection that will work for her?

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

Answer: D

NEW QUESTION 541
- (Exam Topic 5)
Which tier in the N-tier application architecture is responsible for moving and processing data between the tiers?

A. Application Layer

B. Data tier
C. Presentation tier
D. Logic tier

Answer: D

NEW QUESTION 546
- (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 551
- (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 556
- (Exam Topic 5)
A penetration test was done at a company. After the test, a report was written and given to the company's IT authorities. A section from the report is shown below:
According to the section from the report, which of the following choice is true?

A. MAC Spoof attacks cannot be performed.
B. Possibility of SQL Injection attack is eliminated.
C. A stateful firewall can be used between intranet (LAN) and DMZ.
D. There is access control policy between VLANs.

Answer: C

NEW QUESTION 559
- (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 564
- (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 566
- (Exam Topic 5)
What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

A. Residual risk

B. Inherent risk
C. Deferred risk
D. Impact risk

Answer: A

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

NEW QUESTION 569
- (Exam Topic 5)
Which of the following is a low-tech way of gaining unauthorized access to systems?

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

Answer: A

Explanation:
Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access.
References: https://en.wikipedia.org/wiki/Social_engineering_(security)

NEW QUESTION 570
- (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 573
- (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 574
- (Exam Topic 5)
An Internet Service Provider (ISP) has a need to authenticate users connecting using analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network.
Which AAA protocol is most likely able to handle this requirement?

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

Answer: A

Explanation:
Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services. These networks may incorporate modems, DSL, access points, VPNs, network ports, web servers, etc.
References: https://en.wikipedia.org/wiki/RADIUS

NEW QUESTION 577
- (Exam Topic 5)
To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in

an attempt to crash the program.
What term is commonly used when referring to this type of testing?

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

Answer: A

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

NEW QUESTION 581
- (Exam Topic 5)
A hacker has managed to gain access to a Linux host and stolen the password file from /etc/passwd. How can he use it?

A. The password file does not contain the passwords themselves.
B. He can open it and read the user ids and corresponding passwords.
C. The file reveals the passwords to the root user only.
D. He cannot read it because it is encrypted.

Answer: A

NEW QUESTION 582
- (Exam Topic 6)
While you were gathering information as part of security assessments for one of your clients, you were able to gather data that show your client is involved with fraudulent activities. What should you do?

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

Answer: A

NEW QUESTION 586
- (Exam Topic 6)
What type of malware is it that restricts access to a computer system that it infects and demands that the user pay a certain amount of money, cryptocurrency, etc. to the operators of the malware to remove the restriction?

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

Answer: A

NEW QUESTION 587
- (Exam Topic 6)
Matthew received an email with an attachment named "YouWon$10Grand.zip." The zip file contains a file named "HowToClaimYourPrize.docx.exe." Out of excitement and curiosity, Matthew opened the said file. Without his knowledge, the file copies itself to Matthew's APPDATA\local directory and begins to beacon to a Command-and-control server to download additional malicious binaries. What type of malware has Matthew encountered?

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

Answer: B

NEW QUESTION 588
- (Exam Topic 6)
Which type of security feature stops vehicles from crashing through the doors of a building?

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

Answer: B

NEW QUESTION 589

- (Exam Topic 6)
Which Type of scan sends a packets with no flags set?

A. Open Scan
B. Null Scan
C. Xmas Scan
D. Half-Open Scan

Answer: B

NEW QUESTION 593
- (Exam Topic 6)
Which of the following is a wireless network detector that is commonly found on Linux?

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

Answer: A

NEW QUESTION 595
- (Exam Topic 6)
A server has been infected by a certain type of Trojan. The hacker intended to utilize it to send and host junk mails. What type of Trojan did the hacker use?

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

Answer: C

NEW QUESTION 600
- (Exam Topic 6)
It has been reported to you that someone has caused an information spillage on their computer. You go to the computer, disconnect it from the network, remove the keyboard and mouse, and power it down. What step in incident handling did you just complete?

A. Containment
B. Eradication
C. Recovery
D. Discovery

Answer: A

NEW QUESTION 603
- (Exam Topic 6)
As an Ethical Hacker you are capturing traffic from your customer network with Wireshark and you need to find and verify just SMTP traffic. What command in Wireshark will help you to find this kind of traffic?

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

Answer: B

NEW QUESTION 608
- (Exam Topic 6)
What is the term coined for logging, recording and resolving events in a company?

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

Answer: C

NEW QUESTION 610
- (Exam Topic 6)
You are manually conducting Idle Scanning using Hping2. During your scanning you notice that almost every query increments the IPID regardless of the port being queried. One or two of the queries cause the IPID to increment by more than one value. Why do you think this occurs?

A. The zombie you are using is not truly idle.
B. A stateful inspection firewall is resetting your queries.
C. Hping2 cannot be used for idle scanning.
D. These ports are actually open on the target system.

Answer: A

NEW QUESTION 614
- (Exam Topic 6)
You've just gained root access to a Centos 6 server after days of trying. What tool should you use to maintain access?

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

Answer: B

NEW QUESTION 619
- (Exam Topic 6)
........is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.
Fill in the blank with appropriate choice.

A. Collision Attack
B. Evil Twin Attack
C. Sinkhole Attack
D. Signal Jamming Attack

Answer: B

NEW QUESTION 621
- (Exam Topic 6)
The chance of a hard drive failure is known to be once every four years. The cost of a new hard drive is $500. EF (Exposure Factor) is about 0.5. Calculate for the Annualized Loss Expectancy (ALE).

A. $62.5
B. $250
C. $125
D. $65.2

Answer: A

NEW QUESTION 626
- (Exam Topic 6)
SNMP is a protocol used to query hosts, servers, and devices about performance or health status data. This protocol has long been used by hackers to gather great amount of information about remote hosts. Which of the following features makes this possible? (Choose two.)

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

Answer: BD

NEW QUESTION 629
- (Exam Topic 6)
This configuration allows NIC to pass all traffic it receives to the Central Processing Unit (CPU), instead of passing only the frames that the controller is intended to receive. Select the option that BEST describes the above statement.

A. Multi-cast mode
B. WEM
C. Promiscuous mode
D. Port forwarding

Answer: C

NEW QUESTION 632
- (Exam Topic 6)
Which of the following is a form of penetration testing that relies heavily on human interaction and often involves tricking people into breaking normal security procedures?

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

Answer: A

NEW QUESTION 636
- (Exam Topic 6)
Which among the following is a Windows command that a hacker can use to list all the shares to which the current user context has access?

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

Answer: B

NEW QUESTION 640
- (Exam Topic 6)
Backing up data is a security must. However, it also has certain level of risks when mishandled. Which of the following is the greatest threat posed by backups?

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

Answer: D

NEW QUESTION 641
- (Exam Topic 6)
Sandra has been actively scanning the client network on which she is doing a vulnerability assessment test. While conducting a port scan she notices open ports in the range of 135 to 139.
What protocol is most likely to be listening on those ports?

A. Finger
B. FTP
C. Samba
D. SMB

Answer: D

NEW QUESTION 644
- (Exam Topic 6)
Which of the following tools would MOST LIKELY be used to perform security audit on various of forms of network systems?

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

Answer: B

NEW QUESTION 645
- (Exam Topic 6)
Which of the following is a restriction being enforced in "white box testing?"

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

Answer: B

NEW QUESTION 648
- (Exam Topic 6)
In order to prevent particular ports and applications from getting packets into an organization, what does a firewall check?

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

Answer: D

NEW QUESTION 653
- (Exam Topic 6)
Defining rules, collaborating human workforce, creating a backup plan, and testing the plans are within what phase of the Incident Handling Process?

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

Answer: A

NEW QUESTION 656
- (Exam Topic 6)
It is a widely used standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. This protocol is specifically designed for transporting event messages. Which of the following is being described?

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

Answer: C

NEW QUESTION 658
- (Exam Topic 6)
Which of the following BEST describes how Address Resolution Protocol (ARP) works?

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

Answer: D

NEW QUESTION 661
- (Exam Topic 6)
There are several ways to gain insight on how a cryptosystem works with the goal of reverse engineering the process. A term describes when two pieces of data result in the same value is?

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

Answer: A

NEW QUESTION 662
- (Exam Topic 6)
Name two software tools used for OS guessing? (Choose two.)

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

Answer: AC

NEW QUESTION 663
- (Exam Topic 6)
Which of the following is designed to verify and authenticate individuals taking part in a data exchange within an enterprise?

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

Answer: C

NEW QUESTION 667
- (Exam Topic 6)
A possibly malicious sequence of packets that were sent to a web server has been captured by an Intrusion Detection System (IDS) and was saved to a PCAP file. As a network administrator, you need to determine whether this packets are indeed malicious. What tool are you going to use?

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

Answer: C

NEW QUESTION 671
- (Exam Topic 6)
Your next door neighbor, that you do not get along with, is having issues with their network, so he yells to his spouse the network's SSID and password and you

hear them both clearly. What do you do with this information?

A. Nothing, but suggest to him to change the network's SSID and password.
B. Sell his SSID and password to friends that come to your house, so it doesn't slow down your network.
C. Log onto to his network, after all it's his fault that you can get in.
D. Only use his network when you have large downloads so you don't tax your own network.

Answer: A

NEW QUESTION 675
- (Exam Topic 6)
The following are types of Bluetooth attack EXCEPT ?

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

Answer: D

NEW QUESTION 676
- (Exam Topic 6)
Suppose you've gained access to your client's hybrid network. On which port should you listen to in order to know which Microsoft Windows workstations has its file sharing enabled?

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

Answer: C

NEW QUESTION 680
- (Exam Topic 6)
Which of the following is a vulnerability in GNU's bash shell (discovered in September of 2014) that gives attackers access to run remote commands on a vulnerable system?

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

Answer: A

NEW QUESTION 683
- (Exam Topic 6)
A big company, who wanted to test their security infrastructure, wants to hire elite pen testers like you. During the interview, they asked you to show sample reports from previous penetration tests. What should you do?

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

Answer: C

NEW QUESTION 685
- (Exam Topic 6)
An nmap command that includes the host specification of 202.176.56-57.* will scan number of hosts.

A. 2
B. 256
C. 512
D. Over 10, 000

Answer: C

NEW QUESTION 690
- (Exam Topic 6)
A specific site received 91 ICMP_ECHO packets within 90 minutes from 47 different sites.
77 of the ICMP_ECHO packets had an ICMP ID:39612 and Seq:57072. 13 of the ICMP_ECHO packets had an ICMP ID:0 and Seq:0. What can you infer from this information?

A. The packets were sent by a worm spoofing the IP addresses of 47 infected sites
B. ICMP ID and Seq numbers were most likely set by a tool and not by the operating system
C. All 77 packets came from the same LAN segment and hence had the same ICMP ID and Seq number
D. 13 packets were from an external network and probably behind a NAT, as they had an ICMP ID 0 and Seq 0

Answer: B

NEW QUESTION 695
- (Exam Topic 6)
What is the approximate cost of replacement and recovery operation per year of a hard drive that has a value of $300 given that the technician who charges $10/hr would need 10 hours to restore OS and Software and needs further 4 hours to restore the database from the last backup to the new hard disk? Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%).

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

Answer: D

NEW QUESTION 696
- (Exam Topic 6)
What attack is used to crack passwords by using a precomputed table of hashed passwords?

A. Brute Force Attack
B. Hybrid Attack
C. Rainbow Table Attack
D. Dictionary Attack

Answer: C

NEW QUESTION 701
- (Exam Topic 7)
Every company needs a formal written document which spells out to employees precisely what they are allowed to use the company's systems for, what is prohibited, and what will happen to them if they break the rules. Two printed copies of the policy should be given to every employee as soon as possible after they join the organization. The employee should be asked to sign one copy, which should be safely filed by the company. No one should be allowed to use the company's computer systems until they have signed the policy in acceptance of its terms.
What is this document called?

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

Answer: B

NEW QUESTION 705
- (Exam Topic 7)
This kind of password cracking method uses word lists in combination with numbers and special characters:

A. Hybrid
B. Linear
C. Symmetric
D. Brute Force

Answer: A

NEW QUESTION 708
- (Exam Topic 7)
One of your team members has asked you to analyze the following SOA record.
What is the TTL?
Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.)

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

Answer: D

NEW QUESTION 709
- (Exam Topic 7)
What is the proper response for a NULL scan if the port is closed?

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

Answer: E

NEW QUESTION 710
- (Exam Topic 7)
In the context of Windows Security, what is a 'null' user?

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

Answer: C

NEW QUESTION 711
- (Exam Topic 7)
Within the context of Computer Security, which of the following statements describes Social Engineering best?

A. Social Engineering is the act of publicly disclosing information
B. Social Engineering is the means put in place by human resource to perform time accounting
C. Social Engineering is the act of getting needed information from a person rather than breaking into a system
D. Social Engineering is a training program within sociology studies

Answer: C

NEW QUESTION 715
- (Exam Topic 7)
You have successfully logged on a Linux system. You want to now cover your trade Your login attempt may be logged on several files located in /var/log. Which file does NOT belongs to the list:

A. user.log
B. auth.fesg
C. wtmp
D. btmp

Answer: C

NEW QUESTION 719
- (Exam Topic 7)
Bob is going to perform an active session hijack against Brownies Inc. He has found a target that allows session oriented connections (Telnet) and performs the sequence prediction on the target operating system. He manages to find an active session due to the high level of traffic on the network. What is Bob supposed to do next?

A. Take over the session
B. Reverse sequence prediction
C. Guess the sequence numbers
D. Take one of the parties offline

Answer: C

NEW QUESTION 724
- (Exam Topic 7)
You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?

A. Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account
B. Package the Sales.xls using Trojan wrappers and telnet them back your home computer
C. You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques
D. Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account

Answer: C

NEW QUESTION 729
- (Exam Topic 7)
Fingerprinting an Operating System helps a cracker because:

A. It defines exactly what software you have installed
B. It opens a security-delayed window based on the port being scanned
C. It doesn't depend on the patches that have been applied to fix existing security holes
D. It informs the cracker of which vulnerabilities he may be able to exploit on your system

Answer: D

NEW QUESTION 731

- (Exam Topic 7)
Windows LAN Manager (LM) hashes are known to be weak.
Which of the following are known weaknesses of LM? (Choose three.)

A. Converts passwords to uppercase.
B. Hashes are sent in clear text over the network.
C. Makes use of only 32-bit encryption.
D. Effective length is 7 characters.

Answer: ABD

NEW QUESTION 736
- (Exam Topic 7)
Which of the following LM hashes represent a password of less than 8 characters? (Choose two.)

A. BA810DBA98995F1817306D272A9441BB
B. 44EFCE164AB921CQAAD3B435B51404EE
C. 0182BD0BD4444BF836077A718CCDF409
D. CEC52EB9C8E3455DC2265B23734E0DAC
E. B757BF5C0D87772FAAD3B435B51404EE
F. E52CAC67419A9A224A3B108F3FA6CB6D

Answer: BE

NEW QUESTION 738
- (Exam Topic 7)
Bob is acknowledged as a hacker of repute and is popular among visitors of "underground" sites.
Bob is willing to share his knowledge with those who are willing to learn, and many have expressed their interest in learning from him. However, this knowledge has a risk associated with it, as it can be used for malevolent attacks as well.
In this context, what would be the most effective method to bridge the knowledge gap between the "black" hats or crackers and the "white" hats or computer security professionals? (Choose the test answer.)

A. Educate everyone with books, articles and training on risk analysis, vulnerabilities and safeguards.
B. Hire more computer security monitoring personnel to monitor computer systems and networks.
C. Make obtaining either a computer security certification or accreditation easier to achieve so more individuals feel that they are a part of something larger than life.
D. Train more National Guard and reservist in the art of computer security to help out in times of emergency or crises.

Answer: A

NEW QUESTION 743
- (Exam Topic 7)
You have retrieved the raw hash values from a Windows 2000 Domain Controller. Using social engineering, you come to know that they are enforcing strong passwords. You understand that all users are required to use passwords that are at least 8 characters in length. All passwords must also use 3 of the 4 following categories: lower case letters, capital letters, numbers and special characters. With your existing knowledge of users, likely user account names and the possibility that they will choose the easiest passwords possible, what would be the fastest type of password cracking attack you can run against these hash values and still get results?

A. Online Attack
B. Dictionary Attack
C. Brute Force Attack
D. Hybrid Attack

Answer: D

NEW QUESTION 744
- (Exam Topic 7)
What is a NULL scan?

A. A scan in which all flags are turned off
B. A scan in which certain flags are off
C. A scan in which all flags are on
D. A scan in which the packet size is set to zero
E. A scan with an illegal packet size

Answer: A

NEW QUESTION 748
- (Exam Topic 7)
Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site. One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message "Hacker Message: You are dead! Freaks!" From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact.
No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend
could see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using hisdial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith. After his modem

connected, he quickly typed www.masonins.com in his browser to reveal the following web page:

```
H@cker Mess@ge:
Y0u @re De@d! Fre@ks!
```

After seeing the defaced Web site, he disconnected his dial-up line, reconnected to the internal network, and used Secure Shell (SSH) to log in directly to the Web server. He ran Tripwire against the entire Web site, and determined that every system file and all the Web content on the server were intact. How did the attacker accomplish this hack?

A. ARP spoofing
B. SQL injection
C. DNS poisoning
D. Routing table injection

Answer: C

NEW QUESTION 750
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

312-50v10 Practice Exam Features:

* 312-50v10 Questions and Answers Updated Frequently

* 312-50v10 Practice Questions Verified by Expert Senior Certified Staff

* 312-50v10 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 312-50v10 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The 312-50v10 Practice Test Here