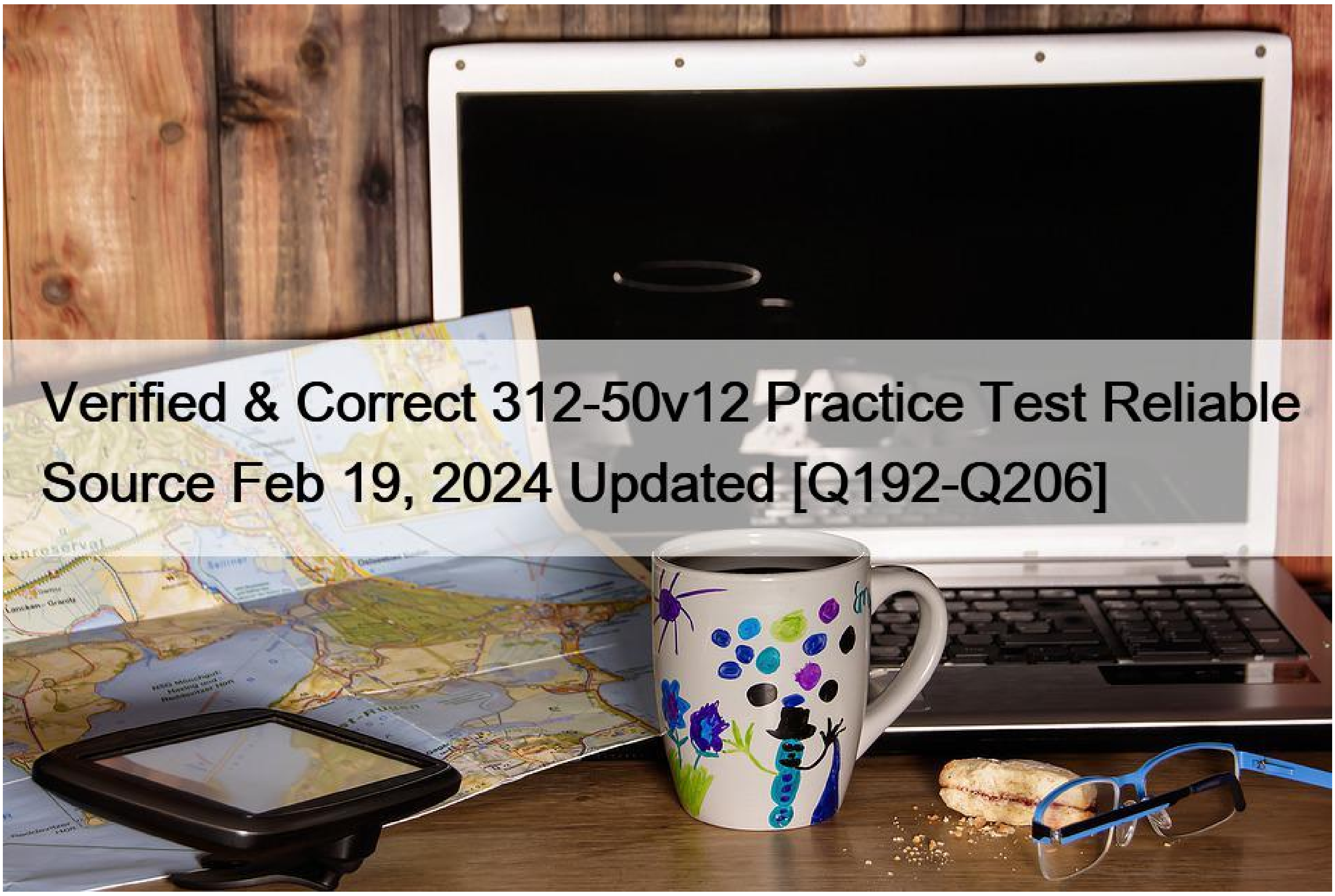
Verified & Correct 312-50v12 Practice Test Reliable Source Feb 19, 2024 Updated [Q192-Q206


Verified & Correct 312-50v12 Practice Test Reliable Source Feb 19, 2024 Updated [Q192-Q206]

Verified & Correct 312-50v12 Practice Test Reliable Source Feb 19, 2024 Updated Free ECCouncil 312-50v12 Exam Files Downloaded Instantly NO.192 Which of the following statements about a zone transfer is correct? (Choose three.)
* A zone transfer is accomplished with the DNS
* A zone transfer is accomplished with the nslookup service
* A zone transfer passes all zone information that a DNS server maintains
* A zone transfer passes all zone information that a nslookup server maintains
* A zone transfer can be prevented by blocking all inbound TCP port 53 connections
* Zone transfers cannot occur on the Internet

NO.193 This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such as GCMP-2S6. MMAC-SHA384, and ECDSA using a 384-bit elliptic curve. Which is this wireless security protocol?
* WPA2 Personal
* WPA3-Personal
* WPA2-Enterprise
* WPA3-Enterprise

Enterprise, governments, and financial institutions have greater security with WPA3-Enterprise. WPA3-Enterprise builds upon

WPA2 and ensures the consistent application of security protocol across the network. WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to raised protect sensitive data: * Authenticated encryption: 256-bit Galois/Counter Mode Protocol (GCMP-256) * Key derivation and confirmation: 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384) * Key establishment and authentication: Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) employing a 384-bit elliptic curve * Robust management frame protection: 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256) The 192-bit security mode offered by WPA3-Enterprise ensures the proper combination of cryptographic tools are used and sets a uniform baseline of security within a WPA3 network.

It protects sensitive data using many cryptographic algorithms It provides authenticated encryption using GCMP-256 It uses HMAC-SHA-384 to generate cryptographic keys It uses ECDSA-384 for exchanging keys

NO.194 Security administrator John Smith has noticed abnormal amounts of traffic coming from local computers at night. Upon reviewing, he finds that user data have been exfilltrated by an attacker. AV tools are unable to find any malicious software, and the IDS/IPS has not reported on any non-whitelisted programs, what type of malware did the attacker use to bypass the company&#8217;s application whitelisting?

* Phishing malware
* Zero-day malware
* File-less malware
* Logic bomb malware

https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html Fileless malware can easily evade various security controls, organizations need to focus on monitoring, detecting, and preventing malicious activities instead of using traditional approaches such as scanning for malware through file signatures.Also known as non-malware, infects legitimate software, applications, and other protocols existing in the system to perform various malicious activities.It resides in the system&#8217;s RAM. It injects malicious code into the running processes. (P.966/950)

NO.195 Why containers are less secure that virtual machines?

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

NO.196 A company&#8217;s Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.

What kind of Web application vulnerability likely exists in their software?

* Cross-site scripting vulnerability
* SQL injection vulnerability
* Web site defacement vulnerability
* Gross-site Request Forgery vulnerability

There is no single, standardized classification of cross-site scripting flaws, but most experts distinguish between at least two primary flavors of XSS flaws: non-persistent and persistent. In this issue, we consider the non-persistent cross-site scripting vulnerability.

The non-persistent (or reflected) cross-site scripting vulnerability is by far the most basic type of web vulnerability. These holes show up when the data provided by a web client, most commonly in HTTP query parameters (e.g. HTML form submission), is used immediately by server-side scripts to parse and display a page of results for and to that user, without properly sanitizing the content.

Because HTML documents have a flat, serial structure that mixes control statements, formatting, and the actual content, any non-validated user-supplied data included in the resulting page without proper HTML encoding, may lead to markup injection. A classic example of a potential vector is a site search engine: if one searches for a string, the search string will typically be redisplayed verbatim on the result page to indicate what was searched for. If this response does not properly escape or reject HTML control characters, a cross-site scripting flaw will ensue.

NO.197 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.)
* 200303028
* 3600
* 604800
* 2400
* 60
* 4800

NO.198 John, a disgruntled ex-employee of an organization, contacted a professional hacker to exploit the organization. In the attack process, the professional hacker Installed a scanner on a machine belonging to one of the vktims and scanned several machines on the same network to Identify vulnerabilities to perform further exploitation. What is the type of vulnerability assessment tool employed by John in the above scenario?
* Proxy scanner
* Agent-based scanner
* Network-based scanner
* Cluster scanner

Network-based scanner

A network-based vulnerability scanner, in simplistic terms, is the process of identifying loopholes on a computer&#8217;s network or IT assets, which hackers and threat actors can exploit. By implementing this process, one can successfully identify their organization&#8217;s current risk(s). This is not where the buck stops; one can also verify the effectiveness of your system&#8217;s security measures while improving internal and external defenses. Through this review, an organization is well equipped to take an extensive inventory of all systems, including operating systems, installed software, security patches, hardware, firewalls, anti-virus software, and much more.

Agent-based scanner

Agent-based scanners make use of software scanners on each and every device; the results of the scans are reported back to the central server. Such scanners are well equipped to find and report out on a range of vulnerabilities.

NOTE: This option is not suitable for us, since for it to work, you need to install a special agent on each computer before you start collecting data from them.

NO.199 You are using a public Wi-Fi network inside a coffee shop. Before surfing the web, you use your VPN to prevent intruders from sniffing your traffic. If you did not have a VPN, how would you identify whether someone is performing an ARP spoofing attack on your laptop?
* You should check your ARP table and see if there is one IP address with two different MAC addresses.
* You should scan the network using Nmap to check the MAC addresses of all the hosts and look for duplicates.
* You should use netstat to check for any suspicious connections with another IP address within the LAN.
* You cannot identify such an attack and must use a VPN to protect your traffic, r

NO.200 What would be the fastest way to perform content enumeration on a given web server by using the Gobuster tool?
* Performing content enumeration using the bruteforce mode and 10 threads
* Shipping SSL certificate verification

* Performing content enumeration using a wordlist
* Performing content enumeration using the bruteforce mode and random file extensions

NO.201 Which iOS jailbreaking technique patches the kernel during the device boot so that it becomes jailbroken after each successive reboot?
* Tethered jailbreaking
* Semi-tethered jailbreaking
* Untethered jailbreaking
* Semi-Untethered jailbreaking
An untethered jailbreak is one that allows a telephone to finish a boot cycle when being pwned with none interruption to jailbreak-oriented practicality.

Untethered jailbreaks area unit the foremost sought-after of all, however they&#8217;re additionally the foremost difficult to attain due to the powerful exploits and organic process talent they need. associate unbound jailbreak is sent over a physical USB cable association to a laptop or directly on the device itself by approach of associate application-based exploit, like a web site in campaign.

Upon running associate unbound jailbreak, you&#8217;ll be able to flip your pwned telephone off and on once more while not running the jailbreak tool once more. all of your jailbreak tweaks and apps would then continue in operation with none user intervention necessary.

It&#8217;s been an extended time since IOS has gotten the unbound jailbreak treatment. the foremost recent example was the computer-based Pangu break, that supported most handsets that ran IOS nine.1. We&#8217;ve additionally witnessed associate unbound jailbreak within the kind of JailbreakMe, that allowed users to pwn their handsets directly from the mobile campaign applications programme while not a laptop.

NO.202 Abel, a cloud architect, uses container technology to deploy applications/software including all its dependencies, such as libraries and configuration files, binaries, and other resources that run independently from other processes in the cloud environment. For the containerization of applications, he follows the five-tier container technology architecture. Currently. Abel is verifying and validating image contents, signing images, and sending them to the registries. Which of the following tiers of the container technology architecture Is Abel currently working in?
* Tier-1: Developer machines
* Tier-4: Orchestrators
* Tier-3: Registries
* Tier-2: Testing and accreditation systems
The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

formal declaration by a designated accrediting authority (DAA) or principal accrediting authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. See authorization to operate (ATO). Rationale: The Risk Management Framework uses a new term to refer to this concept, and it is called authorization.

Identifies the information resources covered by an accreditation decision, as distinguished from separately accredited information resources that are interconnected or with which information is exchanged via messaging. Synonymous with Security Perimeter.

For the purposes of identifying the Protection Level for confidentiality of a system to be accredited, the system has a conceptual boundary that extends to all intended users of the system, both directly and indirectly connected, who receive output from the system. See authorization boundary. Rationale: The Risk Management Framework uses a new term to refer to the concept of accreditation, and it is called authorization. Extrapolating, the accreditation boundary would then be referred to as the authorization boundary.

NO.203 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?
* tcp.srcport= = 514 && ip.src= = 192.168.0.99
* tcp.srcport= = 514 && ip.src= = 192.168.150
* tcp.dstport= = 514 && ip.dst= = 192.168.0.99
* tcp.dstport= = 514 && ip.dst= = 192.168.0.150

NO.204 What does the following command in netcat do?

nc -l -u -p55555 < /etc/passwd
* logs the incoming connections to /etc/passwd file
* loads the /etc/passwd file to the UDP port 55555
* grabs the /etc/passwd file when connected to UDP port 55555
* deletes the /etc/passwd file when connected to the UDP port 55555

NO.205 What kind of detection techniques is being used in antivirus softwares that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it&#8217;s made on the premiers environment-
* VCloud based
* Honypot based
* Behaviour based
* Heuristics based

NO.206 Garry is a network administrator in an organization. He uses SNMP to manage networked devices from a remote location. To manage nodes in the network, he uses MIB. which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mlb or by entering the DNS library name and Lseries.mlb. He is currently retrieving information from an MIB that contains object types for workstations and server services. Which of the following types of MIB is accessed by Garry in the above scenario?
* LNMIB2.MIB
* WINS.MIB
* DHCP.MIS
* MIB_II.MIB

DHCP.MIB: Monitors network traffic between DHCP servers and remote hosts

? HOSTMIB.MIB: Monitors and manages host resources

? LNMIB2.MIB: Contains object types for workstation and server services

? MIBJI.MIB: Manages TCP/IP-based Internet using a simple architecture and system

? WINS.MIB: For the Windows Internet Name Service (WINS)

Pass ECCouncil 312-50v12 exam Dumps 100 Pass Guarantee With Latest Demo: https://www.braindumpsit.com/312-50v12_real-exam.html]