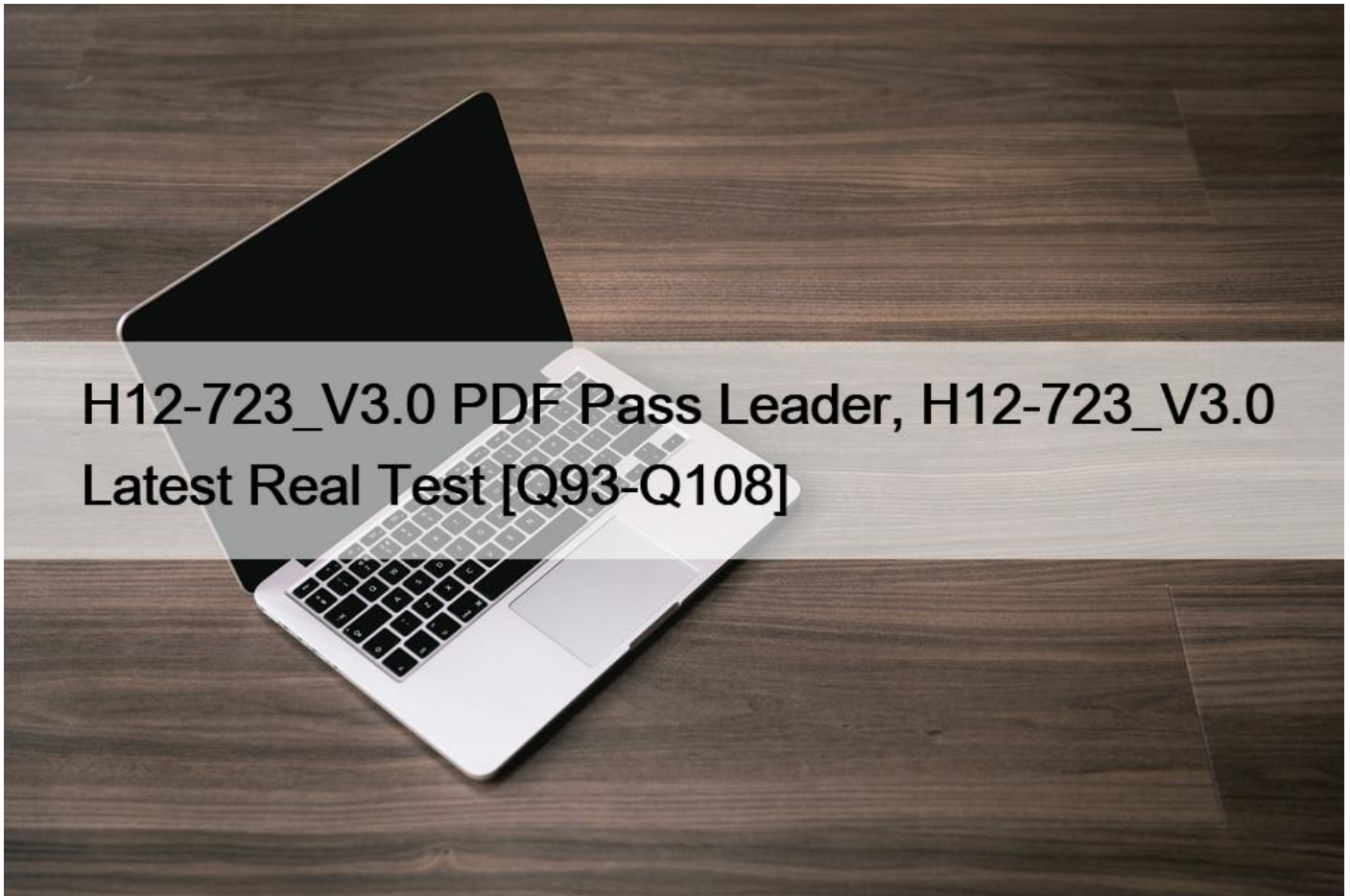


H12-723_V3.0 PDF Pass Leader, H12-723_V3.0 Latest Real Test [Q93-Q108]



H12-723_V3.0 PDF Pass Leader, H12-723_V3.0 Latest Real Test
Valid H12-723_V3.0 Test Answers & H12-723_V3.0 Exam PDF

NO.93 In the WLAN wireless access scenario, which of the following network security technologies belong to user access security?

(Multiple choice)

- * AP Certification
- * Linkauthentication
- * User access authentication
- * data encryption

NO.94 When configuring the antivirus software policy, if you set 'The required antivirus software violation level is not installed or running'; 'for'; 'generally'; 'And check'; 'out Now serious violation of the rules prohibits access to the network'; 'Options. When the user uses Any office Certify, The certification is passed, but the result of the security check Can the user access the network when the virus software is not turned on?

- * Can access the network? Can also access network resources.
- * Cannot access the network.
- * Can pick up? The network needs to be repaired before you can access network resources.
- * You can access the network, but you need to re-authenticate to access network resources.

NO.95 For hardware SACC Access control, if the terminal does not pass the authentication, it can access the resources of the post-authentication domain. This phenomenon may be caused by the following reasons?

(Multiple choice)

- * Authentication data flow has passed SACG filter.
- * TSM No hardware is added to the system SACG equipment.
- * SACG Enable the default inter-domain packetfiltering.
- * Privileges are misconfigured IP

NO.96 Web Standards that come with the client and operating system 8021 The instrument client only has the function of identity authentication: It does not support the execution of inspection strategies and monitoring strategies. Any Office The client supports all inspection strategies and monitoring strategies.

- * True
- * False

NO.97 Which of the following options are relevant to Any Office The description of the solution content is correct?

(Multiple choice)

- * Provide unified and secure access to enterprise mobile applications on mobile terminals.
- * The tunnel is dedicated and cannot be penetrated by viruses.
- * Applications are quickly integrated and can be extended.
- * It can be quickly integrated and docked with the enterprise application cloud platform.

NO.98 A network adopts Portal Authentication, the user finds the pushed Web No username entered on the page/The place of the password. This failure may Which of the following causes?

- * Agile Controller-CampusThere is no corresponding user on.
- * switch AAA Configuration error.
- * The switch is not turned on Portal Function.
- * Portal The push page on the server is wrong.

NO.99 Jailbroken mobile terminalMobile terminals with non-compliant applications installed or terminals with non-compliant lock screen passwords connecting to the corporate network for office operations are not safe for companies. Any Office How to solve the problem of mobile office system?

- * Directly discard data sent by devices that do not comply with regulations
- * Certification of non-compliant equipment.
- * Check for non-compliant terminals, Prohibit unsafe devices from accessing the network.
- * Send alarm information to notify the administrator to deal with it.

NO.100 The user access security solution is one-kind”End to end”Security architecture. The user access security architecture includes three key components:Terminal equipment, network access equipment and access server.

- * True
- * False

NO.101 Mobile smartphone, tablet PC users through Any Office Client and AE Establish IPSec Encrypted tunnel, After passing the certification and compliance check, visit the enterprise business.

- * True
- * False

NO.102 When using local guest account authentication, usually use(Portal The authentication method pushes the authentication

page to the visitor. Before the user is authenticated, when the admission control device receives the HTTP The requested resource is not Portal Server authentication URL When, how to deal with the access control equipment.

- * Discard message
- * URL Address redirected to Portal Authentication page
- * Direct travel
- * Send authentication information to authentication server

NO.103 Traditional network single–The strategy is difficult to cope with the current complex situations such as diversified users, diversified locations, diversified terminals, diversified applications, and insecure experience.

- * True
- * False

NO.104 User access authentication technology does not include which of the following options?

- * Authentication
- * Isolation repair’
- * Security check
- * Access control

NO.105 In the visitor reception hall of a company, there are many temporary terminal users, and the administrator hopes that users do not need to provide any account numbers and passwords. access Internet. Which of the following authentication methods can be used for access?

- * Local account authentication
- * Anonymous authentication
- * AD Account Verification
- * MAC Certification

NO.106 Regarding the role of each role in the Portal authentication framework, which of the following descriptions are correct? (multiple choice)

- * The AAA server saves information such as usernames and passwords for authentication of access users.
- * The Web server saves informationsuch as user names and passwords for authentication of access users.
- * The AAA server is used to push the Portal authentication page to the user.
- * The web server is used to push the Portal authentication page to the user.

NO.107 On WIDS functional WLAN Regarding the judgment of illegal devices in the network, which of the following statements are correct? (Multiple choice)

- * all Ad-hoc The device will be directly judged as an illegal device
- * Not this AC Access AP Is illegal AP
- * Not this AC Access STA Is illegal STA
- * Not this AC Access STA,Also need to check access AP Does it contain law

NO.108 In enterprises where terminal host access control management is relatively strict, administrators hope to bind terminal hosts and accounts to prevent terminal users from accessing the controlled network from unauthorized terminal hosts at will. Regarding the description of binding the terminal host and account, which of the following is correct?

- * exist Any Office When logging in with an account for the first time, the terminal host is automatically bound to the current account, but the automatic binding process requires administrator approval
- * When other accounts need to be authenticated on the bound terminal host, there is no need to find the asset owner who is bound for the first time to authorize themselves.
- * Binding terminal hosts and accounts is only applicable to terminal users through Any Office Scenarios for authentication, Not applicable Web Agent Plugins and Web The scenario where the client authenticates.
- * There are only consoles in the account binding terminal host, which cannot be configured by the administrator.

H12-723_V3.0 Dumps Ensure Your Passing:

https://www.examlabs.com/Huawei/HCIP-Security/best-H12-723_V3.0-exam-dumps.html