640-554 Q&As

Implementing Cisco IOS Network Security (IINS v2.0)

Pass Cisco 640-554 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/640-554.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which statement about IPv6 address allocation is true?

A. IPv6-enabled devices can be assigned only one IPv6 IP address.

B. A DHCP server is required to allocate IPv6 IP addresses.

C. IPv6-enabled devices can be assigned multiple IPv6 IP addresses.

D. ULA addressing is required for Internet connectivity.

Correct Answer: C

QUESTION 2

Which two protocols enable Cisco Configuration Professional to pull IPS alerts from a Cisco ISR router? (Choose two.)

A. syslog

B. SDEE

C. FTP

D. TFTP

E. SSH

F. HTTPS

Correct Answer: BF

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd805c4ea8.html

Step 4: Enabling IOS IPS

The fourth step is to configure IOS IPS using the following sequence of steps:

Step 4.1: Create a rule name (This will be used on an interface to enable IPS)

ip ips name

router#configure terminal router(config)# ip ips name iosips

You can specify an optional extended or standard access control list (ACL) to filter the traffic that will be scanned by this rule name. All traffic that is permitted by the ACL is subject to inspection by the IPS. Traffic that is denied by the ACL is

not inspected by the IPS. router(config)#ip ips name ips list ?

Numbered access list WORD Named access list Step 4.2: Configure IPS signature storage location, this is the directory `ips\\' created in Step 2 ip ips config location flash: router(config)#ip ips config location flash:ips Step 4.3: Enable IPS SDEE event notification ip ips notify sdee router(config)#ip ips notify sdee To use SDEE, the HTTP server must be enabled (via the `ip http server\\' command). If the HTTP server is not enabled, the router cannot respond to the SDEE

clients because it cannot see the requests. SDEE notification is disabled by default and must be explicitly enabled.

QUESTION 3

Which protocol secures router management session traffic?

A. SSTP

B. POP

C. Telnet

D. SSH

Correct Answer: D

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml

Encrypting Management Sessions

Because information can be disclosed during an interactive management session, this traffic must be encrypted so that a malicious user cannot gain access to the data being transmitted. Encrypting the traffic allows a secure remote access connection to the device. If the traffic for a management session is sent over the network in cleartext, an attacker can obtain sensitive information about the device and the network. An administrator is able to establish an encrypted and secure remote access management connection to a device by using the SSH or HTTPS (Secure Hypertext Transfer Protocol) features. Cisco IOS software supports SSH version 1.0 (SSHv1), SSH version 2.0 (SSHv2), and HTTPS that uses Secure Sockets Layer (SSL) and Transport Layer Security (TLS) for authentication and data encryption. Note that SSHv1 and SSHv2 are not compatible.

Cisco IOS software also supports the Secure Copy Protocol (SCP), which allows an encrypted and secure connection for copying device configurations or software images. SCP relies on SSH. This example configuration enables SSH on a Cisco IOS device: ! ip domain-name example.com ! crypto key generate rsa modulus 2048 ! ip ssh time-out 60 ip ssh authentication-retries 3 ip ssh source-interface GigabitEthernet 0/1 ! line vty 0 4 transport input ssh !

QUESTION 4

Which four tasks are required when you configure Cisco IOS IPS using the Cisco Configuration Professional IPS wizard? (Choose four.)

A. Select the interface(s) to apply the IPS rule.

B. Select the traffic flow direction that should be applied by the IPS rule.

C. Add or remove IPS alerts actions based on the risk rating.

D. Specify the signature file and the Cisco public key.

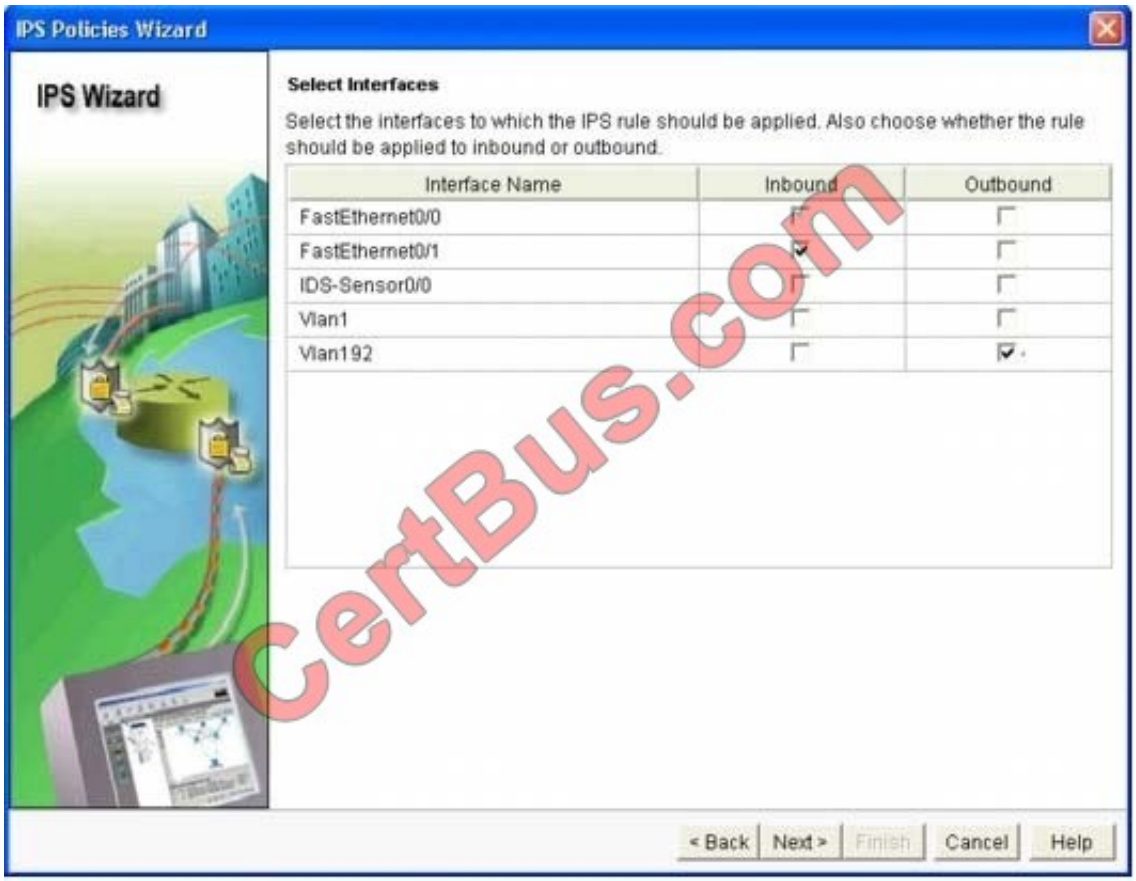
E. Select the IPS bypass mode (fail-open or fail-close).

F. Specify the configuration location and select the category of signatures to be applied to the selected interface(s).

Correct Answer: ABDF

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd8066d265.html

Step 11. At the `Select Interfaces\\' screen, select the interface and the direction that IOS IPS will be applied to, then click `Next\\' to continue.



Step 12. At the `IPS Policies Wizard\\' screen, in the `Signature File\\' section, select the first radio button "Specify the signature file you want to use with IOS IPS", then click the "..." button to bring up a dialog box to specify the location of the signature package file, which will be the directory specified in Step 6. In this example, we use tftp to download the signature package to the router.

Step 13. In the `Configure Public Key\\' section, enter `realm-cisco.pub\\' in the `Name\\' text field, then copy and paste the following public key\\'s key-string in the `Key\\' text field. This public key can be download from

Cisco.com at: http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup. Click `Next\\' to continue. 30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101 00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16 17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128 B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E 5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35 FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85 50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36 006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE 2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3 F3020301 0001

QUESTION 5

Which characteristic is the foundation of Cisco Self-Defending Network technology?

A. secure connectivity

B. threat control and containment

C. policy management

D. secure network platform

Correct Answer: D

http://www.cisco.com/en/US/solutions/ns170/networking_solutions_products_genericcontent0900aecd8051f378.html Create a Stronger Defense Against Threats Each day, you reinvent how you conduct business by adopting Internet-based business models. But Internet connectivity without appropriate security can compromise the gains you hope to make. In today\\'s connected environment, outbreaks spread globally in a matter of minutes, which means your security systems must react instantly. Maintaining security using tactical, point solutions introduces complexity and inconsistency, but integrating security throughout the network protects the information that resides on it. Three components are critical to effective information security: ?A secure network platform with integrated security to which you can easily add advanced security technologies and services ?Threat control services focused on antivirus protection and policy enforcement that continuously monitor network activity and prevent or mitigate problems ?Secure communication services that maintain the privacy and confidentiality of sensitive data, voice, video, and wireless communications while cost-effectively extending the reach of your network

QUESTION 6

Which router management feature provides for the ability to configure multiple administrative views?

A. role-based CLI

B. virtual routing and forwarding

C. secure config privilege {level}

D. parser view view name

Correct Answer: A

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtclivws.html

Role-Based CLI Access

The Role-Based CLI Access feature allows the network administrator to define "views," which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration

(Config) mode commands. Views restrict user access to Cisco IOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible. Thus,

network administrators can exercise better control over access to Cisco networking devices.

QUESTION 7

Which two protocols can SNMP use to send messages over a secure communications channel? (Choose two.)

A. DTLS

B. TLS

C. ESP

D. AH

E. ISAKMP

Correct Answer: AB

QUESTION 8

Which two countermeasures can mitigate ARP spoofing attacks? (Choose two.)

A. port security

B. DHCP snooping

C. IP source guard

D. dynamic ARP inspection

Correct Answer: BD

QUESTION 9

What is the transition order of STP states on a Layer 2 switch interface?

A. listening, learning, blocking, forwarding, disabled

B. listening, blocking, learning, forwarding, disabled

C. blocking, listening, learning, forwarding, disabled

D. forwarding, listening, learning, blocking, disabled

Correct Answer: C

Explanation: Each Layer 2 interface on a switch using spanning tree exists in one of these states:

Blocking -- The interface does not participate in frame forwarding.

Listening -- The first transitional state after the blocking state when the spanning tree determines that the interface should participate in frame forwarding.

Learning -- The interface prepares to participate in frame forwarding.

Forwarding -- The interface forwards frames.

Disabled -- The interface is not participating in spanning tree because of a shutdown port, no link on the port, or no spanning-tree instance running on the port

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2950/software/release/12-1_22_ea11x/configuration/guide/scg/swstp.html

QUESTION 10

Which three statements about access lists are true? (Choose three.)

A. Extended access lists should be placed as near as possible to the destination.

B. Extended access lists should be placed as near as possible to the source.

C. Standard access lists should be placed as near as possible to the destination.

D. Standard access lists should be placed as near as possible to the source.

E. Standard access lists filter on the source address.

F. Standard access lists filter on the destination address.

Correct Answer: BCE

QUESTION 11

Which four methods are used by hackers? (Choose four.)

A. footprint analysis attack

B. privilege escalation attack

C. buffer Unicode attack

D. front door attacks

E. social engineering attack

F. Trojan horse attack

Correct Answer: ABEF

https://learningnetwork.cisco.com/servlet/JiveServlet/download/15823-1-57665/CCNA%20Security%20(640-554)%20Portable%20Command%20Guide_ch01.pdf

Thinking Like a Hacker

The following seven steps may be taken to compromise targets and applications:

Step 1 Perform footprint analysis

Hackers generally try to build a complete profile of a target company\\'s security posture using a broad range of easily available tools and techniques. They can discover organizational domain names, network blocks, IP addresses of systems,

ports, services that are used, and more.

Step 2 Enumerate applications and operating systems

Special readily available tools are used to discover additional target information. Ping sweeps use Internet Control Message Protocol (ICMP) to discover devices on a network. Port scans discover TCP/UDP port status.

Other tools include Netcat, Microsoft EPDump and Remote Procedure Call (RPC) Dump, GetMAC, and software development kits (SDKs).

Step 3 Manipulate users to gain access

Social engineering techniques may be used to manipulate target employees to acquire passwords. They may call or email them and try to convince them to reveal passwords without raising any concern or suspicion.

Step 4 Escalate privileges

To escalate their privileges, a hacker may attempt to use Trojan horse programs and get target users to unknowingly copy malicious code to their corporate system.

Step 5 Gather additional passwords and secrets

With escalated privileges, hackers may use tools such as the pwdump and LSADump applications to gather passwords from machines running Windows.

Step 6 Install back doors

Hacker may attempt to enter through the "front door," or they may use "back doors" into the system. The backdoor method means bypassing normal authentication while attempting to remain undetected. A common backdoor point is a

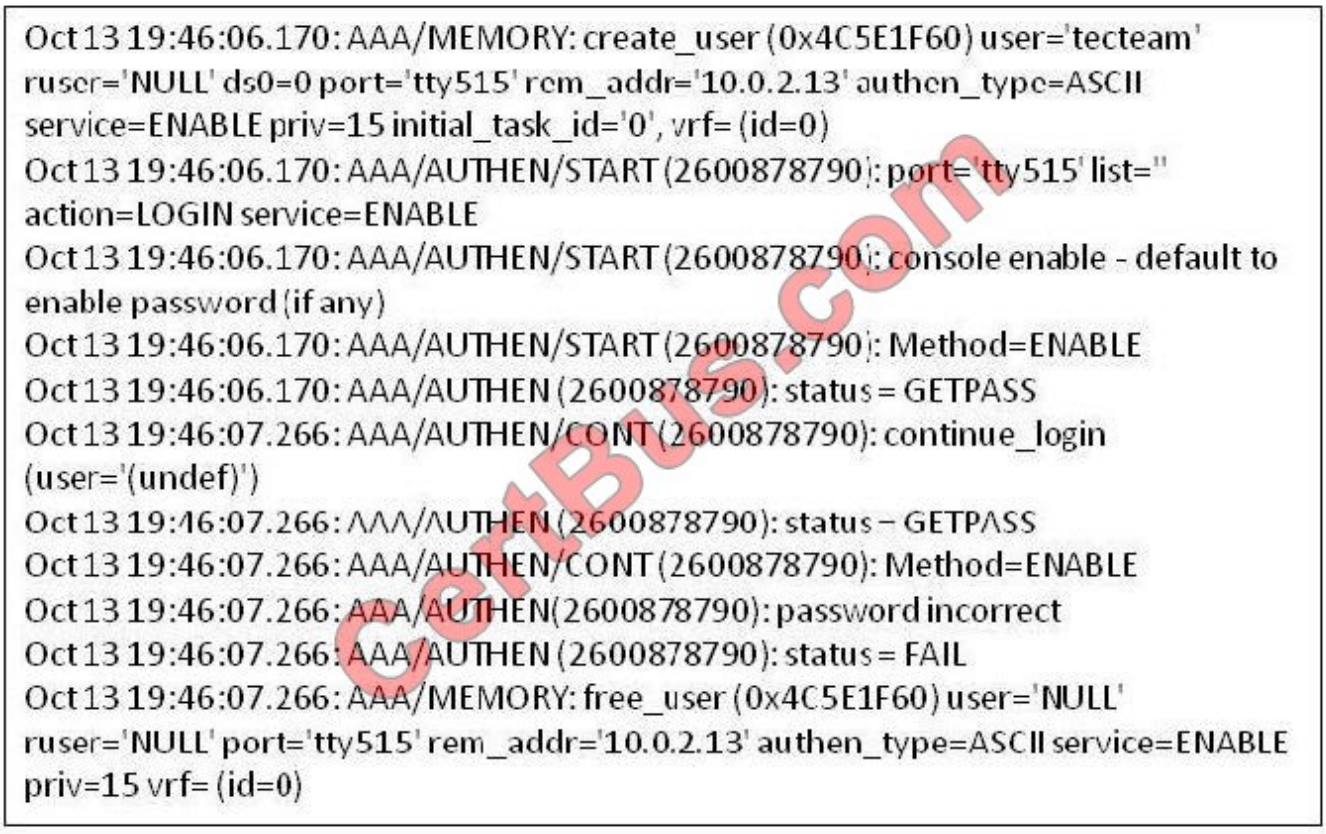
listening port that provides remote access to the system.

Step 7 Leverage the compromised system

After hackers gain administrative access, they attempt to hack other systems.

QUESTION 12

Refer to the exhibit.



Which statement about this output is true?

A. The user logged into the router with the incorrect username and password.

B. The login failed because there was no default enable password.

C. The login failed because the password entered was incorrect.

D. The user logged in and was given privilege level 15.

Correct Answer: C

http://www.cisco.com/en/US/docs/ios/12_2/debug/command/reference/dbfaaa.html

debug aaa authentication To display information on AAA/Terminal Access Controller Access Control System Plus (TACACS+) authentication, use the debug aaa authentication privileged EXEC command. To disable debugging command, use the no form of the command. debug aaa authentication no debug aaa authentication The following is sample output from the debug aaa authentication command. A single EXEC login that uses the "default" method list and the first method, TACACS +, is displayed. The TACACS+ server sends a GETUSER request to prompt for the username and then a GETPASS request to prompt for the password, and finally a PASS response to indicate a successful login. The number 50996740 is the session ID, which is unique for each authentication. Use this ID number to distinguish between different authentications if several are occurring concurrently. Router# debug aaa authentication

6:50:12:

AAA/AUTHEN: create_user user=\\'\\' ruser=\\'\\' port=\\'tty19\\' rem_addr=\\'172.31.60.15\\' authen_type=1 service=1 priv=1

6:50:12:

AAA/AUTHEN/START (0): port=\\'tty19\\' list=\\'\\' action=LOGIN service=LOGIN

6:50:12:

AAA/AUTHEN/START (0): using "default" list

6:50:12:

AAA/AUTHEN/START (50996740): Method=TACACS+

6:50:12:

TAC+ (50996740): received authen response status = GETUSER

6:50:12:

AAA/AUTHEN (50996740): status = GETUSER

6:50:15:

AAA/AUTHEN/CONT (50996740): continue_login

6:50:15:

AAA/AUTHEN (50996740): status = GETUSER

6:50:15:

AAA/AUTHEN (50996740): Method=TACACS+

6:50:15:

TAC+: send AUTHEN/CONT packet

6:50:15:

TAC+ (50996740): received authen response status = GETPASS

6:50:15:

AAA/AUTHEN (50996740): status = GETPASS

6:50:20:

AAA/AUTHEN/CONT (50996740): continue_login

6:50:20:

AAA/AUTHEN (50996740): status = GETPASS

6:50:20:

AAA/AUTHEN (50996740): Method=TACACS+

6:50:20:

TAC+: send AUTHEN/CONT packet

6:50:20:

TAC+ (50996740): received authen response status = PASS

6:50:20:

AAA/AUTHEN (50996740): status = PASS

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.certbus.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: