920-806

Nortel Advanced Data Networking Technology

DEMO

QUESTION NO: 1

An employee wants to set up a wireless network at home, so that the employee can work from anywhere in the house. They know that using the default security settings on the WLAN would leave their network open to attack. They would like to avoid eavesdropping passive network attacks. Which security procedure best provides authentication, encryption, and authorization?

A. Enable 128-bit Wired Equivalent Privacy (WEP).
B. Enable Temporal key integrity protocol (TKIP).
C. Disable broadcast of the Service Set Identifier (SSID).
D. Limit logins to a single MAC address.
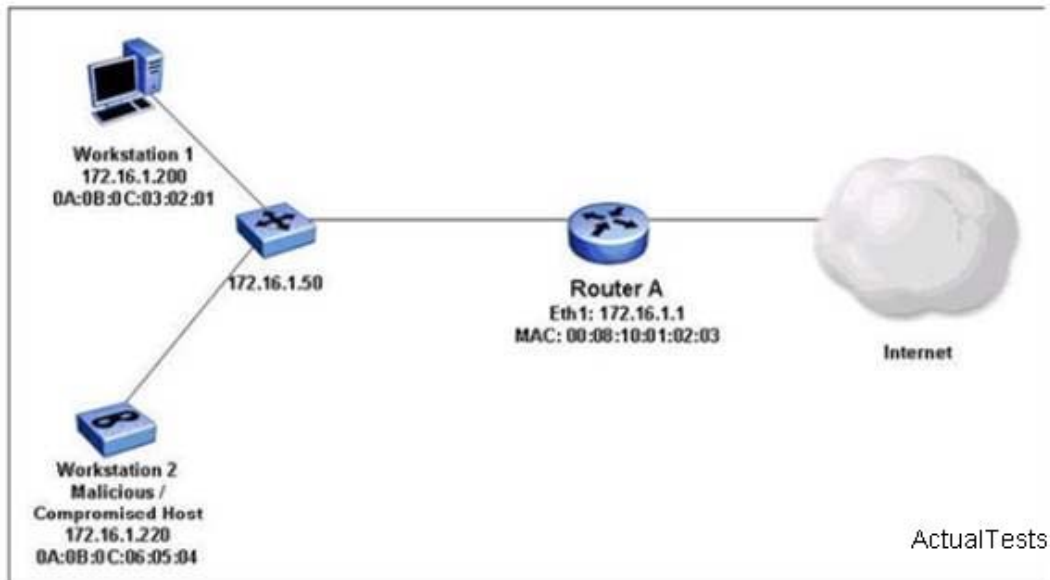
Answer: B

QUESTION NO: 2

A customer is requesting help with deciding what authentication protocol they should use with their Extensible Authentication Protocol over LAN (EAPoL) configuration. Their environment contains the following: switches that support EAP-MD5, EAP-TLS, and PEAP-MSCHAPv2 corporate workstations that run Microsoft Windows 2000 corporate servers that run Microsoft Windows 2003 The solution should have the following characteristics: user credentials should be username and password machine credentials should be hostname and password authenticator credentials should be digital certificates a single sign-on solution machine authentication should occur transparently using a random password assigned to the computer in the domain user authentication should occur transparently using the user credentials when the user logs into the computeruser authentication should occur transparently using the userWhich Extensible Authentication Protocol (EAP) authentication protocol should they select?

A. EAP-MD5
B. EAP-TLS
C. PEAP-MSCHAPv2
D. no supported authentication protocol supports all the requirements

Answer: C

QUESTION NO: 3

Click on the Exhibit button. Workstation 1 wants to send traffic through the router to the Internet. The host on 172.16.1.220 has been compromised by a hacker. The malicious host sends a Gratuitous ARP to Workstation 1 reporting 172.16.1.1 is at 0A:0B:0C:06:05:04 and to Router A reporting 182.16.1.200 is at 0A:0B:0C:06:05:04. Which technique and which type of attack did the hacker use?

A. ARP spoofing, man-in-the-middle

B. ARP spoofing, denial-of-service

C. DHCP spoofing, man-in-the-middle

D. DHCP spoofing, denial-of-service

Answer: A

QUESTION NO: 4

A hacker would like to capture traffic that belongs to other users in the same VLAN on the same switch. To do this they would like to make the switch flood all of the packets on the VLAN. Which technique would the hacker use?

A. ARP spoofing

B. DHCP spoofing

C. MAC overflow

D. ICMP echo

Answer: C

QUESTION NO: 5

A customer is trying to decide what type of VPN to implement. They are trying to decide between an IPSec VPN and a Secure Socket Layer (SSL) VPN. They need to support remote access and branch office VPNs. Which option should they choose and why?

A. SSL VPN, because it does not require client software installation.

B. SSL VPN, because it supports the use of a web browser to establish the VPN.

C. IPSec VPN, because it supports branch office and remote access users.

D. IPSec VPN, because it is supported by all router and firewall implementations.

Answer: C

QUESTION NO: 6

A new corporate policy states that packet capture software or hardware cannot be used on the network. The Information Technology (IT) department has requested that they be excluded from this policy. Which justification best explains why IT needs packet capture software?

A. to troubleshoot device "reachability" issues

B. to troubleshoot communication issues using the software combined with port mirroring

C. to capture user name and password information on the same collision domain

D. to bill departments for network use

Answer: B

QUESTION NO: 7

A hacker has targeted your website for the purpose of denying people access. To make their attack effective they have placed software that will attack your website on multiple machines. What is this type of attack called?

A. man-in-the-middle attacks

B. multiple denial of service attacks

C. distributed denial of service attack

D. packet capture attacks

Answer: C

QUESTION NO: 8

A customer is concerned about implementing Internet Group Management Protocol (IGMP) v2 on their network. They wonder what would happen if a multicast application on their PC either died or was shut down before sending the leave group message. What should you tell the customer to reassure them?

A. The PC will issue a leave message automatically when it receives multicast traffic for a group to which it is not subscribed.

B. The switch will send the multicast stream to the port attached to the PC until the multicast stream ends or the port is inactive.