Passed Cisco 350-018 Exam with Pass4sure and Lead2pass PDF & VCE (21-30)

QUESTION 21
An attacker configures an access point to broadcast the same SSID that is used at a public hot- spot, and launches a deauthentication attack against the clients that are connected to the hot-spot, with the hope that the clients will then associate to the AP of the attacker. In addition to the deauthentication attack, what attack has been launched?

A. man-in-the-middle
B. MAC spoofing
C. Layer 1 DoS
D. disassociation attack

Answer: A

QUESTION 22
Which statement best describes the concepts of rootkits and privilege escalation?

A. Rootkits propagate themselves.
B. Privilege escalation is the result of a rootkit.
C. Rootkits are a result of a privilege escalation.
D. Both of these require a TCP port to gain access.

Answer: B

QUESTION 23
Refer to the exhibit. Which message of the ISAKMP exchange is failing?

```
ISAKMP (62): processing SA payload. message ID = 0
ISAKMP (62): Checking ISAKMP transform 1 against priority 10 policy
                      encryption DES-CBC
                      hash SHA
                      default group 1
                      auth pre-share
ISAKMP (62): atts are acceptable. Next payload is 0
ISAKMP (62): SA is doing pre-shared key authentication
ISAKMP (62): processing KE payload. message ID = 0
ISAKMP (62): processing NONCE payload. message ID = 0
ISAKMP (62): SKEYID state generated
ISAKMP (62): processing vendor id payload
ISAKMP (62): speaking to another Cisco IOS box!
ISAKMP: reserved not zero on ID payload!
%CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 172.16.100.201
 failed its sanity check or is malformed
```

A. main mode 1
B. main mode 3
C. aggressive mode 1
D. main mode 5
E. aggressive mode 2

Answer: B

QUESTION 24

Which multicast capability is not supported by the Cisco ASA appliance?

A. ASA configured as a rendezvous point
B. sending multicast traffic across a VPN tunnel
C. NAT of multicast traffic
D. IGMP forwarding (stub) mode

Answer: B

QUESTION 25
Refer to the exhibit. What type of attack is being mitigated on the Cisco ASA appliance?

```
regex App_regex_1
"[uU][nN][iI][oO][nN]([%]2[0bB]|[+])([aA][lL][lL]([%]2[0bB]|[+]))?
[sS][eE][lL][eE][cC][tT]"
regex App_regex_2 "[Ss][Ee][Ll][Ee][Cc][Tt](%2[0bB]|+)[^\r\x00-
\x19\x7f-\xff]+(%2[0bB]|+)[Ff][Rr][Oo][Mm](%2[0bB]|+)"
!
class-map WebServers
 match port tcp eq www
class-map type inspect http match-any App-map
 match request body regex App_regex_1
 match request body regex App_regex_2
!
policy-map type inspect http drop-Protocol
parameters
  body-match-maximum  3000
class App-map
  drop-connection log
policy-map protocol-traffic
class WebServers
  inspect http drop-Protocol
!
service-policy protocol-traffic interface outside
```

A. HTTPS certificate man-in-the-middle attack
B. HTTP distributed denial of service attack
C. HTTP Shockwave Flash exploit
D. HTTP SQL injection attack

Answer: D

QUESTION 26
Which method of output queuing is supported on the Cisco ASA appliance?

A. CBWFQ
B. priority queuing
C. MDRR
D. WFQ
E. custom queuing

Answer: B

QUESTION 27
Which four values can be used by the Cisco IPS appliance in the risk rating calculation? (Choose four.)

A. attack severity rating
B. target value rating
C. signature fidelity rating
D. promiscuous delta
E. threat rating
F. alert rating

Answer: ABCD

QUESTION 28
Which three authentication methods does the Cisco IBNS Flexible Authentication feature support? (Choose three.)

A. cut-through proxy
B. dot1x
C. MAB
D. SSO
E. web authentication

Answer: BCE

QUESTION 29
Troubleshooting the web authentication fallback feature on a Cisco Catalyst switch shows that clients with the 802.1X supplicant are able to authenticate, but clients without the supplicant are not able to use web authentication. Which configuration option will correct this issue?

A. switch(config)# aaa accounting auth-proxy default start-stop group radius
B. switch(config-if)# authentication host-mode multi-auth
C. switch(config-if)# webauth
D. switch(config)# ip http server
E. switch(config-if)# authentication priority webauth dot1x

Answer: D

QUESTION 30
Which option on the Cisco ASA appliance must be enabled when implementing botnet traffic filtering?

A. HTTP inspection
B. static entries in the botnet blacklist and whitelist
C. global ACL
D. NetFlow
E. DNS inspection and DNS snooping

Answer: E

If you want to pass Cisco 350-018 successfully, donot missing to read latest lead2pass Cisco 350-018 practice exams.
If you can master all lead2pass questions you will able to pass 100% guaranteed.

http://www.lead2pass.com/350-018.html