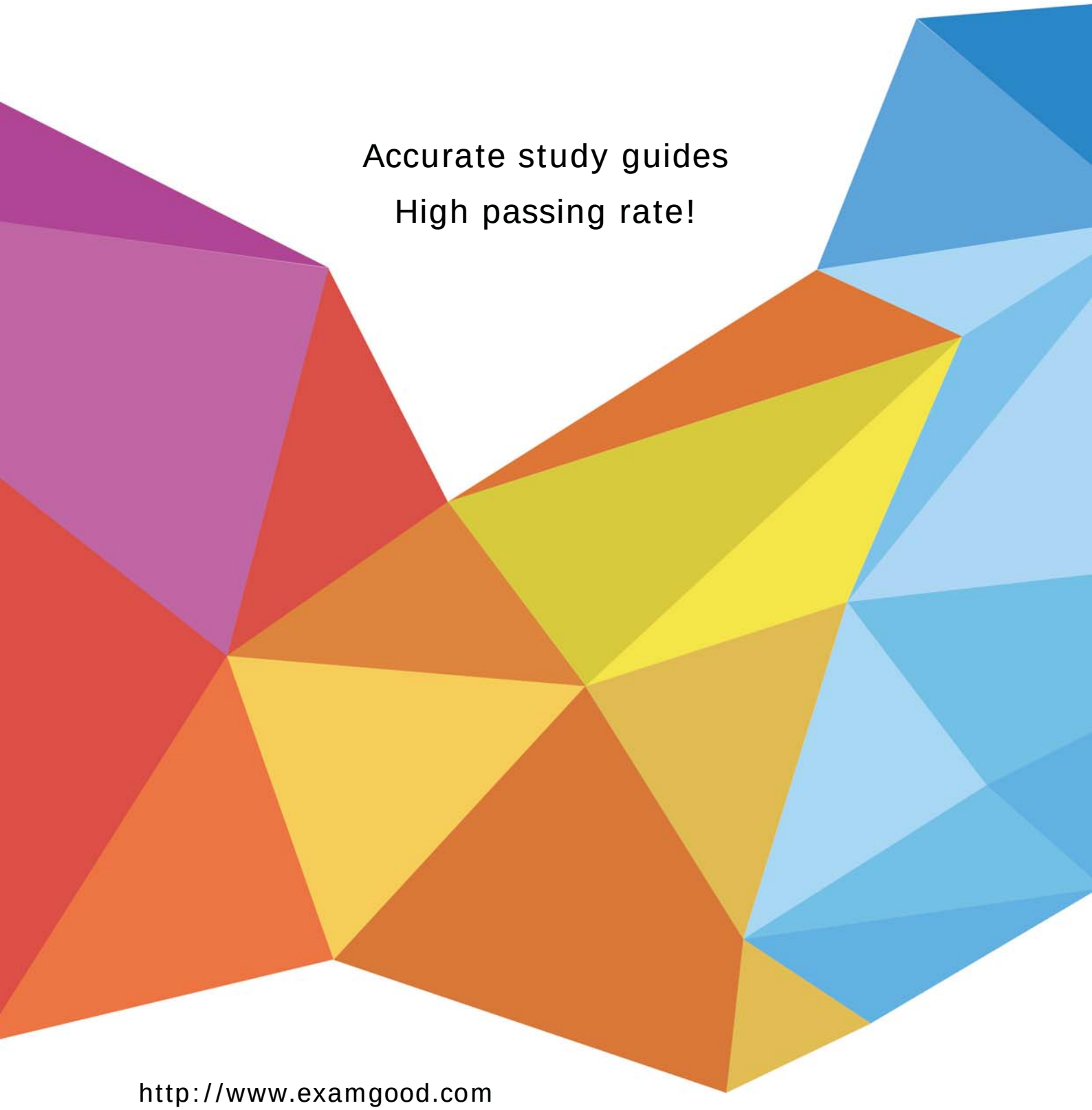
EXAMGOOD

QUESTION & ANSWER

Exam Good provides update free of charge in one year!



Accurate study guides

High passing rate!

Exam : **GCCC**

Title : GIAC Critical Controls Certification (GCCC)

Version : DEMO

1.Dragonfly Industries requires firewall rules to go through a change management system before they are configured. Review the change management log.

Line	Date	Port	Internal Host(s)	External Host(s)	In/Out/Both	Length rule is needed	Reason
1	1/15/2013	22	8.8.207.97	10.10.12.100	in	6 weeks	software set-up
2	5/12/2013	25	10.1.1.7	any	out	indefinite	marketing mail delivery
3	6/17/2013	8080	10.10.12.252	8.8.0.0/24	in	indefinite	network backup transfers
4	10/21/2013	80	any	74.125.228.2	out	indefinite	prevent video browsing
5	4/4/2014	443	10.10.12.17	any	in	indefinite	enable secure access

Which of the following lines in your firewall ruleset has expired and should be removed from the configuration?

A. access-list outbound permit tcp host 10.1.1.7 any eq smtp

B. access-list outbound deny tcp any host 74.125.228.2 eq www

C. access-list inbound permit tcp 8.8.0.0 0.0.0.255 10.10.12.252 eq 8080

D. access-list inbound permit tcp host 8.8.207.97 host 10.10.12.100 eq ssh

Answer: D

2.Which of the following actions produced the output seen below?

```
C3PO:Documents student$ diff firewallrules.txt firewallrules2.txt

< access-list inbound permit tcp 8.8.0.0 0.0.0.255 10.10.12.252 eq 8080
---
> access-list inbound permit tcp 8.8.0.0 0.0.0.255 10.10.12.252 eq 8080
> access-list inbound permit tcp host 209.7.159.53 any 3389
```

A. An access rule was removed from firewallrules.txt

B. An access rule was added to firewallrules2.txt

C. An access rule was added to firewallrules.txt

D. An access rule was removed from firewallrules2.txt

Answer: B

3.An organization has implemented a policy to detect and remove malicious software from its network. Which of the following actions is focused on correcting rather than preventing attack?

A. Configuring a firewall to only allow communication to whitelisted hosts and ports

B. Using Network access control to disable communication by hosts with viruses

C. Disabling autorun features on all workstations on the network

D. Training users to recognize potential phishing attempts

Answer: B

4.An Internet retailer's database was recently exploited by a foreign criminal organization via a remote attack. The initial exploit resulted in immediate root-level access.

What could have been done to prevent this level of access being given to the intruder upon successful exploitation?

A. Configure the DMZ firewall to block unnecessary service

B. Install host integrity monitoring software

C. Install updated anti-virus software

D. Configure the database to run with lower privileges

Answer: D

5.As part of an effort to implement a control on E-mail and Web Protections, an organization is monitoring their webserver traffic.
Which event should they receive an alert on?
A. The number of website hits is higher that the daily average
B. The logfiles of the webserver are rotated and archived
C. The website does not respond to a SYN packet for 30 minutes
D. The website issues a RST to a client after the connection is idle
Answer: C