GCIA Q&As

GIAC Certified Intrusion Analyst

Pass GIAC GCIA Exam with 100% Guarantee

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

https://www.leads4pass.com/gcia.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has written the following snort signature:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"John be alert"; flow:to_server,established; content:"Content-Disposition|3A|"; nocase;
pcre:"/filename\s*=\s* *?\.(?=[abcdehijlmnoprsvwx]) (a(d[ep]|s[dfk])|c ([ho]m|li|md|pp)|d(iz|ll|ot)|e(m[fl]|xe)|h(lp|sq|ta)|jse?|m(d[abew]|s [ip])|p(p[st]
|f|[lm]|ot)|r(eg|tf)|s(cr|[hy]s|wf)|v(b[es]?|cf|xd)|w(m [dfsz]|p[dmsz]|s[cfh])|xl[tw]|bat|ms|lnk|nws|ocx)[\x27\x22\n\r\s]/iR"; classtype:suspicious-filename-
detect; sid:721; rev:8;)
```

Which of the following statements about this snort signature is true?

A. It detects the session splicing IDS evasion attack.

B. It detects AOL IM chat.

C. It detects Yahoo IM chat.

D. It detects the bad file attachments coming to the mail server.

Correct Answer: D

QUESTION 2

You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. A branch office is connected to the headquarters through a T1 line. Users at the branch office report poor voice quality on the IP phone while communicating with the headquarters. You find that an application, named WorkReport, at the branch office is suffocating bandwidth by sending large packets for file synchronization. You need to improve the voice quality on the IP phone. Which of the following steps will you choose to accomplish this?

A. Configure traffic shaping to increase the time interval for the WorkReport packets.

B. Configure traffic shaping to increase the time interval for the IP phone packets.

C. Configure traffic shaping to reduce bandwidth for the IP phone.

D. Configure traffic shaping to reduce bandwidth for WorkReport.

Correct Answer: D

QUESTION 3

Which of the following wireless security features provides the best wireless security mechanism?

A. WPA

B. WPA with Pre Shared Key

C. WPA with 802.1X authentication

D. WEP

Correct Answer: C

QUESTION 4

Which of the following Linux file systems is a journaled file system?

A. ext3

B. ext4

C. ext2

D. ext

Correct Answer: A

QUESTION 5

Which of the following conclusions can be drawn from viewing the given output generated by the PING command-line utility?

A. The network bandwidth is heavily utilized.

B. The IP address of the destination computer is not resolved.

C. There is no connectivity between the source and the destination computer.

D. The hub is not working.

Correct Answer: C