GCIH Q&As

GIAC Certified Incident Handler

Pass GIAC GCIH Exam with 100% Guarantee

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

https://www.geekcert.com/gcih.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

FILL BLANK

Fill in the blank with the appropriate name of the tool.

_____ scans for rootkits by comparing SHA-1 hashes of important files with known good ones in online database.

A. rkhunter

Correct Answer: A

QUESTION 2

Which of the following netcat parameters makes netcat a listener that automatically restarts itself when a connection is dropped?

A. -u

B. -l

C. -p

D. -L

Correct Answer: D

QUESTION 3

Which Wireless LAN discovery tool uses active scanning in order to detect wireless networks?

A. Air Magnet

B. WarVOX

C. Kismet

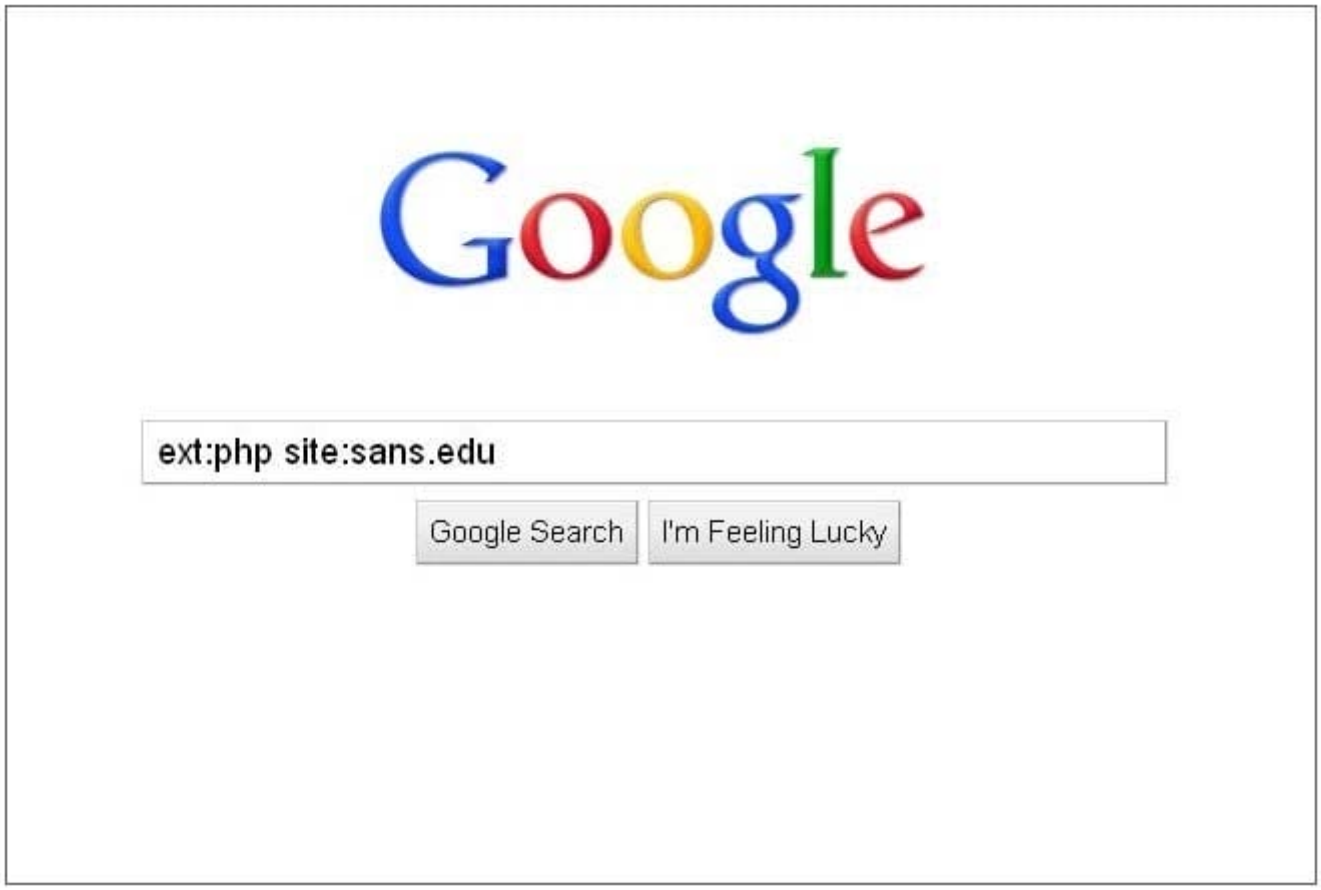
D. NetStumbler

Correct Answer: D

NetStumbler (version 0.4 and earlier) works solely by sending out a constant stream of probe requests without an SSID, hoping that an access point will respond with a probe response that includes its SSID.

QUESTION 4

Analyze the screenshot below. What will the search return?



A. Files with the extension .php from the domain sans.edu

B. Documents containing the term "php" from the site www.sans.edu

C. Links to the site www.sans.edu containing PHP documents

D. Files with valid PHP headers from the domain sans.edu

Correct Answer: A

The search will return all files of type php from the site sans.edu

QUESTION 5

How would a worm be able to affect hosts running different operating systems be classified?

A. Zero-Day Worm

B. Multi-Platform Worm

C. Polymorphic Worm

D. Fast Flux Worm

Correct Answer: B

While not mainstream (yet), we have already seen a small number of multi-platform worms released against the Internet. For example, in May 2001, the Sadmind/IIS worm mushroomed through the Internet, targeting Sun Solaris and Microsoft

Windows.

Other types of worm classifications or characteristics, such as zero-day, polymorphic and fast flux, do not meet this definition.