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.passapply.com/gcih.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which security practice is most likely to reduce worm infections?

A. Encryption

B. Awareness training

C. Administrative privilege controls

D. Device inventory

E. Patching

Correct Answer: B

QUESTION 2

Which of the following attacks capture the secret value like a hash and reuse it later to gain access to a system without ever decrypting or decoding the hash?

A. Cross Site Scripting attack

B. Replay attack

C. Rainbow attack

D. Hashing attack

Correct Answer: B

QUESTION 3

During which Incident Handling phase would steps for preventing successful worm attacks occur, such as developing patch management and file encryption policies and processes?

A. Preparation

B. Containment

C. Identification

D. Eradication

E. Recovery

Correct Answer: A

When protecting your network from malware, such as worms, examples of controls to consider during the Preparation phase include: Buffer overflow defenses help a lot here: Patches, non-executable system stacks, and host-based IPS A process for rapidly testing and deploying patches when available Encrypt data on your hard drives: If it\\'s stolen by a

worm or bot, attackers can\\'t read it...unless they also steal the key

QUESTION 4

Which of the following devices would return information about internal targets during an ACK scan?

A. A firewall that does not monitor the connection state of an inbound packet

B. A web-proxy that allows only outbound connections over tcp/8080

C. An IDS connected to a mirror port of the border router

D. A border device that drops inbound connections that use a flag other than SYN

Correct Answer: A

An ACK scan is particularly useful in getting through simple router-based firewalls. If a router allows "established" connections in (and is not using any stateful inspection), an attacker can use ACK scans to send packets into the network. A border device (firewall, advanced router, etc.) that requires state for inbound connections will be definition drop inbound packets with the ACK flag, negating the effectiveness of an ACK scan. A web-proxy that only allows outbound connections will ignore an ACK scan. An IDS connected to a mirror port does not have an IP address to target with an ACK scan nor is there anything "behind the IDS" to map.

QUESTION 5

Which of the following HTTP requests is the SQL injection attack?

A. http://www.xsecurity.com/cgiin/bad.cgi?foo=..%fc%80%80%80%80%af../bin/ls%20-al

B. http://www.victim.com/example?accountnumber=67891andcreditamount=999999999

C. http://www.myserver.com/search.asp?lname=adam%27%3bupdate%20usertable%20set% 20pass wd%3d %27hCx0r%27%3b--%00

D. http://www.myserver.com/script.php?mydata=%3cscript%20src=%22http%3a%2f%2fwww.yourser ver.c0m %2fbadscript.js%22%3e%3c%2fscript%3e

Correct Answer: C