



CERTSWARRIOR

GIAC GLIR

GIAC Linux Incident Responder

Questions&AnswersPDF

ForMoreInformation:

<https://www.certswarrior.com/>

Features:

- 90DaysFreeUpdates
- 30DaysMoneyBackGuarantee
- InstantDownloadOncePurchased
- 24/7OnlineChat Support
- ItsLatestVersion

Visit us at: <https://www.certswarrior.com/exam/glir>

Latest Version: 6.0

Question: 1

Which tools can help in viewing or processing logs from the systemd journal?
(Choose two)

- A. journalctl
- B. less
- C. auditctl
- D. rsyslog

Answer: A,D

Question: 2

Which issues can affect the reliability of Linux forensic timelines?
(Choose two)

- A. Logging of shell history
- B. Use of SSDs with TRIM functionality
- C. Log rotation and overwrites
- D. Excessive CPU usage

Answer: B,C

Question: 3

Where are boot-related messages typically logged in Linux systems?

- A. /var/log/messages
- B. /var/log/boot.log
- C. /var/log/audit/audit.log
- D. /var/log/secure

Answer: B

Question: 4

What actions are essential when mounting evidence from a disk image for analysis?
(Choose two)

- A. Use a read-write mode for deeper inspection
- B. Mount using a loop device
- C. Ensure system time is synchronized
- D. Record hash values before and after mounting

Answer: B,D

Question: 5

Which command provides a list of active network connections on a Linux system?

- A. ss -tuln
- B. lsof -nP
- C. mount
- D. ps -ef

Answer: A

Question: 6

What is a typical sign of file-based persistence in a Linux environment?

- A. A cron job set to delete temp files hourly
- B. A suspicious binary copied to /usr/local/bin
- C. A symlink created in /etc/skel
- D. A temporary file in /tmp/ directory

Answer: B

Question: 7

Where are user-installed libraries typically stored in a Linux system?

- A. /usr/lib
- B. /lib64
- C. /lib
- D. /var/lib

Answer: A

Question: 8

Why is it important to integrate threat intelligence into incident response playbooks?

- A. To eliminate the need for log review
- B. To ensure patches are automatically installed
- C. To bypass Linux kernel security modules
- D. To tailor detection and response steps based on known threat behavior

Answer: D

Question: 9

What does the regular expression `^/home/[a-z]+$` match?

- A. All files ending with `.home`
- B. Directories under `/home` with numeric characters
- C. Paths under `/home` ending with lowercase letters only
- D. Files in `/home` with capital letters

Answer: C

Question: 10

Which Linux directories are critical for storing kernel modules and drivers?
(Choose two)

- A. `/lib/modules`
- B. `/usr/src`
- C. `/boot`
- D. `/dev`

Answer: A,C



CERTSWARRIOR

FULL PRODUCT INCLUDES:

Money Back Guarantee



Instant Download after Purchase



90 Days Free Updates



PDF Format Digital Download



24/7 Live Chat Support



Latest Syllabus Updates



For More Information – Visit link below:

<https://www.certswarrior.com>

16 USD Discount Coupon Code: U89DY2AQ