250-441 Q&As

Administration of Symantec Advanced Threat Protection 3.0

Pass Symantec 250-441 Exam with 100% Guarantee

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

https://www.passapply.com/250-441.html

100% Passing Guarantee
100% Money Back Assurance

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

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

QUESTION 1

Which stage of an Advanced Persistent Threat (APT) attack do attackers map an organization\\'s defenses from the inside?

A. Discovery

B. Capture

C. Exfiltration

D. Incursion

Correct Answer: A

Reference: http://www.whymeridian.com/blog/bid/399610/5-Stages-of-an-Advanced-Persistent-ThreatAttack-on-Your-Network

QUESTION 2

Which stage of an Advanced Persistent Threat (APT) attack do attackers send information back to the home base?

A. Capture

B. Incursion

C. Discovery

D. Exfiltration

Correct Answer: D

Reference: https://www.symantec.com/content/en/us/enterprise/white_papers/badvanced_persistent_threats_WP_21215957.en-us.pdf

QUESTION 3

What should an Incident Responder do to mitigate a false positive?

A. Add to Whitelist

B. Run an indicators of compromise (IOC) search

C. Submit to VirusTotal

D. Submit to Cynic

Correct Answer: B

QUESTION 4

Which final steps should an Incident Responder take before using ATP to rejoin a remediated endpoint to the network, according to Symantec best practices?

A. Run an additional antivirus scan with the latest definitions. If the scan comes back as clean, rejoin the computer to the production network.

B. Run Windows Update to patch the system with the latest service pack. Once the system is up-to-date, rejoin the computer to the production network.

C. Use SymDiag to run a Threat Scan Analysis on the machine. Once the analysis comes back as clean, rejoin the computer to the production network.

D. Upgrade the client to the latest version of SEP. Once the client is upgraded, rejoin the computer to the production network.

Correct Answer: D

QUESTION 5

An Incident Responder wants to run a database search that will list all client named starting with SYM. Which syntax should the responder use?

A. hostname like "SYM"

B. hostname "SYM"

C. hostname "SYM*"

D. hostname like "SYM*"

Correct Answer: A

Reference: https://support.symantec.com/en_US/article.HOWTO124805.html