PCCET Q&As

Palo Alto Networks Certified Cybersecurity Entry-level Technician

Pass Palo Alto Networks PCCET Exam with 100% Guarantee

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

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

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

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

QUESTION 1

Anthem server breaches disclosed Personally Identifiable Information (PII) from a number of its servers. The infiltration by hackers was attributed to which type of vulnerability?

A. an intranet-accessed contractor\\'s system that was compromised

B. exploitation of an unpatched security vulnerability

C. access by using a third-party vendor\\'s password

D. a phishing scheme that captured a database administrator\\'s password

Correct Answer: D

QUESTION 2

On an endpoint, which method should you use to secure applications against exploits?

A. endpoint-based firewall

B. strong user passwords

C. full-disk encryption

D. software patches

Correct Answer: D

New software vulnerabilities and exploits are discovered all the time and thus diligent software patch management is required by system and security administrators in every organization.

QUESTION 3

A user is provided access over the internet to an application running on a cloud infrastructure. The servers, databases, and code of that application are hosted and maintained by the vendor.

Which NIST cloud service model is this?

A. IaaS

B. SaaS

C. PaaS

D. CaaS

Correct Answer: B

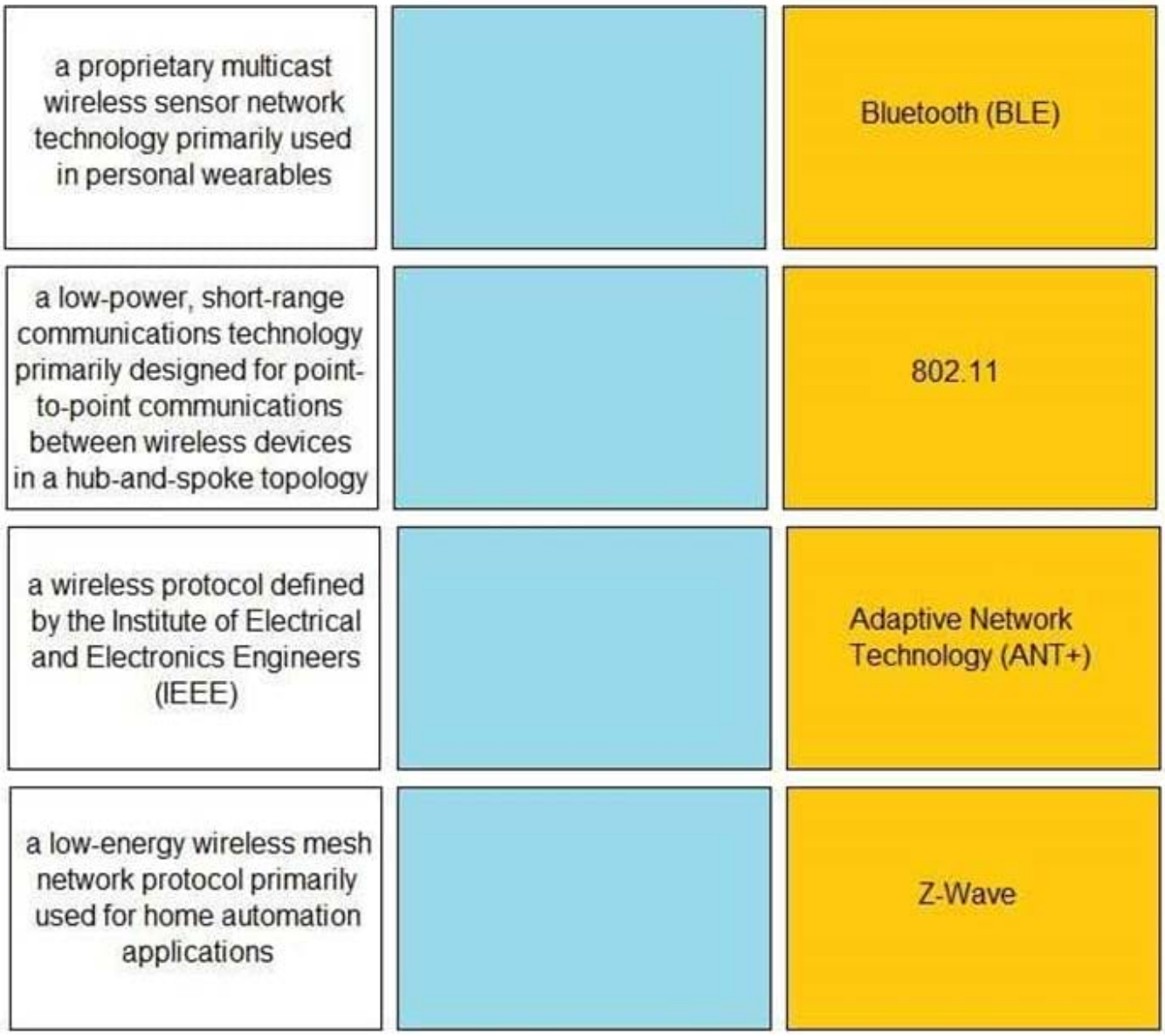
SaaS - User responsible for only the data, vendor responsible for rest

QUESTION 4

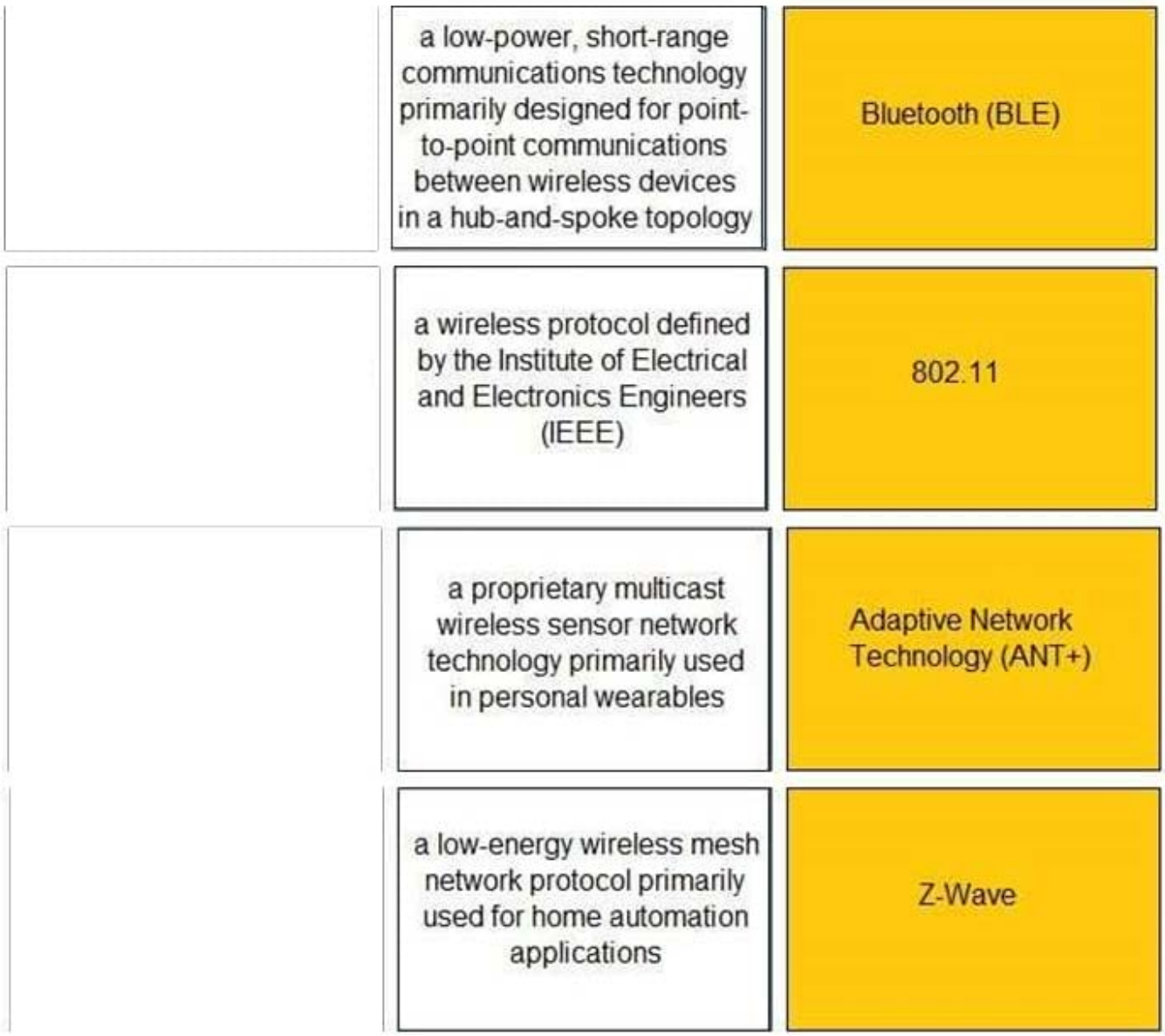
DRAG DROP

Match the IoT connectivity description with the technology.

Select and Place:



Correct Answer:



QUESTION 5

Which method is used to exploit vulnerabilities, services, and applications?

A. encryption

B. port scanning

C. DNS tunneling

D. port evasion

Correct Answer: D

Attack communication traffic is usually hidden with various techniques and tools, including: Encryption with SSL, SSH (Secure Shell), or some other custom or proprietary encryption Circumvention via proxies, remote access tools, or

tunneling. In some instances, use of cellular networks enables complete circumvention of the target network for attack C2 traffic. Port evasion using network anonymizers or port hopping to traverse over any available open ports Fast Flux (or Dynamic DNS) to proxy through multiple infected endpoints or multiple, ever-changing C2 servers to reroute traffic and make determination of the true destination or attack source difficult DNS tunneling is used for C2 communications and data infiltration

Latest PCCET Dumps PCCET Exam Questions PCCET Braindumps