Free Questions for PCCET by ebraindumps

Shared by Mueller on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- encryption

B- port scanning

C- DNS tunneling

D- port evasion

Answer:

D

Explanation:

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

Question 2

Question Type: **MultipleChoice**

Which type of malware takes advantage of a vulnerability on an endpoint or server?

Options:

A- technique

B- patch

C- vulnerability

D- exploit

Answer:

A

Question 3

Question Type: **MultipleChoice**

How does Prisma SaaS provide protection for Sanctioned SaaS applications?

Options:

A- Prisma SaaS connects to an organizations internal print and file sharing services to provide protection and sharing visibility

B- Prisma SaaS does not provide protection for Sanctioned SaaS applications because they are secure

C- Prisma access uses Uniform Resource Locator (URL) Web categorization to provide protection and sharing visibility

D- Prisma SaaS connects directly to sanctioned external service providers SaaS application service to provide protection and sharing visibility

Answer:

D

Explanation:

Prisma SaaS connects directly to the applications themselves, therefore providing continuous silent monitoring of the risks within the sanctioned SaaS applications, with detailed visibility that is not possible with traditional security solutions.

Question 4

Question Type: MultipleChoice

What is the key to "taking down" a botnet?

Options:

A- prevent bots from communicating with the C2

B- install openvas software on endpoints

C- use LDAP as a directory service

D- block Docker engine software on endpoints

Answer:

A

Question 5

Question Type: **MultipleChoice**

What does Palo Alto Networks Cortex XDR do first when an endpoint is asked to run an executable?

Options:

A- run a static analysis

B- check its execution policy

C- send the executable to WildFire

D- run a dynamic analysis

Answer:

B

Question 6

Question Type: **MultipleChoice**

Which IoT connectivity technology is provided by satellites?

Options:

A- 4G/LTE

B- VLF

C- L-band

D- 2G/2.5G

Answer:

C

Explanation:

2G/2.5G: 2G connectivity remains a prevalent and viable IoT connectivity option due

to the low cost of 2G modules, relatively long battery life, and large installed base of

2G sensors and M2M applications.

3G: IoT devices with 3G modules use either Wideband Code Division Multiple Access

(W-CDMA) or Evolved High Speed Packet Access (HSPA+ and Advanced HSPA+) to

achieve data transfer rates of 384Kbps to 168Mbps.

4G/Long-Term Evolution (LTE): 4G/LTE networks enable real-time IoT use cases, such

as autonomous vehicles, with 4G LTE Advanced Pro delivering speeds in excess of

3Gbps and less than 2 milliseconds of latency.

5G: 5G cellular technology provides significant enhancements compared to 4G/LTE

networks and is backed by ultra-low latency, massive connectivity and scalability for IoT devices, more efficient use of the licensed spectrum, and network slicing for application traffic prioritization.

Question 7

Question Type: MultipleChoice

SecOps consists of interfaces, visibility, technology, and which other three elements? (Choose three.)

Options:

A- People

B- Accessibility

C- Processes

D- Understanding

E- Business

Answer:

A, C, E

Explanation:

The six pillars include:

1. Business (goals and outcomes)

2. People (who will perform the work)

3. Interfaces (external functions to help achieve goals)

4. Visibility (information needed to accomplish goals)

5. Technology (capabilities needed to provide visibility and enable people)

6. Processes (tactical steps required to execute on goals)

All elements must tie back to the business itself and the goals of the security operations

Question 8

Question Type: MultipleChoice

In which two cloud computing service models are the vendors responsible for vulnerability and patch management of the underlying operating system? (Choose two.)

Options:

A- SaaS

B- PaaS

C- On-premises

D- IaaS

Answer:

A, B

Question 9

Question Type: **MultipleChoice**

Data Loss Prevention (DLP) and Cloud Access Security Broker (CASB) fall under which Prisma access service layer?

Options:

A- Network

B- Management

C- Cloud

D- Security

Answer:

D

Explanation:

A SASE solution converges networking and security services into one unified, cloud-delivered solution (see Figure 3-12) that includes the following:

Networking

Software-defined wide-area networks (SD-WANs)

Virtual private networks (VPNs)

Zero Trust network access (ZTNA)

Quality of Service (QoS)

Security

Firewall as a service (FWaaS)

Domain Name System (DNS) security

Threat prevention

Secure web gateway (SWG)

Data loss prevention (DLP)

Cloud access security broker (CASB)

Question 10

Question Type: MultipleChoice

In SecOps, what are two of the components included in the identify stage? (Choose two.)

Options:

A- Initial Research

B- Change Control

C- Content Engineering

D- Breach Response

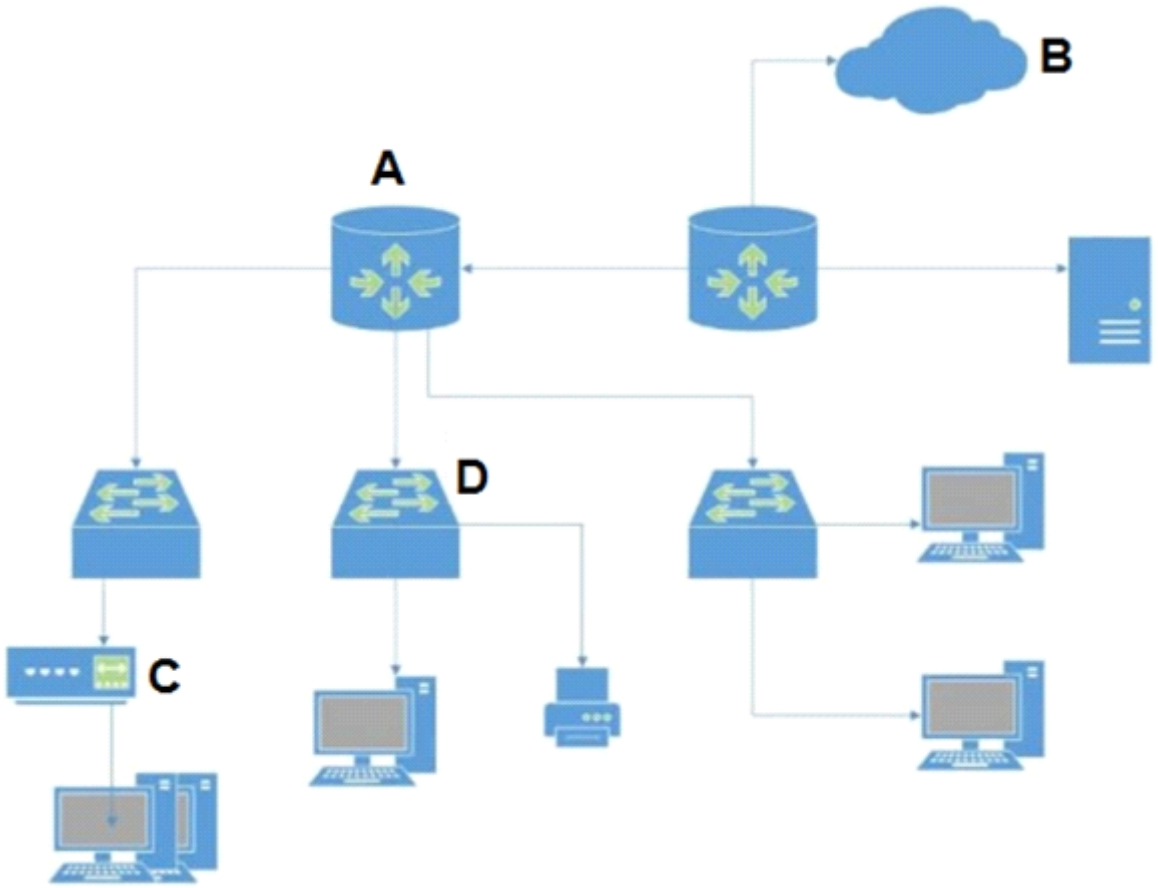
Answer:

A, C

Question 11

Question Type: MultipleChoice

In the attached network diagram, which device is the switch?



Options:

A- A

B- B

C- C

D- D

Answer:

D