Vendor: Palo Alto Networks

Exam Code: PCCET

Exam Name: Palo Alto Networks Certified Cybersecurity Entry-level Technician

Version: DEMO

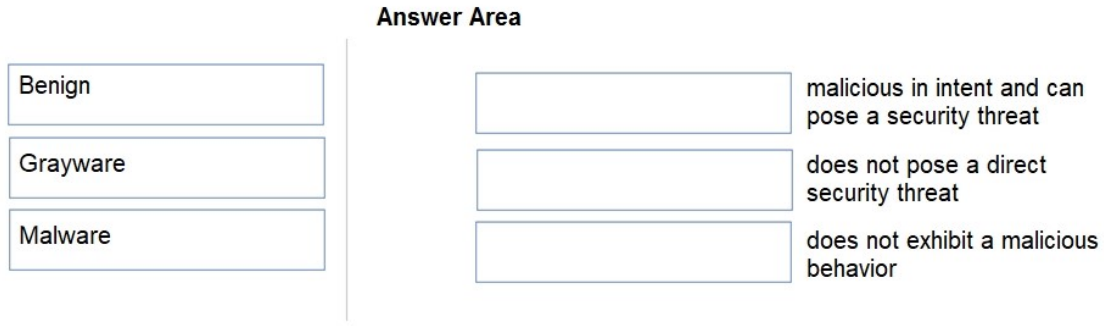
QUESTION 1
Which method is used to exploit vulnerabilities, services, and applications?

A. encryption
B. port scanning
C. DNS tunneling
D. port evasion

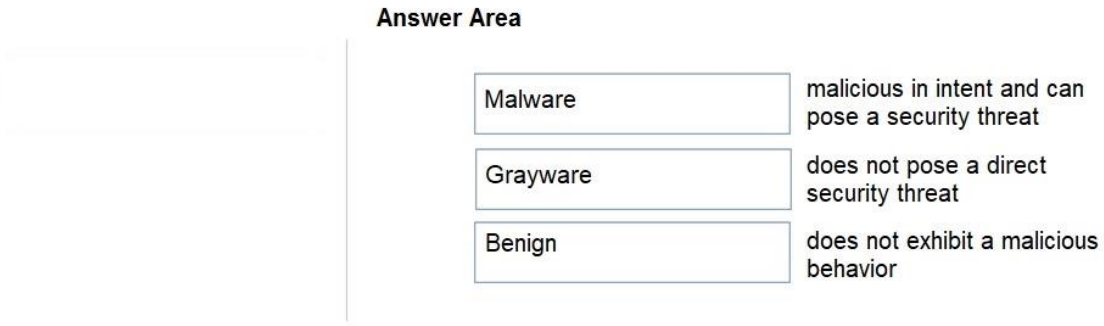
Answer: D
Explanation:
Attack communication traffic is usually hidden with various techniques and tools, including:
Encryption with SSL, SSH (Secure Shell), or some other custom or proprietary encryption
Circumvention via proxies, remote access tools, or tunneling. In some instances, use of cellular 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
Drag and Drop Question

Match the Palo Alto Networks WildFire analysis verdict with its definition.



Answer:



Explanation:
Benign: Safe and does not exhibit malicious behavior

Grayware: No security risk but might display obtrusive behavior (for example, adware, spyware, and browser helper objects)
Malware: Malicious in nature and intent and can pose a security threat (for example, viruses, worms, trojans, root kits, botnets, and remote-access toolkits) Phishing: Malicious attempt to trick the recipient into revealing sensitive data

QUESTION 3
Which element of the security operations process is concerned with using external functions to help achieve goals?

A. interfaces
B. business
C. technology
D. people

Answer: A
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)

QUESTION 4
Which classification of IDS/IPS uses a database of known vulnerabilities and attack profiles to identify intrusion attempts?

A. Statistical-based
B. Knowledge-based
C. Behavior-based
D. Anomaly-based

Answer: B
Explanation:
A knowledge-based system uses a database of known vulnerabilities and attack profiles to identify intrusion attempts. These types of systems have lower false-alarm rates than behavior-based systems but must be continually updated with new attack signatures to be effective.
A behavior-based system uses a baseline of normal network activity to identify unusual patterns or levels of network activity that may be indicative of an intrusion attempt. These types of systems are more adaptive than knowledge-based systems and therefore may be more effective in detecting previously unknown vulnerabilities and attacks, but they have a much higher false-positive rate than knowledge-based systems.

QUESTION 5
Which analysis detonates previously unknown submissions in a custom-built, evasion-resistant virtual environment to determine real-world effects and behavior?

A. Dynamic
B. Pre-exploit protection

C. Bare-metal
D. Static

Answer: A
Explanation:
The WildFire cloud-based malware analysis environment is a cyber threat prevention service that identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment.

QUESTION 6
Which type of Wi-Fi attack depends on the victim initiating the connection?

A. Evil twin
B. Jasager
C. Parager
D. Mirai

Answer: A
Explanation:
Perhaps the easiest way for an attacker to find a victim to exploit is to set up a wireless access point that serves as a bridge to a real network. An attacker can inevitably bait a few victims with "free Wi- Fi access." The main problem with this approach is that it requires a potential victim to stumble on the access point and connect. The attacker can't easily target a specific victim, because the attack depends on the victim initiating the connection.
https://www.paloaltonetworks.com/blog/2013/11/wireless-man-middle/

QUESTION 7
Which organizational function is responsible for security automation and eventual vetting of the solution to help ensure consistency through machine-driven responses to security issues?

A. NetOps
B. SecOps
C. SecDevOps
D. DevOps

Answer: B
Explanation:
Security operations (SecOps) is a necessary function for protecting the digital way of life, for global businesses and customers. SecOps requires continuous improvement in operations to handle fast- evolving threats. SecOps needs to arm security operations professionals with high-fidelity intelligence, contextual data, and automated prevention workflows to quickly identify and respond to these threats. SecOps must leverage automation to reduce strain on analysts and execute the Security Operation Center's (SOC) mission to identify, investigate, and mitigate threats.

QUESTION 8
Which Palo Alto Networks tools enable a proactive, prevention-based approach to network automation that accelerates security analysis?

A. MineMeld
B. AutoFocus

C. WildFire
D. Cortex XDR

Answer: B
Explanation:
Palo Alto Networks AutoFocus enables a proactive, prevention-based approach to network security that puts automation to work for security professionals. Threat intelligence from the service is made directly accessible in the Palo Alto Networks platform, including PAN-OS software and Panorama. AutoFocus speeds the security team's existing workflows, which allows for in-depth investigation into suspicious activity, without additional specialized resources.

QUESTION 9
Which endpoint product from Palo Alto Networks can help with SOC visibility?

A. STIX
B. Cortex XDR
C. WildFire
D. AutoFocus

Answer: B
Explanation:
XDR solutions bring a proactive approach to threat detection and response. It delivers visibility across all data, including endpoint, network, and cloud data, while applying analytics and automation to address today's increasingly sophisticated threats. With XDR, cybersecurity teams can:
- Identify hidden, stealthy, and sophisticated threats proactively and quickly
- Track threats across any source or location within the organization
- Increase the productivity of the people operating the technology
- Get more out of their security investments
- Conclude investigations more efficiently

QUESTION 10
Which technique changes protocols at random during a session?

A. use of non-standard ports
B. port hopping
C. hiding within SSL encryption
D. tunneling within commonly used services

Answer: B
Explanation:
Port hopping, in which ports and protocols are randomly changed during a session.

QUESTION 11
What is the primary security focus after consolidating data center hypervisor hosts within trust levels?

A. control and protect inter-host traffic using routers configured to use the Border Gateway Protocol (BGP) dynamic routing protocol
B. control and protect inter-host traffic by exporting all your traffic logs to a sysvol log server using the User Datagram Protocol (UDP)

C. control and protect inter-host traffic by using IPv4 addressing
D. control and protect inter-host traffic using physical network security appliances

Answer: D
Explanation:
Consolidating servers within trust levels: Organizations often consolidate servers within the same trust level into a single virtual computing environment: ... ... This virtual systems capability enables a single physical device to be used to simultaneously meet the unique requirements of multiple VMs or groups of VMs. Control and protection of inter-host traffic with physical network security appliances that are properly positioned and configured is the primary security focus.

QUESTION 12
Which product from Palo Alto Networks extends the Security Operating Platform with the global threat intelligence and attack context needed to accelerate analysis, forensics, and hunting workflows?

A. Global Protect
B. WildFire
C. AutoFocus
D. STIX

Answer: C
Explanation:
AutoFocus makes over a billion samples and sessions, including billions of artifacts, immediately actionable for security analysis and response efforts. AutoFocus extends the product portfolio with the global threat intelligence and attack context needed to accelerate analysis, forensics, and hunting workflows. Together, the platform and AutoFocus move security teams away from legacy manual approaches that rely on aggregating a growing number of detectionbased alerts and post-event mitigation, to preventing sophisticated attacks and enabling proactive hunting activities.

QUESTION 13
Which characteristic of serverless computing enables developers to quickly deploy application code?

A. Uploading cloud service autoscaling services to deploy more virtual machines to run their application code based on user demand
B. Uploading the application code itself, without having to provision a full container image or any OS virtual machine components
C. Using cloud service spot pricing to reduce the cost of using virtual machines to run their application code
D. Using Container as a Service (CaaS) to deploy application containers to run their code.

Answer: B
Explanation:
In serverless apps, the developer uploads only the app package itself, without a full container image or any OS components. The platform dynamically packages it into an image, runs the image in a container, and (if needed) instantiates the underlying host OS and VM and the hardware required to run them.

QUESTION 14
Which Palo Alto Networks product provides playbooks with 300+ multivendor integrations that

help solve any security use case?

A. Cortex XSOAR
B. Prisma Cloud
C. AutoFocus
D. Cortex XDR

Answer: A
Explanation:
SOAR tools ingest aggregated alerts from detection sources (such as SIEMs, network security tools, and mailboxes) before executing automatable, process-driven playbooks to enrich and respond to these alerts.
https://www.paloaltonetworks.com/cortex/security-operations-automation

QUESTION 15
What does SIEM stand for?

A. Security Infosec and Event Management
B. Security Information and Event Management
C. Standard Installation and Event Media
D. Secure Infrastructure and Event Monitoring

Answer: B
Explanation:
Originally designed as a tool to assist organizations with compliance and industry-specific regulations, security information and event management (SIEM) is a technology that has been around for almost two decades.

QUESTION 16
Which option is an example of a North-South traffic flow?

A. Lateral movement within a cloud or data center
B. An internal three-tier application
C. Client-server interactions that cross the edge perimeter
D. Traffic between an internal server and internal user

Answer: C
Explanation:
North-south refers to data packets that move in and out of the virtualized environment from the host network or a corresponding traditional data center. North-south traffic is secured by one or more physical form factor perimeter edge firewalls.

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: **ASTR14**