Free Questions for 200-201 by dumpssheet

Shared by Dominguez on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit. An attacker scanned the server using Nmap. What did the attacker obtain from this scan?

Options:

A- Identified a firewall device preventing the pert state from being returned.

B- Identified open SMB ports on the server

C- Gathered information on processes running on the server

D- Gathered a list of Active Directory users

Answer:

C

Question 2

Question Type: MultipleChoice

What is the difference between indicator of attack (IoA) and indicators of compromise (IoC)?

Options:

A- IoA is the evidence that a security breach has occurred, and IoC allows organizations to act before the vulnerability can be exploited.

B- IoA refers to the individual responsible for the security breach, and IoC refers to the resulting loss.

C- IoC is the evidence that a security breach has occurred, and IoA allows organizations to act before the vulnerability can be exploited.

D- IoC refers to the individual responsible for the security breach, and IoA refers to the resulting loss.

Answer:

C

Question 3

Question Type: **MultipleChoice**

An employee received an email from a colleague's address asking for the password for the domain controller. The employee noticed a missing letter within the sender's address. What does this incident describe?

Options:

A- brute-force attack

B- insider attack

C- shoulder surfing

D- social engineering

Answer:

B

Question 4

Question Type: **MultipleChoice**

Which security model assumes an attacker within and outside of the network and enforces strict verification before connecting to any system or resource within the organization?

Options:

A- Biba

B- Object-capability

C- Take-Grant

D- Zero Trust

Answer:

D

Explanation:

Zero Trust securityis an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter.

Question 5

Question Type: **MultipleChoice**

Which two elements of the incident response process are stated in NIST SP 800-61 r2? (Choose two.)

Options:

A- detection and analysis

B- post-incident activity

C- vulnerability scoring

D- vulnerability management

E- risk assessment

Answer:

A, B

Question 6

Question Type: MultipleChoice

Refer to the exhibit. An employee received an email from an unknown sender with an attachment and reported it as a phishing attempt. An engineer uploaded the file to Cuckoo for further analysis. What should an engineer interpret from the provided Cuckoo report?

Options:

A- Win32.polip.a.exe is an executable file and should be flagged as malicious.

B- The file is clean and does not represent a risk.

C- Cuckoo cleaned the malicious file and prepared it for usage.

D- MD5 of the file was not identified as malicious.

Answer:

C

Question 7

Question Type: **MultipleChoice**

Why is HTTPS traffic difficult to screen?

Options:

A- HTTPS is used internally and screening traffic (or external parties is hard due to isolation.

B- The communication is encrypted and the data in transit is secured.

C- Digital certificates secure the session, and the data is sent at random intervals.

D- Traffic is tunneled to a specific destination and is inaccessible to others except for the receiver.

Answer:

B

Question 8

Question Type: **MultipleChoice**

An engineer discovered a breach, identified the threat's entry point, and removed access. The engineer was able to identify the host, the IP address of the threat actor, and the application the threat actor targeted. What is the next step the engineer should take according to the NIST SP 800-61 Incident handling guide?

Options:

A- Recover from the threat.

B- Analyze the threat.

C- Identify lessons learned from the threat.

D- Reduce the probability of similar threats.

Answer:

A

Explanation:

Per: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Question 9

Question Type: **MultipleChoice**

A developer is working on a project using a Linux tool that enables writing processes to obtain these required results:

If the process is unsuccessful, a negative value is returned.

If the process is successful, 0 value is returned to the child process, and the process ID is sent to the parent process.

Which component results from this operation?

Options:

A- parent directory name of a file pathname

B- process spawn scheduled

C- macros for managing CPU sets

D- new process created by parent process

Answer:

D

Explanation:

There are two tasks with specially distinguished process IDs: swapper or sched has process ID 0 and is responsible for paging, and is actually part of the kernel rather than a normal user-mode process. Process ID 1 is usually the init process primarily responsible for starting and shutting down the system. Originally, process ID 1 was not specifically reserved for init by any technical measures: it simply had this ID as a natural consequence of being the first process invoked by the kernel. More recent Unix systems typically have additional kernel components visible as 'processes', in which case PID 1 is actively reserved for the init process to maintain consistency with older systems

Question 10

Question Type: **MultipleChoice**

Which metric should be used when evaluating the effectiveness and scope of a Security Operations Center?

Options:

A- The average time the SOC takes to register and assign the incident.

B- The total incident escalations per week.

C- The average time the SOC takes to detect and resolve the incident.

D- The total incident escalations per month.

Answer:

C