Cisco 350-201 Mock Exam

Shared by Davis on 17-06-2026

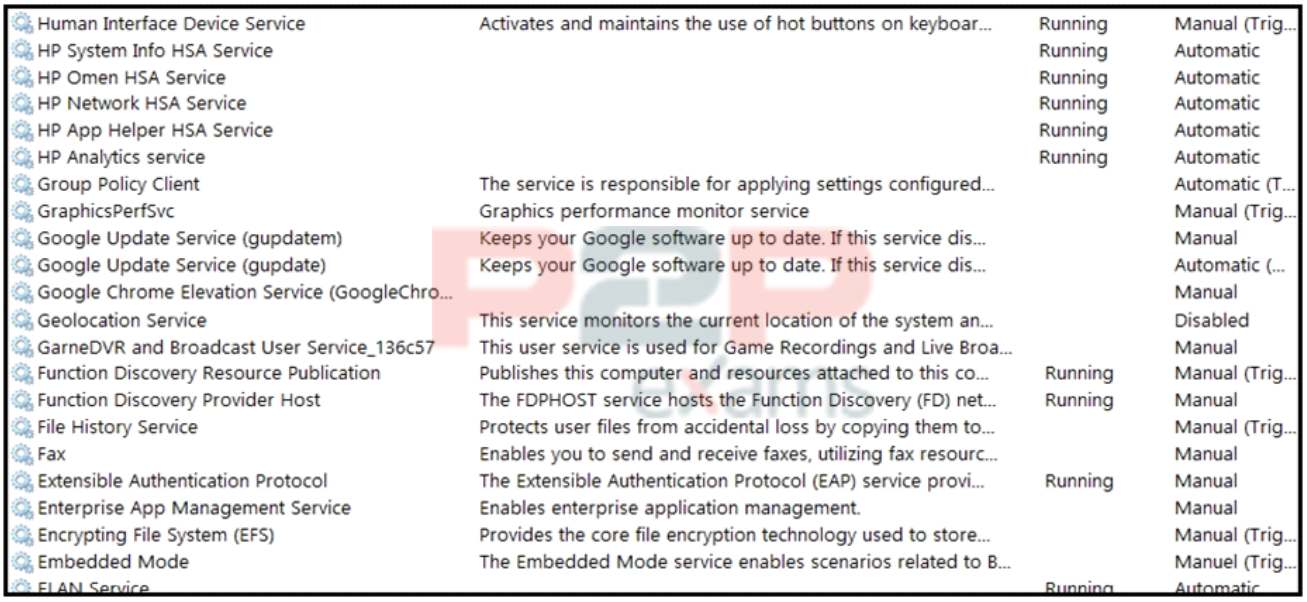
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.



Human Interface Device Service	Activates and maintains the use of hot buttons on keyboar...	Running	Manual (Trig...
HP System Info HSA Service		Running	Automatic
HP Omen HSA Service		Running	Automatic
HP Network HSA Service		Running	Automatic
HP App Helper HSA Service		Running	Automatic
HP Analytics service		Running	Automatic
Group Policy Client	The service is responsible for applying settings configured...		Automatic (T...
GraphicsPerfSvc	Graphics performance monitor service		Manual (Trig...
Google Update Service (gupdatem)	Keeps your Google software up to date. If this service dis...		Manual
Google Update Service (gupdate)	Keeps your Google software up to date. If this service dis...		Automatic (...
Google Chrome Elevation Service (GoogleChro...			Manual
Geolocation Service	This service monitors the current location of the system an...		Disabled
GarneDVR and Broadcast User Service_136c57	This user service is used for Game Recordings and Live Broa...		Manual
Function Discovery Resource Publication	Publishes this computer and resources attached to this co...	Running	Manual (Trig...
Function Discovery Provider Host	The FDPHOST service hosts the Function Discovery (FD) net...	Running	Manual
File History Service	Protects user files from accidental loss by copying them to...		Manual (Trig...
Fax	Enables you to send and receive faxes, utilizing fax resourc...		Manual
Extensible Authentication Protocol	The Extensible Authentication Protocol (EAP) service provi...	Running	Manual
Enterprise App Management Service	Enables enterprise application management.		Manual
Encrypting File System (EFS)	Provides the core file encryption technology used to store...		Manual (Trig...
Embedded Mode	The Embedded Mode service enables scenarios related to B...		Manuel (Trig...
ELAN Service		Running	Automatic

An engineer received multiple reports from employees unable to log into systems with the error: The Group Policy Client service failed to logon -- Access is denied. Through further analysis, the engineer discovered several unexpected modifications to system settings. Which type of breach is occurring?

Options:

A- malware break
B- data theft
C- elevation of privileges
D- denial-of-service

Answer:

C

Question 2

Question Type: MultipleChoice

Refer to the exhibit.

Asset	Threat	Vulnerability	Likelihood (1-10)	Impact (1-10)
Servers	Natural Disasters – Flooding	Server Room is on the zero floor	3	10
Secretary Workstation	Usage of illegitimate software	Inadequate control of software	7	6
Payment Process	Eavesdropping, Misrouting/re-routing of messages	Unencrypted communications	5	10
Website	Website Intrusion	No IDS/IPS usage	6	8

Which asset has the highest risk value?

Options:

A- servers
B- website
C- payment process
D- secretary workstation

Answer:

C

Question 3

Question Type: MultipleChoice

A SOC analyst is investigating a recent email delivered to a high-value user for a customer whose network their organization monitors. The email includes a suspicious attachment titled ''Invoice RE: 0004489''. The

hash of the file is gathered from the Cisco Email Security Appliance. After searching Open Source Intelligence, no available history of this hash is found anywhere on the web. What is the next step in analyzing this attachment to allow the analyst to gather indicators of compromise?

Options:

A- Run and analyze the DLP Incident Summary Report from the Email Security Appliance
B- Ask the company to execute the payload for real time analysis
C- Investigate further in open source repositories using YARA to find matches
D- Obtain a copy of the file for detonation in a sandbox

Answer:

D

Question 4

Question Type: MultipleChoice

An organization installed a new application server for IP phones. An automated process fetched user credentials from the Active Directory server, and the application will have access to on-premises and cloud services. Which security threat should be mitigated first?

Options:

A- aligning access control policies
B- exfiltration during data transfer
C- attack using default accounts
D- data exposure from backups

Answer:

B

Question 5

Question Type: MultipleChoice

What is a limitation of cyber security risk insurance?

Options:

A- It does not cover the costs to restore stolen identities as a result of a cyber attack
B- It does not cover the costs to hire forensics experts to analyze the cyber attack
C- It does not cover the costs of damage done by third parties as a result of a cyber attack
D- It does not cover the costs to hire a public relations company to help deal with a cyber attack

Answer:

A

Question 6

Question Type: MultipleChoice

Refer to the exhibit.

```
try
{
    using (MemoryStream memoryStream = new MemoryStream())
    {
        memoryStream.Position = 32L;
        using (AesCryptoServiceProvider aesCryptoServiceProvider = new AesCryptoServiceProvider())
        {
            aesCryptoServiceProvider.KeySize = 128;
            aesCryptoServiceProvider.BlockSize = 128;
            aesCryptoServiceProvider.Mode = CipherMode.CBC;
            aesCryptoServiceProvider.Padding = PaddingMode.PKCS7;
            aesCryptoServiceProvider.Key = key;
            aesCryptoServiceProvider.GenerateIV();
            using (CryptoStream cryptoSream = new CryptoStream(memoryStream, aesCryptoServiceProvider.CreateEncryptor(), CryptoStreamMode.Write))
            {
                memoryStream.Write(aesCryptoServiceProvider.IV, 0, aesCryptoServiceProvider.IV.Length);
                cryptoStream.Write(input, 0, input.Length);
                cryptoStream.FlushFinalBlock();
                using (HMACSHA256 hMACSHA = new HMACSHA256(bytes))
                {
                    byte[] array = hMACSHA.ComputeHash(memoryStream.ToArray(), 32, memoryStream.ToArray().Length - 32);
                    memoryStream.Position = 0L;
                    memoryStream.Write(array, 0, array.Length);
                }
            }
        }
        result = memoryStream.ToArray();
    }
}
catch
{
}
```

An engineer is performing a static analysis on a malware and knows that it is capturing keys and webcam events on a company server. What is the indicator of compromise?

Options:

A- The malware is performing comprehensive fingerprinting of the host, including a processor, motherboard manufacturer, and connected removable storage.

B- The malware is a ransomware querying for installed anti-virus products and operating systems to encrypt and render unreadable until payment is made for file decryption.

C- The malware has moved to harvesting cookies and stored account information from major browsers and configuring a reverse proxy for intercepting network activity.

D- The malware contains an encryption and decryption routine to hide URLs/IP addresses and is storing the output of loggers and webcam captures in locally encrypted files for retrieval.

Answer:

B

Question 7

Question Type: MultipleChoice

How does Wireshark decrypt TLS network traffic?

Options:

A- with a key log file using per-session secrets
B- using an RSA public key
C- by observing DH key exchange
D- by defining a user-specified decode-as

Answer:

A

Question 8

Question Type: MultipleChoice

Refer to the exhibit.

```
<employees>
  <employee>
    <lastname>Smith</lastname>
    <firstname>Richard</firstname>
  </employee>
  <employee>
    <lastname>Witzel</lastname>
    <firstname>Sevan</firstname>
  </employee>
</employees>
```

Which data format is being used?

Options:

A- JSON
B- HTML
C- XML
D- CSV

Answer:

B

Question 9

Question Type: MultipleChoice

An organization suffered a security breach in which the attacker exploited a Netlogon Remote Protocol vulnerability for further privilege escalation. Which two actions should the incident response team take to

prevent this type of attack from reoccurring? (Choose two.)

Options:

A- Implement a patch management process.
B- Scan the company server files for known viruses.
C- Apply existing patches to the company servers.
D- Automate antivirus scans of the company servers.
E- Define roles and responsibilities in the incident response playbook.

Answer:

D, E

Question 10

Question Type: MultipleChoice

A logistic company must use an outdated application located in a private VLAN during the migration to new technologies. The IPS blocked and reported an unencrypted communication. Which tuning option should be applied to IPS?

Options:

A- Allow list only authorized hosts to contact the application's IP at a specific port.
B- Allow list HTTP traffic through the corporate VLANS.
C- Allow list traffic to application's IP from the internal network at a specific port.
D- Allow list only authorized hosts to contact the application's VLAN.

Answer:

D

Question 11

Question Type: MultipleChoice

Based on GDPR, what should be done with data to ensure its confidentiality, integrity, and availability?

Options:

A- Perform a vulnerability assessment
B- Conduct a data protection impact assessment
C- Conduct penetration testing
D- Perform awareness testing

Answer:

B