CAS-003$^{Q\&As}$

CompTIA Advanced Security Practitioner (CASP+)

QUESTION 1

After the install process, a software application executed an online activation process. After a few months, the system experienced a hardware failure. A backup image of the system was restored on a newer revision of the same brand and model device. After the restore, the specialized application no longer works. Which of the following is the MOST likely cause of the problem?

A. The binary files used by the application have been modified by malware.

B. The application is unable to perform remote attestation due to blocked ports.

C. The restored image backup was encrypted with the wrong key.

D. The hash key summary of hardware and installed software no longer match.

Correct Answer: D

Different software vendors have different methods of identifying a computer used to activate software. However, a common component used in software activations is a hardware key (or hardware and software key). This key is a hash value generated based on the hardware (and possibly software) installed on the system.

For example, when Microsoft software is activated on a computer, the software generates an installation ID that consists of the software product key used during the installation and a hardware key (hash value generated from the computer\\'s hardware). The installation ID is submitted to Microsoft for software activation.

Changing the hardware on a system can change the hash key which makes the software think it is installed on another computer and is therefore not activated for use on that computer. This is most likely what has happened in this question.

QUESTION 2

A system worth $100,000 has an exposure factor of eight percent and an ARO of four. Which of the following figures is the system\\'s SLE?

A. $2,000

B. $8,000

C. $12,000

D. $32,000

Correct Answer: B

Single Loss Expectancy (SLE) is mathematically expressed as: Asset value (AV) x Exposure Factor (EF)

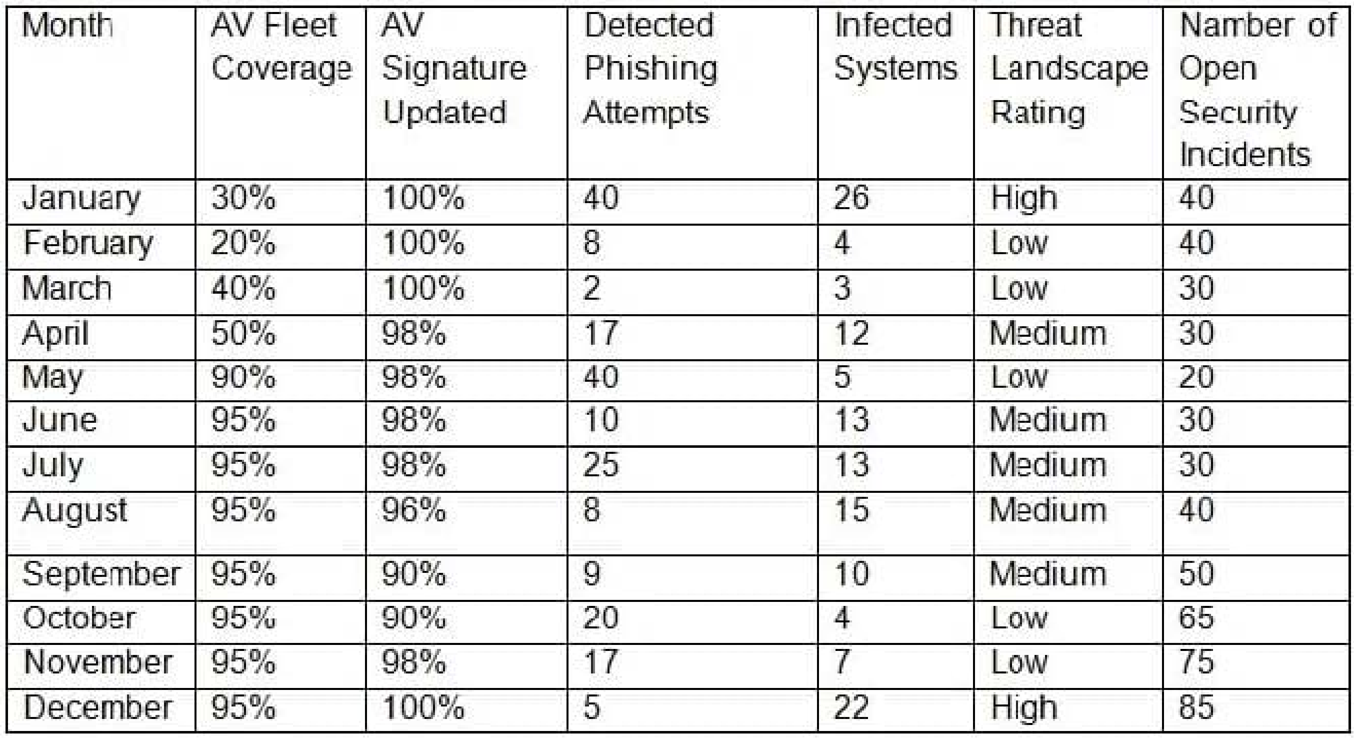
SLE = AV x EF = $100 000 x 8% = $ 8 000

References: http://www.financeformulas.net/Return_on_Investment.html

https://en.wikipedia.org/wiki/Risk_assessment

QUESTION 3

A security technician receives a copy of a report that was originally sent to the board of directors by the Chief Information Security Officer (CISO). The report outlines the following KPI/KRI data for the last 12 months:



Month	AV Fleet Coverage	AV Signature Updated	Detected Phishing Attempts	Infected Systems	Threat Landscape Rating	Namber of Open Security Incidents
January	30%	100%	40	26	High	40
February	20%	100%	8	4	Low	40
March	40%	100%	2	3	Low	30
April	50%	98%	17	12	Medium	30
May	90%	98%	40	5	Low	20
June	95%	98%	10	13	Medium	30
July	95%	98%	25	13	Medium	30
August	95%	96%	8	15	Medium	40
September	95%	90%	9	10	Medium	50
October	95%	90%	20	4	Low	65
November	95%	98%	17	7	Low	75
December	95%	100%	5	22	High	85

Which of the following BEST describes what could be interpreted from the above data?

A. 1. AV coverage across the fleet improved

2.

There is no correlation between infected systems and AV coverage.

3.

There is no correlation between detected phishing attempts and infected systems

4.

A correlation between threat landscape rating and infected systems appears to exist.

5.

Effectiveness and performance of the security team appears to be degrading.

B. 1. AV signature coverage has remained consistently high

2.

AV coverage across the fleet improved

3.

A correlation between phishing attempts and infected systems appears to exist

4.

There is a correlation between the threat landscape rating and the security team\\'s performance.

5.

There is no correlation between detected phishing attempts and infected systems

C. 1. There is no correlation between infected systems and AV coverage

2.

AV coverage across the fleet improved

3.

A correlation between phishing attempts and infected systems appears to exist

4.

There is no correlation between the threat landscape rating and the security team\\'s performance.

5.

There is a correlation between detected phishing attempts and infected systems

D. 1. AV coverage across the fleet declined

2.

There is no correlation between infected systems and AV coverage.

3.

A correlation between phishing attempts and infected systems appears to exist

4.

There is no correlation between the threat landscape rating and the security team\\'s performance

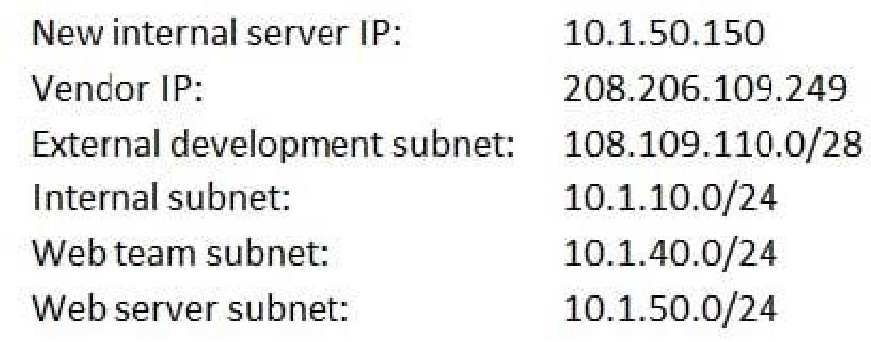
5.

Effectiveness and performance of the security team appears to be degrading.

Correct Answer: A

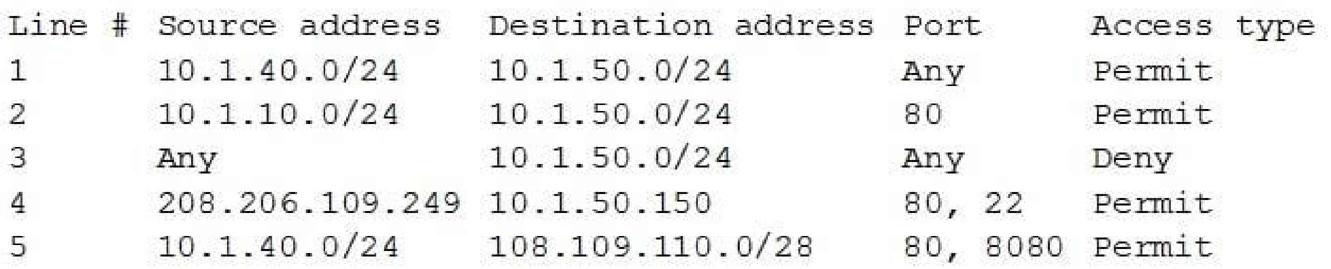
QUESTION 4

A request has been approved for a vendor to access a new internal server using only HTTPS and SSH to manage the back-end system for the portal. Internal users just need HTTP and HTTPS access to all internal web servers. All other external access to the new server and its subnet is not allowed. The security manager must ensure proper access is configured.



New internal server IP:	10.1.50.150
Vendor IP:	208.206.109.249
External development subnet:	108.109.110.0/28
Internal subnet:	10.1.10.0/24
Web team subnet:	10.1.40.0/24
Web server subnet:	10.1.50.0/24

Below is a snippet from the firewall related to that server (access is provided in a top-down model):



Line #	Source address	Destination address	Port	Access type
1	10.1.40.0/24	10.1.50.0/24	Any	Permit
2	10.1.10.0/24	10.1.50.0/24	80	Permit
3	Any	10.1.50.0/24	Any	Deny
4	208.206.109.249	10.1.50.150	80, 22	Permit
5	10.1.40.0/24	108.109.110.0/28	80, 8080	Permit

Which of the following lines should be configured to allow the proper access? (Choose two.)

A. Move line 3 below line 4 and change port 80 to 443 on line 4.

B. Move line 3 below line 4 and add port 443 to line.

C. Move line 4 below line 5 and add port 80 to 8080 on line 2.

D. Add port 22 to line 2.

E. Add port 22 to line 5.

F. Add port 443 to line 2.

G. Add port 443 to line 5.

Correct Answer: BF

QUESTION 5

A newly hired security analyst has joined an established SOC team. Not long after going through corporate orientation, a new attack method on web-based applications was publicly revealed. The security analyst immediately brings this new information to the team lead, but the team lead is not concerned about it.

Which of the following is the MOST likely reason for the team lead\\'s position?

A. The organization has accepted the risks associated with web-based threats.

B. The attack type does not meet the organization\\'s threat model.

C. Web-based applications are on isolated network segments.

D. Corporate policy states that NIPS signatures must be updated every hour.

Correct Answer: A

CAS-003 VCE Dumps CAS-003 Study Guide CAS-003 Exam Questions