```
Please contact your system administrator.

Add correct host key in /Users/scott/.ssh/known_hosts to get rid of this message.

Offending ECDSA key in /Users/scott/.ssh/known_hosts:47

ECDSA host key for ec2-192-168-1-1.compute-1.amazonaws.com has changed and you have
requested strict checking.

Host key verification failed.
```

When you connect to a server via SSH, it gets a fingerprint for the ECDSA key, which it then saves to your home directory under ~/.ssh/known_hosts. This is done after first connecting to the server, and will prompt you with a message like this:

```
$ ssh ec2-user@ec2-192-168-1-1.compute-1.amazonaws.com

The authenticity of host 'ec2-192-168-1-1.compute-1.amazonaws.com (192.168.1.1)' can't be
established.

ECDSA key fingerprint is SHA256:hotsxb/qVi1/ycUU2wXF6mfGH++Yk7WYZv0r+tIhg4I.

Are you sure you want to continue connecting (yes/no)?
```

If you enter 'yes', then the fingerprint is saved to the known_hosts file, which SSH then consults every time you connect to that server.

But what happens if a server's ECDSA key has changed since you last connected to it? This is alarming because it could actually mean that you're connecting to a different server without knowing it. If this new server is malicious then it would be able to view all data sent to and from your connection, which could be used by whoever set up the server. This is called a man-in-the-middle attack. This scenario is exactly what the "WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!" message is trying to warn you about.

Of course, this isn't always the case, and there are many reasons for the ECDSA key fingerprint to change for a server. In my case, I had an elastic IP address on AWS and assigned it to a different server after redeploying our application. The IP address and hostname I was connecting to were the same, but the underlying server was different, which is what tripped the SSH client to issue this warning.

Fixing the Issue
If you are 100% sure that this was expected behavior and that there is no potential security issue, you'll need to fix the issue before continuing.

The easiest ways I've found to fix this problem is the following two solutions.

Manually Resolve via known_hosts:

- In the warning message find the line that tells you where the offending ECDSA key is located in the known_hosts file. In my example this line said "Offending ECDSA key in /Users/scott/.ssh/known_hosts:47", which refers to line 47.
- Open the known_hosts file specified in the warning message
- Delete the line specified in the warning message

By deleting this line, your SSH client won't have an ECDSA key fingerprint to compare to, and thus will ask you again to verify the authenticity of the server the next time you connect. Once done, you'll have a new fingerprint in our known_hosts file for this server, and the warning will be gone.

Resolve Using ssh-keygen

Another solution would be to use the ssh-keygen utility to delete the offending key from your known_hosts file, which can be done with the following command:

```
$ ssh-keygen -R [hostname-or-IP]
```

So in my example I'd use it like this:

```
$ ssh-keygen -R ec2-192-168-1-1.compute-1.amazonaws.com
```

This method is good if you don't want to manually alter the known_hosts file yourself, and the utility is easier to use if you have multiple hostnames and IP addresses to fix. It can also handle hashed hostnames in a known_hosts.old file.

QUESTION 13
An organization has implemented a policy requiring the use of conductive metal lockboxes for personal electronic devices outside of a secure research lab. Which of the following did the organization determine to be the GREATEST risk to intellectual property when creating this policy?

A. The theft of portable electronic devices
B. Geotagging in the metadata of images
C. Bluesnarfing of mobile devices
D. Data exfiltration over a mobile hotspot

Correct Answer: D

QUESTION 14
An organization that is located in a flood zone is MOST likely to document the concerns associated with the restoration of IT operation in a:

A. business continuity plan
B. communications plan.
C. disaster recovery plan.
D. continuity of operations plan

Correct Answer: C

QUESTION 15
A startup company is using multiple SaaS and IaaS platform to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

A. SIEM
B. DLP
C. CASB
D. SWG

Correct Answer: C

QUESTION 16
On which of the following is the live acquisition of data for forensic analysis MOST dependent? (Choose two.)

A. Data accessibility
B. Legal hold
C. Cryptographic or hash algorithm
D. Data retention legislation
E. Value and volatility of data
F. Right-to-audit clauses

Correct Answer: EF

QUESTION 17
Which of the following allows for functional test data to be used in new systems for testing and training purposes to protect the real data?

A. Data encryption
B. Data masking
C. Data deduplication
D. Data minimization

Correct Answer: B
Explanation:
https://ktechproducts.com/Data-mask#:~:text=Data%20Masking%20is%20a%20method%20of%20creating%20a,partial%20data%20based%20on%20the%20user%E2%80%99s%20security%20permissions.

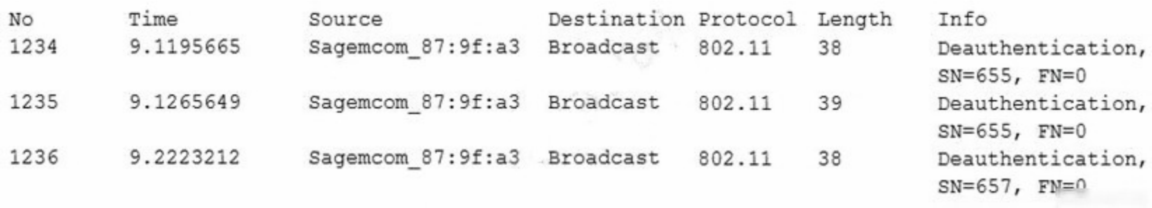
The main reason for applying masking to a data field is to protect data that is classified as personally identifiable information, sensitive personal data, or commercially sensitive data. However, the data must remain usable for the purposes of undertaking valid test cycles. It must also look real and appear consistent. It is more common to have masking applied to data that is represented outside of a corporate production system. In other words, where data is needed for the purpose of application development, building program extensions and conducting various test cycles https://en.wikipedia.org/wiki/Data_masking

QUESTION 18
A small business just recovered from a ransomware attack against its file servers by purchasing the decryption keys from the attackers. The issue was triggered by a phishing email and the IT administrator wants to ensure it does not happen again. Which of the following should the IT administrator do FIRST after recovery?

A. Scan the NAS for residual or dormant malware and take new daily backups that are tested on a frequent basis
B. Restrict administrative privileges and patch ail systems and applications.
C. Rebuild all workstations and install new antivirus software
D. Implement application whitelisting and perform user application hardening

Correct Answer: A

QUESTION 19
A user reports constant lag and performance issues with the wireless network when working at a local coffee shop. A security analyst walks the user through an installation of Wireshark and get a five-minute pcap to analyze. The analyst observes the following output:



```
No      Time         Source              Destination Protocol Length   Info
1234    9.1195665    Sagemcom_87:9f:a3   Broadcast    802.11   38      Deauthentication,
                                                                        SN=655, FN=0
1235    9.1265649    Sagemcom_87:9f:a3   Broadcast    802.11   39      Deauthentication,
                                                                        SN=655, FN=0
1236    9.2223212    Sagemcom_87:9f:a3   Broadcast    802.11   38      Deauthentication,
                                                                        SN=657, FN=0
```

Which of the following attacks does the analyst MOST likely see in this packet capture?

A. Session replay
B. Evil twin
C. Bluejacking
D. ARP poisoning

Correct Answer: B
Explanation:
https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack

One of the main purposes of deauthentication used in the hacking community is to force clients to connect to an evil twin access point which then can be used to capture network packets transferred between the client and the access point.

QUESTION 20
Which of the following BEST explains the difference between a data owner and a data custodian?

A. The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data
B. The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protection to the data
C. The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data
D. The data owner grants the technical permissions for data access, while the data custodian maintains the database access controls to the data

Correct Answer: B
Explanation:
Data Owner - the administrator/CEO/board/president of a company Data custodian - the ones taking care of the actual data - like IT staff (generally) or HR staff (for HR-related data) https://security.stackexchange.com/questions/218049/what-is-the-difference-between-data-owner-data-custodian-and-system-owner https://www.nicolaaskham.com/blog/2019/4/12/whats-the-difference-between-data-owners-and-data-custodians

QUESTION 21
A network administrator has been asked to install an IDS to improve the security posture of an organization. Which of the following control types is an IDS?

A. Corrective
B. Physical
C. Detective
D. Administrative

Correct Answer: C
Explanation:
IDS = Intrusion Detection System. It is passive and only notifies instead of blocking anything.

QUESTION 22
A company recently set up an e-commerce portal to sell its product online. The company wants to start accepting credit cards for payment, which requires compliance with a security standard. Which of the following standards must the company comply with before accepting credit cards on its e-commerce platform?

A. PCI DSS
B. ISO 22301
C. ISO 27001
D. NIST CSF

Correct Answer: A

QUESTION 23
A database administrator needs to ensure all passwords are stored in a secure manner, so the administrate adds randomly generated data to each password before string. Which of the following techniques BEST explains this action?

A. Predictability
B. Key stretching
C. Salting
D. Hashing

Correct Answer: C

QUESTION 24
A RAT that was used to compromise an organization's banking credentials was found on a user's computer. The RAT evaded antivirus detection. It was installed by a user who has local administrator rights to the system as part of a remote management tool set. Which of the following recommendations would BEST prevent this from reoccurring?

A. Create a new acceptable use policy.
B. Segment the network into trusted and untrusted zones.
C. Enforce application whitelisting.
D. Implement DLP at the network boundary.

Correct Answer: C

QUESTION 25
A company recently transitioned to a strictly BYOD culture due to the cost of replacing lost or damaged corporate-owned mobile devices. Which of the following technologies would be BEST