Exam - Introduksjon til datasikkerhet DCS3101

Candidate number: 8073

Q1)

I would support that storing all the data on a single server would be bad for the company. Maybe, it's their only option because it's a startup company, but from the CIA triad this can impact the availability tremendously, because if consider a ddos attack, it can cause the server to not be available for some time, and if the company relies the server being available, it can cause a lot of harm in terms of customer satisfaction, and more importantly, money.

Q2)

There are many risks involved with having a personal main configured to the company network. For example, the individual may be reusing that same e-mail passwords on other different places, so with a credential stuffing attack they can gain access to the account, and if its then configured to the company network then that can be even more dangerous. Another attack can be a spear phishing attack, where the attacker would lure the user to gain access to the account in some way. We see that the harm is clearly with the fact that the mail is configured to the company network, so if the mail account is compromised then it also poses a threat to the company's resources, so it's a much bigger loss and damage then if it wasn't configured to the company network.

Q3)

From the truth table of the xor, we know that 2 equals output a 0, so if x and y are equal, the xor'd output will be 0. And if we do this operation with all of these given variables, then there is a predictable symmetric combination that is not secure at all, and is easy to decipher. F

Q4)

In a zero day exploit the attack occurs the same day (zero-day) that the weakness is discovered in the software. I would argue that DDoS attack are more of a threat towards the availability in CIA triad, whilst a zero-day exploit is more of a threat towards confidentiality, integrity and availability in the CIA triad, because it can be many different things depending on the context. So, if there is a zero-day exploit because of a human programming error, it

can target some customers data and compromise the confidentiality and integrity or if it targets the server it can also compromise the server and compromise the availability.

Q5)

The statement is not true because SHA-2 does not produce 222 bit length output.

Q6)

This is definitely a dangerous design, because if all the passwords are being hashed with the same salt, then an attacker who manages to find the salt, are then able to decrypt all the other passwords rather than some single instances, so the dangers are infinitely larger. Therefore, the design should include unique salts and not the same.

Q7)

I am not sure, because when I did this I couldn't find a multiplicative inverse of 3597

Q8)

The CEO will not be able to access his older email without having the right PGP key. Once the PGP key is lost, then there is no way of obtaining the data from the email, unless the intern set up a key server, which in that case would allow him to generate a new key.

Q9)

SSL stripping attack where the attacker intercepts a request from the user to the server. The attacker will then continue to establish an HTTPS connection between himself and the server, and an unsecured HTTP connection with the user, acting as a "bridge" between them.

Q10)

Yes. A keylogger monitors each keystroke of the user and this can be used for a spear phishing attack. The attacker can lure the user to click a malicious link, and by monitoring the keystroke they can gather personal information, such as password or credit card number.

Q11)
The statement is true.

Q12)

A requirement is high identification speed. What is the point of using for example fingerprint on my phone if it's very slow and I can just insert the code instead? We want the identification speed to be high in order for the performance to be good.
Another requirement is reliability. There shouldn't be a case, where one day the face-scan works, and another day it doesn't, it should be consistent and reliable.
Lastly, another key requirement for a biometric system is Acceptability, by that I mean. to which extend are users willing to accept the use of it. Is there a feeling of privacy breaching, or is the user comfortable with it?

Q13)

Obviously, the bank services have highly critical resources, so the log-in process should be secure. With a fingerprint based log-in system there are some challenges however, such as the fact that fingerprints leave behind evidence at a crime scene as "latents" (e.g. fingerprints on a glass). An attacker can use this in some sort of way by anti-spoofing, by artificial fingerprints or other ways. Another attack that can be relevant here is denial of service, where the attacker aims to make the resource unavailable and disrupting its services.

This can be solved by having multiple authentication steps, with a mix of biometrical and non-biometrical systems so that the attacker can't gain access simply by bypassing the fingerprint step. Furthermore, there should

Q14)

There are many issues here. Firstly, using code that is from different snippets is dangerous because it can contain different functionalities that the programmer is not aware of. When you copy the code, you might also copy any vulnerabilities. Furthermore, because it is opensource, the company could have issues with failure to track the open source components and update if they needed to.

Q15)

I would not accept the recommendation. Firewalls can only monitor/filter known traffic that is declared malicious, it cannot prevent covert attacks or internal attacks. On the other hand, Network Intrusion Detection Systems (NIDS) will monitor and detect any suspicious activity within the network and checks every single packet for dangerous content, which is much more secure

I would rather operate a NIDS alongside a firewall in order to identify and neutralize anything that does get through the firewall or that originates from within. Furthermore, if dangerous traffic manages to get through the firewall, I will have the NIDS as the second line of defence to identify the dangerous packets being sent. This design would be much more secure.

Q16)

A company should not only have external firewalls, but also internal firewalls because you want to monitor the internal traffic for the computer. The external firewall monitors the network's perimeter and dangerous traffic from the outside, but if dangerous traffic manages to go through, then internal firewalls are also needed as they protect the network from the attack that has already gotten past the perimeter

Q17)

It is important to update a security system continuously because with there are being developed new viruses and new attack methods, so to update the security system with antivirus systems is really important. If we don't update antivirus system, then there is no point of having it, as new viruses and methods can cause harm.
However, despite the updates some threats that still remain for the user such as polymorphic malware, where the **malware** constantly changes its distinct features in order to evade detection

Q18)

According to the authors the middleware layer attacks are: Man-in-the-middle attack, SQL injection attack, Signature wrapping attack, Cloud malware injection, Flooding attack in cloud.

According to the authors, a sleep deprivation attacks is an attack where the adversary tries to drain the battery of low-powered IoT edge devices. It can lead to a denial of service from the nodes in the IoT application due to a dead battery, and it's can be done by running infinite loops in the edge devices using malicious code.

Q19)

A firewall is a check point that protects the internal networks against attack from outside network and the check point decides which traffic can pass in & out based on different rules. It monitors the network traffic and prevent unauthorized access from entering the network and
they create a safety barrier between a private network and the public internet. For this reason the firewalls are included in the **detect and deny** part of the cyber kill chain.

Q20)

It is not smart to use social media on company laptop because a lot of phishing and social engineering attacks occur on social media, and if such an attack is successful it can cause harm to the company through the network for example. In order to enforce a policy, the company can block the use of social media from their networks.

Q21)

When we get a computer from a crime scene, we don't know what it involves at all. It can be full of malware and different viruses. They have probably done everything in order to delete traces leading to and from them and done so by using all the tricks in the book, so we should be careful. Therefore, the read-only setting should be used in this setting .
because since the criminal wants to delete all traces leading to and from them, they may have used programs to infect other computers.