Segwit:

Transaciton malleability was fixed by segwit:

* The hash of the transaction (digital fingerprint of the transaction), this can be exploited by when you send someone form example bitcoin from one persokn to anoter itj isj common to have a transaction ID on the transaction so that the person you r sending money to can confirm that they have gotten the money from you. However the person recieving the money could change the transaction ID (change the signature) and say to Alice that they didnt revcieve their transaction, even thought they got the money.
* Segwit fixes this issue with thransaction malleability so that you cant change the transacttion ID

What is segwit?

1. Full blocks how did it change that problem
2. How did it stop transaction mallability

Without Having a hard fork.

1. Instead of extending the size of each block we can instead decrease the size of each transaction so we can fit more transactions into each and every block. We remove the signatures from the transaction datastructure because the signatures are quite large. Ijnstead we keep the signature sepperate. Inputs in a transaction used to contain the signature, but we store them by the side instead. The signature is only used once on every node, so therefore that one node check the signature that is beside the transaction before it is approved and sent to the memepool, only need to validate it once. Signatures is still used, but just removed from the transaction itself.
2. By removing the signature from the transaction, you are no longer able to change the transaction signature and then changing the hash of the transaction to fool other people.

Implementation and deployment:

* It was not forced upon everyone, but was incentivized because it lowered the transaction fees
* Needed to be able to seperate between normalk transactions and segwit transactions.
* Goal to make it a soft fork (optional), didnt want a split in the change.
* Needed to contract the rules (soft fork).
* They had to work with the old programming language because they couldnt expand the rules.

Segwit homework:

1. What was a proposed alternative to Segwit?

Increasing the block size from 1mB to 2 mB and would have resulted in a hard fork

1. What did Segwit solve more than just the scaling issue?

It also solved the transaction mallability issue (people chagning the transaction ID)

1. How is Segwit and the Lightning network connected?

Because the lightning network relies on unconfirmed transactions and segwit madet these a lot less riskier by removing the transaction mallability issue.

1. Are people, wallets and other services forced to use Segwit?

No they are not