Task 1:

One example of a side channel attack is a power analysis attack. Here, the attacker uses the patterns found in power consumption to make educated guesses at the key. Different operations require different amounts of power, which can be analysed to find sensitive data.

Power analysis attacks are effective against cryptographic systems using algorithms like AES or RSA. Especially devices such as smart cards, IoT devices, or embedded systems are vulnerable.

Generally, this side channel aims to leak cryptographic keys or intermediate values found during encryption.

While there haven't been any major real life attacks using power analysis side channels, researchers in the 90s demonstrated such attacks on DES and RSA encrypted smart cards.

There are several fixes one can implement to make such attacks more difficult to pull off. One such method is by using blinding techniques, where random values or "masking operations" are introduced to make deducing information more difficult. Another option is to design algorithms where the power consumption is equal during the entire operation. Finally, some microcontrollers have been designed to limit any amount of power leakage outside the system.

- https://www.allaboutcircuits.com/technical-articles/a-basic-introduction-to-power-based-side-channel-attacks/

Task 2:

Slowloris is a Denial-Of-Service Attack, which works my opening several partial HTTP connections to a server, and then keeping them open by sending further partial HTTP requests. This keeps the HTTP connections from closing, and prevents the server from being able to make real connections.

Other DDoS attacks prevent the server from working by flooding the target with a huge amount of data or traffic. Slowloris, however, uses much less bandwidth. Instead, it targets the server's "connection pool", which makes it easier for the attacker to pull off and harder for the server to detect.

Slowloris has the effect of bringing down webservers using DDoS strategies. This prevents legitimate connection attempts from working, leading to downtime and potential loss of revenue for the website owner.

There are a few way a webserver can secure itself from a Slowloris attack. One option is to increase server availability by allowing a greater number of clients to connect to the server at any one time. Another option is to limit the amount of allowed incoming requests. This includes limiting the amount of connections a single IP address can make, restricting slow connections, or limiting how long a client can stay connected. The use of "load balancers" can also be used to plit up traffic.

One example of a famous Slowloris attack was used during the 2009 Iranian presidential elections on sites ran by the Iranian government.

- https://www.cloudflare.com/en-gb/learning/ddos/ddos-attack-tools/slowloris/
- https://www.imperva.com/learn/ddos/slowloris/