1. XSS (Cross side scripting) attack can be infused by putting the malicious code which gets automatically run in any comment section or feedback section of any webpage, usually a blogging page.
This can hamper the reputation of a site and the attacker may place any private data or personal credentials

→ XSS is a client side code injection attack. The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate webpage or web application.

→ The actual attack occurs when the victim visits the web page or web application that executes the malicious code.

→ The web appl$^n$ becomes a vehicle to deliver the malicious script to the user's browser.

→ Vulnerable vehicles that are commonly used for cross-site scripting attacks are forums, msg boards & web pages that allow comments

2. Firewall.

It is a type of filter in ~~nt~~ n/w security, allowing or disallowing incoming or outgoing activity based on security measures we specify.

→ Firewall performs 2 basic security functions for a n/w. These are known as packet filtering and acting as an application proxy.

Functionality :-

→ A firewalled system analyzes network traffic based on rules. A firewall only welcomes those incoming connections that it has been configured to accept.

→ It does so by allowing or blocking specific data packets — units of communication we send over digital networks — based on pre-established security rules.

3 (i) Spear-phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim.

(ii) Man-in-the Middle (MitM) attack.

(iii) SQL injection

4. The Reserve Bank of India governor, Raghuram Rajan launched 'Sachet' portal, sachet.rbi.org.in to check illegal money collection.

5. Yes, Patching prevents ransomware & malware attacks, as a patch is a piece of code that improves a program

already installed into your system, like as an update, ie if a bug is found on a program already installed on our machine, a patch would be created to fix this issue without the need of reworking the entire code. As patch management has the most critical & obvious benefit is better n/w security. By securing our n/w, we can avoid data theft, legal issues & lasting reputation damage.