Submitted by : Aayushi Bansal

<u>DSC IGDTUW</u>

<u>Cybersecurity</u>

<u>Assignment - 1</u>

<u>Ans.1</u>   Cross site scripting (XSS)

this attack can be infused by putting the malicious code in any comment section or feedback section of webpage. It can hamper the reputation of a website.

XSS attacks use third-party web resources to run scripts in the victim's application. When the victim requests a page from the website, the website transmits the page, with the attacker's payload as part of the HTML body, to the victim's browser.

<u>Ans 2.</u> 'windows defender firewall' is used in operating systems to prevent uninvited network traffic.

- It filters internet traffic coming in and going out of your computer to minimize security risks.
- It prevents unsafe apps from connecting to the internet without your consent, as well as unsolicited external attempts to connect to our network.
- It makes it harder for malware or hackers to attack your system.
- Most computers & networks use IP addresses & ports to connect with each other. A firewall looks at both of these, providing or blocking access based on whether it deems the request safe or not.
- It is especially useful if we use Wi-Fi networks to connect to the internet.

Ans 3.   a) Phishing attack

b) Man-in-the-middle attack

c) SQL attack

Ans 4.   Sachet

URL of the website : www.sachet.rbi.org.in

Ans 5.   A patch is a piece of code that improves a program already installed in the system. It is mostly used by companies to update their softwares to prevent themselves from security breaches. When a company find a vulnerability or a bug in the software, it uses patches to fix the issue without the need of reworking the entire code.

Because patching is used to fix the bugs which are already present in the system, it cannot completely protect the system or software from ransomware or malware attacks.

So instead of using patching for prevention from ransomware or malware attacks, a better practice would be to keep our software & operating system updated always, use secure authentication methods and install a strong anti-virus and firewall on our system.