Rebecca Dias
BE CMPN A
19/18 2027

MIS

Q1]

Zero day attacks are cyber attacks that occur on the same day when a weakness and or vulnerabilities are found in a software system. Hackers who find out will then exploit the vulnerabilities before the developer fixes it.

How to avoid a zero day attack, some ways are listed below:-

① Penetration testing

Before hackers or third parties discover weaknesses and vulnerabilities, you should routinely do penetration testing. Penetration testing services will conduct several tests to find vulnerabilities in the system so that issues can be fixed immediately by the developer.

② use a web application firewall.

Web application firewall (WAF) can protect you from various attacks. WAF will protect your system for any suspicious activity for a time 24 hrs. Every traffic will be checked, and WAF will deny access when finding traffic that indicates a threat.

③   Using the security application.

It is recommended to use a security application that has the following features.

• Anti — malware protection

~~stuue~~ security applications must have features to detect and remove malware threats such as viruses, trojans, worms etc.

• Vulnerability scanning

The application must have the ability to look for vulnerabilities or weakness in the system.