1)Phishing - хакер, маскує свої сайти, повідомлення то що, як надійні сервіси, жертва сама водить свою персональну інфу, тим самим хакер її отримує. Хакер може зробити сайт, подібний на офіційни замінивши в адресі сайту наприклад l на велику, O на 0 то що
2)Back door - шкідливе ПЗ, установлене хакером для отримання віддаленого доступу до системи без авторизації

3)Logic bombs шкідливий код, який переважно вписується або на початок програми, або в кінець. Цей код може вивести програму з ладу

4)DOS - атака з поодинокого джерела. Блокує доступ авторизованим користувачам до пк. Атака проводиться переповненням легального трафіку зовнішніми повідомленнями

5)DDoS-атака (Distributed Denial of Service) - те саме, що і DOS, але з багатьох джерел, пк, ip адрес. Переважно перед тим комп'ютери заражають черв'яками, також можуть атакувати за допомогою ботнету
Ботнет — це комп'ютерна мережа, що складається з деякої кількості хостів, із запущеними ботами — автономним програмним забезпеченням

6)Trojan horse - програми, які містять в собі шкідливий код, але маскуються під звичайні програми, легко зловити при піратстві

7) Virus - програма, яка інфікує файли пк і включає до них спеціальні команди. Команди виконуються, коли завантаженні інфікованого файлу в RAM(оперативну пам'ять). Вірус не може розповсюджуватися сам(на відміну від черв'яків), поширення вимагає втручання, переважно це робить несвідомо користувач, можуть розповсюджуватися через USB-накопичувачі або email. Можуть вплітатися в конфігурацію Windows, шляхом зміни ключових файлів або параметрів реєстру, це дозволяє лишатися вірусу активним після перезавантаження пк і змінювати поведінку ОП. Можуть видаляти/шифрувати файли. Може красти персональну інфу, яка могла бути у файлах. В вірусі може міститися спеціальний код для створення ботнетів для подальших DDOS атак

8)IP-спуфінг (spoof) - хакер використовує ip жертви в своїх цілях

9)Worm - незалежні програми, які можуть поширюватися інтернетом абокопіювати себе на інший пк. Використовують email або вразливості програм

10)vishing - підвид фішингу, який використову телефонні дзвінки

11)sniffer - сканує мережевий трафік для отримання певної інфи: паролі логіни тощо

12)pharming на відміну від phishing ця атака, яка маніпулює DNS таким чином, що ми перенаправляємся на підробку сайту, де можемо ввести свої дані.

13)zero-day Спосіб запобігання кіберзахисту. Загроза реалізується того сямого
дня, коли громадськість дізнасться про наявність у системі безпеки
урязливих місць

14) smishing - атаки, що використовують текстові або SMS-повідомлення для залучення

уваги жертви;

15) whaling - атаки направлені на високопоставлених чинів компаній, директорів тощо

16) SMB Relay - тип атаки який використовує вразливості SMB протоколу. Зловмисник може перехопити інформацію, яка йшла по мережі за допомогою цього протоколу і використати її

17) DNS Spoofing - зловмисник видає себе за DNS-сервер і відправляє відповіді на DNS-запити, які відрізняються від відповідей, відправленими легітивним сервером. Може відправити хибні ip-адреси, хостів і інші види брехливої інфи, використовується для pharming. Зловмисник може перенаправити запити аутентифікації на підроблений сервер, тим самим даючи можливість хакеру ввійти в систему. Для запобігання використовувати: DNSSEC і перевіряти журнали DNS на підозрілу активність

18) DCSync - це тип атаки, у якій зловмисник імітує контролер домену та запитує
реплікацію даних облікового запису AD(Active Directory). Ці дані можуть містити конфіденційну

нформацію, таку як паролі та хеші. Отримавши ці дані, зловмисник може використовувати їх для подальших атак на мережу. Запобігається протоколом LDAP через SL/TLS - шифрує трафік

19) Pass-the-Hash - зловмисник викрадає хеш пароля, потім використовує його для аутентифікації, фактично його не знаючи. Отримують шляхом перехоплення трафіку або доступом до скомпроментованої машини. Щоб запобігти цьому можна використовувати шифрування типу Kerbedos і ізолювати машину, яка постраждала.

20) Password Spraying - Зловмисник намагається увійти в AD за допомогою списку часто

використовуваних паролів, сподіваючись отримати доступ до одного або кількох

облікових записів. Він може використовувати автоматизовані інструменти для перевірки

великої кількості паролів зі списком імен користувачів.

21) Spam - спам

22) MITM Man-in-the-Middle - Коли зловмисник перехоплює канал зв'язку між двома системами, і

отримує доступ до всієї інформації, що передається. Атакуюча сторона

отримує дані авторизації користувача і здійснює журналювання усього сеансу зв’язку, запуск команд

та їх виконання.

23) SSH Brute-force - перебір пароля

24) XXS attack - використовує вразливий сервер для атаки на користувача. Разом з веб-сторінкою, жертва отримує зловмисний код HTML, тим самим хакери можуть вкрасти файли cookies або виконувати інші дії

25) SQL Injection - є одним із найпоширеніших векторів атак, які хакери використовують для крадіжки

даних. Цей тип мережевої атаки поширений на погано розроблені програми та веб-сайти. Оскільки

вони містять уразливі поля для введення користувачів (наприклад, сторінки пошуку та входу, форми

запитів на продукти та підтримку, область коментарів тощо), хакери можуть легко зламати, змінивши

сценарії.

26) Ransom - запуск всередину комп’ютера шкідливого програмного забезпечення,

що шифрує дані або робить їх копію задля подальшого шантажу власника цих даних

і отримання за них викупу. Крім даних, може заблокувати як доступ до всієї

операційної системи, так і до її окремих частин.