Атаки

Опис кібератак

1. **Phishing**
   Атака, що використовує підроблені електронні листи або веб-сайти для обману користувачів із метою викрадення конфіденційної інформації, наприклад, паролів або даних карток. Зловмисник зазвичай маскується під легітимну організацію, щоб отримати довіру жертви.
2. **Backdoor**
   Шкідливий код або програма, яка створює прихований доступ до комп'ютера або мережі, обходячи стандартні механізми автентифікації. Зазвичай використовується для довгострокового доступу до системи без відома її власника.
3. **Logic Bombs**
   Програмний код, що активується при виконанні певних умов, наприклад, у визначений час або за конкретної події, часто для руйнування даних. Може бути вбудований в інше програмне забезпечення та діяти без видимих ознак до певного моменту.
4. **DoS (Denial of Service)**
   Атака, яка перевантажує сервер або систему запитами, унеможливлюючи її нормальну роботу. Мета — зробити ресурси або сервери недоступними для користувачів.
5. **DDoS (Distributed Denial of Service)**
   Розподілена DoS-атака, що використовує велику кількість пристроїв для одночасного перевантаження цілі. Зазвичай здійснюється через ботнети, що складаються з заражених пристроїв.
6. **Trojan Horse**
   Шкідлива програма, яка маскується під легітимне програмне забезпечення, але фактично виконує шкідливі дії, такі як крадіжка даних або надання віддаленого доступу до системи.
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-Spoofing**
   Техніка, за допомогою якої зловмисник підробляє IP-адресу, щоб видавати себе за інший пристрій у мережі. Це може бути використано для обхідної атаки або приховування реального місцезнаходження зловмисника.
9. **Worm**
   Само відтворюваний шкідливий код, що поширюється по мережах без необхідності заражати файли. Може передаватися без участі користувача, автоматично заражаючи нові системи.
10. **Vishing**
    Соціальна інженерія, що використовує телефонні дзвінки для обману жертв із метою викрадення даних, таких як номери кредитних карток або паролі. Зловмисники можуть видавати себе за співробітників банку або інших організацій.
11. **Sniffer**
    Інструмент, що перехоплює мережевий трафік, зокрема для збору конфіденційної інформації, такої як паролі, номери кредитних карток та інші особисті дані.
12. **Pharming**
    Атака, яка перенаправляє користувачів із легітимних вебсайтів на підроблені, навіть якщо введено правильну URL-адресу. Це може статися через зміни в локальних налаштуваннях DNS або на рівні сервера.
13. **Zero-Day**
    Атака, що використовує вразливості програмного забезпечення до того, як виробник випустить виправлення. Такі вразливості називаються "нульовим днем", оскільки про них нічого не відомо до моменту атаки.
14. **Smishing**
    Фішингова атака через текстові повідомлення (**SMS**) для отримання конфіденційної інформації. Повідомлення можуть виглядати як офіційні запити від банків чи інших установ.

15. **Whaling**
    Цільова фішингова атака на **високопосадовців** або керівників організацій. Атаки часто виглядають як важливі бізнес-запити або інструкції від імені топ-менеджменту.
16. **SMB Relay**
    Атака, що перехоплює й повторно використовує автентифікаційні запити протоколу SMB для несанкціонованого доступу. Зловмисник спочатку визначає цільову систему в мережі, яка вразлива до атак SMB Relay, потім перехоплює запити автентифікації SMB від інших систем у мережі. Далі зловмисник передає запит автентифікації на контролер домену в мережі для отримання облікових даних домену для користувача, який спочатку зробив запит на автентифікацію. Маючи доступ до облікових даних домену, зловмисник може виконувати різноманітні зловмисні дії в мережі, наприклад створювати нові облікові записи користувачів, підвищувати привілеї та отримувати доступ до конфіденційних даних.

    Щоб запобігти атакам SMB Relay на Active Directory, необхідно переконатися, що всі системи в мережі оновлені з останніми виправленнями безпеки
17. **DNS Spoofing**
    Атака, що підробляє відповіді DNS-серверів, перенаправляючи користувачів на шкідливі ресурси що дозволяє перехоплювати трафік і потенційно отримувати доступ до конфіденційної інформації.

    У контексті Active Directory, підробка DNS може використовуватися для перенаправлення запитів автентифікації на підроблений сервер, дозволяючи зловмиснику перехоплювати облікові дані для входу.
18. **DCSync**
    це тип атаки, у якій зловмисник імітує контролер домену та запитує реплікацію даних облікового запису AD. Ці дані можуть містити конфіденційну інформацію, таку як паролі та хеші. Отримавши ці дані, зловмисник може використовувати їх для подальших атак на мережу.

    Щоб запобігти атакам DCSync, організації повинні використовувати безпечні протоколи зв’язку, такі як LDAP через SSL/TLS, щоб захистити конфіденційні дані AD під час передачі. Крім того, потрібно використовувати шифрування для захисту конфіденційних даних у стані зберігання, наприклад вмісту бази даних AD

19. **Pass-the-Hash**
    У цьому типі атаки зловмисник викрадає хеш пароля облікового запису AD і використовує його для автентифікації, не знаючи фактичного пароля. Цю атаку можна здійснити шляхом перехоплення мережевого трафіку, доступу до скомпрометованої машини або використання шкідливого програмного забезпечення. Коли зловмисник отримує доступ до облікового запису, він може видати себе за законного користувача та отримати доступ до конфіденційних ресурсів.
20. **Password Spraying**
    Техніка, яка перевіряє один і той самий пароль на великій кількості облікових записів для уникнення блокування. Зловмисник використовує список популярних паролів, сподіваючись, що хоча б один з них буде правильним. Щоб запобігти, організації повинні заохочувати використання надійних паролів і впроваджувати політику блокування облікових записів, яка запобігає атакам підбору. Крім того, багатофакторна автентифікація може ускладнити зловмисникам отримання доступу
21. **Spam**
    Масове розсилання небажаних електронних повідомлень із метою реклами чи шахрайства.
22. **MITM (Man-in-the-Middle)**
    Атака, в якій зловмисник перехоплює та змінює трафік між двома сторонами, залишаючись непоміченим. Мета такої атаки - крадіжка або фальсифікування переданої інформації, або ж отримання доступу до ресурсів мережі. Убезпечити себе можна лише шляхом криптошифрування переданих даних.
23. **SSH Brute-Force**
    Атака методом перебору паролів на SSH-сервер, щоб отримати доступ до віддаленого сервера.
24. **XXS (Cross-Site Scripting) Attack**
    Впровадження шкідливих скриптів у веб-сайти, які виконуються у браузері користувача. Разом із веб-сторінкою, яку завантажує жертва, вона отримує зловмисний код, інтегрований в HTML. Цей код виконує шкідливий сценарій на комп’ютері жертви, наприклад, надсилати хакерам файли cookie з особистими даними користувача.
25. **SQL Injection**
    Цей тип мережевої атаки поширений на погано розроблені програми та веб-сайти оскільки вони містять уразливі поля для введення

користувачів. Атака, що впроваджує шкідливий SQL-код у запити до бази даних для доступу до інформації чи її зміни.

26. **Ransomware**
    Шкідливе ПЗ, 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
27. **Spear Phishing**
    Цільова фішингова атака, спрямована на **конкретну особу** чи організацію. Зловмисники використовують персоналізовані повідомлення, щоб отримати доступ до конфіденційної інформації, наприклад, паролів або фінансових даних.
28. **SEO Attack**
    Зловмисники маніпулюють результатами пошукових систем, щоб шкідливі сайти потрапляли на високі позиції. Це може призвести до зараження комп'ютерів користувачів через фальшиві сайти.
29. **Browser Hooking**
    Атака, де зловмисники впроваджують шкідливі скрипти на вебсайти для викрадення особистих даних користувачів, таких як паролі або банківські реквізити, через браузер.
30. **Source routing specification**
    атака на маршрутизацію, якою має слідувати IP-пакет, можна визначити маршрут так, щоб обійти фаєрвол. Однак зловмисник повинен знати IP-адресу, маску підмережі та настройки шлюзу за замовчуванням, щоб досягти цього.
31. **Miniature fragment attack**
    зловмисник фрагментує IP-пакет на менші частини і пропускає їх через фаєрвол, з надією, що буде перевірено лише першу частину фрагментованих пакетів, а інші пройдуть без перевірки.