SSH Brute-force.

Однією з найпопулярніших атак є атака методом перебору паролів. Якщо запустити сервіс SSH, доступ до якого можливий з Інтернету, то в журналі автентифікації користувачів можна спостерігати багато записів невдалого підключення користувача admin/root, так начебто він постійно вводить невірний пароль. Саме так і виглядає атака методом перебору паролів, більш відома як bruteforce.

MITM Man-in-the-Middle

З англ. «Людина посередині». Коли зловмисник перехоплює канал зв'язку між двома системами, і отримує доступ до всієї інформації, що передається. Мета такої атаки - крадіжка або фальсифікування переданої інформації, або ж отримання доступу до ресурсів мережі Тому в чисто технічному плані убезпечити себе можна лише шляхом криптошифрування переданих даних. Атакуюча сторона отримує дані авторизації користувача і здійснює журналювання усього сеансу зв’язку, запуск команд та їх виконання.

Міжсайтовий скріптинг (XXS).

Цей поширений тип атак використовує шкідливий код для запуску певного сценарію у веб-браузері або програмі. Специфіка подібних атак полягає в тому, що замість безпосередньої атаки на сервер зловмисники використовують вразливий сервер для атаки на користувача. Разом із веб-сторінкою, яку завантажує жертва, вона отримує зловмисний код, інтегрований в HTLM. Цей код продовжує виконувати шкідливий сценарій на комп’ютері жертви, наприклад, надсилати хакерам файли cookie з особистими даними користувача.

SQL Injection

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.

whaling - атаки, спрямовані на керівників вищої ланки;

smishing - атаки, що використовують текстові або SMS-повідомлення для залучення уваги жертви;

«Розпилення» пароля (Password Spraying) є одним із найпоширеніших типів атак на Active Directory. 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. Отримавши доступ до облікового запису, зловмисники потенційно можуть викрасти конфіденційну інформацію або встановити зловмисне програмне забезпечення на скомпрометованій машині. Щоб запобігти атакам з «розпиленням» паролів, 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 до облікових запи-сів, навіть якщо вони мають правильний пароль.

Pass-the-Hash.

У цьому типі атаки зловмисник викрадає хеш пароля облікового запису AD і використовує його для автентифікації користувача, 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 конфіден-ційних ресурсів. Щоб запобігти атакам передачі хешу, організації повинні використовувати надійні алгоритми шифрування для захисту хешів паролів, наприклад шифрування Kerberos. Вони також повинні використовувати ізоляцію домену, щоб запобігти доступу зловмисників до інших машин у мережі після того, як вони скомпроме-тували одну машину.DNS-спуфінг (DNS Spoofing) – це тип атаки, під час якої зловмисник перенаправляє DNS-запити на підро-блений сервер, що дозволяє йому 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. Для того, щоб запобігти атакам DNS-спуфінгу, слід запровадити безпечні протоколи DNS, наприклад DNSSEC, і регулярно перевіряти свої журнали DNS на наявність підозрілої активності.

Атака DCSync – це тип атаки, у якій зловмисник імітує контролер домену та запитує реплікацію даних обліко-вого 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

SMB Relay – це тип атаки, яка використовує слабкість у протоколі SMB (Server Message Block), який вико-ристовується системами Windows для спільного використання файлів і принтерів. Атака працює шляхом перехо-плення та передачі запитів автентифікації SMB між клієнтом і цільовим сервером. 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 отри-мання 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 ство-рювати 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. Крім того, потрібно запровадити сегментацію мережі та контроль доступу, щоб обмежити поширення атак. Також необхідно відстежувати мережевий трафік на наявність ознак атак SMB Relay, таких як численні запити автентифікації з однієї IP-адреси, та використовувати такі технології, як підпи-сання SMB і шифрування SMB

Ransomware — 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.

Mimikatz – це інструмент, який дозволяє зловмиснику отримувати з пам’яті чисті текстові паролі, хеші та інші облікові дані автентифікації. Його також можна використовувати для підвищення привілеїв і виконання команд у скомпрометованій системі.

Bloodhound – інструмент, який допомагає визначати вразливості в середовищах Active Directory. Він відображає зв’язки між користувачами, групами, комп’ютерами та іншими ресурсами в межах домену, що допомагає зловмисникам визначити потенційні шляхи для проведення атаки.

Empire – це пост-експлуатаційний інструмент, який дозволяє зловмисникам контролювати скомпрометовані системи та виконувати різні дії, такі як: виконання команд, завантаження та завантаження файлів, а також перехід до інших систем.

CrackMapExec – це інструмент тестування на проникнення, який дозволяє зловмисникам перевіряти безпеку середовищ Active Directory, виконуючи різні атаки, такі як «розпилення» пароля, передача хешу та атаки Golden Ticket.

Nmap – це популярний інструмент відображення мережі та сканування портів, який можна використовувати для визначення відкритих портів і служб у системах у мережі. Його можна використовувати для прослуховування мережі, щоб зібрати інформацію про середовище Active Directory та виявити потенційні вразливості.

Metasploit – це фреймворк для тестування на проникнення, який включає низку інструментів для використання вразливостей у системах. Він містить модулі для атак на середовища Active Directory, такі як атака SMB relay, яка дозволяє зловмисникам перехоплювати та ретранслювати запити автентифікації SMB, щоб отримати доступ до системи жертви.

Responder – це інструмент, який можна використовувати для отримання облікових даних із систем у мережі. Він працює шляхом підробки мережевих служб і захоплення облікових даних, надісланих системами, які намагаються автентифікуватися за допомогою цих служб. Це можна використовувати для збору облікових даних для облікових записів Active Directory.

PowerUp – це сценарій PowerShell, який використовується для підвищення привілеїв у середовищах Windows. Він містить модулі для виявлення неправильно налаштованих ACL, пошуку шляхів обслуговування та виявлення інших уразливостей, які можна використати для отримання вищих привілеїв у Active Directory.

LaZagne – інструмент відновлення пароля, який можна використовувати для вилучення паролів, що зберігаються в системі. Він містить модулі для відновлення паролів, що зберігаються в різних програмах і службах, у тому числі тих, що використовуються Active Directory, наприклад у файлі NTDS.dit