Махницький О.В. – старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ.

ВИКОРИСТАННЯ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ДЛЯ КРАДІЖКИ ОСОБИСТИХ ДАНИХ

Сама слабка ланка в ланцюзі інформаційної безпеки - це людина. Використовуючи соціальну інженерію зловмисники отримують доступ до конфіденційних даних користувачів. Розглянемо, як саме це відбувається. Але для початку розберемося з самим поняттям соціальної інженерії.

Соціальна інженерія - метод отримання необхідного доступу до інформації, заснований на особливостях психології людей. Основною метою соціальної інженерії є отримання доступу до конфіденційної інформації, паролів, банківських даних і інших захищених систем. Термін соціальна інженерія з'явився не так давно, але сам метод отримання інформації таким чином використовується досить давно. Співробітники силових і відомчих структур, які хотіли б залучити деяку державну таємницю, використання політтехнологій, та й ми самі, при бажанні отримати щось, часто навіть не розуміючи цього, використовуємо методи соціальної інженерії.

Загальні типи соціальної інженерії та методи захисту від них.

Претекстінг - це набір дій, відпрацьованих за певним, заздалегідь складеним сценарієм, в результаті якого жертва може видати будь-яку інформацію або вчинити певну дію. Найчастіше даний вид атаки передбачає використання голосових засобів, таких як Skype, телефон і т.п.

Для використання цієї техніки зловмисникові необхідно спочатку мати деякі дані про жертви (ім'я співробітника; посаду; назва проектів, з якими він працює; дату народження). Зловмисник спочатку використовує реальні запити з ім'ям співробітників компанії і, після того як увійде в довіру, отримує необхідну йому інформацію.

Фішинг – техніка інтернет - шахрайства, спрямована на отримання конфіденційної інформації користувачів – авторизаційних даних різних систем. Основним видом фітингових атак є підроблений лист, відправлений жертві по електронній пошті, який виглядає як офіційний лист від платіжної системи або банку. У листі міститься форма для введення персональних даних (пін-код, логін і пароль і т.п.) або посилання на web-сторінки, де розташовується така форма. Причини довіри жертви до подібних сторінок можуть бути різні: блокування облікового запису, поломка в системі, втрата даних та інше.

Троянський кінь - це техніка ґрунтується на цікавості, страху або інших емоціях користувачів. Зловмисник відправляє лист жертві за допомогою електронної пошти, як додаток до якого знаходиться «оновлення» антивірусу, ключ до грошового виграшу або компромат на співробітника. Насправді ж у вкладенні знаходиться шкідлива програма, яка

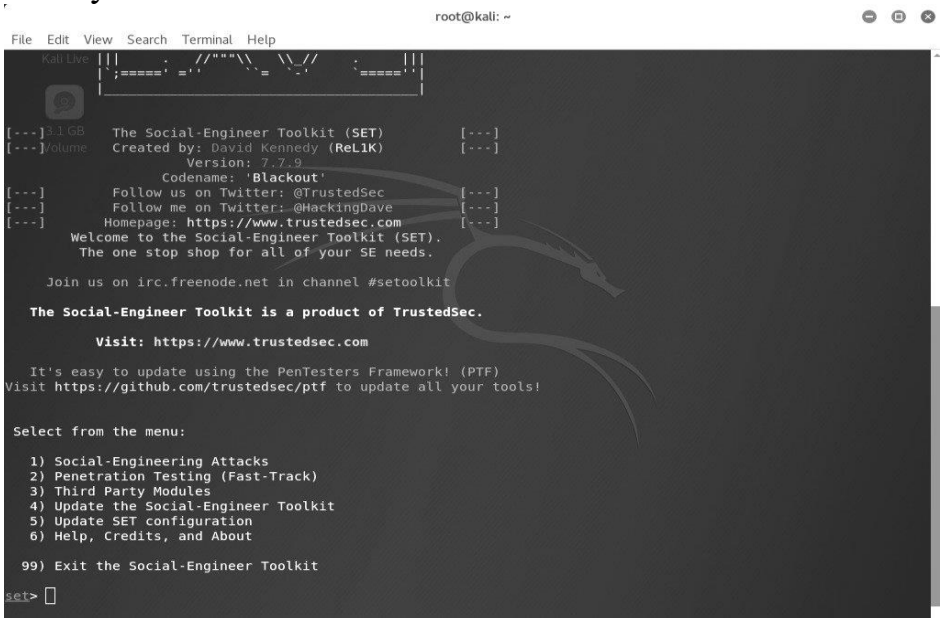
після того, як користувач запустить її на своєму комп'ютері, буде використовуватися для збору або заміни інформації зловмисником.

Кви про кво (послуга за послугу) - дана техніка передбачає звернення зловмисника до користувача по електронній пошті або корпоративному телефону. Зловмисник може представитися, наприклад, співробітником технічної підтримки та інформувати про виникнення технічних проблем на робочому місці. Далі він повідомляє про необхідність їх усунення. У процесі «рішення» такої проблеми, зловмисник підштовхує жертву на вчинення дій, що дозволяють атакуючому виконати певні команди або встановити необхідне програмне забезпечення на комп'ютері жертви.

Дорожнє яблуко - цей метод є адаптацію троянського коня і полягає у використанні фізичних носіїв (CD, флеш-накопичувачів). Зловмисник зазвичай підкидає такий носій в загальнодоступних місцях на території компанії (парковки, столові, робочі місця співробітників, туалети). Для того, щоб у співробітника виник інтерес до даного носія, зловмисник може нанести на носій логотип компанії і якусь підпис. Наприклад, «дані про продажі», «зарплата співробітників», «звіт в податкову» і інше.

Зворотна соціальна інженерія - даний вид атаки спрямований на створення такої ситуації, при якій жертва змушена буде сама звернеться до зловмисника за «допомогою». Наприклад, зловмисник може вислати лист з телефонами і контактами «служби підтримки» і через деякий час створити оборотні неполадки в комп'ютері жертви. Користувач в такому випадку подзвонить або зв'яжеться по електронній пошті із зловмисником сам, і в процесі «виправлення» проблеми зловмисник зможе отримати необхідні йому дані.

Далі розглянемо, один з найпотужніших і універсальних інструментів, соціальної інженерії. Він має назву Social-Engineer Toolkit, його загальний вигляд на малюнку 1.



Мал.1. Загальний вид інструменту Social-Engineer Toolkit.

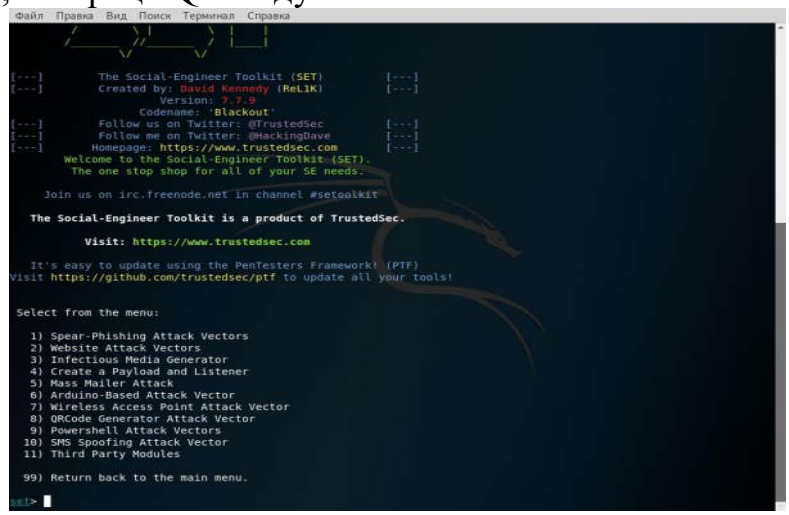
Основні напрямки використання інструменту.

Соціально-технічні атаки.

Розділ включає в себе список векторів для атак:

- Вектори атаки веб-сайтів.
- інфекційний медіа генератор.
- Створення корисного навантаження і слухача.
- масова атака.
- Вектор атаки на основі Arduino.
- Вектор атаки бездротової точки доступу.
- Вектор атаки генератора QRCode.
- Вектори атаки Powershell.

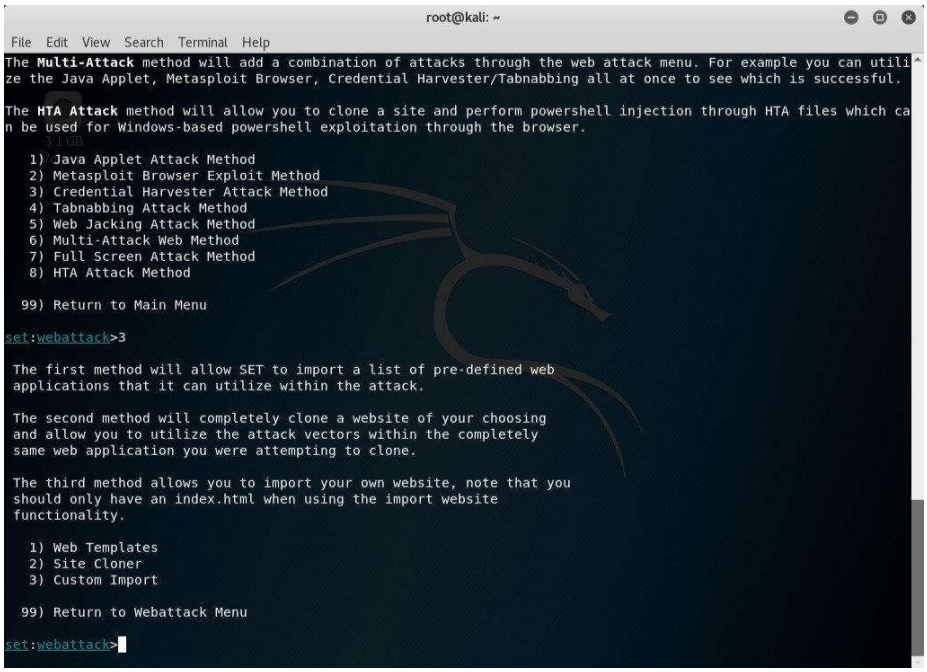
Сам розділ може працювати в декількох напрямках, починаючи від створення і впровадження шкідливих навантажень, масових атак, атак на різні точки Wi-Fi, генерації QR-коду та інше.



Мал. 2. Розділи соціально-технічної атаки в Social-Engineer Toolkit

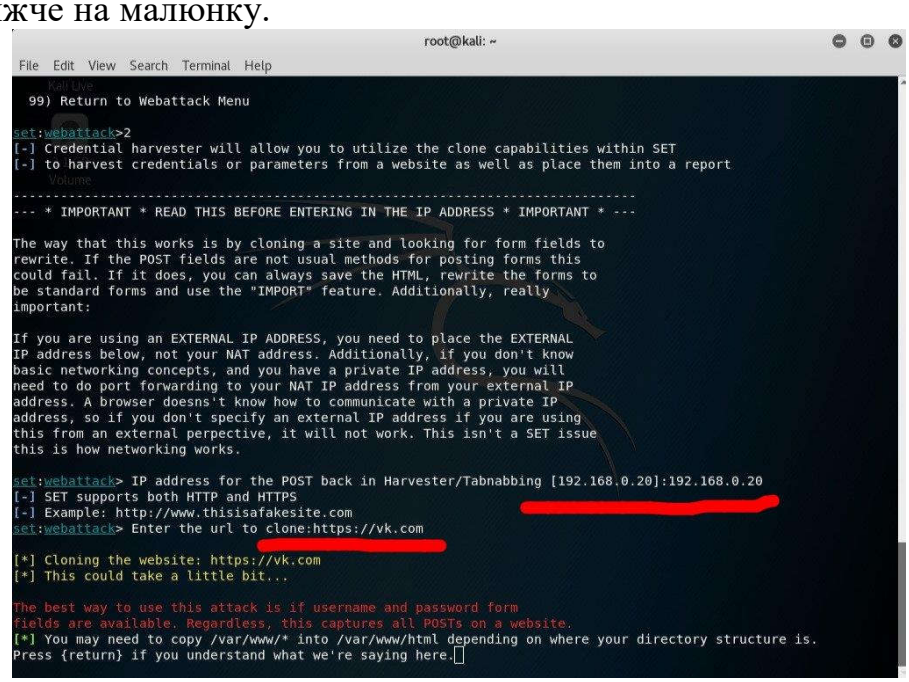
Далі розглянемо, як це працює на практиці.

Припустимо, зловмисникові необхідно зібрати дані про конкретну жертву, дізнатися логіни, паролі та мати доступ до всієї листуванні. Значить, для цього він використовує метод атаки на харвестер (тобто на збір інформації). Кіберзлочинець надходить наступним чином: вибирає пункт Social-Engineering Attacks (Соціально-технічні атаки), потім – Website Attack Vectors (Вектори веб-сайтів), після цього – Credential Harvester Attack Method (Спосіб атаки на харвестер). З'явиться три пункти меню: 1) Шаблони веб сайтів; 2) Клонування сайтів; 3) для користувача імпорт.



Мал. 3. Харвестерні тип вибір вектора атаки

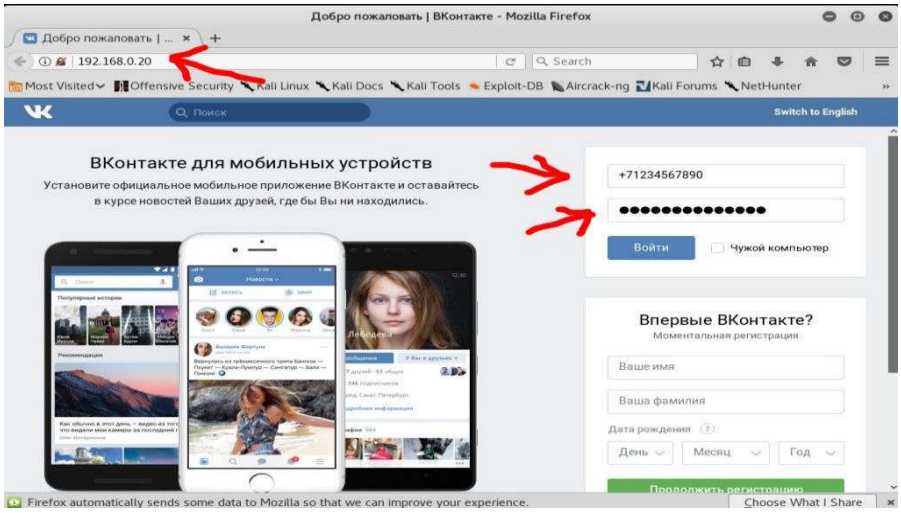
Далі зловмисник дізнається тип своєї мережевої адреси, так Social-Engineer Toolkit знатиме, куди перенаправляти всю зібрану інформацію. Для цього вводиться команда ifconfig. В даному випадку це адреса 192.168.0.20 (IP-адреса, що присвоюється вашому інтерфейсу) - його зловмисник буде клонувати і надалі атакувати. Приклад з соціальною мережею ВКонтакте показаний нижче на малюнку.



Мал. 4. Введення мережевого адреси і клонування сайту для атаки

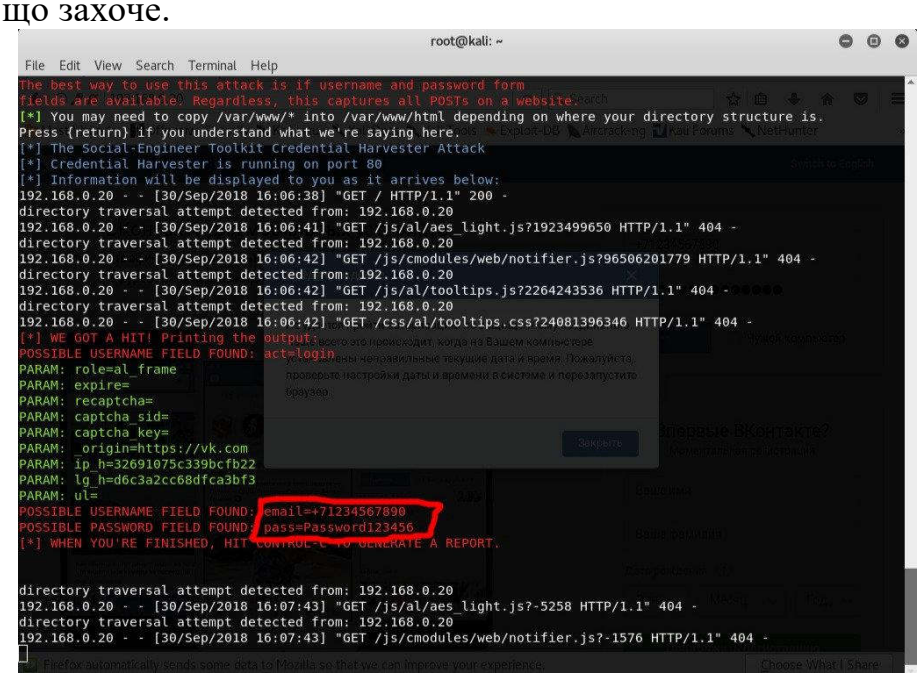
Після завершення конфігурації зловмисник використовує стандартний сервіс для конвертації посилання і відправляє її жертві. Зазвичай

надсилається посилання на фото або цікавий контент від імені друга або колеги. Після переходу за посиланням користувач бачить знайомий інтерфейс. Однак подивившись в адресний рядок, можна звернути увагу, що замість звичного адреси там зазначено той самий 192.168.0.20 Через неуважність багато хто просто не звертають на це увагу і вводять свої логін і пароль.



Мал. 5. Вид підробленої сторінки

Після введення своїх конфіденційних даних система пропонує жертві зайти пізніше, нібито стався якийсь збій або пара логін-пароль не розпізнає. Що ж тим часом бачить зловмисник? Логін і пароль, які ввела жертва. Тим самим він придбав повний доступ і тепер може вводити логін і пароль користувача сервісу, під його профілем входити в його акаунт і здійснювати в ньому все, що захоче.



Мал. 6. Кінцевий результат - зловмисник отримує логін і пароль.

Не виключено, що останні події, пов'язані з витоком персональних даних співробітників Ощадбанку , мали місце завдяки цьому інструменту. Він відмінно підходить для такого типу атаки, і з його допомогою можна також проводити масову розсилку клієнтам Ощадбанку від імені співробітників, чия база вже знаходиться в руках зловмисників. В цілому, Social-Engineer Toolkit - потужний інструмент, яким поки немає рівних. У більш ранніх версіях була функція відправки SMS від імені будь-якого абонента і будь-якої організації, але пізніше розробники відключили модуль. І якби він діяв в даний час, то проникнення в систему було б набагато легше, оскільки SMS-підтвердження як додатковий захист зараз поширене

Метод соціальної інженерії - це тонке мистецтво. Оволодівши їм, можна бути впевненим, що бажаний результат буде отримано в 90-95% - все залежить від кмітливості зловмисника і від підходу до певної жертві. Як правило, на цю вудку трапляються неуважні люди, які не так вимогливі до власної безпеки і рідко звертають увагу на незначні на перший погляд деталі (посилання в браузерному рядку, текст та інше). Слід зазначити, що досвідчені користувачі теж потрапляють на це, хоча і рідше.

Як же уникнути подібних неприємностей? Якщо ви використовуєте соціальні мережі для спілкування, то обов'язково крім введення логіну і паролю використовуйте двофакторну аутентифікацію, тим самим ви створите складність зловмисникові для проникнення в ваш профіль.

Уважно дивіться на посилання в браузерному рядку - як правило, він дуже схожий з оригіналом, різниця в парі букв або цифр. Так що неуважний користувач може і не помітити обману. Завжди краще перевірити ще раз, якщо є можливість: як правило, офіційні сайти справжніх організацій знаходяться на самому першому рядку пошукових систем. Якщо вам прийшла підозріла посилання або прохання від одного, подруги, колеги, то не полінуйтеся зв'язатися з адресатом іншим способом і уточнити, чи він її надіслав. Будьте пильні, бережіть свої дані.

Мирошниченко В.О. - доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат технічних наук, доцент

ДЕЯКІ АСПЕКТИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ У ДЕРЖАВАХ ЄВРОПЕЙСЬКОГО СОЮЗУ

Без сумніву, можна стверджувати, що інформаційно-комунікаційні технології мають фундаментальний вплив на суспільство. У цьому сенсі можливості "інформаційного суспільства" є важливими для економічного зростання, освіти, конкуренції, комунікації та інформаційного обміну, можливостей мобільності та працевлаштування. Однак суспільство постійно